Cluster et SVM peering

ONTAP 9

NetApp
August 21, 2024

Sommaire

Cluster et SVM peering

Présentation du cluster et de SVM peering

Il est possible de créer des relations entre les clusters source et de destination et entre les machines virtuelles de stockage source et de destination. Vous devez créer des relations de pairs entre ces entités avant de répliquer des copies Snapshot à l'aide de SnapMirror.

ONTAP 9.3 apporte des améliorations qui simplifient la configuration des relations entre les clusters et les SVM. Les procédures de peering de clusters et de SVM sont disponibles pour toutes les versions de ONTAP 9. Utilisez la procédure appropriée pour votre version de ONTAP.

Vous effectuez les procédures à l'aide de l'interface de ligne de commandes, et non de System Manager ou d'un outil de script automatisé.

Préparation du cluster et de la SVM peering

Bases du peering

Vous devez créer des relations *peer* entre les clusters source et de destination, et entre les SVM source et destination avant de pouvoir répliquer les copies Snapshot à l'aide de SnapMirror. Une relation de type peer-to-peer définit les connexions réseau qui permettent aux clusters et aux SVM d'échanger les données de manière sécurisée.

Les clusters et les SVM dans des relations entre pairs communiquent sur le réseau intercluster à l'aide de *interfaces logiques (LIF) intercluster.* une LIF intercluster est une LIF qui prend en charge le service d'interface réseau « intercluster-core » et qui est généralement créée en utilisant la politique de service d'interface réseau « default-intercluster ». On doit créer des LIF intercluster sur chaque nœud des clusters en cours de peering.

Les LIFs intercluster utilisent des routes qui appartiennent au SVM système auquel elles sont assignées. ONTAP crée automatiquement un SVM système pour les communications au niveau du cluster au sein d'un IPspace.

Les topologies en mode « Fan-Out » et en cascade sont toutes deux prises en charge. Dans une topologie en cascade, il suffit de créer des réseaux intercluster entre les clusters principal et secondaire, et entre les clusters secondaire et tertiaire. Il n'est pas nécessaire de créer un réseau intercluster entre le cluster principal et le cluster tertiaire.

Il est possible (mais pas conseillé) à un administrateur de supprimer le service intercluster de la politique de service default-intercluster. Dans ce cas, les LIFs créées à l'aide de « Default-intercluster » ne seront en fait pas des LIFs intercluster. Pour vérifier que la politique de service par défaut-intercluster contient le service intercluster-core, utiliser la commande suivante :

```
network interface service-policy show -policy default-intercluster
```

Conditions préalables au peering de clusters

Avant de configurer le peering de cluster, vous devez vérifier que la connectivité, le port,

l'adresse IP, le sous-réseau, le pare-feu, et les exigences de nommage des clusters sont respectées.

> À partir de ONTAP 9.6, Cluster peering fournit par défaut la prise en charge du chiffrement TLS 1.2 AES-256 GCM pour la réplication des données. Les chiffrements de sécurité par défaut (« PSK-AES256-GCM-SHA384 ») sont requis pour que le chiffrement de cluster fonctionne même si le chiffrement est désactivé.
>
> À partir de ONTAP 9.11.1, les chiffrements de sécurité DHE-PSK sont disponibles par défaut.
>
> À partir de ONTAP 9.15.1, Cluster peering assure par défaut la prise en charge du chiffrement TLS 1.3 pour la réplication des données.

Les besoins en connectivité

Chaque LIF intercluster du cluster local doit pouvoir communiquer avec chaque LIF intercluster sur le cluster distant.

Bien qu'il ne soit pas nécessaire, il est généralement plus simple de configurer les adresses IP utilisées pour les LIF intercluster dans le même sous-réseau. Les adresses IP peuvent résider dans le même sous-réseau que les LIF de données ou dans un autre sous-réseau. Le sous-réseau utilisé dans chaque cluster doit respecter les exigences suivantes :

- Le sous-réseau doit appartenir au broadcast domain qui contient les ports utilisés pour la communication intercluster.
- Le sous-réseau doit disposer de suffisamment d'adresses IP disponibles pour allouer à une LIF intercluster par nœud.

  Par exemple, dans un cluster à quatre nœuds, le sous-réseau utilisé pour la communication intercluster doit disposer de quatre adresses IP disponibles.

Chaque nœud doit disposer d'un LIF intercluster avec une adresse IP sur le réseau intercluster.

Les LIF intercluster peuvent disposer d'une adresse IPv4 ou IPv6.

> ONTAP vous permet de migrer vos réseaux de peering depuis IPv4 vers IPv6 en autorisant éventuellement la présence des deux protocoles simultanément sur les LIF intercluster. Dans les versions précédentes, toutes les relations intercluster pour un cluster entier étaient au format IPv4 ou IPv6. Cela signifiait que le changement de protocole était potentiellement source de perturbation.

Configuration requise pour les ports

Vous pouvez utiliser des ports dédiés pour la communication intercluster ou partager les ports utilisés par le réseau de données. Les ports doivent répondre aux exigences suivantes :

- Tous les ports utilisés pour communiquer avec un cluster distant donné doivent se trouver dans le même IPspace.

  Vous pouvez utiliser plusieurs IPspaces pour gérer plusieurs clusters dans un même cluster. Une connectivité à maillage complet par paire est requise uniquement au sein d'un IPspace.

- Le broadcast domain utilisé pour la communication intercluster doit inclure au moins deux ports par nœud afin que la communication intercluster puisse basculer d'un port vers un autre.

  Les ports ajoutés à un domaine de diffusion peuvent être des ports réseau physiques, des VLAN ou des groupes d'interfaces (ifgrps).

- Tous les ports doivent être câblés.
- Tous les ports doivent être en état de santé.
- Les paramètres MTU des ports doivent être cohérents.

Exigences relatives au pare-feu

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

Les pare-feu et la politique de pare-feu intercluster doivent autoriser les protocoles suivants :

- Trafic ICMP bidirectionnel
- Le trafic TCP initié bidirectionnel vers les adresses IP de toutes les LIFs intercluster sur les ports 11104 et 11105
- HTTPS bidirectionnel entre les LIFs intercluster

  Bien que HTTPS n'est pas requis lors de la configuration du peering de clusters à l'aide de l'interface de ligne de commande, HTTPS est requis plus tard si vous utilisez System Manager pour configurer la protection des données.

