



Cluster- und SVM-Peering mit der CLI

ONTAP 9

NetApp
April 24, 2024

Inhalt

- Cluster- und SVM-Peering mit der CLI 1
 - Übersicht über Cluster- und SVM-Peering mit der CLI 1
 - Cluster- und SVM-Peering werden vorbereitet 1
 - Konfigurieren Sie Intercluster LIFs 5
 - Konfiguration von Peer-Beziehungen 18
 - Cluster-Peering-Verschlüsselung für vorhandene Peer-Beziehungen aktivieren 26
 - Entfernen Sie die Cluster-Peering-Verschlüsselung von einer vorhandenen Peer-Beziehung 27

Cluster- und SVM-Peering mit der CLI

Übersicht über Cluster- und SVM-Peering mit der CLI

Sie können Peer-Beziehungen zwischen Quell- und Ziel-Clustern und zwischen Quell- und Ziel-Storage Virtual Machines (SVMs) erstellen. Sie müssen Peer-Beziehungen zwischen diesen Einheiten erstellen, bevor Sie Snapshot Kopien mit SnapMirror replizieren können.

ONTAP 9.3 bietet Verbesserungen, die die Konfiguration von Peer-Beziehungen zwischen Clustern und SVMs vereinfachen. Die Peering-Verfahren für Cluster und SVMs sind für alle ONTAP 9-Versionen verfügbar. Sie sollten das entsprechende Verfahren für Ihre ONTAP-Version verwenden.

Die entsprechenden Verfahren werden über die Befehlszeilenschnittstelle (CLI) und nicht mit System Manager oder einem automatisierten Scripting-Tool ausgeführt.

Cluster- und SVM-Peering werden vorbereitet

Peering-Grundlagen

Sie müssen *Peer-Beziehungen* zwischen Quell- und Ziel-Clustern und zwischen Quell- und Ziel-SVMs erstellen, bevor Sie Snapshot Kopien mit SnapMirror replizieren können. Eine Peer-Beziehung definiert Netzwerkverbindungen, mit denen Cluster und SVMs einen sicheren Datenaustausch ermöglichen.

Cluster und SVMs in Peer-Beziehungen kommunizieren über das Cluster-Netzwerk mithilfe von logischen Schnittstellen (LIFs) zwischen Clustern. Eine Intercluster LIF ist eine LIF, die den „Intercluster-Core“-Netzwerkschnittstellungsservice unterstützt und normalerweise mithilfe der Service-Richtlinie zur Netzwerkschnittstelle „default-intercluster“ erstellt wird. Sie müssen für jeden Node in den Clustern, die Peering durchführen, Intercluster-LIFs erstellen.

Intercluster-LIFs verwenden Routen, die zur System-SVM gehören, der sie zugewiesen sind. ONTAP erstellt innerhalb eines IPspaces automatisch eine System-SVM für die Kommunikation auf Cluster-Ebene.

Fan-out- und Kaskadentopologien werden unterstützt. In einer Kaskadentopologie müssen lediglich Cluster-Netzwerke zwischen den primären und sekundären Clustern sowie zwischen den sekundären und tertiären Clustern erstellt werden. Sie müssen kein Cluster-Netzwerk zwischen dem primären und dem tertiären Cluster erstellen.



Ein Administrator kann den Intercluster-Core-Service aus der Standard-Intercluster-Service-Richtlinie entfernen (aber nicht ratsam). Wenn dies der Fall ist, sind LIFs, die mit „default-intercluster“ erstellt wurden, tatsächlich keine Intercluster-LIFs. Verwenden Sie den folgenden Befehl, um zu überprüfen, ob die Cluster-Standard-Service-Richtlinie den Intercluster-Core-Service enthält:

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

Voraussetzungen für Cluster-Peering

Bevor Sie Cluster-Peering einrichten, sollten Sie bestätigen, dass Konnektivität, Port, IP-Adresse, Subnetz, Firewall, Und die Anforderungen für die Cluster-Benennung erfüllen.



Ab ONTAP 9.6 bietet Cluster-Peer-Verschlüsselung standardmäßig TLS 1.2 AES-256 GCM-Verschlüsselung für Datenreplizierung. Die Standard-Sicherheitskiffren („PSK-AES256-GCM-SHA364“) sind erforderlich, damit Cluster-Peering funktioniert, auch wenn die Verschlüsselung deaktiviert ist.

Ab ONTAP 9.11.1 sind die DHE-PSK-Sicherheitsschlüssel standardmäßig verfügbar.

Konnektivitätsanforderungen erfüllen

Jede Intercluster LIF auf dem lokalen Cluster muss in der Lage sein, mit jeder Intercluster LIF auf dem Remote-Cluster zu kommunizieren.

Es ist zwar nicht erforderlich, aber in der Regel ist es einfacher, die IP-Adressen zu konfigurieren, die für Intercluster LIFs im selben Subnetz verwendet werden. Die IP-Adressen können sich im gleichen Subnetz wie Daten-LIFs oder in einem anderen Subnetz befinden. Das in jedem Cluster verwendete Subnetz muss die folgenden Anforderungen erfüllen:

- Das Subnetz muss zur Broadcast-Domäne gehören, die die Ports enthält, die für die Kommunikation zwischen Clustern verwendet werden.
- Das Subnetz muss über genügend IP-Adressen verfügen, um einer Intercluster LIF pro Node zuzuweisen.

Beispielsweise muss in einem Cluster mit vier Nodes das für die Kommunikation zwischen Clustern verwendete Subnetz vier verfügbare IP-Adressen haben.

Jeder Node muss über eine Intercluster-LIF mit einer IP-Adresse im Intercluster-Netzwerk verfügen.

