



Peering de cluster e SVM

ONTAP 9

NetApp
January 17, 2025

Índice

- Peering de cluster e SVM 1
 - Visão geral do peering de cluster e SVM 1
 - Preparar-se para peering de cluster e SVM 1
 - Configurar LIFs entre clusters 5
 - Configurar relações entre pares 18
 - Habilitar a criptografia de peering de cluster em um relacionamento de pares existente 27
 - Remova a criptografia de peering de cluster de um relacionamento de pares existente 27

Peering de cluster e SVM

Visão geral do peering de cluster e SVM

Você pode criar relacionamentos entre clusters de origem e destino e entre máquinas virtuais de armazenamento de origem e destino (SVMs). Você precisa criar relacionamentos entre pares entre essas entidades antes de poder replicar cópias Snapshot usando o SnapMirror.

O ONTAP 9.3 oferece aprimoramentos que simplificam a maneira como você configura relacionamentos entre clusters e SVMs. Os procedimentos de peering de cluster e SVMs estão disponíveis para todas as versões do ONTAP 9. Você deve usar o procedimento apropriado para sua versão do ONTAP.

Você executa os procedimentos usando a interface de linha de comando (CLI), não o System Manager ou uma ferramenta de script automatizado.

Preparar-se para peering de cluster e SVM

Noções básicas de peering

Você deve criar relacionamentos *peer* entre clusters de origem e destino e entre SVMs de origem e destino antes de poder replicar cópias Snapshot usando o SnapMirror. Um relacionamento de pares define conexões de rede que permitem que clusters e SVMs troquem dados com segurança.

Clusters e SVMs em relações entre pares se comunicam pela rede entre clusters usando *interfaces lógicas* (LIFs). um LIF entre clusters é um LIF que suporta o serviço de interface de rede "entre clusters-core" e é normalmente criado usando a política de serviço de interface de rede "default-clusters". É necessário criar LIFs entre clusters em cada nó nos clusters que estão sendo perados.

Os LIFs usam rotas que pertencem ao SVM do sistema ao qual são atribuídos. O ONTAP cria automaticamente um sistema SVM para comunicações em nível de cluster em um espaço de IPspace.

Topologias de fan-out e cascata são suportadas. Em uma topologia em cascata, você só precisa criar redes entre clusters primários e secundários e entre clusters secundários e secundários. Não é necessário criar uma rede entre clusters primário e terciário.



É possível (mas não aconselhável) que um administrador remova o serviço entre clusters da política de serviços padrão entre clusters. Se isso ocorrer, LIFs criadas usando "default-clusters" não serão, na verdade, LIFs entre clusters. Para confirmar que a política de serviço padrão contém o serviço entre clusters-core, use o seguinte comando:

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

Pré-requisitos para peering de cluster

Antes de configurar o peering de cluster, você deve confirmar se os requisitos de conectividade, porta, endereço IP, sub-rede, firewall e nomenclatura de cluster são atendidos.

A partir do ONTAP 9.6, o peering de cluster fornece suporte de criptografia TLS 1,2 AES-256 GCM para replicação de dados por padrão. As cifras de segurança padrão ("PSK-AES256-GCM-SHA384") são necessárias para que o peering de cluster funcione mesmo que a criptografia esteja desativada.



Começando com ONTAP 9.11,1, as cifras de segurança DHE-PSK estão disponíveis por padrão.

A partir do ONTAP 9.15,1, o peering de cluster fornece suporte de criptografia TLS 1,3 para replicação de dados por padrão.

Requisitos de conectividade

Cada LIF no cluster local deve ser capaz de se comunicar com cada LIF entre clusters no cluster remoto.

Embora não seja necessário, geralmente é mais simples configurar os endereços IP usados para LIFs entre clusters na mesma sub-rede. Os endereços IP podem residir na mesma sub-rede que os LIFs de dados ou em uma sub-rede diferente. A sub-rede usada em cada cluster deve atender aos seguintes requisitos:

- A sub-rede deve pertencer ao domínio de broadcast que contém as portas usadas para comunicação entre clusters.
- A sub-rede deve ter endereços IP suficientes disponíveis para alocar a um LIF entre clusters por nó.

Por exemplo, em um cluster de quatro nós, a sub-rede usada para comunicação entre clusters deve ter quatro endereços IP disponíveis.

Cada nó deve ter um LIF entre clusters com um endereço IP na rede entre clusters.

LIFs podem ter um endereço IPv4 ou um endereço IPv6 entre clusters.