La valeur par défaut `intercluster` La politique de pare-feu permet l'accès via le protocole HTTPS et à partir de toutes les adresses IP (0.0.0.0/0). Vous pouvez modifier ou remplacer la stratégie si nécessaire.

Regroupement des clusters

Les clusters doivent répondre aux exigences suivantes :

- Un cluster ne peut pas se trouver dans une relation entre pairs et plus de 255 clusters.

Utiliser des ports partagés ou dédiés

Vous pouvez utiliser des ports dédiés pour la communication intercluster ou partager les ports utilisés par le réseau de données. Lors de la décision de partager des ports, vous devez tenir compte de la bande passante du réseau, de l'intervalle de réplication et de la disponibilité des ports.

Vous pouvez partager les ports sur un cluster en utilisant des ports dédiés sur l'autre.

La bande passante du réseau

Si vous disposez d'un réseau haut débit (par exemple 10 GbE), vous disposez peut-être d'une bande passante LAN locale suffisante pour effectuer la réplication à l'aide des mêmes ports 10 GbE utilisés pour l'accès aux données.

Vous devriez même comparer votre bande passante WAN disponible à celle de votre réseau local. Si la bande passante WAN disponible est bien inférieure à 10 GbE, vous devrez peut-être utiliser des ports dédiés.

À l'exception de cette règle, on peut trouver lorsque tous les nœuds du cluster répliquent des données, auquel cas l'utilisation de la bande passante est généralement répartie entre ces nœuds.

Si vous n'utilisez pas de ports dédiés, la taille de l'unité de transmission maximale (MTU) du réseau de réplication doit généralement être identique à la taille de MTU du réseau de données.

Intervalle de réplication

Si la réplication se déroule en dehors des heures de pointe, vous devriez pouvoir utiliser des ports de données pour la réplication, même sans connexion LAN 10 GbE.

Si la réplication a lieu pendant les heures de bureau, vous devez tenir compte de la quantité de données à répliquer et de la quantité de bande passante nécessaire pour créer des conflits avec les protocoles de données. Si l'utilisation du réseau par les protocoles de données (SMB, NFS, iSCSI) est supérieure à 50 %, il est recommandé d'utiliser des ports dédiés pour la communication intercluster afin de permettre des performances non dégradées en cas de basculement du nœud.

Disponibilité du port

Si vous déterminez que le trafic de réplication interfère sur le trafic de données, vous pouvez migrer des LIFs intercluster vers n'importe quel autre port partagé intercluster sur le même nœud.

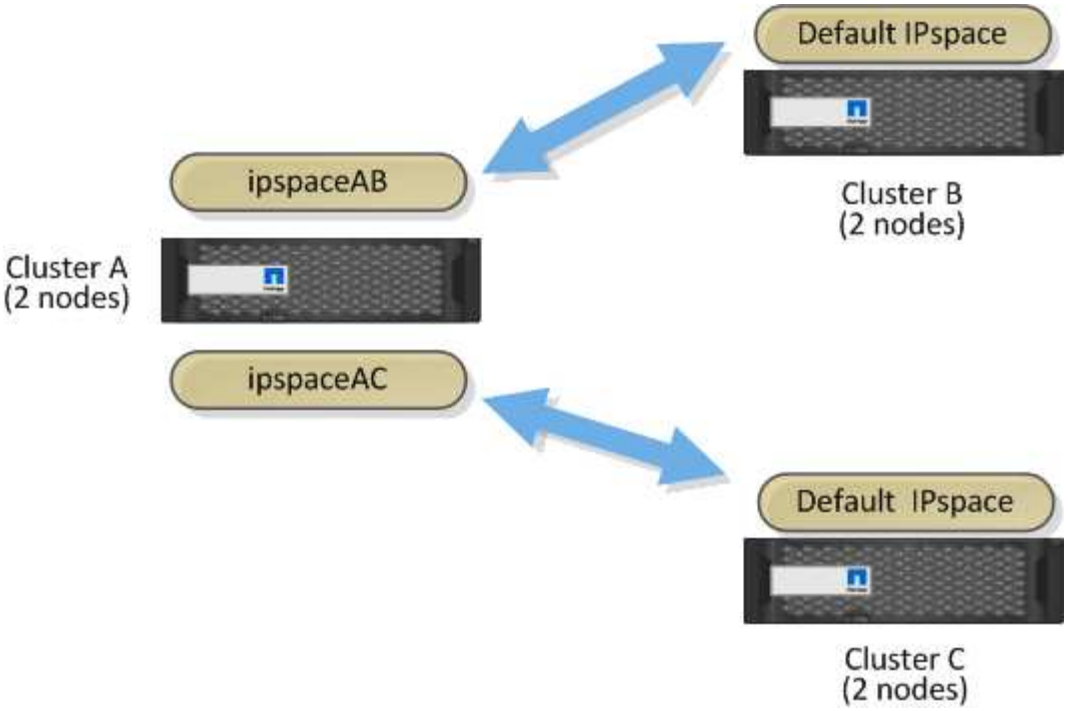
Vous pouvez également dédier des ports VLAN à la réplication. La bande passante du port est partagée entre tous les VLAN et le port de base.

Utilisez les IPspaces personnalisés pour isoler le trafic de réplication

Vous pouvez utiliser des IPspaces personnalisés pour séparer les interactions d'un cluster avec ses pairs. Appelée *connectivité intercluster désignée*, cette configuration permet aux fournisseurs de services d'isoler le trafic de réplication dans des environnements mutualisés.

Supposons, par exemple, que vous souhaitez que le trafic de réplication entre le Cluster A et le Cluster B soit séparé du trafic de réplication entre le Cluster A et le Cluster C. Pour ce faire, vous pouvez créer deux IPspaces sur le Cluster A.

Un IPspace contient les LIF intercluster que vous utilisez pour communiquer avec le Cluster B. L'autre contient les LIFs intercluster que vous utilisez pour communiquer avec le Cluster C, comme indiqué sur l'illustration suivante.



Pour une configuration IPspace personnalisée, consultez le *Network Management Guide*.

Configurer les LIFs intercluster

Configurer les LIFs intercluster sur des ports data partagés

Vous pouvez configurer les LIFs intercluster sur des ports partagés avec le réseau de données. Cela réduit le nombre de ports nécessaires pour la mise en réseau intercluster.

Étapes

1. Lister les ports dans le cluster :

   ```
   network port show
   ```

   Pour connaître la syntaxe complète de la commande, reportez-vous à la page man.