Intercluster-LIFs können eine IPv4-Adresse oder eine IPv6-Adresse besitzen.



Mit ONTAP können Sie Ihre Peering-Netzwerke von IPv4 zu IPv6 migrieren, da Sie optional beide Protokolle gleichzeitig auf den Intercluster LIFs anwesend sein können. In früheren Versionen waren alle Cluster-Beziehungen für einen gesamten Cluster entweder IPv4 oder IPv6. Somit war eine Änderung der Protokolle ein potenziell störendes Ereignis.

Port-Anforderungen

Sie können dedizierte Ports für die Cluster-übergreifende Kommunikation verwenden oder vom Datennetzwerk verwendete Ports freigeben. Ports müssen folgende Anforderungen erfüllen:

- Alle Ports, die für die Kommunikation mit einem bestimmten Remote-Cluster verwendet werden, müssen sich im selben IPspace befinden.

Sie können mehrere IPspaces verwenden, um mit mehreren Clustern zu Punkten. Paarweise ist Vollmaschenverbindung nur innerhalb eines IPspaces erforderlich.

- Die Broadcast-Domäne, die für die Intercluster-Kommunikation verwendet wird, muss mindestens zwei Ports pro Node enthalten, damit die Intercluster-Kommunikation von einem Port zu einem anderen Port ausfallen kann.

Ports, die einer Broadcast-Domäne hinzugefügt werden, können physische Netzwerk-Ports, VLANs oder Interface Groups (iffrps) sein.

- Alle Ports müssen verkabelt sein.
- Alle Ports müssen sich in einem ordnungsgemäßen Zustand befinden.
- Die MTU-Einstellungen der Ports müssen konsistent sein.

Anforderungen an die Firewall



Ab ONTAP 9.10.1 sind Firewall-Richtlinien veraltet und werden vollständig durch LIF-Servicerichtlinien ersetzt. Weitere Informationen finden Sie unter "[Konfigurieren Sie Firewallrichtlinien für LIFs](#)".

Firewalls und die Cluster-übergreifende Firewall-Richtlinie müssen folgende Protokolle zulassen:

- Bidirektionaler ICMP-Datenverkehr
- Bidirektionaler, initiiertes TCP-Datenverkehr zu den IP-Adressen aller Intercluster-LIFs über die Ports 11104 und 11105
- Bidirektionales HTTPS zwischen den Intercluster-LIFs

Obwohl HTTPS nicht erforderlich ist, wenn Sie Cluster-Peering über die CLI einrichten, wird später HTTPS erforderlich, wenn Sie den Datenschutz mit System Manager konfigurieren.

Der Standardwert `intercluster` Firewall-Richtlinie ermöglicht den Zugriff über das HTTPS-Protokoll und über alle IP-Adressen (0.0.0.0/0). Sie können die Richtlinie bei Bedarf ändern oder ersetzen.

Cluster-Anforderungen erfüllen

Cluster müssen die folgenden Anforderungen erfüllen:

- Ein Cluster kann nicht in einer Peer-Beziehung mit mehr als 255 Clustern sein.

Verwenden Sie gemeinsam genutzte oder dedizierte Ports

Sie können dedizierte Ports für die Cluster-übergreifende Kommunikation verwenden oder vom Datennetzwerk verwendete Ports freigeben. Bei der Entscheidung, ob Ports gemeinsam genutzt werden sollen, müssen Sie die Netzwerkbandbreite, das Replikationsintervall und die Portverfügbarkeit berücksichtigen.



Sie können Ports für einen Peering Cluster gemeinsam nutzen, während Sie auf dem anderen dedizierte Ports verwenden.

Netzwerkbandbreite

Wenn Sie ein High-Speed-Netzwerk wie 10 GbE haben, verfügen Sie möglicherweise über ausreichend lokale LAN-Bandbreite, um eine Replikation mit denselben 10 GbE-Ports durchzuführen, die für den Datenzugriff verwendet werden.

Selbst dann sollten Sie Ihre verfügbare WAN-Bandbreite mit Ihrer LAN-Bandbreite vergleichen. Wenn die verfügbare WAN-Bandbreite deutlich weniger als 10 GbE beträgt, müssen Sie möglicherweise dedizierte Ports

verwenden.



Eine Ausnahme von dieser Regel besteht unter Umständen darin, dass alle oder viele Nodes im Cluster Daten replizieren. In diesem Fall wird die Bandbreitenauslastung normalerweise über verschiedene Nodes verteilt.

Wenn Sie keine dedizierten Ports verwenden, sollte die MTU-Größe (Maximum Transmission Unit) des Replikationsnetzwerks in der Regel mit der MTU-Größe des Datennetzwerks übereinstimmen.

Replikationsintervall

Wenn die Replizierung in Zeiten geringerer Auslastung stattfindet, sollten Sie in der Lage sein, Daten-Ports für die Replizierung zu nutzen, auch ohne eine 10-GbE-LAN-Verbindung.

Wenn die Replizierung während der normalen Geschäftszeiten stattfindet, müssen Sie die Menge der zu replizierenden Daten berücksichtigen und entscheiden, ob es so viel Bandbreite erfordert, dass es Konflikte mit den Datenprotokollen verursachen kann. Wenn die Netzwerkauslastung durch Datenprotokolle (SMB, NFS, iSCSI) über 50 % liegt, sollten dedizierte Ports für die Kommunikation zwischen Clustern verwendet werden. Damit wird bei einem Node-Failover die Performance nicht beeinträchtigt.

Port-Verfügbarkeit

Wenn Sie feststellen, dass der Replizierungsverkehr den Datenverkehr beeinträchtigt, können Sie LIFs zwischen Clustern auf jeden anderen Cluster-fähigen, gemeinsam genutzten Port desselben Nodes migrieren.

