Gestion du réseau

ONTAP 9

NetApp
February 13, 2026

This PDF was generated from https://docs.netapp.com/fr-fr/ontap/networking/networking_reference.html on February 13, 2026. Always check docs.netapp.com for the latest.

Sommaire

Gestion du réseau

Commencez

Visualiser le réseau ONTAP à l'aide de System Manager

Depuis la version ONTAP 9.8, System Manager affiche un graphique présentant les composants et la configuration de votre réseau, ce qui vous permet d'afficher les chemins de connexion réseau entre les hôtes, les ports, les SVM, les volumes, etc. Depuis la version ONTAP 9.12.1, vous pouvez afficher l'association de la LIF et du sous-réseau sur la grille des interfaces réseau.

Le graphique s'affiche lorsque vous sélectionnez **réseau > vue d'ensemble** ou lorsque vous sélectionnez → dans la section **réseau** du tableau de bord.

Les catégories de composants suivantes sont indiquées sur le graphique :

- Hôtes
- Ports de stockage
- Interfaces réseau
- Machines virtuelles de stockage
- Composants d'accès aux données

Chaque section fournit des informations supplémentaires que vous pouvez placer le curseur de la souris sur ou sélectionner pour effectuer des tâches de gestion et de configuration du réseau.

Si vous utilisez le Gestionnaire système classique (disponible uniquement dans ONTAP 9.7 et versions antérieures), reportez-vous à la section "Gestion du réseau".

Exemples

Voici quelques exemples des nombreuses façons dont vous pouvez interagir avec le graphique pour afficher des détails sur chaque composant ou lancer des actions pour gérer votre réseau :

- Cliquez sur un hôte pour afficher sa configuration : les ports, les interfaces réseau, les machines virtuelles de stockage et les composants d'accès aux données qui lui sont associés.
- Passez la souris sur le nombre de volumes d'une VM de stockage pour sélectionner un volume pour en afficher les détails.
- Sélectionnez une interface iSCSI pour afficher ses performances la semaine dernière.
- Cliquez sur ⋮ en regard d'un composant pour lancer des actions de modification de ce composant.
- Déterminez rapidement l'emplacement des problèmes dans votre réseau, indiqué par un « X » à côté de composants défectueux.

Vidéo de visualisation réseau de System Manager

En savoir plus sur les composants réseau d'un cluster ONTAP

Vous devez vous familiariser avec les composants réseau d'un cluster avant de configurer ce dernier. La configuration des composants de mise en réseau physique d'un cluster en composants logiques offre la flexibilité et la fonctionnalité de colocation d'ONTAP.

Les différents composants réseau d'un cluster sont les suivants :

- Ports physiques

  Les cartes réseau (NIC) et les adaptateurs de bus hôte (HBA) fournissent des connexions physiques (Ethernet et Fibre Channel) de chaque nœud aux réseaux physiques (gestion et réseaux de données).

  Pour connaître la configuration requise du site, les informations de switch, le câblage des ports et le câblage du port intégré du contrôleur, consultez le Hardware Universe à l'adresse "hwu.netapp.com".

- Ports logiques

  Les réseaux locaux virtuels (VLAN) et les groupes d'interfaces constituent les ports logiques. Les groupes d'interfaces traitent plusieurs ports physiques comme un seul port, tandis que les VLAN divisent un port physique en plusieurs ports distincts.

- Les IPspaces

  Les IPspaces permettent de créer un espace d'adresse IP distinct pour chaque SVM dans un cluster. Ainsi, les clients se trouvant dans des domaines réseau distincts d'un point de vue administratif peuvent accéder aux données du cluster tout en utilisant des adresses IP redondantes à partir de la même plage de sous-réseaux.

- Les domaines de diffusion

  Un broadcast domain resgrand dans un IPspace et contient un groupe de ports réseau, potentiellement depuis plusieurs nœuds du cluster, qui appartiennent au même réseau de couche 2. Les ports du groupe sont utilisés dans un SVM pour le trafic de données.

- Sous-réseaux

  Un sous-réseau est créé au sein d'un domaine de diffusion et contient un pool d'adresses IP appartenant au même sous-réseau de couche 3. Ce pool d'adresses IP simplifie l'allocation d'adresses IP lors de la création de LIF.

- Interfaces logiques

  Une interface logique (LIF) est une adresse IP ou un WWPN (World port Name) associé à un port. Il est associé à des attributs tels que les groupes de basculement, les règles de basculement et les règles de pare-feu. Une LIF communique sur le réseau par l'intermédiaire du port (physique ou logique) auquel elle est actuellement liée.

  Les différents types de LIF d'un cluster sont des LIFs de données, des LIFs de management du cluster-scoped, des LIFs de management du nœud-scoped, des LIFs intercluster et des LIFs de cluster. La propriété des LIFs dépend du SVM où réside la LIF. Les LIF de données sont détenues par des SVM de données, des LIF de gestion « node-scoped », un système de gestion Cluster-scoped et des LIF intercluster sont au sein des SVM admin, et des LIF de cluster appartiennent au SVM.

- Zones DNS

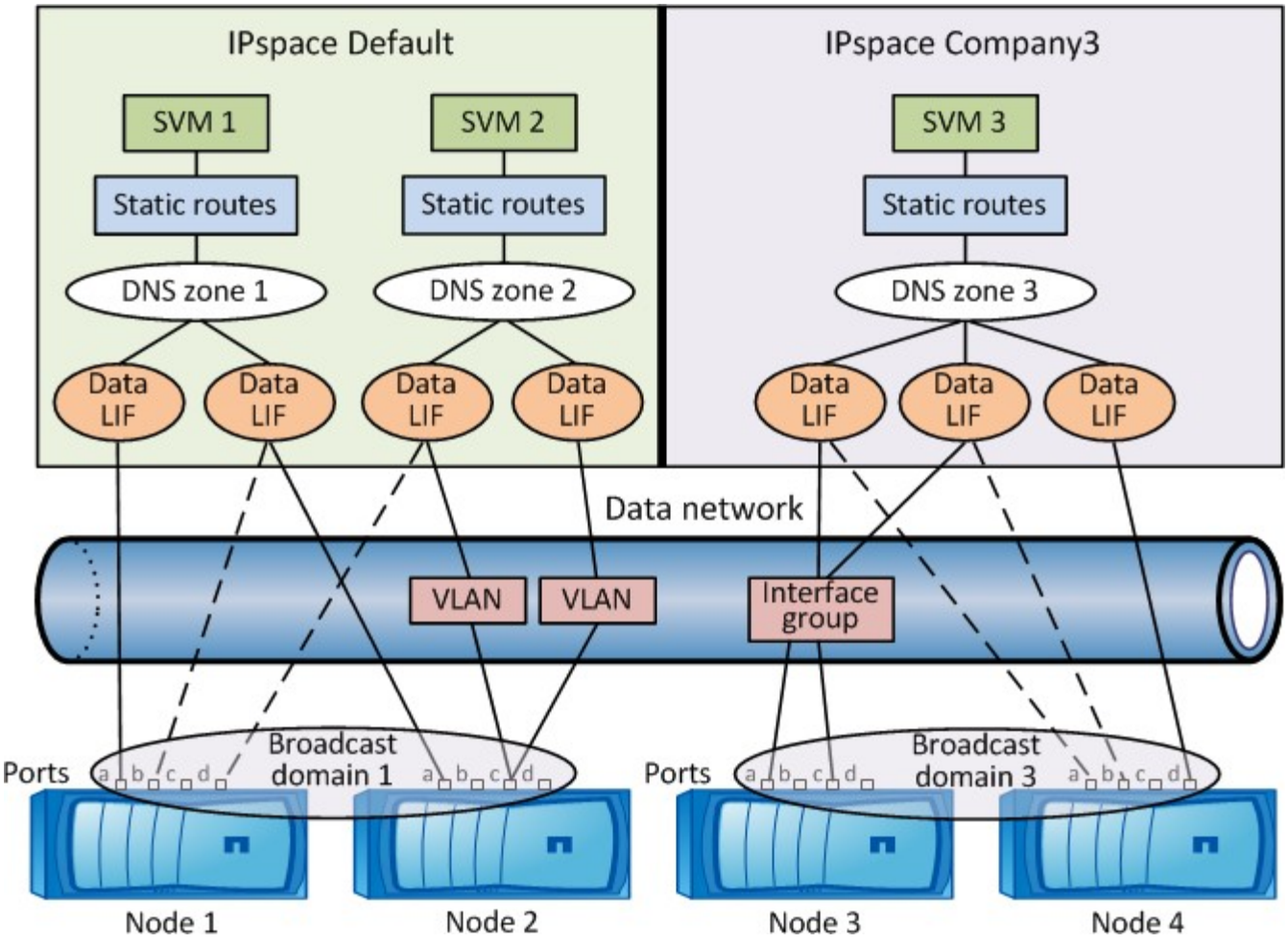
  La zone DNS peut être spécifiée lors de la création de la LIF, ce qui fournit un nom à exporter via le serveur DNS du cluster. Plusieurs LIF peuvent partager le même nom, ce qui permet à la fonctionnalité d'équilibrage de la charge DNS de distribuer les adresses IP pour le nom en fonction du chargement.

  Les SVM peuvent avoir plusieurs zones DNS.

- Routage

  Chaque SVM est autonome en matière de mise en réseau. Un SVM possède des LIFs et des routes qui peuvent atteindre chacun des serveurs externes configurés.

  La figure suivante montre comment les différents composants réseau sont associés dans un cluster à quatre nœuds :

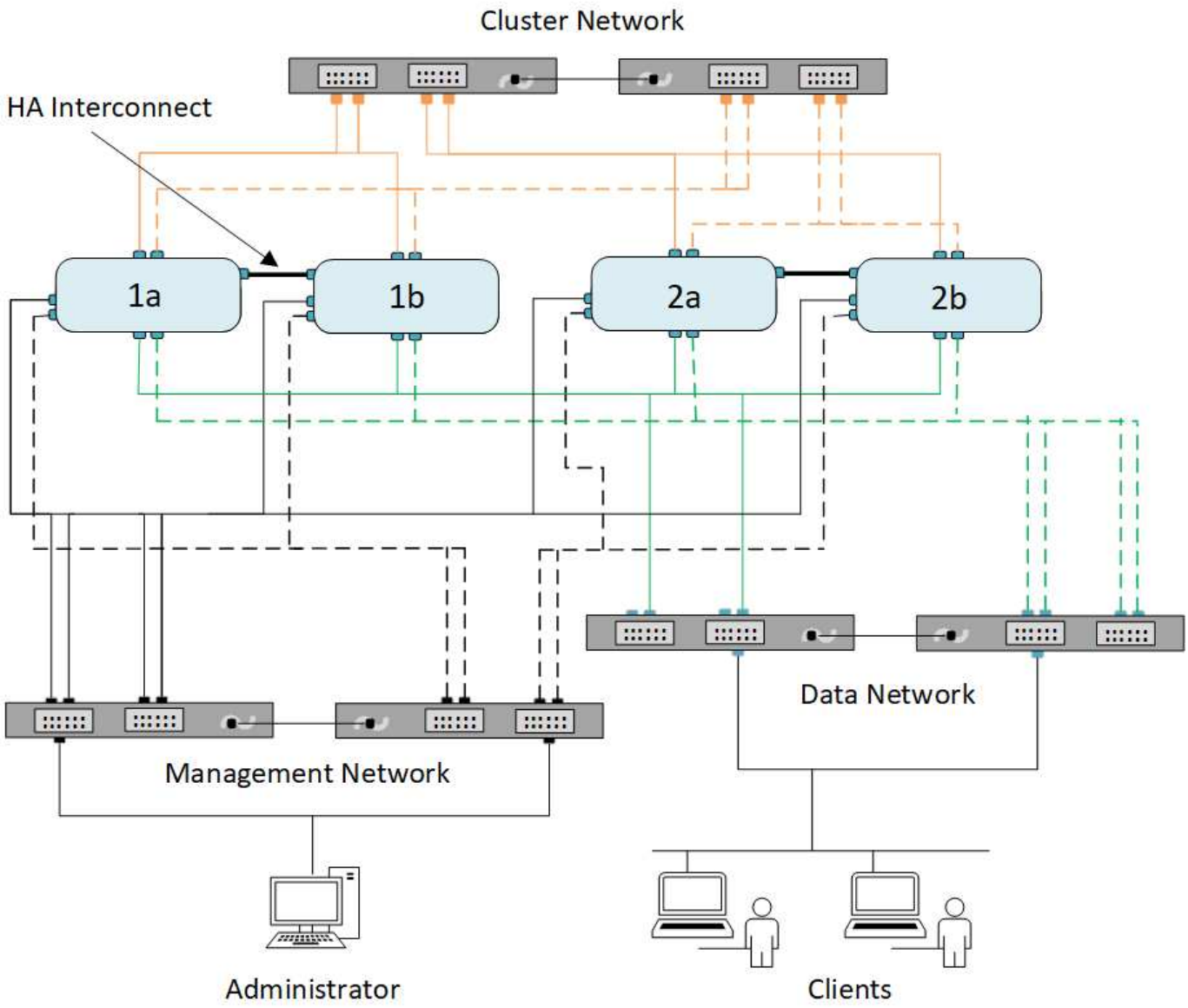


Meilleures pratiques pour le câblage réseau ONTAP

Les meilleures pratiques en matière de câblage réseau séparent le trafic sur les réseaux suivants : cluster, gestion et données.

Vous devez câbler un cluster de manière à ce que le trafic du cluster se trouve sur un réseau distinct de tout autre trafic. Le trafic de gestion de réseau est séparé du trafic de données et du trafic intracluster, mais cette pratique est facultative. La maintenance de réseaux distincts permet d'obtenir de meilleures performances, une administration simplifiée et une meilleure sécurité et gestion de l'accès aux nœuds.

Le schéma suivant illustre le câblage réseau d'un cluster HA à quatre nœuds qui comprend trois réseaux distincts :



Vous devez suivre certaines directives lors du câblage des connexions réseau :

- Chaque nœud doit être connecté à trois réseaux distincts.

  Un réseau est destiné à la gestion, un autre à l'accès aux données et une autre à la communication intracluster. Les réseaux de données et de gestion peuvent être séparés de façon logique.

- Vous pouvez disposer de plusieurs connexions réseau de données à chaque nœud pour améliorer le flux de trafic client (données).
- Un cluster peut être créé sans connexions réseau de données, mais il doit inclure une connexion d'interconnexion de cluster.
- Il doit toujours y avoir deux connexions de cluster ou plus à chaque nœud.

Pour plus d'informations sur le câblage réseau, reportez-vous au "Centre de documentation du système AFF et FAS" et le "Hardware Universe".

Détermination de la politique de basculement de LIF à utiliser dans un réseau ONTAP

Les domaines de diffusion, les groupes de basculement et les règles de basculement fonctionnent ensemble afin de déterminer quel port reprendre le contrôle lorsque le nœud ou le port sur lequel une LIF est configurée tombe en panne.

Un broadcast domain répertorie tous les ports accessibles sur le même réseau Ethernet de couche 2. Un paquet de diffusion Ethernet envoyé à partir de l'un des ports est visible par tous les autres ports du domaine de diffusion. Cette caractéristique de reachbilité commune d'un broadcast domain est importante pour les LIFs car si une LIF devait basculer vers n'importe quel autre port du broadcast, elle pourrait toujours atteindre tous les hôtes locaux et distants accessibles depuis le port d'origine.

Les Failover Groups regroupent les ports d'un broadcast domain capable de procurer le failover de LIF les uns pour les autres. Chaque broadcast domain dispose d'un failover group qui inclut tous ses ports. Ce failover group contenant l'ensemble des ports du broadcast domain est le Default et recommandé pour le LIF. Vous pouvez créer des groupes de basculement avec des sous-ensembles plus petits que vous définissez, par exemple un groupe de ports de basculement dont la vitesse de liaison est identique au sein d'un domaine de diffusion.

Une politique de basculement détermine la façon dont une LIF utilise les ports d'un failover group lorsqu'un nœud ou un port tombe en panne. Considérez la stratégie de basculement comme un type de filtre appliqué à un groupe de basculement. Les cibles de basculement d'une LIF (l'ensemble des ports vers lesquels une LIF peut basculer) sont déterminées en appliquant la politique de basculement de la LIF au failover group de la LIF dans le broadcast domain.

Vous pouvez afficher les cibles de basculement d'une LIF à l'aide de la commande CLI suivante :

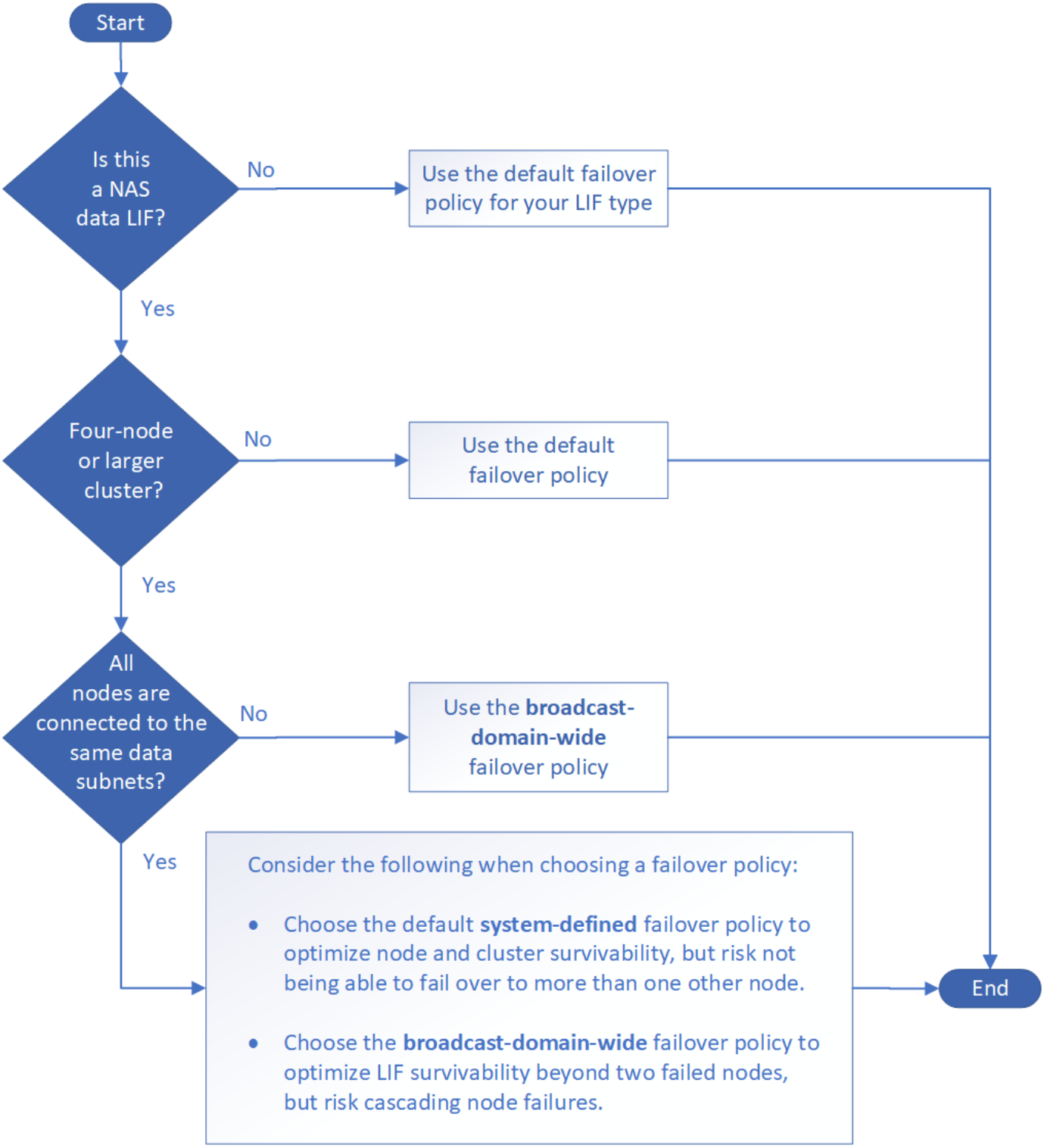
```
network interface show -failover
```

NetApp recommande fortement d'utiliser la stratégie de basculement par défaut pour votre type de LIF.

Décider de la règle de basculement LIF à utiliser

Vous pouvez choisir d'utiliser la stratégie de basculement par défaut recommandée ou de la modifier en fonction de votre type et de votre environnement LIF.

Arbre de décision de stratégie de basculement



Stratégies de basculement par défaut par type de LIF

Type de LIF	Règle de basculement par défaut	Description
Les LIF BGP	désactivé	La LIF ne bascule pas vers un autre port.
LIF de cluster	local uniquement	La LIF bascule vers les ports du même nœud uniquement.

LIF Cluster-mgmt	broadcast-domain-large	La LIF bascule vers les ports du même broadcast domain, sur n'importe quel nœud du cluster.
LIF intercluster	local uniquement	La LIF bascule vers les ports du même nœud uniquement.
LIF de données NAS	défini par le système	LIF bascule vers un autre nœud qui n'est pas le partenaire de haute disponibilité.
LIF node management	local uniquement	La LIF bascule vers les ports du même nœud uniquement.
LIF de données SAN	désactivé	La LIF ne bascule pas vers un autre port.

La règle de basculement « sfo-partenaire uniquement » n'est pas une valeur par défaut, mais elle peut être utilisée pour le basculement de la LIF vers un port du nœud de rattachement ou du partenaire SFO uniquement.

Informations associées

- "interface réseau affiche"

Workflow de basculement de chemin NAS

Configurez le basculement de chemin NAS sur le réseau ONTAP

Si vous connaissez déjà les concepts de base de la mise en réseau, vous pourrez peut-être gagner du temps en configurant votre réseau en consultant ce flux de travail pratique pour la configuration du basculement de chemin NAS.

Le workflow de configuration du basculement de chemin NAS est différent dans ONTAP 9.7 et les versions antérieures. Si vous devez configurer le basculement NAS sur un réseau exécutant ONTAP 9.7 ou une version antérieure, reportez-vous au workflow "Workflow de basculement de chemin NAS (ONTAP 9.7 et versions antérieures)".

Une LIF NAS migre automatiquement vers un port réseau survivant après une panne de liaison sur son port actuel. Vous pouvez utiliser les valeurs par défaut de ONTAP pour gérer le basculement de chemin.

Une LIF SAN ne migre pas (sauf si vous la déplacez manuellement après l'échec de la liaison). La technologie de chemins d'accès multiples sur l'hôte achemine le trafic vers une autre LIF. Pour plus d'informations, voir "Administration SAN".

1 **"Remplissez la feuille de travail"**

Utilisez la fiche pour planifier le basculement de chemin NAS.

2 **"Créez les IPspaces"**

Créer un espace d'adresse IP distinct pour chaque SVM d'un cluster.

3 **"Déplacez les domaines de diffusion vers les IPspaces"**

Déplacer les domaines de diffusion dans les IPspaces.

4 **"Créer des SVM"**

Création des SVM pour le service de données aux clients.

5 **"Créez des LIF"**

Créez des LIF sur les ports que vous souhaitez utiliser pour accéder à des données.

6 **"Configurer les services DNS pour le SVM"**

Configurer les services DNS pour le SVM avant de créer un serveur NFS ou SMB.

Fiche technique pour le basculement de chemin NAS sur le réseau ONTAP

Avant de configurer le basculement du chemin NAS, vous devez remplir toutes les sections de la fiche technique.

Les informations relatives au basculement NAS sur le réseau ONTAP sont différentes dans ONTAP 9.7 et les versions antérieures. Si vous devez configurer le basculement NAS sur un réseau exécutant ONTAP 9.7 ou une version antérieure, reportez-vous à la section "Fiche technique pour la configuration de basculement de chemin NAS (ONTAP 9.7 et versions antérieures)".

Configuration IPspace

Les IPspaces permettent de créer un espace d'adresse IP distinct pour chaque SVM dans un cluster. Ainsi, les clients se trouvant dans des domaines réseau distincts d'un point de vue administratif peuvent accéder aux données du cluster tout en utilisant des adresses IP redondantes à partir de la même plage de sous-réseaux.

Informations	Obligatoire ?	Vos valeurs
Nom IPspace Identifiant unique de l'IPspace.	Oui.	

Configuration broadcast domain

Un domaine de diffusion regroupe les ports qui appartiennent au même réseau de couche 2 et définit la MTU pour les ports de domaine de diffusion.

Les domaines de diffusion sont affectés à un IPspace. Un IPspace peut contenir un ou plusieurs domaines de diffusion.

Le port vers lequel une LIF échoue doit être membre du failover group pour le LIF. Pour chaque broadcast domain créé par ONTAP, un failover group avec le même nom est également créé qui contient tous les ports du broadcast domain.

Informations	Obligatoire ?	Vos valeurs
Nom IPspace L'IPspace à lequel le domaine de diffusion est affecté. Cet IPspace doit exister.	Oui.	
Nom du domaine de diffusion Nom du domaine de diffusion. Ce nom doit être unique dans l'IPspace.	Oui.	
MTU La valeur maximale de l'unité de transmission pour le domaine de diffusion, généralement définie sur **1500** ou **9000**. La valeur MTU est appliquée à tous les ports du domaine de diffusion et à tous les ports ajoutés ultérieurement au domaine de diffusion. La valeur MTU doit correspondre à tous les périphériques connectés à ce réseau. Notez que le MTU doit être défini sur 1500 octets au maximum pour la gestion des ports e0M et le trafic du processeur de service.	Oui.	
Ports Les ports sont affectés à des domaines de diffusion en fonction de l'accessibilité. Une fois l'affectation du port terminée, vérifiez l'accessibilité en exécutant le `network port reachability show` commande. Ces ports peuvent être des ports physiques, des VLAN ou des groupes d'interfaces. Pour en savoir plus, `network port reachability show` consultez le "Référence de commande ONTAP".	Oui.	

Configuration de sous-réseau

Un sous-réseau contient des pools d'adresses IP et une passerelle par défaut qui peuvent être affectés aux LIF utilisées par des SVM résidant dans l'IPspace.

- Lors de la création d'une LIF sur un SVM, vous pouvez spécifier le nom du sous-réseau au lieu de fournir une adresse IP et un sous-réseau.
- Étant donné qu'un sous-réseau peut être configuré avec une passerelle par défaut, il n'est pas nécessaire de créer la passerelle par défaut dans une étape distincte lors de la création d'un SVM.

- Un domaine de diffusion peut contenir un ou plusieurs sous-réseaux.
- Vous pouvez configurer des LIF SVM qui se trouvent sur des sous-réseaux différents en associant plusieurs sous-réseaux au domaine de diffusion de l'IPspace.
- Chaque sous-réseau doit contenir des adresses IP qui ne se chevauchent pas avec les adresses IP attribuées à d'autres sous-réseaux dans le même IPspace.
- Vous pouvez attribuer des adresses IP spécifiques aux LIF de données d'un SVM et créer une passerelle par défaut pour la SVM au lieu d'utiliser un sous-réseau.

Informations	Obligatoire ?	Vos valeurs
Nom IPspace L'IPspace à lequel le sous-réseau sera affecté. Cet IPspace doit exister.	Oui.	
Nom du sous-réseau Nom du sous-réseau. Ce nom doit être unique dans l'IPspace.	Oui.	
Nom du domaine de diffusion Domaine de diffusion auquel le sous-réseau sera affecté. Ce domaine de diffusion doit résider dans l'IPspace spécifié.	Oui.	
Nom et masque de sous-réseau Sous-réseau et masque dans lequel les adresses IP résident.	Oui.	
Passerelle Vous pouvez spécifier une passerelle par défaut pour le sous-réseau. Si vous n'attribuez pas de passerelle lors de la création du sous-réseau, vous pouvez en affecter une ultérieurement.	Non	

Plages d'adresses IP Vous pouvez spécifier une plage d'adresses IP ou des adresses IP spécifiques. Par exemple, vous pouvez spécifier une plage telle que : `192.168.1.1-192.168.1.100, 192.168.1.112, 192.168.1.145` Si vous ne spécifiez pas de plage d'adresses IP, la plage complète d'adresses IP dans le sous-réseau spécifié est disponible pour l'attribuer aux LIF.	Non	
Forcer la mise à jour des associations LIF Spécifie s'il faut forcer la mise à jour des associations LIF existantes. Par défaut, la création de sous-réseau échoue si des interfaces de processeur de service ou des interfaces réseau utilisent les adresses IP dans les plages fournies. L'utilisation de ce paramètre associe toutes les interfaces adressées manuellement avec le sous-réseau et permet à la commande de réussir.	Non	

Configuration d'un SVM

Vous utilisez des SVM pour fournir des données aux clients et aux hôtes.

Les valeurs que vous enregistrez servent à créer un SVM de données par défaut. Si vous créez un SVM source MetroCluster, consultez la "Guide d'installation et de configuration de MetroCluster FAS-Attached" ou le "Guide d'installation et de configuration d'stretch MetroCluster".

Informations	Obligatoire ?	Vos valeurs
Nom du SVM Nom de domaine complet (FQDN) du SVM. Ce nom doit être unique pour toutes les ligues de groupe.	Oui.	
Nom du volume root Le nom du volume root du SVM.	Oui.	
Nom de l'agrégat Nom de l'agrégat qui détient le volume root du SVM. Cet agrégat doit exister.	Oui.	

Style de sécurité Le style de sécurité du volume root du SVM. Les valeurs possibles sont **ntfs**, **unix** et **mixte**.	Oui.	
Nom IPspace L'IPspace à lequel la SVM est affectée. Cet IPspace doit exister.	Non	
Définition du langage SVM Langue par défaut à utiliser pour le SVM et ses volumes. Si vous ne spécifiez pas de langue par défaut, le langage SVM par défaut est défini sur **C.UTF-8**. Le paramètre de langage SVM détermine le jeu de caractères utilisé pour afficher les noms de fichiers et les données de tous les volumes NAS de la SVM. Vous pouvez modifier la langue une fois le SVM créé.	Non	

Configuration de LIF

Un SVM fournit des données aux clients et hôtes via une ou plusieurs interfaces logiques réseau (LIF).

Informations	Obligatoire ?	Vos valeurs
Nom du SVM Nom du SVM pour la LIF.	Oui.	
Nom de LIF Nom de la LIF. Vous pouvez attribuer plusieurs LIF de données par nœud, et vous pouvez attribuer des LIF à n'importe quel nœud du cluster, pourvu que le nœud dispose de ports de données disponibles. Pour assurer la redondance, vous devez créer au moins deux LIF de données pour chaque sous-réseau de données, et les LIF attribuées à un sous-réseau particulier doivent recevoir des ports home-logiques sur différents nœuds. **Important :** si vous configurez un serveur SMB afin d'héberger Hyper-V ou SQL Server sur SMB pour des solutions de continuité de l'activité, la SVM doit disposer d'au moins une LIF de données sur chaque nœud du cluster.	Oui.	

Stratégie de service Politique de service pour la LIF. La politique de service définit les services réseau pouvant utiliser LIF. Les services et les règles de service intégrés sont disponibles pour la gestion du trafic de données et de gestion sur les SVM de données et de système.	Oui.	
Protocoles autorisés Les LIF basées sur IP ne nécessitent pas de protocoles autorisés. Utilisez plutôt la ligne de stratégie de service. Spécifier les protocoles autorisés pour les LIFs SAN sur les ports FibreChannel. Ce sont les protocoles qui peuvent utiliser cette LIF. Les protocoles qui utilisent la LIF ne peuvent pas être modifiés après la création de la LIF. Vous devez spécifier tous les protocoles lors de la configuration de la LIF.	Non	
Nœud de départ Le nœud sur lequel la LIF renvoie lorsque la LIF est rétablie dans son home port. Vous devez enregistrer un home node pour chaque LIF de données.	Oui.	
Home port ou broadcast domain Choisissez l’une des options suivantes : **Port** : spécifiez le port sur lequel l’interface logique renvoie lorsque la LIF est rétablie sur son port home. Cela n’est fait que pour la première LIF dans le sous-réseau d’un IPspace, sinon elle n’est pas requise. **Broadcast Domain**: Préciser le broadcast domain, et le système sélectionne le port approprié auquel l’interface logique renvoie lorsque le LIF est rétabli sur son home port.	Oui.	
Nom du sous-réseau Sous-réseau à affecter à la SVM. Toutes les LIF de données utilisées pour créer des connexions SMB disponibles en continu avec les serveurs applicatifs doivent se trouver sur le même sous-réseau.	Oui (en cas d’utilisation d’un sous-réseau)	

Configuration DNS

Vous devez configurer DNS sur le SVM avant de créer un serveur NFS ou SMB.

Informations	Obligatoire ?	Vos valeurs
Nom du SVM Nom du SVM sur lequel vous souhaitez créer un serveur NFS ou SMB.	Oui.	
Nom de domaine DNS Liste de noms de domaine à ajouter à un nom d'hôte lors de la résolution de nom hôte-IP. Indiquez d'abord le domaine local, suivi des noms de domaine pour lesquels les requêtes DNS sont le plus souvent effectuées.	Oui.	
Adresses IP des serveurs DNS Liste des adresses IP des serveurs DNS qui fourniront une résolution de nom pour le serveur NFS ou SMB. Les serveurs DNS répertoriés doivent contenir les enregistrements SRV nécessaires à la localisation des serveurs LDAP Active Directory et des contrôleurs de domaine du domaine auquel le serveur SMB sera rattaché. L'enregistrement SRV permet de mapper le nom d'un service au nom d'ordinateur DNS d'un serveur offrant ce service. La création du serveur SMB échoue si ONTAP ne parvient pas à obtenir les enregistrements d'emplacement de service par le biais de requêtes DNS locales. La façon la plus simple de s'assurer que ONTAP puisse localiser les enregistrements SRV Active Directory est de configurer des serveurs DNS intégrés à Active Directory en tant que serveurs DNS SVM. Vous pouvez utiliser des serveurs DNS non intégrés à Active Directory à condition que l'administrateur DNS ait ajouté manuellement les enregistrements SRV à la zone DNS qui contient des informations sur les contrôleurs de domaine Active Directory. Pour plus d'informations sur les enregistrements SRV intégrés à Active Directory, reportez-vous à la rubrique "Fonctionnement de la prise en charge DNS pour Active Directory sur Microsoft TechNet".	Oui.	

Configuration DNS dynamique

Avant de pouvoir utiliser DNS dynamique pour ajouter automatiquement des entrées DNS à vos serveurs DNS intégrés à Active Directory, vous devez configurer DNS dynamique (DDNS) sur le SVM.

Des enregistrements DNS sont créés pour chaque LIF de données sur le SVM. En créant plusieurs LIF de données sur le SVM, vous pouvez établir des connexions client avec équilibrage de la charge aux adresses IP attribuées. La charge DNS équilibre les connexions effectuées à l'aide du nom d'hôte aux adresses IP attribuées selon une séquence périodique.

Informations	Obligatoire ?	Vos valeurs
Nom du SVM SVM sur lequel vous souhaitez créer un serveur NFS ou SMB.	Oui.	
Si vous souhaitez utiliser DDNS Indique s'il faut utiliser DDNS. Les serveurs DNS configurés sur le SVM doivent prendre en charge DDNS. Par défaut, DDNS est désactivé.	Oui.	
Utilisation de DDNS sécurisé ou non Secure DDNS est pris en charge uniquement avec un DNS intégré à Active Directory. Si votre DNS intégré à Active Directory n'autorise que les mises à jour DDNS sécurisées, la valeur de ce paramètre doit être vraie. Par défaut, Secure DDNS est désactivé. Secure DDNS ne peut être activé qu'après la création d'un serveur SMB ou d'un compte Active Directory pour la SVM.	Non	
FQDN du domaine DNS Le FQDN du domaine DNS. Vous devez utiliser le même nom de domaine configuré pour les services de nom DNS sur la SVM.	Non	

Ports réseau

En savoir plus sur la configuration des ports réseau ONTAP

Les ports sont des ports physiques (NIC) ou virtualisés, comme des groupes d'interfaces ou des VLAN.

Les réseaux locaux virtuels (VLAN) et les groupes d'interfaces constituent les ports virtuels. Les groupes d'interfaces traitent plusieurs ports physiques comme un seul port, tandis que les VLAN subdivisent un port physique en plusieurs ports logiques distincts.

- Ports physiques : les LIFs peuvent être configurées directement sur des ports physiques.
- Groupe d'interface : agrégat de ports contenant au moins deux ports physiques qui agissent comme un

seul port de jonction. Un groupe d'interface peut être multimode ou dynamique en mode unique.

- VLAN : port logique qui reçoit et envoie le trafic VLAN-balisé (norme IEEE 802.1Q). Les caractéristiques du port VLAN incluent l'ID VLAN du port. Les ports physiques sous-jacents ou les ports de groupe d'interfaces sont considérés comme des ports de jonction VLAN et les ports de commutateur connectés doivent être configurés pour faire le lien entre les ID VLAN.

  Les ports physiques sous-jacents ou les ports d'interface group d'un port VLAN peuvent continuer à héberger les LIFs, qui transmettent et reçoivent du trafic non balisé.

- Port IP virtuel (VIP) : port logique utilisé comme port de home port pour une LIF VIP. Les ports VIP sont créés automatiquement par le système et ne prennent en charge qu'un nombre limité d'opérations. Les ports VIP sont pris en charge à partir de ONTAP 9.5.

la convention d'appellation des ports est *énuméberLetter* :

- Le premier caractère décrit le type de port.
  « e » représente Ethernet.
- Le second caractère indique l'emplacement numéroté de l'adaptateur de port.
- Le troisième caractère indique la position du port sur un adaptateur multiport.
  « a » indique le premier port, « b » indique le second port, etc.

Par exemple : `e0b` Indique qu'un port Ethernet est le second port sur la carte mère du nœud.

Les VLAN doivent être nommés à l'aide de la syntaxe `port_name-vlan-id`.

`port_name` spécifie le port physique ou le groupe d'interface.

`vlan-id` Spécifie l'identification VLAN sur le réseau. Par exemple : `e1c-80` Est un nom de VLAN valide.

Configurez les ports réseau

Combinez les ports physiques pour créer des groupes d'interface ONTAP

Un groupe d'interface, également appelé Groupe d'agrégation de liens (LAG), est créé en combinant deux ports physiques ou plus sur le même nœud en un seul port logique. Le port logique offre une résilience accrue, une disponibilité accrue et un partage de charge accru.

Types de groupe d'interface

Le système de stockage prend en charge trois types de groupes d'interfaces : mode unique, multimode statique et multimode dynamique. Chaque groupe d'interface fournit différents niveaux de tolérance aux pannes. Les groupes d'interfaces multimode fournissent des méthodes pour équilibrer la charge du trafic réseau.

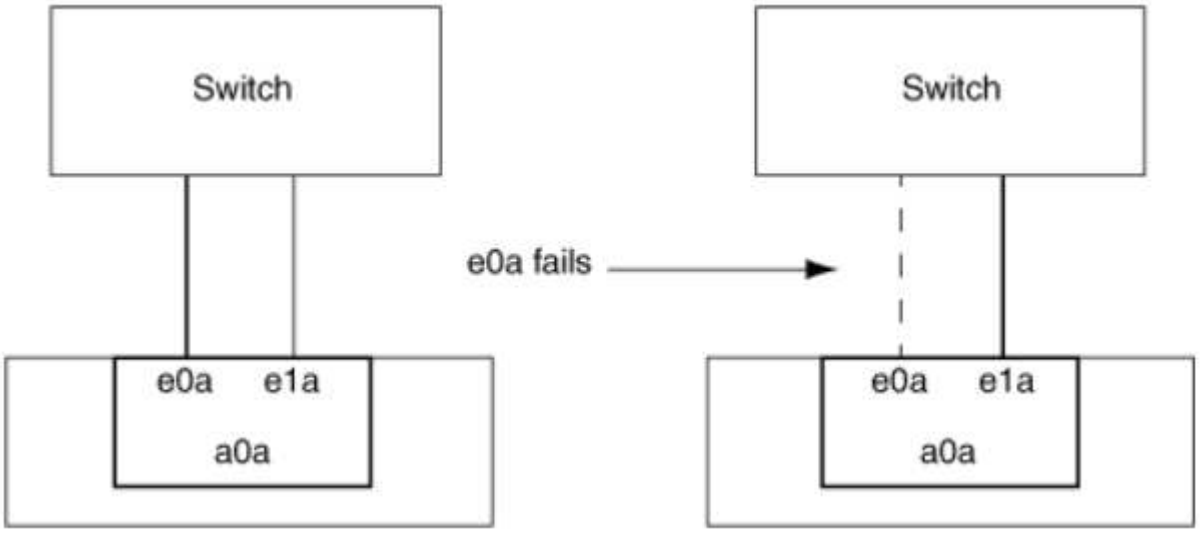
Caractéristiques des groupes d'interfaces monomode

Dans un groupe d'interface à mode unique, une seule des interfaces du groupe d'interface est active. Les autres interfaces sont en veille, prêtes à prendre le relais en cas de défaillance de l'interface active.

Caractéristiques des groupes d'interfaces monomode :

- Pour le basculement, le cluster surveille la liaison active et contrôle le basculement.
  Comme le cluster surveille la liaison active, aucune configuration de commutateur n'est requise.
- Il peut y avoir plusieurs interfaces en veille dans un groupe d'interface à mode unique.
- Si un groupe d'interface à mode unique couvre plusieurs commutateurs, vous devez connecter les switchs à l'aide d'une liaison ISL (Inter-Switch Link).
- Pour un groupe d'interface à mode unique, les ports switchs doivent être situés dans le même domaine de diffusion.
- Les paquets ARP de contrôle de liaison, dont l'adresse source est 0.0.0.0, sont envoyés sur les ports pour vérifier que les ports se trouvent dans le même domaine de diffusion.

La figure suivante illustre un exemple de groupe d'interfaces monomode. Dans la figure, e0a et e1a font partie du groupe d'interface a0a mode unique. Si l'interface active e0a, tombe en panne, l'interface e1a de secours prend le relais et maintient la connexion au commutateur.



Pour profiter de la fonctionnalité Single-mode, l'approche recommandée consiste à utiliser des groupes de basculement. L'utilisation d'un failover group permet de continuer à utiliser le second port pour d'autres LIFs et de ne pas avoir à le conserver. En outre, les groupes de basculement peuvent couvrir plus de deux ports et couvrir plusieurs nœuds.

Caractéristiques des groupes d'interfaces multimode statiques

La mise en œuvre du groupe d'interfaces multimode statique dans ONTAP est conforme à la norme IEEE 802.3ad (statique). Tout switch qui prend en charge les agrégats, mais qui ne dispose pas d'échange de paquets de contrôle pour la configuration d'un agrégat, peut être utilisé avec des groupes d'interfaces multimode statiques.

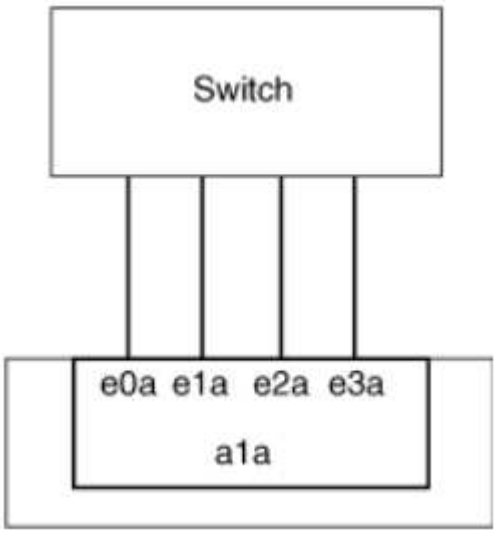
Les groupes d'interfaces multimode statiques ne sont pas conformes à la norme IEEE 802.3ad (dynamique), également appelée protocole LACP (Link Aggregation Control Protocol). Le protocole LACP est l'équivalent du protocole PAgP (Port Aggregation Protocol), le protocole propriétaire d'agrégation de liens de Cisco.

Les caractéristiques d'un groupe d'interfaces multimode statique sont les suivantes :

- Toutes les interfaces du groupe d'interface sont actives et partagent une seule adresse MAC.
  - Plusieurs connexions individuelles sont distribuées sur les interfaces du groupe d'interface.

    - Chaque connexion ou session utilise une interface au sein du groupe d'interface.
      Lorsque vous utilisez le schéma d'équilibrage de charge séquentiel, toutes les sessions sont distribuées sur les liaisons disponibles par paquet et ne sont pas liées à une interface particulière du groupe d'interfaces.
- Les groupes d'interfaces multimode statiques peuvent effectuer une restauration en cas de défaillance d'une interface jusqu'à « n-1 », où n est le nombre total d'interfaces qui forment le groupe d'interface.
- Si un port tombe en panne ou est débranché, le trafic qui traverserait la liaison défaillante est automatiquement redistribué à l'une des interfaces restantes.
- Les groupes d'interfaces multimode statiques peuvent détecter une perte de liaison, mais ils ne peuvent pas détecter une perte de connectivité au client ou les erreurs de configuration de commutateur qui pourraient affecter la connectivité et les performances.
- Un groupe d'interfaces multimode statiques nécessite un commutateur qui prend en charge l'agrégation de liens sur plusieurs ports de commutateur.
  Le commutateur est configuré de sorte que tous les ports auxquels sont connectées les liaisons d'un groupe d'interfaces font partie d'un seul port logique. Certains commutateurs ne prennent pas en charge l'agrégation de liens des ports configurés pour les trames Jumbo. Pour plus d'informations, consultez la documentation du fournisseur de votre commutateur.
- Plusieurs options d'équilibrage de charge sont disponibles pour distribuer le trafic entre les interfaces d'un groupe d'interfaces multimode statique.

La figure suivante illustre un exemple de groupe d'interfaces multimode statiques. Les interfaces e0a, e1a, e2a et e3a font partie du groupe d'interface multimode a1a. Les quatre interfaces du groupe d'interfaces multimode a1a sont actives.



Il existe plusieurs technologies qui permettent de répartir le trafic dans un lien agrégé unique sur plusieurs commutateurs physiques. Les technologies utilisées pour activer cette fonctionnalité varient selon les produits de mise en réseau. Les groupes d'interfaces multimode statiques en ONTAP sont conformes à la norme IEEE 802.3. Si une technologie particulière d'agrégation de liens de commutateur multiple est dite compatible avec les normes IEEE 802.3 ou conforme à celles-ci, elle doit fonctionner avec ONTAP.

La norme IEEE 802.3 indique que le périphérique de transmission d'une liaison agrégée détermine l'interface physique pour la transmission. Par conséquent, ONTAP est uniquement responsable de la distribution du trafic sortant et ne peut pas contrôler l'arrivée des trames entrantes. Si vous souhaitez gérer ou contrôler la transmission du trafic entrant sur une liaison agrégée, cette transmission doit être modifiée sur le périphérique réseau directement connecté.

Groupe d’interfaces multimode dynamique

Les groupes d’interfaces multimode dynamiques implémentent le protocole LACP (Link Aggregation Control Protocol) pour communiquer l’appartenance aux groupes au commutateur directement connecté. LACP vous permet de détecter la perte de l’état de liaison et l’incapacité du nœud à communiquer avec le port de switch DAS.

La mise en œuvre de groupes d’interfaces multimode dynamiques dans ONTAP est conforme à la norme IEEE 802.3 AD (802.1 AX). ONTAP ne prend pas en charge le protocole PAgP (Port Aggregation Protocol), qui est un protocole propriétaire d’agrégation de liens de Cisco.

Un groupe d’interfaces multimode dynamique requiert un switch qui prend en charge LACP.

ONTAP implémente un LACP en mode actif non configurable qui fonctionne bien avec les switchs configurés en mode actif ou passif. ONTAP implémente les temporisateurs LACP longs et courts (pour une utilisation avec des valeurs non configurables 3 secondes et 90 secondes), comme spécifié dans IEEE 802.3 AD (802.1AX).

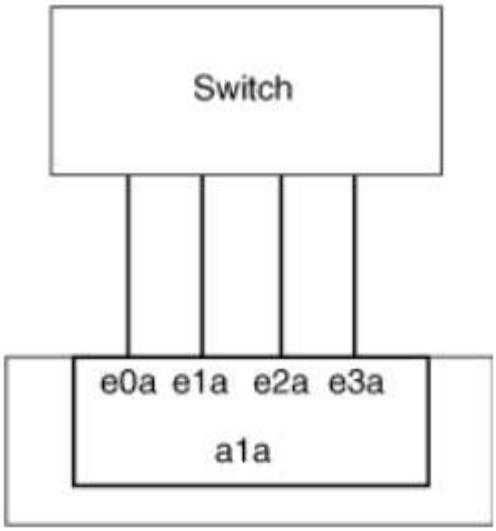
L’algorithme d’équilibrage de charge ONTAP détermine le port membre à utiliser pour transmettre le trafic sortant et ne contrôle pas la réception des trames entrantes. Le commutateur détermine le membre (port physique individuel) de son groupe de canaux de port à utiliser pour la transmission, en fonction de l’algorithme d’équilibrage de charge configuré dans le groupe de canaux de port du commutateur. Par conséquent, la configuration du commutateur détermine le port membre (port physique individuel) du système de stockage pour recevoir le trafic. Pour plus d’informations sur la configuration du commutateur, reportez-vous à la documentation fournie par votre fournisseur de commutateur.

Si une interface individuelle ne parvient pas à recevoir de paquets de protocole LACP successifs, cette interface individuelle est marquée comme « Lag_inactive » dans la sortie de la commande « ifgrp status ». Le trafic existant est automatiquement redirigé vers les interfaces actives restantes.

Les règles suivantes s’appliquent lors de l’utilisation de groupes d’interfaces multimode dynamiques :

- Les groupes d’interfaces multimodes dynamiques doivent être configurés de manière à utiliser les méthodes d’équilibrage de charge basées sur les ports, les protocoles IP, MAC ou Round Robin.
- Dans un groupe d’interfaces multimode dynamiques, toutes les interfaces doivent être actives et partager une adresse MAC unique.

La figure suivante illustre un exemple de groupe d’interfaces multimode dynamiques. Les interfaces e0a, e1a, e2a et e3a font partie du groupe d’interface multimode a1a. Les quatre interfaces du groupe d’interfaces multimode dynamique a1a sont actives.



Équilibrage de la charge dans les groupes d'interfaces multimode

Vous pouvez vous assurer que toutes les interfaces d'un groupe d'interfaces multimodes sont utilisées de manière égale pour le trafic sortant en utilisant l'adresse IP, l'adresse MAC, les méthodes d'équilibrage de charge séquentielles ou basées sur les ports pour distribuer le trafic réseau de manière égale sur les ports d'un groupe d'interfaces multimodes.

La méthode d'équilibrage de charge d'un groupe d'interfaces multimode ne peut être spécifiée que lorsque le groupe d'interfaces est créé.

Meilleure pratique : l'équilibrage de charge basé sur les ports est recommandé chaque fois que possible. Utilisez l'équilibrage de charge basé sur les ports, sauf si le réseau a une raison ou une limitation spécifique qui l'empêche.

Équilibrage de charge basé sur des ports

L'équilibrage de charge basé sur les ports est la méthode recommandée.

Vous pouvez égaliser le trafic sur un groupe d'interfaces multimode en fonction des ports de la couche de transport (TCP/UDP) en utilisant la méthode d'équilibrage de charge basée sur les ports.

La méthode d'équilibrage de charge basée sur le port utilise un algorithme de hachage rapide sur les adresses IP source et de destination, ainsi que le numéro de port de la couche de transport.

Équilibrage de la charge des adresses IP et MAC

L'équilibrage de la charge des adresses IP et MAC est le moyen d'égaliser le trafic sur les groupes d'interfaces multimodes.

Ces méthodes d'équilibrage de charge utilisent un algorithme de hachage rapide sur les adresses source et de destination (adresse IP et adresse MAC). Si le résultat de l'algorithme de hachage est mappé à une interface qui n'est pas à l'état de la liaison ACTIVE, l'interface active suivante est utilisée.

> Ne sélectionnez pas la méthode d'équilibrage de charge de l'adresse MAC lors de la création de groupes d'interfaces sur un système qui se connecte directement à un routeur. Dans une telle configuration, pour chaque trame IP sortante, l'adresse MAC de destination est l'adresse MAC du routeur. Par conséquent, une seule interface du groupe d'interface est utilisée.

L’équilibrage de charge d’adresse IP fonctionne de la même manière pour les adresses IPv4 et IPv6.

Équilibrage séquentiel de la charge

Vous pouvez utiliser l’équilibrage séquentiel des charges pour distribuer de manière égale des paquets entre plusieurs liaisons à l’aide d’un algorithme de permutation circulaire. Vous pouvez utiliser l’option séquentielle pour équilibrer la charge du trafic d’une connexion unique sur plusieurs liaisons afin d’augmenter le débit de connexion unique.

Cependant, étant donné que l’équilibrage séquentiel de la charge peut causer une livraison de paquets hors de la commande, les performances peuvent être extrêmement faibles. Par conséquent, l’équilibrage séquentiel de la charge n’est généralement pas recommandé.

Créez un groupe d’interfaces ou LAG

Vous pouvez créer un groupe d’interface ou LAG (monomode, multimode statique ou multimode dynamique) afin de présenter une interface unique aux clients en combinant les capacités des ports réseau agrégés.

La procédure à suivre dépend de l’interface que vous utilisez—System Manager ou de l’interface de ligne de commandes :

System Manager

Utilisez System Manager pour créer un LAG

Étapes

1. Sélectionnez **réseau > port Ethernet > + Groupe d'agrégation de liens** pour créer un LAG.
2. Sélectionnez le nœud dans la liste déroulante.
3. Choisissez parmi les options suivantes :
   a. ONTAP à **sélectionne automatiquement le domaine de diffusion (recommandé)**.
   b. Pour sélectionner manuellement un domaine de diffusion.
4. Sélectionnez les ports pour former le LAG.
5. Sélectionnez le mode :
   a. Unique : un seul port est utilisé à la fois.
   b. Multiples : tous les ports peuvent être utilisés simultanément.
   c. LACP : le protocole LACP détermine les ports qui peuvent être utilisés.
6. Sélectionner l'équilibrage de charge :
   a. Sur IP
   b. Basé SUR MAC
   c. Port
   d. Séquentiel
7. Enregistrez les modifications.

CLI

Utilisez l'interface de ligne de commande pour créer un groupe d'interfaces

Lors de la création d'un groupe d'interfaces multimode, vous pouvez spécifier l'une des méthodes d'équilibrage de charge suivantes :

- `port`: Le trafic réseau est distribué sur la base des ports de la couche de transport (TCP/UDP). Il s'agit de la méthode d'équilibrage de charge recommandée.
- `mac`: Le trafic réseau est distribué sur la base d'adresses MAC.
- `ip`: Le trafic réseau est distribué sur la base des adresses IP.
- `sequential`: Le trafic réseau est distribué au fur et à mesure qu'il est reçu.

> L'adresse MAC d'un groupe d'interfaces est déterminée par l'ordre des ports sous-jacents et la façon dont ces ports s'initialisent au démarrage. Vous ne devez donc pas présumer que l'adresse MAC ifgrp est conservée entre les redémarrages ou les mises à niveau ONTAP.

Étape

Utilisez le `network port ifgrp create` commande permettant de créer un groupe d'interface.

Vous devez nommer les groupes d'interface à l'aide de la syntaxe `a<number><letter>`. Par exemple, a0A, a0b, a1c et a2a sont des noms de groupes d'interfaces valides.

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

L'exemple suivant montre comment créer un groupe d'interfaces nommé a0a avec une fonction de distribution de port et un mode multimode :

```
network port ifgrp create -node cluster-1-01 -ifgrp a0a -distr-func port -mode multimode
```

Ajoutez un port à un groupe d'interfaces ou LAG

Vous pouvez ajouter jusqu'à 16 ports physiques à un groupe d'interfaces ou LAG pour toutes les vitesses de port.