   L'exemple suivant montre les ports réseau dans `cluster01`:

```
cluster01::> network port show
                                                                  Speed
(Mbps)
Node   Port      IPspace      Broadcast Domain Link   MTU    Admin/Oper
------ --------- ------------ ---------------- ----- -------
------------
cluster01-01
       e0a       Cluster      Cluster          up     1500   auto/1000
       e0b       Cluster      Cluster          up     1500   auto/1000
       e0c       Default      Default          up     1500   auto/1000
       e0d       Default      Default          up     1500   auto/1000
cluster01-02
       e0a       Cluster      Cluster          up     1500   auto/1000
       e0b       Cluster      Cluster          up     1500   auto/1000
       e0c       Default      Default          up     1500   auto/1000
       e0d       Default      Default          up     1500   auto/1000
```

2. Créer des LIF intercluster sur un SVM admin (IPspace par défaut) ou un SVM système (IPspace personnalisé) :

Option	Description
Dans ONTAP 9.6 et plus tard:	`network interface create -vserver` *`system_SVM`* `-lif` *`LIF_name`* `-service -policy default-intercluster -home -node` *`node`* `-home-port port -address` *`port_IP`* `-netmask` *`netmask`*
Dans ONTAP 9.5 et versions antérieures:	`network interface create -vserver` *`system_SVM`* `-lif` *`LIF_name`* `-role intercluster -home-node` *`node`* `-home -port` *`port`* `-address` *`port_IP`* `-netmask` *`netmask`*

Pour connaître la syntaxe complète de la commande, reportez-vous à la page man.

L'exemple suivant illustre la création de LIFs intercluster `cluster01_icl01` et `cluster01_icl02`:

```
cluster01::> network interface create -vserver cluster01 -lif
cluster01_icl01 -service-
policy default-intercluster -home-node cluster01-01 -home-port e0c
-address 192.168.1.201
-netmask 255.255.255.0

cluster01::> network interface create -vserver cluster01 -lif
cluster01_icl02 -service-
policy default-intercluster -home-node cluster01-02 -home-port e0c
-address 192.168.1.202
-netmask 255.255.255.0
```

3. Vérifier que les LIFs intercluster ont été créés :

Option	Description
Dans ONTAP 9.6 et plus tard:	`network interface show -service-policy default-intercluster`
Dans ONTAP 9.5 et versions antérieures:	`network interface show -role intercluster`

Pour connaître la syntaxe complète de la commande, reportez-vous à la page man.

```
cluster01::> network interface show -service-policy default-intercluster
            Logical    Status     Network            Current
Current Is
Vserver     Interface  Admin/Oper Address/Mask       Node          Port
Home
----------- ---------- ---------- ------------------ -------------
------- ----
cluster01
            cluster01_icl01
                       up/up      192.168.1.201/24   cluster01-01  e0c
true
            cluster01_icl02
                       up/up      192.168.1.202/24   cluster01-02  e0c
true
```

4. Vérifier que les LIFs intercluster sont redondants :

Option	Description
Dans ONTAP 9.6 et plus tard:	`network interface show –service-policy default-intercluster -failover`
Dans ONTAP 9.5 et versions antérieures:	`network interface show -role intercluster -failover`

Pour connaître la syntaxe complète de la commande, reportez-vous à la page man.

L'exemple suivant indique que les LIFs intercluster `cluster01_icl01` et `cluster01_icl02` sur le `e0c` le port basculera vers le `e0d` port.

```
cluster01::> network interface show -service-policy default-intercluster
–failover
         Logical         Home                  Failover        Failover
Vserver  Interface       Node:Port             Policy          Group
-------- --------------- --------------------- --------------- --------
cluster01
         cluster01_icl01 cluster01-01:e0c   local-only
192.168.1.201/24
                            Failover Targets: cluster01-01:e0c,
                                              cluster01-01:e0d
         cluster01_icl02 cluster01-02:e0c   local-only
192.168.1.201/24
                            Failover Targets: cluster01-02:e0c,
                                              cluster01-02:e0d
```

Configurer les LIFs intercluster sur les ports dédiés

Vous pouvez configurer les LIFs intercluster sur des ports dédiés. Cela augmente généralement la bande passante disponible pour le trafic de réplication.

Étapes

1. Lister les ports dans le cluster :

   `network port show`

   Pour connaître la syntaxe complète de la commande, reportez-vous à la page man.

   L'exemple suivant montre les ports réseau dans `cluster01`:

```
cluster01::> network port show
                                                                  Speed
(Mbps)
Node   Port      IPspace      Broadcast Domain Link   MTU    Admin/Oper
------ --------- ------------ ---------------- ----- -------
------------
cluster01-01
       e0a       Cluster      Cluster          up     1500   auto/1000
       e0b       Cluster      Cluster          up     1500   auto/1000
       e0c       Default      Default          up     1500   auto/1000
       e0d       Default      Default          up     1500   auto/1000
       e0e       Default      Default          up     1500   auto/1000
       e0f       Default      Default          up     1500   auto/1000
cluster01-02
       e0a       Cluster      Cluster          up     1500   auto/1000
       e0b       Cluster      Cluster          up     1500   auto/1000
       e0c       Default      Default          up     1500   auto/1000
       e0d       Default      Default          up     1500   auto/1000
       e0e       Default      Default          up     1500   auto/1000
       e0f       Default      Default          up     1500   auto/1000
```

2. Déterminer les ports disponibles pour dédier aux communications intercluster :

   `network interface show -fields home-port,curr-port`

   Pour connaître la syntaxe complète de la commande, reportez-vous à la page man.