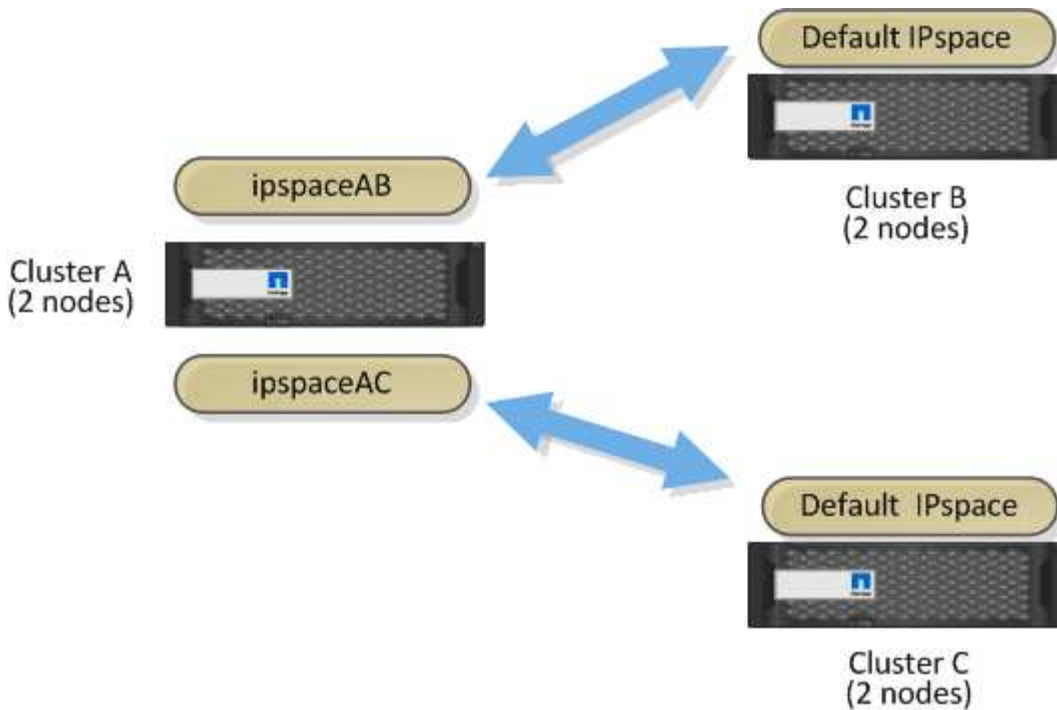
Sie können auch VLAN-Ports für die Replikation zuweisen. Die Bandbreite des Ports wird von allen VLANs und dem Basis-Port gemeinsam genutzt.

Verwenden Sie benutzerdefinierte IPspaces, um den Replikationsverkehr zu isolieren

Sie können benutzerdefinierte IPspaces verwenden, um die Interaktionen eines Clusters mit seinen Peers voneinander zu trennen. Diese Konfiguration, die als *designierte Intercluster-Konnektivität* bezeichnet wird, ermöglicht Service-Providern die Isolierung des Replizierungsdatenverkehrs in mandantenfähigen Umgebungen.

Angenommen, Sie möchten den Replizierungsverkehr zwischen Cluster A und Cluster B vom Replizierungsdatenverkehr zwischen Cluster A und Cluster C trennen. Hierzu können Sie auf Cluster A zwei IPspaces erstellen.

Ein IPspace enthält die Intercluster LIFs, die Sie zur Kommunikation mit Cluster B. verwenden. Die andere enthält die Intercluster-LIFs, die Sie für die Kommunikation mit Cluster C verwenden, wie in der folgenden Abbildung dargestellt.



Informationen zur benutzerdefinierten Konfiguration von IPspace finden Sie im Handbuch_Network Management_.

Konfigurieren Sie Intercluster LIFs

Konfigurieren Sie Intercluster-LIFs an gemeinsam genutzten Datenports

Sie können Intercluster-LIFs an Ports konfigurieren, die gemeinsam mit dem Datennetzwerk verwendet werden. Auf diese Weise wird die Anzahl der Ports reduziert, die Sie für Intercluster-Netzwerke benötigen.

Schritte

1. Liste der Ports im Cluster:

```
network port show
```

Eine vollständige Befehlssyntax finden Sie in der man-Page.

Im folgenden Beispiel werden die Netzwerkports in angezeigt `cluster01`:

```
cluster01::> network port show
```

(Mbps)						Speed
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. Intercluster LIFs können Sie entweder auf einer Administrator-SVM (Standard-IPspace) oder einer System-SVM (Custom IPspace) erstellen:

Option	Beschreibung
Im ONTAP 9.6 und höher:	<code>network interface create -vserver system_SVM -lif LIF_name -service -policy default-intercluster -home -node node -home-port port -address port_IP -netmask netmask</code>
In ONTAP 9.5 und früher:	<code>network interface create -vserver system_SVM -lif LIF_name -role intercluster -home-node node -home -port port -address port_IP -netmask netmask</code>

Eine vollständige Befehlssyntax finden Sie in der man-Page.