O ONTAP permite que você migre suas redes de peering de IPv4 para IPv6, permitindo opcionalmente que ambos os protocolos estejam presentes simultaneamente nas LIFs entre clusters. Em versões anteriores, todas as relações entre clusters para um cluster inteiro eram IPv4 ou IPv6. Isso significava que a mudança de protocolos era um evento potencialmente disruptivo.

Requisitos portuários

Você pode usar portas dedicadas para comunicação entre clusters ou compartilhar portas usadas pela rede de dados. As portas devem atender aos seguintes requisitos:

- Todas as portas usadas para se comunicar com um determinado cluster remoto devem estar no mesmo espaço IPspace.

Você pode usar vários IPspaces para fazer pares com vários clusters. A conectividade de malha completa em pares é necessária apenas dentro de um espaço IPspace.

- O domínio de broadcast usado para comunicação entre clusters deve incluir pelo menos duas portas por nó para que a comunicação entre clusters possa fazer failover de uma porta para outra porta.

As portas adicionadas a um domínio de broadcast podem ser portas de rede físicas, VLANs ou grupos de interface (ifgrps).

- Todas as portas devem ser cabeadas.
- Todas as portas devem estar em um estado saudável.
- As configurações de MTU das portas devem ser consistentes.

Requisitos de firewall



A partir do ONTAP 9.10,1, as políticas de firewall são obsoletas e totalmente substituídas por políticas de serviço LIF. Para obter mais informações, "[Configurar políticas de firewall para LIFs](#)" consulte .

Os firewalls e a política de firewall entre clusters devem permitir os seguintes protocolos:

- Tráfego ICMP bidirecional
- Tráfego TCP iniciado bidirecional para os endereços IP de todas as LIFs entre clusters nas portas 11104 e 11105
- HTTPS bidirecional entre os LIFs entre clusters

Embora o HTTPS não seja necessário quando você configura o peering de cluster usando a CLI, o HTTPS é necessário mais tarde se você usar o System Manager para configurar a proteção de dados.

A política de firewall predefinida `intercluster` permite o acesso através do protocolo HTTPS e de todos os endereços IP (0,0.0,0/0). Você pode modificar ou substituir a política, se necessário.

Requisito de cluster

Os clusters precisam atender aos seguintes requisitos:

- Um cluster não pode estar em um relacionamento de pares com mais de 255 clusters.

Use portas compartilhadas ou dedicadas

Você pode usar portas dedicadas para comunicação entre clusters ou compartilhar portas usadas pela rede de dados. Ao decidir se deseja compartilhar portas, você precisa considerar a largura de banda da rede, o intervalo de replicação e a disponibilidade da porta.



Você pode compartilhar portas em um cluster com peered enquanto usa portas dedicadas no outro.

Largura de banda da rede

Se você tiver uma rede de alta velocidade, como 10 GbE, talvez tenha largura de banda local suficiente para executar a replicação usando as mesmas portas de 10 GbE usadas para acesso aos dados.

Mesmo assim, você deve comparar a largura de banda da WAN disponível com a largura de banda da LAN. Se a largura de banda da WAN disponível for significativamente menor que 10 GbE, talvez seja necessário usar portas dedicadas.



A única exceção a essa regra pode ser quando todos ou muitos nós no cluster replicarem dados, caso em que a utilização da largura de banda é normalmente espalhada pelos nós.

Se você não estiver usando portas dedicadas, o tamanho máximo da unidade de transmissão (MTU) da rede de replicação geralmente deve ser o mesmo que o tamanho da MTU da rede de dados.

Intervalo de replicação

Se a replicação ocorrer em horas fora do pico, você poderá usar portas de dados para replicação mesmo sem uma conexão LAN de 10 GbE.

Se a replicação ocorrer durante o horário comercial normal, você precisa considerar a quantidade de dados que serão replicados e se ela precisará de tanta largura de banda que poderia causar contenção com protocolos de dados. Se a utilização da rede por protocolos de dados (SMB, NFS, iSCSI) for superior a 50%, deverá utilizar portas dedicadas para comunicação entre clusters, para permitir uma performance não degradada se ocorrer failover de nó.

Disponibilidade da porta

Se você determinar que o tráfego de replicação está interferindo no tráfego de dados, poderá migrar LIFs para qualquer outra porta compartilhada com capacidade para clusters no mesmo nó.