   L'exemple suivant indique ces ports `e0e` et `e0f` Ne se sont pas affectés de LIFs :

```
cluster01::> network interface show -fields home-port,curr-port
vserver lif                  home-port curr-port
------- -------------------- --------- ---------
Cluster cluster01-01_clus1   e0a       e0a
Cluster cluster01-01_clus2   e0b       e0b
Cluster cluster01-02_clus1   e0a       e0a
Cluster cluster01-02_clus2   e0b       e0b
cluster01
        cluster_mgmt         e0c       e0c
cluster01
        cluster01-01_mgmt1   e0c       e0c
cluster01
        cluster01-02_mgmt1   e0c       e0c
```

3. Créer un failover group pour les ports dédiés :

`network interface failover-groups create -vserver system_SVM -failover-group failover_group -targets physical _or_logical_ports`

L'exemple suivant attribue des ports `e0e` et `e0f` vers le groupe de basculement `intercluster01` Sur le SVM système `cluster01`:

```
cluster01::> network interface failover-groups create -vserver cluster01
-failover-group
intercluster01 -targets
cluster01-01:e0e,cluster01-01:e0f,cluster01-02:e0e,cluster01-02:e0f
```

4. Vérifier que le groupe de basculement a été créé :

   `network interface failover-groups show`

   Pour connaître la syntaxe complète de la commande, reportez-vous à la page man.

```
cluster01::> network interface failover-groups show
                                  Failover
Vserver          Group            Targets
---------------- ----------------
--------------------------------------------
Cluster
                 Cluster
                                  cluster01-01:e0a, cluster01-01:e0b,
                                  cluster01-02:e0a, cluster01-02:e0b
cluster01
                 Default
                                  cluster01-01:e0c, cluster01-01:e0d,
                                  cluster01-02:e0c, cluster01-02:e0d,
                                  cluster01-01:e0e, cluster01-01:e0f
                                  cluster01-02:e0e, cluster01-02:e0f
                 intercluster01
                                  cluster01-01:e0e, cluster01-01:e0f
                                  cluster01-02:e0e, cluster01-02:e0f
```

5. Créer les LIF intercluster sur le SVM système et les assigner au failover group.

Option	Description
Dans ONTAP 9.6 et plus tard:	`network interface create -vserver system_SVM -lif LIF_name -service -policy default-intercluster -home -node node -home- port port -address port_IP -netmask netmask -failover -group failover_group`

Option	Description
Dans ONTAP 9.5 et versions antérieures:	`network interface create -vserver system_SVM -lif LIF_name -role intercluster -home-node node -home -port port -address port_IP -netmask netmask -failover-group failover_group`

Pour connaître la syntaxe complète de la commande, reportez-vous à la page man.

L'exemple suivant illustre la création de LIFs intercluster `cluster01_icl01` et `cluster01_icl02` dans le groupe de basculement `intercluster01`:

```
cluster01::> network interface create -vserver cluster01 -lif
cluster01_icl01 -service-
policy default-intercluster -home-node cluster01-01 -home-port e0e
-address 192.168.1.201
-netmask 255.255.255.0 -failover-group intercluster01

cluster01::> network interface create -vserver cluster01 -lif
cluster01_icl02 -service-
policy default-intercluster -home-node cluster01-02 -home-port e0e
-address 192.168.1.202
-netmask 255.255.255.0 -failover-group intercluster01
```

6. Vérifier que les LIFs intercluster ont été créés :

Option	Description
Dans ONTAP 9.6 et plus tard:	`network interface show -service-policy default-intercluster`
Dans ONTAP 9.5 et versions antérieures:	`network interface show -role intercluster`

Pour connaître la syntaxe complète de la commande, reportez-vous à la page man.

```
cluster01::> network interface show -service-policy default-intercluster
            Logical    Status     Network            Current
Current Is
Vserver     Interface  Admin/Oper Address/Mask       Node          Port
Home
----------- ---------- ---------- ------------------ -------------
------- ----
cluster01
            cluster01_icl01
                       up/up      192.168.1.201/24   cluster01-01  e0e
true
            cluster01_icl02
                       up/up      192.168.1.202/24   cluster01-02  e0f
true
```

7. Vérifier que les LIFs intercluster sont redondants :

Option	Description
Dans ONTAP 9.6 et plus tard:	`network interface show -service-policy default-intercluster -failover`
Dans ONTAP 9.5 et versions antérieures:	`network interface show -role intercluster -failover`

Pour connaître la syntaxe complète de la commande, reportez-vous à la page man.

L'exemple suivant indique que les LIFs intercluster `cluster01_icl01` et `cluster01_icl02` Sur le SVM`e0e` le port basculera vers le `e0f` port.

```
cluster01::> network interface show -service-policy default-intercluster
-failover
         Logical         Home                  Failover        Failover
Vserver  Interface       Node:Port             Policy          Group
-------- --------------- --------------------- --------------- --------
cluster01
         cluster01_icl01 cluster01-01:e0e   local-only
intercluster01
                            Failover Targets:  cluster01-01:e0e,
                                               cluster01-01:e0f
         cluster01_icl02 cluster01-02:e0e   local-only
intercluster01
                            Failover Targets:  cluster01-02:e0e,
                                               cluster01-02:e0f
```

Configurez les LIF intercluster dans des IPspaces personnalisés

Vous pouvez configurer les LIF intercluster dans des IPspaces personnalisés. Il est ainsi possible d'isoler le trafic de réplication dans des environnements mutualisés.

Lorsque vous créez un IPspace personnalisé, le système crée une machine virtuelle de stockage système (SVM) afin de servir de conteneur pour les objets système dans cet IPspace. Vous pouvez utiliser le nouveau SVM en tant que conteneur pour toutes les LIF intercluster dans le nouvel IPspace. Le nouveau SVM porte le même nom que l'IPspace personnalisé.

Étapes

1. Lister les ports dans le cluster :

   `network port show`

   Pour connaître la syntaxe complète de la commande, reportez-vous à la page man.

   L'exemple suivant montre les ports réseau dans `cluster01`:

```
cluster01::> network port show
                                                                  Speed
(Mbps)
Node   Port      IPspace      Broadcast Domain Link   MTU    Admin/Oper
------ --------- ------------ ---------------- ----- -------
------------
cluster01-01
       e0a       Cluster      Cluster          up     1500   auto/1000
       e0b       Cluster      Cluster          up     1500   auto/1000
       e0c       Default      Default          up     1500   auto/1000
       e0d       Default      Default          up     1500   auto/1000
       e0e       Default      Default          up     1500   auto/1000
       e0f       Default      Default          up     1500   auto/1000
cluster01-02
       e0a       Cluster      Cluster          up     1500   auto/1000
       e0b       Cluster      Cluster          up     1500   auto/1000
       e0c       Default      Default          up     1500   auto/1000
       e0d       Default      Default          up     1500   auto/1000
       e0e       Default      Default          up     1500   auto/1000
       e0f       Default      Default          up     1500   auto/1000
```

2. Créez des IPspaces personnalisés sur le cluster :

   `network ipspace create -ipspace` *`ipspace`*

   L'exemple suivant crée l'IPspace personnalisé `ipspace-IC1`:

```
cluster01::> network ipspace create -ipspace ipspace-IC1
```

3. Déterminer les ports disponibles pour dédier aux communications intercluster :

   `network interface show -fields home-port,curr-port`

   Pour connaître la syntaxe complète de la commande, reportez-vous à la page man.

