



Ports réseau

ONTAP 9

NetApp
April 24, 2024

This PDF was generated from https://docs.netapp.com/fr-fr/ontap/networking/configure_network_ports_@cluster_administrators_only@_overview.html on April 24, 2024. Always check docs.netapp.com for the latest.

Sommaire

- Ports réseau 1
 - Configuration des ports réseau 1
 - Configurez les ports réseau 1

Ports réseau

Configuration des ports réseau

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 *énumérerLetter* :

- 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

Combinaison de ports physiques pour créer des groupes d'interfaces

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.

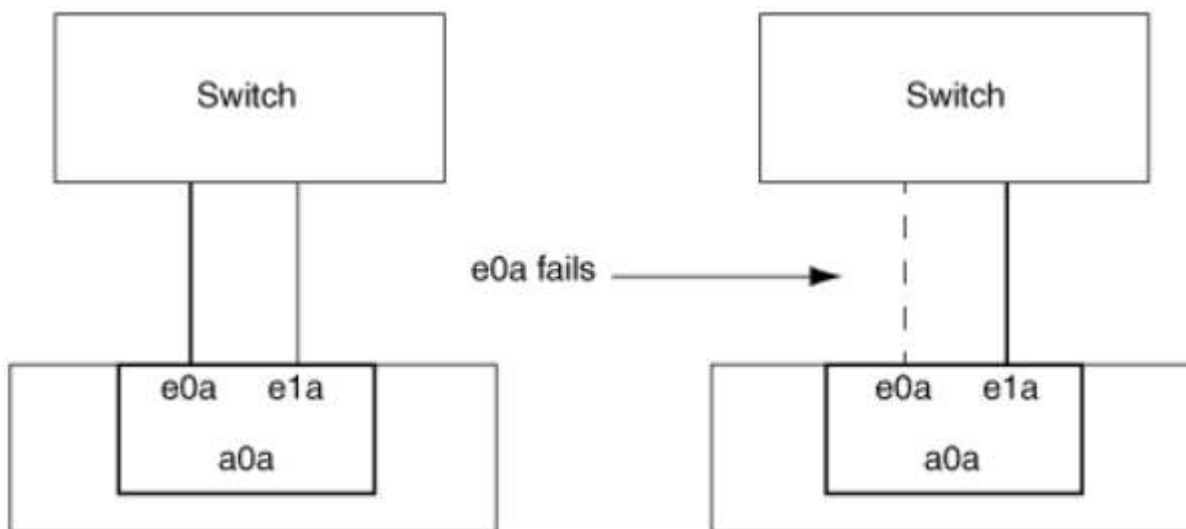
Caractéristiques des groupes d'interfaces monomode

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 switches à l'aide d'une liaison ISL (Inter-Switch Link).
- Pour un groupe d'interface à mode unique, les ports switches 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 switches 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).

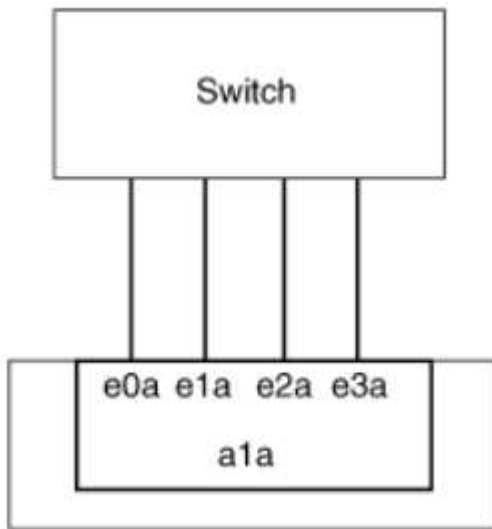
L'algorithme d'équilibrage de charge ONTAP détermine le port membre à utiliser pour transmettre le trafic sortant et ne contrôle pas la réception des trames entrantes. Le commutateur détermine le membre (port physique individuel) de son groupe de canaux de port à utiliser pour la transmission, en fonction 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 multimode sont utilisées de la même manière pour le trafic sortant à l'aide des méthodes d'équilibrage de charge basées sur l'adresse IP, l'adresse MAC, l'ordre séquentiel ou le port pour distribuer le trafic réseau de façon égale sur les ports réseau d'un groupe d'interfaces multimode.

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.