Im folgenden Beispiel werden Intercluster-LIFs erstellt `cluster01_icl01` Und `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. Überprüfen Sie, ob die Intercluster-LIFs erstellt wurden:

Option	Beschreibung
Im ONTAP 9.6 und höher:	<code>network interface show -service-policy default-intercluster</code>
In ONTAP 9.5 und früher:	<code>network interface show -role intercluster</code>

Eine vollständige Befehlssyntax finden Sie in der man-Page.

```
cluster01::> network interface show -service-policy default-intercluster
Current Is
Vserver      Logical      Status      Network      Current
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. Vergewissern Sie sich, dass die Intercluster-LIFs redundant sind:

Option	Beschreibung
Im ONTAP 9.6 und höher:	network interface show -service-policy default-intercluster -failover
In ONTAP 9.5 und früher:	network interface show -role intercluster -failover

Eine vollständige Befehlssyntax finden Sie in der man-Page.

Das folgende Beispiel zeigt, dass die Intercluster-LIFs sind `cluster01_icl01` Und `cluster01_icl02` Auf dem `e0c` Ein Failover des Ports zum erfolgt `e0d` Port:

```
cluster01::> network interface show -service-policy default-intercluster
-failover
```

Vserver	Logical Interface	Home Node:Port	Failover Policy	Failover 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	

Konfigurieren Sie Intercluster-LIFs auf dedizierten Ports

Sie können Intercluster-LIFs auf dedizierten Ports konfigurieren. Dadurch wird typischerweise die verfügbare Bandbreite für den Replizierungsverkehr erhöht.

Schritte

1. Liste der Ports im Cluster:

```
network port show
```

Eine vollständige Befehlssyntax finden Sie in der man-Page.

Im folgenden Beispiel werden die Netzwerkports in angezeigt `cluster01`:

```
cluster01::> network port show
```

(Mbps)		Speed				
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. Bestimmen Sie, welche Ports für die Intercluster-Kommunikation verfügbar sind:

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

Eine vollständige Befehlssyntax finden Sie in der man-Page.

Im folgenden Beispiel werden die Ports angezeigt e0e Und e0f Es wurden keine LIFs zugewiesen:

```
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. Erstellen Sie eine Failover-Gruppe für die dedizierten Ports:

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

Im folgenden Beispiel werden Ports zugewiesen e0e Und e0f Zur Failover-Gruppe intercluster01 Auf der System-SVM 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. Vergewissern Sie sich, dass die Failover-Gruppe erstellt wurde:

```
network interface failover-groups show
```

Eine vollständige Befehlssyntax finden Sie in der man-Page.

```
cluster01::> network interface failover-groups show
```

Vserver	Group	Failover 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. Erstellen Sie Intercluster-LIFs auf der System-SVM und weisen Sie sie der Failover-Gruppe zu.

Option	Beschreibung
Im ONTAP 9.6 und höher:	<pre>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</pre>

Option	Beschreibung
In ONTAP 9.5 und früher:	network interface create -vserver <i>system_SVM</i> -lif <i>LIF_name</i> -role intercluster -home-node <i>node</i> -home-port <i>port</i> -address <i>port_IP</i> -netmask <i>netmask</i> -failover-group <i>failover_group</i>

Eine vollständige Befehlssyntax finden Sie in der man-Page.

Im folgenden Beispiel werden Intercluster-LIFs erstellt `cluster01_icl01` Und `cluster01_icl02` In der Failover-Gruppe `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. Überprüfen Sie, ob die Intercluster-LIFs erstellt wurden:

Option	Beschreibung
Im ONTAP 9.6 und höher:	network interface show -service-policy default-intercluster
In ONTAP 9.5 und früher:	network interface show -role intercluster

Eine vollständige Befehlssyntax finden Sie in der man-Page.

```

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. Vergewissern Sie sich, dass die Intercluster-LIFs redundant sind:

Option	Beschreibung
Im ONTAP 9.6 und höher:	<code>network interface show -service-policy default-intercluster -failover</code>
In ONTAP 9.5 und früher:	<code>network interface show -role intercluster -failover</code>

Eine vollständige Befehlssyntax finden Sie in der man-Page.

Das folgende Beispiel zeigt, dass die Intercluster-LIFs sind `cluster01_icl01` Und `cluster01_icl02` Auf der SVM `e0e` Ein Failover des Ports zum erfolgt `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

```

Konfigurieren Sie Intercluster LIFs in benutzerdefinierten IPspaces

Sie können Intercluster-LIFs in benutzerdefinierten IPspaces konfigurieren. Auf diese Weise lässt sich der Replizierungs-Datenverkehr in mandantenfähigen Umgebungen isolieren.

Wenn Sie einen benutzerdefinierten IPspace erstellen, erstellt das System eine Storage Virtual Machine (SVM) des Systems, die als Container für die Systemobjekte in diesem IPspace dient. Sie können die neue SVM als Container für alle Intercluster LIFs im neuen IPspace verwenden. Die neue SVM hat den gleichen Namen wie der benutzerdefinierte IPspace.

Schritte

1. Liste der Ports im Cluster:

```
network port show
```

Eine vollständige Befehlssyntax finden Sie in der man-Page.

Im folgenden Beispiel werden die Netzwerkports in angezeigt `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. Erstellen Sie benutzerdefinierte IPspaces auf dem Cluster:

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

Im folgenden Beispiel wird der benutzerdefinierte IPspace erstellt `ipspace-IC1`:

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

3. Bestimmen Sie, welche Ports für die Intercluster-Kommunikation verfügbar sind:

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

Eine vollständige Befehlssyntax finden Sie in der man-Page.