   L'exemple suivant indique ces ports `e0e` et `e0f` Ne se sont pas affectés de LIFs :

```
cluster01::> network interface show -fields home-port,curr-port
vserver lif                  home-port curr-port
------- -------------------- --------- ---------
Cluster cluster01_clus1   e0a       e0a
Cluster cluster01_clus2   e0b       e0b
Cluster cluster02_clus1   e0a       e0a
Cluster cluster02_clus2   e0b       e0b
cluster01
        cluster_mgmt         e0c       e0c
cluster01
        cluster01-01_mgmt1   e0c       e0c
cluster01
        cluster01-02_mgmt1   e0c       e0c
```

4. Supprimer les ports disponibles du broadcast domain par défaut :

   `network port broadcast-domain remove-ports -broadcast-domain Default -ports ports`

   Un port ne peut pas se trouver dans plusieurs domaines de diffusion à la fois. Pour connaître la syntaxe complète de la commande, reportez-vous à la page man.

   L'exemple suivant supprime les ports `e0e` et `e0f` depuis le broadcast domain par défaut :

```
cluster01::> network port broadcast-domain remove-ports -broadcast
-domain Default -ports
cluster01-01:e0e,cluster01-01:e0f,cluster01-02:e0e,cluster01-02:e0f
```

5. Vérifiez que les ports ont été supprimés du broadcast domain par défaut :

   `network port show`

   Pour connaître la syntaxe complète de la commande, reportez-vous à la page man.

   L'exemple suivant indique ces ports `e0e` et `e0f` ont été supprimés du broadcast domain par défaut :

```
cluster01::> network port show
                                                          Speed (Mbps)
Node   Port    IPspace   Broadcast Domain Link   MTU    Admin/Oper
------ ------- --------- --------------- ----- ------- ------------
cluster01-01
       e0a     Cluster    Cluster          up    9000  auto/1000
       e0b     Cluster    Cluster          up    9000  auto/1000
       e0c     Default    Default          up    1500  auto/1000
       e0d     Default    Default          up    1500  auto/1000
       e0e     Default    -                up    1500  auto/1000
       e0f     Default    -                up    1500  auto/1000
       e0g     Default    Default          up    1500  auto/1000
cluster01-02
       e0a     Cluster    Cluster          up    9000  auto/1000
       e0b     Cluster    Cluster          up    9000  auto/1000
       e0c     Default    Default          up    1500  auto/1000
       e0d     Default    Default          up    1500  auto/1000
       e0e     Default    -                up    1500  auto/1000
       e0f     Default    -                up    1500  auto/1000
       e0g     Default    Default          up    1500  auto/1000
```

6. Créer un domaine de diffusion dans l'IPspace personnalisé :

   `network port broadcast-domain create -ipspace` *`ipspace`* `-broadcast-domain` *`broadcast_domain`* `-mtu` *`MTU`* `-ports` *`ports`*

   L'exemple suivant crée le domaine de diffusion `ipspace-IC1-bd` Dans l'IPspace `ipspace-IC1`:

```
cluster01::> network port broadcast-domain create -ipspace ipspace-IC1
-broadcast-domain
ipspace-IC1-bd -mtu 1500 -ports cluster01-01:e0e,cluster01-01:e0f,
cluster01-02:e0e,cluster01-02:e0f
```

7. Vérifiez que le domaine de diffusion a été créé :

   `network port broadcast-domain show`

   Pour connaître la syntaxe complète de la commande, reportez-vous à la page man.

```
cluster01::> network port broadcast-domain show
IPspace Broadcast                                       Update
Name    Domain Name    MTU  Port List                   Status Details
------- ----------- ------  ---------------------------- --------------
Cluster Cluster       9000
                            cluster01-01:e0a             complete
                            cluster01-01:e0b             complete
                            cluster01-02:e0a             complete
                            cluster01-02:e0b             complete
Default Default       1500
                            cluster01-01:e0c             complete
                            cluster01-01:e0d             complete
                            cluster01-01:e0f             complete
                            cluster01-01:e0g             complete
                            cluster01-02:e0c             complete
                            cluster01-02:e0d             complete
                            cluster01-02:e0f             complete
                            cluster01-02:e0g             complete
ipspace-IC1
        ipspace-IC1-bd
                      1500
                            cluster01-01:e0e             complete
                            cluster01-01:e0f             complete
                            cluster01-02:e0e             complete
                            cluster01-02:e0f             complete
```

8. Créer les LIFs intercluster sur le SVM système et les assigner au broadcast domain :

Option	Description
Dans ONTAP 9.6 et plus tard:	`network interface create -vserver` *`system_SVM`* `-lif` *`LIF_name`* `-service -policy default-intercluster -home -node` *`node`* `-home-port` *`port`* `-address` *`port_IP`* `-netmask` *`netmask`*
Dans ONTAP 9.5 et versions antérieures:	`network interface create -vserver` *`system_SVM`* `-lif` *`LIF_name`* `-role intercluster -home-node` *`node`* `-home -port` *`port`* `-address` *`port_IP`* `-netmask` *`netmask`*

Le LIF est créé dans le broadcast domain auquel le home port est attribué. Le broadcast domain a un failover group par défaut avec le même nom que le broadcast domain. Pour connaître la syntaxe complète de la commande, reportez-vous à la page man.

L'exemple suivant illustre la création de LIFs intercluster `cluster01_icl01` et `cluster01_icl02` dans le domaine de broadcast `ipspace-IC1-bd`:

```
cluster01::> network interface create -vserver ipspace-IC1 -lif
cluster01_icl01 -service-
policy default-intercluster -home-node cluster01-01 -home-port e0e
-address 192.168.1.201
-netmask 255.255.255.0

cluster01::> network interface create -vserver ipspace-IC1 -lif
cluster01_icl02 -service-
policy default-intercluster -home-node cluster01-02 -home-port e0e
-address 192.168.1.202
-netmask 255.255.255.0
```

9. Vérifier que les LIFs intercluster ont été créés :

Option	Description
Dans ONTAP 9.6 et plus tard:	`network interface show -service-policy default-intercluster`
Dans ONTAP 9.5 et versions antérieures:	`network interface show -role intercluster`

Pour connaître la syntaxe complète de la commande, reportez-vous à la page man.

```
cluster01::> network interface show -service-policy default-intercluster
            Logical    Status     Network            Current
Current Is
Vserver     Interface  Admin/Oper Address/Mask       Node          Port
Home
----------- ---------- ---------- ------------------ -------------
------- ----
ipspace-IC1
            cluster01_icl01
                       up/up      192.168.1.201/24   cluster01-01  e0e
true
            cluster01_icl02
                       up/up      192.168.1.202/24   cluster01-02  e0f
true
```

10. Vérifier que les LIFs intercluster sont redondants :

Option	Description
Dans ONTAP 9.6 et plus tard:	`network interface show -service-policy default-intercluster -failover`
Dans ONTAP 9.5 et versions antérieures:	`network interface show -role intercluster -failover`

Pour connaître la syntaxe complète de la commande, reportez-vous à la page man.

