



Peering di cluster e SVM

ONTAP 9

NetApp
August 21, 2024

Sommario

- Peering di cluster e SVM 1
 - Panoramica del peering di cluster e SVM 1
 - Preparatevi per il peering di cluster e SVM 1
 - Configurare le LIF tra cluster 5
 - Configurare le relazioni peer 18
 - Abilitare la crittografia del peering del cluster su una relazione peer esistente 27
 - Rimuovere la crittografia di peering del cluster da una relazione peer esistente 27

Peering di cluster e SVM

Panoramica del peering di cluster e SVM

È possibile creare relazioni peer tra cluster di origine e di destinazione e tra macchine virtuali storage di origine e di destinazione (SVM). È necessario creare relazioni peer tra queste entità prima di poter replicare le copie Snapshot utilizzando SnapMirror.

ONTAP 9.3 offre miglioramenti che semplificano il modo in cui si configurano le relazioni peer tra cluster e SVM. Le procedure di peering del cluster e delle SVM sono disponibili per tutte le versioni di ONTAP 9. Utilizzare la procedura appropriata per la versione di ONTAP in uso.

Le procedure vengono eseguite utilizzando l'interfaccia della riga di comando (CLI), non System Manager o uno strumento di scripting automatico.

Preparatevi per il peering di cluster e SVM

Nozioni di base sul peering

È necessario creare *relazioni peer* tra cluster di origine e di destinazione e tra SVM di origine e di destinazione prima di poter replicare le copie Snapshot utilizzando SnapMirror. Una relazione peer definisce le connessioni di rete che consentono a cluster e SVM di scambiare dati in modo sicuro.

I cluster e le SVM nelle relazioni tra pari comunicano sulla rete intercluster utilizzando *LIF (Intercluster Logical Interface)*. Una LIF intercluster è una LIF che supporta il servizio di interfaccia di rete "intercluster-core" e viene generalmente creata utilizzando la policy del servizio di interfaccia di rete "intercluster predefinito". È necessario creare LIF intercluster su ogni nodo dei cluster sottoposti a peering.

Le LIF di intercluster utilizzano i percorsi che appartengono alla SVM di sistema a cui sono assegnate. ONTAP crea automaticamente una SVM di sistema per le comunicazioni a livello di cluster all'interno di un IPspace.

Sono supportate entrambe le topologie fan-out e cascata. In una topologia a cascata, è necessario creare solo reti di intercluster tra i cluster primario e secondario e tra i cluster secondario e terziario. Non è necessario creare una rete di intercluster tra il cluster primario e il cluster terzo.



È possibile (ma non consigliabile) che un amministratore rimuova il servizio intercluster-core dalla policy di servizio intercluster predefinita. In questo caso, i LIF creati utilizzando "intercluster predefinito" non saranno effettivamente LIF intercluster. Per confermare che la policy di servizio dell'intercluster predefinito contiene il servizio intercluster-core, utilizzare il seguente comando:

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

Prerequisiti per il peering del cluster

Prima di configurare il peering del cluster, verificare che la connettività, la porta, l'indirizzo IP, la subnet, il firewall, e i requisiti di naming dei cluster sono soddisfatti.

A partire da ONTAP 9,6, il peering dei cluster fornisce il supporto per la crittografia TLS 1,2 AES-256 GCM per la replica dei dati per impostazione predefinita. I cifrari di sicurezza predefiniti ("PSK-AES256-GCM-SHA384") sono necessari affinché il peering del cluster funzioni anche se la crittografia è disattivata.



A partire da ONTAP 9.11.1, le crittografie di sicurezza DHE-PSK sono disponibili per impostazione predefinita.

A partire da ONTAP 9.15.1, il peering dei cluster offre il supporto per la crittografia TLS 1,3 per la replica dei dati, per impostazione predefinita.

Requisiti di connettività

Ogni LIF di intercluster sul cluster locale deve essere in grado di comunicare con ogni LIF di intercluster sul cluster remoto.