La procédure à suivre dépend de l'interface que vous utilisez—System Manager ou de l'interface de ligne de commandes :

System Manager

Utilisez System Manager pour ajouter un port à un LAG

Étapes

1. Sélectionnez **réseau > port Ethernet > LAG** pour modifier un LAG.
2. Sélectionnez des ports supplémentaires sur le même nœud à ajouter au LAG.
3. Enregistrez les modifications.

CLI

Utilisez l'interface de ligne de commande pour ajouter des ports à un groupe d'interfaces

Étape

Ajout de ports réseau au groupe d'interface :

```
network port ifgrp add-port
```

L'exemple suivant montre comment ajouter le port e0c à un groupe d'interfaces nommé a0A :

```
network port ifgrp add-port -node cluster-1-01 -ifgrp a0a -port e0c
```

Depuis ONTAP 9.8, les groupes d'interface sont automatiquement placés dans un domaine de diffusion approprié environ une minute après l'ajout du premier port physique au groupe d'interface. Si vous ne souhaitez pas que ONTAP le fait, et préférez placer manuellement le ifgrp sur un domaine de broadcast, spécifiez ensuite le `-skip-broadcast-domain-placement` dans le cadre du `ifgrp add-port` commande.

Pour en savoir plus sur `network port ifgrp add-port` les restrictions de configuration qui s'appliquent aux groupes d'interfaces de port, consultez le "Référence de commande ONTAP".

Supprimer un port d'un groupe d'interfaces ou LAG

Vous pouvez supprimer un port d'un groupe d'interface qui héberge les LIFs, tant qu'il ne s'agit pas du dernier port du groupe d'interfaces. Il n'y a pas d'exigence que le groupe d'interface ne doit pas héberger les LIFs d'hôtes, ni que le groupe d'interface ne doit pas être le home port d'une LIF compte tenu de ne pas supprimer

le dernier port du groupe d'interface. Cependant, si vous supprimez le dernier port, vous devez d'abord migrer ou déplacer les LIF du groupe d'interface.

Description de la tâche

Vous pouvez supprimer jusqu'à 16 ports (interfaces physiques) d'un groupe d'interfaces ou LAG.

La procédure à suivre dépend de l'interface que vous utilisez—System Manager ou de l'interface de ligne de commandes :

System Manager

Utilisez System Manager pour supprimer un port d'un LAG

Étapes

1. Sélectionnez **réseau > port Ethernet > LAG** pour modifier un LAG.
2. Sélectionnez les ports à supprimer du LAG.
3. Enregistrez les modifications.

CLI

Utilisez l'interface de ligne de commande pour supprimer des ports d'un groupe d'interfaces

Étape

Suppression des ports réseau d'un groupe d'interfaces :

```
network port ifgrp remove-port
```

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

L'exemple suivant montre comment supprimer le port e0c d'un groupe d'interfaces nommé a0A :

```
network port ifgrp remove-port -node cluster-1-01 -ifgrp a0a -port e0c
```

Supprimer un groupe d'interfaces ou LAG

Vous pouvez supprimer des groupes d'interfaces ou des groupes LAG si vous souhaitez configurer des LIF directement sur les ports physiques sous-jacents ou décider de modifier le groupe d'interfaces ou le mode LAG ou la fonction de distribution.

Avant de commencer

- Le groupe d'interface ou LAG ne doit pas héberger de LIF.
- Le groupe d'interface ou LAG ne doit pas être le port de départ, ni la cible de basculement d'une LIF.

La procédure à suivre dépend de l'interface que vous utilisez—System Manager ou de l'interface de ligne de commandes :

System Manager

Utilisez System Manager pour supprimer un LAG

Étapes

1. Sélectionnez **réseau > port Ethernet > LAG** pour supprimer un LAG.
2. Sélectionnez le LAG à supprimer.
3. Supprimer le LAG.

CLI

Utilisez l'interface de ligne de commande pour supprimer un groupe d'interfaces

Étape

Utilisez le `network port ifgrp delete` commande permettant de supprimer un groupe d'interface.

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

L'exemple suivant montre comment supprimer un groupe d'interfaces nommé a0b :

```
network port ifgrp delete -node cluster-1-01 -ifgrp a0b
```

Configurez les VLAN ONTAP sur les ports physiques

Vous pouvez utiliser des VLAN dans ONTAP pour assurer une segmentation logique des réseaux en créant des domaines de diffusion distincts, définis sur la base d'un port de commutateur, par opposition aux domaines de diffusion traditionnels, définis sur des limites physiques.

Un VLAN peut s'étendre sur plusieurs segments de réseau physique. Les stations terminales appartenant à un VLAN sont liés par fonction ou application.

Par exemple, les stations d'extrémité d'un VLAN peuvent être regroupées par des départements, tels que l'ingénierie et la comptabilité, ou par des projets, tels que la release1 et la rele2. Étant donné que la proximité physique des stations de fin n'est pas essentielle dans un VLAN, vous pouvez disperser géographiquement les stations de fin et encore contenir le domaine de diffusion dans un réseau commuté.

Dans ONTAP 9.14.1 et 9.13.1, les ports non balisés qui ne sont utilisés par aucune interface logique (LIF) et qui ne disposent pas de connectivité VLAN native sur le commutateur connecté sont marqués comme dégradés. Cela permet d'identifier les ports inutilisés et n'indique pas une panne. Les VLAN natifs autorisent le trafic non balisé sur le port de base ifgrp, comme les diffusions ONTAP CFM. Configurez les VLAN natifs sur le commutateur pour éviter de bloquer le trafic non balisé.

Vous pouvez gérer des VLAN en créant, en supprimant ou en affichant des informations les concernant.

> Vous ne devez pas créer de VLAN sur une interface réseau avec le même identifiant que le VLAN natif du commutateur. Par exemple, si l'interface réseau e0b est sur un VLAN 10 natif, vous ne devez pas créer de VLAN e0b-10 sur cette interface.

Créez un VLAN

Vous pouvez créer un VLAN pour la maintenance de domaines de diffusion distincts au sein du même domaine réseau en utilisant System Manager ou le `network port vlan create` commande.

Avant de commencer

Vérifiez que les exigences suivantes ont été respectées :

- Les commutateurs déployés sur le réseau doivent soit être conformes aux normes IEEE 802.1Q, soit disposer d'une implémentation spécifique au fournisseur de VLAN.
- Pour prendre en charge plusieurs VLAN, une station d'extrémité doit être configurée de manière statique pour appartenir à un ou plusieurs VLAN.
- Le VLAN n'est pas connecté à un port hébergeant une LIF de cluster.
- Le VLAN n'est pas connecté aux ports affectés à l'IPspace Cluster.
- Le VLAN n'est pas créé sur un port de groupe d'interfaces qui ne contient aucun port membre.

Description de la tâche

La création d'un VLAN connecte le VLAN au port réseau d'un nœud spécifié d'un cluster.

Lorsque vous configurez un VLAN sur un port pour la première fois, le port risque de tomber en panne, entraînant une déconnexion temporaire du réseau. Les ajouts de VLAN ultérieurs au même port n'affectent pas l'état du port.

> Vous ne devez pas créer de VLAN sur une interface réseau avec le même identifiant que le VLAN natif du commutateur. Par exemple, si l'interface réseau e0b est sur un VLAN 10 natif, vous ne devez pas créer de VLAN e0b-10 sur cette interface.

La procédure à suivre dépend de l'interface que vous utilisez—System Manager ou de l'interface de ligne de commandes :

System Manager

Utilisez System Manager pour créer un VLAN

Depuis ONTAP 9.12.0, vous pouvez sélectionner automatiquement le domaine de diffusion ou manuellement sur dans la liste. Auparavant, les domaines de diffusion étaient toujours sélectionnés automatiquement en fonction de la connectivité de couche 2. Si vous sélectionnez manuellement un domaine de diffusion, un avertissement s'affiche pour indiquer que la sélection manuelle d'un domaine de diffusion peut entraîner une perte de connectivité.

Étapes

1. Sélectionnez **réseau > port Ethernet > + VLAN**.
2. Sélectionnez le nœud dans la liste déroulante.
3. Choisissez parmi les options suivantes :
   a. ONTAP à **sélectionne automatiquement le domaine de diffusion (recommandé)**.
   b. Pour sélectionner manuellement un domaine de diffusion dans la liste.
4. Sélectionnez les ports pour former le VLAN.
5. Spécifiez l'ID du VLAN.
6. Enregistrez les modifications.

CLI

Utilisez l'interface de ligne de commande pour créer un VLAN

Dans certaines circonstances, si vous voulez créer le port VLAN sur un port dégradé sans corriger le problème matériel ou toute mauvaise configuration logicielle, alors vous pouvez définir le `-ignore -health-status` paramètre du `network port modify` commande en tant que `true`.

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

Étapes

1. Utilisez le `network port vlan create` Pour créer un VLAN.
2. Vous devez spécifier l' `vlan-name` ou le `port` et `vlan-id` Options lors de la création d'un VLAN. Le nom du VLAN est une combinaison du nom du port (ou du groupe d'interfaces) et de l'identificateur du VLAN du commutateur réseau, avec un tiret entre les deux. Par exemple : `e0c-24` et `e1c-80` Sont des noms de VLAN valides.

L'exemple suivant montre comment créer un VLAN `e1c-80` connecté au port réseau `e1c` sur le nœud `cluster-1-01`:

```
network port vlan create -node cluster-1-01 -vlan-name e1c-80
```

Depuis ONTAP 9.8, les VLAN sont automatiquement placés dans des domaines de diffusion appropriés environ une minute après leur création. Si vous ne souhaitez pas que ONTAP le fait, et préférez placer manuellement le VLAN dans un domaine de diffusion, spécifiez le `-skip-broadcast-domain -placement` dans le cadre du `vlan create` commande.

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

Modifiez un VLAN

Vous pouvez modifier le domaine de diffusion ou désactiver un VLAN.

Utilisez System Manager pour modifier un VLAN

Depuis ONTAP 9.12.0, vous pouvez sélectionner automatiquement le domaine de diffusion ou manuellement sur dans la liste. Auparavant, les domaines de diffusion étaient toujours sélectionnés automatiquement en fonction de la connectivité de couche 2. Si vous sélectionnez manuellement un domaine de diffusion, un avertissement s'affiche pour indiquer que la sélection manuelle d'un domaine de diffusion peut entraîner une perte de connectivité.

Étapes

1. Sélectionnez **réseau > port Ethernet > VLAN**.
2. Sélectionnez l'icône de modification.
3. Effectuez l'une des opérations suivantes :
   - Modifiez le domaine de diffusion en sélectionnant un autre domaine dans la liste.
   - Décochez la case **Enabled**.
4. Enregistrez les modifications.

Supprimer un VLAN

Vous devrez peut-être supprimer un VLAN avant de retirer une carte réseau de son logement. Lorsque vous supprimez un VLAN, il est automatiquement supprimé de toutes les règles et groupes de basculement qui l'utilisent.

Avant de commencer

Assurez-vous qu'il n'y a pas de LIFs associées au VLAN.

Description de la tâche

La suppression du dernier VLAN d'un port peut provoquer une déconnexion temporaire du réseau du port.

La procédure à suivre dépend de l'interface que vous utilisez—System Manager ou de l'interface de ligne de commandes :

System Manager

Utilisez System Manager pour supprimer un VLAN

Étapes

1. Sélectionnez **réseau > port Ethernet > VLAN**.
2. Sélectionnez le VLAN à supprimer.
3. Cliquez sur **Supprimer**.

CLI

Utilisez l'interface de ligne de commande pour supprimer un VLAN

Étape

Utilisez le `network port vlan delete` Commande de suppression d'un VLAN.

L'exemple suivant montre comment supprimer un VLAN `e1c-80` dans le port réseau `e1c` sur le nœud `cluster-1-01`:

```
network port vlan delete -node cluster-1-01 -vlan-name e1c-80
```

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

Modifiez les attributs des ports réseau ONTAP

Vous pouvez modifier les paramètres de négociation automatique, duplex, contrôle du flux, vitesse et état d'un port réseau physique.

Avant de commencer

Le port que vous souhaitez modifier ne doit pas héberger les LIFs.

Description de la tâche

- Il n'est pas recommandé de modifier les paramètres d'administration des interfaces réseau 100 GbE, 40 GbE, 10 GbE ou 1 GbE.

  Les valeurs que vous définissez pour le mode duplex et la vitesse du port sont appelées paramètres administratifs. En fonction des limites du réseau, les paramètres d'administration peuvent différer des paramètres opérationnels (c'est-à-dire le mode duplex et la vitesse utilisés par le port).

- Il n'est pas recommandé de modifier les paramètres d'administration des ports physiques sous-jacents dans un groupe d'interfaces.

  Le `-up-admin` paramètre (disponible au niveau des privilèges avancés) modifie les paramètres administratifs du port.

- Il n'est pas recommandé de régler le `-up-admin` Paramètre administratif sur false pour tous les ports d'un nœud, ou pour le port qui héberge la dernière LIF de cluster opérationnelle sur un nœud.
- Il n'est pas recommandé de modifier la taille MTU du port de gestion, `e0M`.

- La taille MTU d'un port dans un domaine de diffusion ne peut pas être modifiée à partir de la valeur MTU définie pour le domaine de diffusion.
- La taille MTU d'un VLAN ne peut pas dépasser la valeur de la taille MTU de son port de base.

Étapes

1. Modifier les attributs d'un port réseau :

   `network port modify`

2. Vous pouvez définir le `-ignore-health-status` champ à true pour spécifier que le système peut ignorer l'état de santé du port réseau d'un port spécifié.

   Le statut de l'état de santé des ports réseau est automatiquement modifié et passe de dégradé à sain, et ce port peut désormais être utilisé pour héberger les LIFs. Vous devez définir le contrôle de flux des ports du cluster sur `none`. Par défaut, le contrôle de flux est défini sur `full`.

La commande suivante désactive le contrôle de flux sur le port e0b en définissant le contrôle de flux sur aucun :

```
network port modify -node cluster-1-01 -port e0b -flowcontrol-admin none
```

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

Créez des ports 10GbE pour les réseaux ONTAP en convertissant les ports de carte réseau 40 GbE

Vous pouvez convertir les cartes réseau X1144A-R6 et X91440A-R6 40GbE pour prendre en charge quatre ports 10GbE.

Si vous connectez une plateforme matérielle prenant en charge l'une de ces cartes réseau à un cluster prenant en charge l'interconnexion de cluster 10GbE et les connexions de données client, la carte réseau doit être convertie pour fournir les connexions 10GbE nécessaires.

Avant de commencer

Vous devez utiliser un câble de dérivation pris en charge.

Description de la tâche

Pour obtenir la liste complète des plates-formes prenant en charge les cartes réseau, reportez-vous au "Hardware Universe".

> Sur la carte réseau X1144A-R6, seul le port A peut être converti pour prendre en charge les quatre connexions 10GbE. Une fois le port A converti, le port e n'est pas disponible pour utilisation.

Étapes

1. Passez en mode maintenance.
2. Convertissez le NIC de la prise en charge de 40 GbE en prise en charge de 10 GbE.

```
nicadmin convert -m [40G | 10G] [port-name]
```

3. Après avoir utilisé la commande convert, arrêtez le nœud.
4. Installez ou remplacez le câble.
5. En fonction du modèle matériel, utilisez le processeur de service ou le contrôleur BMC (Baseboard Management Controller) pour mettre le nœud sous tension et mettre le nœud en marche pour que la conversion prenne effet.

Configurez les ports UTA X1143A-R6 pour le réseau ONTAP

Par défaut, l'adaptateur cible unifié X1143A-R6 est configuré en mode cible FC, mais vous pouvez configurer ses ports en tant que ports Ethernet 10 Gb et FCoE (CNA) ou ports FC 16 Gb ou ports cibles. 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.

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. Afficher la configuration des ports :

```
system hardware unified-connect show
```

2. Configurez les ports nécessaires pour Fibre Channel (FC) ou CNA (Converged Network adapter) :

```
system node hardware unified-connect modify -node <node_name> -adapter
<adapter_name> -mode {fcp|cna}
```

3. Connectez les câbles appropriés pour FC ou Ethernet 10 Gbit.
4. 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.

Convertissez le port UTA2 pour une utilisation dans le réseau ONTAP

Vous pouvez convertir votre port UTA2 en mode CNA (Converged Network adapter) en mode FC (Fibre Channel), ou inversement.

Vous devez faire passer le mode CNA au mode FC dans le mode UTA2 lorsque vous devez changer le support physique qui connecte le port à son réseau ou pour prendre en charge les initiateurs FC et la cible.

Du mode CNA au mode FC

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 :
     - Déplacez les LIF, retirez le port du ifgrp ou supprimez les VLAN.
     - Supprimez manuellement le port en exécutant la `network port delete` commande. Si la `network port delete` commande échoue, l'administrateur doit résoudre 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 gestionnaire vif ne supprime pas le port, l'administrateur doit le supprimer manuellement après le redémarrage à l'aide de la `network port delete` commande.

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

5. Vérifiez que le SFP+ est installé correctement :

```
network fcp adapter show -instance -node -adapter
```

   Pour le CNA, vous devez utiliser un SFP Ethernet 10 Gbit. Pour ce faire, vous devez utiliser un SFP 8 Gbit ou un SFP 16 Gbit avant de modifier la configuration sur le nœud.

Du mode FC au mode CNA

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 cna
```

3. Redémarrez le nœud
4. Vérifiez que le SFP+ correct est installé.

   Pour le CNA, vous devez utiliser un SFP Ethernet 10 Gbit.

Convertissez les modules optiques CNA/UTA2 pour le réseau ONTAP

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".

Supprimez les cartes réseau des nœuds de cluster ONTAP

Vous devrez peut-être retirer une carte réseau défectueuse de son logement ou la déplacer vers un autre emplacement pour des raisons de maintenance.

> La procédure de suppression d'une carte réseau est différente dans ONTAP 9.7 et les versions antérieures. Si vous devez supprimer une carte réseau d'un nœud de cluster ONTAP exécutant ONTAP 9.7 ou une version antérieure, reportez-vous à la procédure "Suppression d'une carte réseau du nœud (ONTAP 9.7 ou version antérieure)".

Étapes

1. Mettez le nœud hors tension.
2. Retirez physiquement la carte réseau de son logement.

3. Mettez le nœud sous tension.
4. Vérifiez que le port a été supprimé :

```
network port show
```

> ONTAP supprime automatiquement le port de n'importe quel groupe d'interfaces. Si le port était le seul membre d'un groupe d'interfaces, le groupe d'interfaces est supprimé. Pour en savoir plus, `network port show` consultez le "Référence de commande ONTAP".

5. Si des VLAN y sont configurés sur le port, ils sont déplacés. Vous pouvez afficher les VLAN déplacés à l'aide de la commande suivante :

```
cluster controller-replacement network displaced-vlans show
```

> Le `displaced-interface show`, `displaced-vlans show`, et `displaced-vlans restore` les commandes sont uniques et ne nécessitent pas le nom de la commande entièrement qualifié, qui commence par `cluster controller-replacement network`.

6. Ces VLAN sont supprimés, mais peuvent être restaurés à l'aide de la commande suivante :

```
displaced-vlans restore
```

7. Si des LIFs de type port y sont configurées, ONTAP sélectionne automatiquement de nouveaux ports d'accueil pour ces LIFs sur un autre port du même broadcast domain. Si aucun port domestique approprié n'est trouvé sur le même filer, ces LIF sont considérées comme déplacées. Vous pouvez afficher les LIFs déplacées à l'aide de la commande suivante :

   `displaced-interface show`

8. Lorsqu'un nouveau port est ajouté au broadcast domain sur le même node, les home ports des LIFs sont automatiquement restaurés. Vous pouvez également définir le port d'accueil à l'aide de `network interface modify -home-port -home-node or use the displaced- interface restore` commande.

Informations associées

- "suppression de l'interface déplacée du réseau de remplacement du contrôleur de cluster"
- "modification de l'interface réseau"

Surveiller les ports réseau

Surveillez l'état de santé des ports réseau ONTAP

La gestion ONTAP des ports réseau inclut un contrôle automatique de l'état de santé et un ensemble de moniteurs pour vous aider à identifier les ports réseau qui ne conviennent pas à l'hébergement des LIF.

Description de la tâche

Si un contrôle de l'état détermine qu'un port réseau est défectueux, il avertit les administrateurs via un message EMS ou indique que le port est dégradé. ONTAP évite d'héberger les LIF sur des ports réseau dégradés si d'autres cibles de basculement sont présentes pour cette LIF. Un port peut se dégrader en raison d'un événement de panne logicielle, tel que le fait de sauter des liaisons (rebondissement rapide des liaisons entre le haut et le bas) ou le partitionnement réseau :

- Les ports réseaux du cluster IPspace sont marqués comme détériorées lorsqu'ils connaissent une liaison flipatent ou une perte de la capacité de couche 2 (L2) à d'autres ports réseau du domaine de diffusion.
- Les ports réseau des IPspaces sans cluster sont marqués comme dégradés lorsqu'ils réalisent des liaisons téléphoniques.

Vous devez connaître les comportements suivants d'un port dégradé :

- Un port dégradé ne peut pas être inclus dans un VLAN ou dans un groupe d'interfaces.

  Si un port membre d'un groupe d'interface est marqué comme dégradé, mais que le groupe d'interfaces est toujours marqué comme défectueux, les LIF peuvent être hébergées sur ce groupe d'interface.

- Les LIF sont automatiquement migrées depuis les ports dégradés vers les ports sains.
- Lors d'un événement de basculement, un port dégradé n'est pas considéré comme la cible de basculement. Si aucun port défectueux n'est disponible, les ports LIF hôtes sont dégradés conformément à la politique de basculement normale.
- Vous ne pouvez ni créer, ni migrer, ni restaurer une LIF vers un port dégradé.

  Vous pouvez modifier le `ignore-health-status` définition du port réseau sur `true`. Vous pouvez ensuite héberger une LIF sur les ports sains.

Étapes

1. Connectez-vous au mode de privilège avancé :

   ```
   set -privilege advanced
   ```

2. Vérifiez les moniteurs d'intégrité qui sont activés pour surveiller l'intégrité des ports du réseau :

   ```
   network options port-health-monitor show
   ```

   L'état de santé d'un port est déterminé par la valeur des moniteurs d'intégrité.

   Les contrôles d'état suivants sont disponibles et activés par défaut dans ONTAP :

   - Surveillance de l'état du cerclage : surveille le cerclage de liaison

     Si la liaison d'un port est plus d'une fois dans cinq minutes, ce port est marqué comme dégradé.

   - Moniteur d'intégrité de la capacité d'accessibilité L2 : surveille si tous les ports configurés dans le même domaine de diffusion ont une capacité d'accessibilité L2 entre eux

     Ce contrôle de l'état signale les problèmes de réabilité L2 dans tous les IPspaces, mais il marque

uniquement les ports du cluster IPspace comme étant dégradés.

- Contrôle CRC : surveille les statistiques CRC sur les ports

  Ce contrôle de l'état ne marque pas un port comme dégradé mais génère un message EMS lorsqu'un taux de défaillance CRC très élevé est observé.

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

3. Activez ou désactivez tous les moniteurs de santé pour un IPspace comme vous le souhaitez en utilisant le `network options port-health-monitor modify` commande.

   Pour en savoir plus, `network options port-health-monitor modify` consultez le "Référence de commande ONTAP".

4. Pour afficher l'état de santé détaillé d'un port :

```
network port show -health
```

Le résultat de la commande affiche le statut d'état de santé du port, `ignore health status` paramètre et liste des raisons pour lesquelles le port est marqué comme dégradé.

Un état de santé du port peut être `healthy` ou `degraded`.

Si le `ignore health status` le paramètre est `true`, il indique que le statut de l'état de santé du port a été modifié de `degraded` à `healthy` par l'administrateur.

Si le `ignore health status` le paramètre est `false`, l'état d'intégrité du port est déterminé automatiquement par le système.

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

Surveiller l'accessibilité des ports réseau ONTAP

La surveillance de l'accessibilité est intégrée à ONTAP 9.8 et versions ultérieures. Utilisez cette surveillance pour identifier si la topologie de réseau physique ne correspond pas à la configuration ONTAP. Dans certains cas, ONTAP peut réparer l'accessibilité des ports. Dans d'autres cas, des étapes supplémentaires sont nécessaires.

Description de la tâche

Utilisez ces commandes pour vérifier, diagnostiquer et réparer les erreurs de configuration du réseau qui ne ONTAP correspondent pas au câblage physique ou à la configuration du commutateur réseau.

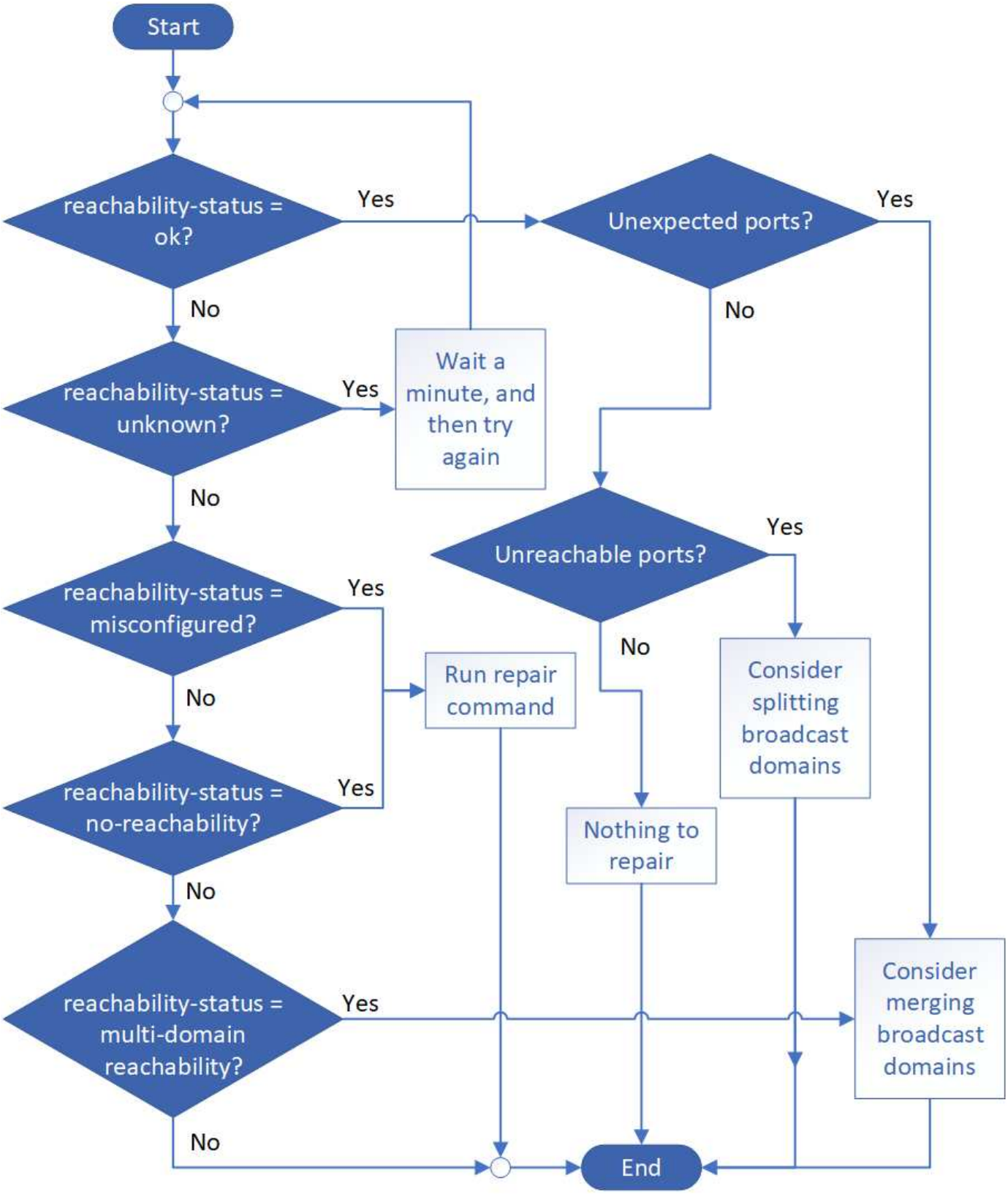
Étape

1. Afficher la capacité de port :

```
network port reachability show
```

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

2. Utilisez l'arbre de décision et le tableau suivants pour déterminer l'étape suivante, le cas échéant.



État-accessibilité	Description
ok	Le port a une capacité de réachbilité de couche 2 à son domaine de diffusion attribué. Si l'état de la capacité d'accessibilité est « ok », mais qu'il y a des « ports inattendus », envisagez de fusionner un ou plusieurs domaines de diffusion. Pour plus d'informations, reportez-vous à la *Unexpected ports* row suivante. Si le statut de la capacité d'accessibilité est « ok », mais qu'il y a des « ports inaccessibles », envisagez de diviser un ou plusieurs domaines de diffusion. Pour plus d'informations, reportez-vous à la ligne *ports inaccessibles* suivante. Si l'état de la capacité de reprise est « ok » et qu'il n'y a pas de ports inattendus ou inaccessibles, votre configuration est correcte.
Ports inattendus	Le port a une capacité de réachbilité de couche 2 à son domaine de diffusion attribué ; cependant, il a également la possibilité de reachcapacité de couche 2 à au moins un autre domaine de broadcast. Examinez la connectivité physique et la configuration du commutateur pour déterminer si elle est incorrecte ou si le domaine de diffusion attribué au port doit être fusionné avec un ou plusieurs domaines de diffusion. Pour plus d'informations, voir "Fusionner les domaines de diffusion".
Ports inaccessibles	Si un seul domaine de diffusion a été partitionné en deux ensembles de capacité d'accès différents, vous pouvez fractionner un domaine de diffusion pour synchroniser la configuration ONTAP avec la topologie de réseau physique. En général, la liste des ports inaccessibles définit l'ensemble des ports qui doivent être divisés en un autre domaine de diffusion après avoir vérifié que la configuration physique et du commutateur est exacte. Pour plus d'informations, voir "Séparer les domaines de diffusion".
mauvaise configuration de la capacité de réachbilité	Le port n'a pas la capacité de reachcapacité de couche 2 à son domaine de diffusion affecté ; cependant, le port a une capacité de réachcapacité de couche 2 à un domaine de diffusion différent. Vous pouvez réparer l'accessibilité du port. Lorsque vous exécutez la commande suivante, le système affecte le port au broadcast domain auquel il a la capacité de reachcapacité : `network port reachability repair -node -port` Pour plus d'informations, voir "Réparation de l'accessibilité de l'orifice".

sans trabilité	Le port n'a pas la possibilité de reachcapacité de couche 2 à un domaine de diffusion existant. Vous pouvez réparer l'accessibilité du port. Lorsque vous exécutez la commande suivante, le système affecte le port à un nouveau domaine de diffusion créé automatiquement dans l'IPspace par défaut : `network port reachability repair -node -port` Pour plus d'informations, voir "Réparation de l'accessibilité de l'orifice". Pour en savoir plus, `network port reachability repair` consultez le "Référence de commande ONTAP".
accessibilité multi-domaines	Le port a une capacité de réachbilité de couche 2 à son domaine de diffusion attribué ; cependant, il a également la possibilité de reachcapacité de couche 2 à au moins un autre domaine de broadcast. Examinez la connectivité physique et la configuration du commutateur pour déterminer si elle est incorrecte ou si le domaine de diffusion attribué au port doit être fusionné avec un ou plusieurs domaines de diffusion. Pour plus d'informations, voir "Fusionner les domaines de diffusion" ou "Réparation de l'accessibilité de l'orifice".
inconnu	Si l'état de la capacité d'accessibilité est « inconnu », attendez quelques minutes et essayez à nouveau la commande.

Une fois que vous avez réparé un port, vous devez vérifier et résoudre les LIFs et les VLAN déplacés. Si le port faisait partie d'un groupe d'interfaces, vous devez également connaître ce qui s'est passé pour ce groupe. Pour plus d'informations, voir "Réparation de l'accessibilité de l'orifice".

En savoir plus sur l'utilisation des ports sur le réseau ONTAP

Plusieurs ports connus sont réservés aux communications ONTAP avec des services spécifiques. Les conflits de ports se produisent si une valeur de port dans votre environnement de réseau de stockage est identique à celle d'un port ONTAP.

Trafic entrant

Le trafic entrant sur votre stockage ONTAP utilise les protocoles et ports suivants :

Protocole	Port	Objectif
Tous les protocoles ICMP	Tout	Envoi d'une requête ping à l'instance
TCP	22	Secure Shell Access à l'adresse IP de la LIF de cluster management ou d'une LIF de node management
TCP	80	Accès à la page Web de l'adresse IP du LIF de cluster management
TCP/UDP	111	RPCBIND, appel de procédure distante pour NFS
UDP	123	NTP, protocole de l'heure réseau

TCP	135	MSRPC, appel de procédure distante Microsoft
TCP	139	NETBIOS-SSN, session de service NetBIOS pour CIFS
TCP/UDP	161-162	SNMP, protocole de gestion de réseau simple
TCP	443	Accès sécurisé à la page web à l'adresse IP du LIF de cluster management
TCP	445	MS Active Domain Services, Microsoft SMB/CIFS sur TCP avec trame NetBIOS
TCP/UDP	658	Montage NFS pour interagir avec un système de fichiers distant comme s'il s'agissait d'un système local
TCP	749	Kerberos
UDP	953	Nom démon
TCP/UDP	2049	Démon du serveur NFS
TCP	2050	Protocole de volume distant NRV, NetApp
TCP	3260	Accès iSCSI via le LIF de données iSCSI
TCP/UDP	4045	Démon de verrouillage NFS
TCP/UDP	4046	Surveillance de l'état du réseau pour NFS
UDP	4049	Devis RPC NFS
UDP	4444	KRB524, Kerberos 524
UDP	5353	DNS multicast
TCP	10000	Sauvegarde à l'aide du protocole NDMP (Network Data Management Protocol)
TCP	11104	Peering de cluster, gestion bidirectionnelle des sessions de communication intercluster pour SnapMirror
TCP	11105	Peering de cluster, transfert de données SnapMirror bidirectionnel à l'aide de LIF intercluster
SSL/TLS	30000	Accepte les connexions de contrôle sécurisées NDMP entre le serveur DMA et NDMP via des sockets sécurisés (SSL/TLS). Les scanners de sécurité peuvent signaler une vulnérabilité sur le port 30000.

Trafic sortant

Le trafic sortant sur votre stockage ONTAP peut être configuré à l'aide de règles de base ou avancées, selon les besoins de l'entreprise.

Règles de base pour les appels sortants

Tous les ports peuvent être utilisés pour tout le trafic sortant via les protocoles ICMP, TCP et UDP.

Protocole	Port	Objectif
Tous les protocoles ICMP	Tout	Tout le trafic sortant
Tous les protocoles TCP	Tout	Tout le trafic sortant
Tous les protocoles UDP	Tout	Tout le trafic sortant

Règles de sortie avancées

Si vous avez besoin de règles rigides pour le trafic sortant, vous pouvez utiliser les informations suivantes pour ouvrir uniquement les ports requis pour la communication sortante par ONTAP.

Active Directory

Protocole	Port	Source	Destination	Objectif
TCP	88	LIF node management, data LIF (NFS, CIFS, iSCSI)	Forêt Active Directory	Authentification Kerberos V.
UDP	137	LIF node management, data LIF (NFS, CIFS)	Forêt Active Directory	Service de noms NetBIOS
UDP	138	LIF node management, data LIF (NFS, CIFS)	Forêt Active Directory	Service de datagrammes NetBIOS
TCP	139	LIF node management, data LIF (NFS, CIFS)	Forêt Active Directory	Session de service NetBIOS
TCP	389	LIF node management, data LIF (NFS, CIFS)	Forêt Active Directory	LDAP
UDP	389	LIF node management, data LIF (NFS, CIFS)	Forêt Active Directory	LDAP
TCP	445	LIF node management, data LIF (NFS, CIFS)	Forêt Active Directory	Microsoft SMB/CIFS sur TCP avec encadrement NetBIOS
TCP	464	LIF node management, data LIF (NFS, CIFS)	Forêt Active Directory	Modifier et définir le mot de passe Kerberos V (SET_CHANGE)
UDP	464	LIF node management, LIF Data (NFS, CIFS)	Forêt Active Directory	Administration des clés Kerberos
TCP	749	LIF node management, LIF Data (NFS, CIFS)	Forêt Active Directory	Modifier et définir le mot de passe Kerberos V (RPCSEC_GSS)

AutoSupport

Protocole	Port	Source	Destination	Objectif
TCP	80	FRV de gestion des nœuds	support.netapp.com	AutoSupport (uniquement si le protocole de transport est passé de HTTPS à HTTP)

SNMP

Protocole	Port	Source	Destination	Objectif
TCP/UDP	162	FRV de gestion des nœuds	Serveur de surveillance	Surveillance par des interruptions SNMP

SnapMirror

Protocole	Port	Source	Destination	Objectif
TCP	11104	FRV InterCluster	Baies de stockage inter-clusters ONTAP	Gestion des sessions de communication intercluster pour SnapMirror

Autres services

Protocole	Port	Source	Destination	Objectif
TCP	25	FRV de gestion des nœuds	Serveur de messagerie	Les alertes SMTP peuvent être utilisées pour AutoSupport
UDP	53	FRV de gestion des nœuds et FRV de données (NFS, CIFS)	DNS	DNS
UDP	67	FRV de gestion des nœuds	DHCP	Serveur DHCP
UDP	68	FRV de gestion des nœuds	DHCP	Client DHCP pour la première configuration
UDP	514	FRV de gestion des nœuds	Serveur Syslog	Messages de transfert syslog
TCP	5010	FRV InterCluster	Sauvegarder le terminal ou restaurer le terminal	Des opérations de sauvegarde et de restauration pour la fonctionnalité Backup vers S3
TCP	18600 à 18699	FRV de gestion des nœuds	Serveurs de destination	Copie NDMP

En savoir plus sur les ports internes ONTAP

Le tableau suivant répertorie les ports utilisés en interne par ONTAP et leurs fonctions. ONTAP utilise ces ports pour diverses fonctions, telles que l'établissement d'une communication LIF intracluster.

Cette liste n'est pas exhaustive et peut varier selon les environnements.

Port/Protocole	Composant/fonction
514	Syslog

900	RPC NetApp Cluster
902	RPC NetApp Cluster
904	RPC NetApp Cluster
905	RPC NetApp Cluster
910	RPC NetApp Cluster
911	RPC NetApp Cluster
913	RPC NetApp Cluster
914	RPC NetApp Cluster
915	RPC NetApp Cluster
918	RPC NetApp Cluster
920	RPC NetApp Cluster
921	RPC NetApp Cluster
924	RPC NetApp Cluster
925	RPC NetApp Cluster
927	RPC NetApp Cluster
928	RPC NetApp Cluster
929	RPC NetApp Cluster
930	Services du noyau et fonctions de gestion (KSMF)
931	RPC NetApp Cluster
932	RPC NetApp Cluster
933	RPC NetApp Cluster
934	RPC NetApp Cluster
935	RPC NetApp Cluster
936	RPC NetApp Cluster
937	RPC NetApp Cluster
939	RPC NetApp Cluster
940	RPC NetApp Cluster
951	RPC NetApp Cluster
954	RPC NetApp Cluster
955	RPC NetApp Cluster
956	RPC NetApp Cluster
958	RPC NetApp Cluster
961	RPC NetApp Cluster
963	RPC NetApp Cluster

964	RPC NetApp Cluster
966	RPC NetApp Cluster
967	RPC NetApp Cluster
975	Protocole KMIP (Key Management Interoperability Protocol)
982	RPC NetApp Cluster
983	RPC NetApp Cluster
5125	Port de contrôle secondaire pour le disque
5133	Port de contrôle secondaire pour le disque
5144	Port de contrôle secondaire pour le disque
65502	Étendue des nœuds SSH
65503	Partage de LIF
7700	Gestionnaire de sessions de cluster (CSM)
7810	RPC NetApp Cluster
7811	RPC NetApp Cluster
7812	RPC NetApp Cluster
7813	RPC NetApp Cluster
7814	RPC NetApp Cluster
7815	RPC NetApp Cluster
7816	RPC NetApp Cluster
7817	RPC NetApp Cluster
7818	RPC NetApp Cluster
7819	RPC NetApp Cluster
7820	RPC NetApp Cluster
7821	RPC NetApp Cluster
7822	RPC NetApp Cluster
7823	RPC NetApp Cluster
7824	RPC NetApp Cluster
7835-7839 et 7845-7849	Ports TCP pour la communication intracluster
8023	Périmètre de nœud TELNET
8443	Port NAS ONTAP S3 pour Amazon FSx
8514	Étendue du nœud RSH
9877	Port client KMIP (hôte local interne uniquement)
10006	Port TCP pour la communication d’interconnexion HA

Les IPspaces

En savoir plus sur la configuration ONTAP IPspace

Les IPspaces permettent de configurer un cluster ONTAP unique afin d'y accéder aux clients à partir de plusieurs domaines réseau distincts d'un point de vue administratif, même si ces clients utilisent la même plage de sous-réseau d'adresses IP. Cela permet de séparer le trafic client pour des raisons de confidentialité et de sécurité.

Un IPspace définit un espace d'adresse IP distinct dans lequel les SVM (Storage Virtual machines) résident. Les ports et les adresses IP définis pour un IPspace ne sont applicables qu'au sein de cet IPspace. Une table de routage distincte est conservée pour chaque SVM au sein d'un IPspace. Par conséquent, aucun routage de trafic cross-SVM ou cross-IPspace n'a lieu.

Les IPspaces prennent en charge les adresses IPv4 et IPv6 sur leurs domaines de routage.

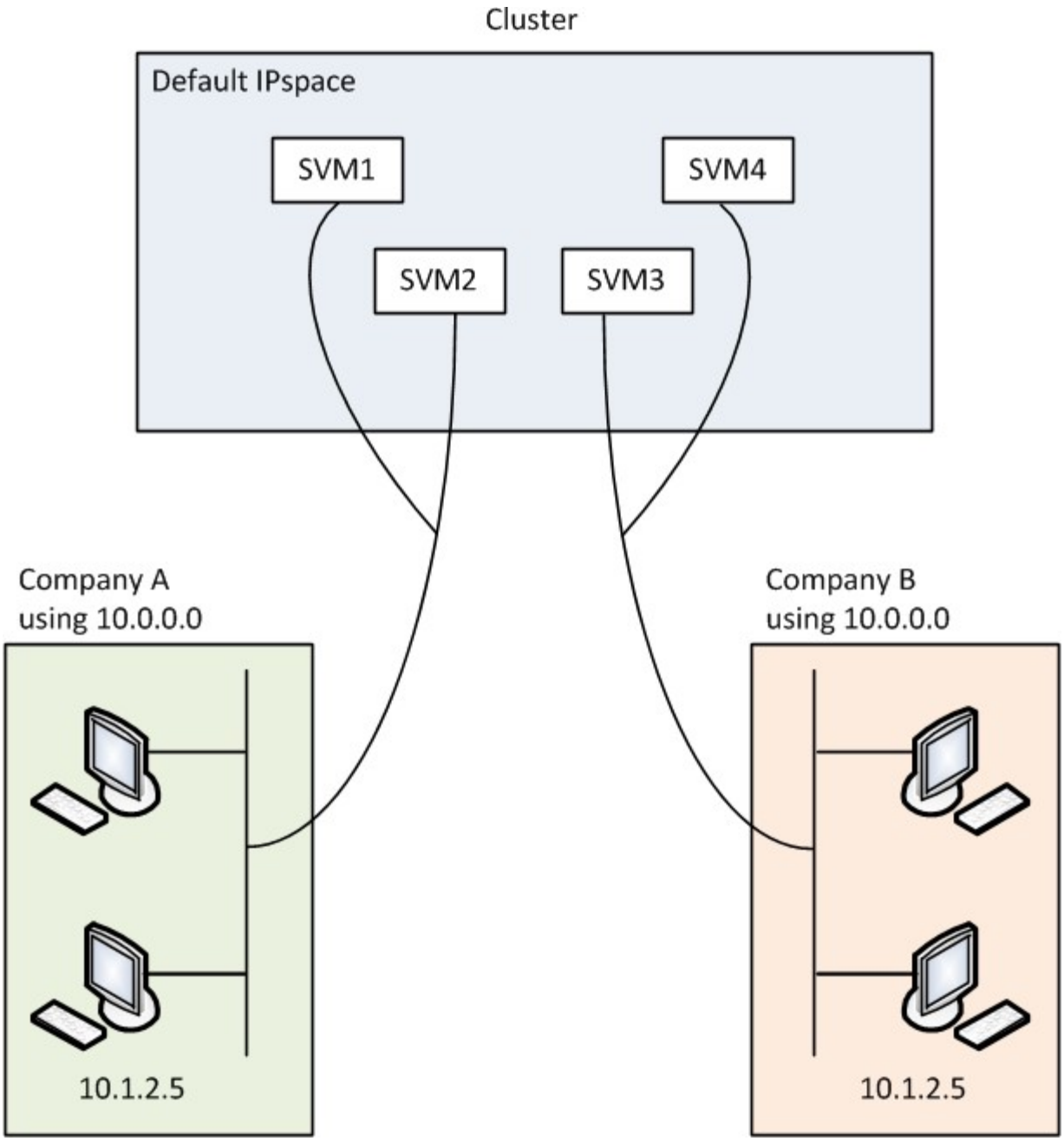
Si vous gérez le stockage pour une seule organisation, vous n'avez pas besoin de configurer les IPspaces. Si vous gérez le stockage de plusieurs entreprises sur un même cluster ONTAP, et qu'aucun de vos clients n'a de configurations réseau contradictoires, vous n'avez également besoin d'utiliser les IPspaces. Dans de nombreux cas, l'utilisation de machines virtuelles de stockage (SVM), avec leurs propres tables de routage IP distinctes, peut être utilisée pour isoler les configurations réseau uniques au lieu d'utiliser les IPspaces.

Exemple d'utilisation des IPspaces

Une application commune pour l'utilisation des IPspaces est le besoin d'un fournisseur de services de stockage (SSP) pour connecter les clients des entreprises A et B à un cluster ONTAP sur site du SSP. Dans les deux cas, les deux entreprises utilisent les mêmes plages d'adresse IP privées.

Le SSP crée des SVM sur le cluster pour chaque client et fournit un chemin réseau dédié entre deux SVM et le réseau de l'entreprise A, et entre les deux autres SVM et le réseau de l'entreprise B.

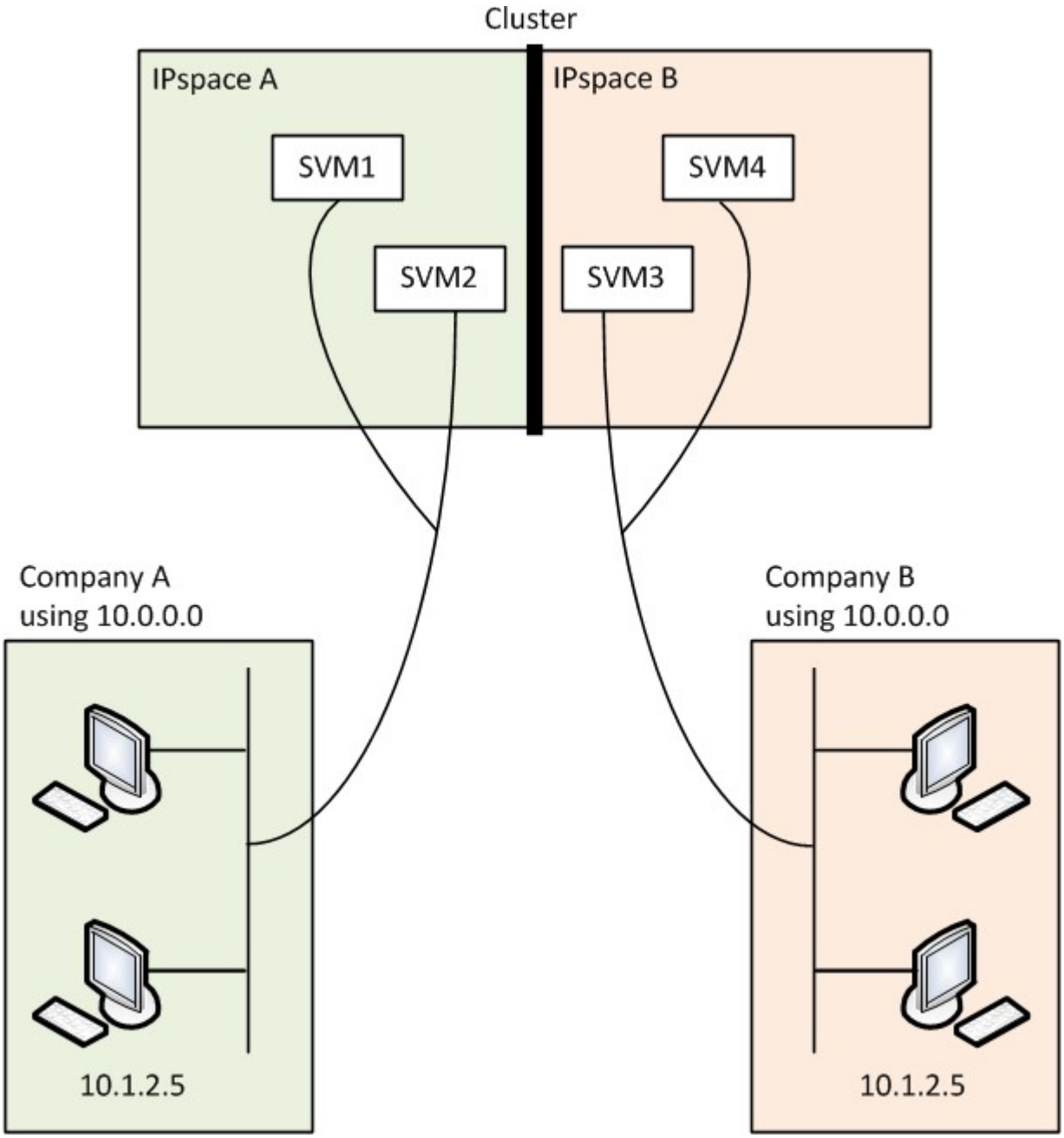
Ce type de déploiement est présenté dans l'illustration suivante et fonctionne si les deux sociétés utilisent des plages d'adresses IP non privées. Cependant, l'illustration montre que les deux sociétés utilisent les mêmes plages d'adresses IP privées, ce qui cause des problèmes.



Les deux entreprises utilisent le sous-réseau de l'adresse IP privée 10.0.0.0, ce qui entraîne les problèmes suivants :

- Les SVM du cluster sur le site SSP ont des adresses IP contradictoires si les deux entreprises décident d'utiliser la même adresse IP pour leurs SVM respectifs.
- Même si les deux entreprises conviennent d'utiliser différentes adresses IP pour leurs SVM, des problèmes peuvent survenir.
- Par exemple, si un client du réseau A possède la même adresse IP qu'un client du réseau B, les paquets destinés à un client de l'espace d'adresse A peuvent être routés vers un client dans l'espace d'adresse B, et vice versa.
- Si les deux sociétés décident d'utiliser des espaces d'adresse mutuellement exclusifs (par exemple, A utilise 10.0.0.0 avec un masque de réseau 255.128.0.0 et B utilise 10.128.0.0 avec un masque de réseau 255.128.0.0), Le SSP doit configurer des routes statiques sur le cluster pour acheminer le trafic de manière appropriée vers les réseaux A et B.

- Cette solution n'est ni évolutive (en raison des routes statiques), ni sécurisée (le trafic de diffusion est envoyé à toutes les interfaces du cluster).pour résoudre ces problèmes, le SSP définit deux IPspaces sur le cluster : un pour chaque entreprise. Étant donné qu'aucun trafic cross-IPspace n'est routé, les données de chaque entreprise sont acheminées de manière sécurisée vers son réseau respectif même si tous les SVM sont configurés dans l'espace d'adresse 10.0.0.0, comme illustré ci-dessous :



De plus, les adresses IP mentionnées par les différents fichiers de configuration, tels que `/etc/ hosts` fichier, le `/etc/hosts.equiv` fichier, et `the /etc/rc` Fichier, sont relatifs à cet IPspace. Les IPspaces permettent au SSP de configurer la même adresse IP pour plusieurs SVM, sans conflit.

Propriétés standard des IPspaces

Les IPspaces spéciaux sont créés par défaut lors de la première création du cluster. De plus, des machines virtuelles de stockage spéciales sont créées pour chaque IPspace.

Deux IPspaces sont créés automatiquement lors de l'initialisation du cluster :

- IPspace par défaut

  Cet IPspace est un conteneur pour les ports, les sous-réseaux et les SVM qui servent de données. Si votre configuration n'a pas besoin d'IPspaces distinctes pour les clients, tous les SVM peuvent être créés dans cet IPspace. Cet IPspace contient également les ports de gestion du cluster et des nœuds.

- IPspace « cluster »

  Cet IPspace contient tous les ports de cluster de tous les nœuds du cluster. Il est créé automatiquement lors de la création du cluster. Il assure la connectivité au réseau interne privé du cluster. À mesure que les nœuds supplémentaires rejoint le cluster, les ports de cluster à partir de ces nœuds sont ajoutés à l'IPspace « Cluster ».

Un SVM « système » existe pour chaque IPspace. Lorsque vous créez un IPspace, un SVM système par défaut du même nom est créé :

- Le SVM système pour le « Cluster » IPspace transmet le trafic du cluster entre les nœuds d'un cluster sur le réseau interne de cluster privé.

  Il est géré par l'administrateur du cluster, et il porte le nom « Cluster ».

- Le SVM système pour l'IPspace « par défaut » transmet le trafic de gestion du cluster et des nœuds, y compris le trafic intercluster entre les clusters.

  Il est géré par l'administrateur du cluster, et il utilise le même nom que le cluster.

- Le SVM système pour un IPspace personnalisé que vous créez implique le trafic de gestion pour ce SVM.

  Il est géré par l'administrateur du cluster, et il utilise le même nom que l'IPspace.

Un ou plusieurs SVM pour les clients peuvent exister dans un IPspace. Chaque SVM client dispose de ses propres volumes et configurations de données, et il est administré indépendamment des autres SVM.

Créez des IPspaces pour le réseau ONTAP

Les IPspaces sont des espaces d'adresse IP distincts dans lesquels les serveurs de stockage virtuels (SVM) résident. Vous pouvez créer des IPspaces lorsque vos SVM ont besoin de leur propre stockage, administration et routage sécurisés. Les IPspaces permettent de créer un espace d'adresse IP distinct pour chaque SVM dans un cluster. Ainsi, les clients se trouvant dans des domaines réseau distincts d'un point de vue administratif peuvent accéder aux données du cluster tout en utilisant des adresses IP redondantes à partir de la même plage de sous-réseaux.

Description de la tâche

Il existe une limite de 512 IPspaces au niveau du cluster. La limite à l'échelle du cluster est réduite à 256 IPspaces pour les clusters contenant des nœuds de 6 Go de RAM. Reportez-vous au Hardware Universe pour déterminer si des limites supplémentaires s'appliquent à votre plateforme.

"NetApp Hardware Universe"

Un nom IPspace ne peut pas être « tous », car « tous » est un nom réservé au système.

Avant de commencer

Vous devez être un administrateur de cluster pour effectuer cette tâche.

Étape

1. Création d'un IPspace :