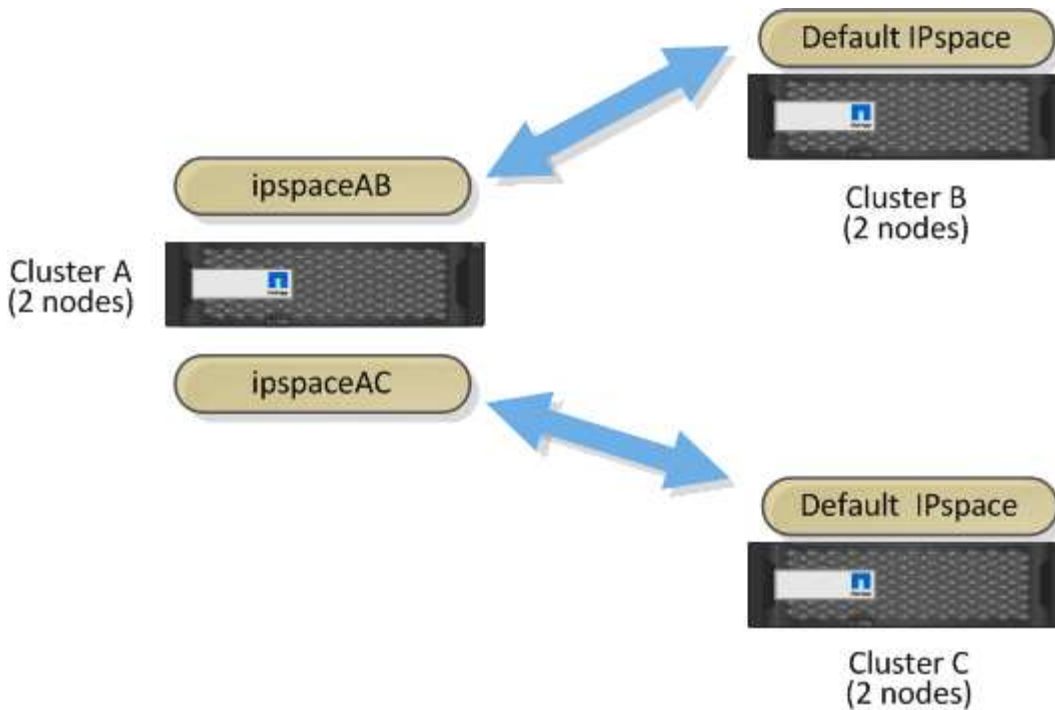
Você também pode dedicar portas VLAN para replicação. A largura de banda da porta é compartilhada entre todas as VLANs e a porta base.

Use IPspaces personalizados para isolar o tráfego de replicação

Você pode usar IPspaces personalizados para separar as interações que um cluster tem com seus pares. Chamada de *conetividade entre clusters designada*, essa configuração permite que os provedores de serviços isolem o tráfego de replicação em ambientes multitenant.

Suponha, por exemplo, que você deseja que o tráfego de replicação entre o Cluster A e o Cluster B seja separado do tráfego de replicação entre o Cluster A e o Cluster C. para conseguir isso, você pode criar dois espaços IPspaces no Cluster A.

Um IPspace contém as LIFs entre clusters que você usa para se comunicar com o Cluster B. o outro contém as LIFs entre clusters que você usa para se comunicar com o Cluster C, como mostrado na ilustração a seguir.



Para a configuração de IPspace personalizada, consulte o *Network Management Guide*.

Configurar LIFs entre clusters

Configurar LIFs entre clusters em portas de dados compartilhados

Você pode configurar LIFs entre clusters em portas compartilhadas com a rede de dados. Isso reduz o número de portas de que você precisa para redes entre clusters.

Passos

1. Liste as portas no cluster:

```
network port show
```

Para obter a sintaxe completa do comando, consulte a página `man`.

