Configurez les ports réseau

ONTAP 9

NetApp
February 13, 2026

Sommaire

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.

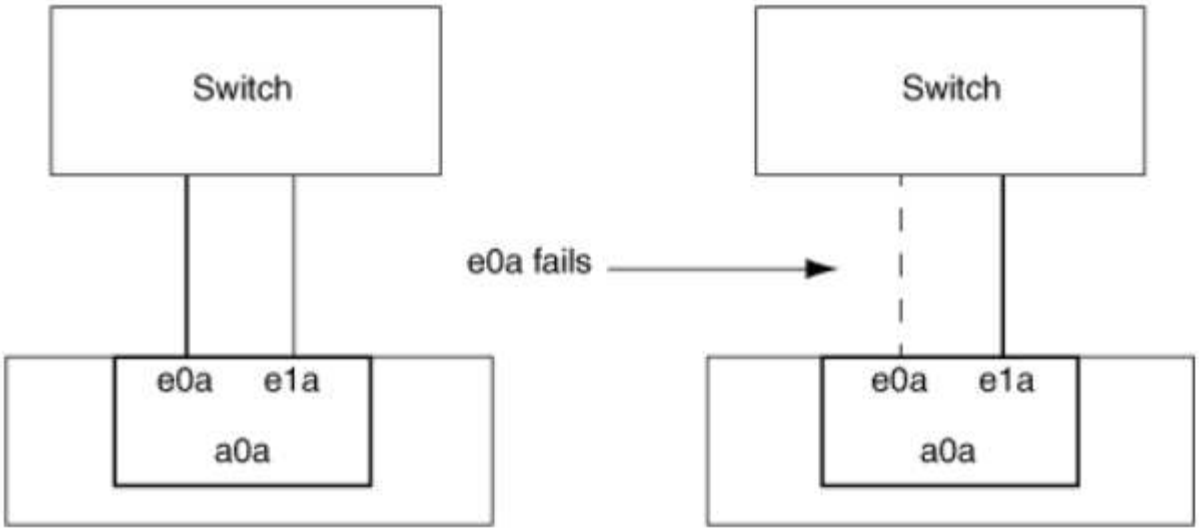
Caractéristiques des groupes d'interfaces monomode

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.

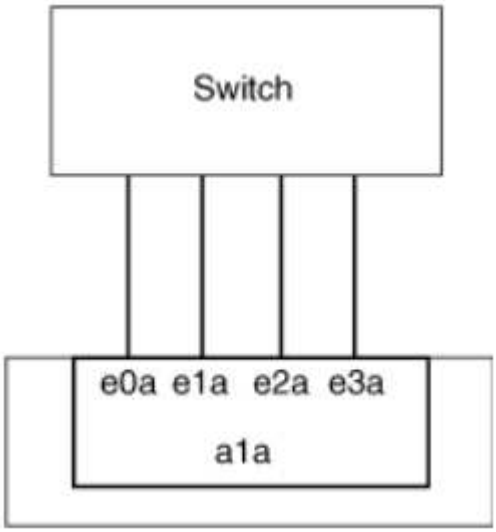
Les caractéristiques d'un groupe d'interfaces multimode statique sont les suivantes :

- 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).

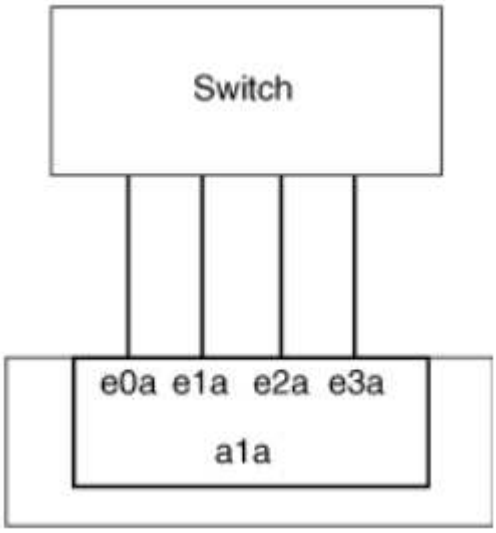
L’algorithme d’équilibrage de charge ONTAP détermine le port membre à utiliser pour transmettre le trafic sortant et ne contrôle pas la réception des trames entrantes. Le commutateur détermine le membre (port physique individuel) de son groupe de canaux de port à utiliser pour la transmission, en fonction 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.