```
network ipspace create -ipspace ipspace_name
```

`ipspace_name` Est le nom de l'IPspace que vous souhaitez créer. La commande suivante crée l'IPspace ipspace1 sur un cluster :

```
network ipspace create -ipspace ipspace1
```

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

2. Afficher les IPspaces :

`network ipspace show`

```
IPspace             Vserver List          Broadcast Domains
------------------- --------------------- ----------------------------
Cluster             Cluster               Cluster
Default             Cluster1              Default
ipspace1            ipspace1              -
```

L'IPspace est créé, ainsi que le système SVM pour l'IPspace. Le SVM système transmet le trafic de gestion.

Une fois que vous avez terminé

Si vous créez un IPspace dans un cluster avec une configuration MetroCluster, les objets IPspace doivent être répliqués manuellement sur les clusters partenaires. Tout SVM créé et affecté à un IPspace avant la réplication de l'IPspace ne sera pas répliqué sur les clusters partenaires.

Les domaines de diffusion sont créés automatiquement dans l'IPspace par défaut et peuvent être déplacés entre les IPspaces à l'aide de la commande suivante :

```
network port broadcast-domain move
```

Par exemple, si vous souhaitez déplacer un domaine de diffusion de « default » à « ips1 », à l'aide de la commande suivante :

```
network port broadcast-domain move -ipspace Default -broadcast-domain
Default -to-ipspace ips1
```

Afficher les IPspaces sur le réseau ONTAP

Vous pouvez afficher la liste des IPspaces qui existent dans un cluster et afficher les serveurs de stockage virtuels (SVM), les domaines de diffusion et les ports affectés à chaque IPspace.

Étape

Affichage des IPspaces et des SVM dans un cluster :

```
network ipspace show [-ipspace ipspace_name]
```

La commande suivante affiche tous les IPspaces, le SVM et les domaines de diffusion dans le cluster :

```
network ipspace show
IPspace        Vserver List             Broadcast Domains
-------------  -----------------------  -------------------
Cluster
               Cluster                  Cluster
Default
               vs1, cluster-1            Default
ipspace1
               vs3, vs4, ipspace1       bcast1
```

La commande suivante affiche les nœuds et les ports faisant partie de l'IPspace ipspace1 :

```
network ipspace show -ipspace ipspace1
IPspace name: ipspace1
Ports: cluster-1-01:e0c, cluster-1-01:e0d, cluster-1-01:e0e, cluster-1-
02:e0c, cluster-1-02:e0d, cluster-1-02:e0e
Broadcast Domains: Default-1
Vservers: vs3, vs4, ipspace1
```

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

Supprimez les IPspaces du réseau ONTAP

Si vous n'avez plus besoin d'un IPspace, vous pouvez le supprimer.

Avant de commencer

Il ne doit y avoir aucun domaine de diffusion, aucune interface réseau ou SVM associé à l'IPspace que vous

souhaitez supprimer.

Les IPspaces « Default » (Cluster-defined) et « Cluster » (Cluster-defined IPspaces) ne peuvent pas être supprimés.

Étape

Suppression d'un IPspace :

```
network ipspace delete -ipspace ipspace_name
```

La commande suivante supprime IPspace ipspace1 du cluster :

```
network ipspace delete -ipspace ipspace1
```

Pour en savoir plus, `network ipspace delete` consultez le "Référence de commande ONTAP".

Les domaines de diffusion

Découvrez les domaines de diffusion ONTAP

Les domaines de diffusion sont destinés à regrouper les ports réseau qui appartiennent au même réseau de couche 2. Les ports du groupe peuvent ensuite être utilisés par une machine virtuelle de stockage (SVM) pour le trafic de données ou de gestion.

> La gestion des domaines de diffusion est différente dans ONTAP 9.7 et les versions antérieures. Si vous devez gérer des domaines de diffusion sur un réseau exécutant ONTAP 9.7 et des versions antérieures, reportez-vous "Présentation du domaine de diffusion (ONTAP 9.7 et versions antérieures)"à la section .

Un domaine de diffusion réside dans un IPspace. Lors de l'initialisation du cluster, le système crée deux broadcast domain :

- Le broadcast domain « Default » contient les ports qui sont dans le « Default » IPspace.

  Ces ports servent principalement à transmettre des données. Les ports de management des clusters et de management des nœuds sont également présents dans ce broadcast domain.

- Le broadcast domain « Cluster » contient les ports qui sont dans le « Cluster » IPspace.

  Ces ports sont utilisés pour la communication de cluster et incluent tous les ports de cluster de tous les nœuds du cluster.

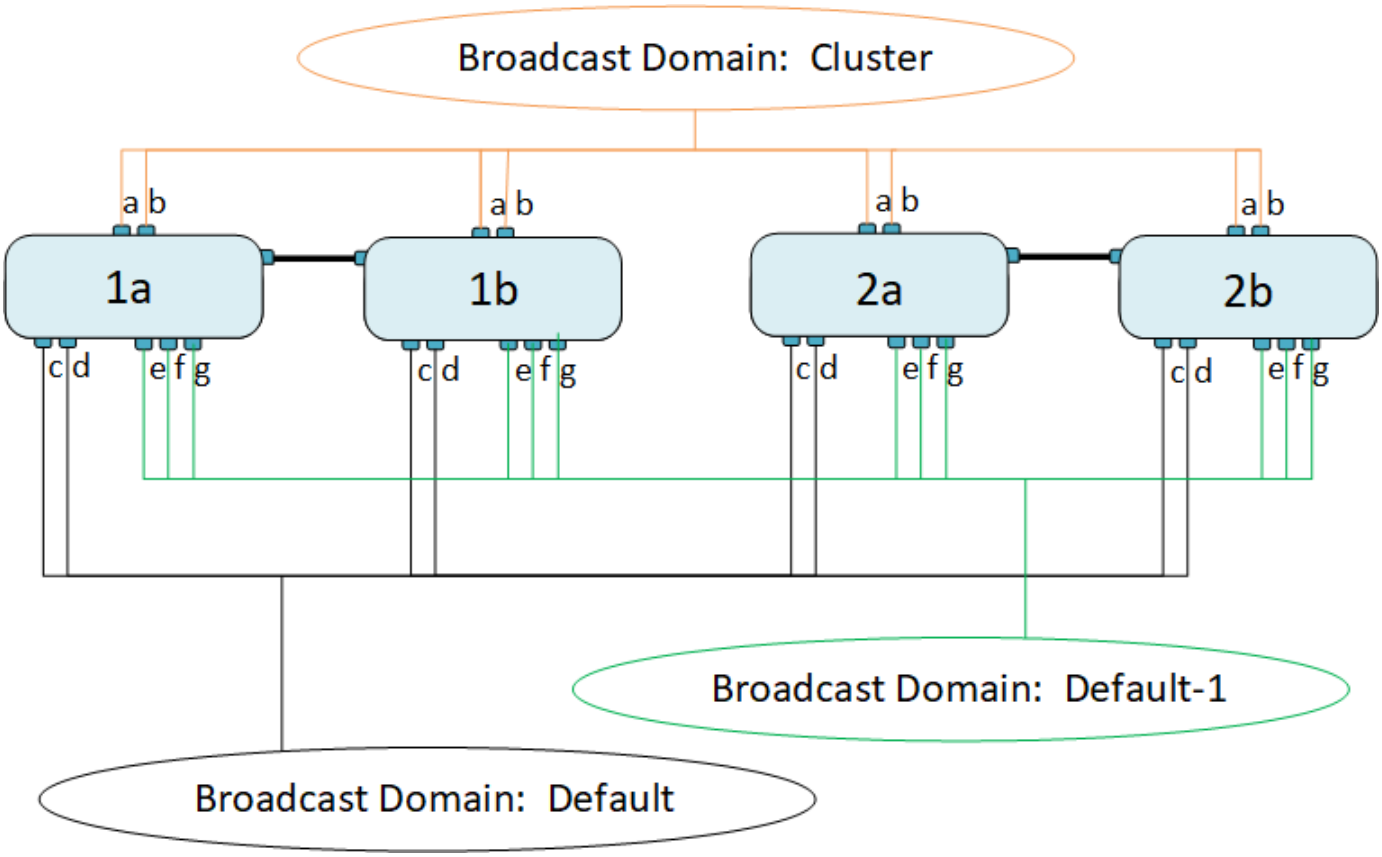
  Le système crée des domaines de diffusion supplémentaires dans l'IPspace par défaut si nécessaire. Le broadcast domain « Default » contient le home-port de la LIF de gestion, ainsi que tous les autres ports qui ont une accessibilité de couche 2 à ce port. Les domaines de diffusion supplémentaires sont nommés « default-1 », « default-2 », etc.

Exemple d'utilisation de domaines de diffusion

Un broadcast domain est un ensemble de ports réseau dans le même IPspace qui peut également être réachstable au niveau de la couche 2, notamment les ports de nombreux nœuds du cluster.

L'illustration montre les ports assignés à trois broadcast domain dans un cluster à quatre nœuds :

- Le broadcast domain « Cluster » est créé automatiquement lors de l'initialisation du cluster et il contient les ports a et b de chaque nœud du cluster.
- Le broadcast domain est également créé automatiquement lors de l'initialisation du cluster et il contient les ports c et d de chaque nœud du cluster.
- Le système crée automatiquement tout domaine de diffusion supplémentaire lors de l'initialisation du cluster en fonction de la capacité d'accès au réseau de couche 2. Ces domaines de diffusion supplémentaires sont nommés default-1, default-2, etc.



Un failover group du même nom avec les mêmes ports réseau que chacun des domaines de broadcast est créé automatiquement. Ce failover group est automatiquement géré par le système, ce qui signifie qu'à mesure que des ports sont ajoutés ou supprimés du broadcast domain, ils sont automatiquement ajoutés ou supprimés de ce failover group.

Créer des domaines de diffusion ONTAP

Les domaines de diffusion regroupent des ports réseau dans le cluster qui appartiennent au même réseau de couche 2. Les ports peuvent ensuite être utilisés par les SVM.

Les domaines de diffusion sont automatiquement créés lors de l'opération de création ou de jointure du cluster. Depuis ONTAP 9.12.0, outre les domaines de diffusion créés automatiquement, vous pouvez ajouter manuellement un domaine de diffusion dans System Manager.

La procédure de création des domaines de diffusion est différente dans ONTAP 9.7 et les versions antérieures. Si vous devez créer des domaines de diffusion sur un réseau exécutant ONTAP 9.7 et des versions antérieures, reportez-vous "Créer un domaine de diffusion (ONTAP 9.7 et versions antérieures)"à la section .

Avant de commencer

Les ports que vous prévoyez d'ajouter au broadcast domain ne doivent pas appartenir à un autre broadcast domain. Si les ports que vous souhaitez utiliser appartiennent à un autre domaine de diffusion mais sont inutilisés, supprimez ces ports du domaine de diffusion d'origine.

Description de la tâche

- Tous les noms de domaine de diffusion doivent être uniques au sein d'un IPspace.
- Les ports ajoutés à un domaine de diffusion peuvent être des ports réseau physiques, des VLAN ou des groupes d'interfaces/groupes d'agrégation de liens (LAG/ifgrps).
- Si les ports que vous souhaitez utiliser appartiennent à un autre domaine de diffusion, mais sont inutilisés, supprimez-les du domaine de diffusion existant avant de les ajouter au nouveau.
- L'unité de transmission maximale (MTU) des ports ajoutés à un domaine de diffusion est mise à jour vers la valeur MTU définie dans le domaine de diffusion.
- La valeur MTU doit correspondre à tous les périphériques connectés à ce réseau de couche 2, à l'exception du trafic de gestion du port e0M.
- Si vous ne spécifiez pas de nom IPspace, le domaine de diffusion est créé dans l'IPspace « par défaut ».

Pour faciliter la configuration du système, un failover group du même nom est créé automatiquement contenant les mêmes ports.

System Manager

Étapes

1. Sélectionnez **réseau > Présentation > domaine de diffusion**.
2. Cliquez sur + Add
3. Nommez le domaine de diffusion.
4. Définissez la MTU.
5. Sélectionner l'IPspace.
6. Enregistrez le domaine de diffusion.

Vous pouvez modifier ou supprimer un domaine de diffusion après son ajout.

CLI

Si vous utilisez ONTAP 9.8 et les versions ultérieures, les domaines de diffusion sont créés automatiquement en fonction de l'accessibilité de couche 2. Pour plus d'informations, voir "Réparation de l'accessibilité de l'orifice".

Vous pouvez également créer manuellement un domaine de diffusion.

Étapes

1. Afficher les ports qui ne sont pas actuellement affectés à un broadcast domain :

   ```
   network port show
   ```

   Si l'affichage est grand, utilisez le `network port show -broadcast-domain` commande pour afficher uniquement les ports non assignés.

2. Créer un broadcast domain :

   ```
   network port broadcast-domain create -broadcast-domain
   broadcast_domain_name -mtu mtu_value [-ipspace ipspace_name] [-ports
   ports_list]
   ```

   a. `broadcast_domain_name` est le nom du domaine de diffusion que vous souhaitez créer.

   b. `mtu_value` Est la taille de MTU des paquets IP ; 1500 et 9000 sont des valeurs types.

      Cette valeur est appliquée à tous les ports ajoutés à ce broadcast domain.

   c. `ipspace_name` Est le nom de l'IPspace à laquelle ce broadcast domain sera ajouté.

      L'IPspace par défaut est utilisé sauf si vous spécifiez une valeur pour ce paramètre.

   d. `ports_list` est la liste des ports qui seront ajoutés au broadcast domain.

      Les ports sont ajoutés au format `node_name:port_number`, par exemple, `node1:e0c`.

3. Vérifiez que le domaine de diffusion a été créé comme vous le souhaitez :

   ```
   network port show -instance -broadcast-domain new_domain
   ```

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

Exemple

La commande suivante crée broadcast domain bcast1 dans l'IPspace par défaut, définit le MTU sur 1500 et ajoute quatre ports :

`network port broadcast-domain create -broadcast-domain` *`bcast1`* `-mtu` *`1500`* `-ports` *`cluster1-01:e0e,cluster1-01:e0f,cluster1-02:e0e,cluster1-02:e0f`*

Pour en savoir plus, `network port broadcast-domain create` consultez le "Référence de commande ONTAP".

Une fois que vous avez terminé

Vous pouvez définir le pool d'adresses IP qui seront disponibles dans le broadcast domain en créant un sous-réseau, ou encore attribuer des SVM et des interfaces au IPspace à ce moment. Pour plus d'informations, voir "Cluster et SVM peering".

Si vous devez modifier le nom d'un domaine de diffusion existant, utilisez le `network port broadcast-domain rename` commande.

Pour en savoir plus, `network port broadcast-domain rename` consultez le "Référence de commande ONTAP".

Ajoutez ou supprimez des ports d'un domaine de diffusion ONTAP

Les domaines de diffusion sont automatiquement créés lors de l'opération de création ou de jointure du cluster. Il n'est pas nécessaire de supprimer manuellement les ports des domaines de diffusion.

Si l'accessibilité du port réseau a changé, via la connectivité réseau physique ou la configuration du commutateur, et qu'un port réseau appartient à un autre domaine de diffusion, reportez-vous à la rubrique suivante :

"Réparation de l'accessibilité de l'orifice"

> La procédure d'ajout ou de suppression de ports pour les domaines de diffusion est différente dans ONTAP 9.7 et les versions antérieures. Si vous devez ajouter ou supprimer des ports de domaines de diffusion sur un réseau exécutant ONTAP 9.7 et des versions antérieures, reportez-vous à la section "Ajouter ou supprimer des ports d'un domaine de diffusion (ONTAP 9.7 et versions antérieures)".

System Manager

À partir de ONTAP 9.14.1, vous pouvez utiliser System Manager pour réaffecter des ports Ethernet sur des domaines de diffusion. Il est recommandé d'attribuer chaque port Ethernet à un domaine de diffusion. Ainsi, si vous annulez l'attribution d'un port Ethernet à un domaine de diffusion, vous devez le réaffecter à un autre domaine de diffusion.

Étapes

Pour réaffecter des ports Ethernet, effectuez les opérations suivantes :

1. Sélectionnez **réseau > vue d'ensemble**.
2. Dans la section **Broadcast Domains**, sélectionnez ⋮ en regard du nom de domaine.
3. Dans le menu déroulant, sélectionnez **Modifier**.
4. Sur la page **Edit Broadcast Domain**, désélectionnez les ports Ethernet que vous souhaitez réaffecter à un autre domaine.
5. Pour chaque port désélectionné, la fenêtre **réaffecter le port Ethernet** s'affiche. Sélectionnez le domaine de diffusion auquel vous souhaitez réaffecter le port, puis sélectionnez **réaffecter**.
6. Sélectionnez tous les ports que vous souhaitez affecter au domaine de diffusion actuel et enregistrez vos modifications.

CLI

Si l'accessibilité du port réseau a changé, via la connectivité réseau physique ou la configuration du commutateur, et qu'un port réseau appartient à un autre domaine de diffusion, reportez-vous à la rubrique suivante :

"Réparation de l'accessibilité de l'orifice"

Vous pouvez également ajouter ou supprimer manuellement des ports de domaines de diffusion à l'aide du `network port broadcast-domain add-ports` ou le `network port broadcast-domain remove-ports` commande.

Avant de commencer

- Vous devez être un administrateur de cluster pour effectuer cette tâche.
- Les ports que vous prévoyez d'ajouter à un broadcast domain ne doivent pas appartenir à un autre broadcast domain.
- Les ports qui appartiennent déjà à un groupe d'interface ne peuvent pas être ajoutés individuellement à un broadcast domain.

Description de la tâche

Les règles suivantes s'appliquent lors de l'ajout et de la suppression de ports réseau :

Lors de l'ajout de ports…	Lors de la suppression des ports…
Les ports peuvent être des ports réseau, des VLAN ou des groupes d'interfaces (ifgrps).	S/O
Les ports sont ajoutés au groupe de basculement défini par le système du broadcast domain.	Les ports sont supprimés de tous les failover groups dans le broadcast domain.
La MTU des ports est mise à jour vers la valeur MTU définie dans le domaine de diffusion.	La MTU des ports est inchangée.

L'IPspace des ports est mis à jour vers la valeur IPspace du broadcast domain.	Les ports sont déplacés vers l'IPspace « par défaut » sans attribut de domaine de diffusion.

Si vous supprimez le dernier port membre d'un groupe d'interfaces à l'aide de la `network port ifgrp remove-port` commande, le port du groupe d'interfaces est supprimé du broadcast domain car un port vide du groupe d'interfaces n'est pas autorisé dans un broadcast domain. Pour en savoir plus, `network port ifgrp remove-port` consultez le "Référence de commande ONTAP".

Étapes

1. Affiche les ports actuellement affectés ou non affectés à un domaine de diffusion à l'aide de l' `network port show` commande.
2. Ajouter ou supprimer des ports réseau du broadcast domain :

Les fonctions que vous recherchez…	Utiliser…
Permet d'ajouter des ports à un domaine de diffusion	`network port broadcast-domain add-ports`
Supprime des ports d'un broadcast domain	`network port broadcast-domain remove-ports`

3. Vérifiez que les ports ont été ajoutés ou supprimés du broadcast domain :

   `network port show`

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

Exemples d'ajout et de suppression de ports

La commande suivante ajoute le port e0g sur le nœud cluster-1-01 et le port e0g sur le nœud cluster-1-02 au broadcast domain bcast1 dans l'IPspace par défaut :

```
cluster-1::> network port broadcast-domain add-ports -broadcast-domain bcast1
-ports cluster-1-01:e0g,cluster1-02:e0g
```

La commande suivante ajoute deux ports de cluster à broadcast domain Cluster dans le Cluster IPspace :

```
cluster-1::> network port broadcast-domain add-ports -broadcast-domain Cluster
-ports cluster-2-03:e0f,cluster2-04:e0f -ipspace Cluster
```

La commande suivante supprime le port e0e sur le nœud cluster1-01 du broadcast domain bcast1 dans le Default IPspace :

```
cluster-1::> network port broadcast-domain remove-ports -broadcast-domain
bcast1 -ports cluster-1-01:e0e
```

Pour en savoir plus, `network port broadcast-domain remove-ports` consultez le "Référence de commande ONTAP".

Informations associées

- "Référence de commande ONTAP"

Réparer l’accessibilité du port ONTAP

Les domaines de diffusion sont créés automatiquement. Cependant, si un port est recâblage ou si la configuration du commutateur change, un port peut avoir besoin d’être réparé dans un domaine de diffusion différent (nouveau ou existant).

ONTAP peut détecter et recommander automatiquement des solutions aux problèmes de câblage réseau en fonction de la capacité de couche 2 d’un composant de domaine de diffusion (ports ethernet).

Un câblage incorrect pendant peut provoquer une affectation de port de domaine de diffusion inattendue. Depuis ONTAP 9.10.1, le cluster vérifie automatiquement la présence de problèmes de câblage réseau en vérifiant la capacité de port après la configuration du cluster ou lorsqu’un nouveau nœud rejoint un cluster existant.

System Manager

Si un problème de capacité de port est détecté, System Manager recommande une opération de réparation pour résoudre le problème.

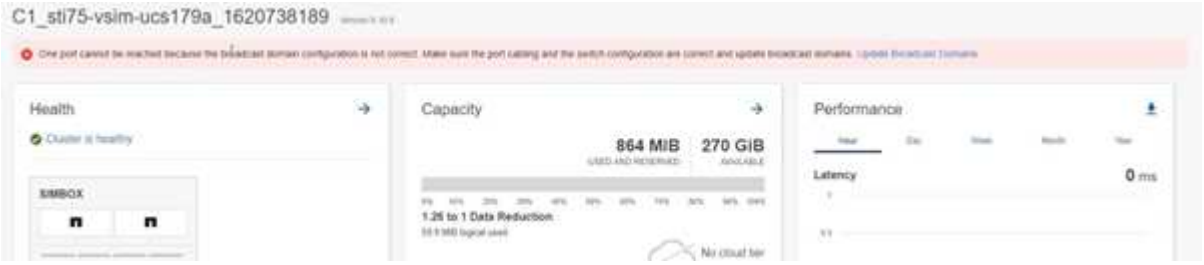
Une fois le cluster configuré, des problèmes de câblage réseau sont signalés sur le tableau de bord.

Après l'ajout d'un nouveau nœud à un cluster, des problèmes de câblage réseau apparaissent sur la page nœuds.

Vous pouvez également afficher l'état du câblage réseau sur le schéma de réseau. Les problèmes de capacité de port sont indiqués sur le schéma du réseau par une icône d'erreur rouge.

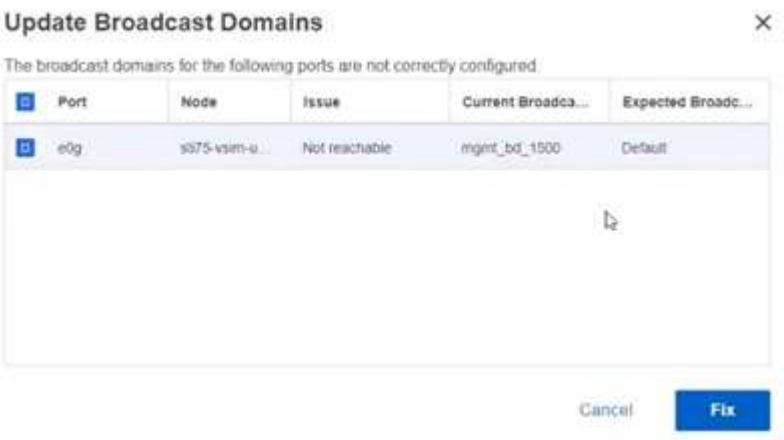
Post-configuration du cluster

Une fois le cluster configuré, si le système détecte un problème de câblage réseau, un message s'affiche sur le tableau de bord.



Étapes

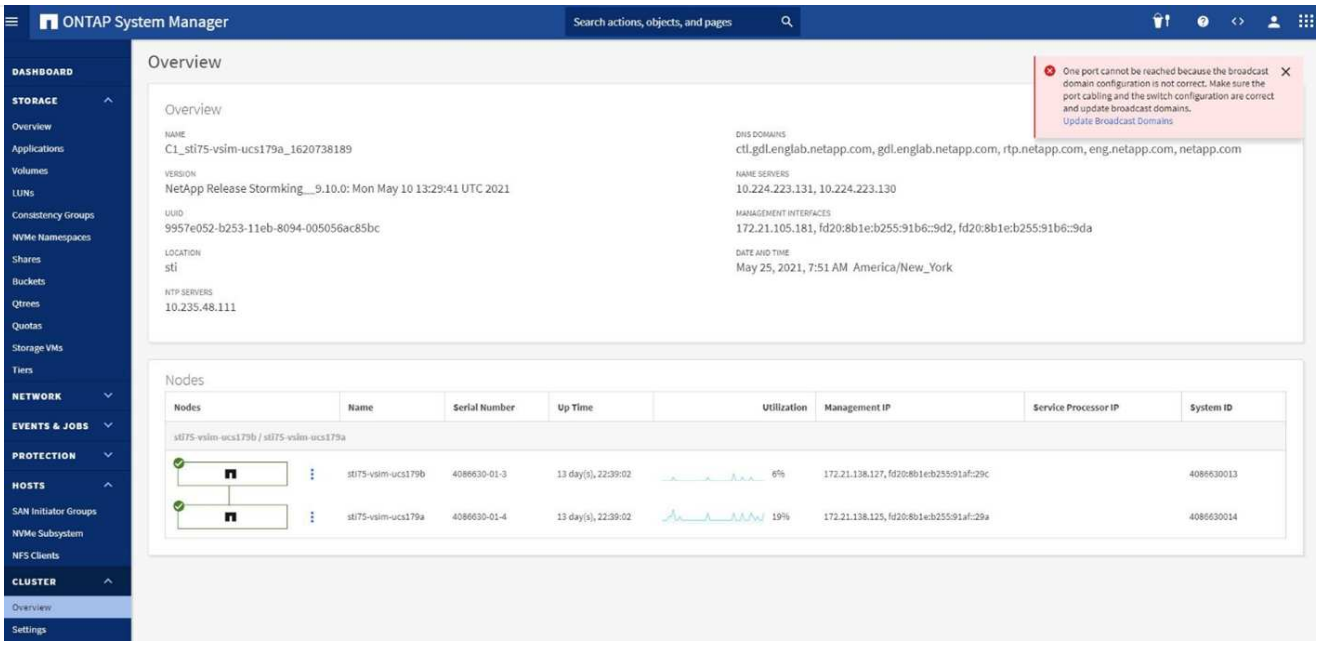
1. Corriger le câblage comme indiqué dans le message.
2. Cliquez sur le lien pour lancer la boîte de dialogue mettre à jour les domaines de diffusion.
   La boîte de dialogue mettre à jour les domaines de diffusion s'ouvre.



3. Examinez les informations sur le port, y compris le nœud, les problèmes, le domaine de diffusion actuel et le domaine de diffusion attendu.
4. Sélectionnez les ports à réparer et cliquez sur **Fix**.
   Le système déplace les ports du domaine de diffusion actuel vers le domaine de diffusion attendu.

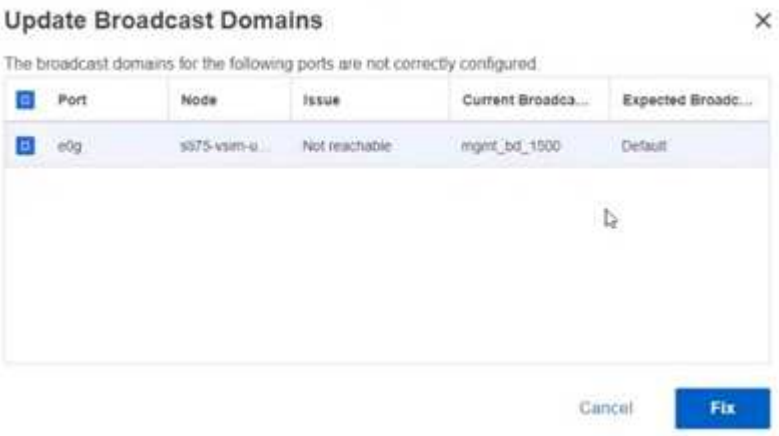
Jointure post-nœud

Après l'ajout d'un nouveau nœud à un cluster, si le système détecte un problème de câblage réseau, un message s'affiche sur la page nœuds.



Étapes

1. Corriger le câblage comme indiqué dans le message.
2. Cliquez sur le lien pour lancer la boîte de dialogue mettre à jour les domaines de diffusion.
   La boîte de dialogue mettre à jour les domaines de diffusion s'ouvre.



3. Examinez les informations sur le port, y compris le nœud, les problèmes, le domaine de diffusion actuel et le domaine de diffusion attendu.
4. Sélectionnez les ports à réparer et cliquez sur **Fix**.
   Le système déplace les ports du domaine de diffusion actuel vers le domaine de diffusion attendu.

CLI

Avant de commencer

Vous devez être un administrateur de cluster pour effectuer cette tâche.

Description de la tâche

Une commande est disponible pour réparer automatiquement la configuration du domaine de diffusion pour un port basé sur la capacité d'accessibilité de couche 2 détectée par ONTAP.

Étapes

1. Vérifiez la configuration et le câblage de votre commutateur.

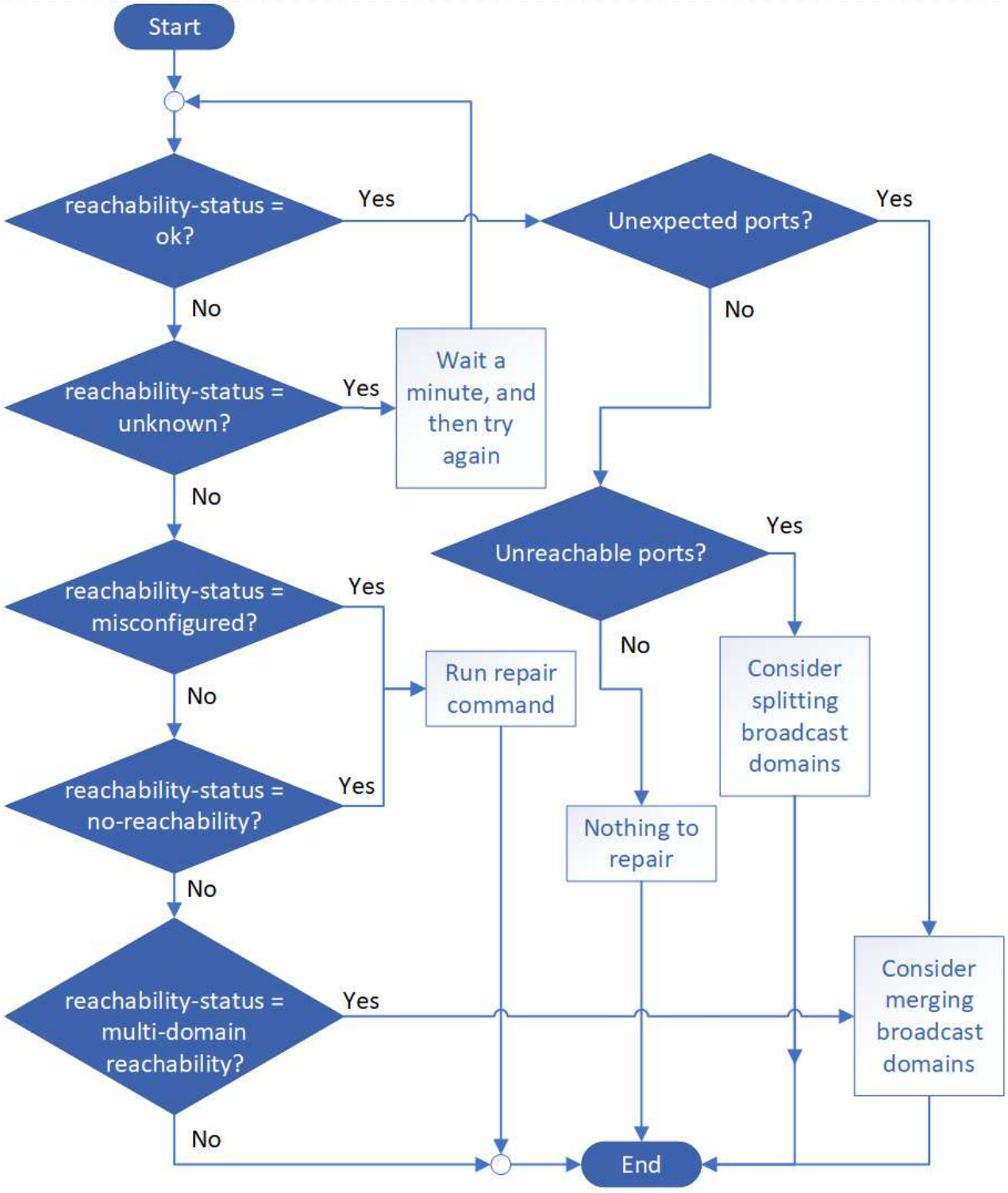
2. Vérifiez l'accessibilité du port :

   ```
   network port reachability show -detail -node -port
   ```

   La sortie de la commande contient les résultats de l'accessibilité.

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

3. Utilisez l'arbre décisionnel et le tableau ci-dessous pour comprendre les résultats de l'accessibilité et déterminer ce que, le cas échéant, faire ensuite.



État-accessibilité	Description

ok	Le port a une capacité de réachbilité de couche 2 à son domaine de diffusion attribué. Si l'état de la capacité d'accessibilité est « ok », mais qu'il y a des « ports inattendus », envisagez de fusionner un ou plusieurs domaines de diffusion. Pour plus d'informations, reportez-vous à la *Unexpected ports* row suivante. Si le statut de la capacité d'accessibilité est « ok », mais qu'il y a des « ports inaccessibles », envisagez de diviser un ou plusieurs domaines de diffusion. Pour plus d'informations, reportez-vous à la ligne *ports inaccessibles* suivante. Si l'état de la capacité de reprise est « ok » et qu'il n'y a pas de ports inattendus ou inaccessibles, votre configuration est correcte.
Ports inattendus	Le port a une capacité de réachbilité de couche 2 à son domaine de diffusion attribué ; cependant, il a également la possibilité de reachcapacité de couche 2 à au moins un autre domaine de broadcast. Examinez la connectivité physique et la configuration du commutateur pour déterminer s'il est incorrect ou si le domaine de diffusion attribué au port doit être fusionné avec un ou plusieurs domaines de diffusion. Pour plus d'informations, voir "Fusionner les domaines de diffusion".
Ports inaccessibles	Si un seul domaine de diffusion a été partitionné en deux ensembles de capacité d'accès différents, vous pouvez fractionner un domaine de diffusion pour synchroniser la configuration ONTAP avec la topologie de réseau physique. En général, la liste des ports inaccessibles définit l'ensemble des ports qui doivent être divisés en un autre domaine de diffusion après avoir vérifié que la configuration physique et du commutateur est exacte. Pour plus d'informations, voir "Séparer les domaines de diffusion".
mauvaise configuration de la capacité de réachbilité	Le port n'a pas la capacité de reachcapacité de couche 2 à son domaine de diffusion affecté ; cependant, le port a une capacité de réachcapacité de couche 2 à un domaine de diffusion différent. Vous pouvez réparer l'accessibilité du port. Lorsque vous exécutez la commande suivante, le système affecte le port au broadcast domain auquel il a la capacité de reachcapacité : `network port reachability repair -node -port`

sans trabilité	Le port n'a pas la possibilité de reachcapacité de couche 2 à un domaine de diffusion existant. Vous pouvez réparer l'accessibilité du port. Lorsque vous exécutez la commande suivante, le système affecte le port à un nouveau domaine de diffusion créé automatiquement dans l'IPspace par défaut : `network port reachability repair -node -port` **Remarque :** si tous les ports membres du groupe d'interfaces (ifgrp) signalent `no-reachability`, exécutant le `network port reachability repair` sur chaque port membre, chaque port est supprimé de l'ifgrp et placé dans un nouveau domaine de diffusion, ce qui entraîne la suppression de l'ifgrp lui-même. Avant d'utiliser le `network port reachability repair` vérifiez que le domaine de diffusion accessible du port correspond à ce que vous attendez en fonction de la topologie de votre réseau physique. Pour en savoir plus, `network port reachability repair` consultez le "Référence de commande ONTAP".
accessibilité multi-domaines	Le port a une capacité de réachbilité de couche 2 à son domaine de diffusion attribué ; cependant, il a également la possibilité de reachcapacité de couche 2 à au moins un autre domaine de broadcast. Examinez la connectivité physique et la configuration du commutateur pour déterminer s'il est incorrect ou si le domaine de diffusion attribué au port doit être fusionné avec un ou plusieurs domaines de diffusion. Pour plus d'informations, voir "Fusionner les domaines de diffusion".
inconnu	Si l'état de la capacité d'accessibilité est « inconnu », attendez quelques minutes et essayez à nouveau la commande.

Après avoir réparé un port, vérifiez s'il y a des LIFs et des VLAN déplacés. Si le port faisait partie d'un groupe d'interfaces, vous devez également connaître ce qui s'est passé pour ce groupe.

LIF

Lorsqu'un port est réparé et déplacé dans un autre domaine de diffusion, tous les LIFs configurés sur le port réparé se voient automatiquement attribuer un nouveau port de base. Si possible, ce port home est sélectionné dans le même domaine de diffusion sur le même nœud. Vous pouvez également sélectionner un port home port à partir d'un autre nœud ou, s'il n'existe aucun port home approprié, celui-ci sera effacé.

Si le port de rattachement d'une LIF est déplacé vers un autre nœud ou est désactivé, la LIF est considérée comme ayant été « déplacée ». Vous pouvez afficher ces LIFs déplacées à l'aide de la commande suivante :

```
displaced-interface show
```

Si des LIF sont déplacées, il faut soit :

- Restaurer le domicile de la LIF déplacée :

```
displaced-interface restore
```

- Définir l'origine du LIF manuellement :

  ```
  network interface modify -home-port -home-node
  ```

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

- Supprimer l'entrée de la table « déplacés-interface » si vous êtes satisfait du domicile actuellement configuré du LIF :

  ```
  displaced-interface delete
  ```

VLAN

Si le port réparé comporte des VLAN, ces derniers sont automatiquement supprimés mais sont également enregistrés comme ayant été « déplacés ». Vous pouvez afficher les VLAN déplacés suivants :

```
displaced-vlans show
```

En cas de déplacement de réseaux locaux virtuels, vous devez :

- Restaurez les VLAN sur un autre port :

  ```
  displaced-vlans restore
  ```

- Supprimez l'entrée du tableau « déplacés-vlan » :

  ```
  displaced-vlans delete
  ```

Groupes d'interface

Si le port réparé faisait partie d'un groupe d'interfaces, il est retiré de ce groupe d'interfaces. S'il s'agissait du seul port membre attribué au groupe d'interface, le groupe d'interface lui-même est supprimé.

Informations associées

- "Vérifiez votre configuration réseau après la mise à niveau"
- "Surveiller l'accessibilité des ports réseau"
- "Référence de commande ONTAP"

Déplacez les domaines de diffusion ONTAP dans les IPspaces

À partir de ONTAP 9.8, vous pouvez déplacer les domaines de diffusion créés par le système en fonction de l'accessibilité de la couche 2 dans les IPspaces que vous avez créés.

Avant de déplacer le domaine de diffusion, vous devez vérifier l'accessibilité des ports de vos domaines de diffusion.

L'analyse automatique des ports peut déterminer quels ports peuvent se toucher et les placer dans le même domaine de diffusion, mais cette analyse ne peut pas déterminer l'IPspace approprié. Si le domaine de

diffusion appartient à un IPspace non-défaut, vous devez le déplacer manuellement en suivant les étapes de cette section.

Avant de commencer

Les domaines de diffusion sont automatiquement configurés dans le cadre des opérations de création et de jointure du cluster. ONTAP définit le broadcast domain « Default » comme l'ensemble des ports qui ont une connectivité de couche 2 vers le home port de l'interface de gestion sur le premier nœud créé dans le cluster. D'autres domaines de diffusion sont créés, si nécessaire, et sont nommés **default-1**, **default-2**, etc.

Lorsqu'un nœud rejoint un cluster existant, ses ports réseau rejoignent automatiquement les domaines de diffusion existants en fonction de leur accessibilité de couche 2. S'ils n'ont pas la possibilité de reacher un domaine de diffusion existant, les ports sont placés dans un ou plusieurs nouveaux domaines de diffusion.

Description de la tâche

- Les ports avec LIF de cluster sont automatiquement placés dans l'IPspace « Cluster ».
- Les ports qui reachcapacité au home port de la LIF node-management sont placés dans le broadcast « default ».
- Les autres domaines de diffusion sont automatiquement créés par ONTAP dans le cadre de l'opération de création ou de jointure du cluster.
- Au fur et à mesure de l'ajout de VLAN et de groupes d'interface, ils sont automatiquement placés dans le domaine de diffusion approprié une minute après leur création.

Étapes

1. Vérifiez l'accessibilité des ports de vos domaines de diffusion. ONTAP surveille automatiquement l'accessibilité de couche 2. Utilisez la commande suivante pour vérifier que chaque port a été ajouté à un broadcast domain et a la capacité de reachable « ok ».

   ```
   network port reachability show -detail
   ```

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

2. Si nécessaire, déplacez les domaines de diffusion vers d'autres IPspaces :

   ```
   network port broadcast-domain move
   ```

   Par exemple, si vous souhaitez déplacer un domaine de diffusion de « Default » à « ips1 » :

   ```
   network port broadcast-domain move -ipspace Default -broadcast-domain Default
   -to-ipspace ips1
   ```

Informations associées

- "déplacement broadcast-domain port réseau"

Diviser les domaines de diffusion ONTAP

Si l'accessibilité des ports réseau a changé, via la connectivité réseau physique ou la configuration du commutateur, De plus, un groupe de ports réseau précédemment configurés dans un domaine de diffusion unique est désormais partitionné en deux ensembles de capacité d'accès différents, vous pouvez fractionner un domaine de

diffusion pour synchroniser la configuration ONTAP avec la topologie de réseau physique.

> La procédure de fractionnement des domaines de diffusion est différente dans ONTAP 9.7 et les versions antérieures. Si vous devez séparer les domaines de diffusion sur un réseau exécutant ONTAP 9.7 et les versions antérieures, reportez-vous à la section "Domaines de diffusion divisés (ONTAP 9.7 ou version antérieure)".

Pour déterminer si un domaine de diffusion de port réseau est partitionné en plusieurs ensembles d'accessibilité, utilisez la `network port reachability show -details` commande et faites attention aux ports qui n'ont pas de connectivité les uns avec les autres (« ports inaccessibles »). En général, la liste des ports inaccessibles définit l'ensemble des ports qui doivent être divisés en un autre domaine de diffusion, après avoir vérifié que la configuration physique et du commutateur est exacte. Pour en savoir plus, `network port reachability show` consultez le "Référence de commande ONTAP".

Étape

Diviser un domaine de diffusion en deux domaines de diffusion :

```
network port broadcast-domain split -ipspace <ipspace_name> -broadcast
-domain <broadcast_domain_name> -new-broadcast-domain
<broadcast_domain_name> -ports <node:port,node:port>
```

- `ipspace_name` est le nom de l'ipspace où réside le domaine de diffusion.
- `-broadcast-domain` est le nom du domaine de diffusion qui sera partagé.
- `-new-broadcast-domain` est le nom du nouveau domaine de diffusion qui sera créé.
- `-ports` est le nom du nœud et le port à ajouter au nouveau broadcast domain.

Informations associées

- "répartition broadcast-domain du port réseau"

Fusionner les domaines de diffusion ONTAP

Si la capacité d'accessibilité des ports réseau a changé, soit par le biais de la connectivité réseau physique, soit par la configuration des commutateurs, et si deux groupes de ports réseau précédemment configurés dans plusieurs domaines de diffusion sont désormais tous des domaines de partage, la fusion de deux domaines de diffusion peut être utilisée pour synchroniser la configuration ONTAP avec la topologie du réseau physique.

> La procédure de fusion des domaines de diffusion est différente dans ONTAP 9.7 et les versions antérieures. Si vous devez fusionner des domaines de diffusion sur un réseau exécutant ONTAP 9.7 et des versions antérieures, reportez-vous à la section "Fusionner les domaines de diffusion (ONTAP 9.7 ou version antérieure)".

Pour déterminer si plusieurs domaines de diffusion appartiennent à un ensemble d'accessibilité, utilisez le `network port reachability show -details` commandez et faites attention aux ports configurés dans un autre domaine de diffusion qui ont réellement une connectivité les uns avec les autres (« Ports inattendus

»). En général, la liste des ports inattendus définit l'ensemble des ports qui doivent être fusionnés dans le domaine de diffusion après avoir vérifié que la configuration physique et de commutateur est exacte.

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

Étape

Fusionner les ports d'un domaine de diffusion dans un domaine de diffusion existant :

```
network port broadcast-domain merge -ipspace <ipspace_name> -broadcast
-domain <broadcast_domain_name> -into-broadcast-domain
<broadcast_domain_name>
```

- `ipspace_name` est le nom de l'ipspace où résident les domaines de diffusion.
- `-broadcast-domain` est le nom du domaine de diffusion qui sera fusionné.
- `-into-broadcast-domain` est le nom du domaine de diffusion qui recevra des ports supplémentaires.

Informations associées

- "port réseau broadcast-domain-merge"

Modifiez la valeur MTU pour les ports d'un domaine de diffusion ONTAP

Vous pouvez modifier la valeur MTU d'un domaine de diffusion pour modifier la valeur MTU de tous les ports de ce domaine de diffusion. Cela peut être fait pour prendre en charge les modifications de topologie effectuées sur le réseau.

> La procédure de modification de la valeur MTU pour les ports de domaine de diffusion est différente dans ONTAP 9.7 et les versions antérieures. Si vous devez modifier la valeur MTU pour les ports de domaine de diffusion sur un réseau exécutant ONTAP 9.7 et des versions antérieures, reportez-vous à la section "Modifier la valeur MTU pour les ports d'un domaine de diffusion (ONTAP 9.7 et versions antérieures)".

System Manager

À partir de ONTAP 9.12.1, vous pouvez utiliser System Manager pour modifier la valeur MTU d'un domaine de diffusion afin de changer la valeur MTU de tous les ports de ce domaine de diffusion.

Étapes

1. Sélectionnez **Network > Broadcast Domains**.
2. Dans la section **Domaines de diffusion**, sélectionnez le nom du broadcast domain pour lequel vous souhaitez modifier la valeur MTU.
3. Un message vous invite à confirmer la modification de la valeur MTU pour tous les ports du domaine de diffusion. Cliquez sur **Oui** pour procéder à la modification.
4. Modifiez la valeur MTU si nécessaire et enregistrez vos modifications.

   Le système applique la nouvelle valeur MTU à tous les ports du domaine de diffusion, ce qui provoque une brève interruption du trafic sur ces ports.

CLI

Avant de commencer

La valeur MTU doit correspondre à tous les périphériques connectés à ce réseau de couche 2, à l'exception du trafic de gestion du port e0M.

Description de la tâche

La modification de la valeur MTU entraîne une brève interruption du trafic sur les ports concernés. Le système affiche un message auquel vous devez répondre par **y** pour valider la modification de la MTU.

Étape

Modifier la valeur MTU pour tous les ports d'un domaine de diffusion :

```
network port broadcast-domain modify -broadcast-domain
<broadcast_domain_name> -mtu <mtu_value> [-ipspace <ipspace_name>]
```

Où :

- `broadcast_domain` est le nom du domaine de diffusion.
- `mtu` Est la taille de MTU des paquets IP ; 1500 et 9000 sont des valeurs types.
- `ipspace` est le nom de l'espace IP dans lequel ce domaine de diffusion réside. L'IPspace « Default » est utilisé sauf si vous spécifiez une valeur pour cette option.

  La commande suivante modifie la MTU à 9000 pour tous les ports du domaine de diffusion bcast1 :

  ```
  network port broadcast-domain modify -broadcast-domain <Default-1>
  -mtu < 9000 >
  Warning: Changing broadcast domain settings will cause a momentary
  data-serving interruption.
  Do you want to continue? {y|n}: <y>
  ```

Informations associées

- "port réseau broadcast-domain modify"

Afficher les domaines de diffusion ONTAP

Vous pouvez afficher la liste des domaines de broadcast au sein de chaque IPspace dans un cluster. La sortie affiche également la liste des ports et la valeur MTU pour chaque domaine de diffusion.

> La procédure d'affichage des domaines de diffusion est différente dans ONTAP 9.7 et les versions antérieures. Si vous devez afficher des domaines de diffusion sur un réseau exécutant ONTAP 9.7 et des versions antérieures, reportez-vous "Afficher les domaines de diffusion (ONTAP 9.7 ou version antérieure)"à la section .

Étape

Afficher les broadcast domain et les ports associés dans le cluster :

```
network port broadcast-domain show
```

La commande suivante affiche tous les broadcast domain et les ports associés du cluster :

```
network port broadcast-domain show
IPspace Broadcast                                 Update
Name    Domain Name  MTU   Port List              Status Details
------- ------------ -----  ---------------------- --------------
Cluster Cluster      9000
                           cluster-1-01:e0a       complete
                           cluster-1-01:e0b       complete
                           cluster-1-02:e0a       complete
                           cluster-1-02:e0b       complete
Default Default      1500
                           cluster-1-01:e0c       complete
                           cluster-1-01:e0d       complete
                           cluster-1-02:e0c       complete
                           cluster-1-02:e0d       complete
        Default-1    1500
                           cluster-1-01:e0e       complete
                           cluster-1-01:e0f       complete
                           cluster-1-01:e0g       complete
                           cluster-1-02:e0e       complete
                           cluster-1-02:e0f       complete
                           cluster-1-02:e0g       complete
```

La commande suivante affiche les ports du broadcast domain default-1 qui ont un statut de mise à jour de l'erreur, ce qui indique que le port n'a pas pu être mis à jour correctement :

```
network port broadcast-domain show -broadcast-domain Default-1 -port
-update-status error

IPspace Broadcast                                 Update
Name    Domain Name  MTU   Port List              Status Details
------- ------------ -----  ---------------------- --------------
Default Default-1    1500
                            cluster-1-02:e0g       error
```

Informations associées

- "broadcast-domain-domain port réseau show"

Supprimer les domaines de diffusion ONTAP

Si vous n'avez plus besoin d'un domaine de diffusion, vous pouvez le supprimer. Cela déplace les ports associés à ce broadcast domain vers le « Default » IPspace.

Avant de commencer

Il ne doit y avoir aucun sous-réseau, aucune interface réseau ou SVM associé au broadcast domain que vous souhaitez supprimer.

Description de la tâche

- Le domaine de diffusion « Cluster » créé par le système ne peut pas être supprimé.
- Tous les Failover Groups liés au broadcast domain sont supprimés lorsque vous supprimez le broadcast domain.

La procédure à suivre dépend de l'interface que vous utilisez—System Manager ou de l'interface de ligne de commandes :

System Manager

À partir de ONTAP 9.12.0, vous pouvez utiliser System Manager pour supprimer un domaine de diffusion

L'option de suppression n'est pas affichée lorsque le broadcast domain contient des ports ou est associé à un sous-réseau.

Étapes

1. Sélectionnez **réseau > Présentation > domaine de diffusion**.
2. Sélectionnez ⋮ **> Supprimer** en regard du domaine de diffusion que vous souhaitez supprimer.

CLI

Utilisez l'interface de ligne de commande pour supprimer un domaine de diffusion

Étape

Supprimer un broadcast domain :

```
network port broadcast-domain delete -broadcast-domain broadcast_domain_name
[-ipspace ipspace_name]
```

La commande suivante supprime le domaine de diffusion default-1 dans IPspace ipspace1 :

```
network port broadcast-domain delete -broadcast-domain Default-1 -ipspace
ipspace1
```

Informations associées

- "suppression broadcast-domain port réseau"

Groupes et règles de basculement

En savoir plus sur le basculement LIF sur les réseaux ONTAP

Le basculement de LIF désigne la migration automatique d'une LIF vers un autre port réseau en réponse à une défaillance de liaison sur le port actuel de la LIF. Ce composant clé assure la haute disponibilité des connexions aux SVM. La configuration du basculement de LIF implique la création d'un groupe de basculement, la modification de la LIF afin d'utiliser le groupe de basculement et la spécification d'une règle de basculement.

Un failover group contient un ensemble de ports réseau (ports physiques, VLAN et groupes d'interfaces) à partir d'un ou de plusieurs nœuds d'un cluster. Les ports réseau présents dans le failover group définissent les cibles de failover disponibles pour le LIF. Un groupe de basculement peut disposer des LIF de données intercluster, node management, et NAS qui y sont attribuées.

Lorsqu'une LIF est configurée sans une cible de basculement valide, une panne se produit lorsque la LIF tente de basculer. Vous pouvez utiliser `network interface show -failover` la commande pour vérifier la configuration du basculement. Pour en savoir plus, `network interface show` consultez le "Référence de commande ONTAP".

Lorsque vous créez un broadcast domain, un failover group du même nom est créé automatiquement contenant les mêmes ports réseau. Ce failover group est automatiquement géré par le système, ce qui signifie qu'à mesure que des ports sont ajoutés ou supprimés du broadcast domain, ils sont automatiquement ajoutés ou supprimés de ce failover group. Cela est fourni comme une efficacité pour les administrateurs qui ne souhaitent pas gérer leurs propres groupes de basculement.

Créer des groupes de basculement ONTAP

Vous créez un failover group de ports réseau de sorte qu'une LIF peut automatiquement migrer vers un autre port en cas de défaillance de liaison sur le port actuel du LIF. Cela permet au système de rediriger le trafic réseau vers d'autres ports disponibles dans le cluster.

Description de la tâche

Vous utilisez le `network interface failover-groups create` commande pour créer le groupe et ajouter des ports au groupe.

- Les ports ajoutés à un failover group peuvent être des ports réseau, des VLAN ou des groupes d'interfaces (ifgrps).
- Tous les ports ajoutés au failover group doivent appartenir au même broadcast domain.
- Un seul port peut résider dans plusieurs groupes de basculement.
- Si vous avez des LIF dans différents VLAN ou domaines de diffusion, vous devez configurer des groupes de basculement pour chaque VLAN ou domaine de diffusion.
- Les groupes de basculement ne s'appliquent pas aux environnements SAN iSCSI ou FC.

Étape

Création d'un groupe de basculement :

`network interface failover-groups create -vserver` *`vserver_name`* `-failover-group` *`failover_group_name`* `-targets` *`ports_list`*

- *`vserver_name`* Est le nom du SVM pouvant utiliser le failover group.
- *`failover_group_name`* est le nom du groupe de basculement que vous souhaitez créer.
- *`ports_list`* est la liste des ports qui seront ajoutés au failover group.
  Les ports sont ajoutés au format *node_name>:<port_number>*, par exemple, node1:e0c.

La commande suivante crée le failover group fg3 pour SVM vs3 et ajoute deux ports :

```
network interface failover-groups create -vserver vs3 -failover-group fg3
-targets cluster1-01:e0e,cluster1-02:e0e
```

Une fois que vous avez terminé

- Vous devez appliquer le groupe de basculement à une LIF maintenant que le groupe de basculement a été créé.
- L'application d'un groupe de basculement qui ne fournit pas de cible de basculement valide pour une LIF entraîne un message d'avertissement.

Si une LIF ne disposant pas de tentatives de basculement cible valides, une panne peut se produire.

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

Configurer les paramètres de basculement ONTAP sur une LIF

Vous pouvez configurer une LIF afin de basculer vers un groupe spécifique de ports réseau en appliquant une politique de basculement et un failover group à la LIF. Vous pouvez également désactiver le basculement d'une LIF vers un autre port.

Description de la tâche

- Lors de la création d'une LIF, le basculement LIF est activé par défaut et la liste des ports cibles disponibles est déterminée par le groupe de basculement par défaut et la règle de basculement basée sur le type et la stratégie de service LIF.

  Depuis 9.5, vous pouvez spécifier une policy de services pour le LIF qui définit les services réseau pouvant utiliser le LIF. Certains services réseau imposent des restrictions de basculement sur une LIF.

  > Si la politique de service d'une LIF est modifiée de façon à limiter davantage le basculement, la politique de basculement de la LIF est automatiquement mise à jour par le système.

- Vous pouvez modifier le comportement de basculement des LIFs en spécifiant des valeurs des paramètres -failover-group et -failover-policy dans la commande network interface modify.
- La modification d'une LIF entraînant l'absence de cible de basculement valide entraîne un message d'avertissement.

  Si une LIF ne disposant pas de tentatives de basculement cible valides, une panne peut se produire.

- À partir de ONTAP 9.11.1, sur les plateformes de baie SAN 100 % Flash (ASA), le basculement de LIF iSCSI est automatiquement activé sur les LIF iSCSI nouvellement créées sur les machines virtuelles de stockage nouvellement créées.

  En outre, c'est possible "Activez manuellement le basculement de LIF iSCSI sur des LIF iSCSI préexistantes", C'est-à-dire les LIF créées avant la mise à niveau vers ONTAP 9.11.1 ou version ultérieure.

- La liste suivante décrit la manière dont le paramètre -failover-policy affecte les ports cibles sélectionnés dans le failover group :

  > Pour le basculement LIF iSCSI, seules les règles de basculement `local-only`, `sfo-partner-only` et `disabled` sont pris en charge.

  - `broadcast-domain-wide` s'applique à tous les ports de tous les nœuds du failover group.
  - `system-defined` S'applique uniquement aux ports du nœud de rattachement de la LIF et à un autre nœud du cluster, généralement un partenaire non- SFO, le cas échéant.
  - `local-only` S'applique uniquement aux ports du nœud de rattachement du LIF.
  - `sfo-partner-only` S'applique uniquement aux ports du nœud de rattachement du LIF et à son partenaire SFO.
  - `disabled` Indique que le LIF n'est pas configuré pour le basculement.

Étapes

Configurez les paramètres de basculement pour une interface existante :

```
network interface modify -vserver <vserver_name> -lif <lif_name> -failover
-policy <failover_policy> -failover-group <failover_group>
```

Exemples de configuration des paramètres de basculement et de désactivation du basculement

La commande suivante définit la règle de basculement sur broadcast-domain-large et utilise les ports du failover group fg3 comme cibles de basculement pour LIF data1 sur SVM vs3 :

```
network interface modify -vserver vs3 -lif data1 -failover-policy
broadcast-domain-wide -failover-group fg3

network interface show -vserver vs3 -lif * -fields failover-
group,failover-policy

vserver lif              failover-policy       failover-group
------- -------------- ---------------        --------------
vs3     data1          broadcast-domain-wide  fg3
```

La commande suivante désactive le basculement pour LIF data1 sur le SVM vs3 :

```
network interface modify -vserver vs3 -lif data1 -failover-policy disabled
```

Informations associées

- "interface réseau"

Commandes ONTAP pour la gestion des groupes et des règles de basculement

Vous pouvez utiliser le `network interface failover-groups` commandes permettant de gérer les groupes de basculement. Vous utilisez le `network interface modify` Commande permettant de gérer les groupes de basculement et les règles de basculement appliquées à une LIF.

Les fonctions que vous recherchez…	Utilisez cette commande…
Ajout de ports réseau à un groupe de basculement	`network interface failover-groups add-targets`
Supprime les ports réseau d'un groupe de basculement	`network interface failover-groups remove-targets`

Modifier les ports réseau d'un failover group	`network interface failover-groups modify`
Afficher les groupes de basculement actuels	`network interface failover-groups show`
Configurer le basculement sur un LIF	`network interface modify -failover -group -failover-policy`
Afficher le failover group et la policy de failover utilisés par chaque LIF	`network interface show -fields failover-group, failover-policy`
Renommer un groupe de basculement	`network interface failover-groups rename`
Supprime un groupe de basculement	`network interface failover-groups delete`

La modification d'un groupe de basculement de manière à ce qu'il n'assure pas une cible de basculement valide pour une LIF du cluster peut entraîner une panne lorsqu'une LIF tente de basculer.

Informations associées

- "interface réseau"

Sous-réseaux (administrateurs du cluster uniquement)

En savoir plus sur les sous-réseaux du réseau ONTAP

Les sous-réseaux vous permettent d'allouer des blocs spécifiques, ou des pools, d'adresses IP pour votre configuration réseau ONTAP. Cela vous permet de créer plus facilement les LIF en spécifiant un nom de sous-réseau au lieu de spécifier l'adresse IP et les valeurs du masque réseau.

Un sous-réseau est créé au sein d'un domaine de diffusion et contient un pool d'adresses IP appartenant au même sous-réseau de couche 3. Les adresses IP d'un sous-réseau sont allouées aux ports dans le domaine de broadcast lorsque les LIFs sont créées. Lorsque les LIF sont supprimées, les adresses IP sont renvoyées au pool de sous-réseau et sont disponibles pour les futures LIF.

Il est recommandé d'utiliser les sous-réseaux, car ils facilitent considérablement la gestion des adresses IP et facilitent la création des LIF. En outre, si vous spécifiez une passerelle lors de la définition d'un sous-réseau, une route par défaut vers cette passerelle est ajoutée automatiquement au SVM lorsqu'une LIF est créée à l'aide de ce sous-réseau.

Créez des sous-réseaux pour le réseau ONTAP

Vous pouvez créer un sous-réseau pour allouer des blocs spécifiques d'adresses IPv4 ou IPv6 à utiliser ultérieurement lors de la création de LIF pour la SVM.

Cela vous permet de créer plus facilement les LIF en spécifiant un nom de sous-réseau au lieu de spécifier une adresse IP et des valeurs de masque réseau pour chaque LIF.

Avant de commencer

Vous devez être un administrateur de cluster pour effectuer cette tâche.

Le broadcast domain et IPspace où vous prévoyez d'ajouter le sous-réseau doivent déjà exister.

Description de la tâche

- Tous les noms de sous-réseau doivent être uniques au sein d'un IPspace.
- Lorsque vous ajoutez des plages d'adresses IP à un sous-réseau, vous devez vous assurer qu'il n'y a pas d'adresses IP redondantes dans le réseau de sorte que différents sous-réseaux ou hôtes ne tentent pas d'utiliser la même adresse IP.
- Si vous spécifiez une passerelle lors de la définition d'un sous-réseau, une route par défaut vers cette passerelle est ajoutée automatiquement au SVM lorsqu'une LIF est créée à l'aide de ce sous-réseau. Si vous n'utilisez pas de sous-réseaux ou si vous n'indiquez pas de passerelle lors de la définition d'un sous-réseau, vous devez utiliser le `route create` Commande pour ajouter manuellement une route au SVM.
- NetApp recommande la création d'objets de sous-réseau pour toutes les LIFs sur les SVM de données. Cela est particulièrement important dans les configurations MetroCluster, où l'objet de sous-réseau permet à ONTAP de déterminer les cibles de basculement sur le cluster de destination, car chaque objet de sous-réseau possède un broadcast associé.

Étapes

Vous pouvez créer un sous-réseau avec ONTAP System Manager ou l'interface de ligne de commandes ONTAP.

System Manager

Depuis ONTAP 9.12.0, vous pouvez utiliser System Manager pour créer un sous-réseau.

Étapes

1. Sélectionnez **réseau > Présentation > sous-réseaux**.
2. Cliquez sur + Add pour créer un sous-réseau.
3. Nommez le sous-réseau.
4. Spécifiez l'adresse IP du sous-réseau.
5. Définissez le masque de sous-réseau.
6. Définissez la plage d'adresses IP qui comprend le sous-réseau.
7. Si utile, spécifiez une passerelle.
8. Sélectionnez le domaine de diffusion auquel appartient le sous-réseau.
9. Enregistrez les modifications.
   a. Si l'adresse IP ou la plage saisie est déjà utilisée par une interface, le message suivant s'affiche : `An IP address in this range is already in use by a LIF. Associate the LIF with this subnet?`
   b. Lorsque vous cliquez sur **OK**, la LIF existante est associée au sous-réseau.

CLI

Pour créer un sous-réseau, utilisez l'interface de ligne de commandes.