Sebbene non sia necessario, è in genere più semplice configurare gli indirizzi IP utilizzati per le LIF di intercluster nella stessa subnet. Gli indirizzi IP possono risiedere nella stessa sottorete dei file LIF dei dati o in una sottorete diversa. La subnet utilizzata in ciascun cluster deve soddisfare i seguenti requisiti:

- La subnet deve appartenere al dominio di trasmissione che contiene le porte utilizzate per la comunicazione tra cluster.
- La subnet deve disporre di un numero sufficiente di indirizzi IP da allocare a un LIF intercluster per nodo.

Ad esempio, in un cluster a quattro nodi, la subnet utilizzata per la comunicazione tra cluster deve avere quattro indirizzi IP disponibili.

Ciascun nodo deve disporre di una LIF intercluster con un indirizzo IP sulla rete intercluster.

Le LIF di intercluster possono avere un indirizzo IPv4 o IPv6.



ONTAP consente di migrare le reti peering da IPv4 a IPv6, consentendo la presenza simultanea di entrambi i protocolli nelle LIF dell'intercluster. Nelle versioni precedenti, tutte le relazioni tra cluster per un intero cluster erano IPv4 o IPv6. Ciò significava che la modifica dei protocolli era un evento potenzialmente disgregativo.

Requisiti delle porte

È possibile utilizzare porte dedicate per la comunicazione tra cluster o condividere le porte utilizzate dalla rete dati. Le porte devono soddisfare i seguenti requisiti:

- Tutte le porte utilizzate per comunicare con un determinato cluster remoto devono trovarsi nello stesso IPspace.

È possibile utilizzare più IPspaces per eseguire il peer con più cluster. La connettività full-mesh a coppie è necessaria solo all'interno di un IPspace.

- Il dominio di broadcast utilizzato per la comunicazione tra cluster deve includere almeno due porte per nodo in modo che la comunicazione tra cluster possa eseguire il failover da una porta a un'altra.

Le porte aggiunte a un dominio di broadcast possono essere porte di rete fisiche, VLAN o gruppi di interfacce (ifgrps).

- Tutte le porte devono essere cablate.
- Tutte le porte devono essere in buono stato.
- Le impostazioni MTU delle porte devono essere coerenti.

Requisiti del firewall



A partire da ONTAP 9.10.1, le policy firewall sono obsolete e completamente sostituite con le policy di servizio LIF. Per ulteriori informazioni, vedere "[Configurare le policy firewall per le LIF](#)".

I firewall e i criteri di firewall tra cluster devono consentire i seguenti protocolli:

- Traffico ICMP bidirezionale
- Traffico TCP avviato in modo bidirezionale verso gli indirizzi IP di tutti i LIF intercluster sulle porte 11104 e 11105
- HTTPS bidirezionale tra le LIF dell'intercluster

Sebbene HTTPS non sia richiesto quando si imposta il peering del cluster utilizzando la CLI, HTTPS è richiesto in seguito se si utilizza System Manager per configurare la protezione dei dati.

L'impostazione predefinita `intercluster` La policy firewall consente l'accesso tramite il protocollo HTTPS e da tutti gli indirizzi IP (0.0.0.0/0). Se necessario, è possibile modificare o sostituire la policy.

Requisito del cluster

I cluster devono soddisfare i seguenti requisiti:

- Un cluster non può trovarsi in una relazione peer con più di 255 cluster.

Utilizzare porte condivise o dedicate

È possibile utilizzare porte dedicate per la comunicazione tra cluster o condividere le porte utilizzate dalla rete dati. Per decidere se condividere le porte, è necessario considerare la larghezza di banda della rete, l'intervallo di replica e la disponibilità delle porte.



È possibile condividere le porte su un cluster peered utilizzando le porte dedicate sull'altro.

Larghezza di banda della rete

Se si dispone di una rete ad alta velocità, ad esempio 10 GbE, potrebbe essere disponibile una larghezza di banda LAN locale sufficiente per eseguire la replica utilizzando le stesse porte 10 GbE utilizzate per l'accesso ai dati.