The screenshot shows the 'Add Link Aggregation Group' dialog box in the ONTAP System Manager interface. The dialog has a dark blue header with the title 'Add Link Aggregation Group' and a close button (X). Below the header, there are several sections for configuration:

- NODE:** A dropdown menu showing 'sti47-vs1m-ucs521e'.
- BROADCAST DOMAIN:** A dropdown menu showing 'Automatically select broadcast domain (Recommended)'. A red arrow points to this dropdown with a note: 'Note: Instead of a global switch or checkbox, what if we expose BD dropdown with "Automatic" as a default selection?'.
- PORTS TO INCLUDE:** Two checkboxes labeled 'e0e' and 'e0f', both of which are unchecked.
- MODE:** Three radio button options: 'Single' (selected), 'Multiple', and 'LACP'. Below 'Single' is the text 'Only one port is used at a time.' Below 'Multiple' is 'All ports can be used simultaneously.' Below 'LACP' is 'The LACP protocol determines the ports that can be used.'
- LOAD DISTRIBUTION:** Two radio button options: 'IP based' (selected) and 'MAC based'. Below 'IP based' is the text 'Network traffic is distributed based on the destination IP address.' Below 'MAC based' is 'Network traffic is distributed based on the next-hop MAC addresses.'

At the bottom of the dialog, there are three small icons: a refresh icon, a save icon, and a cancel icon.

CLI

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

Pour obtenir la liste complète des restrictions de configuration qui s'appliquent aux groupes d'interfaces de port, reportez-vous à la section `network port ifgrp add-port` page de manuel.

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 plus d'informations sur cette commande, voir ["Commandes ONTAP 9"](#).

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
```

Pour plus d'informations sur cette commande, voir ["Commandes ONTAP 9"](#).

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.

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
```

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 plus d'informations sur cette commande, voir "[Commandes ONTAP 9](#)".

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 sur des 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 9.13.1 et 9.14.1, les ports non balisés qui ne sont utilisés par aucune interface logique (LIF) et qui ne disposent pas d'une 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, tel que les diffusions CFM ONTAP. Configurez des VLAN natifs sur le commutateur pour empêcher le blocage du trafic non marqué.

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 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`.

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 plus d'informations sur cette commande, voir ["Commandes ONTAP 9"](#).

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
```

Modifier les attributs de port réseau

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
```

Convertissez les ports NIC 40 GbE en ports 10 GbE multiples pour assurer la connectivité 10 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.

Suppression d'une carte réseau du nœud (ONTAP 9.8 et versions ultérieures)

Cette rubrique s'applique à ONTAP 9.8 et versions ultérieures. Vous devrez peut-être retirer une carte réseau défectueuse de son logement ou la déplacer vers un autre emplacement pour des raisons de maintenance.

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.

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.

Suppression d'une carte réseau du nœud (ONTAP 9.7 ou version antérieure)

Cette rubrique s'applique à ONTAP 9.7 ou version antérieure. Vous devrez peut-être retirer une carte réseau défectueuse de son logement ou la déplacer vers un autre emplacement pour des raisons de maintenance.

Avant de commencer

- Toutes les LIFs hébergées sur les ports NIC doivent avoir été migrées ou supprimées.
- Aucun des ports NIC ne peut être le home ports des LIFs.
- Vous devez disposer de privilèges avancés pour supprimer les ports d'une carte réseau.

Étapes

1. Supprimez les ports de la carte réseau :

```
network port delete
```

2. Vérifier que les ports ont été supprimés :

```
network port show
```

3. Répétez l'étape 1 si la sortie de la commande network port show affiche toujours le port supprimé.

Surveiller les ports réseau

Contrôle de l'état de santé des ports réseau

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 flipant 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.

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.

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.

Surveiller l'accessibilité des ports réseau (ONTAP 9.8 et versions ultérieures)