```
network subnet create -subnet-name subnet_name -broadcast-domain
<broadcast_domain_name> [- ipspace <ipspace_name>] -subnet
<subnet_address> [-gateway <gateway_address>] [-ip-ranges
<ip_address_list>] [-force-update-lif-associations <true>]
```

- `subnet_name` est le nom du sous-réseau de couche 3 que vous souhaitez créer.

  Le nom peut être une chaîne de texte comme "Mgmt" ou une valeur IP de sous-réseau spécifique comme 192.0.2.0/24.

- `broadcast_domain_name` est le nom du domaine de diffusion sur lequel le sous-réseau sera stocké.
- `ipspace_name` Est le nom de l'IPspace auquel le broadcast domain appartient.

  L'IPspace par défaut est utilisé sauf si vous spécifiez une valeur pour cette option.

- `subnet_address` Est l'adresse IP et le masque du sous-réseau ; par exemple, 192.0.2.0/24.
- `gateway_address` est la passerelle pour la route par défaut du sous-réseau ; par exemple, 192.0.2.1.
- `ip_address_list` Est la liste, ou plage, des adresses IP qui seront allouées au sous-réseau.

  Les adresses IP peuvent être des adresses individuelles, une plage d'adresses IP ou une combinaison dans une liste séparée par des virgules.

- La valeur `true` peut être réglé pour le `-force-update-lif-associations` option.

  Cette commande échoue si un processeur de service ou une interface réseau utilisent actuellement les adresses IP de la plage spécifiée. Si cette valeur est définie sur true, elle associe toutes les interfaces adressées manuellement avec le sous-réseau actuel et permet à la commande de réussir.

La commande suivante crée le sous-réseau sub1 dans broadcast domain Default-1 dans l'IPspace par défaut. Il ajoute une adresse IP et un masque de sous-réseau IPv4, la passerelle et une plage d'adresses IP :

```
network subnet create -subnet-name sub1 -broadcast-domain Default-1
-subnet 192.0.2.0/24 - gateway 192.0.2.1 -ip-ranges 192.0.2.1-
192.0.2.100, 192.0.2.122
```

La commande suivante crée le sous-réseau sub2 dans broadcast domain Default dans le « IPspace par défaut ». Il ajoute une plage d'adresses IPv6 :

```
network subnet create -subnet-name sub2 -broadcast-domain Default
-subnet 3FFE::/64 - gateway 3FFE::1 -ip-ranges "3FFE::10-3FFE::20"
```

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

Une fois que vous avez terminé

Vous pouvez attribuer des SVM et des interfaces à un IPspace en utilisant les adresses dans le sous-réseau.

Si vous devez modifier le nom d'un sous-réseau existant, utilisez le `network subnet rename` commande.

Pour en savoir plus, `network subnet rename` consultez le "Référence de commande ONTAP".

Ajoutez ou supprimez des adresses IP d'un sous-réseau pour le réseau ONTAP

Vous pouvez ajouter des adresses IP lors de la création initiale d'un sous-réseau ou ajouter des adresses IP à un sous-réseau existant déjà. Vous pouvez également supprimer les adresses IP d'un sous-réseau existant. Cela vous permet d'allouer uniquement les adresses IP requises pour les SVM.

La procédure à suivre dépend de l'interface que vous utilisez—System Manager ou de l'interface de ligne de commandes :

System Manager

À partir de ONTAP 9.12.0, vous pouvez utiliser System Manager pour ajouter ou supprimer des adresses IP vers ou depuis un sous-réseau

Étapes

1. Sélectionnez **réseau > Présentation > sous-réseaux**.
2. Sélectionnez ⋮ **> Modifier** en regard du sous-réseau à modifier.
3. Ajoutez ou supprimez des adresses IP.
4. Enregistrez les modifications.
   a. Si l'adresse IP ou la plage saisie est déjà utilisée par une interface, le message suivant s'affiche : `An IP address in this range is already in use by a LIF. Associate the LIF with this subnet?`
   b. Lorsque vous cliquez sur **OK**, la LIF existante est associée au sous-réseau.

CLI

Utilisez l'interface de ligne de commande pour ajouter ou supprimer des adresses IP vers ou depuis un sous-réseau

Description de la tâche

Lors de l'ajout d'adresses IP, une erreur se produit si un processeur de service ou une interface réseau utilise les adresses IP de la plage ajoutée. Si vous souhaitez associer des interfaces adressées manuellement au sous-réseau actuel, vous pouvez définir le `-force-update-lif-associations` option à `true`.

Lors de la suppression d'adresses IP, une erreur s'affiche si un processeur de service ou une interface réseau utilise les adresses IP en cours de suppression. Si vous souhaitez que les interfaces continuent à utiliser les adresses IP après leur suppression du sous-réseau, vous pouvez définir le `-force-update -lif-associations` option à `true`.

Étape

Ajout ou suppression d'adresses IP d'un sous-réseau :

Les fonctions que vous recherchez…	Utilisez cette commande…
Ajoutez des adresses IP à un sous-réseau	plages d'extension de sous-réseau
Supprimez les adresses IP d'un sous-réseau	plages de suppression du sous-réseau

La commande suivante ajoute les adresses IP 192.0.2.82 à 192.0.2.85 au sous-réseau 1 :

```
network subnet add-ranges -subnet-name <sub1> -ip-ranges <192.0.2.82-
192.0.2.85>
```

La commande suivante supprime l'adresse IP 198.51.100.9 du sous-réseau 3 :

```
network subnet remove-ranges -subnet-name <sub3> -ip-ranges
<198.51.100.9>
```

Si la plage actuelle comprend 1 à 10 et 20 à 40 et que vous voulez ajouter 11 à 19 et 41 à 50 (en autorisant 1 à 50), vous pouvez chevaucher la plage d'adresses existante à l'aide de la commande suivante. Cette commande ajoute uniquement les nouvelles adresses, sans affecter les adresses existantes :

```
network subnet add-ranges -subnet-name <sub3> -ip-ranges <198.51.10.1-
198.51.10.50>
```

Pour en savoir plus sur `network subnet add-ranges` et `network subnet remove-ranges` dans le "Référence de commande ONTAP".

Modifiez les propriétés de sous-réseau du réseau ONTAP

Vous pouvez modifier l'adresse de sous-réseau et la valeur de masque, l'adresse de passerelle ou la plage d'adresses IP dans un sous-réseau existant.

Description de la tâche

- Lors de la modification des adresses IP, vous devez vous assurer qu'il n'y a pas d'adresses IP qui se chevauchent dans le réseau de sorte que les différents sous-réseaux ou hôtes ne tentent pas d'utiliser la même adresse IP.
- Si vous ajoutez ou modifiez l'adresse IP de la passerelle, la passerelle modifiée s'applique aux nouveaux SVM lorsqu'une LIF est créée en utilisant le sous-réseau. Une route par défaut vers la passerelle est créée pour le SVM si cette route n'existe pas déjà. Vous pouvez avoir à ajouter manuellement une nouvelle route à la SVM lorsque vous modifiez l'adresse IP de la passerelle.

La procédure à suivre dépend de l'interface que vous utilisez—System Manager ou de l'interface de ligne de commandes :

System Manager

À partir de ONTAP 9.12.0, vous pouvez utiliser System Manager pour modifier les propriétés du sous-réseau

Étapes

1. Sélectionnez **réseau > Présentation > sous-réseaux**.
2. Sélectionnez **> Modifier** en regard du sous-réseau à modifier.
3. Apportez les modifications nécessaires.
4. Enregistrez les modifications.
   a. Si l'adresse IP ou la plage saisie est déjà utilisée par une interface, le message suivant s'affiche : `An IP address in this range is already in use by a LIF. Associate the LIF with this subnet?`
   b. Lorsque vous cliquez sur **OK**, la LIF existante est associée au sous-réseau.

CLI

Utilisez l'interface de ligne de commande pour modifier les propriétés du sous-réseau

Étape

Modifier les propriétés du sous-réseau :

```
network subnet modify -subnet-name <subnet_name> [-ipspace
<ipspace_name>] [-subnet <subnet_address>] [-gateway <gateway_address>]
[-ip-ranges <ip_address_list>] [-force-update-lif-associations <true>]
```

- `subnet_name` est le nom du sous-réseau à modifier.
- `ipspace` Est le nom de l'IPspace où réside le sous-réseau.
- `subnet` est la nouvelle adresse et le nouveau masque du sous-réseau, le cas échéant ; par exemple, 192.0.2.0/24.
- `gateway` est la nouvelle passerelle du sous-réseau, le cas échéant ; par exemple, 192.0.2.1. La saisie **""** supprime l'entrée de passerelle.
- `ip_ranges` Nouvelle liste ou plage d'adresses IP qui seront allouées au sous-réseau, le cas échéant. Les adresses IP peuvent être des adresses individuelles, une plage ou des adresses IP, ou une combinaison dans une liste séparée par des virgules. La plage spécifiée ici remplace les adresses IP existantes.
- `force-update-lif-associations` Est requis lorsque vous modifiez la plage d'adresses IP. Vous pouvez définir la valeur **true** pour cette option lors de la modification de la plage d'adresses IP. Cette commande échoue si un processeur de service ou une interface réseau utilisent les adresses IP de la plage spécifiée. La définition de cette valeur sur **true** associe toutes les interfaces adressées manuellement avec le sous-réseau actuel et permet à la commande de réussir.

La commande suivante modifie l'adresse IP de la passerelle du sous-réseau 3 :

```
network subnet modify -subnet-name <sub3> -gateway <192.0.3.1>
```

Pour en savoir plus, `network subnet modify` consultez le "Référence de commande ONTAP".

Afficher les sous-réseaux du réseau ONTAP

Vous pouvez afficher la liste des adresses IP allouées à chaque sous-réseau au sein d'un IPspace. Le résultat indique également le nombre total d'adresses IP disponibles dans chaque sous-réseau, ainsi que le nombre d'adresses actuellement utilisées.

La procédure à suivre dépend de l'interface que vous utilisez—System Manager ou de l'interface de ligne de commandes :

System Manager

À partir de ONTAP 9.12.0, vous pouvez utiliser System Manager pour afficher les sous-réseaux

Étapes

1. Sélectionnez **réseau > Présentation > sous-réseaux**.
2. Afficher la liste des sous-réseaux.

CLI

Utilisez l'interface de ligne de commande pour afficher les sous-réseaux

Étape

Afficher la liste des sous-réseaux et les plages d'adresses IP associées utilisés dans ces sous-réseaux :

```
network subnet show
```

La commande suivante affiche les sous-réseaux et les propriétés du sous-réseau :

```
network subnet show

IPspace: Default
Subnet                  Broadcast               Avail/
Name   Subnet           Domain    Gateway       Total   Ranges
-----  ---------------- --------- ------------ --------
-----------------------
sub1   192.0.2.0/24      bcast1   192.0.2.1     5/9     192.0.2.92-
192.0.2.100
sub3   198.51.100.0/24  bcast3   198.51.100.1   3/3
198.51.100.7,198.51.100.9
```

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

Supprimez les sous-réseaux du réseau ONTAP

Si vous n'avez plus besoin d'un sous-réseau et que vous souhaitez désaffecter les adresses IP qui ont été attribuées au sous-réseau, vous pouvez le supprimer.

La procédure à suivre dépend de l'interface que vous utilisez—System Manager ou de l'interface de ligne de commandes :

System Manager

À partir de ONTAP 9.12.0, vous pouvez utiliser System Manager pour supprimer un sous-réseau

Étapes

1. Sélectionnez **réseau > Présentation > sous-réseaux**.
2. Sélectionnez ⋮ **> Supprimer** en regard du sous-réseau à supprimer.
3. Enregistrez les modifications.

CLI

Utilisez l'interface de ligne de commande pour supprimer un sous-réseau

Description de la tâche

Vous recevrez une erreur si un processeur de service ou une interface réseau utilise actuellement des adresses IP dans les plages spécifiées. Si vous souhaitez que les interfaces continuent à utiliser les adresses IP, même après la suppression du sous-réseau, vous pouvez définir l'option -force-update-lif -associations à true afin de supprimer l'association du sous-réseau avec les LIF.

Étape

Supprimer un sous-réseau :

```
network subnet delete -subnet-name subnet_name [-ipspace ipspace_name] [-
force-update-lif- associations true]
```

La commande suivante supprime le sous-réseau sub1 dans IPspace ipspace1 :

```
network subnet delete -subnet-name sub1 -ipspace ipspace1
```

Pour en savoir plus, `network subnet delete` consultez le "Référence de commande ONTAP".

Créez des SVM pour le réseau ONTAP

Vous devez créer un SVM afin de fournir des données aux clients.

Avant de commencer

- Vous devez être un administrateur de cluster pour effectuer cette tâche.
- Vous devez savoir quel style de sécurité le volume root du SVM sera mis en place.

  Si vous prévoyez d'implémenter une solution Hyper-V ou SQL Server over SMB sur ce SVM, vous devez utiliser le style de sécurité NTFS pour le volume root. Au moment de leur création, les volumes contenant des fichiers Hyper-V ou des fichiers de base de données SQL doivent être définis sur la sécurité NTFS. En définissant le style de sécurité du volume racine sur NTFS, vous assurez que vous ne créez pas de

volumes de données UNIX ou de type sécurité mixte par inadvertance.

- À partir de ONTAP 9.13.1, vous pouvez définir une capacité maximale pour une machine virtuelle de stockage. Vous pouvez également configurer des alertes lorsque la SVM approche un niveau de capacité seuil. Pour plus d'informations, voir Gestion de la capacité des SVM.

System Manager

Vous pouvez utiliser System Manager pour créer une machine virtuelle de stockage.

Étapes

1. Sélectionnez **machines virtuelles de stockage**.
2. Cliquez + Add pour créer une VM de stockage.
3. Nommez la VM de stockage.
4. Sélectionnez le protocole d'accès :
   - SMB/CIFS, NFS
   - ISCSI
   - FC
   - NVMe
     i. Si vous sélectionnez **Activer SMB/CIFS**, effectuez la configuration suivante :

Champ ou case à cocher	Description
Nom de l'administrateur	Préciser le nom d'utilisateur administrateur pour la VM de stockage SMB/CIFS.
Mot de passe	Préciser le mot de passe administrateur pour la VM de stockage SMB/CIFS.
Nom du serveur	Spécifier le nom du serveur pour la VM de stockage SMB/CIFS
Domaine Active Directory	Spécifiez le domaine Active Directory pour fournir l'authentification utilisateur pour la machine virtuelle de stockage SMB/CIFS.
Unité organisationnelle	Spécifiez l'unité organisationnelle dans le domaine Active Directory associé au serveur SMB/CIFS. « CN=calculateurs » est la valeur par défaut, qui peut être modifiée.
Cryptage des données tout en accédant aux partages de la machine virtuelle de stockage	Cochez cette case pour chiffrer les données à l'aide de SMB 3.0 pour empêcher tout accès non autorisé aux fichiers sur les partages de la machine virtuelle de stockage SMB/CIFS.
Domaines	Ajoutez, supprimez ou réorganisez les domaines répertoriés pour la machine virtuelle de stockage SMB/CIFS.
Serveurs de noms	Ajoutez, supprimez ou réorganisez les serveurs de noms pour la machine virtuelle de stockage SMB/CIFS.

Langue par défaut	Spécifie le paramètre de codage de langue par défaut pour la VM de stockage et ses volumes. Utilisez l'interface de ligne de commandes pour modifier les paramètres des volumes individuels d'une machine virtuelle de stockage.
Interface réseau	Pour chaque interface réseau configurée pour la machine virtuelle de stockage, sélectionnez un sous-réseau existant (s'il existe au moins un sous-réseau) ou spécifiez **sans sous-réseau** et renseignez les champs **adresse IP** et **masque de sous-réseau**. Si utile, cochez la case **utiliser le même masque de sous-réseau et la même passerelle pour toutes les interfaces** suivantes. Vous pouvez permettre au système de sélectionner automatiquement le port d'accueil ou de sélectionner manuellement celui que vous souhaitez utiliser dans la liste.
Gérer le compte d'administrateur	Cochez cette case pour gérer le compte d'administrateur de la machine virtuelle de stockage. Lorsque cette option est sélectionnée, spécifiez le nom d'utilisateur, le mot de passe, confirmez le mot de passe et indiquez si vous souhaitez ajouter une interface réseau pour la gestion des machines virtuelles de stockage.

1. Si vous sélectionnez **Activer NFS**, effectuez la configuration suivante :

Champ ou case à cocher	Description
Cochez la case Autoriser l'accès client NFS	Cochez cette case si tous les volumes créés sur la VM de stockage NFS doivent utiliser le chemin du volume racine «/ » pour monter et parcourir. Ajoutez des règles à la stratégie d'export « default » pour permettre un parcours de montage ininterrompu.

Règles	Cliquez + Add pour créer des règles. • Spécification client : spécifiez les noms d'hôte, les adresses IP, les groupes réseau ou les domaines. • Protocoles d'accès : sélectionnez une combinaison des options suivantes : ◦ SMB/CIFS ◦ FlexCache ◦ NFS ▪ NFSv3 ▪ NFSv4 • Détails d'accès : pour chaque type d'utilisateur, spécifiez le niveau d'accès, soit en lecture seule, en lecture/écriture ou superutilisateur. Les types d'utilisateur sont les suivants : ◦ Tout ◦ Tous (en tant qu'utilisateur anonyme) ◦ UNIX ◦ Kerberos 5 ◦ Kerberos 5i ◦ Kerberos 5p ◦ NTLM Enregistrez la règle.
Langue par défaut	Spécifie le paramètre de codage de langue par défaut pour la VM de stockage et ses volumes. Utilisez l'interface de ligne de commandes pour modifier les paramètres des volumes individuels d'une machine virtuelle de stockage.
Interface réseau	Pour chaque interface réseau configurée pour la machine virtuelle de stockage, sélectionnez un sous-réseau existant (s'il existe au moins un sous-réseau) ou spécifiez **sans sous-réseau** et renseignez les champs **adresse IP** et **masque de sous-réseau**. Si utile, cochez la case **utiliser le même masque de sous-réseau et la même passerelle pour toutes les interfaces** suivantes. Vous pouvez permettre au système de sélectionner automatiquement le port d'accueil ou de sélectionner manuellement celui que vous souhaitez utiliser dans la liste.

Gérer le compte d'administrateur	Cochez cette case pour gérer le compte d'administrateur de la machine virtuelle de stockage. Lorsque cette option est sélectionnée, spécifiez le nom d'utilisateur, le mot de passe, confirmez le mot de passe et indiquez si vous souhaitez ajouter une interface réseau pour la gestion des machines virtuelles de stockage.

1. Si vous sélectionnez **Activer iSCSI**, effectuez la configuration suivante :

Champ ou case à cocher	Description
Interface réseau	Pour chaque interface réseau configurée pour la machine virtuelle de stockage, sélectionnez un sous-réseau existant (s'il existe au moins un sous-réseau) ou spécifiez **sans sous-réseau** et renseignez les champs **adresse IP** et **masque de sous-réseau**. Si utile, cochez la case **utiliser le même masque de sous-réseau et la même passerelle pour toutes les interfaces** suivantes. Vous pouvez permettre au système de sélectionner automatiquement le port d'accueil ou de sélectionner manuellement celui que vous souhaitez utiliser dans la liste.
Gérer le compte d'administrateur	Cochez cette case pour gérer le compte d'administrateur de la machine virtuelle de stockage. Lorsque cette option est sélectionnée, spécifiez le nom d'utilisateur, le mot de passe, confirmez le mot de passe et indiquez si vous souhaitez ajouter une interface réseau pour la gestion des machines virtuelles de stockage.

1. Si vous sélectionnez **Activer FC**, effectuez la configuration suivante :

Champ ou case à cocher	Description
Configurez les ports FC	Sélectionnez les interfaces réseau sur les nœuds que vous souhaitez inclure dans la VM de stockage. Deux interfaces réseau par nœud sont recommandées.
Gérer le compte d'administrateur	Cochez cette case pour gérer le compte d'administrateur de la machine virtuelle de stockage. Lorsque cette option est sélectionnée, spécifiez le nom d'utilisateur, le mot de passe, confirmez le mot de passe et indiquez si vous souhaitez ajouter une interface réseau pour la gestion des machines virtuelles de stockage.

1. Si vous sélectionnez **Activer NVMe/FC**, effectuez la configuration suivante :

Champ ou case à cocher	Description
Configurez les ports FC	Sélectionnez les interfaces réseau sur les nœuds que vous souhaitez inclure dans la VM de stockage. Deux interfaces réseau par nœud sont recommandées.
Gérer le compte d'administrateur	Cochez cette case pour gérer le compte d'administrateur de la machine virtuelle de stockage. Lorsque cette option est sélectionnée, spécifiez le nom d'utilisateur, le mot de passe, confirmez le mot de passe et indiquez si vous souhaitez ajouter une interface réseau pour la gestion des machines virtuelles de stockage.

1. Si vous sélectionnez **Activer NVMe/TCP**, effectuez la configuration suivante :

Champ ou case à cocher	Description
Interface réseau	Pour chaque interface réseau configurée pour la machine virtuelle de stockage, sélectionnez un sous-réseau existant (s'il existe au moins un sous-réseau) ou spécifiez **sans sous-réseau** et renseignez les champs **adresse IP** et **masque de sous-réseau**. Si utile, cochez la case **utiliser le même masque de sous-réseau et la même passerelle pour toutes les interfaces** suivantes. Vous pouvez permettre au système de sélectionner automatiquement le port d'accueil ou de sélectionner manuellement celui que vous souhaitez utiliser dans la liste.
Gérer le compte d'administrateur	Cochez cette case pour gérer le compte d'administrateur de la machine virtuelle de stockage. Lorsque cette option est sélectionnée, spécifiez le nom d'utilisateur, le mot de passe, confirmez le mot de passe et indiquez si vous souhaitez ajouter une interface réseau pour la gestion des machines virtuelles de stockage.

1. Enregistrez les modifications.

CLI

Pour créer un sous-réseau, utilisez l'interface de ligne de commandes de ONTAP.

Étapes

1. Déterminer les agrégats candidats à l'ajout du volume root du SVM.

```
storage aggregate show -has-mroot false
```

Vous devez choisir un agrégat qui dispose d'au moins 1 Go d'espace libre pour contenir le volume root. Si vous prévoyez de configurer l'audit NAS sur le SVM, vous devez disposer d'au moins 3 Go d'espace libre supplémentaire sur l'agrégat racine, l'espace supplémentaire étant utilisé pour créer le volume d'activation de l'audit lorsque l'audit est activé.

> Si l'audit NAS est déjà activé sur un SVM existant, le volume intermédiaire de l'agrégat est créé immédiatement après la fin de la création de l'agrégat.

2. Noter le nom de l'agrégat sur lequel vous souhaitez créer le volume root du SVM.
3. Si vous prévoyez de spécifier une langue lors de la création du SVM et ne connaissez pas la valeur à utiliser, identifier et enregistrer la valeur du langage que vous souhaitez spécifier :

   ```
   vserver create -language ?
   ```

4. Si vous prévoyez de spécifier une snapshot policy lors de la création de la SVM et ne connaissez pas le nom de la politique, lister les policies disponibles et identifier et enregistrer le nom de la snapshot policy à utiliser :

   ```
   volume snapshot policy show -vserver vserver_name
   ```

5. Si vous prévoyez de spécifier une politique de quotas lors de la création de la SVM et ne connaissez pas le nom de la politique, lister les policies disponibles et identifier et enregistrer le nom de la politique de quotas que vous souhaitez utiliser :

   ```
   volume quota policy show -vserver vserver_name
   ```

6. Création d'un SVM :

   ```
   vserver create -vserver vserver_name -aggregate aggregate_name -rootvolume
   root_volume_name -rootvolume-security-style {unix|ntfs|mixed} [-ipspace
   IPspace_name] [-language <language>] [-snapshot-policy
   snapshot_policy_name] [-quota-policy quota_policy_name] [-comment comment]
   ```

   ```
   vserver create -vserver vs1 -aggregate aggr3 -rootvolume vs1_root
   -rootvolume-security-style ntfs -ipspace ipspace1 -language
   en_US.UTF-8
   ```

   ```
   [Job 72] Job succeeded: Vserver creation completed
   ```

7. Vérifier que la configuration des SVM est correcte.

   ```
   vserver show -vserver vs1
   ```

```
Vserver: vs1
Vserver Type: data
Vserver Subtype: default
Vserver UUID: 11111111-1111-1111-1111-111111111111
Root Volume: vs1_root
Aggregate: aggr3
NIS Domain: -
Root Volume Security Style: ntfs
LDAP Client: -
Default Volume Language Code: en_US.UTF-8
Snapshot Policy: default
Comment:
Quota Policy: default
List of Aggregates Assigned: -
Limit on Maximum Number of Volumes allowed: unlimited
Vserver Admin State: running
Vserver Operational State: running
Vserver Operational State Stopped Reason: -
Allowed Protocols: nfs, cifs, ndmp
Disallowed Protocols: fcp, iscsi
QoS Policy Group: -
Config Lock: false
IPspace Name: ipspace1
Is Vserver Protected: false
```

Dans cet exemple, la commande crée le SVM nommé « vs1 » dans l'IPspace « ipspace1 ». Le volume racine est nommé « vs1_root » et est créé sur aggr3 avec le style de sécurité NTFS.

À partir de la version ONTAP 9.13.1, vous pouvez définir un modèle de groupe de règles de QoS adaptative, en appliquant une limite au niveau du débit et du plafond aux volumes du SVM. Vous ne pouvez appliquer cette politique qu'après avoir créé la SVM. Pour en savoir plus sur ce processus, voir Définissez un modèle de groupe de règles adaptatives.

Interfaces logiques

Présentation de la LIF

En savoir plus sur la configuration LIF d'un cluster ONTAP

Une LIF (Logical interface) représente un point d'accès réseau à un nœud du cluster. Vous pouvez configurer les LIF sur les ports sur lesquels le cluster envoie et reçoit des communications sur le réseau.

Un administrateur de cluster peut créer, afficher, modifier, migrer, restaurer, Ou supprimez les LIFs. Un administrateur SVM ne peut afficher que les LIFs associées à la SVM.

Une LIF est une adresse IP ou un WWPN qui présente des caractéristiques associées, telles qu'une politique de service, un port d'accueil, un nœud de rattachement, une liste de ports à basculer et une politique de pare-feu. Vous pouvez configurer les LIF sur les ports sur lesquels le cluster envoie et reçoit des communications sur le réseau.

Depuis ONTAP 9.10.1, les politiques de pare-feu sont obsolètes et intégralement remplacées par les politiques de service de LIF. Pour plus d'informations, voir "Configuration des politiques de pare-feu pour les LIF".

Les LIFs peuvent être hébergées sur les ports suivants :

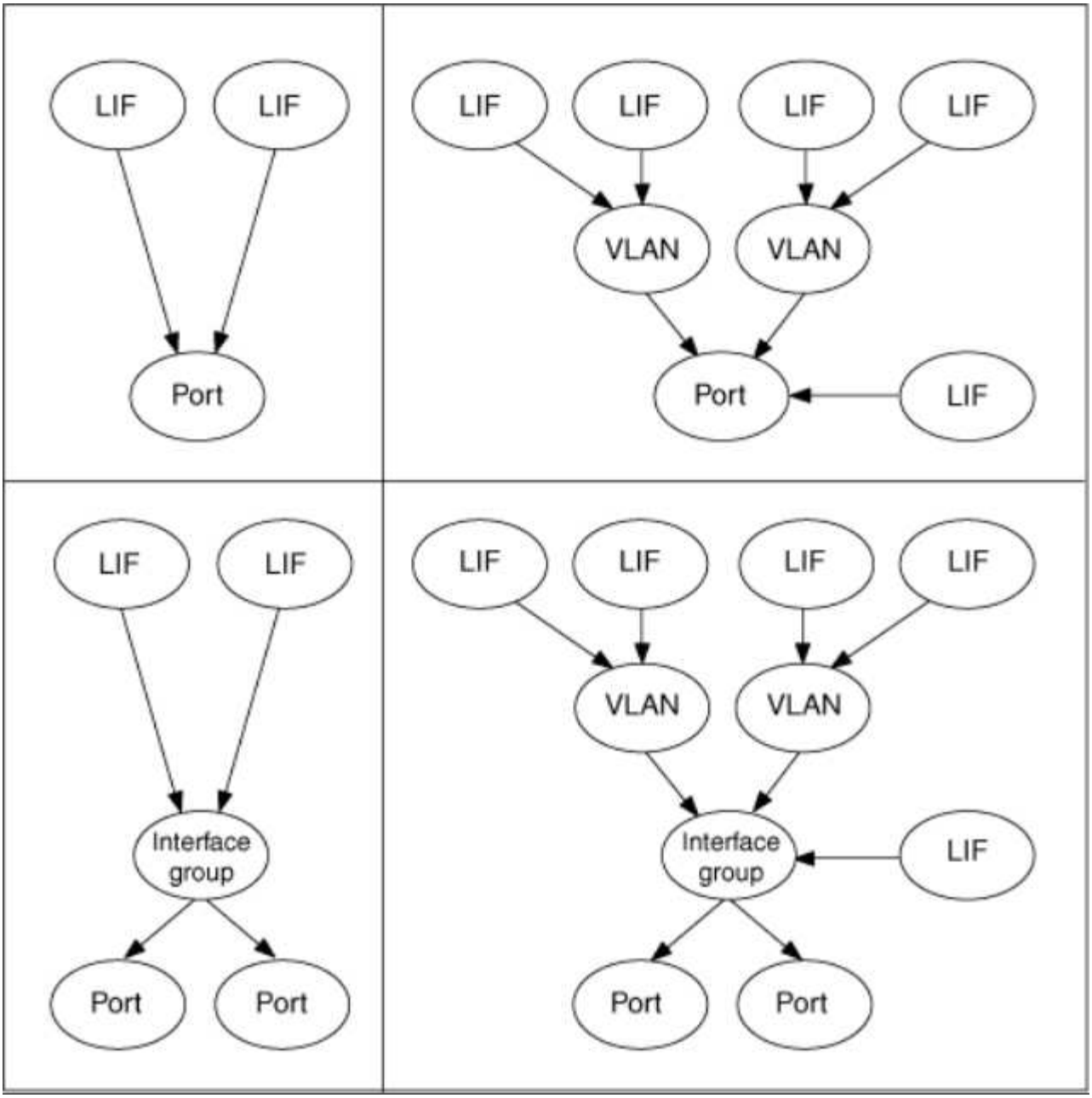
- Ports physiques ne faisant pas partie de groupes d'interfaces
- Groupes d'interface
- VLAN
- Ports physiques ou groupes d'interfaces qui hébergent des VLAN
- Ports VIP (Virtual IP

  Depuis ONTAP 9.5, les LIFs VIP sont prises en charge et hébergées sur des ports VIP.

Lors de la configuration des protocoles SAN tels que FC sur une LIF, ils seront associés à un WWPN.

"Administration SAN"

La figure suivante illustre la hiérarchie de ports dans un système ONTAP :



Basculement et rétablissement de LIF

Un basculement de LIF se produit lorsqu'une LIF se déplace de son nœud ou port de rattachement vers le nœud ou le port HA Partner. Un basculement de LIF peut être déclenché automatiquement par ONTAP ou manuellement par un administrateur du cluster pour certains événements, tels qu'un lien Ethernet physique en panne ou un nœud qui dévie du quorum de la base de données répliquée (RDB). Lorsqu'un basculement de LIF se produit, ONTAP continue son fonctionnement normal sur le nœud partenaire jusqu'à ce que la raison du basculement soit résolue. Lorsque le nœud ou le port de rattachement retrouve sa santé, la LIF est reconvertie du partenaire HA en nœud ou port de rattachement. Ce retour s'appelle un retour.

Pour le basculement et le rétablissement LIF, les ports de chaque nœud doivent appartenir au même broadcast domain. Pour vérifier que les ports appropriés de chaque nœud appartiennent au même broadcast domain, consultez les documents suivants :

- ONTAP 9.8 et versions ultérieures : "Réparation de l'accessibilité de l'orifice"
- ONTAP 9.7 et versions antérieures : "Ajouter ou supprimer des ports d'un broadcast domain"

Pour les LIF avec basculement LIF activé (automatiquement ou manuellement), les points suivants s'appliquent :

- Pour les LIF utilisant une policy de service de données, vous pouvez vérifier les restrictions de failover-policy :
  - ONTAP 9.6 et versions ultérieures : "LIF et politiques de services dans ONTAP 9.6 et versions ultérieures"
  - ONTAP 9.5 et versions antérieures : "Rôles LIF dans ONTAP 9.5 et versions antérieures"
- La restauration automatique des LIF se produit lorsque la restauration automatique est définie sur `true` Et lorsque le port de attache de la LIF est sain et peut héberger la LIF.
- En cas de basculement de nœud planifié ou non planifié, la LIF sur le nœud repris bascule vers le partenaire haute disponibilité. Le port sur lequel la LIF tombe en panne est déterminé par vif Manager.
- Une fois le basculement terminé, le LIF fonctionne normalement.
- Lorsqu'un rétablissement est initié, la LIF retourne à son nœud et port de rattachement, si la restauration automatique est définie sur `true`.
- Lorsqu'une liaison ethernet est indisponible sur un port hébergeant une ou plusieurs LIF, vif Manager migre les LIFs du port DOWN vers un autre port du même broadcast domain. Le nouveau port peut se trouver sur le même nœud ou sur son partenaire HA. Une fois la liaison restaurée et si la restauration automatique est définie sur `true`, Le vif Manager restaure les LIF sur leur nœud de rattachement et leur port de rattachement.
- Lorsqu'un nœud quitte le quorum RDB (Replicated database), il migre les LIF du nœud de quorum vers son partenaire haute disponibilité. Une fois que le nœud revient au quorum et que la restauration automatique est définie sur `true`, Le vif Manager restaure les LIF sur leur nœud de rattachement et leur port de rattachement.

En savoir plus sur la compatibilité des LIF ONTAP avec les types de ports

Les LIF peuvent présenter des caractéristiques différentes pour prendre en charge différents types de ports.

> Lorsque les LIF intercluster et de gestion sont configurées dans le même sous-réseau, le trafic de gestion peut être bloqué par un pare-feu externe et les connexions AutoSupport et NTP peuvent tomber en panne. Vous pouvez restaurer le système en exécutant le `network interface modify -vserver` *`vserver name`* `-lif` *`intercluster LIF`* `-status -admin up|down` Commande pour basculer le LIF intercluster. Cependant, vous devez définir la LIF intercluster et la LIF de gestion dans différents sous-réseaux pour éviter ce problème.

LIF	Description
LIF de données	LIF associée à un SVM (Storage Virtual machine) et servant à la communication avec les clients. Vous pouvez avoir plusieurs LIFs data sur un port. Ces interfaces peuvent migrer ou basculer sur l'ensemble du cluster. Vous pouvez modifier une LIF de données afin de servir de LIF de gestion SVM en modifiant sa politique de pare-feu en gestion. Les sessions établies aux serveurs NIS, LDAP, Active Directory, WINS, et DNS utilisent les LIFs data.

LIF Cluster	Une LIF utilisée pour acheminer le trafic intracluster entre les nœuds d'un cluster. Les LIFs cluster doivent toujours être créées sur les ports de type cluster. Les LIFs de cluster peuvent basculer entre les ports de cluster sur le même nœud, mais elles ne peuvent pas être migrées ou basculer vers un nœud distant. Lorsqu'un nouveau nœud rejoint un cluster, les adresses IP sont générées automatiquement. Toutefois, si vous souhaitez attribuer manuellement des adresses IP aux LIF de cluster, vous devez vous assurer que les nouvelles adresses IP se trouvent dans la même plage de sous-réseau que les LIF de cluster existantes.
LIF Cluster-management	LIF qui offre une interface de gestion unique pour l'ensemble du cluster. Une LIF de cluster management peut basculer vers n'importe quel nœud du cluster. Il ne peut pas basculer vers le cluster ou les ports intercluster
FRV InterCluster	LIF utilisée pour la communication, la sauvegarde et la réplication entre clusters. Vous devez créer une LIF intercluster sur chaque node du cluster avant qu'une relation de peering de cluster ne puisse être établie. Ces LIFs peuvent uniquement basculer sur les ports du même nœud. Ils ne peuvent pas être migrés ni basculés vers un autre nœud du cluster.
FRV de gestion des nœuds	Une LIF qui fournit une adresse IP dédiée pour gérer un nœud particulier dans un cluster. Les LIFs de node-management sont créées au moment de la création ou de l'arrivée du cluster. Ces LIFs sont utilisées pour la maintenance du système, par exemple lorsqu'un nœud devient inaccessible depuis le cluster.
LIF VIP	Une LIF VIP est toute LIF de données créée sur un port VIP. Pour en savoir plus, voir "Configuration des LIF IP virtuelles (VIP)".

Informations associées

- "modification de l'interface réseau"

Politiques de service LIF et rôles pris en charge pour votre version ONTAP

Au fil du temps, la façon dont ONTAP gère le type de trafic pris en charge sur les LIF a changé.

- ONTAP 9.5 et les versions antérieures utilisent des rôles LIF et des services de pare-feu.
- Les versions ONTAP 9.6 et ultérieures utilisent les stratégies de service LIF :
  - La version ONTAP 9.5 a introduit les stratégies de service LIF.
  - ONTAP 9.6 a remplacé les rôles LIF par des stratégies de service LIF.
  - ONTAP 9.10.1 a remplacé les services de pare-feu par des politiques de service LIF.

La méthode que vous configurez dépend de la version de ONTAP que vous utilisez.

Pour en savoir plus sur :

- Politiques de pare-feu, voir "Commande : firewall-policy-show".

- Rôles LIF, voir "Rôles LIF (ONTAP 9.5 et versions antérieures)".
- Politiques de service LIF, voir "LIF et règles de service (ONTAP 9.6 et versions ultérieures)".

Découvrez les LIF ONTAP et les règles de service

Vous pouvez attribuer des politiques de service (au lieu de rôles LIF ou de politiques de pare-feu) aux LIF qui déterminent le type de trafic pris en charge pour les LIF. Les stratégies de service définissent une collection de services réseau prise en charge par une LIF. ONTAP fournit un ensemble de règles de service intégrées qui peuvent être associées à une LIF.

La méthode de gestion du trafic réseau est différente dans ONTAP 9.7 et les versions antérieures. Si vous devez gérer le trafic sur un réseau exécutant ONTAP 9.7 et les versions antérieures, reportez-vous à la section "Rôles LIF (ONTAP 9.5 et versions antérieures)".

Les protocoles FCP et NVMe/FCP ne nécessitent actuellement pas de service-policy.

Vous pouvez afficher les stratégies de service et leurs détails à l'aide de la commande suivante : `network interface service-policy show`

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

Les fonctionnalités qui ne sont pas liées à un service spécifique utiliseront un comportement défini par le système pour sélectionner les LIFs pour les connexions sortantes.

Les applications qui se trouvent sur une LIF avec une politique de service vide peuvent se comporter de manière inattendue.

Règles de service pour les SVM système

Le SVM d'administration et tout SVM système contiennent des politiques de service qui peuvent être utilisées pour les LIF au sein de ce SVM, y compris les LIFs de type management et intercluster. Ces règles sont automatiquement créées par le système lorsqu'un IPspace est créé.

Le tableau suivant répertorie les règles intégrées pour les LIF dans les SVM système à partir de ONTAP 9.12.1. Pour les autres versions, afficher les politiques de service et leurs détails à l'aide de la commande suivante :

```
network interface service-policy show
```

Politique	Services inclus	Rôle équivalent	Description
valeur-par-défaut intercluster	intercluster-core, management-https	intercluster	Utilisé par les LIFs transportant le trafic intercluster. Attention : le service intercluster est disponible depuis le ONTAP 9.5 avec le nom net-intercluster service policy.

annonce-route-par-défaut	gestion-bgp	-	Utilisé par les LIFs transportant des connexions homologues BGP Remarque : disponible auprès de ONTAP 9.5 avec le nom net-route-announce service policy.
gestion par défaut	management-core, management-https, management-http, management-ssh, management-autosupport, management-ems, management-dns-client, management-ad-client, management-ldap-client, management-nis-client, management-ntp-client, transfert-journalisation-gestion	nœuds de gestion et de gestion de cluster	Utilisez cette politique de gestion étendue du système pour créer des LIFs de gestion du type node-and-cluster détenues par un SVM système. Ces LIF peuvent être utilisées pour les connexions sortantes vers des serveurs DNS, AD, LDAP ou NIS, ainsi que pour prendre en charge des connexions supplémentaires pour prendre en charge les applications s'exécutant pour le compte de l'ensemble du système. À partir de ONTAP 9.12.1, vous pouvez utiliser le `management-log-forwarding` service pour contrôler les LIFs utilisées pour transférer les journaux d'audit à un serveur syslog distant.

Le tableau suivant liste les services que les LIFs peuvent utiliser sur un SVM système depuis ONTAP 9.11.1 :

Service	Limites du basculement	Description
intercluster-core	home-node-uniquement	Services intercluster de base
cœur de gestion	-	Services de gestion centrale
management-ssh	-	Services d'accès à la gestion SSH
gestion-http	-	Services de gestion de l'accès HTTP
gestion-https	-	Services pour l'accès à la gestion HTTPS
gestion-autosupport	-	Services liés à l'imputation de charges utiles AutoSupport
gestion-bgp	port d'origine uniquement	Services liés aux interactions BGP par les pairs
backup-ndmp-control	-	Services pour les commandes de sauvegarde NDMP
gestion-ems	-	Services d'accès à la messagerie de gestion

client-ntp-management	-	Introduit dans ONTAP 9.10.1. Services pour l'accès client NTP.
serveur-ntp-management	-	Introduit dans ONTAP 9.10.1. Services pour l'accès à la gestion de serveurs NTP
management-portmap	-	Services de gestion de portmap
serveur-rsh de gestion	-	Services de gestion de serveur rsh
serveur-gestion-snmp	-	Services de gestion de serveur SNMP
serveur-telnet-gestion	-	Services de gestion de serveur telnet
transfert de journaux de gestion	-	Introduit dans ONTAP 9.12.1. Services de transfert de journaux d'audit

Règles de service pour les SVM de données

Tous les SVM de données contiennent des règles de service qui peuvent être utilisées par les LIF de ce SVM.

Le tableau ci-dessous répertorie les règles intégrées pour les LIF dans des SVM de données commençant par ONTAP 9.11.1. Pour les autres versions, afficher les politiques de service et leurs détails à l'aide de la commande suivante :

```
network interface service-policy show
```

Politique	Services inclus	Protocole de données équivalent	Description
gestion par défaut	data-core, management-https, management-http, management-ssh, management-dns-client, management-ad-client, management-ldap-client, management-nis-client	Aucune	Utiliser cette politique de gestion « SVM-scoped » pour créer des LIFs de management du SVM détenues par un SVM de données. Ces LIF peuvent fournir un accès SSH ou HTTPS aux administrateurs du SVM. Lorsque nécessaire, ces LIF peuvent être utilisées pour des connexions sortantes vers des serveurs DNS externes, AD, LDAP ou NIS.
blocs de données par défaut	cœur de données, iscsi	iscsi	Utilisée par les LIF transportant un trafic de données SAN orienté bloc. Depuis ONTAP 9.10.1, la règle « default-data-blocks » est obsolète. Utilisez plutôt la stratégie de service « default-data-iscsi ».

fichiers-données-par-défaut	data-core, data-fpolicy-client, data-dns-serveur, data-FlexCache, data-cifs, data-nfs, management-dns-client, management-ad-client, management-ldap-client, management-nis-client	nfs, cifs, fcache	Utilisez la stratégie par défaut-data-Files pour créer des LIF NAS qui prennent en charge des protocoles de données basés sur des fichiers. Parfois, il n'y a qu'une seule LIF présente au SVM, donc cette politique permet à la LIF d'être utilisée pour les connexions sortantes vers un serveur DNS externe, AD, LDAP ou NIS. Si vous préférez que ces connexions utilisent uniquement des LIF de gestion, vous pouvez supprimer ces services à de cette règle.
iscsi-données-par-défaut	cœur de données, iscsi	iscsi	Utilisé par les LIF transportant le trafic de données iSCSI.
données-défaut-nvme-tcp	cœur de données, nvme-tcp	nvme-tcp	Utilisé par les LIF transportant du trafic de données NVMe/TCP.

Le tableau ci-dessous répertorie les services pouvant être utilisés sur un SVM de données ainsi que les restrictions imposées par chaque service à la politique de basculement d'une LIF à partir de la ONTAP 9.11.1 :

Service	Restrictions de basculement	Description
management-ssh	-	Services d'accès à la gestion SSH
gestion-http	-	Introduit dans ONTAP 9.10.1 Services de gestion de l'accès HTTP
gestion-https	-	Services pour l'accès à la gestion HTTPS
management-portmap	-	Services d'accès à la gestion de portmap
serveur-gestion-snmp	-	Introduit dans ONTAP 9.10.1 Services pour l'accès à la gestion de serveur SNMP
cœur des données	-	Services de données centrales
nfs-données	-	Service de données NFS
cifs-données	-	Service de données CIFS
flexcache	-	Service de données FlexCache

iscsi données	Port d'attache uniquement pour l'AFF/FAS ; partenaire sfo uniquement pour ASA	Service de données iSCSI
backup-ndmp-control	-	Introduit dans ONTAP 9.10.1 Backup NDMP contrôle le service de données
serveur-données-dns	-	Introduit dans ONTAP 9.10.1 Service de données du serveur DNS
client-données fpolicy	-	Service de données de stratégie de filtrage de fichiers
tcp-nvme-données	port d'origine uniquement	Introduit dans ONTAP 9.10.1 Service de données TCP NVMe
serveur data s3	-	Service de données des serveurs simple Storage Service (S3)

Vous devez savoir comment les règles de service sont attribuées aux LIF dans les SVM de données :

- Lorsqu'un SVM de données est créé avec une liste de services de données, les règles de service « fichiers de données par défaut » et « blocs de données par défaut » intégrées à ce SVM sont créées à l'aide des services spécifiés.
- Si un SVM de données est créé sans spécifier une liste de services de données, les règles de service « fichiers de données par défaut » et « blocs de données par défaut » intégrées à ce SVM sont créées à l'aide d'une liste de services de données par défaut.

  La liste des services de données par défaut comprend les services iSCSI, NFS, NVMe, SMB et FlexCache.

- Lorsqu'une LIF est créée avec une liste de protocoles de données, une politique de service équivalente aux protocoles de données spécifiés est assignée à la LIF.
- Si aucune stratégie de service équivalente n'existe, une stratégie de service personnalisée est créée.
- Lorsqu'une LIF est créée sans une policy de service ou une liste de protocoles de données, la politique de service default-data-Files est assignée à la LIF par défaut.

Service Data-core

Le service « Data-core » permet à des composants qui utilisaient auparavant les LIF avec le rôle de données de fonctionner comme prévu sur les clusters mis à niveau pour gérer les LIF à l'aide de politiques de service plutôt que de rôles LIF (qui sont obsolètes dans ONTAP 9.6).

La spécification data-core en tant que service n'ouvre aucun port du pare-feu, mais le service doit être inclus dans toute politique de service d'un SVM de données. Par exemple, la règle de service Default-data-Files contient les services suivants par défaut :

- cœur des données
- nfs-données
- cifs-données

- flexcache

Le service « data-core » doit être inclus dans la règle afin de garantir que toutes les applications utilisant la LIF comme prévu, mais que les trois autres services peuvent être supprimés, si nécessaire.

Service LIF côté client

Depuis ONTAP 9.10.1, ONTAP fournit des services LIF côté client pour de nombreuses applications. Ces services permettent de contrôler les LIFs utilisées pour les connexions sortantes pour le compte de chaque application.

Les nouveaux services suivants permettent aux administrateurs de contrôler la liste des LIF utilisées comme adresses source pour certaines applications.

Service	Restrictions des SVM	Description
client-annonce-gestion	-	Depuis ONTAP 9.11.1, ONTAP fournit un service client Active Directory pour les connexions sortantes vers un serveur AD externe.
client-dns-gestion	-	À partir de ONTAP 9.11.1, ONTAP fournit un service client DNS pour les connexions sortantes vers un serveur DNS externe.
gestion-ldap-client	-	Depuis ONTAP 9.11.1, ONTAP fournit un service client LDAP pour les connexions sortantes vers un serveur LDAP externe.
gestion-nis-client	-	À partir de ONTAP 9.11.1, ONTAP fournit un service client NIS pour les connexions sortantes à un serveur NIS externe.
client-ntp-management	système uniquement	Depuis ONTAP 9.10.1, ONTAP fournit un service client NTP pour les connexions sortantes vers un serveur NTP externe.
client-données fpolicy	données uniquement	Depuis ONTAP 9.8, ONTAP fournit un service client pour les connexions FPolicy de sortie.

Chacun des services est automatiquement inclus dans certaines règles de service intégrées, mais les administrateurs peuvent les supprimer des règles intégrées ou les ajouter à des règles personnalisées afin de contrôler les LIF utilisées pour les connexions sortantes pour le compte de chaque application.

Informations associées

- "interface réseau service-policy show"

Gestion des LIF

Configurer des politiques de service LIF pour un cluster ONTAP

Vous pouvez configurer les stratégies de service LIF afin d'identifier un seul service ou

une liste de services qui utiliseront une LIF.

Création d'une policy de service pour les LIFs

Vous pouvez créer une policy de service pour les LIF. Vous pouvez affecter une stratégie de service à une ou plusieurs LIF, permettant ainsi au LIF de transporter du trafic pour un seul service ou une liste de services.

Vous avez besoin de privilèges avancés pour exécuter le `network interface service-policy create` commande.

Description de la tâche

Les services et les règles de service intégrés sont disponibles pour la gestion du trafic de données et de gestion sur les SVM de données et de système. La plupart des cas d'utilisation sont satisfaits à l'aide d'une règle de service intégrée plutôt que de créer une règle de service personnalisée.

Vous pouvez modifier ces règles de service intégrées, si nécessaire.

Étapes

1. Afficher les services disponibles dans le cluster :

   ```
   network interface service show
   ```

   Les services représentent les applications auxquelles un LIF accède, ainsi que les applications servies par le cluster. Chaque service inclut zéro ou plus de ports TCP et UDP sur lesquels l'application écoute.

   Les services de gestion et de données supplémentaires suivants sont disponibles :

   ```
   cluster1::> network interface service show

   Service                     Protocol:Ports
   -------                     --------------
   cluster-core                -
   data-cifs                   -
   data-core                   -
   data-flexcache              -
   data-iscsi                  -
   data-nfs                    -
   intercluster-core           tcp:11104-11105
   management-autosupport      -
   management-bgp              tcp:179
   management-core             -
   management-https            tcp:443
   management-ssh              tcp:22
   12 entries were displayed.
   ```

2. Afficher les politiques de service qui existent dans le cluster :

```
cluster1::> network interface service-policy show

Vserver   Policy                       Service: Allowed Addresses
--------- --------------------------
---------------------------------------
cluster1
          default-intercluster         intercluster-core: 0.0.0.0/0
                                       management-https: 0.0.0.0/0

          default-management           management-core: 0.0.0.0/0
                                       management-autosupport: 0.0.0.0/0
                                       management-ssh: 0.0.0.0/0
                                       management-https: 0.0.0.0/0

          default-route-announce       management-bgp: 0.0.0.0/0

Cluster
          default-cluster              cluster-core: 0.0.0.0/0

vs0
          default-data-blocks          data-core: 0.0.0.0/0
                                       data-iscsi: 0.0.0.0/0

          default-data-files           data-core: 0.0.0.0/0
                                       data-nfs: 0.0.0.0/0
                                       data-cifs: 0.0.0.0/0
                                       data-flexcache: 0.0.0.0/0

          default-management           data-core: 0.0.0.0/0
                                       management-ssh: 0.0.0.0/0
                                       management-https: 0.0.0.0/0

7 entries were displayed.
```

3. Création d'une règle de services :

```
cluster1::> set -privilege advanced
Warning: These advanced commands are potentially dangerous; use them
only when directed to do so by technical support.
Do you wish to continue? (y or n): y

cluster1::> network interface service-policy create -vserver <svm_name>
-policy <service_policy_name> -services <service_name> -allowed
-addresses <IP_address/mask,...>
```

- « nom_service » indique une liste de services à inclure dans la stratégie.
- "IP_address/mask" spécifie la liste des masques de sous-réseau pour les adresses autorisées à accéder aux services dans la stratégie de service. Par défaut, tous les services spécifiés sont ajoutés avec une liste d'adresses par défaut autorisée de 0.0.0.0/0, ce qui permet le trafic de tous les sous-réseaux. Lorsqu'une liste d'adresses autorisées par défaut est fournie, les LIF utilisant la règle sont configurées pour bloquer toutes les demandes avec une adresse source qui ne correspond à aucun des masques spécifiés.

  L'exemple suivant montre comment créer une stratégie de service de données, *svm1_Data_policy*, pour une SVM qui inclut *NFS* et *SMB* services :

```
cluster1::> set -privilege advanced
Warning: These advanced commands are potentially dangerous; use them
only when directed to do so by technical support.
Do you wish to continue? (y or n): y

cluster1::> network interface service-policy create -vserver svm1
-policy svm1_data_policy -services data-nfs,data-cifs,data-core
```

  L'exemple suivant montre comment créer une politique de service intercluster :

```
cluster1::> set -privilege advanced
Warning: These advanced commands are potentially dangerous; use them
only when directed to do so by technical support.
Do you wish to continue? (y or n): y

cluster1::> network interface service-policy create -vserver cluster1
-policy intercluster1 -services intercluster-core
```

4. Vérifiez que la stratégie de service est créée.