L'exemple suivant indique que les LIFs intercluster `cluster01_icl01` et `cluster01_icl02` Sur le SVM `e0e` le port passe au port « e0f'port :

```
cluster01::> network interface show -service-policy default-intercluster
-failover
         Logical         Home                  Failover        Failover
Vserver  Interface       Node:Port             Policy          Group
-------- --------------- --------------------- --------------- --------
ipspace-IC1
         cluster01_icl01 cluster01-01:e0e   local-only
intercluster01
                            Failover Targets:  cluster01-01:e0e,
                                               cluster01-01:e0f
         cluster01_icl02 cluster01-02:e0e   local-only
intercluster01
                            Failover Targets:  cluster01-02:e0e,
                                               cluster01-02:e0f
```

Configurer les relations de pairs

Créer une relation entre clusters

Avant de protéger vos données en les répliquant sur un cluster distant à des fins de sauvegarde des données et de reprise sur incident, vous devez créer une relation entre les pairs de cluster entre le cluster local et distant.

Plusieurs stratégies de protection par défaut sont disponibles. Vous devez avoir créé vos stratégies de protection si vous souhaitez utiliser des stratégies personnalisées.

Avant de commencer

- Si vous utilisez l'interface de ligne de commandes ONTAP, vous devez avoir créé des LIFs intercluster sur chaque nœud des clusters peering en utilisant l'une des méthodes suivantes :
  - "Configurer les LIFs intercluster sur des ports data partagés"
  - "Configurer les LIFs intercluster sur des ports data dédiés"
  - "Configurez les LIF intercluster dans des IPspaces personnalisés"

- Les clusters doivent exécuter ONTAP 9.3 ou version ultérieure. (Si les clusters exécutent ONTAP 9.2 ou une version antérieure, reportez-vous aux procédures de la "ce document archivé".)

Étapes

Effectuez cette tâche à l'aide de ONTAP System Manager ou de l'interface de ligne de commandes de ONTAP.

System Manager

1. Dans le cluster local, cliquez sur **Cluster > Paramètres**.
2. Dans la section **intercluster Settings**, cliquez sur **Add Network interfaces** et entrez l'adresse IP et le masque de sous-réseau pour ajouter les interfaces réseau intercluster du cluster.

   Répétez cette étape sur le cluster distant.
3. Dans le cluster distant, cliquez sur **Cluster > Paramètres**.
4. Cliquez sur ⋮ dans la section **homologues du cluster** et sélectionnez **générer une phrase de passe**.
5. Sélectionnez la version du cluster ONTAP distant.
6. Copiez la phrase de passe générée.
7. Dans le cluster local, sous **clusters homologues**, cliquez sur ⋮ et sélectionnez **Peer Cluster**.
8. Dans la fenêtre **Peer Cluster**, collez la phrase de passe et cliquez sur **Initiate cluster peering**.

CLI

1. Sur le cluster destination, créez une relation entre pairs et le cluster source :

   ```
   cluster peer create -generate-passphrase -offer-expiration
   <MM/DD/YYYY HH:MM:SS|1...7days|1...168hours> -peer-addrs
   <peer_LIF_IPs> -initial-allowed-vserver-peers <svm_name|*> -ipspace
   <ipspace>
   ```

   Si vous spécifiez les deux `-generate-passphrase` et `-peer-addrs`, Uniquement le cluster dont les LIFs intercluster sont spécifiés dans `-peer-addrs` peut utiliser le mot de passe généré.

   Vous pouvez ignorer `-ipspace` Option si vous n'utilisez pas un IPspace personnalisé. Pour connaître la syntaxe complète de la commande, reportez-vous à la page man.

   Si vous créez la relation de peering dans ONTAP 9.6 ou version ultérieure et que vous ne souhaitez pas que les communications de peering de clusters soient cryptées, vous devez utiliser le `-encryption-protocol-proposed none` option pour désactiver le cryptage.

   L'exemple suivant crée une relation de cluster peer-to-peer avec un cluster distant non spécifié, et autorise pré-les relations de pairs avec les SVM `vs1` et `vs2` sur le cluster local :

```
cluster02::> cluster peer create -generate-passphrase -offer
-expiration 2days -initial-allowed-vserver-peers vs1,vs2

                    Passphrase: UCa+6lRVICXeL/gq1WrK7ShR
               Expiration Time: 6/7/2017 08:16:10 EST
  Initial Allowed Vserver Peers: vs1,vs2
            Intercluster LIF IP: 192.140.112.101
              Peer Cluster Name: Clus_7ShR (temporary generated)

Warning: make a note of the passphrase - it cannot be displayed
again.
```

L'exemple suivant crée une relation de cluster peer-to-peer avec le cluster distant aux adresses IP LIF intercluster 192.140.112.103 et 192.140.112.104, et autorise pré-une relation de peer-to-peer avec n'importe quel SVM sur le cluster local :

```
cluster02::> cluster peer create -generate-passphrase -peer-addrs
192.140.112.103,192.140.112.104 -offer-expiration 2days -initial
-allowed-vserver-peers *

                    Passphrase: UCa+6lRVICXeL/gq1WrK7ShR
               Expiration Time: 6/7/2017 08:16:10 EST
  Initial Allowed Vserver Peers: vs1,vs2
            Intercluster LIF IP: 192.140.112.101,192.140.112.102
              Peer Cluster Name: Clus_7ShR (temporary generated)

Warning: make a note of the passphrase - it cannot be displayed
again.
```

L'exemple suivant crée une relation de cluster peer-to-peer avec un cluster distant non spécifié, et autorise pré-les relations de pairs avec les SVM`vs1` et `vs2` sur le cluster local :

```
cluster02::> cluster peer create -generate-passphrase -offer
-expiration 2days -initial-allowed-vserver-peers vs1,vs2

                    Passphrase: UCa+6lRVICXeL/gq1WrK7ShR
               Expiration Time: 6/7/2017 08:16:10 EST
  Initial Allowed Vserver Peers: vs1,vs2
            Intercluster LIF IP: 192.140.112.101
              Peer Cluster Name: Clus_7ShR (temporary generated)

Warning: make a note of the passphrase - it cannot be displayed
again.
```

2. Sur le cluster source, authentifier le cluster source sur le cluster destination :

```
cluster peer create -peer-addrs <peer_LIF_IPs> -ipspace <ipspace>
```

Pour connaître la syntaxe complète de la commande, reportez-vous à la page man.