O exemplo a seguir mostra as portas de rede no `cluster01`:

```

cluster01::> network port show

(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. Crie LIFs entre clusters em um administrador SVM (IPspace padrão) ou em um sistema SVM (IPspace personalizado):

Opção	Descrição
Em ONTAP 9.6 e posteriores:	<code>network interface create -vserver <i>system_SVM</i> -lif <i>LIF_name</i> -service -policy default-intercluster -home -node <i>node</i> -home-port <i>port</i> -address <i>port_IP</i> -netmask <i>netmask</i></code>
Em ONTAP 9.5 e anteriores:	<code>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></code>

Para obter a sintaxe completa do comando, consulte a página `man`.

O exemplo a seguir cria LIFs entre clusters `cluster01_icl01` e `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. Verifique se as LIFs entre clusters foram criadas:

Opção	Descrição
Em ONTAP 9.6 e posteriores:	<code>network interface show -service-policy default-intercluster</code>
Em ONTAP 9.5 e anteriores:	<code>network interface show -role intercluster</code>

Para obter a sintaxe completa do comando, consulte a página `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. Verifique se as LIFs entre clusters são redundantes:

Opção	Descrição
Em ONTAP 9.6 e posteriores:	<code>network interface show -service-policy default-intercluster -failover</code>
Em ONTAP 9.5 e anteriores:	<code>network interface show -role intercluster -failover</code>

Para obter a sintaxe completa do comando, consulte a página `man`.

O exemplo a seguir mostra que os LIFs entre clusters `cluster01_icl01` e `cluster01_icl02` na `e0c` porta irão falhar para a `e0d` porta.

```
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
```

Configurar LIFs entre clusters em portas dedicadas

Você pode configurar LIFs entre clusters em portas dedicadas. Isso normalmente aumenta a largura de banda disponível para o tráfego de replicação.

Passos

1. Liste as portas no cluster:

```
network port show
```

Para obter a sintaxe completa do comando, consulte a página `man`.

O exemplo a seguir mostra as portas de rede no `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. Determine quais portas estão disponíveis para se dedicar à comunicação entre clusters:

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

Para obter a sintaxe completa do comando, consulte a página man.

O exemplo a seguir mostra que portas e0e e e0f não foram atribuídas 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. Crie um grupo de failover para as portas dedicadas:

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

O exemplo a seguir atribui portas e0e e e0f ao grupo de failover intercluster01 no SVM do sistema 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. Verifique se o grupo de failover foi criado:

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

Para obter a sintaxe completa do comando, consulte a página man.

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

5. Crie LIFs entre clusters no sistema e atribua-os ao grupo de failover.

Opção	Descrição
Em ONTAP 9.6 e posteriores:	<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 -failover -group failover_group</code>

Opção	Descrição
Em ONTAP 9.5 e anteriores:	<code>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></code>

Para obter a sintaxe completa do comando, consulte a página `man`.

O exemplo a seguir cria LIFs entre clusters `cluster01_icl01` e `cluster01_icl02` no grupo failover `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. Verifique se as LIFs entre clusters foram criadas:

Opção	Descrição
Em ONTAP 9.6 e posteriores:	<code>network interface show -service-policy default-intercluster</code>
Em ONTAP 9.5 e anteriores:	<code>network interface show -role intercluster</code>

Para obter a sintaxe completa do comando, consulte a página `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. Verifique se as LIFs entre clusters são redundantes:

Opção	Descrição
Em ONTAP 9.6 e posteriores:	<code>network interface show -service-policy default-intercluster -failover</code>
Em ONTAP 9.5 e anteriores:	<code>network interface show -role intercluster -failover</code>

Para obter a sintaxe completa do comando, consulte a página `man`.

O exemplo a seguir mostra que os LIFs entre clusters `cluster01_icl01` e `cluster01_icl02` a porta SVM `e0e` farão failover para a `e0f` porta.

```

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

```

Configurar LIFs entre clusters em IPspaces personalizados

Você pode configurar LIFs entre clusters em IPspaces personalizados. Isso permite isolar o tráfego de replicação em ambientes multitenant.

Quando você cria um IPspace personalizado, o sistema cria uma máquina virtual de storage do sistema (SVM) para servir como um contêiner para os objetos do sistema nesse IPspace. Você pode usar o novo SVM como contêiner para quaisquer LIFs entre clusters no novo IPspace. O novo SVM tem o mesmo nome que o IPspace personalizado.

Passos

1. Liste as portas no cluster:

```
network port show
```

Para obter a sintaxe completa do comando, consulte a página `man`.

O exemplo a seguir mostra as portas de rede no `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. Crie IPspaces personalizados no cluster:

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

O exemplo a seguir cria o IPspace personalizado `ipspace-IC1` :

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

3. Determine quais portas estão disponíveis para se dedicar à comunicação entre clusters:

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

Para obter a sintaxe completa do comando, consulte a página man.

O exemplo a seguir mostra que portas e0e e e0f não foram atribuídas 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. Remova as portas disponíveis do domínio de broadcast padrão:

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

Uma porta não pode estar em mais de um domínio de broadcast de cada vez. Para obter a sintaxe completa do comando, consulte a página man.

O exemplo a seguir remove portas e0e e e0f do domínio de broadcast padrão:

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

5. Verifique se as portas foram removidas do domínio de broadcast padrão:

```
network port show
```

Para obter a sintaxe completa do comando, consulte a página man.

O exemplo a seguir mostra que as portas e0e e e0f foram removidas do domínio de broadcast padrão:


```
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. Crie um domínio de broadcast no IPspace personalizado:

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

O exemplo a seguir cria o domínio de broadcast `ipspace-IC1-bd` no 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. Verifique se o domínio de broadcast foi criado:

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

Para obter a sintaxe completa do comando, consulte a página `man`.

```

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

```

8. Crie LIFs entre clusters no sistema SVM e atribua-os ao domínio de broadcast:

Opção	Descrição
Em ONTAP 9.6 e posteriores:	<code>network interface create -vserver <i>system_SVM</i> -lif <i>LIF_name</i> -service -policy default-intercluster -home -node <i>node</i> -home-port <i>port</i> -address <i>port_IP</i> -netmask <i>netmask</i></code>
Em ONTAP 9.5 e anteriores:	<code>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></code>

O LIF é criado no domínio de broadcast ao qual a porta inicial é atribuída. O domínio de broadcast tem um grupo de failover padrão com o mesmo nome do domínio de broadcast. Para obter a sintaxe completa do comando, consulte a página man.

O exemplo a seguir cria LIFs entre clusters `cluster01_icl01` e `cluster01_icl02` no domínio 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. Verifique se as LIFs entre clusters foram criadas:

Opção	Descrição
Em ONTAP 9.6 e posteriores:	<code>network interface show -service-policy default-intercluster</code>
Em ONTAP 9.5 e anteriores:	<code>network interface show -role intercluster</code>

Para obter a sintaxe completa do comando, consulte a página `man`.

```
cluster01::> network interface show -service-policy default-intercluster
Current Is
Vserver   Logical   Status   Network   Current
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. Verifique se as LIFs entre clusters são redundantes:

Opção	Descrição
Em ONTAP 9.6 e posteriores:	<code>network interface show -service-policy default-intercluster -failover</code>
Em ONTAP 9.5 e anteriores:	<code>network interface show -role intercluster -failover</code>

Para obter a sintaxe completa do comando, consulte a página `man`.

O exemplo a seguir mostra que os LIFs entre clusters `cluster01_icl01` e `cluster01_icl02` a porta SVM `e0e` fazem failover para a porta `e0f`:

```
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
```

Configurar relações entre pares

Crie um relacionamento de pares de cluster

Antes de proteger seus dados replicando-os em um cluster remoto para fins de backup de dados e recuperação de desastres, você deve criar um relacionamento de peers de clusters entre o cluster local e o cluster remoto.

Sobre esta tarefa

Este procedimento aplica-se aos sistemas FAS, AFF e ASA atuais. Se você tiver um sistema ASA R2 (ASA A1K, ASA A70 ou ASA A90), siga ["estes passos"](#) para criar a replicação de snapshot de configuração. Os sistemas ASA R2 fornecem uma experiência de ONTAP simplificada específica para clientes somente SAN.

Várias políticas de proteção padrão estão disponíveis. Você deve ter criado suas políticas de proteção se quiser usar políticas personalizadas.

Antes de começar

- Se você estiver usando a CLI do ONTAP, crie LIFs entre clusters em todos os nós dos clusters que estão

sendo direcionados usando um dos seguintes métodos:

- ["Configurar LIFs entre clusters em portas de dados compartilhados"](#)
- ["Configurar LIFs entre clusters em portas de dados dedicadas"](#)
- ["Configurar LIFs entre clusters em IPspaces personalizados"](#)
- Os clusters precisam estar executando o ONTAP 9.3 ou posterior. (Se os clusters estiverem executando o ONTAP 9.2 ou anterior, consulte os procedimentos em ["este documento arquivado"](#).)



Passos

Execute esta tarefa usando o Gerenciador de sistema do ONTAP ou a CLI do ONTAP.

System Manager

1. No cluster local, clique em **Cluster > Settings**.
2. Na seção **Configurações de cluster**, clique em **Adicionar interfaces de rede** e insira o endereço IP e a máscara de sub-rede para adicionar interfaces de rede entre clusters para o cluster.

Repita este passo no painel remoto.

3. No cluster remoto, clique em **Cluster > Settings**.
4. Clique  na seção **Cluster Peers** e selecione **Generate Passphrase** (gerar frase-passe).
5. Selecione a versão remota do cluster do ONTAP.
6. Copie a frase-passe gerada.
7. No cluster local, em **Cluster Peers**, clique  e selecione **Peer cluster**.
8. Na janela **cluster de pares**, cole a frase-passe e clique em **Iniciar peering de cluster**.

CLI

1. No cluster de destino, crie uma relação de pares com o cluster de origem:

```
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  
<ip>space
```

Se você especificar ambos `-generate-passphrase` e `-peer-addr`s, somente o cluster cujos LIFs entre clusters são especificados em `-peer-addr`s poderá usar a senha gerada.

Você pode ignorar a `-ip>space` opção se não estiver usando um IPspace personalizado. Para obter a sintaxe completa do comando, consulte a página man.

Se você estiver criando o relacionamento de peering no ONTAP 9.6 ou posterior e não quiser que as comunicações de peering entre clusters sejam criptografadas, use a `-encryption-protocol -proposed none` opção para desativar a criptografia.

O exemplo a seguir cria um relacionamento de peer de cluster com um cluster remoto não especificado e pré-autoriza relacionamentos entre pares com SVMs e `vs1 vs2` no 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.
```

O exemplo a seguir cria um relacionamento de peer de cluster com o cluster remoto nos endereços IP de LIF 192.140.112.103 e 192.140.112.104 e pré-autoriza um relacionamento de pares com qualquer SVM no cluster local:

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

O exemplo a seguir cria um relacionamento de peer de cluster com um cluster remoto não especificado e pré-autoriza relacionamentos entre pares com SVMs evs1 vs2 no 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. No cluster de origem, autentique o cluster de origem no cluster de destino:

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

Para obter a sintaxe completa do comando, consulte a página man.

O exemplo a seguir autentica o cluster local para o cluster remoto nos endereços IP 192.140.112.101 e 192.140.112.102 do LIF:

```
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.

Digite a senha para o relacionamento de pares quando solicitado.

3. Verifique se o relacionamento de pares de cluster foi criado:

```
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. Verifique a conectividade e o status dos nós no relacionamento de pares:

```
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
```

Outras maneiras de fazer isso em ONTAP

Para executar estas tarefas com...	Veja este conteúdo...
System Manager Classic (disponível com o ONTAP 9.7 e versões anteriores)	"Visão geral da preparação para recuperação de desastres em volume"

Criar um relacionamento entre pares SVM entre clusters

Você pode usar o `vserver peer create` comando para criar um relacionamento entre SVMs em clusters locais e remotos.

Antes de começar

- Os clusters de origem e destino devem ser percorridos.

- Os clusters devem estar executando o ONTAP 9.3. (Se os clusters estiverem executando o ONTAP 9.2 ou anterior, consulte os procedimentos em ["este documento arquivado"](#).)
- Você deve ter relações de pares "pré-autorizadas" para os SVMs no cluster remoto.

Para obter mais informações, ["Criando um relacionamento de cluster peer"](#) consulte .

Sobre esta tarefa

No ONTAP 9.2 e anteriores, você pode autorizar um relacionamento de pares para apenas um SVM de cada vez. Isso significa que você precisa executar o `vserver peer accept` comando cada vez que você autorizar um relacionamento de pares SVM pendente.

A partir do ONTAP 9.3, você pode "pré-autorizar" relacionamentos de pares para vários SVMs, listando os SVMs na `-initial-allowed-vserver` opção quando você cria um relacionamento de peer de cluster. Para obter mais informações, ["Criando um relacionamento de cluster peer"](#) consulte .

Passos

1. No cluster de destino de proteção de dados, exiba os SVMs que são pré-autorizados para peering:

```
vserver peer permission show
```

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

2. No cluster de origem de proteção de dados, crie um relacionamento de mesmo nível com um SVM pré-autorizado no cluster de destino de proteção de dados:

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

Para obter a sintaxe completa do comando, consulte a página `man`.

O exemplo a seguir cria um relacionamento entre o SVM local `pvs1` e o SVM remoto pré-autorizado `vs1` :

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

3. Verifique o relacionamento entre pares SVM:

```
vserver peer show
```

```

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

```

Adicione um relacionamento entre pares SVM entre clusters

Se você criar um SVM depois de configurar um relacionamento de pares de cluster, precisará adicionar um relacionamento de mesmo nível para o SVM manualmente. Você pode usar o `vserver peer create` comando para criar um relacionamento entre pares entre SVMs. Após a criação do relacionamento de pares, você pode executar `vserver peer accept` no cluster remoto para autorizar o relacionamento de pares.