Im folgenden Beispiel werden die Ports angezeigt e0e Und e0f Es wurden keine LIFs zugewiesen:

```
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. Entfernen Sie die verfügbaren Ports aus der Standard-Broadcast-Domäne:

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

Ein Port darf nicht mehrere Broadcast-Domänen gleichzeitig haben. Eine vollständige Befehlssyntax finden Sie in der man-Page.

Im folgenden Beispiel werden Ports entfernt e0e Und e0f In der Standard-Broadcast-Domäne:

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

5. Vergewissern Sie sich, dass die Ports aus der Standard-Broadcast-Domäne entfernt wurden:

```
network port show
```

Eine vollständige Befehlssyntax finden Sie in der man-Page.

Im folgenden Beispiel werden die Ports angezeigt e0e Und e0f Wurden aus der Standard-Broadcast-Domäne entfernt:


```
cluster01::> network port show
```

Node	Port	IPspace	Broadcast Domain	Link	MTU	Speed (Mbps) 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. Erstellen Sie eine Broadcast-Domäne im benutzerdefinierten IPspace:

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

Im folgenden Beispiel wird die Broadcast-Domäne erstellt `ipspace-IC1-bd` im 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. Vergewissern Sie sich, dass die Broadcast-Domäne erstellt wurde:

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

Eine vollständige Befehlssyntax finden Sie in der man-Page.

```

cluster01::> network port broadcast-domain show
IPspace Broadcast
Name      Domain Name      MTU      Port List
-----
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. Erstellen von Intercluster-LIFs auf der System-SVM, und weisen Sie sie der Broadcast-Domäne zu:

Option	Beschreibung
Im ONTAP 9.6 und höher:	<pre> network interface create -vserver system_SVM -lif LIF_name -service -policy default-intercluster -home -node node -home-port port -address port_IP -netmask netmask </pre>
In ONTAP 9.5 und früher:	<pre> network interface create -vserver system_SVM -lif LIF_name -role intercluster -home-node node -home -port port -address port_IP -netmask netmask </pre>

Die LIF wird in der Broadcast-Domäne erstellt, der der Home-Port zugewiesen ist. Die Broadcast-Domäne besitzt eine Standard-Failover-Gruppe mit demselben Namen wie die Broadcast-Domäne. Eine vollständige Befehlssyntax finden Sie in der man-Page.

Im folgenden Beispiel werden Intercluster-LIFs erstellt `cluster01_icl01` Und `cluster01_icl02` In der Broadcast-Domäne `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. Überprüfen Sie, ob die Intercluster-LIFs erstellt wurden:

Option	Beschreibung
Im ONTAP 9.6 und höher:	<code>network interface show -service-policy default-intercluster</code>
In ONTAP 9.5 und früher:	<code>network interface show -role intercluster</code>

Eine vollständige Befehlssyntax finden Sie in der man-Page.

```
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. Vergewissern Sie sich, dass die Intercluster-LIFs redundant sind:

Option	Beschreibung
Im ONTAP 9.6 und höher:	network interface show -service-policy default-intercluster -failover
In ONTAP 9.5 und früher:	network interface show -role intercluster -failover

Eine vollständige Befehlssyntax finden Sie in der man-Page.

Das folgende Beispiel zeigt, dass die Intercluster-LIFs sind `cluster01_icl01` Und `cluster01_icl02` Auf der SVM `e0e` Port-Failover zum Port `e0f`:

```
cluster01::> network interface show -service-policy default-intercluster
-failover
```

Vserver	Logical Interface	Home Node:Port	Failover Policy	Failover 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	

Konfiguration von Peer-Beziehungen

Erstellen einer Cluster-Peer-Beziehung

Sie können das verwenden `cluster peer create` Befehl zum Erstellen einer Peer-Beziehung zwischen einem lokalen und einem Remote-Cluster. Nachdem die Peer-Beziehung erstellt wurde, können Sie ausführen `cluster peer create` Im Remote-Cluster zur Authentifizierung beim lokalen Cluster.

Bevor Sie beginnen

- Sie müssen auf jedem Node in den Clustern, die Peering durchführen, Intercluster LIFs erstellt haben.
- Die Cluster müssen ONTAP 9.3 oder höher ausführen. (Wenn auf den Clustern ONTAP 9.2 oder eine frühere Version ausgeführt wird, lesen Sie die Verfahren in ["Dieses archivierte Dokument"](#).)



Schritte

Führen Sie diese Aufgabe über ONTAP System Manager oder die ONTAP-CLI aus.

System Manager

1. Klicken Sie im lokalen Cluster auf **Cluster > Einstellungen**.
2. Klicken Sie im Abschnitt **Intercluster-Einstellungen** auf **Netzwerkschnittstellen hinzufügen** und fügen Sie dem Cluster Intercluster-Netzwerkschnittstellen hinzu.

Wiederholen Sie diesen Schritt auf dem Remote-Cluster.

3. Klicken Sie im Remote-Cluster auf **Cluster > Einstellungen**.
4. Klicken Sie Auf  Wählen Sie im Abschnitt **Cluster Peers** die Option **Passphrase generieren** aus.
5. Wählen Sie die Remote-ONTAP-Cluster-Version aus.
6. Generierte Passphrase kopieren.
7. Klicken Sie im lokalen Cluster unter **Cluster Peers** auf  Und wählen Sie **Peer Cluster**.
8. Fügen Sie im Fenster **Peer Cluster** die Passphrase ein und klicken Sie auf **Cluster-Peering initiieren**.

CLI

1. Erstellen Sie auf dem Ziel-Cluster eine Peer-Beziehung mit dem Quell-Cluster:

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

Wenn Sie beides angeben `-generate-passphrase` Und `-peer-addr`s, Nur der Cluster, dessen Intercluster LIFs in angegeben sind `-peer-addr`s Kann das generierte Passwort verwenden.

Sie können die ignorieren `-ip>space` Option, wenn kein benutzerdefinierter IPspace verwendet wird. Eine vollständige Befehlssyntax finden Sie in der man-Page.

Wenn Sie die Peering-Beziehung in ONTAP 9.6 oder höher erstellen und keine clusterübergreifende Peering-Kommunikation verschlüsselt werden soll, müssen Sie den verwenden `-encryption -protocol-proposed none` Option zum Deaktivieren der Verschlüsselung.

Im folgenden Beispiel wird eine Cluster-Peer-Beziehung mit einem nicht festgelegten Remote-Cluster erstellt und Peer-Beziehungen zu SVMs vorab autorisiert `vs1` Und `vs2` Auf dem lokalen Cluster:

```
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.
```

Im folgenden Beispiel wird eine Cluster-Peer-Beziehung zum Remote-Cluster unter LIF IP-Adressen 192.140.112.103 und 192.140.112.104 erstellt und eine Peer-Beziehung mit jeder SVM auf dem lokalen Cluster vorab autorisiert:

```
cluster02::> cluster peer create -generate-passphrase -peer-addr
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.
```

Im folgenden Beispiel wird eine Cluster-Peer-Beziehung mit einem nicht festgelegten Remote-Cluster erstellt und Peer-Beziehungen zu SVMs vorab autorisiert `vs1` und `vs2` auf dem lokalen Cluster:

```
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. Authentifizierung des Quellclusters auf dem Quellcluster beim Ziel-Cluster:

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

Eine vollständige Befehlssyntax finden Sie in der man-Page.

Im folgenden Beispiel wird der lokale Cluster an den Remote-Cluster unter LIF-IP-Adressen 192.140.112.101 und 192.140.112.102 authentifiziert:

```
cluster01::> cluster peer create -peer-addr  
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.

Geben Sie die Passphrase für die Peer-Beziehung ein, wenn Sie dazu aufgefordert werden.

3. Vergewissern Sie sich, dass die Cluster-Peer-Beziehung erstellt wurde:

```
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. Prüfen Sie die Konnektivität und den Status der Knoten in der Peer-Beziehung:

```
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
```

Weitere Möglichkeiten dies in ONTAP zu tun

So führen Sie diese Aufgaben durch:	Inhalt anzeigen...
Der neu gestaltete System Manager (verfügbar ab ONTAP 9.7)	"Bereiten Sie sich auf Spiegelung und Vaulting vor"
System Manager Classic (verfügbar mit ONTAP 9.7 und älter)	"Überblick über die Vorbereitung der Volume Disaster Recovery"

Erstellen einer Cluster-übergreifende SVM-Peer-Beziehung

Sie können das verwenden `vserver peer create` Befehl zum Erstellen einer Peer-Beziehung zwischen SVMs auf lokalen und Remote-Clustern.

Bevor Sie beginnen

- Die Quell- und Ziel-Cluster müssen Peering durchgeführt werden.
- Auf den Clustern muss ONTAP 9.3 ausgeführt werden. (Wenn auf den Clustern ONTAP 9.2 oder eine frühere Version ausgeführt wird, lesen Sie die Verfahren in ["Dieses archivierte Dokument"](#).)
- Es müssen „vorab autorisierte“ Peer-Beziehungen für die SVMs auf dem Remote-Cluster vorhanden sein.

Weitere Informationen finden Sie unter ["Erstellen einer Cluster-Peer-Beziehung"](#).

Über diese Aufgabe

In ONTAP 9.2 und älteren Versionen können Sie jeweils nur für eine SVM eine Peer-Beziehung autorisieren. Dies bedeutet, dass Sie das ausführen müssen `vserver peer accept`. Führen Sie jedes Mal einen Befehl aus, wenn Sie eine ausstehende SVM-Peer-Beziehung autorisieren.

Ab ONTAP 9.3 können Sie Peer-Beziehungen für mehrere SVMs vorab autorisieren. Dazu müssen Sie die SVMs in der Liste auflisten `-initial-allowed-vserver` Option, wenn Sie eine Cluster-Peer-Beziehung erstellen. Weitere Informationen finden Sie unter ["Erstellen einer Cluster-Peer-Beziehung"](#).

Schritte

1. Zeigen Sie im Zielcluster zur Datensicherung die SVMs an, die für Peering vorab autorisiert sind:

```
vserver peer permission show
```

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

2. Erstellen Sie im Quell-Cluster für die Datensicherung eine Peer-Beziehung zu einer vorab autorisierten SVM auf dem Ziel-Cluster für die Datensicherung:

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

Eine vollständige Befehlssyntax finden Sie in der man-Page.

Im folgenden Beispiel wird eine Peer-Beziehung zwischen der lokalen SVM erstellt `pvs1` Und der vorab autorisierten Remote-SVM `vs1`:

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

3. Überprüfung der SVM-Peer-Beziehung:

```
vserver peer show
```

```
cluster01::> vserver peer show
```

	Peer	Peer		Peering
Remote	Vserver	State	Peer Cluster	Applications
Vserver				
-----	-----	-----	-----	-----

pvs1	vs1	peered	cluster02	snapmirror
vs1				

Fügen Sie eine Cluster-übergreifende SVM-Peer-Beziehung hinzu

Wenn Sie nach der Konfiguration einer Cluster-Peer-Beziehung eine SVM erstellen, müssen Sie manuell eine Peer-Beziehung für die SVM hinzufügen. Sie können das verwenden `vserver peer create` Befehl zum Erstellen einer Peer-Beziehung zwischen SVMs. Nachdem die Peer-Beziehung erstellt wurde, können Sie ausführen `vserver peer accept` Auf dem Remote-Cluster, um die Peer-Beziehung zu autorisieren.

Bevor Sie beginnen

Die Quell- und Ziel-Cluster müssen Peering durchgeführt werden.

Über diese Aufgabe

Sie können eine Peer-Beziehungen zwischen SVMs im selben Cluster für das lokale Daten-Backup erstellen. Weitere Informationen finden Sie im `vserver peer create` Man-Page.