L'exemple suivant authentifie le cluster local sur le cluster distant aux adresses IP 192.140.112.101 et 192.140.112.102 de LIF intercluster :

```
cluster01::> cluster peer create -peer-addrs
192.140.112.101,192.140.112.102

Notice: Use a generated passphrase or choose a passphrase of 8 or
more characters.
        To ensure the authenticity of the peering relationship, use
a phrase or sequence of characters that would be hard to guess.

Enter the passphrase:
Confirm the passphrase:

Clusters cluster02 and cluster01 are peered.
```

Entrez la phrase de passe de la relation homologue lorsque vous y êtes invité.

3. Vérifiez que la relation entre clusters a été créée :

```
cluster peer show -instance
```

```
cluster01::> cluster peer show -instance

                                Peer Cluster Name: cluster02
                    Remote Intercluster Addresses: 192.140.112.101,
192.140.112.102
               Availability of the Remote Cluster: Available
                              Remote Cluster Name: cluster2
                              Active IP Addresses: 192.140.112.101,
192.140.112.102
                            Cluster Serial Number: 1-80-123456
                   Address Family of Relationship: ipv4
               Authentication Status Administrative: no-authentication
                  Authentication Status Operational: absent
                                  Last Update Time: 02/05 21:05:41
                       IPspace for the Relationship: Default
```

4. Vérifier la connectivité et l'état des nœuds de la relation peer-to-peer :

```
cluster peer health show
```

```
cluster01::> cluster peer health show
Node       cluster-Name                Node-Name
             Ping-Status               RDB-Health Cluster-Health
Avail…
---------- --------------------------- ---------  ---------------
--------
cluster01-01
           cluster02                   cluster02-01
             Data: interface_reachable
             ICMP: interface_reachable true       true
true
                                       cluster02-02
             Data: interface_reachable
             ICMP: interface_reachable true       true
true
cluster01-02
           cluster02                   cluster02-01
             Data: interface_reachable
             ICMP: interface_reachable true       true
true
                                       cluster02-02
             Data: interface_reachable
             ICMP: interface_reachable true       true
true
```

D'autres façons de le faire dans ONTAP

Pour effectuer ces tâches avec…	Voir ce contenu…
System Manager Classic (disponible avec ONTAP 9.7 et versions antérieures)	"Présentation de la préparation de la reprise sur incident de volume"

Créer une relation SVM peer-to-peer

Vous pouvez utiliser le `vserver peer create` Commande pour créer une relation entre les SVM sur des clusters locaux et distants.

Avant de commencer

- Les clusters source et destination doivent être associés.

- Les clusters doivent exécuter ONTAP 9.3. (Si les clusters exécutent ONTAP 9.2 ou une version antérieure, reportez-vous aux procédures de la "ce document archivé".)
- Vous devez avoir des relations de pairs « pré-autorisées » pour les SVM sur le cluster distant.

  Pour plus d'informations, voir "Création d'une relation entre clusters".

Description de la tâche

Dans ONTAP 9.2 et versions antérieures, vous pouvez autoriser une relation de pairs pour un seul SVM à la fois. Cela signifie que vous devez exécuter `vserver peer accept` Chaque fois que vous autorisez une relation de SVM peer en attente.

Depuis ONTAP 9.3, vous pouvez « pré-autoriser » des relations entre pairs pour plusieurs SVM en répertoriant les SVM dans le `-initial-allowed-vserver` option lors de la création d'une relation de type cluster. Pour plus d'informations, voir "Création d'une relation entre clusters".

Étapes

1. Sur le cluster destination de protection des données, afficher les SVM qui sont pré-autorisés pour le peering :

   `vserver peer permission show`

   ```
   cluster02::> vserver peer permission show
   Peer Cluster         Vserver               Applications
   -------------------  --------------------  --------------------
   cluster02            vs1,vs2               snapmirror
   ```

2. Sur le cluster source de protection des données, créez une relation entre pairs et un SVM pré-autorisé sur le cluster cible de protection des données :

   `vserver peer create -vserver` *`local_SVM`* `-peer-vserver` *`remote_SVM`*

   Pour connaître la syntaxe complète de la commande, reportez-vous à la page man.

   L'exemple suivant crée une relation de pairs entre le SVM local `pvs1` Et le SVM distant pré-autorisé `vs1`:

   ```
   cluster01::> vserver peer create -vserver pvs1 -peer-vserver vs1
   ```

3. Vérifier la relation entre SVM et :

   `vserver peer show`

```
cluster01::> vserver peer show
            Peer        Peer                           Peering
Remote
Vserver     Vserver     State        Peer Cluster      Applications
Vserver
----------- ----------- ------------ ----------------- --------------
---------
pvs1        vs1         peered       cluster02         snapmirror
vs1
```

Ajouter une relation SVM peer-to-peer intercluster

Si vous créez un SVM après avoir configuré une relation de cluster peer-to-peer, vous devez ajouter manuellement une relation de peer-to-peer pour la SVM. Vous pouvez utiliser le `vserver peer create` Commande pour créer une relation entre SVM. Une fois la relation homologue créée, vous pouvez exécuter `vserver peer accept` sur le cluster distant, afin d'autoriser la relation peer-to-peer.

Avant de commencer

Les clusters source et destination doivent être associés.

Description de la tâche

Vous pouvez créer des relations peer-to-peer entre les SVM et dans le même cluster pour la sauvegarde des données locales. Pour plus d'informations, reportez-vous à la section `vserver peer create` page de manuel.

Les administrateurs utilisent parfois le `vserver peer reject` Commande permettant de refuser une relation SVM peer-to-peer proposée. Si la relation entre les SVM se trouve dans le `rejected` état, vous devez supprimer la relation pour en créer une nouvelle. Pour plus d'informations, reportez-vous à la section `vserver peer delete` page de manuel.