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

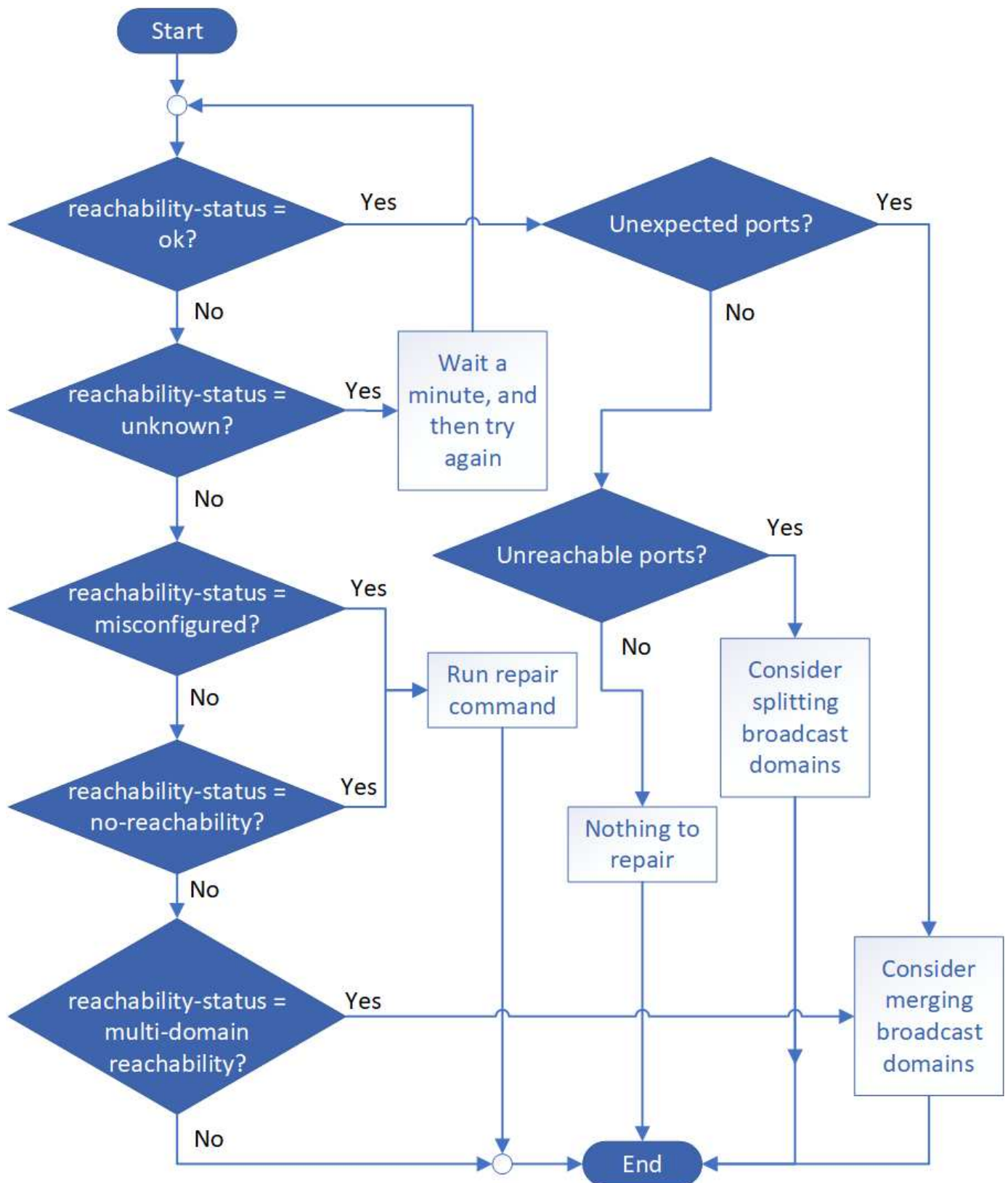
Utilisez ces commandes pour vérifier, diagnostiquer et réparer les erreurs de configuration du réseau qui ne correspondent pas au câblage physique ou à la configuration du commutateur réseau.

Étape

1. Afficher la capacité de port :

```
network port reachability show
```

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



| État-accessibilité | Description |
|--------------------|-------------|
|--------------------|-------------|

| | |
|---|---|
| ok | <p>Le port a une capacité de réachabilité 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 <i>Unexpected ports row</i> suivante.</p> <p>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 <i>ports inaccessibles</i> suivante.</p> <p>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.</p> |
| Ports inattendus | <p>Le port a une capacité de réachabilité 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.</p> <p>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.</p> <p>Pour plus d'informations, voir "Fusionner les domaines de diffusion".</p> |
| Ports inaccessibles | <p>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.</p> <p>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.</p> <p>Pour plus d'informations, voir "Séparer les domaines de diffusion".</p> |
| mauvaise configuration de la capacité de réachabilité | <p>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 reachcapacité de couche 2 à un domaine de diffusion différent.</p> <p>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 :</p> <pre>network port reachability repair -node -port</pre> <p>Pour plus d'informations, voir "Réparation de l'accessibilité de l'orifice".</p> |
| sans trabilité | <p>Le port n'a pas la possibilité de reachcapacité de couche 2 à un domaine de diffusion existant.</p> <p>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 :</p> <pre>network port reachability repair -node -port</pre> <p>Pour plus d'informations, voir "Réparation de l'accessibilité de l'orifice".</p> |