Administratoren verwenden gelegentlich das `vserver peer reject` Befehl zum Ablehnen einer vorgeschlagenen SVM-Peer-Beziehung. Wenn die Beziehung zwischen SVMs sich in der befindet `rejected` Status: Sie müssen die Beziehung löschen, bevor Sie eine neue erstellen können. Weitere Informationen finden Sie im `vserver peer delete` Man-Page.

Schritte

1. Erstellen Sie für das Quell-Cluster für die Datensicherung eine Peer-Beziehung mit einer SVM auf dem Ziel-Cluster:

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

Im folgenden Beispiel wird eine Peer-Beziehung zwischen der lokalen SVM erstellt `pvs1` Und die Remote-SVM `vs1`

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

Wenn die lokalen und Remote-SVMs dieselben Namen haben, müssen Sie zum Erstellen der SVM-Peer-Beziehung einen „*local Name*“ verwenden:

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

2. Vergewissern Sie sich beim Quell-Cluster für die Datensicherung, dass die Peer-Beziehung initiiert wurde:

```
vserver peer show-all
```

Eine vollständige Befehlssyntax finden Sie in der man-Page.

Das folgende Beispiel zeigt die Peer-Beziehung zwischen SVM_{pvs1} Und SVM_{vs1} Wurde initiiert:

```
cluster01::> vserver peer show-all
```

Vserver	Peer Vserver	Peer State	Peer Cluster	Peering Applications
-----	-----	-----	-----	-----
pvs1	vs1	initiated	Cluster02	snapmirror

3. Zeigen Sie auf dem Ziel-Cluster für die Datensicherung die ausstehende SVM-Peer-Beziehung an:

```
vserver peer show
```

Eine vollständige Befehlssyntax finden Sie in der man-Page.

Im folgenden Beispiel werden die ausstehenden Peer-Beziehungen für aufgeführt cluster02:

```
cluster02::> vserver peer show
```

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

4. Autorisieren Sie auf dem Ziel-Cluster zur Datensicherung die ausstehende Peer-Beziehung:

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

Eine vollständige Befehlssyntax finden Sie in der man-Page.

Das folgende Beispiel autorisiert die Peer-Beziehung zwischen der lokalen SVM _{vs1} Und die Remote-SVM _{pvs1}:

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

5. Überprüfung der SVM-Peer-Beziehung:

```
vserver peer show
```

```
cluster01::> vserver peer show
```

Remote Vserver	Peer Vserver	Peer State	Peer Cluster	Peering Applications
-----	-----	-----	-----	-----
pvs1 vs1	vs1	peered	cluster02	snapmirror

Cluster-Peering-Verschlüsselung für vorhandene Peer-Beziehungen aktivieren

Ab ONTAP 9.6 ist die Cluster-Peering-Verschlüsselung bei allen neu erstellten Cluster-Peering-Beziehungen standardmäßig aktiviert. Die Cluster-Peering-Verschlüsselung verwendet einen vorab gemeinsam genutzten Schlüssel (PSK) und die Transport Security Layer (TLS) zum sicheren clusterübergreifenden Peering von Kommunikation. Dadurch wird eine zusätzliche Sicherheitsschicht zwischen den Peering Clustern hinzugefügt.

Über diese Aufgabe

Wenn Sie Peering-Cluster auf ONTAP 9.6 oder höher aktualisieren und die Peering-Beziehung in ONTAP 9.5 oder früher erstellt wurde, muss die Cluster-Peering-Verschlüsselung nach dem Upgrade manuell aktiviert werden. Beide Cluster in der Peering-Beziehung müssen ONTAP 9.6 oder höher ausführen, um die Verschlüsselung von Cluster-Peering zu aktivieren.

Schritte

1. Aktivieren Sie auf dem Ziel-Cluster die Verschlüsselung für die Kommunikation mit dem Quell-Cluster:

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

2. Geben Sie bei Aufforderung eine Passphrase ein.
3. Aktivieren Sie auf dem Quell-Cluster für Datensicherung die Verschlüsselung zur Kommunikation mit dem Ziel-Cluster:

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

4. Geben Sie bei der entsprechenden Aufforderung dieselbe Passphrase ein, die im Ziel-Cluster eingegeben wurde.

Entfernen Sie die Cluster-Peering-Verschlüsselung von einer vorhandenen Peer-Beziehung

Die Cluster-Peering-Verschlüsselung wird standardmäßig für alle in ONTAP 9.6 oder höher erstellten Peer-Beziehungen aktiviert. Wenn Sie keine Verschlüsselung für Cluster-übergreifende Peering-Kommunikation verwenden möchten, können Sie diese deaktivieren.

Schritte

1. Ändern Sie auf dem Ziel-Cluster die Kommunikation mit dem Quell-Cluster, um die Verwendung von Cluster-Peering-Verschlüsselung einzustellen:

- Geben Sie Folgendes ein, um die Verschlüsselung zu entfernen, aber die Authentifizierung beizubehalten:

```
cluster peer modify _source_cluster_ -auth-status-admin use-  
authentication -encryption-protocol-proposed none
```

- Um Verschlüsselung und Authentifizierung zu entfernen, geben Sie Folgendes ein:

```
cluster peer modify _source_cluster_ -auth-status no-authentication
```

2. Geben Sie bei Aufforderung eine Passphrase ein.

3. Deaktivieren Sie auf dem Quellcluster die Verschlüsselung für die Kommunikation mit dem Ziel-Cluster:

- Geben Sie Folgendes ein, um die Verschlüsselung zu entfernen, aber die Authentifizierung beizubehalten:

```
cluster peer modify _destination_cluster_ -auth-status-admin use-  
authentication -encryption-protocol-proposed none
```