Étapes

1. Sur le cluster source de protection des données, créez une relation entre pairs et un SVM sur le cluster cible de protection des données :

   `vserver peer create -vserver` *`local_SVM`* `-peer-vserver` *`remote_SVM`* `-applications snapmirror|file-copy|lun-copy -peer-cluster` *`remote_cluster`*

   L'exemple suivant crée une relation de pairs entre le SVM local`pvs1` Et le SVM distant`vs1`

   ```
   cluster01::> vserver peer create -vserver pvs1 -peer-vserver vs1
   -applications snapmirror -peer-cluster cluster02
   ```

   Si les SVM locaux et distants ont les mêmes noms, vous devez utiliser un *local name* pour créer la relation SVM peer :

```
cluster01::> vserver peer create -vserver vs1 -peer-vserver
vs1 -applications snapmirror -peer-cluster cluster01
-local-name cluster1vs1LocallyUniqueName
```

2. Sur le cluster source de protection des données, vérifiez que la relation de pairs a été initiée :

   `vserver peer show-all`

   Pour connaître la syntaxe complète de la commande, reportez-vous à la page man.

   L'exemple suivant montre que la relation de pairs entre SVM`pvs1` Et SVM`vs1` a été lancé :

```
cluster01::> vserver peer show-all
            Peer        Peer                      Peering
Vserver     Vserver     State      Peer Cluster   Applications
--------    --------    ---------  -------------  ------------
pvs1        vs1         initiated   Cluster02       snapmirror
```

3. Sur le cluster destination de protection des données, afficher la relation SVM peer-to-peer en attente :

   `vserver peer show`

   Pour connaître la syntaxe complète de la commande, reportez-vous à la page man.

   L'exemple suivant répertorie les relations homologues en attente pour `cluster02`:

```
cluster02::> vserver peer show

                  Peer              Peer
Vserver           Vserver           State
-----------       -----------       ------------
vs1               pvs1              pending
```

4. Sur le cluster cible de protection des données, autoriser la relation peer-to-peer en attente :

   `vserver peer accept -vserver` *`local_SVM`* `-peer-vserver` *`remote_SVM`*

   Pour connaître la syntaxe complète de la commande, reportez-vous à la page man.

   L'exemple suivant autorise la relation de pairs entre la SVM locale `vs1` Et le SVM distant `pvs1`:

```
cluster02::> vserver peer accept -vserver vs1 -peer-vserver pvs1
```

5. Vérifier la relation entre SVM et :

```
vserver peer show
```

```
cluster01::> vserver peer show
            Peer        Peer                           Peering
Remote
Vserver     Vserver     State        Peer Cluster      Applications
Vserver
----------- ----------- ------------ ----------------- --------------
---------
pvs1        vs1         peered       cluster02         snapmirror
vs1
```

Activer le chiffrement de peering de cluster sur une relation de pairs existante

Depuis ONTAP 9.6, le chiffrement de peering de cluster est activé par défaut sur toutes les relations de peering de cluster que nous avons récemment créées. Le chiffrement de peering de cluster utilise une clé pré-partagée (PSK) et la couche de sécurité du transport (TLS) pour sécuriser les communications de peering entre clusters. Cela ajoute une couche de sécurité supplémentaire entre les clusters avec points.

Description de la tâche

Si vous mettez à niveau des clusters de peering vers ONTAP 9.6 ou version ultérieure et que la relation de peering a été créée dans ONTAP 9.5 ou version antérieure, le chiffrement de peering de cluster doit être activé manuellement après la mise à niveau. Les deux clusters de la relation de peering doivent exécuter ONTAP 9.6 ou version ultérieure afin de permettre le cryptage du cluster peering.

Étapes

1. Sur le cluster de destination, activez le chiffrement pour les communications avec le cluster source :

   ```
   cluster peer modify source_cluster -auth-status-admin use-authentication
   -encryption-protocol-proposed tls-psk
   ```

2. Entrez une phrase de passe lorsque vous y êtes invité.
3. Sur le cluster source de protection des données, activez le chiffrement pour la communication avec le cluster cible de protection des données :

   ```
   cluster peer modify data_protection_destination_cluster -auth-status-admin
   use-authentication -encryption-protocol-proposed tls-psk
   ```

4. Indiquez la même phrase secrète entrée sur le cluster de destination.

Retirer le cryptage de peering de cluster d'une relation de pairs existante

Par défaut, le cryptage de peering de cluster est activé sur toutes les relations entre pairs

créées dans ONTAP 9.6 ou version ultérieure. Si vous ne souhaitez pas utiliser le cryptage pour les communications de peering intercluster, vous pouvez le désactiver.

Étapes

1. Sur le cluster de destination, modifiez les communications avec le cluster source pour interrompre l'utilisation du chiffrement de peering de cluster :
   - Pour supprimer le cryptage mais maintenir l'authentification, entrez :

     ```
     cluster peer modify <source_cluster> -auth-status-admin use-
     authentication -encryption-protocol-proposed none
     ```

   - Pour supprimer le cryptage et l'authentification :
     i. Modifiez la stratégie de peering de cluster pour autoriser l'accès non authentifié :

        ```
        cluster peer policy modify -is-unauthenticated-access-permitted
        true
        ```

     ii. Modifier le cryptage et l'accès d'authentification :

        ```
        cluster peer modify <source_cluster> -auth-status no-
        authentication
        ```

2. Lorsque vous y êtes invité, saisissez la phrase de passe.
3. Confirmez la phrase de passe en la saisissant à nouveau.
4. Sur le cluster source, désactiver le cryptage pour la communication avec le cluster destination :
   - Pour supprimer le cryptage mais maintenir l'authentification, entrez :

     ```
     cluster peer modify <destination_cluster> -auth-status-admin use-
     authentication -encryption-protocol-proposed none
     ```

   - Pour supprimer le cryptage et l'authentification :
     i. Modifiez la stratégie de peering de cluster pour autoriser l'accès non authentifié :

        ```
        cluster peer policy modify -is-unauthenticated-access-permitted
        true
        ```

     ii. Modifier le cryptage et l'accès d'authentification :

        ```
        cluster peer modify <destination_cluster> -auth-status no-
        authentication
        ```

5. Lorsque vous y êtes invité, entrez et saisissez à nouveau la phrase de passe que vous avez utilisée sur le cluster de destination.