```
cluster1::> network interface service-policy show
```

Le résultat suivant indique les règles de service disponibles :

```
cluster1::> network interface service-policy show

Vserver   Policy                       Service: Allowed Addresses
--------- --------------------------
---------------------------------------
cluster1
          default-intercluster         intercluster-core: 0.0.0.0/0
                                       management-https: 0.0.0.0/0

          intercluster1                intercluster-core: 0.0.0.0/0

          default-management           management-core: 0.0.0.0/0
                                       management-autosupport: 0.0.0.0/0
                                       management-ssh: 0.0.0.0/0
                                       management-https: 0.0.0.0/0

          default-route-announce       management-bgp: 0.0.0.0/0

Cluster
          default-cluster              cluster-core: 0.0.0.0/0

vs0
          default-data-blocks          data-core: 0.0.0.0/0
                                       data-iscsi: 0.0.0.0/0

          default-data-files           data-core: 0.0.0.0/0
                                       data-nfs: 0.0.0.0/0
                                       data-cifs: 0.0.0.0/0
                                       data-flexcache: 0.0.0.0/0

          default-management           data-core: 0.0.0.0/0
                                       management-ssh: 0.0.0.0/0
                                       management-https: 0.0.0.0/0

          svm1_data_policy             data-core: 0.0.0.0/0
                                       data-nfs: 0.0.0.0/0
                                       data-cifs: 0.0.0.0/0

9 entries were displayed.
```

Une fois que vous avez terminé

Assigner la policy de service à une LIF soit au moment de la création, soit en modifiant une LIF existante.

Assigner une policy de service à une LIF

Vous pouvez affecter une policy de service à une LIF au moment de la création de cette LIF ou en modifiant la LIF. Une policy de service définit la liste de services qui peuvent être utilisés avec la LIF.

Description de la tâche

Vous pouvez attribuer des règles de service pour les LIF dans les SVM admin et data.

Étape

Selon l'heure à laquelle vous souhaitez affecter la policy de service à une LIF, effectuez l'une des actions suivantes :

Si vous êtes…	Affecter la stratégie de service…
Création d'une LIF	Interface réseau create -vserver svm_name -lif <lif_name> -home-node <nom_node> -home-port <nom_port> {(-adresse <adresse_IP> -masque de réseau <adresse_IP>) -subnet-name <nom_sous-réseau>} -service-policy <nom_service>
Modification d'une LIF	interface réseau modify -vserver <svm_name> -lif <lif_name> -service-policy <service_name>

Lorsque vous spécifiez une policy de services pour une LIF, il n'est pas nécessaire de spécifier le protocole de données et le rôle de cette dernière. La création des LIF en spécifiant le rôle et les protocoles de données est également pris en charge.

Une politique de service peut uniquement être utilisée par les LIFs dans le même SVM que vous avez spécifié lors de la création de la policy de service.

Exemples

L'exemple suivant montre comment modifier la policy de service d'une LIF pour utiliser la policy de service de gestion par défaut :

```
cluster1::> network interface modify -vserver cluster1 -lif lif1 -service
-policy default-management
```

Commandes permettant de gérer les règles de service LIF

Utilisez le `network interface service-policy` Commandes permettant de gérer les règles de service LIF.

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

Avant de commencer

La modification de la politique de service d'une LIF dans une relation SnapMirror active interrompt la planification de la réplication. Si vous convertissez une LIF de intercluster en non-intercluster (ou inversement), ces modifications ne sont pas répliquées sur le cluster peering. Pour mettre à jour le Peer Cluster après avoir modifié la politique de service LIF, effectuez d'abord la procédure `snapmirror abort` ensuite resynchroniser la relation de réplication.

Les fonctions que vous recherchez…	Utilisez cette commande…
Création d'une stratégie de service (privilèges avancés requis)	`network interface service-policy create`
Ajouter une entrée de service supplémentaire à une stratégie de service existante (privilèges avancés requis)	`network interface service-policy add-service`
Cloner une stratégie de service existante (privilèges avancés requis)	`network interface service-policy clone`
Modification d'une entrée de service dans une stratégie de service existante (privilèges avancés requis)	`network interface service-policy modify-service`
Suppression d'une entrée de service d'une stratégie de service existante (privilèges avancés requis)	`network interface service-policy remove-service`
Renommer une stratégie de service existante (privilèges avancés requis)	`network interface service-policy rename`
Suppression d'une stratégie de service existante (privilèges avancés requis)	`network interface service-policy delete`
Restaurer une stratégie de service intégrée à son état d'origine (privilèges avancés requis)	`network interface service-policy restore-defaults`
Afficher les stratégies de service existantes	`network interface service-policy show`

Informations associées

- "présentation du service d'interface réseau"
- "stratégie de service de l'interface réseau"
- "annulation de snapmirror"

Création des LIF ONTAP

Un SVM fournit des données aux clients via une ou plusieurs interfaces logiques réseau (LIF). Vous devez créer les LIFs sur les ports que vous souhaitez utiliser pour accéder aux données. Une LIF (interface réseau) est une adresse IP associée à un port physique ou logique. En cas de panne d'un composant, une LIF peut basculer vers un autre port physique ou la migrer vers un autre port, ce qui continue à communiquer avec le réseau.

Et des meilleures pratiques

Les ports de commutateur connectés à ONTAP doivent être configurés en tant que ports de périphérie « spanning Tree » afin de réduire les retards lors de la migration des LIF.

Avant de commencer

- Vous devez être un administrateur de cluster pour effectuer cette tâche.
- Le port réseau physique ou logique sous-jacent doit avoir été configuré pour que le statut administratif soit activé.
- Si vous prévoyez d'utiliser un nom de sous-réseau pour allouer la valeur de l'adresse IP et du masque de réseau à une LIF, le sous-réseau doit déjà exister.

  Les sous-réseaux contiennent un pool d'adresses IP qui appartiennent au même sous-réseau de couche 3. Ils sont créés à l'aide de System Manager ou de `network subnet create` commande.

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

- Le mécanisme de spécification du type de trafic traité par une LIF a changé. Pour ONTAP 9.5 et versions antérieures, la LIF utilisait des rôles pour spécifier le type de trafic qu'elle entraînerait. Depuis ONTAP 9.6, les LIF utilisent des politiques de service pour spécifier le type de trafic qu'elles seraient à traiter.

Description de la tâche

- Vous ne pouvez pas attribuer des protocoles NAS et SAN à la même LIF.

  Les protocoles pris en charge sont SMB, NFS, FlexCache, iSCSI et FC ; ISCSI et FC ne peuvent pas être associés à d'autres protocoles. Les protocoles NAS et SAN Ethernet peuvent toutefois être présents sur le même port physique.

  - Vous ne devez pas configurer les LIF qui transportent le trafic SMB afin de revenir automatiquement à leurs nœuds de départ. Cette recommandation est obligatoire si le serveur SMB doit héberger une solution pour la continuité de l'activité avec Hyper-V ou SQL Server over SMB.
- Vous pouvez créer des LIF IPv4 et IPv6 sur le même port réseau.
- Tous les services de mappage de noms et de résolution de noms d'hôte utilisés par un SVM, tel que DNS, NIS, LDAP, et Active Directory, Doit être accessible à partir d'au moins une LIF gérant le trafic de données du SVM.
- Une LIF gérant le trafic intracluster entre des nœuds ne doit pas se trouver sur le même sous-réseau que le trafic de gestion d'une LIF ou encore le trafic de données géré par une LIF.
- La création d'une LIF ne disposant pas de cible de basculement valide entraîne un message d'avertissement.
- Si vous disposez d'un grand nombre de LIF dans le cluster, vous pouvez vérifier la capacité LIF prise en charge sur le cluster :
  - System Manager : depuis ONTAP 9.12.0, consultez le débit de la grille de l'interface réseau.
  - Interface de ligne de commandes : utilisez le `network interface capacity show` Et la capacité LIF prise en charge sur chaque nœud à l'aide de `network interface capacity details show` commande (au niveau de privilège avancé).

    Pour en savoir plus sur `network interface capacity show` et `network interface capacity details show` dans le "Référence de commande ONTAP".

- Depuis ONTAP 9.7, si d'autres LIF existent déjà pour le SVM dans le même sous-réseau, il n'est pas nécessaire de spécifier le home port de la LIF. ONTAP choisit automatiquement un port aléatoire sur le nœud de rattachement spécifié dans le même domaine de diffusion que les autres LIFs déjà configurées dans le même sous-réseau.

  Le protocole FC-NVMe est pris en charge à partir de la version ONTAP 9.4. Si vous créez une LIF FC-

NVMe, notez les éléments suivants :

  - Le protocole NVMe doit être pris en charge par l'adaptateur FC sur lequel la LIF est créée.
  - FC-NVMe est le seul protocole de données sur les LIF de données.

- Un trafic de gestion des LIF doit être configuré pour chaque SVM (Storage Virtual machine) prenant en charge les protocoles SAN.
- Les LIFs et namespaces NVMe doivent être hébergés sur le même nœud.
- Un maximum de deux LIF NVMe traitant le trafic de données peut être configuré par SVM, par nœud.
- Lorsque vous créez une interface réseau avec un sous-réseau, ONTAP sélectionne automatiquement une adresse IP disponible à partir du sous-réseau sélectionné et l'attribue à l'interface réseau. Vous pouvez modifier le sous-réseau s'il y a plusieurs sous-réseaux, mais vous ne pouvez pas modifier l'adresse IP.
- Lorsque vous créez (ajoutez) un SVM, pour une interface réseau, vous ne pouvez pas spécifier une adresse IP comprise dans la plage d'un sous-réseau existant. Vous recevrez une erreur de conflit de sous-réseau. Ce problème survient sur d'autres flux de production d'une interface réseau, comme la création ou la modification des interfaces réseau inter-cluster dans les paramètres des SVM ou les paramètres du cluster.
- Depuis la version ONTAP 9.10.1, les `network interface` commandes CLI incluent un `-rdma -protocols` paramètre pour les configurations NFS sur RDMA. La création d'interfaces réseau pour les configurations NFS sur RDMA est prise en charge dans System Manager à partir de ONTAP 9.12.1. Pour plus d'informations, voir Configuration DES LIF pour NFS sur RDMA.
- Depuis la version ONTAP 9.11.1, le basculement automatique des LIF iSCSI est disponible sur les plateformes ASA (All-Flash SAN Array).

  Le basculement de LIF iSCSI est automatiquement activé (la règle de basculement est définie sur `sfo-partner-only` la valeur de restauration automatique est définie sur `true`) Sur les LIF iSCSI nouvellement créées si aucune LIF iSCSI n'existe dans le SVM spécifié ou si toutes les LIFs iSCSI existantes du SVM spécifié sont déjà activées avec le basculement LIF iSCSI.

  Si après une mise à niveau vers ONTAP 9.11.1 ou version ultérieure, vous disposez de LIF iSCSI existantes dans un SVM qui n'ont pas été activées avec la fonctionnalité de basculement LIF iSCSI et que vous créez de nouvelles LIF iSCSI dans le même SVM, les nouvelles LIF iSCSI supposent la même politique de basculement (`disabled`) Des LIFs iSCSI existantes du SVM.

  "Basculement de LIF iSCSI pour les plateformes ASA"

Depuis ONTAP 9.7, ONTAP choisit automatiquement le port de base d'une LIF, tant qu'au moins une LIF existe déjà dans le même sous-réseau dans cet IPspace. ONTAP choisit un port home-port dans le même domaine de diffusion que d'autres LIFs de ce sous-réseau. Vous pouvez toujours spécifier un port home port, mais ce n'est plus nécessaire (sauf si aucune LIF n'existe encore dans ce sous-réseau dans l'IPspace spécifié).

Depuis ONTAP 9.12.0, la procédure à suivre dépend de l'interface que vous utilisez—System Manager ou de l'interface de ligne de commandes :

System Manager

Utilisez System Manager pour ajouter une interface réseau

Étapes

1. Sélectionnez **réseau > Présentation > interfaces réseau**.
2. Sélectionnez + Add .
3. Sélectionnez l'un des rôles d'interface suivants :
   a. Les données
   b. Intercluster
   c. Gestion SVM
4. Sélectionnez le protocole :
   a. SMB/CIFS ET NFS
   b. ISCSI
   c. FC
   d. NVMe/FC
   e. NVMe/TCP
5. Nommez la LIF ou acceptez le nom généré par vos sélections précédentes.
6. Acceptez le nœud de départ ou utilisez le menu déroulant pour en sélectionner un.
7. Si au moins un sous-réseau est configuré dans l'IPspace du SVM sélectionné, la liste déroulante sous-réseau est affichée.
   a. Si vous sélectionnez un sous-réseau, choisissez-le dans la liste déroulante.
   b. Si vous continuez sans sous-réseau, la liste déroulante broadcast domain s'affiche :
      i. Spécifiez l'adresse IP. Si l'adresse IP est utilisée, un message d'avertissement s'affiche.
      ii. Spécifiez un masque de sous-réseau.
8. Sélectionnez le port d'accueil dans le domaine de diffusion, soit automatiquement (recommandé), soit en sélectionnant un dans le menu déroulant. Le contrôle du port Home s'affiche en fonction du domaine de diffusion ou de la sélection du sous-réseau.
9. Enregistrez l'interface réseau.

CLI

Utilisez l'interface de ligne de commande pour créer une LIF

Étapes

1. Déterminez les ports de broadcast domain que vous souhaitez utiliser pour le LIF.

   ```
   network port broadcast-domain show -ipspace ipspace1
   ```

```
IPspace     Broadcast                         Update
Name        Domain name   MTU   Port List     Status Details
ipspace1
            default       1500
                                node1:e0d     complete
                                node1:e0e     complete
                                node2:e0d     complete
                                node2:e0e     complete
```

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

2. Vérifiez que le sous-réseau que vous souhaitez utiliser pour les LIF contient suffisamment d'adresses IP inutilisées.

   `network subnet show -ipspace` *`ipspace1`*

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

3. Créez une ou plusieurs LIF sur les ports que vous souhaitez utiliser pour accéder aux données.

   > NetApp recommande la création d'objets de sous-réseau pour toutes les LIFs sur les SVM de données. Cela est particulièrement important dans les configurations MetroCluster, où l'objet de sous-réseau permet à ONTAP de déterminer les cibles de basculement sur le cluster de destination, car chaque objet de sous-réseau possède un broadcast associé. Pour obtenir des instructions, reportez-vous à "Créez un sous-réseau"la .

```
network interface create -vserver _SVM_name_ -lif _lif_name_
-service-policy _service_policy_name_ -home-node _node_name_ -home
-port port_name {-address _IP_address_ - netmask _Netmask_value_ |
-subnet-name _subnet_name_} -firewall- policy _policy_ -auto-revert
{true|false}
```

   - `-home-node` Est le nœud vers lequel la LIF renvoie lorsque `network interface revert` La commande est exécutée sur le LIF.

     Vous pouvez également indiquer si la LIF doit revenir automatiquement au nœud home et au port home-port avec l'option -auto-revert.

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

   - `-home-port` Est le port physique ou logique vers lequel la LIF renvoie lorsque `network interface revert` La commande est exécutée sur le LIF.
   - Vous pouvez spécifier une adresse IP avec le `-address` et `-netmask` ou vous activez l'allocation à partir d'un sous-réseau avec `-subnet_name` option.

- Lors de l'utilisation d'un sous-réseau pour fournir l'adresse IP et le masque de réseau, si le sous-réseau a été défini avec une passerelle, une route par défaut vers cette passerelle est ajoutée automatiquement au SVM lorsqu'une LIF est créée à l'aide de ce sous-réseau.
- Si vous attribuez des adresses IP manuellement (sans utiliser de sous-réseau), vous devrez peut-être configurer une route par défaut vers une passerelle si des clients ou des contrôleurs de domaine se trouvent sur un autre sous-réseau IP. Pour en savoir plus, `network route create` consultez le "Référence de commande ONTAP".
- `-auto-revert` Vous permet de spécifier si une LIF de données est automatiquement rétablie sur le nœud de rattachement en cas de démarrage, de modifications du statut de la base de données de gestion ou lors de la connexion réseau. Le paramètre par défaut est `false`, mais vous pouvez le définir sur `true` selon les stratégies de gestion de réseau de votre environnement.
- `-service-policy` Depuis ONTAP 9.5, vous pouvez attribuer une policy de service pour la LIF avec le `-service-policy` option.
  Lorsqu'une politique de services est spécifiée pour une LIF, cette règle est utilisée pour construire un rôle par défaut, une politique de basculement et une liste de protocoles de données pour la LIF. Dans ONTAP 9.5, les stratégies de service sont prises en charge uniquement pour les services de pairs intercluster et BGP. Dans ONTAP 9.6, vous pouvez créer des stratégies de service pour plusieurs services de données et de gestion.
- `-data-protocol` Permet de créer une LIF qui prend en charge les protocoles FCP ou NVMe/FC. Cette option n'est pas requise lors de la création d'une LIF IP.

4. **Facultatif** : attribuez une adresse IPv6 dans l'option -address :

   a. Utilisez le `network ndp prefix show` Commande permettant d'afficher la liste des préfixes de RA apprises sur diverses interfaces.

      Le `network ndp prefix show` la commande est disponible au niveau de privilège avancé.

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

   b. Utiliser le format `prefix::id` Pour construire l'adresse IPv6 manuellement.

      `prefix` est le préfixe utilisé sur les différentes interfaces.

   Pour calculer le `id`, choisissez un nombre hexadécimal 64 bits aléatoire.

5. Vérifier que la configuration de l'interface LIF est correcte.

   ```
   network interface show -vserver vs1
   ```

```
          Logical    Status     Network          Current   Current Is
Vserver   Interface  Admin/Oper Address/Mask     Node      Port
Home
--------- ---------- ---------- --------------- --------- -------
----
vs1
           lif1       up/up      10.0.0.128/24   node1     e0d
true
```

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

6. Vérifiez que la configuration du groupe de basculement est la plus appropriée.

   `network interface show -failover -vserver vs1`

```
         Logical    Home       Failover        Failover
Vserver  interface  Node:Port  Policy          Group
-------- ---------- ---------  ---------       --------
vs1
         lif1       node1:e0d  system-defined  ipspace1
Failover Targets: node1:e0d, node1:e0e, node2:e0d, node2:e0e
```

7. Vérifiez que l'adresse IP configurée est accessible :

Pour vérifier…	Utiliser…
Adresse IPv4	ping réseau
Adresse IPv6	réseau ping6

Exemples

La commande suivante crée une LIF et spécifie les valeurs d'adresse IP et de masque réseau à l'aide de `-address` et `-netmask` paramètres :

```
network interface create -vserver vs1.example.com -lif datalif1
-service-policy default-data-files -home-node node-4 -home-port e1c
-address 192.0.2.145 -netmask 255.255.255.0 -auto-revert true
```

La commande suivante crée une LIF et attribue des valeurs d'adresse IP et de masque réseau à partir du sous-réseau spécifié (nommé client1_sub) :

```
network interface create -vserver vs3.example.com -lif datalif3
-service-policy default-data-files -home-node node-3 -home-port e1c
-subnet-name client1_sub - auto-revert true
```

La commande suivante crée une LIF NVMe/FC et spécifie le `nvme-fc` protocole de données :

```
network interface create -vserver vs1.example.com -lif datalif1 -data
-protocol nvme-fc -home-node node-4 -home-port 1c -address 192.0.2.145
-netmask 255.255.255.0 -auto-revert true
```

Modifiez les LIFs ONTAP

Vous pouvez modifier une LIF en modifiant les attributs, tels que le nœud de rattachement ou le nœud actuel, l'état administratif, l'adresse IP, le masque de réseau, la règle de basculement, la politique de pare-feu et la politique de service. Vous pouvez également modifier la famille d'adresses d'une LIF d'IPv4 à IPv6.

Description de la tâche

- Lorsque vous modifiez le statut administratif d'une LIF en cas de panne, tout verrouillage NFSv4 en attente est conservé jusqu'à ce que le statut administratif de la LIF soit renvoyé à une date supérieure.

  Pour éviter les conflits de verrouillage pouvant survenir lorsque d'autres LIFs tentent d'accéder aux fichiers verrouillés, vous devez déplacer les clients NFSv4 vers une autre LIF avant de définir le statut administratif sur down.

- Vous ne pouvez pas modifier les protocoles de données utilisés par une LIF FC. Toutefois, vous pouvez modifier les services affectés à une politique de service ou modifier la politique de service attribuée à une LIF IP.

  Pour modifier les protocoles de données utilisés par une LIF FC, il faut supprimer cette LIF, puis la recréer. Pour modifier la stratégie de service à une LIF IP, une brève interruption se produit lors des mises à jour.

- Vous ne pouvez pas modifier le nœud de rattachement ou le nœud actuel d'un LIF de management scoped node-scoped.
- Lors de l'utilisation d'un sous-réseau pour modifier l'adresse IP et la valeur du masque réseau d'une LIF, une adresse IP est allouée à partir du sous-réseau spécifié ; si l'adresse IP précédente de la LIF provient d'un autre sous-réseau, l'adresse IP est renvoyée à ce sous-réseau.
- Pour modifier la famille d'adresses d'une LIF d'IPv4 vers IPv6, vous devez utiliser la notation des deux-points pour l'adresse IPv6 et ajouter une nouvelle valeur pour le `-netmask-length` paramètre.
- Vous ne pouvez pas modifier les adresses IPv6 lien-local configurées automatiquement.
- La modification d'une LIF entraînant l'absence de cible de basculement valide entraîne un message d'avertissement.

  Si une LIF ne disposant pas de tentatives de basculement cible valides, une panne peut se produire.

- Depuis ONTAP 9.5, vous pouvez modifier la politique de service associée à une LIF.

  Dans ONTAP 9.5, les stratégies de service sont prises en charge uniquement pour les services de pairs intercluster et BGP. Dans ONTAP 9.6, vous pouvez créer des stratégies de service pour plusieurs services de données et de gestion.

- Depuis la version ONTAP 9.11.1, le basculement automatique des LIF iSCSI est disponible sur les plateformes ASA (All-Flash SAN Array).

Pour les LIF iSCSI préexistantes, c'est-à-dire les LIF créées avant la mise à niveau vers la version 9.11.1 ou ultérieure, vous pouvez modifier la règle de basculement sur incident en "Activer le basculement automatique de LIF iSCSI".

- ONTAP utilise le protocole NTP (Network Time Protocol) pour synchroniser l'heure sur le cluster. Après avoir modifié les adresses IP LIF, vous devrez peut-être mettre à jour la configuration NTP pour éviter les échecs de synchronisation. Pour plus d'informations, reportez-vous à la"Base de connaissances NetApp : Échec de la synchronisation NTP après un changement d'adresse IP LIF" .

La procédure à suivre dépend de l'interface que vous utilisez—System Manager ou de l'interface de ligne de commandes :

System Manager

À partir de ONTAP 9.12.0, vous pouvez utiliser System Manager pour modifier une interface réseau

Étapes

1. Sélectionnez **réseau > Présentation > interfaces réseau**.
2. Sélectionnez ⋮ **> Modifier** en regard de l'interface réseau que vous souhaitez modifier.
3. Modifiez un ou plusieurs paramètres de l'interface réseau. Pour plus de détails, voir "Créer une LIF".
4. Enregistrez les modifications.

CLI

Utilisez l'interface de ligne de commande pour modifier une LIF

Étapes

1. Modifier les attributs d'une LIF à l'aide de `network interface modify` commande.

   L'exemple suivant montre comment modifier l'adresse IP et le masque de réseau de LIF datalif2 en utilisant une adresse IP et la valeur du masque de réseau de subnet client1_sub :

   ```
   network interface modify -vserver vs1 -lif datalif2 -subnet-name
   client1_sub
   ```

   L'exemple suivant montre comment modifier la politique de service d'une LIF.

   ```
   network interface modify -vserver siteA -lif node1_inter1 -service
   -policy example
   ```

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

2. Vérifiez que les adresses IP sont accessibles.

Si vous utilisez…	Puis utilisez…
Adresses IPv4	`network ping`
Adresses IPv6	`network ping6`

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

Migrez les LIF ONTAP

Vous pouvez avoir à migrer une LIF vers un autre port du même nœud ou d'un autre nœud du cluster, si le port est défectueux ou nécessite une maintenance. La migration

d'une LIF est similaire au basculement de LIF, mais la migration de LIF est une opération manuelle, tandis que le basculement de LIF est la migration automatique d'une LIF en réponse à une défaillance de liaison sur le port réseau actuel du LIF.

Avant de commencer

- Un failover group doit avoir été configuré pour les LIFs.
- Le nœud et les ports de destination doivent être opérationnels et doivent pouvoir accéder au même réseau que le port source.

Description de la tâche

- Les LIF BGP résident sur le port de rattachement et ne peuvent pas être migrées vers un autre nœud ou port.
- Vous devez migrer les LIFs hébergées sur les ports appartenant à une carte réseau vers d'autres ports du cluster, avant de retirer la carte réseau du nœud.
- Vous devez exécuter la commande pour migrer une LIF de cluster à partir du nœud sur lequel la LIF de cluster est hébergée.
- Un LIF node-scoped, tel qu'une LIF node-scoped management, cluster LIF, intercluster LIF, ne peut pas être migré vers un nœud distant.
- Lorsqu'une LIF NFSv4 est migrée entre les nœuds, un délai de 45 secondes peut atteindre les résultats avant que la LIF ne soit disponible sur un nouveau port.

  Pour contourner ce problème, utilisez NFSv4.1 en cas de retard.

- Vous pouvez migrer des LIF iSCSI sur des plateformes ASA exécutant ONTAP 9.11.1 ou une version ultérieure.

  La migration des LIF iSCSI est limitée aux ports du nœud de rattachement ou du partenaire de haute disponibilité.

- Si votre plateforme n'est pas une baie SAN 100 % Flash (ASA) exécutant ONTAP version 9.11.1 ou ultérieure, vous ne pouvez pas migrer les LIF iSCSI d'un nœud vers un autre.

  Pour contourner cette restriction, vous devez créer une LIF iSCSI sur le nœud de destination. En savoir plus sur "Création des LIFs iSCSI".

- Si vous souhaitez migrer une LIF (interface réseau) pour NFS sur RDMA, vous devez vous assurer que le port de destination est compatible RoCE. Vous devez exécuter ONTAP 9.10.1 ou version ultérieure pour migrer une LIF avec l'interface de ligne de commandes ou ONTAP 9.12.1 pour effectuer la migration à l'aide de System Manager. Dans System Manager, une fois que vous avez sélectionné votre port de destination compatible RoCE, vous devez cocher la case en regard de **utiliser les ports RoCE** pour terminer la migration. En savoir plus sur "Configuration des LIFs pour NFS sur RDMA".
- Les opérations de déchargement des copies VMware VAAI échouent lors de la migration du LIF source ou de destination. En savoir plus sur la copie hors chargement :
  - "Les environnements NFS"
  - "Environnements SAN"

La procédure à suivre dépend de l'interface que vous utilisez—System Manager ou de l'interface de ligne de commandes :

System Manager

Utilisez System Manager pour migrer une interface réseau

Étapes

1. Sélectionnez **réseau > Présentation > interfaces réseau**.
2. Sélectionnez ⋮ **> migrer** en regard de l'interface réseau à modifier.

   Pour une LIF iSCSI, dans la boîte de dialogue **Migrate interface**, sélectionnez le nœud de destination et le port du partenaire HA.

   Si vous souhaitez migrer définitivement la LIF iSCSI, cochez la case. La LIF iSCSI doit être hors ligne avant d'être définitivement migrée. De plus, une fois la migration permanente d'une LIF iSCSI, celle-ci ne peut pas être annulée. Il n'y a pas d'option de restauration.

3. Cliquez sur **migrer**.
4. Enregistrez les modifications.

CLI

Utilisez l'interface de ligne de commande pour migrer une LIF

Étape

Selon que vous souhaitez migrer une LIF ou toutes les LIF, effectuez l'action appropriée :

Pour migrer…	Saisissez la commande suivante…
Une LIF spécifique	`network interface migrate`
Toutes les LIF de gestion des données et du cluster sur un nœud	`network interface migrate-all`
Toutes les LIFs hors d'un port	`network interface migrate-all -node <node> -port <port>`

L'exemple suivant montre comment migrer une LIF nommée `datalif1` Sur le SVM `vs0` vers le port `e0d` marche `node0b`:

```
network interface migrate -vserver vs0 -lif datalif1 -dest-node node0b
-dest-port e0d
```

L'exemple suivant montre comment migrer toutes les LIFs de données et cluster-management depuis le nœud actuel (local) :

```
network interface migrate-all -node local
```

Informations associées

- "migration des interfaces réseau"

Restaure une LIF sur son port d'attache après un basculement de nœud ONTAP ou une migration de port

Vous pouvez restaurer une LIF vers son port de base après qu'elle échoue ou qu'elle est migrée vers un autre port manuellement ou automatiquement. Si le port de home d'une LIF particulière n'est pas disponible, la LIF reste sur son port actuel et n'est pas rétablie.

Description de la tâche

- Si vous rétablir d'un point de vue administratif l'état du port de base d'une LIF avant de configurer l'option de restauration automatique, la LIF n'est pas renvoyée au port de base.
- La LIF ne revient pas automatiquement, sauf si la valeur de l'option « auto-revert » est définie sur vrai.
- Vous devez vous assurer que l'option de restauration automatique est activée pour que les LIF puissent revenir à leurs ports de base.

La procédure à suivre dépend de l'interface que vous utilisez—System Manager ou de l'interface de ligne de commandes :

System Manager

Utilisez System Manager pour rétablir une interface réseau à son port d'accueil

Étapes

1. Sélectionnez **réseau > Présentation > interfaces réseau**.
2. Sélectionnez ⋮ **> Revert** en regard de l'interface réseau que vous souhaitez modifier.
3. Sélectionnez **Revert** pour rétablir une interface réseau à son port d'origine.

CLI

Utilisez l'interface de ligne de commande pour rétablir une LIF à son port d'accueil

Étape

Restaurez une LIF manuellement ou automatiquement sur son port de base :

Si vous souhaitez restaurer une LIF vers son port de base…	Entrez ensuite la commande suivante…
Manuellement	`network interface revert -vserver vserver_name -lif lif_name`
Automatiquement	`network interface modify -vserver vserver_name -lif lif_name -auto-revert true`

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

Restaurer une LIF ONTAP mal configurée

Un cluster ne peut pas être créé lorsque le réseau de cluster est câblé à un commutateur,

mais tous les ports configurés dans le Cluster IPspace peuvent atteindre les autres ports configurés dans le Cluster IPspace.

Description de la tâche

Dans un cluster commuté, si une interface réseau de cluster (LIF) est configurée sur le port inapproprié ou si un port de cluster est câblé dans le mauvais réseau, le `cluster create` la commande peut échouer avec l'erreur suivante :

```
Not all local cluster ports have reachability to one another.
Use the "network port reachability show -detail" command for more details.
```

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

Les résultats de la `network port show` commande peuvent afficher que plusieurs ports sont ajoutés au Cluster IPspace car ils sont connectés à un port configuré avec une LIF de cluster. Cependant, les résultats de la `network port reachability show -detail` la commande révèle quels ports n'ont pas de connectivité entre eux.

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

Pour restaurer une LIF de cluster configurée sur un port qui n'est pas accessible aux autres ports configurés avec des LIFs de cluster, effectuez les opérations suivantes :

Étapes

1. Réinitialiser le home port de la LIF de cluster sur le port correct :

   ```
   network port modify -home-port
   ```

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

2. Retirer les ports qui ne disposent pas de LIFs de cluster configurées sur eux du cluster broadcast domain :

   ```
   network port broadcast-domain remove-ports
   ```

   Pour en savoir plus, `network port broadcast-domain remove-ports` consultez le "Référence de commande ONTAP".

3. Création du cluster :

   ```
   cluster create
   ```

Résultat

Une fois le cluster créé, le système détecte la configuration correcte et place les ports dans les domaines de diffusion appropriés.

Informations associées

- "affichage de l'accessibilité des ports réseau"

Supprimez les LIFs ONTAP

Vous pouvez supprimer une interface réseau (LIF) qui n'est plus requise.

Avant de commencer

Les LIFs à supprimer ne doivent pas être en cours d'utilisation.

Étapes

1. Marquez les LIFs que vous souhaitez supprimer comme administrativement arrêtées à l'aide de la commande suivante :

```
network interface modify -vserver vserver_name -lif lif_name -status
-admin down
```

2. Utilisez le `network interface delete` Commande de suppression d'une ou de l'ensemble des LIFs :

Si vous souhaitez supprimer…	Entrez la commande …
Une LIF spécifique	`network interface delete -vserver vserver_name -lif lif_name`
Toutes les LIF	`network interface delete -vserver vserver_name -lif *`

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

   La commande suivante supprime le LIF mgmtlif2 :

```
network interface delete -vserver vs1 -lif mgmtlif2
```

3. Utilisez le `network interface show` Commande pour confirmer que la LIF est supprimée.

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

Configuration des LIF ONTAP Virtual IP (VIP

Certains data centers nouvelle génération utilisent des mécanismes réseau de couche 3 (IP) qui nécessitent le basculement des LIF sur les sous-réseaux. ONTAP prend en charge les LIF de données IP virtuelles (VIP) et le protocole de routage associé, BGP (Border Gateway Protocol), afin de répondre aux exigences de basculement de ces réseaux nouvelle génération.

Description de la tâche

Une LIF de données VIP est une LIF qui ne fait pas partie d'un sous-réseau et est accessible depuis tous les ports qui hébergent une LIF BGP dans le même IPspace. Une LIF de données VIP élimine la dépendance d'un

hôte sur des interfaces réseau individuelles. Étant donné que plusieurs adaptateurs physiques transportent le trafic des données, la charge entière n'est pas concentrée sur un seul adaptateur et le sous-réseau associé. L'existence d'une LIF de données VIP est annoncée pour les routeurs homologues par le biais du protocole de routage, BGP (Border Gateway Protocol).

Les LIF de données VIP offrent les avantages suivants :

- Portabilité de LIF au-delà d'un domaine de broadcast ou d'un sous-réseau : les LIF de données VIP peuvent basculer vers n'importe quel sous-réseau du réseau en annonçant l'emplacement actuel de chaque LIF de données VIP vers des routeurs via BGP.
- Débit global : la LIF de données VIP peut prendre en charge un débit global supérieur à celui d'un port individuel, car les LIF VIP peuvent envoyer ou recevoir simultanément des données provenant de plusieurs sous-réseaux ou ports.

Configuration du protocole BGP (Border Gateway Protocol)

Avant de créer des LIF VIP, vous devez configurer le protocole BGP, qui est le protocole de routage utilisé pour annoncer l'existence d'une LIF VIP pour les routeurs de l'égal.

À partir de ONTAP 9.9.1, VIP fournit une automatisation de route par défaut facultative à l'aide de groupes de pairs BGP pour simplifier la configuration.

ONTAP offre un moyen simple d'apprendre les routes par défaut en utilisant les pairs BGP comme routeurs de saut suivant lorsque l'homologue BGP se trouve sur le même sous-réseau. Pour utiliser la fonction, définissez l' `-use-peer-as-next-hop` attribut à `true`. Par défaut, cet attribut est `false`.

Si vous avez des routes statiques configurées, celles-ci sont encore préférées sur ces routes automatisées par défaut.

Avant de commencer

Le routeur homologue doit être configuré pour accepter une connexion BGP à partir du LIF BGP pour le numéro de système autonome configuré (ASN).

> ONTAP ne traite aucune annonce de route entrante à partir du routeur ; par conséquent, vous devez configurer le routeur homologue pour qu'il n'envoie aucune mise à jour de route au cluster. Cela réduit le temps nécessaire à la communication avec l'homologue pour devenir entièrement fonctionnel et réduit l'utilisation de la mémoire interne dans ONTAP.

Description de la tâche

La configuration du protocole BGP implique la création d'une configuration BGP, la création d'une LIF BGP et la création d'un groupe de pairs BGP. ONTAP crée automatiquement une configuration BGP par défaut avec des valeurs par défaut lorsque le premier groupe de pairs BGP est créé sur un nœud donné.

Une LIF BGP est utilisée pour établir des sessions TCP BGP avec des routeurs homologues. Pour un routeur homologue, une LIF BGP est le prochain saut pour atteindre une LIF VIP. Le basculement est désactivé pour le LIF BGP. Un groupe de pairs BGP annonce les routes VIP pour tous les SVM dans l'IPspace utilisé par le groupe de pairs. L'IPspace utilisé par le groupe de pairs est hérité de la LIF BGP.

À partir de ONTAP 9.16.1, l'authentification MD5 est prise en charge sur les groupes de pairs BGP pour protéger les sessions BGP. Lorsque MD5 est activé, les sessions BGP ne peuvent être établies et traitées que parmi les pairs autorisés, ce qui empêche les interruptions potentielles de la session par un acteur non autorisé.

Les champs suivants ont été ajoutés aux `network bgp peer-group create` commandes et `network bgp peer-group modify` :

- `-md5-enabled <true/false>`
- `-md5-secret <md5 secret in string or hex format>`

Ces paramètres vous permettent de configurer un groupe de pairs BGP avec une signature MD5 pour une sécurité renforcée. Les conditions suivantes s'appliquent à l'utilisation de l'authentification MD5 :

- Vous ne pouvez spécifier le paramètre que `-md5-secret` lorsque le `-md5-enabled` paramètre est défini sur `true`.
- IPSec doit être activé globalement avant de pouvoir activer l'authentification MD5 BGP. La LIF BGP n'est pas nécessaire pour avoir une configuration IPsec active. Reportez-vous à la "Configurez la sécurité IP (IPsec) sur le cryptage filaire".
- NetApp vous recommande de configurer MD5 sur le routeur avant de le configurer sur le contrôleur ONTAP.

Depuis ONTAP 9.9.1, ces champs ont été ajoutés :

- `-asn` Ou `-peer-asn` (valeur de 4 octets) l'attribut lui-même n'est pas nouveau, mais il utilise maintenant un entier de 4 octets.
- `-med`
- `-use-peer-as-next-hop`

Vous pouvez effectuer des sélections avancées de route grâce à la prise en charge du décriminateur multi-sortie (MED) pour la hiérarchisation des chemins. MED est un attribut facultatif du message de mise à jour BGP qui indique aux routeurs de sélectionner le meilleur itinéraire pour le trafic. Le MED est un entier 32 bits non signé (0 - 4294967295) ; les valeurs inférieures sont préférées.

Depuis ONTAP 9.8, ces champs ont été ajoutés au `network bgp peer-group` commande :

- `-asn-prepend-type`
- `-asn-prepend-count`
- `-community`

Ces attributs BGP permettent de configurer le EN TANT qu'attributs de chemin et de communauté pour le groupe de pairs BGP.

> Bien que ONTAP prenne en charge les attributs BGP ci-dessus, les routeurs n'ont pas besoin de les honorer. NetApp vous recommande fortement de confirmer les attributs pris en charge par votre routeur et de configurer les groupes de pairs BGP en conséquence. Pour plus de détails, reportez-vous à la documentation BGP fournie par votre routeur.

Étapes

1. Connectez-vous au niveau de privilège avancé :

   ```
   set -privilege advanced
   ```

2. Facultatif : créez une configuration BGP ou modifiez la configuration par défaut du cluster en effectuant

l'une des opérations suivantes :

a. Créez une configuration BGP :

```
network bgp config create -node {node_name | local} -asn <asn_number>
-holdtime
<hold_time> -routerid <router_id>
```

- Le `-routerid` paramètre accepte une valeur de 32 bits à virgule décimale à points qui ne doit être unique que dans un domaine AS. NetApp vous recommande d'utiliser l'adresse IP de gestion des nœuds (v4) `<router_id>` pour garantir leur caractère unique.
- Bien que ONTAP BGP prenne en charge les nombres ASN 32 bits, seule la notation décimale standard est prise en charge. La notation ASN en pointillés, telle que 65000.1 au lieu de 4259840001 pour un ASN privé, n'est pas prise en charge.

Échantillon avec un ASN de 2 octets :

```
network bgp config create -node node1 -asn 65502 -holdtime 180
-routerid 1.1.1.1
```

Exemple avec un ASN de 4 octets :

```
network bgp config create -node node1 -asn 85502 -holdtime 180 -routerid
1.1.1.1
```

a. Modifiez la configuration BGP par défaut :

```
network bgp defaults modify -asn <asn_number> -holdtime <hold_time>
network bgp defaults modify -asn 65502 -holdtime 60
```

- `<asn_number>` Spécifie le numéro ASN. À partir de ONTAP 9.8, ASN pour BGP prend en charge un entier non négatif de 2 octets. Il s'agit d'un nombre de 16 bits (1 à 65534 valeurs disponibles). À partir de ONTAP 9.9.1, ASN pour BGP prend en charge un entier non négatif de 4 octets (1 à 4294967295). L'ASN par défaut est 65501. ASN 23456 est réservé à l'établissement de session ONTAP avec des pairs qui n'annoncent pas la capacité ASN de 4 octets.
- `<hold_time>` spécifie le temps de maintien en secondes. La valeur par défaut est 180s.

ONTAP ne prend en charge qu'un seul global `<asn_number>`, `<hold_time>`, , et `<router_id>`, même si vous configurez BGP pour plusieurs IPspaces. Le BGP et toutes les informations de routage IP sont complètement isolés au sein d'un IPspace. Un IPspace est équivalent à une instance de routage et de transfert virtuel (VRF).

3. Créez une LIF BGP pour le SVM du système :

   Pour l'IPspace par défaut, le nom du SVM correspond au nom du cluster. Pour les IPspaces supplémentaires, le nom du SVM est identique au nom IPspace.

   ```
   network interface create -vserver <system_svm> -lif <lif_name> -service
   -policy default-route-announce -home-node <home_node> -home-port
   <home_port> -address <ip_address> -netmask <netmask>
   ```

   Vous pouvez utiliser le `default-route-announce` Politique de service pour le LIF BGP ou toute règle de services personnalisée qui contient le service « management-bgp ».

   ```
   network interface create -vserver cluster1 -lif bgp1 -service-policy
   default-route-announce -home-node cluster1-01 -home-port e0c -address
   10.10.10.100 -netmask 255.255.255.0
   ```

4. Créez un groupe d'homologues BGP utilisé pour établir des sessions BGP avec les routeurs homologues distants et configurer les informations de routage VIP annoncées aux routeurs homologues :

   Exemple 1 : créez un groupe de pairs sans route par défaut automatique

   Dans ce cas, l'administrateur doit créer une route statique vers l'homologue BGP.

   ```
   network bgp peer-group create -peer-group <group_name> -ipspace
   <ipspace_name> -bgp-lif <bgp_lif> -peer-address <peer-router_ip_address>
   -peer-asn <peer_asn_number> {-route-preference <integer>} {-asn-prepend-
   type <ASN_prepend_type>} {-asn-prepend-count <integer>} {-med <integer>}
   {-community BGP community list <0-65535>:<0-65535>}
   ```

   ```
   network bgp peer-group create -peer-group group1 -ipspace Default -bgp
   -lif bgp1 -peer-address 10.10.10.1 -peer-asn 65503 -route-preference 100
   -asn-prepend-type local-asn -asn-prepend-count 2 -med 100 -community
   9000:900,8000:800
   ```

   Exemple 2 : créez un groupe de pairs avec une route par défaut automatique

   ```
   network bgp peer-group create -peer-group <group_name> -ipspace
   <ipspace_name> -bgp-lif <bgp_lif> -peer-address <peer-router_ip_address>
   -peer-asn <peer_asn_number> {-use-peer-as-next-hop true} {-route-
   preference <integer>} {-asn-prepend-type <ASN_prepend_type>} {-asn-
   prepend-count <integer>} {-med <integer>} {-community BGP community list
   <0-65535>:<0-65535>}
   ```

```
network bgp peer-group create -peer-group group1 -ipspace Default -bgp
-lif bgp1 -peer-address 10.10.10.1 -peer-asn 65503 -use-peer-as-next-hop
true -route-preference 100 -asn-prepend-type local-asn -asn-prepend
-count 2 -med 100 -community 9000:900,8000:800
```

Exemple 3 : créez un groupe de pairs avec MD5 activé

a. Activer IPsec :

```
security ipsec config modify -is-enabled true
```

b. Créez le groupe de pairs BGP avec MD5 activé :

```
network bgp peer-group create -ipspace Default -peer-group
<group_name> -bgp-lif bgp_lif -peer-address <peer_router_ip_address>
{-md5-enabled true} {-md5-secret <md5 secret in string or hex format>}
```

Exemple avec une clé hexagonale :

```
network bgp peer-group create -ipspace Default -peer-group peer1 -bgp
-lif bgp_lif1 -peer-address 10.1.1.100 -md5-enabled true -md5-secret
0x746573742073656372657400
```

Exemple d'utilisation d'une chaîne :

```
network bgp peer-group create -ipspace Default -peer-group peer1 -bgp
-lif bgp_lif1 -peer-address 10.1.1.100 -md5-enabled true -md5-secret "test
secret"
```

> Après avoir créé le groupe de pairs BGP, un port ethernet virtuel (en commençant par v0a..v0z,v1a…) apparaît lorsque vous exécutez la `network port show` commande. Le MTU de cette interface est toujours indiqué à 1500. Le MTU réel utilisé pour le trafic est dérivé du port physique (BGP LIF), qui est déterminé lors de l'envoi du trafic. Pour en savoir plus, `network port show` consultez le "Référence de commande ONTAP".

Créer une LIF de données VIP (Virtual IP

L'existence d'une LIF de données VIP est annoncée pour les routeurs homologues par le biais du protocole de routage, BGP (Border Gateway Protocol).

Avant de commencer

- Le groupe de pairs BGP doit être configuré et la session BGP pour le SVM sur lequel la LIF est créée doit être active.
- Une route statique vers le routeur BGP ou tout autre routeur du sous-réseau de la LIF BGP doit être créée

pour tout trafic VIP sortant pour la SVM.

- Vous devez activer le routage multivoie afin que le trafic VIP sortant puisse utiliser toutes les routes disponibles.

  Si le routage multichemin n'est pas activé, tout le trafic VIP sortant passe à partir d'une interface unique.

Étapes

1. Créer une LIF de données VIP :

   ```
   network interface create -vserver <svm_name> -lif <lif_name> -role data
   -data-protocol
   {nfs|cifs|iscsi|fcache|none|fc-nvme} -home-node <home_node> -address
   <ip_address> -is-vip true -failover-policy broadcast-domain-wide
   ```

   Un port VIP est automatiquement sélectionné si vous ne spécifiez pas le port d'accueil avec le `network interface create` commande.

   Par défaut, la LIF de données VIP appartient au domaine de diffusion créé par le système, nommé « VIP », pour chaque IPspace. Vous ne pouvez pas modifier le broadcast domain VIP.

   Une LIF de données VIP est accessible simultanément sur tous les ports hébergeant une LIF BGP d'un IPspace. En l'absence de session BGP active pour le SVM de VIP sur le nœud local, la LIF de données VIP bascule vers le port VIP suivant sur le nœud sur lequel une session BGP est établie pour ce SVM.

2. Vérifier que la session BGP est au statut up pour le SVM de la LIF de données VIP :

   ```
   network bgp vserver-status show