- Um Verschlüsselung und Authentifizierung zu entfernen, geben Sie Folgendes ein:

```
cluster peer modify _destination_cluster_ -auth-status no-  
authentication
```

4. Geben Sie bei der entsprechenden Aufforderung dieselbe Passphrase ein, die im Ziel-Cluster eingegeben wurde.

Copyright-Informationen

Copyright © 2024 NetApp. Alle Rechte vorbehalten. Gedruckt in den USA. Dieses urheberrechtlich geschützte Dokument darf ohne die vorherige schriftliche Genehmigung des Urheberrechtsinhabers in keiner Form und durch keine Mittel – weder grafische noch elektronische oder mechanische, einschließlich Fotokopieren, Aufnehmen oder Speichern in einem elektronischen Abrufsystem – auch nicht in Teilen, vervielfältigt werden.

Software, die von urheberrechtlich geschütztem NetApp Material abgeleitet wird, unterliegt der folgenden Lizenz und dem folgenden Haftungsausschluss:

DIE VORLIEGENDE SOFTWARE WIRD IN DER VORLIEGENDEN FORM VON NETAPP ZUR VERFÜGUNG GESTELLT, D. H. OHNE JEGLICHE EXPLIZITE ODER IMPLIZITE GEWÄHRLEISTUNG, EINSCHLIESSLICH, JEDOCH NICHT BESCHRÄNKT AUF DIE STILLSCHWEIGENDE GEWÄHRLEISTUNG DER MARKTGÄNGIGKEIT UND EIGNUNG FÜR EINEN BESTIMMTEN ZWECK, DIE HIERMIT AUSGESCHLOSSEN WERDEN. NETAPP ÜBERNIMMT KEINERLEI HAFTUNG FÜR DIREKTE, INDIREKTE, ZUFÄLLIGE, BESONDERE, BEISPIELHAFTE SCHÄDEN ODER FOLGESCHÄDEN (EINSCHLIESSLICH, JEDOCH NICHT BESCHRÄNKT AUF DIE BESCHAFFUNG VON ERSATZWAREN ODER -DIENSTLEISTUNGEN, NUTZUNGS-, DATEN- ODER GEWINNVERLUSTE ODER UNTERBRECHUNG DES GESCHÄFTSBETRIEBS), UNABHÄNGIG DAVON, WIE SIE VERURSACHT WURDEN UND AUF WELCHER HAFTUNGSTHEORIE SIE BERUHEN, OB AUS VERTRAGLICH FESTGELEGTER HAFTUNG, VERSCHULDENSUNABHÄNGIGER HAFTUNG ODER DELIKTSHAFTUNG (EINSCHLIESSLICH FAHRLÄSSIGKEIT ODER AUF ANDEREM WEGE), DIE IN IRGEND EINER WEISE AUS DER NUTZUNG DIESER SOFTWARE RESULTIEREN, SELBST WENN AUF DIE MÖGLICHKEIT DERARTIGER SCHÄDEN HINGEWIESEN WURDE.

NetApp behält sich das Recht vor, die hierin beschriebenen Produkte jederzeit und ohne Vorankündigung zu ändern. NetApp übernimmt keine Verantwortung oder Haftung, die sich aus der Verwendung der hier beschriebenen Produkte ergibt, es sei denn, NetApp hat dem ausdrücklich in schriftlicher Form zugestimmt. Die Verwendung oder der Erwerb dieses Produkts stellt keine Lizenzierung im Rahmen eines Patentrechts, Markenrechts oder eines anderen Rechts an geistigem Eigentum von NetApp dar.

Das in diesem Dokument beschriebene Produkt kann durch ein oder mehrere US-amerikanische Patente, ausländische Patente oder anhängige Patentanmeldungen geschützt sein.

ERLÄUTERUNG ZU „RESTRICTED RIGHTS“: Nutzung, Vervielfältigung oder Offenlegung durch die US-Regierung unterliegt den Einschränkungen gemäß Unterabschnitt (b)(3) der Klausel „Rights in Technical Data – Noncommercial Items“ in DFARS 252.227-7013 (Februar 2014) und FAR 52.227-19 (Dezember 2007).

Die hierin enthaltenen Daten beziehen sich auf ein kommerzielles Produkt und/oder einen kommerziellen Service (wie in FAR 2.101 definiert) und sind Eigentum von NetApp, Inc. Alle technischen Daten und die Computersoftware von NetApp, die unter diesem Vertrag bereitgestellt werden, sind gewerblicher Natur und wurden ausschließlich unter Verwendung privater Mittel entwickelt. Die US-Regierung besitzt eine nicht ausschließliche, nicht übertragbare, nicht unterlizenzierbare, weltweite, limitierte unwiderrufliche Lizenz zur Nutzung der Daten nur in Verbindung mit und zur Unterstützung des Vertrags der US-Regierung, unter dem die Daten bereitgestellt wurden. Sofern in den vorliegenden Bedingungen nicht anders angegeben, dürfen die Daten ohne vorherige schriftliche Genehmigung von NetApp, Inc. nicht verwendet, offengelegt, vervielfältigt, geändert, aufgeführt oder angezeigt werden. Die Lizenzrechte der US-Regierung für das US-Verteidigungsministerium sind auf die in DFARS-Klausel 252.227-7015(b) (Februar 2014) genannten Rechte beschränkt.

Markeninformationen

NETAPP, das NETAPP Logo und die unter <http://www.netapp.com/TM> aufgeführten Marken sind Marken von NetApp, Inc. Andere Firmen und Produktnamen können Marken der jeweiligen Eigentümer sein.