Antes de começar

Os clusters de origem e destino devem ser percorridos.

Sobre esta tarefa

Você pode criar relacionamentos entre pares entre SVMs no mesmo cluster para backup de dados locais. Para obter mais informações, consulte a `vserver peer create` página de manual.

Os administradores ocasionalmente usam o `vserver peer reject` comando para rejeitar uma proposta de relacionamento com colegas SVM. Se a relação entre SVMs estiver no `rejected` estado, você deverá excluir a relação antes de criar uma nova. Para obter mais informações, consulte a `vserver peer delete` página de manual.

Passos

1. No cluster de origem de proteção de dados, crie um relacionamento de mesmo nível com um SVM no cluster de destino de proteção de dados:

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

O exemplo a seguir cria um relacionamento entre o SVM local `pvs1` e o SVM remoto `vs1`

```

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

```

Se os SVMs locais e remotos tiverem os mesmos nomes, você deverá usar um *local name* para criar o relacionamento de pares SVM:

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

2. No cluster de origem de proteção de dados, verifique se o relacionamento de pares foi iniciado:

```
vserver peer show-all
```

Para obter a sintaxe completa do comando, consulte a página man.

O exemplo a seguir mostra que a relação entre SVM_{pvs1} e SVM_{vs1} foi iniciada:

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

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

3. No cluster de destino da proteção de dados, exiba a relação de pares SVM pendente:

```
vserver peer show
```

Para obter a sintaxe completa do comando, consulte a página man.

O exemplo a seguir lista as relações de pares pendentes para cluster02:

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

Vserver	Peer Vserver	Peer State
vs1	pvs1	pending

4. No cluster de destino de proteção de dados, autorize o relacionamento de pares pendente:

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

Para obter a sintaxe completa do comando, consulte a página man.

O exemplo a seguir autoriza o relacionamento entre pares entre o SVM local vs1 e o SVM remoto pvs1 :

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

5. Verifique o relacionamento entre pares SVM:

```
vserver peer show
```

```
cluster01::> vserver peer show
Peer Peer Peering
Remote
Vserver Vserver State Peer Cluster Applications
Vserver
-----
-----
pvsl1 vs1 peered cluster02 snapmirror
vs1
```

Habilitar a criptografia de peering de cluster em um relacionamento de pares existente

A partir do ONTAP 9.6, a criptografia de peering de cluster é ativada por padrão em todas as relações de peering de cluster recém-criadas. A criptografia de peering de cluster usa uma chave pré-compartilhada (PSK) e a camada de segurança de transporte (TLS) para proteger as comunicações de peering entre clusters. Isso adiciona uma camada adicional de segurança entre os clusters com peering.

Sobre esta tarefa

Se você estiver atualizando clusters peered para o ONTAP 9.6 ou posterior e a relação de peering tiver sido criada no ONTAP 9.5 ou anterior, a criptografia de peering de cluster deve ser ativada manualmente após a atualização. Ambos os clusters no relacionamento de peering devem estar executando o ONTAP 9.6 ou posterior para habilitar a criptografia de peering de cluster.

Passos

1. No cluster de destino, ative a encriptação para comunicações com o cluster de origem:

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

2. Quando solicitado, introduza uma frase-passe.
3. No cluster de origem da proteção de dados, ative a criptografia para comunicação com o cluster de destino da proteção de dados:

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

4. Quando solicitado, introduza a mesma frase-passe introduzida no cluster de destino.

Remova a criptografia de peering de cluster de um relacionamento de pares existente

Por padrão, a criptografia de peering de cluster é ativada em todos os relacionamentos

de pares criados no ONTAP 9.6 ou posterior. Se você não quiser usar criptografia para comunicações de peering entre clusters, você pode desativá-la.

Passos

1. No cluster de destino, modifique as comunicações com o cluster de origem para interromper o uso da criptografia de peering de cluster:

- Para remover a criptografia, mas manter a autenticação, digite:

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

- Para remover criptografia e autenticação:

i. Modifique a política de peering de cluster para permitir acesso não autenticado:

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

ii. Modificar criptografia e acesso de autenticação:

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

2. Quando solicitado, introduza a frase-passe.

3. Confirme a frase-passe reinserindo-a.

4. No cluster de origem, desative a encriptação para comunicação com o cluster de destino:

- Para remover a criptografia, mas manter a autenticação, digite:

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

- Para remover criptografia e autenticação:

i. Modifique a política de peering de cluster para permitir acesso não autenticado:

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

ii. Modificar criptografia e acesso de autenticação:

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

5. Quando solicitado, introduza e introduza novamente a mesma frase-passe utilizada no cluster de destino.

Informações sobre direitos autorais

Copyright © 2025 NetApp, Inc. Todos os direitos reservados. Impresso nos EUA. Nenhuma parte deste documento protegida por direitos autorais pode ser reproduzida de qualquer forma ou por qualquer meio — gráfico, eletrônico ou mecânico, incluindo fotocópia, gravação, gravação em fita ou storage em um sistema de recuperação eletrônica — sem permissão prévia, por escrito, do proprietário dos direitos autorais.