   Node        Vserver  bgp status
           ----------  -------- ---------
           node1       vs1      up
   ```

   Si le statut BGP est de `down` Pour le SVM sur un nœud, la LIF de données VIP bascule vers un nœud différent où l'état BGP est activé pour le SVM. Si le statut BGP est de `down` Sur tous les nœuds, la LIF de données VIP ne peut pas être hébergée n'importe où et possède le statut LIF comme étant arrêté.

Commandes de gestion du protocole BGP

À partir de ONTAP 9.5, vous utilisez le `network bgp` Commandes permettant de gérer les sessions BGP dans ONTAP.

Gérer la configuration BGP

Les fonctions que vous recherchez…	Utilisez cette commande…
Créez une configuration BGP	`network bgp config create`
Modifiez la configuration BGP	`network bgp config modify`

Supprimez la configuration BGP	`network bgp config delete`
Affiche la configuration BGP	`network bgp config show`
Affiche l'état BGP pour le SVM de la LIF VIP	`network bgp vserver-status show`

Gérer les valeurs par défaut du protocole BGP

Les fonctions que vous recherchez…	Utilisez cette commande…
Modifiez les valeurs par défaut du protocole BGP	`network bgp defaults modify`
Affiche les valeurs par défaut du protocole BGP	`network bgp defaults show`

Gérez les groupes de pairs BGP

Les fonctions que vous recherchez…	Utilisez cette commande…
Créez un groupe de pairs BGP	`network bgp peer-group create`
Modifiez un groupe de pairs BGP	`network bgp peer-group modify`
Supprimez un groupe de pairs BGP	`network bgp peer-group delete`
Affiche les informations sur les groupes de pairs BGP	`network bgp peer-group show`
Renommez un groupe d'homologues BGP	`network bgp peer-group rename`

Gérez les groupes de pairs BGP avec MD5

À partir de ONTAP 9.16.1, vous pouvez activer ou désactiver l'authentification MD5 sur un groupe de pairs BGP existant.

> Si vous activez ou désactivez MD5 sur un groupe de pairs BGP existant, la connexion BGP est interrompue et recréée pour appliquer les modifications de configuration MD5.

Les fonctions que vous recherchez…	Utilisez cette commande…
Activez MD5 sur un groupe de pairs BGP existant	`network bgp peer-group modify -ipspace Default -peer-group <group_name> -bgp -lif <bgp_lif> -peer-address <peer_router_ip_address> -md5-enabled true -md5-secret <md5 secret in string or hex format>`
Désactivez MD5 sur un groupe de pairs BGP existant	`network bgp peer-group modify -ipspace Default -peer-group <group_name> -bgp -lif <bgp_lif> -md5-enabled false`

Informations associées

- "Référence de commande ONTAP"
- "bgp réseau"
- "interface réseau"
- "modification de la configuration de sécurité IPsec"

Équilibrer les charges réseau

Optimisez le trafic réseau ONTAP à l'aide de l'équilibrage de la charge DNS

Vous pouvez configurer votre cluster pour qu'il serve les demandes des clients à partir des LIFs chargées correctement. L'utilisation des LIF et des ports est ainsi plus équilibrée, ce qui permet d'améliorer les performances du cluster.

L'équilibrage de la charge DNS permet de sélectionner une LIF de données correctement chargée et d'équilibrer le trafic du réseau utilisateur sur tous les ports disponibles (physique, groupes d'interface et VLAN).

Avec l'équilibrage de la charge DNS, les LIFs sont associées à la zone d'équilibrage de charge d'un SVM. Un serveur DNS à l'échelle du site est configuré pour transférer toutes les requêtes DNS et renvoyer la LIF la moins chargée en fonction du trafic réseau et de la disponibilité des ressources des ports (utilisation du CPU, débit, connexions ouvertes, etc.). L'équilibrage de charge DNS offre les avantages suivants :

- Les nouvelles connexions client sont équilibrées sur les ressources disponibles.
- Aucune intervention manuelle n'est requise pour déterminer quelles LIFs à utiliser lors du montage d'un SVM particulier.
- Équilibrage de la charge DNS prenant en charge NFSv3, NFSv4, NFSv4.1, SMB 2.0, SMB 2.1, SMB 3.0 et S3.

En savoir plus sur l'équilibrage de charge DNS pour le réseau ONTAP

Les clients montent un SVM en spécifiant une adresse IP (associée à une LIF) ou un nom d'hôte (associé à plusieurs adresses IP). Par défaut, les LIFs sont sélectionnées par le serveur DNS à l'échelle du site de manière round-Robin, qui équilibre la charge de travail sur tous les LIFs.

L'équilibrage de charge round-Robin peut entraîner la surcharge de certaines LIF. Vous avez donc la possibilité d'utiliser une zone d'équilibrage de charge DNS qui gère la résolution host-name dans un SVM. L'utilisation d'une zone d'équilibrage de charge DNS permet de mieux équilibrer les nouvelles connexions client sur les ressources disponibles, ce qui améliore les performances du cluster.

Une zone d'équilibrage de charge DNS est un serveur DNS au sein du cluster qui évalue dynamiquement la charge sur toutes les LIFs et renvoie un LIF chargé correctement. Dans une zone d'équilibrage de la charge, DNS attribue un poids (métrique), en fonction de la charge, à chaque LIF.

Un poids est attribué à chaque LIF en fonction de la charge des ports et de l'utilisation du CPU de son nœud de rattachement. Les LIF qui font partie de ports moins chargés ont plus de chances d'être renvoyées dans une requête DNS. Les poids peuvent également être attribués manuellement.

Créez des zones d'équilibrage de charge DNS pour le réseau ONTAP

Vous pouvez créer une zone d'équilibrage de charge DNS afin de faciliter la sélection dynamique d'une LIF basée sur la charge, c'est-à-dire le nombre de clients montés sur une LIF. Vous pouvez créer une zone d'équilibrage de la charge lors de la création d'une LIF de données.

Avant de commencer

Le DNS Forwarder du serveur DNS à l'échelle du site doit être configuré pour transférer toutes les requêtes de la zone d'équilibrage de charge vers les LIFs configurées.

Le"Base de connaissances NetApp : Comment configurer l'équilibrage de charge DNS en mode cluster" contient plus d'informations sur la configuration de l'équilibrage de charge DNS à l'aide de la redirection conditionnelle.

Description de la tâche

- Toute LIF de données peut répondre aux requêtes DNS pour un nom de zone d'équilibrage de charge DNS.
- Une zone d'équilibrage de charge DNS doit porter un nom unique dans le cluster, et le nom de zone doit répondre aux exigences suivantes :
  - Il ne doit pas dépasser 256 caractères.
  - Il doit inclure au moins une période.
  - Le premier et le dernier caractère ne doivent pas être un point ou tout autre caractère spécial.
  - Il ne peut pas inclure d'espace entre les caractères.
  - Chaque étiquette du nom DNS ne doit pas dépasser 63 caractères.

    Un libellé est le texte qui apparaît avant ou après la période. Par exemple, la zone DNS nommée storage.company.com comporte trois étiquettes.

Étape

Utilisez `network interface create` la commande avec `dns-zone` l'option pour créer une zone d'équilibrage de charge DNS. Pour en savoir plus, `network interface create` consultez le "Référence de commande ONTAP".

Si la zone d'équilibrage de charge existe déjà, le LIF le est ajouté.

L'exemple suivant montre comment créer une zone d'équilibrage de charge DNS nommée storage.company.com lors de la création de la LIF `lif1`:

```
network interface create -vserver vs0 -lif lif1 -home-node node1
-home-port e0c -address 192.0.2.129 -netmask 255.255.255.128 -dns-zone
storage.company.com
```

Ajouter ou supprimer une LIF ONTAP d'une zone d'équilibrage de charge

Vous pouvez ajouter ou supprimer une LIF de la zone DNS load balancing d'une machine virtuelle (SVM). Vous pouvez également supprimer toutes les LIFs simultanément d'une zone d'équilibrage de charge.

Avant de commencer

- Toutes les LIFs d'une zone d'équilibrage de charge doivent appartenir au même SVM.
- Une LIF ne peut faire partie que d'une seule zone d'équilibrage de charge DNS.
- Si les LIF appartiennent à un sous-réseau différent, les groupes de basculement doivent avoir été

configurés pour chaque sous-réseau.

Description de la tâche

Une LIF qui est à l'état administratif down est temporairement supprimée de la zone d'équilibrage de la charge DNS. Lorsque la LIF revient au statut administratif up, elle est automatiquement ajoutée à la zone DNS d'équilibrage de la charge.

Étape

Ajouter une LIF à ou supprimer une LIF d'une zone d'équilibrage de la charge :

Les fonctions que vous recherchez…	Entrer…
Ajouter une LIF	`network interface modify -vserver` *`vserver_name`* `-lif` *`lif_name`* `-dns-zone` *`zone_name`* Exemple : `network interface modify -vserver vs1 -lif data1 -dns -zone cifs.company.com`

Supprimer une seule LIF	`network interface modify -vserver` *`vserver_name`* `-lif` *`lif_name`* `-dns-zone none`
	Exemple :
	`network interface modify -vserver vs1 -lif data1 -dns -zone none`

Supprime toutes les LIFs	`network interface modify -vserver` *`vserver_name`* `-lif * -dns-zone none`
	Exemple :
	`network interface modify -vserver vs0 -lif * -dns-zone none`
	Vous pouvez supprimer un SVM d'une zone d'équilibrage de charge en supprimant toutes les LIFs du SVM de cette zone.

Informations associées

- "modification de l'interface réseau"

Configurer les services DNS pour le réseau ONTAP

On doit configurer les services DNS pour le SVM avant de créer un serveur NFS ou SMB. En général, les serveurs de noms DNS sont des serveurs DNS intégrés à Active Directory pour le domaine auquel le serveur NFS ou SMB sera joint.

Description de la tâche

Les serveurs DNS intégrés à Active Directory contiennent les enregistrements SRV (Service Location Records) pour les serveurs LDAP de domaine et de contrôleur de domaine. Si le SVM ne trouve pas les serveurs LDAP et les contrôleurs de domaine Active Directory, l'installation du serveur NFS ou SMB échoue.

Les SVM utilisent la base de données des services de nom d'hôtes ns-switch pour déterminer quels services de noms utiliser et dans quel ordre lors de la recherche d'informations sur les hôtes. Les deux services de noms pris en charge pour la base de données des hôtes sont des fichiers et dns.

Vous devez vous assurer que dns est l'une des sources avant de créer le serveur SMB.

Pour afficher les statistiques des services de noms DNS pour le processus mgwd et SECD, utilisez l'interface utilisateur Statistiques.

Étapes

1. Déterminez la configuration actuelle de la base de données des services de noms des hôtes. Dans cet exemple, la base de données du service nom des hôtes utilise les paramètres par défaut.

   `vserver services name-service *ns-switch* show -vserver *vs1* -database *hosts*`

   ```
   Vserver: vs1
   Name Service Switch Database: hosts
   Vserver: vs1 Name Service Switch Database: hosts
   Name Service Source Order: files, dns
   ```

2. Effectuez les actions suivantes, si nécessaire.

   a. Ajoutez le service de noms DNS dans la base de données du service de noms d'hôtes dans l'ordre souhaité ou réorganisez les sources.

      Dans cet exemple, la base de données hosts est configurée pour utiliser les fichiers DNS et locaux dans cet ordre.

      `vserver services name-service *ns-switch* modify -vserver *vs1* -database *hosts* -sources *dns,files*`

   b. Vérifiez que la configuration des services de noms est correcte.

      `vserver services name-service *ns-switch* show -vserver *vs1* -database *hosts*`

   ```
   Vserver: vs1
   Name Service Switch Database: hosts
   Name Service Source Order: dns, files
   ```

3. Configurez les services DNS.

   `vserver services name-service dns create -vserver *vs1* -domains *example.com,example2.com* -name-servers *10.0.0.50,10.0.0.51*`

   La commande vserver services name-service dns create effectue une validation automatique de la configuration et signale un message d'erreur si ONTAP n'est pas en mesure de contacter le serveur name.

4. Vérifiez que la configuration DNS est correcte et que le service est activé.

```
Vserver: vs1
Domains: example.com, example2.com Name Servers: 10.0.0.50, 10.0.0.51
Enable/Disable DNS: enabled Timeout (secs): 2
Maximum Attempts: 1
```

5. Valider l'état des serveurs de noms.

   `vserver services name-service dns check -vserver vs1`

```
Vserver  Name Server  Status  Status Details
vs1      10.0.0.50    up      Response time (msec): 2
vs1      10.0.0.51    up      Response time (msec): 2
```

Configuration de DNS dynamique sur le SVM

Si vous souhaitez que le serveur DNS intégré à Active Directory enregistre de manière dynamique les enregistrements DNS d'un serveur NFS ou SMB dans DNS, vous devez configurer le DNS dynamique (DDNS) sur le SVM.

Avant de commencer

Les services de nom DNS doivent être configurés sur le SVM. Si vous utilisez DDNS sécurisé, vous devez utiliser des serveurs de noms DNS intégrés à Active Directory et vous devez avoir créé un serveur NFS ou SMB ou un compte Active Directory pour la SVM.

Description de la tâche

Le nom de domaine complet (FQDN) spécifié doit être unique :

Le nom de domaine complet (FQDN) spécifié doit être unique :

- Pour NFS, valeur spécifiée dans `-vserver-fqdn` dans le cadre du `vserver services name-service dns dynamic-update` La commande devient le FQDN enregistré pour les LIFS.
- Pour SMB, les valeurs spécifiées comme nom NetBIOS du serveur CIFS et nom de domaine complet du serveur CIFS deviennent le FQDN enregistré pour les LIFS. Ceci n'est pas configurable dans ONTAP. Dans le scénario suivant, le FQDN du LIF est « CIFS_VS1.EXAMPLE.COM":

```
cluster1::> cifs server show -vserver vs1

                                          Vserver: vs1
                        CIFS Server NetBIOS Name: CIFS_VS1
                    NetBIOS Domain/Workgroup Name: EXAMPLE
                      Fully Qualified Domain Name: EXAMPLE.COM
                              Organizational Unit: CN=Computers
Default Site Used by LIFs Without Site Membership:
                                   Workgroup Name: -
                                   Kerberos Realm: -
                                Authentication Style: domain
                CIFS Server Administrative Status: up
                          CIFS Server Description:
                          List of NetBIOS Aliases: -
```

Pour éviter un échec de configuration d'un FQDN du SVM qui n'est pas conforme aux règles RFC pour les mises à jour DDNS, utilisez un nom de FQDN qui est conforme à RFC. Pour plus d'informations, voir "RFC 1123".

Étapes

1. Configurer DDNS sur le SVM :

   ```
   vserver services name-service dns dynamic-update modify -vserver vserver_name
   -is- enabled true [-use-secure {true|false} -vserver-fqdn
   FQDN_used_for_DNS_updates
   ```

   ```
   vserver services name-service dns dynamic-update modify -vserver vs1 -is
   -enabled true - use-secure true -vserver-fqdn vs1.example.com
   ```

   Les astérisques ne peuvent pas être utilisés dans le cadre du FQDN personnalisé. Par exemple : `*.netapp.com` n'est pas valide.

2. Vérifiez que la configuration DDNS est correcte :

   ```
   vserver services name-service dns dynamic-update show
   ```

   ```
   Vserver  Is-Enabled Use-Secure Vserver FQDN      TTL
   -------- ---------- ---------- ----------------- -------
   vs1      true       true       vs1.example.com   24h
   ```

Configurez les services DNS dynamiques pour le réseau ONTAP

Si vous souhaitez que le serveur DNS intégré à Active Directory enregistre de manière dynamique les enregistrements DNS d'un serveur NFS ou SMB dans DNS, vous devez configurer le DNS dynamique (DDNS) sur le SVM.

Avant de commencer

Les services de nom DNS doivent être configurés sur le SVM. Si vous utilisez DDNS sécurisé, vous devez utiliser des serveurs de noms DNS intégrés à Active Directory et vous devez avoir créé un serveur NFS ou SMB ou un compte Active Directory pour la SVM.

Description de la tâche

Le FQDN spécifié doit être unique.

> Pour éviter un échec de configuration d'un FQDN du SVM qui n'est pas conforme aux règles RFC pour les mises à jour DDNS, utilisez un nom de FQDN qui est conforme à RFC.

Étapes

1. Configurer DDNS sur le SVM :

   ```
   vserver services name-service dns dynamic-update modify -vserver vserver_name
   -is- enabled true [-use-secure {true|false} -vserver-fqdn
   FQDN_used_for_DNS_updates

   vserver services name-service dns dynamic-update modify -vserver vs1 -is
   -enabled true - use-secure true -vserver-fqdn vs1.example.com
   ```

   Les astérisques ne peuvent pas être utilisés dans le cadre du FQDN personnalisé. Par exemple : `*.netapp.com` n'est pas valide.

2. Vérifiez que la configuration DDNS est correcte :

   ```
   vserver services name-service dns dynamic-update show
   ```

   ```
   Vserver  Is-Enabled Use-Secure Vserver FQDN      TTL
   -------- ---------- ---------- ----------------- -------
   vs1      true       true       vs1.example.com   24h
   ```

Résolution du nom d'hôte

En savoir plus sur la résolution des noms d'hôte pour le réseau ONTAP

ONTAP doit être en mesure de traduire des noms d'hôtes en adresses IP numériques afin de fournir un accès aux clients et d'accéder aux services. Pour résoudre les informations relatives aux hôtes, il est nécessaire de configurer des SVM (Storage Virtual machines) afin d'utiliser des services de noms locaux ou externes. ONTAP prend en charge la configuration d'un serveur DNS externe ou la configuration du fichier hosts local pour la résolution du nom d'hôte.

Lorsque vous utilisez un serveur DNS externe, vous pouvez configurer le DNS dynamique (DDNS), qui envoie automatiquement des informations DNS nouvelles ou modifiées de votre système de stockage au serveur DNS. Sans mises à jour DNS dynamiques, vous devez ajouter manuellement des informations DNS (nom DNS et adresse IP) aux serveurs DNS identifiés lorsqu'un nouveau système est mis en ligne ou lorsqu'une information DNS existante change. Ce processus est lent et sujet aux erreurs. Pendant la reprise sur incident,

la configuration manuelle peut avoir de longs temps d'indisponibilité.

Configurer DNS pour la résolution de nom d'hôte pour le réseau ONTAP

Vous utilisez DNS pour accéder aux sources locales ou distantes pour obtenir des informations sur l'hôte. Vous devez configurer DNS pour accéder à l'une de ces sources, ou aux deux.

ONTAP doit être en mesure de rechercher les informations relatives à l'hôte afin de fournir aux clients un accès approprié. Vous devez configurer les services de noms pour permettre à ONTAP d'accéder aux services DNS locaux ou externes afin d'obtenir les informations sur l'hôte.

ONTAP stocke les informations de configuration du service de noms dans un tableau équivalent à `/etc/nsswitch.conf` Fichier sur les systèmes UNIX.

Configurer un SVM et des LIFs de données pour la résolution de nom d'hôte à l'aide d'un serveur DNS externe

Vous pouvez utiliser le `vserver services name-service dns` Commande permettant d'activer DNS sur un SVM et de le configurer afin d'utiliser DNS pour la résolution de nom d'hôte. Les noms d'hôte sont résolus à l'aide de serveurs DNS externes.

Avant de commencer

Un serveur DNS au niveau du site doit être disponible pour les recherches de noms d'hôte.

Vous devez configurer plusieurs serveurs DNS pour éviter un point de défaillance unique. Le `vserver services name-service dns create` Commande émet un avertissement si vous entrez un seul nom de serveur DNS.

Description de la tâche

Voir Configuration des services DNS dynamiques Pour plus d'informations sur la configuration de DNS dynamique sur le SVM.

Étapes

1. Activer le DNS sur le SVM :

```
vserver services name-service dns create -vserver <vserver_name>
-domains <domain_name> -name-servers <ip_addresses> -state enabled
```

La commande suivante permet d'activer les serveurs DNS externes sur le SVM vs1 :

```
vserver services name-service dns create -vserver vs1.example.com
-domains example.com -name-servers 192.0.2.201,192.0.2.202 -state
enabled
```

> Le `vserver services name-service dns create` Commande effectue une validation automatique de la configuration et signale un message d'erreur si ONTAP ne parvient pas à contacter le serveur de noms.

2. Validez l'état des serveurs de noms à l'aide de la `vserver services name-service dns check` commande.

```
vserver services name-service dns check -vserver vs1.example.com
                                        Name Server
Vserver             Name Server     Status       Status Details
-------------       --------------- ------------
--------------------------
vs1.example.com     10.0.0.50       up           Response time (msec): 2
vs1.example.com     10.0.0.51       up           Response time (msec): 2
```

Pour plus d'informations sur les stratégies de service liées à DNS, reportez-vous à la section "LIF et politiques de services dans ONTAP 9.6 et versions ultérieures".

Configurez la table du commutateur de service de noms pour la résolution du nom d'hôte

Vous devez configurer correctement la table du commutateur de service de noms pour permettre à ONTAP de consulter le service de noms local ou externe afin de récupérer les informations relatives à l'hôte.

Avant de commencer

Vous devez avoir déterminé le service de nom à utiliser pour le mappage des hôtes dans votre environnement.

Étapes

1. Ajoutez les entrées nécessaires à la table de changement de nom du service :

```
vserver services name-service ns-switch modify -vserver <vserver_name>
-database <database_name> -source <source_names>
```

2. Vérifiez que le tableau des commutateurs de service de noms contient les entrées attendues dans l'ordre souhaité :

```
vserver services name-service ns-switch show -vserver <vserver_name>
```

Exemple

L'exemple suivant modifie une entrée dans la table des switchs de service de noms pour SVM vs1 afin d'utiliser d'abord le fichier hosts local, puis un serveur DNS externe pour résoudre les noms d'hôtes :

```
vserver services name-service ns-switch modify -vserver vs1 -database
hosts -sources files,dns
```

Commandes ONTAP pour gérer la table ONTAP hosts

Un administrateur de cluster peut ajouter, modifier, supprimer et afficher les entrées de nom d'hôte dans le tableau hosts de la machine virtuelle de stockage (SVM) admin. Un

administrateur SVM peut configurer les entrées de nom d'hôte uniquement pour la SVM attribuée.

Commandes permettant de gérer les entrées locales de nom d'hôte

Vous pouvez utiliser le `vserver services name-service dns hosts` Commande pour créer, modifier ou supprimer des entrées de table hôte DNS.

Lorsque vous créez ou modifiez les entrées de nom d'hôte DNS, vous pouvez spécifier plusieurs adresses d'alias séparées par des virgules.

Les fonctions que vous recherchez…	Utilisez cette commande…
Créez une entrée de nom d'hôte DNS	`vserver services name-service dns hosts create`
Modifier une entrée de nom d'hôte DNS	`vserver services name-service dns hosts modify`
Supprimer une entrée de nom d'hôte DNS	`vserver services name-service dns hosts delete`

Pour plus d'informations sur les `vserver services name-service dns hosts` commandes, reportez-vous à la section "Référence de commande ONTAP".

Sécurisez votre réseau

Configurez la sécurité réseau ONTAP à l'aide de FIPS pour toutes les connexions SSL

ONTAP est conforme aux normes fédérales de traitement de l'information (FIPS) 140-2 pour toutes les connexions SSL. Vous pouvez activer et désactiver le mode SSL FIPS, définir les protocoles SSL globalement et désactiver les chiffrements faibles dans ONTAP.

Par défaut, SSL sur ONTAP est défini avec la conformité FIPS désactivée et les protocoles TLS suivants activés :

- TLSv1.3 (à partir de ONTAP 9.11.1)
- TLSv1.2

Les protocoles TLS suivants étaient activés par défaut dans les versions précédentes de ONTAP :

- TLSv1.1 (désactivé par défaut à partir de ONTAP 9.12.1)
- TLSv1 (désactivé par défaut à partir de ONTAP 9.8)

Lorsque le mode SSL FIPS est activé, la communication SSL de ONTAP à des clients externes ou des composants de serveur en dehors de ONTAP utilise une fonctionnalité crypto pour SSL conforme à la norme FIPS.

Si vous souhaitez que les comptes d'administrateur accèdent aux SVM avec une clé publique SSH, vous devez vous assurer que l'algorithme de clé hôte est pris en charge avant d'activer le mode SSL FIPS.

Remarque : la prise en charge de l'algorithme de clé hôte a changé dans ONTAP 9.11.1 et versions ultérieures.

Version de ONTAP	Types de clés pris en charge	Types de clés non pris en charge
9.11.1 et versions ultérieures	ecdsa-sha2-nistp256	rsa-sha2-512 rsa-sha2-256 ssh-ed25519 ssh-dss ssh-rsa
9.10.1 et versions antérieures	ecdsa-sha2-nistp256 ssh-ed25519	ssh-dss ssh-rsa

Les comptes de clés publiques SSH existants sans les algorithmes de clé pris en charge doivent être reconfigurés avec un type de clé pris en charge avant l'activation de FIPS, sinon l'authentification de l'administrateur échoue.

Pour plus d'informations, voir "Activez les comptes de clé publique SSH".

ONTAP 9.18.1 introduit la prise en charge des algorithmes cryptographiques post-quantiques ML-KEM, ML-DSA et SLH-DSA pour SSL, offrant une couche de sécurité supplémentaire contre les futures attaques potentielles d'ordinateurs quantiques. Ces algorithmes ne sont disponibles que lorsqueLe système FIPS est désactivé. . Les algorithmes cryptographiques post-quantiques sont négociés lorsque FIPS est désactivé et que le pair les prend en charge.

Activez FIPS

Il est recommandé que tous les utilisateurs sécurisés ajustent leur configuration de sécurité immédiatement après l'installation ou la mise à niveau du système. Lorsque le mode SSL FIPS est activé, la communication SSL de ONTAP à des clients externes ou des composants de serveur en dehors de ONTAP utilise une fonctionnalité crypto pour SSL conforme à la norme FIPS.

Lorsque FIPS est activé, vous ne pouvez ni installer ni créer de certificat avec une clé RSA d'une longueur de 4096.

Étapes

1. Changement au niveau de privilège avancé :

   ```
   set -privilege advanced
   ```

2. Activer FIPS :

   ```
   security config modify * -is-fips-enabled true
   ```

3. Lorsque vous êtes invité à continuer, entrez `y`
4. À partir d' ONTAP 9.9.1, le redémarrage n'est pas nécessaire. Si vous exécutez ONTAP 9.8 ou une version antérieure, redémarrez manuellement chaque nœud du cluster un par un.

Exemple

Si vous exécutez ONTAP 9.9.1 ou une version ultérieure, le message d'avertissement ne s'affiche pas.

```
security config modify -is-fips-enabled true

Warning: This command will enable FIPS compliance and can potentially
cause some non-compliant components to fail. MetroCluster and Vserver DR
require FIPS to be enabled on both sites in order to be compatible.
Do you want to continue? {y|n}: y

Warning: When this command completes, reboot all nodes in the cluster.
This is necessary to prevent components from failing due to an
inconsistent security configuration state in the cluster. To avoid a
service outage, reboot one node at a time and wait for it to completely
initialize before rebooting the next node. Run "security config status
show" command to monitor the reboot status.
Do you want to continue? {y|n}: y
```

Pour en savoir plus sur `security config modify` la configuration du mode SSL FIPS et sur le "Référence de commande ONTAP".

Désactivez FIPS

À partir d' ONTAP 9.18.1, SSL dans ONTAP prend en charge les algorithmes cryptographiques post-quantiques ML-KEM, ML-DSA et SLH-DSA. Ces algorithmes ne sont disponibles que lorsque FIPS est désactivé et que le système homologue les prend en charge.

Étapes

1. Changement au niveau de privilège avancé :

   ```
   set -privilege advanced
   ```

2. Désactiver FIPS en tapant :

   ```
   security config modify -is-fips-enabled false
   ```

3. Lorsque vous êtes invité à continuer, entrez `y`.
4. À partir d' ONTAP 9.9.1, le redémarrage n'est pas nécessaire. Si vous exécutez ONTAP 9.8 ou une version antérieure, redémarrez manuellement chaque nœud du cluster.

Si vous devez utiliser le protocole SSLv3, vous devez désactiver FIPS en suivant la procédure ci-dessus. SSLv3 ne peut être activé que lorsque FIPS est désactivé.

Vous pouvez activer SSLv3 avec la commande suivante. Si vous utilisez ONTAP 9.9.1 ou une version ultérieure, vous ne verrez pas le message d'avertissement.

```
security config modify -supported-protocols SSLv3

Warning: Enabling the SSLv3 protocol may reduce the security of the
interface, and is not recommended.
Do you want to continue? {y|n}: y

Warning: When this command completes, reboot all nodes in the cluster.
This is necessary to prevent components from failing due to an
inconsistent security configuration state in the cluster. To avoid a
service outage, reboot one node at a time and wait for it to completely
initialize before rebooting the next node. Run "security config status
show" command to monitor the reboot status.
Do you want to continue? {y|n}: y
```

Affichez l'état de conformité FIPS

Vous pouvez vérifier si le cluster entier exécute les paramètres de configuration de sécurité actuels.

Étapes

1. Si vous exécutez ONTAP 9.8 ou une version antérieure, redémarrez manuellement chaque nœud du cluster un par un.
2. Afficher le statut de conformité actuel :

   `security config show`

   ```
   cluster1::> security config show
   Cluster    Supported
   FIPS Mode  Protocols Supported Cipher Suites
   ---------- ---------
   ------------------------------------------------------------
   false      TLSv1.3,  TLS_RSA_WITH_AES_128_CCM,
   TLS_RSA_WITH_AES_128_CCM_8,
              TLSv1.2   TLS_RSA_WITH_AES_128_GCM_SHA256,
                        TLS_RSA_WITH_AES_128_CBC_SHA,
                        TLS_RSA_WITH_AES_128_CBC_SHA256,
   TLS_RSA_WITH_AES_256_CCM,
                        TLS_RSA_WITH_AES_256_CCM_8,
                        ...
   ```

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

Informations associées

- "FIPS 203 : Norme relative au mécanisme d'encapsulation de clés basé sur un réseau de modules (ML-KEM)"

- "FIPS 204 : Norme de signature numérique basée sur un réseau de modules (ML-DSA)"
- "FIPS 205 : Norme de signature numérique sans état basée sur le hachage (SLH-DSA)"

Configurer le chiffrement IPsec en vol

Préparez-vous à utiliser la sécurité IP sur le réseau ONTAP

À partir de ONTAP 9.8, vous avez la possibilité d'utiliser la sécurité IP (IPSec) pour protéger votre trafic réseau. IPSec est l'une des nombreuses options de chiffrement de données en mouvement ou à la volée disponibles avec ONTAP. Vous devez vous préparer à configurer IPsec avant de l'utiliser dans un environnement de production.

Mise en œuvre de la sécurité IP dans ONTAP

IPSec est une norme Internet gérée par l'IETF. Il assure le cryptage et l'intégrité des données ainsi que l'authentification du trafic circulant entre les terminaux réseau au niveau IP.

Avec ONTAP, IPSec sécurise l'ensemble du trafic IP entre ONTAP et les différents clients, notamment les protocoles NFS, SMB et iSCSI. En plus de la confidentialité et de l'intégrité des données, le trafic réseau est protégé contre plusieurs attaques, telles que les attaques par réexécution et les attaques de l'homme du milieu. ONTAP utilise l'implémentation du mode de transport IPsec. Il s'appuie sur le protocole Internet Key Exchange (IKE) version 2 pour négocier le matériel clé entre ONTAP et les clients utilisant IPv4 ou IPv6.

Lorsque la fonctionnalité IPSec est activée sur un cluster, le réseau requiert une ou plusieurs entrées de la base de données SPD (Security Policy Database) de ONTAP correspondant aux différentes caractéristiques de trafic. Ces entrées sont mappées aux détails de protection spécifiques nécessaires au traitement et à l'envoi des données (par exemple, suite de chiffrement et méthode d'authentification). Une entrée SPD correspondante est également nécessaire pour chaque client.

Pour certains types de trafic, une autre option de chiffrement des données en mouvement peut être préférable. Par exemple, pour le chiffrement du trafic NetApp SnapMirror et de peering de cluster, le protocole TLS (transport Layer Security) est généralement recommandé à la place d'IPsec. En effet, TLS offre de meilleures performances dans la plupart des situations.

Informations associées

- "Internet Engineering Task Force"
- "RFC 4301 : Architecture de sécurité pour le protocole Internet"

Évolution de l'implémentation ONTAP IPsec

IPsec a été introduit pour la première fois avec ONTAP 9.8. Son implémentation a continué d'évoluer dans les versions ultérieures ONTAP , comme décrit ci-dessous.

ONTAP 9.18.1

La prise en charge du déchargement matériel IPsec est étendue au trafic IPv6.

ONTAP 9.17.1

La prise en charge du déchargement matériel IPsec est étendue à "groupes d'agrégation de liens" . "Clés pré-partagées postquantiques (PPK)" sont pris en charge pour l'authentification par clés pré-partagées IPsec (PSK).

ONTAP 9.16.1

Plusieurs opérations cryptographiques, telles que le cryptage et les contrôles d'intégrité, peuvent être déchargées sur une carte NIC prise en charge. Voir Fonctionnalité de déchargement matériel IPsec pour plus d'informations.

ONTAP 9.12.1

La prise en charge du protocole hôte IPSec frontal est disponible dans les configurations MetroCluster IP et MetroCluster FAS. La prise en charge IPsec fournie avec les clusters MetroCluster est limitée au trafic hôte frontal et n'est pas prise en charge sur les LIF intercluster MetroCluster.

ONTAP 9.10.1

Les certificats peuvent être utilisés pour l'authentification IPsec en plus des clés PSK. Avant ONTAP 9.10.1, seules les clés PSK étaient prises en charge pour l'authentification.

ONTAP 9.9.1

Les algorithmes de chiffrement utilisés par IPsec sont validés par la norme FIPS 140-2-2. Ces algorithmes sont traités par le module cryptographique NetApp de ONTAP, qui est certifié FIPS 140-2-2.

ONTAP 9.8

La prise en charge d'IPsec devient initialement disponible en fonction de l'implémentation du mode de transport.

Fonctionnalité de déchargement matériel IPsec

Si vous utilisez ONTAP 9.16.1 ou une version ultérieure, vous avez la possibilité de transférer certaines opérations à forte intensité de calcul, telles que le cryptage et les contrôles d'intégrité, vers une carte de contrôleur d'interface réseau (NIC) installée sur le nœud de stockage. Le débit pour les opérations déchargées sur la carte NIC est d'environ 5 % ou moins. Cela peut considérablement améliorer les performances et le débit du trafic réseau protégé par IPsec.

Exigences et recommandations

Vous devez tenir compte de plusieurs exigences avant d'utiliser la fonction de déchargement matériel IPsec.

Cartes Ethernet prises en charge

Vous devez installer et utiliser uniquement des cartes Ethernet compatibles. Les cartes Ethernet suivantes sont prises en charge à partir d' ONTAP 9.16.1 :

- X50131A (contrôleur Ethernet 2p, 40G/100G/200G/400G)
- X60132A (contrôleur Ethernet 4p, 10G/25G)

ONTAP 9.17.1 ajoute la prise en charge des cartes Ethernet suivantes :

- X50135A (contrôleur Ethernet 2p, 40G/100G)
- X60135A (contrôleur Ethernet 2p, 40G/100G)

Les cartes X50131A et X50135A sont prises en charge sur les plates-formes suivantes :

- ASA A1K
- ASA A90
- ASA A70
- AFF A1K

- AFF A90
- AFF A70

Les cartes X60132A et X60135A sont prises en charge sur les plates-formes suivantes :

- ASA A50
- ASA A30
- ASA A20
- AFF A50
- AFF A30
- AFF A20

Voir le "NetApp Hardware Universe" pour plus d'informations sur les plateformes et cartes prises en charge.

Étendue du cluster

La fonction de déchargement matériel IPSec est configurée globalement pour le cluster. Et ainsi, par exemple, la commande `security ipsec config` s'applique à tous les nœuds du cluster.

Configuration cohérente

Les cartes NIC prises en charge doivent être installées sur tous les nœuds du cluster. Si une carte NIC prise en charge n'est disponible que sur certains nœuds, vous pouvez constater une dégradation importante des performances après un basculement si certaines LIF ne sont pas hébergées sur une carte réseau prenant en charge le déchargement.

Désactiver l'anti-relecture

Vous devez désactiver la protection anti-relecture IPSec sur ONTAP (configuration par défaut) et les clients IPsec. Si elle n'est pas désactivée, la fragmentation et le multi-chemin (route redondante) ne sont pas pris en charge.

Si la configuration IPSec de ONTAP a été modifiée par défaut pour activer la protection anti-replay, utilisez cette commande pour la désactiver :

```
security ipsec config modify -replay-window 0
```

Vous devez vous assurer que la protection anti-relecture IPSec est désactivée sur votre client. Reportez-vous à la documentation IPsec de votre client pour désactiver la protection anti-replay.

Limites

Vous devez tenir compte de plusieurs limitations avant d'utiliser la fonction de déchargement matériel IPsec.

IPv6

À partir d' ONTAP 9.18.1, IPv6 est pris en charge pour la fonction de déchargement matériel IPsec. Avant ONTAP 9.18.1, le déchargement matériel IPsec ne prend pas en charge IPv6.

Numéros de séquence étendus

Les numéros de séquence étendus IPsec ne sont pas pris en charge avec la fonction de déchargement matériel. Seuls les numéros de séquence 32 bits normaux sont utilisés.

Agrégation de liens

À partir d' ONTAP 9.17.1, vous pouvez utiliser la fonction de déchargement matériel IPsec avec un "groupe d'agrégation de liens" .

Avant la version 9.17.1, la fonctionnalité de déchargement matériel IPsec ne prenait pas en charge l'agrégation de liens. Elle ne pouvait pas être utilisée avec une interface ou un groupe d'agrégation de liens administrés via le `network port ifgrp` commandes sur l'interface CLI ONTAP .

Prise en charge de la configuration dans l'interface de ligne de commandes ONTAP

Trois commandes CLI existantes sont mises à jour dans ONTAP 9.16.1 pour prendre en charge la fonctionnalité de déchargement matériel IPSec comme décrit ci-dessous. Voir également "Configurer la sécurité IP dans ONTAP"pour plus d'informations.

Commande ONTAP	Mise à jour
`security ipsec config show`	Le paramètre booléen `Offload Enabled` indique l'état actuel du déchargement de la carte réseau.
`security ipsec config modify`	Le paramètre `is-offload-enabled` peut être utilisé pour activer ou désactiver la fonction de déchargement de carte réseau.
`security ipsec config show-ipsecsa`	Quatre nouveaux compteurs ont été ajoutés pour afficher le trafic entrant et sortant en octets et en paquets.

Prise en charge de la configuration dans l'API REST ONTAP

Deux terminaux d'API REST existants sont mis à jour dans ONTAP 9.16.1 pour prendre en charge la fonctionnalité de déchargement matériel IPSec, comme décrit ci-dessous.

Terminal REST	Mise à jour
`/api/security/ipsec`	Le paramètre `offload_enabled` a été ajouté et est disponible avec la méthode PATCH.
`/api/security/ipsec/security_association`	Deux nouvelles valeurs de compteur ont été ajoutées pour suivre le nombre total d'octets et de paquets traités par la fonction de déchargement.

Pour en savoir plus sur l'API REST ONTAP, y compris "Nouveautés de l'API REST ONTAP", consultez la documentation sur l'automatisation ONTAP. Vous devez également consulter la documentation sur l'automatisation ONTAP pour plus de détails sur "Noeuds finaux IPsec".

Informations associées

- "sécurité ipsec"

Configurer la sécurité IP pour le réseau ONTAP

Plusieurs tâches sont nécessaires pour configurer et activer le chiffrement à la volée IPsec sur votre cluster ONTAP.

Vérifiez "Préparez-vous à utiliser la sécurité IP" avant de configurer IPsec. Par exemple, vous devrez peut-être décider d'utiliser la fonction de déchargement matériel IPSec disponible à partir de ONTAP 9.16.1.

Activez IPsec sur le cluster

Vous pouvez activer IPsec sur le cluster pour vous assurer que les données sont chiffrées en continu et sécurisées pendant le transit.

Étapes

1. Découvrez si IPSec est déjà activé :

   ```
   security ipsec config show
   ```

   Si le résultat inclut `IPsec Enabled: false`, passez à l'étape suivante.

2. Activer IPsec :

   ```
   security ipsec config modify -is-enabled true
   ```

   Vous pouvez activer la fonction de déchargement matériel IPsec à l'aide du paramètre booléen `is-offload-enabled`.

3. Exécutez à nouveau la commande de découverte :

   ```
   security ipsec config show
   ```

   Le résultat inclut maintenant `IPsec Enabled: true`.

Préparez la création de stratégies IPsec avec l'authentification par certificat

Vous pouvez ignorer cette étape si vous utilisez uniquement des clés prépartagées (PSK) pour l'authentification et que vous n'utilisez pas l'authentification par certificat.

Avant de créer une stratégie IPSec qui utilise des certificats pour l'authentification, vous devez vérifier que les conditions préalables suivantes sont remplies :

- ONTAP et le client doivent avoir installé le certificat CA de l'autre partie afin que les certificats de l'entité finale (ONTAP ou le client) soient vérifiables des deux côtés
- Un certificat est installé pour la LIF de ONTAP qui participe à la politique

Les LIF ONTAP peuvent partager des certificats. Un mappage un-à-un entre les certificats et les LIFs n'est pas nécessaire.

Étapes

1. Installez tous les certificats de l'autorité de certification utilisés lors de l'authentification mutuelle, y compris les autorités de certification côté ONTAP et côté client, dans la gestion des certificats ONTAP, sauf s'il est déjà installé (comme c'est le cas pour une autorité de certification racine auto-signée ONTAP).

   Commande exemple

   ```
   cluster::> security certificate install -vserver svm_name -type server-ca
   -cert-name my_ca_cert
   ```

2. Pour vous assurer que l'autorité de certification installée se trouve dans le chemin de recherche de l'autorité de certification IPSec lors de l'authentification, ajoutez les autorités de certification de gestion de certificat ONTAP au module IPSec à l'aide du `security ipsec ca-certificate add` commande.

   Commande exemple
   ```
   cluster::> security ipsec ca-certificate add -vserver svm_name -ca-certs
   my_ca_cert
   ```

3. Créez et installez un certificat pour une utilisation par le LIF ONTAP. L'autorité de certification de l'émetteur de ce certificat doit déjà être installée sur ONTAP et ajoutée à IPsec.

   Commande exemple
   ```
   cluster::> security certificate install -vserver svm_name -type server -cert
   -name my_nfs_server_cert
   ```

Pour plus d'informations sur les certificats dans ONTAP, consultez les commandes de certificat de sécurité dans la documentation de ONTAP 9.

Définir la base de données de règles de sécurité (SPD)

IPSec requiert une entrée SPD avant d'autoriser le trafic à circuler sur le réseau. Ceci est vrai si vous utilisez un PSK ou un certificat pour l'authentification.

Étapes

1. Utilisez le `security ipsec policy create` commande pour :
   a. Sélectionnez l'adresse IP ONTAP ou le sous-réseau d'adresses IP pour participer au transport IPsec.
   b. Sélectionnez les adresses IP des clients qui se connectent aux adresses IP ONTAP.

      Le client doit prendre en charge Internet Key Exchange version 2 (IKEv2) avec une clé pré-partagée (PSK).

   c. Vous pouvez également sélectionner des paramètres de trafic précis, tels que les protocoles de couche supérieure (UDP, TCP, ICMP, etc.), les numéros de port locaux et les numéros de port distants pour protéger le trafic. Les paramètres correspondants sont : `protocols` , `local-ports` et `remote-ports` respectivement.

      Ignorez cette étape pour protéger tout le trafic entre l'adresse IP ONTAP et l'adresse IP du client. La protection de tout le trafic est la valeur par défaut.

   d. Entrez PSK ou PKI (public-Key Infrastructure) pour le `auth-method` paramètre de la méthode d'authentification souhaitée.
      i. Si vous entrez une clé PSK, incluez les paramètres, puis appuyez sur <enter> pour que l'invite vous demande d'entrer et de vérifier la clé pré-partagée.

         Les `local-identity` paramètres et `remote-identity` sont facultatifs si l'hôte et le client utilisent StrongSwan et qu'aucune règle générique n'est sélectionnée pour l'hôte ou le client.

      ii. Si vous entrez une PKI, vous devez également entrer `cert-name`, `local-identity`, `remote-identity` paramètres. Si l'identité du certificat côté distant est inconnue ou si plusieurs identités client sont attendues, entrez l'identité spéciale `ANYTHING`.

e. À partir d' ONTAP 9.17.1, vous pouvez éventuellement saisir une identité de clé pré-partagée postquantique (PPK) avec le `ppk-identity` Paramètre. Les PPK offrent une couche de sécurité supplémentaire contre d'éventuelles attaques futures par ordinateur quantique. Lorsque vous saisissez une identité PPK, vous êtes invité à saisir son secret. Les PPK ne sont pris en charge que pour l'authentification PSK.

En savoir plus sur `security ipsec policy create` dans le "Référence de commande ONTAP" .

```
security ipsec policy create -vserver vs1 -name test34 -local-ip-subnets
192.168.134.34/32 -remote-ip-subnets 192.168.134.44/32
Enter the preshared key for IPsec Policy _test34_ on Vserver _vs1_:
```

```
security ipsec policy create -vserver vs1 -name test34 -local-ip-subnets
192.168.134.34/32 -remote-ip-subnets 192.168.134.44/32 -local-ports 2049
-protocols tcp -auth-method PKI -cert-name my_nfs_server_cert -local
-identity CN=netapp.ipsec.lif1.vs0 -remote-identity ANYTHING
```

Le trafic IP ne peut pas circuler entre le client et le serveur tant que ONTAP et le client n'ont pas configuré les stratégies IPSec correspondantes et que les informations d'identification d'authentification (PSK ou certificat) ne sont pas en place des deux côtés.

Utiliser les identités IPsec

Pour la méthode d'authentification par clé pré-partagée, les identités locales et distantes sont facultatives si l'hôte et le client utilisent StrongSwan et qu'aucune règle générique n'est sélectionnée pour l'hôte ou le client.

Pour la méthode d'authentification PKI/certificat, les identités locales et distantes sont obligatoires. Les identités spécifient quelle identité est certifiée dans le certificat de chaque côté et sont utilisées dans le processus de vérification. Si l'identité distante est inconnue ou si elle peut être de nombreuses identités différentes, utilisez l'identité spéciale `ANYTHING`.

Description de la tâche

Au sein de ONTAP, les identités sont spécifiées en modifiant l'entrée du démon du processeur de service ou pendant sa création. Le démon du processeur de service peut être un nom d'identité avec une adresse IP ou un format de chaîne.

Étapes

1. Utiliser la commande suivante pour modifier un paramètre d'identité SPD existant :

```
security ipsec policy modify
```

Commande exemple

```
security ipsec policy modify -vserver vs1 -name test34 -local-identity
192.168.134.34 -remote-identity client.fooboo.com
```

Configuration client multiple IPsec

Lorsqu'un petit nombre de clients doivent utiliser IPsec, l'utilisation d'une seule entrée SPD pour chaque client est suffisante. Toutefois, lorsque des centaines voire des milliers de clients doivent utiliser IPsec, NetApp

recommande l'utilisation d'une configuration client multiple IPsec.

Description de la tâche

ONTAP prend en charge la connexion de plusieurs clients sur de nombreux réseaux à une seule adresse IP de SVM avec IPsec activé. Vous pouvez effectuer cette opération en utilisant l'une des méthodes suivantes :

- **Configuration du sous-réseau**

  Pour permettre à tous les clients d'un sous-réseau particulier (192.168.134.0/24 par exemple) de se connecter à une seule adresse IP de SVM à l'aide d'une seule entrée de la politique SPD, vous devez spécifier le `remote-ip-subnets` sous-réseau. De plus, vous devez spécifier le `remote-identity` champ avec l'identité côté client correcte.

  > Lors de l'utilisation d'une seule entrée de stratégie dans une configuration de sous-réseau, les clients IPsec de ce sous-réseau partagent l'identité IPsec et la clé pré-partagée (PSK). Cependant, ceci n'est pas vrai avec l'authentification par certificat. Lors de l'utilisation de certificats, chaque client peut utiliser son propre certificat unique ou un certificat partagé pour s'authentifier. ONTAP IPSec vérifie la validité du certificat en fonction des autorités de certification installées dans son magasin de confiance local. ONTAP prend également en charge la vérification de la liste de révocation de certificats (CRL).

- **Autoriser la configuration de tous les clients**

  Pour permettre à n'importe quel client, quelle que soit son adresse IP source, de se connecter à l'adresse IP du SVM IPsec, utilisez l' `0.0.0.0/0` caractère générique lors de la spécification du `remote-ip-subnets` légale.

  De plus, vous devez spécifier le `remote-identity` champ avec l'identité côté client correcte. Pour l'authentification par certificat, vous pouvez entrer `ANYTHING`.

  Aussi, lorsque le `0.0.0.0/0` le caractère générique est utilisé. vous devez configurer un numéro de port local ou distant spécifique à utiliser. Par exemple : `NFS port 2049`.

  Étapes

  a. Utilisez l'une des commandes suivantes pour configurer IPsec pour plusieurs clients.

     i. Si vous utilisez **subnet configuration** pour prendre en charge plusieurs clients IPsec :

     ```
     security ipsec policy create -vserver vserver_name -name policy_name
     -local-ip-subnets IPsec_IP_address/32 -remote-ip-subnets
     IP_address/subnet -local-identity local_id -remote-identity remote_id
     ```

     Commande exemple

     ```
     security ipsec policy create -vserver vs1 -name subnet134 -local-ip-subnets
     192.168.134.34/32 -remote-ip-subnets 192.168.134.0/24 -local-identity
     ontap_side_identity -remote-identity client_side_identity
     ```

     i. Si vous utilisez **Autoriser la configuration de tous les clients** à prendre en charge plusieurs clients IPsec :

     ```
     security ipsec policy create -vserver vserver_name -name policy_name
     -local-ip-subnets IPsec_IP_address/32 -remote-ip-subnets 0.0.0.0/0 -local
     ```

```
-ports port_number -local-identity local_id -remote-identity remote_id
```

Commande exemple

```
security ipsec policy create -vserver vs1 -name test35 -local-ip-subnets
IPsec_IP_address/32 -remote-ip-subnets 0.0.0.0/0 -local-ports 2049 -local
-identity ontap_side_identity -remote-identity client_side_identity
```

Afficher les statistiques IPsec

Lors de la négociation, un canal de sécurité appelé Association de sécurité IKE (sa) peut être établi entre l'adresse IP du SVM ONTAP et l'adresse IP du client. IPSec SAS est installé sur les deux noeuds finaux pour effectuer le cryptage et le décryptage des données. Vous pouvez utiliser les commandes de statistiques pour vérifier l'état des ports SAS IPsec et SAS IKE.

Si vous utilisez la fonction de déchargement matériel IPSec, plusieurs nouveaux compteurs sont affichés avec la commande `security ipsec config show-ipsecsa`.

Exemples de commandes

IKE sa exemple de commande :

```
security ipsec show-ikesa -node hosting_node_name_for_svm_ip
```

Exemple de commande et de sortie IPsec sa :

```
security ipsec show-ipsecsa -node hosting_node_name_for_svm_ip
```

```
cluster1::> security ipsec show-ikesa -node cluster1-node1
            Policy Local           Remote
Vserver     Name   Address         Address         Initator-SPI     State
----------- ------ --------------- --------------- ----------------
-----------
vs1         test34
                   192.168.134.34  192.168.134.44  c764f9ee020cec69
ESTABLISHED
```

Exemple de commande et de sortie IPsec sa :

```
security ipsec show-ipsecsa -node hosting_node_name_for_svm_ip

cluster1::> security ipsec show-ipsecsa -node cluster1-node1
            Policy  Local           Remote          Inbound  Outbound
Vserver     Name    Address         Address         SPI      SPI
State
----------- ------- --------------- --------------- -------- --------
---------
vs1         test34
                    192.168.134.34  192.168.134.44  c4c5b3d6 c2515559
INSTALLED
```

Informations associées

- "installation du certificat de sécurité"
- "sécurité ipsec"

Configurer le chiffrement du réseau du cluster backend ONTAP

À partir d' ONTAP 9.18.1, vous pouvez configurer le chiffrement TLS (Transport Layer Security) pour les données en transit sur le réseau du cluster backend. Ce chiffrement protège les données client stockées dans ONTAP lors de leur transmission entre les nœuds ONTAP du réseau du cluster dorsal.

Description de la tâche

- Le chiffrement du réseau du cluster backend est désactivé par défaut.
- Lorsque le chiffrement du réseau du cluster backend est activé, toutes les données client stockées dans ONTAP sont chiffrées lors de leur transmission entre les nœuds ONTAP sur le réseau du cluster backend. Certains flux de trafic réseau du cluster, tels que les données du chemin de contrôle, ne sont pas chiffrés.
- Par défaut, le chiffrement du réseau du cluster backend utilisera des certificats générés automatiquement pour chaque nœud du cluster. Tu peuxGérer les certificats de chiffrement du réseau du cluster sur chaque nœud pour utiliser un certificat installé personnalisé.

Avant de commencer

- Vous devez être administrateur ONTAP au niveau `admin` niveau de privilège permettant d'effectuer les tâches suivantes.
- Tous les nœuds du cluster doivent exécuter ONTAP 9.18.1 ou une version ultérieure pour activer le chiffrement du réseau du cluster backend.

Activer ou désactiver le chiffrement pour la communication réseau du cluster

Étapes

1. Afficher l'état actuel du chiffrement du réseau du cluster :

```
security cluster-network show
```

Cette commande affiche l'état actuel du chiffrement du réseau du cluster :

```
Cluster-1::*> security cluster-network show

Enabled: true

Mode: tls

Status: READY
```

2. Activer ou désactiver le chiffrement du réseau du cluster backend TLS :

```
security cluster-network modify -enabled <true|false>
```

Cette commande active ou désactive la communication chiffrée des données client en transit sur le réseau du cluster backend.

Gérer les certificats de chiffrement du réseau du cluster

1. Consultez les informations actuelles du certificat de chiffrement du réseau du cluster :

```
security cluster-network certificate show
```

Cette commande affiche les informations actuelles du certificat de chiffrement du réseau du cluster :

```
security cluster-network certificate show
Node                  Certificate Name                    CA
--------------------- ----------------------------------
--------------
node1                 -                                   Cluster-
1_Root_CA
node2                 -                                   Cluster-
1_Root_CA
node3                 google_issued_cert1                 Google_CA1
node4                 google_issued_cert2                 Google_CA1
```

Le nom du certificat et de l'autorité de certification (CA) est affiché pour chaque nœud du cluster.

2. Modifier le certificat de chiffrement du réseau du cluster pour un nœud :