| | |
|------------------------------|---|
| accessibilité multi-domaines | <p>Le port a une capacité de réachabilité 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.</p> <p>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.</p> <p>Pour plus d'informations, voir "Fusionner les domaines de diffusion" ou "Réparation de l'accessibilité de l'orifice".</p> |
| inconnu | <p>Si l'état de la capacité d'accessibilité est « inconnu », attendez quelques minutes et essayez à nouveau la commande.</p> |

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"](#).

Présentation des ports ONTAP

Un certain nombre de ports connus sont réservés pour les communications ONTAP avec des services spécifiques. Des conflits de ports se produisent si une valeur de port dans votre environnement de réseau de stockage est identique à celle du port ONTAP.

Le tableau suivant répertorie les ports TCP et UDP utilisés par ONTAP.

| Service | Port/Protocole | Description |
|---------------|----------------|---------------------------------------|
| ssh | 22/TCP | Connexion au shell sécurisée |
| telnet | 23/TCP | Connexion à distance |
| DNS | 53/TCP | DNS avec équilibrage de charge |
| http | 80/TCP | Protocole de transfert de texte |
| rpcbind | 111/TCP | Appel de procédure à distance |
| rpcbind | 111/UDP | Appel de procédure à distance |
| ntp | 123/UDP | Protocole de temps réseau |
| msrpc | 135/UDP | MSRPC |
| netbios-ssn | 139/TCP | Session de service NetBIOS |
| snmp | 161/UDP | Protocole de gestion de réseau simple |
| https | 443/TCP | HTTP sur TLS |
| microsoft- ds | 445/TCP | Microsoft- ds |
| montage | 635/TCP | Montage NFS |
| montage | 635/UDP | Montage NFS |
| nommé | 953/UDP | Nom démon |

| | | |
|------------------------------------|-------------------|---|
| nfs | 2049/UDP | Démon du serveur NFS |
| nfs | 2049/TCP | Démon du serveur NFS |
| nrv | 2050/TCP | Protocole NetApp Remote Volume |
| iscsi | 3260/TCP | Port cible iSCSI |
| verrouillage | 4045/TCP | Démon de verrouillage NFS |
| verrouillage | 4045/UDP | Démon de verrouillage NFS |
| NSM | 4046/TCP | Moniteur d'état du réseau |
| NSM | 4046/UDP | Moniteur d'état du réseau |
| rquotad | 4049/UDP | Protocole NFS rquotad |
| krb524 | 4444/UDP | Kerberos 524 |
| mdns | 5353/UDP | DNS multicast |
| HTTPS | 5986/UDP | Port HTTPS : protocole binaire d'écoute |
| https | 8443/TCP | Interface graphique 7MTT via https |
| ndmp | 10000/TCP | Protocole de gestion des données réseau |
| Peering de clusters | 11104/TCP | Peering de cluster, bidirectionnel |
| Peering de cluster, bidirectionnel | 11105/TCP | Peering de clusters |
| NDMP | 18600 - 18699/TCP | NDMP |
| NDMP | 30000/TCP | accepte les connexions de contrôle sur les prises femelles sécurisées |
| port témoin cifs | 40001/TCP | port témoin cifs |
| tls | 50000/TCP | Sécurité de la couche de transport |
| iscsi | 65200/TCP | Port iSCSI |

Ports internes ONTAP

Le tableau suivant répertorie les ports TCP et UDP utilisés en interne par ONTAP. Ces ports permettent d'établir une communication LIF intracluster :

| Port/Protocole | Description |
|----------------|--------------------|
| 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 |
| 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 |
| 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 |
| 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 |
| 8023 | Périmètre de nœud TELNET |
| 8514 | Étendue du nœud RSH |
| 9877 | Port client KMIP (hôte local interne uniquement) |

Informations sur le copyright

Copyright © 2024 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 DÉLICTELLE (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.