O software derivado do material da NetApp protegido por direitos autorais está sujeito à seguinte licença e isenção de responsabilidade:

ESTE SOFTWARE É FORNECIDO PELA NETAPP "NO PRESENTE ESTADO" E SEM QUAISQUER GARANTIAS EXPRESSAS OU IMPLÍCITAS, INCLUINDO, SEM LIMITAÇÕES, GARANTIAS IMPLÍCITAS DE COMERCIALIZAÇÃO E ADEQUAÇÃO A UM DETERMINADO PROPÓSITO, CONFORME A ISENÇÃO DE RESPONSABILIDADE DESTES DOCUMENTOS. EM HIPÓTESE ALGUMA A NETAPP SERÁ RESPONSÁVEL POR QUALQUER DANO DIRETO, INDIRETO, INCIDENTAL, ESPECIAL, EXEMPLAR OU CONSEQUENCIAL (INCLUINDO, SEM LIMITAÇÕES, AQUISIÇÃO DE PRODUTOS OU SERVIÇOS SOBRESSALIENTES; PERDA DE USO, DADOS OU LUCROS; OU INTERRUPÇÃO DOS NEGÓCIOS), INDEPENDENTEMENTE DA CAUSA E DO PRINCÍPIO DE RESPONSABILIDADE, SEJA EM CONTRATO, POR RESPONSABILIDADE OBJETIVA OU PREJUÍZO (INCLUINDO NEGLIGÊNCIA OU DE OUTRO MODO), RESULTANTE DO USO DESTES SOFTWARES, MESMO SE ADVERTIDA DA RESPONSABILIDADE DE TAL DANO.

A NetApp reserva-se o direito de alterar quaisquer produtos descritos neste documento, a qualquer momento e sem aviso. A NetApp não assume nenhuma responsabilidade nem obrigação decorrentes do uso dos produtos descritos neste documento, exceto conforme expressamente acordado por escrito pela NetApp. O uso ou a compra deste produto não representam uma licença sob quaisquer direitos de patente, direitos de marca comercial ou quaisquer outros direitos de propriedade intelectual da NetApp.

O produto descrito neste manual pode estar protegido por uma ou mais patentes dos EUA, patentes estrangeiras ou pedidos pendentes.

LEGENDA DE DIREITOS LIMITADOS: o uso, a duplicação ou a divulgação pelo governo estão sujeitos a restrições conforme estabelecido no subparágrafo (b)(3) dos Direitos em Dados Técnicos - Itens Não Comerciais no DFARS 252.227-7013 (fevereiro de 2014) e no FAR 52.227- 19 (dezembro de 2007).

Os dados aqui contidos pertencem a um produto comercial e/ou serviço comercial (conforme definido no FAR 2.101) e são de propriedade da NetApp, Inc. Todos os dados técnicos e software de computador da NetApp fornecidos sob este Contrato são de natureza comercial e desenvolvidos exclusivamente com despesas privadas. O Governo dos EUA tem uma licença mundial limitada, irrevogável, não exclusiva, intransferível e não sublicenciável para usar os Dados que estão relacionados apenas com o suporte e para cumprir os contratos governamentais desse país que determinam o fornecimento de tais Dados. Salvo disposição em contrário no presente documento, não é permitido usar, divulgar, reproduzir, modificar, executar ou exibir os dados sem a aprovação prévia por escrito da NetApp, Inc. Os direitos de licença pertencentes ao governo dos Estados Unidos para o Departamento de Defesa estão limitados aos direitos identificados na cláusula 252.227-7015(b) (fevereiro de 2014) do DFARS.

Informações sobre marcas comerciais

NETAPP, o logotipo NETAPP e as marcas listadas em <http://www.netapp.com/TM> são marcas comerciais da NetApp, Inc. Outros nomes de produtos e empresas podem ser marcas comerciais de seus respectivos proprietários.