```
security cluster-network certificate modify -node <node_name> -name
<certificate_name>
```

Cette commande modifie le certificat de chiffrement du réseau du cluster pour un nœud spécifique. Le certificat doit être installé et signé par une autorité de certification installée avant l'exécution de cette commande. Pour plus d'informations sur la gestion des certificats, veuillez consulter"Gestion des certificats ONTAP avec System Manager" . Si `-name` Si aucun certificat n'est spécifié, le certificat par défaut généré automatiquement est utilisé.

Configuration des politiques de pare-feu pour les LIF du réseau ONTAP

La configuration d'un pare-feu améliore la sécurité du cluster et permet d'empêcher tout accès non autorisé au système de stockage. Par défaut, le pare-feu intégré est configuré pour autoriser l'accès à distance à un ensemble spécifique de services IP pour les données, la gestion et les LIF intercluster.

À partir d'ONTAP 9.10.1 :

- Les politiques de pare-feu sont obsolètes et sont remplacées par les politiques de service LIF. Auparavant, le pare-feu intégré était géré à l'aide de politiques de pare-feu. Cette fonctionnalité s'effectue désormais à l'aide d'une politique de service LIF.
- Toutes les politiques de pare-feu sont vides et n'ouvrent aucun port dans le pare-feu sous-jacent. En revanche, tous les ports doivent être ouverts via une règle de service LIF.
- Aucune action n'est requise après une mise à niveau vers la version 9.10.1 ou ultérieure afin de passer des politiques de pare-feu aux politiques de service LIF. Le système construit automatiquement des politiques de service LIF conformes aux politiques de pare-feu utilisées dans la version précédente de ONTAP. Si vous utilisez des scripts ou d'autres outils qui créent et gèrent des politiques de pare-feu personnalisées, vous devrez peut-être mettre à niveau ces scripts pour créer des stratégies de service personnalisées.

Pour en savoir plus, voir "LIF et politiques de services dans ONTAP 9.6 et versions ultérieures".

Les politiques de pare-feu peuvent être utilisées pour contrôler l'accès aux protocoles de service de gestion tels que SSH, HTTP, HTTPS, Telnet, NTP, NDMP, NDMPS, RSH, DNS OU SNMP. Les politiques de pare-feu ne peuvent pas être définies pour des protocoles de données tels que NFS ou SMB.

Vous pouvez gérer le service et les politiques de pare-feu des manières suivantes :

- Activation ou désactivation du service de pare-feu
- Affichage de la configuration actuelle du service de pare-feu
- Création d'une nouvelle politique de pare-feu avec le nom de la politique et les services réseau spécifiés
- Application d'une politique de pare-feu à une interface logique
- Création d'une nouvelle politique de pare-feu qui est une copie exacte d'une politique existante

  Vous pouvez l'utiliser pour créer une politique avec des caractéristiques similaires au sein d'une même SVM ou pour copier la politique dans une autre SVM.

- Affichage d'informations sur les politiques de pare-feu
- Modification des adresses IP et des masques de réseau utilisés par une politique de pare-feu
- Suppression d'une politique de pare-feu qui n'est pas utilisée par une LIF

Politiques de pare-feu et LIF

Les politiques de pare-feu de LIF sont utilisées pour restreindre l'accès au cluster sur chaque LIF. Vous devez comprendre comment la politique de pare-feu par défaut affecte l'accès au système sur chaque type de LIF, et comment personnaliser une politique de pare-feu pour augmenter ou diminuer la sécurité par rapport à une LIF.

Lors de la configuration d'une LIF à l'aide de la `network interface create` commande ou `network interface modify`, la valeur spécifiée pour le `-firewall-policy` paramètre détermine les protocoles de service et les adresses IP qui sont autorisés à accéder à la LIF. Pour en savoir plus, `network interface` consultez le "Référence de commande ONTAP".

Dans de nombreux cas, vous pouvez accepter la valeur de la stratégie de pare-feu par défaut. Dans d'autres cas, vous devrez peut-être restreindre l'accès à certaines adresses IP et à certains protocoles de service de gestion. Les protocoles de service de gestion disponibles sont : SSH, HTTP, HTTPS, Telnet, NTP, NDMP, NDMPS, RSH, DNS ET SNMP.

La politique de pare-feu de toutes les LIFs de cluster est par défaut définie sur `""` et ne peut pas être modifié.

Le tableau ci-dessous décrit les politiques de pare-feu par défaut qui sont attribuées à chaque LIF, en fonction de leur rôle (ONTAP 9.5 et versions antérieures) ou de la politique de service (ONTAP 9.6 et versions ultérieures) lors de la création de cette LIF :

Politique de pare-feu	Protocoles de service par défaut	Accès par défaut	LIFs appliquées à
gstn	dns, http, https, ndmp, ndmps, ntp, snmp, ssh	Toute adresse (0.0.0.0/0)	Gestion du cluster, gestion SVM et LIF de node-management
gestion-nfs	dns, http, https, ndmp, ndmps, ntp, portmap, snmp, ssh	Toute adresse (0.0.0.0/0)	LIF de données qui prennent également en charge l'accès à la gestion des SVMs
intercluster	https, ndmp, ndmps	Toute adresse (0.0.0.0/0)	Toutes les LIFs intercluster
les données	dns, ndmp, ndmps, portmap	Toute adresse (0.0.0.0/0)	Toutes les LIF de données

Configuration du service portmap

Le service portmap mappe les services RPC aux ports sur lesquels ils écoutent.

Le service portmap était toujours accessible à ONTAP 9.3 et versions antérieures, est devenu configurable dans ONTAP 9.4 à ONTAP 9.6 et est géré automatiquement à partir de ONTAP 9.7.

- Dans ONTAP 9.3 et versions antérieures, le service portmap (rpcbind) était toujours accessible sur le port 111 dans les configurations réseau qui s'appuyaient sur le pare-feu ONTAP intégré plutôt qu'un pare-feu tiers.
- De ONTAP 9.4 à ONTAP 9.6, vous pouvez modifier les politiques de pare-feu pour contrôler si le service

portmap est accessible sur des LIF spécifiques.

- Depuis ONTAP 9.7, le service de pare-feu de portmap est supprimé. En revanche, le port portmap est ouvert automatiquement pour toutes les LIF qui prennent en charge le service NFS.

Le service portmap est configurable dans le pare-feu de ONTAP 9.4 à ONTAP 9.6.

Le reste de cette rubrique explique comment configurer le service de pare-feu portmap pour ONTAP 9.4 à ONTAP 9.6.

En fonction de votre configuration, vous pouvez disautoriser l'accès au service sur des types spécifiques de LIF, généralement les LIF intercluster et de gestion. Dans certains cas, vous pourriez même refuser l'accès aux LIF de données.

Quel comportement pouvez-vous attendre

Les ONTAP 9.4 à ONTAP 9.6 Behavior ont été conçus pour offrir une transition transparente lors de la mise à niveau. Si le service portmap est déjà accessible sur des types spécifiques de LIF, il sera toujours accessible sur ces types de LIF. Comme dans ONTAP 9.3 et versions antérieures, vous pouvez spécifier les services accessibles à l'intérieur du pare-feu dans la politique de pare-feu pour le type de LIF.

Pour que le comportement soit effectif, tous les nœuds du cluster doivent exécuter ONTAP 9.4 à ONTAP 9.6. Seul le trafic entrant est affecté.

Les nouvelles règles sont les suivantes :

- Lors de la mise à niveau vers les versions 9.4 à 9.6, ONTAP ajoute le service portmap à toutes les politiques de pare-feu existantes, par défaut ou personnalisées.
- Lorsque vous créez un cluster ou un nouvel IPspace, ONTAP ajoute le service portmap uniquement à la politique de données par défaut, et non aux politiques de gestion par défaut ou intercluster.
- Vous pouvez ajouter le service portmap aux règles par défaut ou personnalisées selon vos besoins, puis supprimer le service selon vos besoins.

Comment ajouter ou supprimer le service portmap

Pour ajouter le service de mappage de port à une SVM ou à une politique de pare-feu de cluster (le rendre accessible via le pare-feu), entrez :

```
system services firewall policy create -vserver SVM -policy
mgmt|intercluster|data|custom -service portmap
```

Pour supprimer le service portmap d'une SVM ou d'une politique de pare-feu de cluster (celle-ci doit être inaccessible au sein du pare-feu), entrez :

```
system services firewall policy delete -vserver SVM -policy
mgmt|intercluster|data|custom -service portmap
```

Vous pouvez utiliser la commande network interface modify pour appliquer la politique de pare-feu à une LIF existante. Pour en savoir plus sur les commandes décrites dans cette procédure"Référence de commande ONTAP", reportez-vous à la .

Créer une politique de pare-feu et l'affecter à une LIF

Des politiques de pare-feu par défaut sont attribuées à chaque LIF lorsque vous créez la LIF. Dans de nombreux cas, les paramètres par défaut du pare-feu fonctionnent bien et vous n'avez pas besoin de les modifier. Si vous souhaitez modifier les services réseau ou les adresses IP pouvant accéder à une LIF, vous

pouvez créer une politique de pare-feu personnalisée et l'affecter à la LIF.

Description de la tâche

- Vous ne pouvez pas créer de politique de pare-feu avec `policy` nom `data`, `intercluster`, `cluster`, ou `mgmt`.

  Ces valeurs sont réservées aux politiques de pare-feu définies par le système.

- Vous ne pouvez ni définir ni modifier une politique de pare-feu pour les LIFs de cluster.

  La politique de pare-feu des LIFs de cluster est définie sur 0.0.0.0/0 pour tous les types de services.

- Si vous avez besoin de supprimer un service d'une politique, vous devez supprimer la politique de pare-feu existante et en créer une nouvelle.
- Si IPv6 est activé sur le cluster, vous pouvez créer des politiques de pare-feu avec des adresses IPv6.

  Une fois IPv6 activé, `data`, `intercluster`, et `mgmt` Les politiques de pare-feu incluent ::/0, le caractère générique IPv6, dans leur liste d'adresses acceptées.

- Lorsque vous utilisez System Manager pour configurer la fonctionnalité de protection des données sur les clusters, vous devez vous assurer que les adresses IP LIF intercluster sont incluses dans la liste des autorisés et que le service HTTPS est autorisé sur les LIF intercluster et sur les pare-feu de votre entreprise.

  Par défaut, le `intercluster` La politique de pare-feu permet l'accès à partir de toutes les adresses IP (0.0.0.0/0, ou ::/0 pour IPv6) et active les services HTTPS, NDMP et NDMPS. Si vous modifiez cette politique par défaut ou si vous créez votre propre politique de pare-feu pour les LIF intercluster, vous devez ajouter chaque adresse IP LIF intercluster à la liste des autorisés et activer le service HTTPS.

- Depuis ONTAP 9.6, les services de pare-feu HTTPS et SSH ne sont pas pris en charge.

  Dans ONTAP 9.6, le `management-https` et `management-ssh` Les services LIF sont disponibles pour l'accès à la gestion HTTPS et SSH.

Étapes

1. Créer une politique de pare-feu qui sera disponible pour les LIF sur un SVM spécifique :

   `system services firewall policy create -vserver` *`vserver_name`* `-policy` *`policy_name`* `-service` *`network_service`* `-allow-list` *`ip_address/mask`*

   Vous pouvez utiliser cette commande plusieurs fois pour ajouter plusieurs services réseau et une liste d'adresses IP autorisées pour chaque service de la politique de pare-feu.

2. Vérifiez que la stratégie a été correctement ajoutée en utilisant le `system services firewall policy show` commande.
3. Appliquer la politique de pare-feu à une LIF :

   `network interface modify -vserver` *`vserver_name`* `-lif` *`lif_name`* `-firewall-policy` *`policy_name`*

4. Vérifier que la policy a été correctement ajoutée à la LIF à l'aide de l' `network interface show -fields firewall-policy` commande.

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

Exemple de création d'une politique de pare-feu et de son assignation à une LIF

La commande suivante crée une politique de pare-feu nommée Data_http qui active l'accès au protocole HTTP et HTTPS à partir des adresses IP sur le sous-réseau 10.10, applique cette politique à la LIF nommée data1 sur le SVM vs1, puis affiche toutes les politiques de pare-feu sur le cluster :

```
system services firewall policy create -vserver vs1 -policy data_http
-service http - allow-list 10.10.0.0/16
```

```
system services firewall policy show

Vserver Policy       Service    Allowed
------- ------------ ---------- -------------------
cluster-1
        data
                     dns        0.0.0.0/0
                     ndmp       0.0.0.0/0
                     ndmps      0.0.0.0/0
cluster-1
        intercluster
                     https      0.0.0.0/0
                     ndmp       0.0.0.0/0
                     ndmps      0.0.0.0/0
cluster-1
        mgmt
                     dns        0.0.0.0/0
                     http       0.0.0.0/0
                     https      0.0.0.0/0
                     ndmp       0.0.0.0/0
                     ndmps      0.0.0.0/0
                     ntp        0.0.0.0/0
                     snmp       0.0.0.0/0
                     ssh        0.0.0.0/0
vs1
        data_http
                     http       10.10.0.0/16
                     https      10.10.0.0/16

network interface modify -vserver vs1 -lif data1 -firewall-policy
data_http

network interface show -fields firewall-policy

vserver  lif                  firewall-policy
-------  -------------------- ---------------
Cluster  node1_clus_1
Cluster  node1_clus_2
Cluster  node2_clus_1
Cluster  node2_clus_2
cluster-1 cluster_mgmt         mgmt
cluster-1 node1_mgmt1          mgmt
cluster-1 node2_mgmt1          mgmt
vs1      data1                data_http
vs3      data2                data
```

Commandes ONTAP pour gérer le service et les politiques de pare-feu

Vous pouvez utiliser le `system services firewall` commandes permettant de gérer le service de pare-feu, le `system services firewall policy` commandes pour gérer les politiques de pare-feu et `network interface modify` Commande permettant de gérer les paramètres de pare-feu des LIF.

À partir d'ONTAP 9.10.1 :

- Les politiques de pare-feu sont obsolètes et sont remplacées par les politiques de service LIF. Auparavant, le pare-feu intégré était géré à l'aide de politiques de pare-feu. Cette fonctionnalité s'effectue désormais à l'aide d'une politique de service LIF.
- Toutes les politiques de pare-feu sont vides et n'ouvrent aucun port dans le pare-feu sous-jacent. En revanche, tous les ports doivent être ouverts via une règle de service LIF.
- Aucune action n'est requise après une mise à niveau vers la version 9.10.1 ou ultérieure afin de passer des politiques de pare-feu aux politiques de service LIF. Le système construit automatiquement des politiques de service LIF conformes aux politiques de pare-feu utilisées dans la version précédente de ONTAP. Si vous utilisez des scripts ou d'autres outils qui créent et gèrent des politiques de pare-feu personnalisées, vous devrez peut-être mettre à niveau ces scripts pour créer des stratégies de service personnalisées.

Pour en savoir plus, voir "LIF et politiques de services dans ONTAP 9.6 et versions ultérieures".

Les fonctions que vous recherchez…	Utilisez cette commande…
Activez ou désactivez le service de pare-feu	`system services firewall modify`
Affiche la configuration actuelle du service de pare-feu	`system services firewall show`
Créez une politique de pare-feu ou ajoutez un service à une politique de pare-feu existante	`system services firewall policy create`
Appliquer une politique de pare-feu à une LIF	`network interface modify -lif lifname -firewall-policy`
Modifiez les adresses IP et les masques de réseau associés à une politique de pare-feu	`system services firewall policy modify`
Affiche des informations sur les politiques de pare-feu	`system services firewall policy show`
Créez une nouvelle politique de pare-feu qui est une copie exacte d'une politique existante	`system services firewall policy clone`
Supprimez une politique de pare-feu qui n'est pas utilisée par une LIF	`system services firewall policy delete`

Informations associées

- "pare-feu des services système"
- "modification de l'interface réseau"

Marquage QoS (administrateurs du cluster uniquement)

En savoir plus sur la qualité de service (QoS) du réseau ONTAP

Le marquage de la qualité de service (QoS) du réseau vous aide à hiérarchiser différents types de trafic en fonction des conditions du réseau pour utiliser efficacement les ressources du réseau. Vous pouvez définir la valeur DSCP (Dedifférenciée services code point) des paquets IP sortants pour les types de trafic pris en charge par IPspace.

Marquage DSCP pour la conformité UC

Vous pouvez activer le marquage DSCP sur le trafic de paquets IP sortant (sortie) pour un protocole donné avec un code DSCP par défaut ou fourni par l'utilisateur. Le marquage DSCP est un mécanisme de classification et de gestion du trafic réseau et est un composant de la conformité UC (Unified Capability).

Le marquage DSCP (également appelé *QoS marking* ou *Quality of service marking*) est activé en fournissant une valeur IPspace, protocole et DSCP. Les protocoles sur lesquels le marquage DSCP peut être appliqué sont les suivants : NFS, SMB, iSCSI, SnapMirror, NDMP, FTP, HTTP/HTTPS, SSH, Telnet et SNMP.

Si vous ne fournissez pas de valeur DSCP lors de l'activation du marquage DSCP pour un protocole donné, une valeur par défaut est utilisée :

- La valeur par défaut pour les protocoles de données/le trafic est 0x0A (10).
- La valeur par défaut pour les protocoles de contrôle/trafic est 0x30 (48).

Modifier les valeurs de marquage QoS réseau ONTAP

Il est possible de modifier les valeurs du marquage qualité de service (QoS) pour différents protocoles, pour chaque IPspace.

Avant de commencer

Tous les nœuds d'un cluster doivent exécuter la même version de ONTAP.

Étape

Modifiez les valeurs de marquage QoS à l'aide de `network qos-marking modify` commande.

- Le `-ipspace` Paramètre spécifie l'IPspace pour lequel l'entrée de marquage QoS doit être modifiée.
- Le `-protocol` paramètre spécifie le protocole pour lequel l'entrée de marquage QoS doit être modifiée.
- Le `-dscp` Paramètre spécifie la valeur DSCP (Differentiated Services Code point). Les valeurs possibles sont comprises entre 0 et 63.
- Le `-is-enabled` Paramètre permet d'activer ou de désactiver le marquage QoS pour le protocole spécifié dans l'IPspace fourni par le `-ipspace` paramètre.

La commande suivante active le marquage QoS pour le protocole NFS dans l'IPspace par défaut :

```
network qos-marking modify -ipspace Default -protocol NFS -is-enabled true
```

La commande suivante définit la valeur DSCP sur 20 pour le protocole NFS dans l'IPspace par défaut :

```
network qos-marking modify -ipspace Default -protocol NFS -dscp 20
```

Pour en savoir plus sur `network qos-marking modify` et les valeurs possibles du protocole"Référence de commande ONTAP", reportez-vous à la .

Afficher les valeurs de marquage QoS du réseau ONTAP

Vous pouvez afficher les valeurs de marquage QoS pour différents protocoles, pour chaque IPspace.

Étape

Afficher les valeurs de marquage QoS à l'aide du `network qos-marking show` commande.

La commande suivante affiche le marquage QoS pour tous les protocoles dans l'IPspace par défaut :

```
network qos-marking show -ipspace Default
IPspace              Protocol           DSCP  Enabled?
-------------------- ----------------- -----  --------
Default
                     CIFS                 10  false
                     FTP                  48  false
                     HTTP-admin           48  false
                     HTTP-filesrv         10  false
                     NDMP                 10  false
                     NFS                  10  true
                     SNMP                 48  false
                     SSH                  48  false
                     SnapMirror           10  false
                     Telnet               48  false
                     iSCSI                10  false
11 entries were displayed.
```

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

Gestion SNMP (administrateurs du cluster uniquement)

En savoir plus sur SNMP sur le réseau ONTAP

Vous pouvez configurer le protocole SNMP pour surveiller les SVM au sein de votre cluster afin d'éviter les problèmes avant qu'ils ne se produisent et de répondre aux

problèmes en cas de survenue. La gestion de SNMP implique la configuration des utilisateurs SNMP et la configuration des destinations de Traphost SNMP (stations de travail de gestion) pour tous les événements SNMP. SNMP est désactivé par défaut sur les LIFs de données.

Vous pouvez créer et gérer des utilisateurs SNMP en lecture seule dans la SVM de données. Les LIFs data doivent être configurées de sorte à recevoir des requêtes SNMP sur le SVM.

Les postes de travail SNMP de gestion de réseau, ou gestionnaires, peuvent interroger l'agent SNMP du SVM pour obtenir des informations. L'agent SNMP recueille des informations et les transmet aux gestionnaires SNMP. L'agent SNMP génère également des notifications d'interruption lorsque des événements spécifiques se produisent. L'agent SNMP du SVM possède des privilèges en lecture seule ; il ne peut pas être utilisé pour des opérations définies ou pour effectuer une action corrective en réponse à un trap. ONTAP fournit un agent SNMP compatible avec les versions SNMP v1, v2c et v3. SNMPv3 offre une sécurité avancée en utilisant des phrases de passe et le cryptage.

Pour plus d'informations sur la prise en charge SNMP dans les systèmes ONTAP, voir "Tr-4220 : prise en charge SNMP dans Data ONTAP".

Présentation MIB

Une base MIB (Management information base) est un fichier texte qui décrit les objets SNMP et les traps.

Les MIB décrivent la structure des données de gestion du système de stockage et utilisent un espace de noms hiérarchique contenant des identifiants d'objets (OID). Chaque OID identifie une variable qui peut être lue à l'aide de SNMP.

Étant donné que les MIB ne sont pas des fichiers de configuration et que ONTAP ne lit pas ces fichiers, la fonctionnalité SNMP n'est pas affectée par les MIB. ONTAP fournit le fichier MIB suivant :

- Une MIB personnalisées NetApp (`netapp.mib`)

ONTAP prend en charge les MIB IPv6 (RFC 2465), TCP (RFC 4022), UDP (RFC 4113) et ICMP (RFC 2466), qui affichent à la fois des données IPv4 et IPv6.

ONTAP fournit également une référence croisée courte entre les identificateurs d'objet (OID) et les noms courts d'objet dans le `traps.dat` fichier.

> Les dernières versions des fichiers MIB ONTAP et `traps.dat `sont disponibles sur le site de support NetApp. Cependant, les versions de ces fichiers sur le site de support ne correspondent pas nécessairement aux capacités SNMP de votre version ONTAP. Ces fichiers sont fournis pour vous aider à évaluer les fonctions SNMP dans la dernière version de ONTAP.

Interruptions SNMP

Les interruptions SNMP capturent les informations de surveillance du système envoyées en tant que notification asynchrone de l'agent SNMP au gestionnaire SNMP.

Il existe trois types d'interruptions SNMP : standard, intégré et défini par l'utilisateur. Les interruptions définies par l'utilisateur ne sont pas prises en charge dans ONTAP.

Un trap peut être utilisé pour vérifier périodiquement les seuils opérationnels ou les échecs définis dans la MIB. Si un seuil est atteint ou qu'une panne est détectée, l'agent SNMP envoie un message (interruption) aux

Traphosts les alertant de l'événement.

ONTAP prend en charge les traps SNMPv1 et SNMPv3. ONTAP ne prend pas en charge les déroutements SNMPv2c et n'informe pas.

Interruptions SNMP standard

Ces interruptions sont définies dans RFC 1215. Il existe cinq interruptions SNMP standard prises en charge par ONTAP : coldstart, warmstart, Linkdown, linkup et authenticationFailure.

Le trap authenticationFailure est désactivé par défaut. Vous devez utiliser `system snmp authtrap` la commande pour activer le trap. Pour en savoir plus, `system snmp authtrap` consultez le "Référence de commande ONTAP".

Interruptions SNMP intégrées

Les interruptions intégrées sont prédéfinies dans ONTAP et sont automatiquement envoyées aux stations de gestion du réseau de la liste des Traphost si un événement se produit. Ces interruptions, telles que diskFailedShutdown, cpuTooBusy et volume NearlyFull, sont définies dans la MIB personnalisées.

Chaque trappe intégrée est identifiée par un code d'interruption unique.

Créez des communautés SNMP pour le réseau ONTAP

Vous pouvez créer une communauté SNMP qui agit comme un mécanisme d'authentification entre le poste de gestion et le SVM (Storage Virtual machine) en cas d'utilisation des protocoles SNMPv1 et SNMPv2c.

En créant des communautés SNMP dans un SVM de données, vous pouvez exécuter des commandes telles que `snmpwalk` et `snmpget` Sur les LIF de données.

Description de la tâche

- Dans les nouvelles installations de ONTAP, SNMPv1 et SNMPv2c sont désactivés par défaut.

  Les protocoles SNMPv1 et SNMPv2c sont activés après la création d'une communauté SNMP.

- ONTAP prend en charge les communautés en lecture seule.
- Par défaut la politique de pare-feu « données » qui est attribuée aux LIFs de données a le service SNMP défini sur `deny`.

  Vous devez créer une nouvelle politique de pare-feu avec le service SNMP défini sur `allow` Lors de la création d'un utilisateur SNMP pour un SVM de données.

  Depuis ONTAP 9.10.1, les politiques de pare-feu sont obsolètes et intégralement remplacées par les politiques de service de LIF. Pour plus d'informations, voir "Configuration des politiques de pare-feu pour les LIF".

- Vous pouvez créer des communautés SNMP pour les utilisateurs SNMPv1 et SNMPv2c pour la SVM d'administration et la SVM de données.
- Comme un SVM ne fait pas partie de la norme SNMP, les requêtes relatives aux LIF de données doivent inclure l'OID racine NetApp (1.3.6.1.4.1.789), par exemple `snmpwalk -v 2c -c snmpNFS`

10.238.19.14 1.3.6.1.4.1.789.

Étapes

1. Créez une communauté SNMP en utilisant le `system snmp community add` commande. La commande suivante montre comment créer une communauté SNMP dans le SVM admin cluster-1 :

```
system snmp community add -type ro -community-name comty1 -vserver
cluster-1
```

   La commande suivante montre comment créer une communauté SNMP dans le SVM de données vs1 :

```
system snmp community add -type ro -community-name comty2 -vserver vs1
```

2. Vérifiez que les communautés ont été créées à l'aide de la commande system snmp community show.

   La commande suivante présente les deux communautés créées pour SNMPv1 et SNMPv2c :

```
system snmp community show
cluster-1
rocomty1
vs1
rocomty2
```

3. Vérifier si SNMP est autorisé en tant que service dans la politique de pare-feu « data » en utilisant le `system services firewall policy show` commande.

   La commande suivante indique que le service snmp n'est pas autorisé dans la politique de pare-feu « data » par défaut (le service snmp est autorisé dans la politique de pare-feu « mgmt » uniquement) :

```
system services firewall policy show
Vserver Policy       Service    Allowed
------- ------------ ---------- -------------------
cluster-1
        data
                     dns        0.0.0.0/0
                     ndmp       0.0.0.0/0
                     ndmps      0.0.0.0/0
cluster-1
        intercluster
                     https      0.0.0.0/0
                     ndmp       0.0.0.0/0
                     ndmps      0.0.0.0/0
cluster-1
        mgmt
                     dns        0.0.0.0/0
                     http       0.0.0.0/0
                     https      0.0.0.0/0
                     ndmp       0.0.0.0/0
                     ndmps      0.0.0.0/0
                     ntp        0.0.0.0/0
                     snmp       0.0.0.0/0
                     ssh        0.0.0.0/0
```

4. Créez une nouvelle politique de pare-feu qui autorise l'accès à l'aide du système `snmp` service à l'aide du `system services firewall policy create` commande.

   Les commandes suivantes créent une nouvelle politique de pare-feu de données nommée « data1 » qui autorise le `snmp`

```
system services firewall policy create -policy data1 -service snmp
-vserver  vs1 -allow-list 0.0.0.0/0

cluster-1::> system services firewall policy show -service snmp
Vserver  Policy       Service    Allowed
-------  ------------ ---------- -------------------
cluster-1
         mgmt
                      snmp       0.0.0.0/0
vs1
         data1
                      snmp       0.0.0.0/0
```

5. Appliquez la politique de pare-feu à une LIF de données en utilisant la `network interface modify` commande avec le paramètre -firewall-policy.

La commande suivante attribue la nouvelle politique de pare-feu « data1 » à LIF « datalif1 » :

```
network interface modify -vserver vs1 -lif datalif1 -firewall-policy
data1
```

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

Configurer les utilisateurs SNMPv3 dans un cluster ONTAP

SNMPv3 est un protocole sécurisé lorsqu'il est comparé au protocole SNMPv1 et SNMPv2c. Pour utiliser SNMPv3, vous devez configurer un utilisateur SNMPv3 pour exécuter les utilitaires SNMP à partir du gestionnaire SNMP.

Étape

Utilisez le `security login create` commande pour créer un utilisateur SNMPv3.

Vous êtes invité à fournir les informations suivantes :

- ID moteur : la valeur par défaut et la valeur recommandée sont l'ID moteur local
- Protocole d'authentification
- Mot de passe d'authentification
- Protocole de confidentialité
- Mot de passe du protocole de confidentialité

Résultat

L'utilisateur SNMPv3 peut se connecter à partir du gestionnaire SNMP en utilisant le nom d'utilisateur et le mot de passe et en exécutant les commandes de l'utilitaire SNMP.

Paramètres de sécurité SNMPv3

SNMPv3 inclut une fonctionnalité d'authentification qui, lorsqu'elle est sélectionnée, demande aux utilisateurs de saisir leurs noms, un protocole d'authentification, une clé d'authentification et le niveau de sécurité souhaité lors de l'appel d'une commande.

Le tableau suivant répertorie les paramètres de sécurité SNMPv3 :

Paramètre	Option de ligne de commandes	Description
ID d'ingénierie	-E EngineID	ID moteur de l'agent SNMP. La valeur par défaut est local EngineID (recommandé).
Nom de sécurité	-U Nom	Le nom d'utilisateur ne doit pas dépasser 32 caractères.
Protocole d'authentification	-A {none	MD5

SHA	SHA-256}	Le type d'authentification peut être aucun, MD5, SHA ou SHA-256.
AuthKey	-UNE PHRASE DE PASSE	Phrase de passe avec un minimum de huit caractères.
Niveau de sécurité	-L {authNoPriv	AuthPriv
noAuthNoPriv}	Le niveau de sécurité peut être authentification, aucune confidentialité, authentification, confidentialité ou aucune authentification, Aucune confidentialité.	Protocole privé
-x { none	des	aes128}
Le protocole de confidentialité peut être aucun, des ou aes128	Mot de passe privé	-X mot de passe

Exemples de niveaux de sécurité différents

Cet exemple montre comment un utilisateur SNMPv3 créé avec différents niveaux de sécurité peut utiliser les commandes SNMP côté client, telles que `snmpwalk`, pour interroger les objets de cluster.

Pour améliorer les performances, vous devez récupérer tous les objets d'un tableau plutôt qu'un seul objet ou quelques objets du tableau.

Vous devez utiliser `snmpwalk` 5.3.1 ou version ultérieure lorsque le protocole d'authentification est SHA.

Niveau de sécurité : AuthPriv

Le résultat suivant montre la création d'un utilisateur SNMPv3 avec le niveau de sécurité d'authPriv.

```
security login create -user-or-group-name snmpv3user -application snmp
-authentication-method usm
Enter the authoritative entity's EngineID [local EngineID]:
Which authentication protocol do you want to choose (none, md5, sha, sha2-
256) [none]: md5

Enter the authentication protocol password (minimum 8 characters long):
Enter the authentication protocol password again:
Which privacy protocol do you want to choose (none, des, aes128) [none]:
des
Enter privacy protocol password (minimum 8 characters long):
Enter privacy protocol password again:
```

Mode FIPS

```
security login create -user-or-group-name snmpv3user -application snmp
-authmethod usm
Enter the authoritative entity's EngineID [local EngineID]:
Which authentication protocol do you want to choose (sha, sha2-256) [sha]

Enter authentication protocol password (minimum 8 characters long):
Enter authentication protocol password again:
Which privacy protocol do you want to choose (aes128) [aes128]:
Enter privacy protocol password (minimum 8 characters long):
Enter privacy protocol password again:
```

Test snmpwalk

La sortie suivante montre l'utilisateur SNMPv3 exécutant la commande snmpwalk :

Pour améliorer les performances, vous devez récupérer tous les objets d'un tableau plutôt qu'un seul objet ou quelques objets du tableau.

```
$ snmpwalk -v 3 -u snmpv3user -a SHA -A password1! -x DES -X password1! -l
authPriv 192.0.2.62 .1.3.6.1.4.1.789.1.5.8.1.2
Enterprises.789.1.5.8.1.2.1028 = "vol0"
Enterprises.789.1.5.8.1.2.1032 = "vol0"
Enterprises.789.1.5.8.1.2.1038 = "root_vs0"
Enterprises.789.1.5.8.1.2.1042 = "root_vstrap"
Enterprises.789.1.5.8.1.2.1064 = "vol1"
```

Niveau de sécurité : AuthNoPriv

Le résultat suivant montre la création d'un utilisateur SNMPv3 avec le niveau de sécurité authNoPriv.

```
security login create -user-or-group-name snmpv3user -application snmp
-authmethod usm -role read-only
Enter the authoritative entity's EngineID [local EngineID]:
Which authentication protocol do you want to choose (none, md5, sha)
[none]: md5
```

Mode FIPS

FIPS ne vous permet pas de choisir **none** pour le protocole de confidentialité. En conséquence, il n'est pas possible de configurer un utilisateur authNoPriv SNMPv3 en mode FIPS.

Test snmpwalk

La sortie suivante montre l'utilisateur SNMPv3 exécutant la commande snmpwalk :

Pour améliorer les performances, vous devez récupérer tous les objets d'un tableau plutôt qu'un seul objet ou quelques objets du tableau.

```
$ snmpwalk -v 3 -u snmpv3user1 -a MD5 -A password1!  -l authNoPriv
192.0.2.62 .1.3.6.1.4.1.789.1.5.8.1.2
Enterprises.789.1.5.8.1.2.1028 = "vol0"
Enterprises.789.1.5.8.1.2.1032 = "vol0"
Enterprises.789.1.5.8.1.2.1038 = "root_vs0"
Enterprises.789.1.5.8.1.2.1042 = "root_vstrap"
Enterprises.789.1.5.8.1.2.1064 = "vol1"
```

Niveau de sécurité : NoAuthNoPriv

La sortie suivante montre la création d'un utilisateur SNMPv3 avec le niveau de sécurité noAuthNoPriv.

```
security login create -user-or-group-name snmpv3user -application snmp
-authmethod usm -role read-only
Enter the authoritative entity's EngineID [local EngineID]:
Which authentication protocol do you want to choose (none, md5, sha)
[none]: none
```

Mode FIPS

FIPS ne vous permet pas de choisir **none** pour le protocole de confidentialité.

Test snmpwalk

La sortie suivante montre l'utilisateur SNMPv3 exécutant la commande snmpwalk :

Pour améliorer les performances, vous devez récupérer tous les objets d'un tableau plutôt qu'un seul objet ou quelques objets du tableau.

```
$ snmpwalk -v 3 -u snmpv3user2 -l noAuthNoPriv 192.0.2.62
.1.3.6.1.4.1.789.1.5.8.1.2
Enterprises.789.1.5.8.1.2.1028 = "vol0"
Enterprises.789.1.5.8.1.2.1032 = "vol0"
Enterprises.789.1.5.8.1.2.1038 = "root_vs0"
Enterprises.789.1.5.8.1.2.1042 = "root_vstrap"
Enterprises.789.1.5.8.1.2.1064 = "vol1"
```

Pour en savoir plus, `security login create` consultez le "Référence de commande ONTAP".

Configurer des traphosts pour SNMP sur le réseau ONTAP

Vous pouvez configurer le Traphost (gestionnaire SNMP) pour recevoir des notifications (PDU d'interruption SNMP) lorsque des interruptions SNMP sont générées dans le cluster. Vous pouvez spécifier le nom d'hôte ou l'adresse IP (IPv4 ou IPv6) du Traphost SNMP.

Avant de commencer

- Les traps SNMP doivent être activés sur le cluster.

  Les interruptions SNMP et SNMP sont activées par défaut.

- Le DNS doit être configuré sur le cluster pour la résolution des noms de Traphost.
- IPv6 doit être activé sur le cluster pour configurer les Traphosts SNMP à l'aide des adresses IPv6.
- Vous devez avoir spécifié l'authentification d'un modèle de sécurité basé sur l'utilisateur (USM) prédéfini et les informations d'identification de confidentialité lors de la création de traphosts.

Étape

Ajouter un Traphost SNMP :

```
system snmp traphost add
```

Les interruptions ne peuvent être envoyées que lorsqu'au moins une station de gestion SNMP est spécifiée comme un traphost.

La commande suivante ajoute un nouvel hôte SNMPv3 nommé yyy.example.com avec un utilisateur USM connu :

```
system snmp traphost add -peer-address yyy.example.com -usm-username
MyUsmUser
```

La commande suivante ajoute un Traphost à l'aide de l'adresse IPv6 de l'hôte :

```
system snmp traphost add -peer-address 2001:0db8:1:1:209:6bff:feae:6d67
```

Vérifier l'interrogation SNMP dans un cluster ONTAP

Une fois le protocole SNMP configuré, vous devez vérifier que vous pouvez interroger le cluster.

Description de la tâche

Pour interroger un cluster, vous devez utiliser une commande tierce par exemple `snmpwalk`.

Étapes

1. Envoyer une commande SNMP pour interroger le cluster depuis un autre cluster.

   Pour les systèmes exécutant SNMPv1, utilisez la commande CLI `snmpwalk -v version -c community_stringip_address_or_host_name system` Pour découvrir le contenu de la base MIB (Management information base).

   Dans cet exemple, l'adresse IP de la LIF de gestion du cluster dont vous disposez est 10.11.12.123. La commande affiche les informations demandées à partir de la MIB :

   ```
   C:\Windows\System32>snmpwalk -v 1 -c public 10.11.12.123 system

   SNMPv1-MIB::sysDescr.0 = STRING: NetApp Release 8.3.0
              Cluster-Mode: Tue Apr 22 16:24:48 EDT 2014
   SNMPv1-MIB::sysObjectID.0 = OID: SNMPv1-SMI::enterprises.789.2.5
   DISMAN-EVENT-MIB::sysUpTimeInstance = Timeticks: (162644448) 18 days,
   19:47:24.48
   SNMPv1-MIB::sysContact.0 = STRING:
   SNMPv1-MIB::sysName.0 = STRING: systemname.testlabs.com
   SNMPv1-MIB::sysLocation.0 = STRING: Floor 2 Row B Cab 2
   SNMPv1-MIB::sysServices.0 = INTEGER: 72
   ```

   Pour les systèmes exécutant SNMPv2c, utilisez la commande CLI `snmpwalk -v version -c community_stringip_address_or_host_name system` Pour découvrir le contenu de la base MIB (Management information base).

   Dans cet exemple, l'adresse IP de la LIF de gestion du cluster dont vous disposez est 10.11.12.123. La commande affiche les informations demandées à partir de la MIB :

```
C:\Windows\System32>snmpwalk -v 2c -c public 10.11.12.123 system

SNMPv2-MIB::sysDescr.0 = STRING: NetApp Release 8.3.0
            Cluster-Mode: Tue Apr 22 16:24:48 EDT 2014
SNMPv2-MIB::sysObjectID.0 = OID: SNMPv2-SMI::enterprises.789.2.5
DISMAN-EVENT-MIB::sysUpTimeInstance = Timeticks: (162635772) 18 days,
19:45:57.72
SNMPv2-MIB::sysContact.0 = STRING:
SNMPv2-MIB::sysName.0 = STRING: systemname.testlabs.com
SNMPv2-MIB::sysLocation.0 = STRING: Floor 2 Row B Cab 2
SNMPv2-MIB::sysServices.0 = INTEGER: 72
```

Pour les systèmes exécutant SNMPv3, utilisez la commande CLI `snmpwalk -v 3 -a MD5 or SHA -l authnopriv -u username -A passwordip_address_or_host_name system` Pour découvrir le contenu de la base MIB (Management information base).

Dans cet exemple, l'adresse IP de la LIF de gestion du cluster dont vous disposez est 10.11.12.123. La commande affiche les informations demandées à partir de la MIB :

```
C:\Windows\System32>snmpwalk -v 3 -a MD5 -l authnopriv -u snmpv3
       -A password123 10.11.12.123 system

SNMPv3-MIB::sysDescr.0 = STRING: NetApp Release 8.3.0
       Cluster-Mode: Tue Apr 22 16:24:48 EDT 2014
SNMPv3-MIB::sysObjectID.0 = OID: SNMPv3-SMI::enterprises.789.2.5
DISMAN-EVENT-MIB::sysUpTimeInstance = Timeticks: (162666569) 18 days,
19:51:05.69
SNMPv3-MIB::sysContact.0 = STRING:
SNMPv3-MIB::sysName.0 = STRING: systemname.testlabs.com
SNMPv3-MIB::sysLocation.0 = STRING: Floor 2 Row B Cab 2
SNMPv3-MIB::sysServices.0 = INTEGER: 72
```

Commandes ONTAP pour gérer SNMP, traps et traphosts

Vous pouvez utiliser le `system snmp` Commandes permettant de gérer SNMP, les traps et les Traphosts. Vous pouvez utiliser le `security` Commandes permettant de gérer les utilisateurs SNMP par SVM. Vous pouvez utiliser le `event` Commandes pour gérer les événements liés aux traps SNMP.

Commandes permettant de configurer SNMP

Les fonctions que vous recherchez…	Utilisez cette commande…

Activez SNMP sur le cluster	`options -option-name snmp.enable -option-value on` Le service SNMP doit être autorisé conformément à la politique de pare-feu de gestion. Vous pouvez vérifier si le protocole SNMP est autorisé via la commande system services firewall policy show.
Désactiver le protocole SNMP sur le cluster	`options -option-name snmp.enable -option-value off`

Commandes pour la gestion des utilisateurs SNMP v1, v2c et v3

Les fonctions que vous recherchez…	Utilisez cette commande…
Configurez les utilisateurs SNMP	`security login create`
Afficher les utilisateurs SNMP	`security snmpusers`et `security login show -application snmp`
Supprimer les utilisateurs SNMP	`security login delete`
Modifier le nom du rôle de contrôle d'accès d'une méthode de connexion pour les utilisateurs SNMP	`security login modify`

Commandes permettant de fournir des informations de contact et d'emplacement

Les fonctions que vous recherchez…	Utilisez cette commande…
Afficher ou modifier les détails du contact du cluster	`system snmp contact`
Afficher ou modifier les détails d'emplacement du cluster	`system snmp location`

Commandes pour la gestion des communautés SNMP

Les fonctions que vous recherchez…	Utilisez cette commande…
Ajoutez une communauté en lecture seule (ro) pour un SVM ou pour tous les SVM du cluster	`system snmp community add`
Supprimer une communauté ou toutes les communautés	`system snmp community delete`
Afficher la liste de toutes les communautés	`system snmp community show`

Les SVM ne faisant pas partie de la norme SNMP, les requêtes relatives aux LIF de données doivent inclure l'OID racine NetApp (1.3.6.1.4.1.789), par exemple. `snmpwalk -v 2c -c snmpNFS 10.238.19.14 1.3.6.1.4.1.789`.

Commande pour l'affichage des valeurs d'option SNMP

Les fonctions que vous recherchez…	Utilisez cette commande…
Afficher les valeurs actuelles de toutes les options SNMP, y compris le contact de cluster, l'emplacement de contact, si le cluster est configuré pour envoyer des traps, la liste des Traphosts, la liste des communautés et le type de contrôle d'accès	`system snmp show`

Commandes pour la gestion des interruptions SNMP et des Traphosts

Les fonctions que vous recherchez…	Utilisez cette commande…
Activer les traps SNMP envoyés depuis le cluster	`system snmp init -init 1`
Désactiver les traps SNMP envoyés depuis le cluster	`system snmp init -init 0`
Ajoutez un Traphost qui reçoit des notifications SNMP pour des événements spécifiques dans le cluster	`system snmp traphost add`
Supprimer un Traphost	`system snmp traphost delete`
Affiche la liste des Traphosts	`system snmp traphost show`

Commandes pour la gestion des événements liés aux traps SNMP

Les fonctions que vous recherchez…	Utilisez cette commande…
Afficher les événements pour lesquels des interruptions SNMP (intégrées) sont générées	`event route show` Utilisez le `-snmp-support true` Paramètre pour afficher uniquement les événements SNMP. Utilisez le `instance -messagename <message>` paramètre permettant d'afficher une description détaillée de la raison d'un événement et de toute action corrective. Le routage des événements de déroutement SNMP individuels vers des destinations de traphost spécifiques n'est pas pris en charge. Tous les événements de déroutement SNMP sont envoyés à toutes les destinations de Traphost.

Affiche la liste des enregistrements de l'historique des interruptions SNMP, qui sont des notifications d'événements envoyées à des interruptions SNMP	`event snmphistory show`
Supprimer un enregistrement de l'historique des interruptions SNMP	`event snmphistory delete`

Informations associées

- "snmp système"
- "sécurité snmpusers"
- "sécurité"
- "événement"
- "connexion de sécurité"

Gestion du routage dans un SVM

En savoir plus sur le routage des SVM sur le réseau ONTAP

La table de routage d'un SVM détermine le chemin réseau utilisé par la SVM pour communiquer avec une destination. Il est important de comprendre le fonctionnement des tables de routage afin d'éviter les problèmes de réseau avant qu'ils ne surviennent.

Les règles de routage sont les suivantes :

- ONTAP achemine le trafic sur l'itinéraire le plus spécifique disponible.
- ONTAP achemine le trafic sur une route de passerelle par défaut (ayant 0 bits de masque de réseau) comme dernier recours, lorsque des routes plus spécifiques ne sont pas disponibles.

Dans le cas de routes avec la même destination, le même masque de réseau et la même mesure, il n'est pas garanti que le système utilisera la même route après un redémarrage ou après une mise à niveau. Ceci est particulièrement un problème si vous avez configuré plusieurs routes par défaut.

Il est recommandé de configurer une seule route par défaut pour une SVM. Pour éviter toute interruption, vous devez vous assurer que l'itinéraire par défaut est capable d'atteindre toute adresse réseau qui n'est pas accessible par un itinéraire plus spécifique. Pour plus d'informations, voir"Base de connaissances NetApp : SU134 - L'accès au réseau peut être perturbé par une configuration de routage incorrecte dans ONTAP en cluster"

Créez des routes statiques pour le réseau ONTAP

Vous pouvez créer des routes statiques au sein d'une machine virtuelle de stockage (SVM) pour contrôler la manière dont les LIF utilisent le réseau pour le trafic sortant.

Lorsque vous créez une entrée de route associée à un SVM, la route sera utilisée par toutes les LIFs qui sont détenues par le SVM spécifié et qui se trouvent sur le même sous-réseau que la passerelle.

Étape

Utilisez le `network route create` commande pour créer une route.

```
network route create -vserver vs0 -destination 0.0.0.0/0 -gateway
10.61.208.1
```

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

Activez le routage multivoie pour le réseau ONTAP

Si plusieurs routes ont la même mesure pour une destination, seule une des routes est sélectionnée pour le trafic sortant. Cela entraîne l'utilisation d'autres routes pour l'envoi du trafic sortant. Vous pouvez activer le routage multivoie pour équilibrer la charge sur toutes les routes disponibles proportionnellement à leurs mesures, par opposition au routage ECMP, qui équilibre la charge sur les routes disponibles de la même mesure.

Étapes

1. Connectez-vous au niveau de privilège avancé :

   `set -privilege advanced`

2. Activer le routage multivoie :

   `network options multipath-routing modify -is-enabled true`

   Le routage multivoie est activé pour tous les nœuds du cluster.

   ```
   network options multipath-routing modify -is-enabled true
   ```

   Pour en savoir plus, `network options multipath-routing modify` consultez le "Référence de commande ONTAP".

Supprimez les routes statiques du réseau ONTAP

Vous pouvez supprimer une route statique inutile d'une machine virtuelle de stockage (SVM).

Étape

Utilisez le `network route delete` commande pour supprimer une route statique.

L'exemple suivant supprime une route statique associée à SVM vs0 avec une passerelle de 10.63.0.1 et une adresse IP de destination de 0.0.0.0/0 :

```
network route delete -vserver vs0 -gateway 10.63.0.1 -destination
0.0.0.0/0
```

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

Afficher les informations de routage ONTAP

Vous pouvez afficher des informations sur la configuration de routage pour chaque SVM sur le cluster. Cela peut vous aider à diagnostiquer les problèmes de routage impliquant des problèmes de connectivité entre les applications ou les services client et un LIF sur un nœud du cluster.

Étapes

1. Utilisez le `network route show` Commande permettant d'afficher les routes au sein d'un ou plusieurs SVM. L'exemple suivant montre une route configurée sur le SVM vs0 :

```
network route show
  (network route show)
Vserver             Destination     Gateway         Metric
------------------- --------------- --------------- ------
vs0
                    0.0.0.0/0       172.17.178.1    20
```

2. Utilisez le `network route show-lifs` Commande pour afficher l'association des routes et LIFs au sein d'un ou plusieurs SVM.

   L'exemple suivant montre les LIFs avec des routes détenues par le SVM vs0 :

```
network route show-lifs
  (network route show-lifs)

Vserver: vs0
Destination             Gateway                 Logical Interfaces
----------------------  --------------          --------------------
0.0.0.0/0               172.17.178.1            cluster_mgmt,
                                                LIF-b-01_mgmt1,
                                                LIF-b-02_mgmt1
```

   Pour en savoir plus sur `network route show` et `network route show-lifs` dans le "Référence de commande ONTAP".

3. Utilisez le `network route active-entry show` Commande permettant d'afficher les routes installées sur un ou plusieurs nœuds, SVM, sous-réseaux ou routes avec des destinations spécifiées.

   L'exemple suivant montre toutes les routes installées sur un SVM spécifique :

```
network route active-entry show -vserver Data0

Vserver: Data0
Node: node-1
Subnet Group: 0.0.0.0/0
```

```
Destination             Gateway              Interface   Metric  Flags
----------------------  -------------------  ---------   ------  -----
127.0.0.1               127.0.0.1            lo              10  UHS
127.0.10.1              127.0.20.1           losk            10  UHS
127.0.20.1              127.0.20.1           losk            10  UHS

Vserver: Data0
Node: node-1
Subnet Group: fd20:8b1e:b255:814e::/64
Destination             Gateway              Interface   Metric  Flags
----------------------  -------------------  ---------   ------  -----
default                 fd20:8b1e:b255:814e::1
                                             e0d             20  UGS
fd20:8b1e:b255:814e::/64
                        link#4               e0d              0  UC

Vserver: Data0
Node: node-2
Subnet Group: 0.0.0.0/0
Destination             Gateway              Interface   Metric  Flags
----------------------  -------------------  ---------   ------  -----
127.0.0.1               127.0.0.1            lo              10  UHS

Vserver: Data0
Node: node-2
Subnet Group: 0.0.0.0/0
Destination             Gateway              Interface   Metric  Flags
----------------------  -------------------  ---------   ------  -----
127.0.10.1              127.0.20.1           losk            10  UHS
127.0.20.1              127.0.20.1           losk            10  UHS

Vserver: Data0
Node: node-2
Subnet Group: fd20:8b1e:b255:814e::/64
Destination             Gateway              Interface   Metric  Flags
----------------------  -------------------  ---------   ------  -----
default                 fd20:8b1e:b255:814e::1
                                             e0d             20  UGS
fd20:8b1e:b255:814e::/64
                        link#4               e0d              0  UC
fd20:8b1e:b255:814e::1  link#4               e0d              0  UHL
11 entries were displayed.
```

Pour en savoir plus, `network route active-entry show` consultez le "Référence de commande ONTAP".

Supprimez les routes dynamiques des tables de routage pour le réseau ONTAP

Lorsque des redirections ICMP sont reçues pour IPv4 et IPv6, des routes dynamiques sont ajoutées à la table de routage. Par défaut, les routes dynamiques sont supprimées au bout de 300 secondes. Si vous souhaitez maintenir des itinéraires dynamiques pendant une durée différente, vous pouvez modifier la valeur de délai d'exécution.

Description de la tâche

Vous pouvez définir la valeur de temporisation de 0 à 65,535 secondes. Si vous définissez la valeur sur 0, les routes n'expirent jamais. La suppression de routes dynamiques empêche la perte de connectivité causée par la persistance de routes non valides.

Étapes

1. Afficher la valeur de temporisation actuelle.
   - Pour IPv4 :

     ```
     network tuning icmp show
     ```

   - Pour IPv6 :

     ```
     network tuning icmp6 show
     ```

2. Modifiez la valeur de temporisation.
   - Pour IPv4 :

     ```
     network tuning icmp modify -node node_name -redirect-timeout
     timeout_value
     ```

   - Pour IPv6 :

     ```
     network tuning icmp6 modify -node node_name -redirect-v6-timeout
     timeout_value
     ```

3. Vérifiez que la valeur de temporisation a été modifiée correctement.
   - Pour IPv4 :

     ```
     network tuning icmp show
     ```

   - Pour IPv6 :

     ```
     network tuning icmp6 show
     ```

Pour en savoir plus, `network tuning icmp` consultez le "Référence de commande ONTAP".

Informations sur le réseau ONTAP

Afficher des informations sur le réseau ONTAP

Via l'interface de ligne de commandes, vous pouvez afficher des informations relatives aux ports, aux LIF, aux routes, aux règles de basculement, aux groupes de basculement, règles de pare-feu, DNS, NIS et connexions. Depuis ONTAP 9.8, vous pouvez également télécharger les données affichées dans System Manager relatives à votre réseau.

Ces informations peuvent être utiles dans des situations comme la reconfiguration des paramètres réseau ou le dépannage du cluster.

Si vous êtes administrateur de cluster, vous pouvez afficher toutes les informations de mise en réseau disponibles. Si vous êtes administrateur des SVM, vous pouvez afficher uniquement les informations relatives aux SVM qui vous sont attribuées.

Dans System Manager, lorsque vous affichez des informations dans une *vue liste*, vous pouvez cliquer sur **Télécharger** et la liste des objets affichés est téléchargée.

- La liste est téléchargée au format CSV (valeurs séparées par des virgules).
- Seules les données des colonnes visibles sont téléchargées.
- Le nom de fichier CSV est formaté avec le nom de l'objet et un horodatage.

Afficher des informations sur les ports réseau ONTAP

Vous pouvez afficher des informations sur un port spécifique ou sur tous les ports de tous les nœuds du cluster.

Description de la tâche

Les informations suivantes s'affichent :

- Nom du nœud
- Nom du port
- Nom IPspace
- Nom du domaine de diffusion
- État de la liaison (haut ou bas)
- Paramètre MTU
- Réglage de la vitesse du port et état de fonctionnement (1 Gigabit ou 10 gigabits par seconde)
- Paramètre de négociation automatique (vrai ou faux)
- Mode duplex et état de fonctionnement (moitié ou plein)
- Le groupe d'interface du port, le cas échéant
- Les informations de balise VLAN du port, le cas échéant
- État de santé du port (état de santé ou dégradé)

- Raisons pour lesquelles un port est marqué comme dégradé

Si les données d'un champ ne sont pas disponibles (par exemple, le duplex opérationnel et la vitesse d'un port inactif ne sont pas disponibles), la valeur du champ est indiquée comme `-`.

Étape

Affiche les informations relatives aux ports réseau à l'aide du `network port show` commande.

Vous pouvez afficher des informations détaillées pour chaque port en spécifiant le `-instance` paramètre ou obtenir des informations spécifiques en spécifiant les noms de champs à l'aide du `-fields` paramètre.