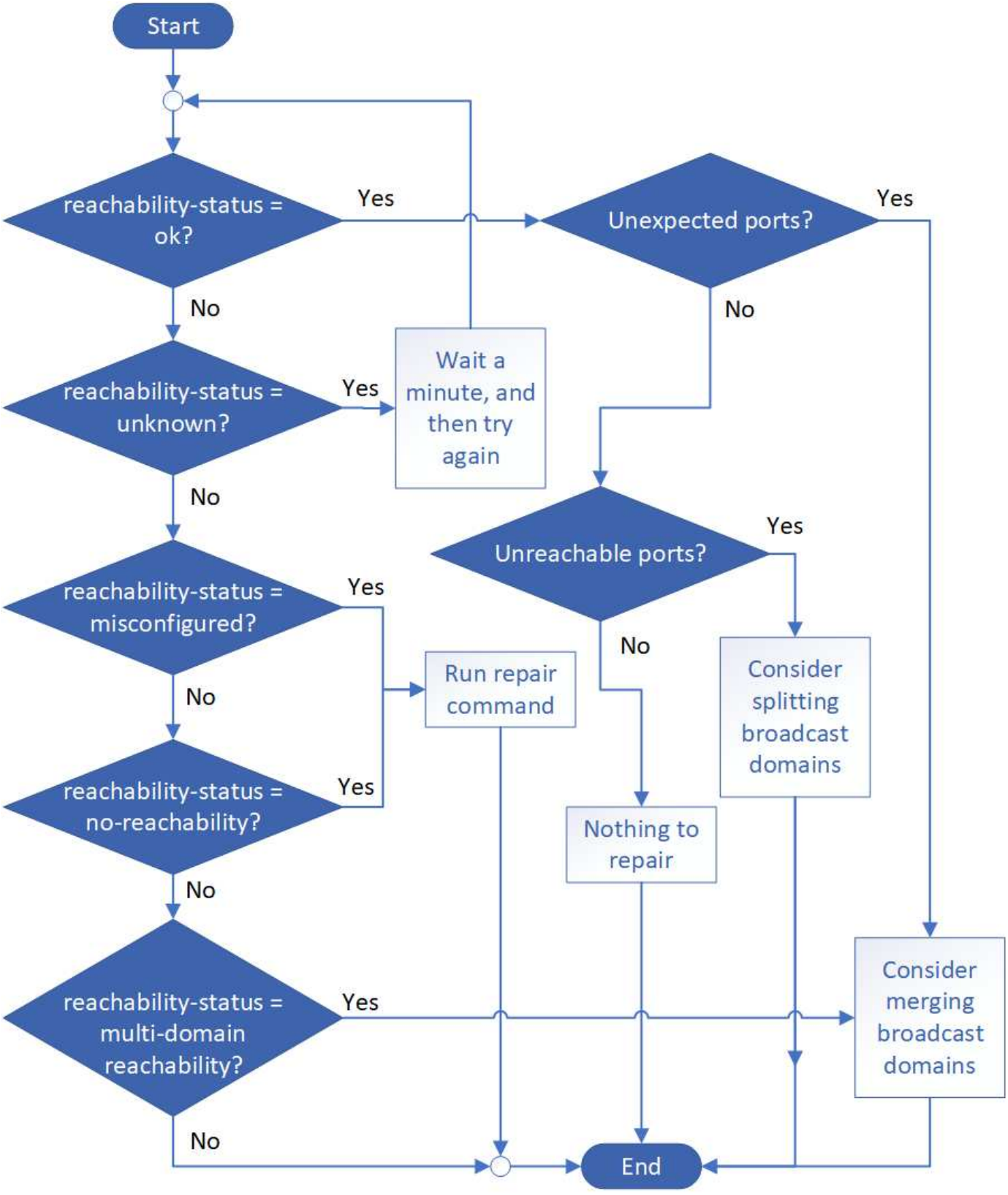
Étape

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