```
network port show
Node: node1

Ignore
                                                  Speed(Mbps) Health
Health
Port      IPspace      Broadcast Domain Link MTU  Admin/Oper  Status
Status
--------- ------------ ---------------- ---- ---- ----------- --------
------
e0a       Cluster      Cluster          up   9000  auto/1000  healthy
false
e0b       Cluster      Cluster          up   9000  auto/1000  healthy
false
e0c       Default      Default          up   1500  auto/1000  degraded
false
e0d       Default      Default          up   1500  auto/1000  degraded
true
Node: node2

Ignore
                                                  Speed(Mbps) Health
Health
Port      IPspace      Broadcast Domain Link MTU  Admin/Oper  Status
Status
--------- ------------ ---------------- ---- ---- ----------- --------
------
e0a       Cluster      Cluster          up   9000  auto/1000  healthy
false
e0b       Cluster      Cluster          up   9000  auto/1000  healthy
false
e0c       Default      Default          up   1500  auto/1000  healthy
false
e0d       Default      Default          up   1500  auto/1000  healthy
false
8 entries were displayed.
```

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

Afficher les informations VLAN ONTAP

Vous pouvez afficher des informations sur un VLAN spécifique ou sur tous les VLAN du cluster.

Description de la tâche

Vous pouvez afficher des informations détaillées pour chaque VLAN en spécifiant le `-instance` paramètre. Vous pouvez afficher des informations spécifiques en spécifiant des noms de champ à l'aide de l' `-fields` paramètre.

Étape

Affiche des informations sur les VLAN à l'aide de `network port vlan show` commande. La commande suivante affiche des informations sur tous les VLAN du cluster :

```
network port vlan show
                  Network Network
Node   VLAN Name Port    VLAN ID  MAC Address
------ --------- ------- -------- -----------------
cluster-1-01
       a0a-10    a0a     10       02:a0:98:06:10:b2
       a0a-20    a0a     20       02:a0:98:06:10:b2
       a0a-30    a0a     30       02:a0:98:06:10:b2
       a0a-40    a0a     40       02:a0:98:06:10:b2
       a0a-50    a0a     50       02:a0:98:06:10:b2
cluster-1-02
       a0a-10    a0a     10       02:a0:98:06:10:ca
       a0a-20    a0a     20       02:a0:98:06:10:ca
       a0a-30    a0a     30       02:a0:98:06:10:ca
       a0a-40    a0a     40       02:a0:98:06:10:ca
       a0a-50    a0a     50       02:a0:98:06:10:ca
```

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

Afficher les informations sur les groupes d'interfaces ONTAP

Vous pouvez afficher des informations relatives à un groupe d'interfaces afin de déterminer sa configuration.

Description de la tâche

Les informations suivantes s'affichent :

- Nœud sur lequel est situé le groupe d'interface
- Liste des ports réseau inclus dans le groupe d'interface
- Nom du groupe d'interface
- Fonction de distribution (MAC, IP, port ou séquentiel)
- Adresse MAC (Media Access Control) du groupe d'interfaces
- Statut de l'activité du port ; c'est-à-dire si tous les ports agrégés sont actifs (participation complète), si certains sont actifs (participation partielle) ou si aucun n'est actif

Étape

Affiche des informations sur les groupes d'interfaces en utilisant le `network port ifgrp show` commande.

Vous pouvez afficher des informations détaillées pour chaque nœud en spécifiant le `-instance` paramètre. Vous pouvez afficher des informations spécifiques en spécifiant des noms de champ à l'aide de l' `-fields` paramètre.

La commande suivante affiche des informations sur tous les groupes d'interfaces du cluster :

```
network port ifgrp show
         Port     Distribution                   Active
Node     IfGrp    Function     MAC Address       Ports   Ports
-------- -------- ------------ ----------------- ------- --------
cluster-1-01
         a0a      ip           02:a0:98:06:10:b2 full    e7a, e7b
cluster-1-02
         a0a      sequential   02:a0:98:06:10:ca full    e7a, e7b
cluster-1-03
         a0a      port         02:a0:98:08:5b:66 full    e7a, e7b
cluster-1-04
         a0a      mac          02:a0:98:08:61:4e full    e7a, e7b
```

La commande suivante affiche des informations détaillées sur les groupes d'interfaces pour un nœud unique :

```
network port ifgrp show -instance -node cluster-1-01

                  Node: cluster-1-01
 Interface Group Name: a0a
Distribution Function: ip
        Create Policy: multimode
          MAC Address: 02:a0:98:06:10:b2
   Port Participation: full
        Network Ports: e7a, e7b
             Up Ports: e7a, e7b
           Down Ports: -
```

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

Afficher les informations relatives aux LIF ONTAP

Vous pouvez afficher des informations détaillées sur une LIF afin de déterminer sa configuration.

Vous pouvez également vouloir afficher ces informations pour diagnostiquer les problèmes de base d'une LIF, comme vérifier la présence d'adresses IP en double ou vérifier si le port réseau appartient au sous-réseau correct. Les administrateurs des SVM (Storage Virtual machine) ne peuvent afficher que les informations concernant les LIFs associées à la SVM.

Description de la tâche

Les informations suivantes s’affichent :

- Adresse IP associée à la LIF
- Statut administratif de la LIF
- Statut opérationnel de la LIF

  L’état opérationnel des LIFs de données est déterminé par le statut du SVM auquel les LIFs de données sont associées. Lorsque le SVM est arrêté, le statut opérationnel de la LIF est modifié en down. Lorsque le SVM est de nouveau démarré, le statut opérationnel devient "active"

- Et le port sur lequel réside la LIF

Si les données d’un champ ne sont pas disponibles (par exemple, s’il n’y a pas d’informations d’état étendu), la valeur du champ est répertoriée comme `-`.

Étape

Afficher les informations LIF via `network interface show` la commande

Vous pouvez afficher des informations détaillées pour chaque LIF en spécifiant le paramètre -instance, ou obtenir des informations spécifiques en spécifiant les noms de champs à l’aide du paramètre -fields.

La commande suivante affiche des informations générales sur toutes les LIFs d’un cluster :

```
network interface show
            Logical    Status     Network          Current      Current Is
Vserver     Interface  Admin/Oper Address/Mask     Node         Port
Home
----------- ---------- ---------- ---------------- ------------ -------
----
example
            lif1         up/up    192.0.2.129/22   node-01
                                                                e0d
false
node
            cluster_mgmt up/up    192.0.2.3/20     node-02
                                                                e0c
false
node-01
            clus1        up/up    192.0.2.65/18    node-01
                                                                e0a
true
            clus2        up/up    192.0.2.66/18    node-01
                                                                e0b
true
            mgmt1        up/up    192.0.2.1/20     node-01
                                                                e0c
true
node-02
            clus1        up/up    192.0.2.67/18    node-02
                                                                e0a
true
            clus2        up/up    192.0.2.68/18    node-02
                                                                e0b
true
            mgmt2        up/up    192.0.2.2/20     node-02
                                                                e0d
true
vs1
            d1           up/up    192.0.2.130/21   node-01
                                                                e0d
false
            d2           up/up    192.0.2.131/21   node-01
                                                                e0d
true
            data3        up/up    192.0.2.132/20   node-02
                                                                e0c
true
```

La commande suivante affiche des informations détaillées sur une seule LIF :

```
network interface show -lif data1 -instance

                    Vserver Name: vs1
          Logical Interface Name: data1
                            Role: data
                   Data Protocol: nfs,cifs
                       Home Node: node-01
                       Home Port: e0c
                    Current Node: node-03
                    Current Port: e0c
               Operational Status: up
                  Extended Status: -
                          Is Home: false
                  Network Address: 192.0.2.128
                          Netmask: 255.255.192.0
            Bits in the Netmask: 18
                IPv4 Link Local: -
                    Subnet Name: -
             Administrative Status: up
                  Failover Policy: local-only
                  Firewall Policy: data
                      Auto Revert: false
   Fully Qualified DNS Zone Name: xxx.example.com
         DNS Query Listen Enable: false
             Failover Group Name: Default
                        FCP WWPN: -
                  Address family: ipv4
                         Comment: -
                  IPspace of LIF: Default
```

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

Afficher les informations de routage pour le réseau ONTAP

Vous pouvez afficher les informations relatives aux routes au sein d'une SVM.

Étape

Selon le type d'informations de routage que vous souhaitez afficher, entrez la commande applicable :

Pour afficher des informations sur…	Entrer…
Routes statiques, par SVM	`network route show`

LIF sur chaque route, par SVM	`network route show-lifs`

Vous pouvez afficher des informations détaillées pour chaque itinéraire en spécifiant le `-instance` paramètre. La commande suivante affiche les routes statiques au sein des SVM en cluster- 1 :

```
network route show
Vserver             Destination     Gateway         Metric
------------------- --------------- --------------- ------
Cluster
                    0.0.0.0/0       10.63.0.1       10
cluster-1
                    0.0.0.0/0       198.51.9.1      10
vs1
                    0.0.0.0/0       192.0.2.1       20
vs3
                    0.0.0.0/0       192.0.2.1       20
```

La commande suivante affiche l'association de routes statiques et d'interfaces logiques (LIF) au sein de tous les SVM au sein du cluster-1 :

```
network route show-lifs
Vserver: Cluster
Destination             Gateway                 Logical Interfaces
----------------------  ----------------------  -------------------
0.0.0.0/0               10.63.0.1               -

Vserver: cluster-1
Destination             Gateway                 Logical Interfaces
----------------------  ----------------------  -------------------
0.0.0.0/0               198.51.9.1              cluster_mgmt,
                                                cluster-1_mgmt1,

Vserver: vs1
Destination             Gateway                 Logical Interfaces
----------------------  ----------------------  -------------------
0.0.0.0/0               192.0.2.1               data1_1, data1_2

Vserver: vs3
Destination             Gateway                 Logical Interfaces
----------------------  ----------------------  -------------------
0.0.0.0/0               192.0.2.1               data2_1, data2_2
```

Pour en savoir plus sur `network route show` et `network route show-lifs` dans le "Référence de commande ONTAP".

Afficher les entrées de la table hôte DNS ONTAP

Les entrées de la table hôte DNS mappent les noms d'hôte aux adresses IP. Vous pouvez afficher les noms d'hôte et d'alias ainsi que l'adresse IP qu'ils mappent à pour tous les SVM d'un cluster.

Étape

Afficher les entrées du nom d'hôte pour tous les SVM via la commande vserver services name-service dns hosts show.

L'exemple suivant affiche les entrées de la table hôte :

```
vserver services name-service dns hosts show
Vserver    Address         Hostname        Aliases
---------- --------------- --------------- ---------------------
cluster-1
           10.72.219.36    lnx219-36       -
vs1
           10.72.219.37    lnx219-37       lnx219-37.example.com
```

Vous pouvez utiliser le `vserver services name-service dns` Commande permettant d'activer DNS sur un SVM et de le configurer afin d'utiliser DNS pour la résolution de nom d'hôte. Les noms d'hôte sont résolus à l'aide de serveurs DNS externes.

Afficher les informations de configuration du domaine DNS ONTAP

Vous pouvez afficher la configuration du domaine DNS d'un ou plusieurs SVM (Storage Virtual machine) dans votre cluster pour vérifier qu'ils sont correctement configurés.

Étape

Affichage des configurations de domaine DNS à l'aide de `vserver services name-service dns show` commande.

La commande suivante affiche les configurations DNS pour tous les SVM du cluster :

```
vserver services name-service dns show
                                                          Name
Vserver         State     Domains                         Servers
--------------- --------- ------------------------ -------------
cluster-1        enabled   xyz.company.com          192.56.0.129,
                                                    192.56.0.130
vs1             enabled   xyz.company.com          192.56.0.129,
                                                    192.56.0.130
vs2             enabled   xyz.company.com          192.56.0.129,
                                                    192.56.0.130
vs3             enabled   xyz.company.com          192.56.0.129,
                                                    192.56.0.130
```

La commande suivante affiche des informations détaillées de configuration DNS pour le SVM vs1 :

```
vserver services name-service dns show -vserver vs1
               Vserver: vs1
               Domains: xyz.company.com
          Name Servers: 192.56.0.129, 192.56.0.130
    Enable/Disable DNS: enabled
        Timeout (secs): 2
      Maximum Attempts: 1
```

Afficher les informations sur les groupes de basculement ONTAP

Vous pouvez afficher des informations sur les groupes de basculement, notamment la liste des nœuds et des ports de chaque failover group, si le failover est activé ou désactivé, et le type de failover policy qui est appliquée à chaque LIF.

Étapes

1. Afficher les ports cibles de chaque failover group en utilisant le `network interface failover-groups show` commande.

   La commande suivante affiche des informations sur tous les groupes de basculement sur un cluster à deux nœuds :

```
network interface failover-groups show
                              Failover
Vserver         Group         Targets
--------------- ------------- --------------------------------
Cluster
                Cluster
                              cluster1-01:e0a, cluster1-01:e0b,
                              cluster1-02:e0a, cluster1-02:e0b
vs1
                Default
                              cluster1-01:e0c, cluster1-01:e0d,
                              cluster1-01:e0e, cluster1-02:e0c,
                              cluster1-02:e0d, cluster1-02:e0e
```

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

2. Afficher les ports cibles et le broadcast domain d'un failover group spécifique en utilisant le `network interface failover-groups show` commande.

   La commande suivante affiche des informations détaillées sur le failover group data12 pour SVM vs4 :

```
network interface failover-groups show -vserver vs4 -failover-group
data12

       Vserver Name: vs4
Failover Group Name: data12
   Failover Targets: cluster1-01:e0f, cluster1-01:e0g, cluster1-02:e0f,
                     cluster1-02:e0g
   Broadcast Domain: Default
```

3. Afficher les paramètres de basculement utilisés par toutes les LIFs à l'aide du `network interface show` commande.

   La commande suivante affiche la règle de basculement et le groupe de basculement utilisés par chaque LIF :

```
network interface show -vserver * -lif * -fields failover-
group,failover-policy
vserver   lif                  failover-policy         failover-group
--------  -------------------  ---------------------   --------------
Cluster   cluster1-01_clus_1   local-only              Cluster
Cluster   cluster1-01_clus_2   local-only              Cluster
Cluster   cluster1-02_clus_1   local-only              Cluster
Cluster   cluster1-02_clus_2   local-only              Cluster
cluster1  cluster_mgmt         broadcast-domain-wide   Default
cluster1  cluster1-01_mgmt1    local-only              Default
cluster1  cluster1-02_mgmt1    local-only              Default
vs1       data1                disabled                Default
vs3       data2                system-defined          group2
```

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

Afficher les cibles de basculement de LIF ONTAP

Vous devrez peut-être vérifier si les stratégies de basculement et les groupes de basculement d'une LIF sont correctement configurés. Pour éviter les erreurs de configuration des règles de basculement, vous pouvez afficher les cibles de basculement d'une seule LIF ou de toutes les LIF.

Description de la tâche

L'affichage des cibles de basculement LIF vous permet de vérifier les points suivants :

- Indique si les LIF sont configurées avec le bon groupe de basculement et la règle de basculement
- Si la liste des ports cibles de basculement obtenue est appropriée pour chaque LIF
- Si la cible de basculement d'une LIF de données n'est pas un port de gestion (e0M)

Étape

Afficher les cibles de basculement d'une LIF à l'aide du `failover` de la `network interface show` commande.

La commande suivante affiche des informations sur les cibles de basculement pour toutes les LIFs d'un cluster à deux nœuds. Le `Failover Targets` Ligne affiche la liste (hiérarchisée) de combinaisons nœud-port pour une LIF donnée.

```
network interface show -failover
         Logical       Home                  Failover        Failover
Vserver  Interface     Node:Port             Policy          Group
-------- ------------ --------------------- --------------- ---------
Cluster
         node1_clus1   node1:e0a             local-only      Cluster
                       Failover Targets: node1:e0a,
                                         node1:e0b
         node1_clus2   node1:e0b             local-only      Cluster
                       Failover Targets: node1:e0b,
                                         node1:e0a
         node2_clus1   node2:e0a             local-only      Cluster
                       Failover Targets: node2:e0a,
                                         node2:e0b
         node2_clus2   node2:e0b             local-only      Cluster
                       Failover Targets: node2:e0b,
                                         node2:e0a
cluster1
         cluster_mgmt  node1:e0c             broadcast-domain-wide
                                                             Default
                       Failover Targets: node1:e0c,
                                         node1:e0d,
                                         node2:e0c,
                                         node2:e0d
         node1_mgmt1   node1:e0c             local-only      Default
                       Failover Targets: node1:e0c,
                                         node1:e0d
         node2_mgmt1   node2:e0c             local-only      Default
                       Failover Targets: node2:e0c,
                                         node2:e0d
vs1
         data1         node1:e0e             system-defined  bcast1
                       Failover Targets: node1:e0e,
                                         node1:e0f,
                                         node2:e0e,
                                         node2:e0f
```

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

Afficher les LIFs ONTAP dans une zone d'équilibrage de la charge

Vous pouvez vérifier si une zone d'équilibrage de charge est correctement configurée en affichant toutes les LIFs qui l'appartiennent. Vous pouvez également afficher la zone d'équilibrage de la charge d'une LIF particulière ou les zones d'équilibrage de la charge pour toutes les LIFs.

Étape

Afficher les LIFs et les détails d'équilibrage de charge que vous recherchez à l'aide de l'une des commandes suivantes

Pour afficher…	Entrer…
LIF dans une zone d'équilibrage de charge spécifique	`network interface show -dns-zone zone_name` `zone_name` spécifie le nom de la zone d'équilibrage de charge.
La zone d'équilibrage de charge d'une LIF particulière	`network interface show -lif lif_name -fields dns-zone`
Les zones d'équilibrage de la charge de tous les LIFs	`network interface show -fields dns-zone`

Exemples d'affichage des zones d'équilibrage de charge pour les LIF

La commande suivante affiche le détail de toutes les LIFs de la zone d'équilibrage de la charge storage.company.com pour SVM vs0 :

```
net int show -vserver vs0 -dns-zone storage.company.com

         Logical    Status     Network           Current   Current Is
Vserver  Interface  Admin/Oper Address/Mask      Node      Port    Home
-------- ---------- ---------- ----------------- --------- ------- ----
vs0
         lif3         up/up    10.98.226.225/20  ndeux-11  e0c     true
         lif4         up/up    10.98.224.23/20   ndeux-21  e0c     true
         lif5         up/up    10.98.239.65/20   ndeux-11  e0c     true
         lif6         up/up    10.98.239.66/20   ndeux-11  e0c     true
         lif7         up/up    10.98.239.63/20   ndeux-21  e0c     true
         lif8         up/up    10.98.239.64/20   ndeux-21  e0c     true
```

La commande suivante affiche les détails de la zone DNS du datas3 :

```
network interface show -lif data3 -fields dns-zone
Vserver  lif    dns-zone
-------  -----  --------
vs0      data3  storage.company.com
```

La commande suivante affiche la liste de toutes les LIFs du cluster et leurs zones DNS correspondantes :

```
network interface show -fields dns-zone
Vserver   lif          dns-zone
-------   ------------ --------
cluster   cluster_mgmt none
ndeux-21  clus1        none
ndeux-21  clus2        none
ndeux-21  mgmt1        none
vs0       data1        storage.company.com
vs0       data2        storage.company.com
```

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

Affichez les connexions du cluster ONTAP

Vous pouvez afficher toutes les connexions actives du cluster ou un nombre de connexions actives sur le nœud par client, interface logique, protocole ou service. Vous pouvez également afficher toutes les connexions d'écoute dans le cluster.

Affichage des connexions actives par le client (administrateurs du cluster uniquement)

Vous pouvez afficher les connexions actives par client pour vérifier le nœud qu'un client spécifique utilise et pour afficher les écarts possibles entre le nombre de clients par nœud.

Description de la tâche

Le nombre de connexions actives par client est utile dans les scénarios suivants :

- Recherche d'un nœud occupé ou surchargé.
- Déterminer pourquoi l'accès d'un client à un volume est lent.

  Vous pouvez afficher des informations sur le nœud auquel le client accède, puis les comparer avec le nœud sur lequel réside le volume. Si l'accès au volume nécessite la gestion du réseau en cluster, les performances des clients peuvent être réduites en raison de l'accès à distance au volume sur un nœud distant sursouscrit.

- Vérification de l'utilisation de tous les nœuds identique pour l'accès aux données.
- Détection des clients disposant d'un nombre de connexions élevé de manière inattendue.
- Vérifier si certains clients ont des connexions à un nœud.

Étape

Affiche le nombre de connexions actives par client sur un nœud à l'aide du `network connections active show-clients` commande.

Pour en savoir plus, `network connections active show-clients` consultez le "Référence de commande ONTAP".

```
network connections active show-clients
Node    Vserver Name    Client IP Address     Count
------  --------------  -----------------     ------
node0   vs0             192.0.2.253               1
        vs0             192.0.2.252               2
        Cluster         192.10.2.124              5
node1   vs0             192.0.2.250               1
        vs0             192.0.2.252               3
        Cluster         192.10.2.123              4
node2   vs1             customer.example.com      1
        vs1             192.0.2.245               3
        Cluster         192.10.2.122              4
node3   vs1             customer.example.org      1
        vs1             customer.example.net      3
        Cluster         192.10.2.121              4
```

Affichage des connexions actives par protocole (administrateurs du cluster uniquement)

Vous pouvez afficher un nombre de connexions actives par protocole (TCP ou UDP) sur un nœud afin de comparer l'utilisation des protocoles au sein du cluster.

Description de la tâche

Le nombre de connexions actives par protocole est utile dans les scénarios suivants :

- Recherche des clients UDP qui perdent leur connexion.

  Si un nœud se trouve à proximité de sa limite de connexion, les clients UDP sont les premiers à être abandonnés.

- Vérification qu'aucun autre protocole n'est utilisé

Étape

Affiche le nombre de connexions actives par protocole sur un nœud à l'aide de `network connections active show-protocols` commande.

Pour en savoir plus, `network connections active show-protocols` consultez le "Référence de commande ONTAP".

```
network connections active show-protocols
Node     Vserver Name  Protocol   Count
-------  ------------  ---------  ------
node0
         vs0           UDP            19
         Cluster       TCP            11
node1
         vs0           UDP            17
         Cluster       TCP             8
node2
         vs1           UDP            14
         Cluster       TCP            10
node3
         vs1           UDP            18
         Cluster       TCP             4
```

Affichage des connexions actives par service (administrateurs du cluster uniquement)

Vous pouvez afficher un nombre de connexions actives par type de service (par exemple, par NFS, SMB, montage, etc.) pour chaque nœud d'un cluster. Cette fonction est utile pour comparer l'utilisation des services au sein du cluster, ce qui permet de déterminer la charge de travail principale d'un nœud.

Description de la tâche

Le nombre de connexions actives par service est utile dans les scénarios suivants :

- Vérifier que tous les nœuds sont utilisés pour les services appropriés et que l'équilibrage de la charge pour ce service fonctionne.
- Vérifier qu'aucun autre service n'est utilisé. Affiche le nombre de connexions actives par service sur un nœud à l'aide du `network connections active show-services` commande.

Pour en savoir plus, `network connections active show-services` consultez le "Référence de commande ONTAP".

```
network connections active show-services
Node        Vserver Name    Service    Count
---------  --------------  ---------  ------
node0
            vs0             mount           3
            vs0             nfs            14
            vs0             nlm_v4          4
            vs0             cifs_srv        3
            vs0             port_map       18
            vs0             rclopcp        27
            Cluster         ctlopcp        60
node1
            vs0             cifs_srv        3
            vs0             rclopcp        16
            Cluster         ctlopcp        60
node2
            vs1             rclopcp        13
            Cluster         ctlopcp        60
node3
            vs1             cifs_srv        1
            vs1             rclopcp        17
            Cluster         ctlopcp        60
```

Afficher les connexions actives par LIF sur un nœud et un SVM

Vous pouvez afficher un nombre de connexions actives pour chaque LIF, par nœud et SVM (Storage Virtual machine), afin d'afficher les déséquilibres de connexion entre les LIF au sein du cluster.

Description de la tâche

Le nombre de connexions actives par LIF est utile dans les scénarios suivants :

- Trouver une LIF surchargée en comparant le nombre de connexions sur chaque LIF.
- Vérification du fonctionnement de l'équilibrage de la charge DNS pour toutes les LIFs de données.
- Comparaison du nombre de connexions aux différents SVM pour trouver les SVM les plus utilisés.

Étape

Afficher le nombre de connexions actives pour chaque LIF par SVM et nœud en utilisant le `network connections active show-lifs` commande.

Pour en savoir plus, `network connections active show-lifs` consultez le "Référence de commande ONTAP".

```
network connections active show-lifs
Node      Vserver Name  Interface Name  Count
--------  ------------  --------------- ------
node0
          vs0           datalif1             3
          Cluster       node0_clus_1         6
          Cluster       node0_clus_2         5
node1
          vs0           datalif2             3
          Cluster       node1_clus_1         3
          Cluster       node1_clus_2         5
node2
          vs1           datalif2             1
          Cluster       node2_clus_1         5
          Cluster       node2_clus_2         3
node3
          vs1           datalif1             1
          Cluster       node3_clus_1         2
          Cluster       node3_clus_2         2
```

Affiche les connexions actives dans un cluster

Vous pouvez afficher des informations sur les connexions actives dans un cluster pour afficher les LIF, le port, l'hôte distant, le service, les SVM (Storage Virtual machines) et le protocole utilisé par des connexions individuelles.

Description de la tâche

L'affichage des connexions actives dans un cluster est utile dans les scénarios suivants :

- Vérifier que chaque client utilise le protocole et le service appropriés sur le nœud.
- Si un client rencontre des difficultés pour accéder aux données à l'aide d'une certaine combinaison de nœud, de protocole et de service, vous pouvez utiliser cette commande pour trouver un client similaire pour la comparaison de la configuration ou de la trace des paquets.

Étape

Afficher les connexions actives dans un cluster à l'aide du `network connections active show` commande.

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

La commande suivante affiche les connexions actives sur le nœud node1 :

```
network connections active show -node node1
Vserver  Interface           Remote
Name     Name:Local Port     Host:Port           Protocol/Service
-------  ------------------  ------------------  ---------------
Node: node1
Cluster  node1_clus_1:50297  192.0.2.253:7700    TCP/ctlopcp
Cluster  node1_clus_1:13387  192.0.2.253:7700    TCP/ctlopcp
Cluster  node1_clus_1:8340   192.0.2.252:7700    TCP/ctlopcp
Cluster  node1_clus_1:42766  192.0.2.252:7700    TCP/ctlopcp
Cluster  node1_clus_1:36119  192.0.2.250:7700    TCP/ctlopcp
vs1      data1:111           host1.aa.com:10741  UDP/port-map
vs3      data2:111           host1.aa.com:10741  UDP/port-map
vs1      data1:111           host1.aa.com:12017  UDP/port-map
vs3      data2:111           host1.aa.com:12017  UDP/port-map
```

La commande suivante montre les connexions actives sur le SVM vs1 :

```
network connections active show -vserver vs1
Vserver  Interface           Remote
Name     Name:Local Port     Host:Port           Protocol/Service
-------  ------------------  ------------------  ---------------
Node: node1
vs1      data1:111           host1.aa.com:10741  UDP/port-map
vs1      data1:111           host1.aa.com:12017  UDP/port-map
```

Affiche les connexions d'écoute dans un cluster

Vous pouvez afficher les informations relatives aux connexions d'écoute dans un cluster pour afficher les LIFs et les ports qui acceptent les connexions pour un protocole et un service donnés.

Description de la tâche

L'affichage des connexions d'écoute dans un cluster est utile dans les scénarios suivants :

- Vérifier que le protocole ou le service désiré est à l'écoute d'une LIF si les connexions client à cette LIF échouent de manière cohérente.
- Vérification de l'ouverture d'un écouteur UDP/rclopcp au niveau de chaque LIF du cluster si l'accès des données à distance à un volume sur un nœud via une LIF sur un autre nœud échoue.
- Vérifier qu'un écouteur UDP/rclopcp est ouvert au niveau de chaque LIF du cluster si le transfert SnapMirror entre deux nœuds du même cluster échoue.
- Vérifier qu'un écouteur TCP/ctlopcp est ouvert sur chaque LIF intercluster si les transferts SnapMirror entre deux nœuds de différents clusters échouent.

Étape

Affichez les connexions d'écoute par nœud à l'aide du `network connections listening show` commande.

```
network connections listening show
Vserver Name     Interface Name:Local Port        Protocol/Service
---------------- -------------------------------  ----------------
Node: node0
Cluster          node0_clus_1:7700                TCP/ctlopcp
vs1              data1:4049                       UDP/unknown
vs1              data1:111                        TCP/port-map
vs1              data1:111                        UDP/port-map
vs1              data1:4046                       TCP/sm
vs1              data1:4046                       UDP/sm
vs1              data1:4045                       TCP/nlm-v4
vs1              data1:4045                       UDP/nlm-v4
vs1              data1:2049                       TCP/nfs
vs1              data1:2049                       UDP/nfs
vs1              data1:635                        TCP/mount
vs1              data1:635                        UDP/mount
Cluster          node0_clus_2:7700                TCP/ctlopcp
```

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

Commandes ONTAP pour diagnostiquer les problèmes réseau

Vous pouvez diagnostiquer des problèmes sur votre réseau à l'aide de commandes telles que `ping`, `traceroute`, `ndp`, et `tcpdump`. Vous pouvez également utiliser des commandes comme `ping6` et `traceroute6` Pour diagnostiquer les problèmes IPv6.

Les fonctions que vous recherchez…	Entrez cette commande…
Vérifiez si le nœud peut atteindre d'autres hôtes sur votre réseau	`network ping`
Vérifiez si le nœud peut atteindre d'autres hôtes sur votre réseau IPv6	`network ping6`
Suivez la route que les paquets IPv4 prennent à un nœud réseau	`network traceroute`
Suivez la route que les paquets IPv6 prennent sur un nœud réseau	`network traceroute6`
Gérer le Protocole de découverte des voisins (NPD)	`network ndp`
Affiche des statistiques sur les paquets reçus et envoyés sur une interface réseau spécifiée ou sur toutes les interfaces réseau	`run -node` *`node_name`* `ifstat` **Note**: Cette commande est disponible à partir du nodeshell.

Affiche des informations sur les périphériques voisins découverts à partir de chaque nœud et port du cluster, y compris le type de périphérique distant et la plate-forme de périphérique	`network device-discovery show`
Afficher les voisins CDP du nœud (ONTAP prend uniquement en charge les publicités CDPv1)	`run -node node_name cdpd show-neighbors` **Note**: Cette commande est disponible à partir du nodeshell.
Suivez les paquets envoyés et reçus sur le réseau	`network tcpdump start -node node-name -port port_name` **Note**: Cette commande est disponible à partir du nodeshell.
Mesure de la latence et du débit entre les nœuds intercluster ou intracluster	`network test -path -source-node source_nodename local -destination -cluster destination_clustername -destination-node destination_nodename -session-type Default, AsyncMirrorLocal, AsyncMirrorRemote, SyncMirrorRemote, or RemoteDataTransfer` Pour plus d'informations, reportez-vous à la section "Gestion des performances".

Informations associées

- "Référence de commande ONTAP"
- "ping réseau"
- "route du réseau"
- "network device-discovery show"
- "réseau npd"

Afficher la connectivité réseau avec les protocoles de détection de voisins

Affichez la connectivité réseau ONTAP avec les protocoles de détection de voisins

Dans un data Center, vous pouvez utiliser des protocoles de découverte voisins pour afficher la connectivité réseau entre une paire de systèmes physiques ou virtuels et leurs interfaces réseau. ONTAP prend en charge deux protocoles de découverte de voisins : le Cisco Discovery Protocol (CDP) et le Link Layer Discovery Protocol (LLDP).

Les protocoles de détection de voisins vous permettent de détecter et d'afficher automatiquement des informations sur les périphériques compatibles avec des protocoles directement connectés sur un réseau. Chaque appareil transmet des informations d'identification, de fonctionnalités et de connectivité. Ces informations sont transmises en trames Ethernet à une adresse MAC multicast et sont reçues par tous les périphériques compatibles avec les protocoles voisins.

Pour que deux périphériques deviennent voisins, un protocole doit être activé et correctement configuré. La fonctionnalité du protocole de découverte est limitée aux réseaux directement connectés. Les voisins peuvent

inclure des périphériques compatibles avec les protocoles, tels que des commutateurs, des routeurs, des ponts, etc. ONTAP prend en charge deux protocoles de détection de voisins, qui peuvent être utilisés individuellement ou conjointement.

Cisco Discovery Protocol (CDP)

CDP est un protocole propriétaire de couche de liaison développé par Cisco Systems. Il est activé par défaut dans ONTAP pour les ports de cluster, mais il doit être activé explicitement pour les ports de données.

Protocole LLDP (Link Layer Discovery Protocol)

LLDP est un protocole indépendant du fournisseur spécifié dans le document de normes IEEE 802.1AB. Elle doit être activée explicitement pour tous les ports.

Utilisez CDP pour détecter la connectivité réseau ONTAP

L'utilisation de CDP pour détecter la connectivité réseau consiste à examiner les considérations relatives au déploiement, à l'activer sur les ports de données, à afficher les périphériques voisins et à ajuster les valeurs de configuration CDP selon les besoins. Le protocole CDP est activé par défaut sur les ports du cluster.

Le protocole CDP doit également être activé sur tous les commutateurs et routeurs avant que les informations relatives aux périphériques voisins puissent être affichées.

Version de ONTAP	Description
9.10.1 et versions antérieures	Le protocole CDP est également utilisé par le contrôle de l'état du switch du cluster pour détecter automatiquement les commutateurs du cluster et du réseau de gestion.
9.11.1 et versions ultérieures	Le protocole CDP est également utilisé par le contrôle de l'état du switch du cluster pour détecter automatiquement les commutateurs du cluster, du stockage et du réseau de gestion.

Informations associées

"Administration du système"

Considérations relatives à l'utilisation de CDP

Par défaut, les périphériques compatibles CDP envoient des publicités CDPv2. Les appareils compatibles CDP envoient des publicités CDPv1 uniquement lorsqu'ils reçoivent des publicités CDPv1. ONTAP ne prend en charge que CDPv1. Par conséquent, lorsqu'un nœud ONTAP envoie des publicités CDPv1, les périphériques voisins compatibles CDP envoient des publicités CDPv1.

Avant d'activer le CDP sur un nœud, tenez compte des informations suivantes :

- Tous les ports CDP sont pris en charge.
- Les publicités CDP sont envoyées et reçues par les ports qui sont à l'état up.
- Le CDP doit être activé sur les appareils d'émission et de réception pour l'envoi et la réception de publicités CDP.
- Les annonces CDP sont envoyées à intervalles réguliers et vous pouvez configurer l'intervalle de temps.

- Lorsque les adresses IP sont modifiées pour une LIF, le nœud envoie les informations mises à jour dans la prochaine publicité CDP.
- ONTAP 9.10.1 et versions antérieures :
  - Le protocole CDP est toujours activé sur les ports du cluster.
  - Le protocole CDP est désactivé par défaut sur tous les ports qui ne sont pas du cluster.
- ONTAP 9.11.1 et versions ultérieures :
  - Le protocole CDP est toujours activé sur les ports du cluster et de stockage.
  - Par défaut, le protocole CDP est désactivé sur tous les ports non-cluster et non-stockage.

> Parfois, lorsque les LIFs sont modifiées sur le nœud, les informations du CDP ne sont pas mises à jour côté du périphérique de réception (par exemple, un switch). Si vous rencontrez un tel problème, vous devez configurer l'interface réseau du nœud sur l'état down, puis sur l'état up.

- Seules les adresses IPv4 sont annoncées dans les publicités CDP.
- Pour les ports réseau physique avec des VLAN, toutes les LIF configurées sur ce port sont annoncées.
- Pour les ports physiques faisant partie d'un groupe d'interfaces, toutes les adresses IP configurées sur ce groupe d'interfaces sont annoncées sur chaque port physique.
- Pour un groupe d'interface qui héberge les VLAN, toutes les LIF configurées sur le groupe d'interface et les VLAN sont annoncés sur chacun des ports réseau.
- En raison de la restriction des paquets CDP à 1500 octets maximum, sur les ports Configuré avec un grand nombre de LIF, seul un sous-ensemble de ces adresses IP peut être signalé sur le commutateur adjacent.

Activer ou désactiver CDP

Pour détecter et envoyer des publicités aux périphériques voisins conformes à la norme CDP, le protocole CDP doit être activé sur chaque nœud du cluster.

Par défaut dans ONTAP 9.10.1 et versions antérieures, CDP est activée sur tous les ports de cluster d'un nœud et désactivée sur tous les ports qui ne sont pas du cluster d'un nœud.

Par défaut dans ONTAP 9.11.1 et versions ultérieures, CDP est activée sur l'ensemble du cluster et des ports de stockage d'un nœud et désactivée sur tous les ports non-cluster et non-stockage d'un nœud.

Description de la tâche

Le `cdpd.enable` Option contrôle si CDP est activée ou désactivée sur les ports d'un nœud :

- Pour les versions ONTAP 9.10.1 et antérieures, on active le CDP sur les ports hors cluster.
- Pour les versions ONTAP 9.11.1 et ultérieures, on active le CDP sur les ports non-cluster et non-stockage.
- Pour les versions ONTAP 9.10.1 et antérieures, off désactive le protocole CDP sur les ports hors cluster ; vous ne pouvez pas désactiver le protocole CDP sur les ports de cluster.
- Pour ONTAP 9.11.1 et versions ultérieures, off désactive le protocole CDP sur les ports non-cluster et non-stockage ; vous ne pouvez pas désactiver le protocole CDP sur les ports du cluster.

Lorsque le protocole CDP est désactivé sur un port connecté à un périphérique compatible CDP, le trafic réseau peut ne pas être optimisé.

Étapes

1. Afficher le paramètre CDP actuel d'un nœud ou de tous les nœuds d'un cluster :

Pour afficher le paramètre CDP de…	Entrer…
Un nœud	`run - node <node_name> options cdpd.enable`
Tous les nœuds d'un cluster	`options cdpd.enable`

2. Activer ou désactiver CDP sur tous les ports d'un nœud, ou sur tous les ports de tous les nœuds d'un cluster :

Pour activer ou désactiver CDP sur…	Entrer…
Un nœud	`run -node node_name options cdpd.enable {on or off}`
Tous les nœuds d'un cluster	`options cdpd.enable {on or off}`

Afficher les informations sur les voisins CDP

Vous pouvez afficher des informations sur les périphériques voisins qui sont connectés à chaque port des nœuds de votre cluster, à condition que le port soit connecté à un périphérique compatible CDP. Vous pouvez utiliser `network device-discovery show -protocol cdp` la commande pour afficher les informations relatives aux voisins. Pour en savoir plus, `network device-discovery show` consultez le "Référence de commande ONTAP".

Description de la tâche

Dans les versions ONTAP 9.10.1 et antérieures, étant donné que le protocole CDP est toujours activé pour les ports de cluster, les informations des voisins CDP sont toujours affichées pour ces ports. Le protocole CDP doit être activé sur des ports autres que le cluster pour que les informations relatives aux voisins s'affichent sur ces ports.

Dans la version ONTAP 9.11.1 et ultérieure, étant donné que le protocole CDP est toujours activé pour les ports de cluster et de stockage, les informations des voisins CDP sont toujours affichées pour ces ports. Le protocole CDP doit être activé sur les ports non-cluster et non-stockage afin que les informations relatives aux voisins s'affichent pour ces ports.

Étape

Affiche des informations sur tous les appareils compatibles CDP connectés aux ports d'un nœud du cluster :

```
network device-discovery show -node node -protocol cdp
```

La commande suivante indique les voisins connectés aux ports du nœud sti2650-212 :

```
network device-discovery show -node sti2650-212 -protocol cdp
Node/       Local  Discovered
Protocol    Port   Device (LLDP: ChassisID)  Interface         Platform
----------- ------ ------------------------- ----------------
----------------
sti2650-212/cdp
            e0M    RTP-LF810-510K37.gdl.eng.netapp.com(SAL1942R8JS)
                                             Ethernet1/14      N9K-
C93120TX
            e0a    CS:RTP-CS01-510K35        0/8               CN1610
            e0b    CS:RTP-CS01-510K36        0/8               CN1610
            e0c    RTP-LF350-510K34.gdl.eng.netapp.com(FDO21521S76)
                                             Ethernet1/21      N9K-
C93180YC-FX
            e0d    RTP-LF349-510K33.gdl.eng.netapp.com(FDO21521S4T)
                                             Ethernet1/22      N9K-
C93180YC-FX
            e0e    RTP-LF349-510K33.gdl.eng.netapp.com(FDO21521S4T)
                                             Ethernet1/23      N9K-
C93180YC-FX
            e0f    RTP-LF349-510K33.gdl.eng.netapp.com(FDO21521S4T)
                                             Ethernet1/24      N9K-
C93180YC-FX
```

La sortie répertorie les périphériques Cisco connectés à chaque port du nœud spécifié.

Configurez la durée de mise en attente des messages CDP

La durée de conservation correspond à la période pendant laquelle les publicités CDP sont stockées en cache sur les périphériques compatibles CDP voisins. Le temps de mise en attente est annoncé dans chaque paquet CDPv1 et mis à jour chaque fois qu'un paquet CDPv1 est reçu par un noeud.

- La valeur du `cdpd.holdtime` L'option doit être définie sur la même valeur sur les deux nœuds d'une paire HA.
- La valeur par défaut du temps de maintien est de 180 secondes, mais vous pouvez entrer des valeurs comprises entre 10 secondes et 255 secondes.
- Si une adresse IP est supprimée avant l'expiration du délai de mise en attente, les informations CDP sont mises en cache jusqu'à ce que le délai de mise en attente expire.

Étapes

1. Afficher l'heure de maintien CDP actuelle d'un nœud ou de tous les nœuds d'un cluster :

Pour afficher le temps de maintien de…	Entrer…
Un nœud	`run -node node_name options cdpd.holdtime`

Tous les nœuds d'un cluster	`options cdpd.holdtime`

2. Configurer le délai de mise en attente du CDP sur tous les ports d'un nœud ou sur tous les ports de tous les nœuds d'un cluster :

Pour activer le temps de maintien…	Entrer…
Un nœud	`run -node node_name options cdpd.holdtime holdtime`
Tous les nœuds d'un cluster	`options cdpd.holdtime holdtime`

Définissez l'intervalle d'envoi de publicités CDP

Les publicités CDP sont envoyées régulièrement aux voisins CDP. Vous pouvez augmenter ou réduire l'intervalle d'envoi de publicités CDP en fonction du trafic réseau et des modifications de la topologie réseau.

- La valeur du `cdpd.interval` L'option doit être définie sur la même valeur sur les deux nœuds d'une paire HA.
- L'intervalle par défaut est de 60 secondes, mais vous pouvez entrer une valeur de 5 à 900 secondes.

Étapes

1. Afficher l'intervalle de temps publicitaire du CDP actuel pour un nœud ou pour tous les nœuds d'un cluster :

Pour afficher l'intervalle de…	Entrer…
Un nœud	`run -node node_name options cdpd.interval`
Tous les nœuds d'un cluster	`options cdpd.interval`

2. Configurer l'intervalle d'envoi de publicités CDP pour tous les ports d'un nœud ou pour tous les ports de tous les nœuds d'un cluster :

Pour définir l'intervalle de…	Entrer…
Un nœud	`run -node node_name options cdpd.interval interval`
Tous les nœuds d'un cluster	`options cdpd.interval interval`

Afficher ou effacer les statistiques CDP

Vous pouvez afficher les statistiques CDP des ports du cluster et non du cluster sur chaque nœud afin de détecter d'éventuels problèmes de connectivité réseau. Les statistiques CDP sont cumulatives à partir de leur dernière suppression.

Description de la tâche

Dans les versions ONTAP 9.10.1 et antérieures, étant donné que le protocole CDP est toujours activé pour les ports, les statistiques CDP sont toujours affichées pour le trafic sur ces ports. Le protocole CDP doit être activé sur les ports pour que les statistiques apparaissent sur ces ports.

Dans les versions ONTAP 9.11.1 et ultérieures, puisque le CDP est toujours activé pour les ports du cluster et de stockage, les statistiques CDP sont toujours affichées pour le trafic sur ces ports. Le protocole CDP doit être activé sur des ports non-cluster ou non-Storage pour que les statistiques de ces ports s'affichent.

Étape

Afficher ou effacer les statistiques CDP actuelles de tous les ports d'un nœud :

Les fonctions que vous recherchez…	Entrer…
Afficher les statistiques CDP	`run -node node_name cdpd show-stats`
Effacer les statistiques CDP	`run -node node_name cdpd zero-stats`

Exemple d'affichage et d'effacement des statistiques

La commande suivante affiche les statistiques CDP avant leur effacement. La sortie affiche le nombre total de paquets envoyés et reçus depuis la dernière suppression des statistiques.

```
run -node node1 cdpd show-stats

RECEIVE
 Packets:          9116  | Csum Errors:        0  | Unsupported Vers:  4561
 Invalid length:      0  | Malformed:          0  | Mem alloc fails:      0
 Missing TLVs:        0  | Cache overflow:     0  | Other errors:         0

TRANSMIT
 Packets:          4557  | Xmit fails:         0  | No hostname:          0
 Packet truncated:    0  | Mem alloc fails:    0  | Other errors:         0

OTHER
 Init failures:       0
```

La commande suivante efface les statistiques CDP :

```
run -node node1 cdpd zero-stats
```

```
run -node node1 cdpd show-stats

RECEIVE
 Packets:            0  | Csum Errors:       0  | Unsupported Vers:     0
 Invalid length:     0  | Malformed:         0  | Mem alloc fails:      0
 Missing TLVs:       0  | Cache overflow:    0  | Other errors:         0

TRANSMIT
 Packets:            0  | Xmit fails:        0  | No hostname:          0
 Packet truncated:   0  | Mem alloc fails:   0  | Other errors:         0

OTHER
 Init failures:      0
```

Une fois les statistiques effacées, elles commencent à s'accumuler après l'envoi ou la réception de la prochaine annonce CDP.

Connexion à des commutateurs Ethernet qui ne prennent pas en charge CDP

Plusieurs commutateurs de fournisseurs ne prennent pas en charge CDP. Voir le"Base de connaissances NetApp : la détection de périphériques ONTAP affiche les nœuds au lieu du commutateur" pour plus de détails.

Il existe deux options pour résoudre ce problème :

- Désactivez CDP et activez LLDP, si pris en charge. Voir "Utilisez LLDP pour détecter la connectivité réseau" pour plus d'informations.
- Configurez un filtre de paquets d'adresses MAC sur les commutateurs pour abandonner les annonces CDP.

Utilisez LLDP pour détecter la connectivité réseau ONTAP

L'utilisation du protocole LLDP pour détecter la connectivité réseau consiste à examiner les considérations de déploiement, à l'activer sur tous les ports, à visualiser les périphériques voisins et à ajuster les valeurs de configuration LLDP si nécessaire.

Le protocole LLDP doit également être activé sur tous les commutateurs et routeurs avant que des informations sur les périphériques voisins puissent être affichées.

ONTAP indique actuellement les structures de valeur de type-longueur (TLV) suivantes :

- ID de châssis
- ID de port
- Durée de vie (TTL)
- Nom du système

  Le nom système TLV n'est pas envoyé sur les périphériques CNA.

Certains adaptateurs réseau convergés (CNA), tels que l'adaptateur X1143 et les ports intégrés UTA2,

contiennent la prise en charge de l'allègement de la charge pour le protocole LLDP :

- Le déchargement LLDP est utilisé pour le pontage du Data Center (DCB).
- Les informations affichées peuvent différer entre le cluster et le commutateur.

  Les données d'ID de châssis et de port affichées par le commutateur peuvent être différentes pour les ports CNA et non CNA.

Par exemple :

- Pour les ports non CNA :
  - L'ID de châssis est une adresse MAC fixe de l'un des ports du nœud
  - ID de port correspond au nom du port respectif sur le nœud
- Pour les ports CNA :
  - L'ID de châssis et l'ID de port sont les adresses MAC des ports respectifs du nœud.

Cependant, les données affichées par le cluster sont cohérentes pour ces types de port.

> La spécification LLDP définit l'accès aux informations collectées via une MIB SNMP. Cependant, ONTAP ne supporte pas actuellement la MIB LLDP.

Activer ou désactiver le protocole LLDP

Pour détecter et envoyer des publicités aux périphériques voisins conformes au protocole LLDP, LLDP doit être activé sur chaque nœud du cluster. Depuis ONTAP 9.7, LLDP est activé par défaut sur tous les ports d'un nœud.

Description de la tâche

Pour ONTAP 9.10.1 et versions antérieures, le `lldp.enable` Option contrôle si LLDP est activé ou désactivé sur les ports d'un nœud :

- `on` Active LLDP sur tous les ports.
- `off` Désactive LLDP sur tous les ports.

Pour ONTAP 9.11.1 et versions ultérieures, le `lldp.enable` Option contrôle si LLDP est activé ou désactivé sur les ports non-cluster et non-stockage d'un nœud :

- `on` Active LLDP sur tous les ports non-cluster et non-stockage.
- `off` Désactive LLDP sur tous les ports non-cluster et non-stockage.

Étapes

1. Afficher le paramètre LLDP actuel pour un nœud ou pour tous les nœuds d'un cluster :
   - Un seul nœud : `run -node node_name options lldp.enable`
   - Tous les nœuds : options `lldp.enable`
2. Activer ou désactiver le protocole LLDP sur tous les ports d'un nœud ou sur tous les ports de tous les nœuds d'un cluster :

Pour activer ou désactiver LLDP activé…	Entrer…
Un nœud	`run -node node_name options lldp.enable {on
off}`	Tous les nœuds d'un cluster
`options lldp.enable {on	off}`

- Un seul nœud :

```
run -node node_name options lldp.enable {on|off}
```

- Tous les nœuds :

```
options lldp.enable {on|off}
```

Afficher les informations de voisinage LLDP

Vous pouvez afficher des informations sur les périphériques voisins qui sont connectés à chaque port des nœuds de votre cluster, à condition que le port soit connecté à un périphérique compatible LLDP. Vous utilisez la commande network device-Discovery show pour afficher les informations relatives aux voisins.

Étape

1. Affiche des informations sur tous les périphériques conformes au protocole LLDP connectés aux ports d'un nœud du cluster :

```
network device-discovery show -node node -protocol lldp
```

La commande suivante affiche les voisins connectés aux ports du nœud cluster-1_01. La sortie répertorie les périphériques compatibles LLDP qui sont connectés à chaque port du nœud spécifié. Si le `-protocol` Option omise, la sortie répertorie également les périphériques compatibles CDP.

```
network device-discovery show -node cluster-1_01 -protocol lldp
Node/       Local  Discovered
Protocol    Port   Device                    Interface         Platform
----------- ------ ------------------------- ----------------
----------------
cluster-1_01/lldp
            e2a    0013.c31e.5c60            GigabitEthernet1/36
            e2b    0013.c31e.5c60            GigabitEthernet1/35
            e2c    0013.c31e.5c60            GigabitEthernet1/34
            e2d    0013.c31e.5c60            GigabitEthernet1/33
```

Réglez l'intervalle de transmission des annonces LLDP

Les annonces du LLDP sont envoyées à intervalles réguliers aux voisins du LLDP. Vous pouvez augmenter ou diminuer l'intervalle d'envoi des annonces LLDP en fonction du trafic réseau et des modifications de la topologie du réseau.

Description de la tâche

L'intervalle par défaut recommandé par IEEE est de 30 secondes, mais vous pouvez entrer une valeur de 5 secondes à 300 secondes.

Étapes

1. Afficher l'intervalle de temps de publicité LLDP actuel pour un nœud ou pour tous les nœuds d'un cluster :
   - Un seul nœud :

     ```
     run -node <node_name> options lldp.xmit.interval
     ```

   - Tous les nœuds :

     ```
     options lldp.xmit.interval
     ```

2. Réglez l'intervalle d'envoi des annonces LLDP pour tous les ports d'un nœud ou pour tous les ports de tous les nœuds d'un cluster :
   - Un seul nœud :

     ```
     run -node <node_name> options lldp.xmit.interval <interval>
     ```

   - Tous les nœuds :

     ```
     options lldp.xmit.interval <interval>
     ```

Réglez la valeur de temps de mise en ligne pour les annonces LLDP

Le temps de mise en service (TTL) est la période pendant laquelle les publicités LLDP sont stockées dans le cache dans les périphériques conformes LLDP voisins. TTL est annoncé dans chaque paquet LLDP et mis à jour chaque fois qu'un paquet LLDP est reçu par un nœud. TTL peut être modifié dans les trames LLDP sortantes.

Description de la tâche

- TTL est une valeur calculée, produit de l'intervalle de transmission (`lldp.xmit.interval`) et le multiplicateur hold (`lldp.xmit.hold`) plus un.
- La valeur par défaut du multiplicateur de maintien est 4, mais vous pouvez entrer des valeurs comprises entre 1 et 100.
- Le TTL par défaut est donc de 121 secondes, comme recommandé par l'IEEE, mais en ajustant l'intervalle de transmission et les valeurs multiplicatrices de maintien, vous pouvez spécifier une valeur pour les trames sortantes de 6 à 30001 secondes.

- Si une adresse IP est supprimée avant l'expiration du TTL, les informations LLDP sont mises en cache jusqu'à expiration du TTL.

Étapes

1. Afficher la valeur du multiplicateur de maintien actuel pour un nœud ou pour tous les nœuds d'un cluster :
   - Un seul nœud :

     ```
     run -node <node_name> options lldp.xmit.hold
     ```

   - Tous les nœuds :

     ```
     options lldp.xmit.hold
     ```

2. Ajustez la valeur du multiplicateur de maintien sur tous les ports d'un nœud ou sur tous les ports de tous les nœuds d'un cluster :
   - Un seul nœud :

     ```
     run -node <node_name> options lldp.xmit.hold <hold_value>
     ```

   - Tous les nœuds :

     ```
     options lldp.xmit.hold <hold_value>
     ```

Afficher ou effacer les statistiques LLDP

Vous pouvez afficher les statistiques LLDP pour les ports cluster et non-cluster sur chaque nœud afin de détecter d'éventuels problèmes de connectivité réseau. Les statistiques LLDP sont cumulatives à partir de la dernière fois qu'elles ont été effacées.

Description de la tâche

Pour les versions ONTAP 9.10.1 et antérieures, étant donné que LLDP est toujours activé pour les ports de cluster, les statistiques LLDP sont toujours affichées pour le trafic sur ces ports. Le protocole LLDP doit être activé sur des ports non-cluster pour que les statistiques s'affichent pour ces ports.

Pour ONTAP 9.11.1 et versions ultérieures, étant donné que LLDP est toujours activé pour le cluster et les ports de stockage, les statistiques LLDP sont toujours affichées pour le trafic sur ces ports. Le protocole LLDP doit être activé sur les ports non-cluster et non-stockage pour que les statistiques s'affichent sur ces ports.

Étape

Afficher ou effacer les statistiques actuelles du LLDP pour tous les ports d'un nœud :

Les fonctions que vous recherchez…	Entrer…
Afficher les statistiques LLDP	`run -node node_name lldp stats`

Effacer les statistiques LLDP	`run -node node_name lldp stats -z`

Affiche et efface un exemple de statistiques

La commande suivante affiche les statistiques LLDP avant leur effacement. La sortie affiche le nombre total de paquets envoyés et reçus depuis la dernière suppression des statistiques.

```
cluster-1::> run -node vsim1 lldp stats

RECEIVE
 Total frames:     190k  | Accepted frames:   190k | Total drops:
0
TRANSMIT
 Total frames:     5195  | Total failures:      0
OTHER
 Stored entries:      64
```

La commande suivante efface les statistiques LLDP.

```
cluster-1::> The following command clears the LLDP statistics:
run -node vsim1 lldp stats -z
run -node node1 lldp stats

RECEIVE
 Total frames:        0  | Accepted frames:     0  | Total drops:
0
TRANSMIT
 Total frames:        0  | Total failures:      0
OTHER
 Stored entries:      64
```

Une fois les statistiques effacées, elles commencent à s'accumuler après l'envoi ou la réception de la prochaine annonce du PLLDP.

Informations sur le copyright

Copyright © 2026 NetApp, Inc. Tous droits réservés. Imprimé aux États-Unis. Aucune partie de ce document protégé par copyright ne peut être reproduite sous quelque forme que ce soit ou selon quelque méthode que ce soit (graphique, électronique ou mécanique, notamment par photocopie, enregistrement ou stockage dans un système de récupération électronique) sans l'autorisation écrite préalable du détenteur du droit de copyright.

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

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

NetApp se réserve le droit de modifier les produits décrits dans le présent document à tout moment et sans préavis. NetApp décline toute responsabilité découlant de l'utilisation des produits décrits dans le présent document, sauf accord explicite écrit de NetApp. L'utilisation ou l'achat de ce produit ne concède pas de licence dans le cadre de droits de brevet, de droits de marque commerciale ou de tout autre droit de propriété intellectuelle de NetApp.

Le produit décrit dans ce manuel peut être protégé par un ou plusieurs brevets américains, étrangers ou par une demande en attente.

LÉGENDE DE RESTRICTION DES DROITS : L'utilisation, la duplication ou la divulgation par le gouvernement sont sujettes aux restrictions énoncées dans le sous-paragraphe (b)(3) de la clause Rights in Technical Data-Noncommercial Items du DFARS 252.227-7013 (février 2014) et du FAR 52.227-19 (décembre 2007).

Les données contenues dans les présentes se rapportent à un produit et/ou service commercial (tel que défini par la clause FAR 2.101). Il s'agit de données propriétaires de NetApp, Inc. Toutes les données techniques et tous les logiciels fournis par NetApp en vertu du présent Accord sont à caractère commercial et ont été exclusivement développés à l'aide de fonds privés. Le gouvernement des États-Unis dispose d'une licence limitée irrévocable, non exclusive, non cessible, non transférable et mondiale. Cette licence lui permet d'utiliser uniquement les données relatives au contrat du gouvernement des États-Unis d'après lequel les données lui ont été fournies ou celles qui sont nécessaires à son exécution. Sauf dispositions contraires énoncées dans les présentes, l'utilisation, la divulgation, la reproduction, la modification, l'exécution, l'affichage des données sont interdits sans avoir obtenu le consentement écrit préalable de NetApp, Inc. Les droits de licences du Département de la Défense du gouvernement des États-Unis se limitent aux droits identifiés par la clause 252.227-7015(b) du DFARS (février 2014).

Informations sur les marques commerciales

NETAPP, le logo NETAPP et les marques citées sur le site http://www.netapp.com/TM sont des marques déposées ou des marques commerciales de NetApp, Inc. Les autres noms de marques et de produits sont des marques commerciales de leurs propriétaires respectifs.