Anche in questo caso, è necessario confrontare la larghezza di banda WAN disponibile con la larghezza di banda della LAN. Se la larghezza di banda WAN disponibile è significativamente inferiore a 10 GbE, potrebbe essere necessario utilizzare porte dedicate.



L'unica eccezione a questa regola potrebbe essere rappresentata dal fatto che tutti o molti nodi del cluster replicano i dati, nel qual caso l'utilizzo della larghezza di banda è in genere distribuito tra i nodi.

Se non si utilizzano porte dedicate, le dimensioni massime dell'unità di trasmissione (MTU) della rete di replica dovrebbero essere le stesse della dimensione MTU della rete dati.

Intervallo di replica

Se la replica avviene in ore non di punta, dovresti essere in grado di utilizzare le porte dati per la replica anche senza una connessione LAN a 10 GbE.

Se la replica avviene durante il normale orario di lavoro, è necessario considerare la quantità di dati che verranno replicati e se richiede una larghezza di banda così elevata da causare conflitti con i protocolli dati. Se l'utilizzo della rete da parte dei protocolli di dati (SMB, NFS, iSCSI) è superiore al 50%, è necessario utilizzare porte dedicate per la comunicazione tra cluster, per consentire prestazioni non degradate in caso di failover del nodo.

Disponibilità delle porte

Se si determina che il traffico di replica interferisce con il traffico dati, è possibile migrare le LIF di intercluster su qualsiasi altra porta condivisa compatibile con intercluster sullo stesso nodo.

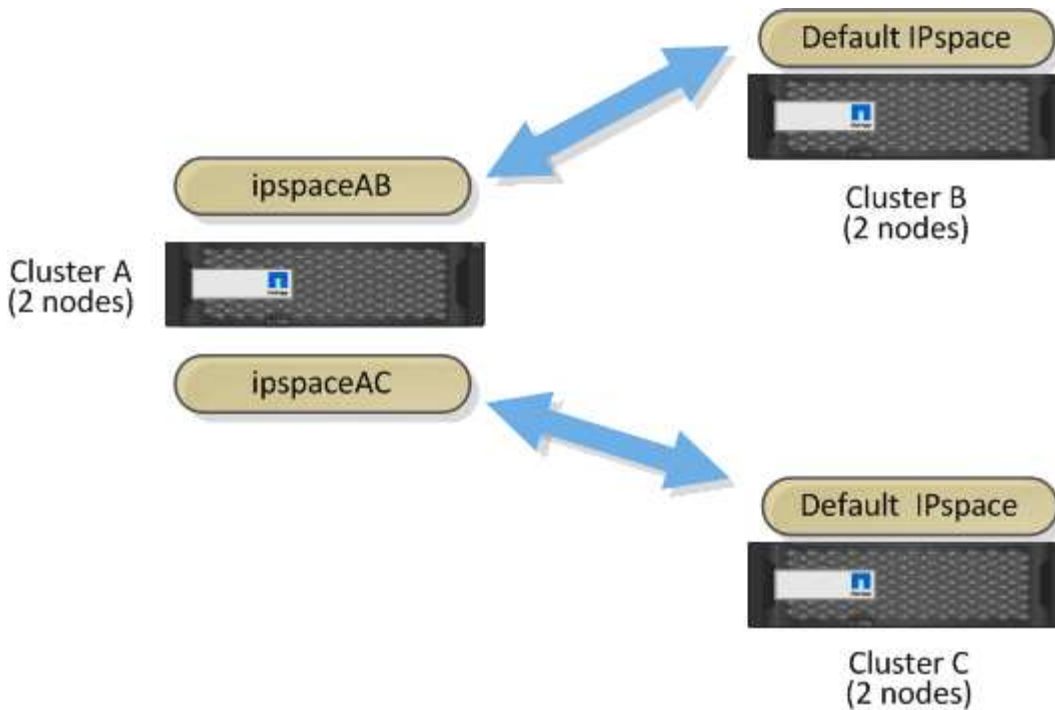
È inoltre possibile dedicare le porte VLAN per la replica. La larghezza di banda della porta è condivisa tra tutte le VLAN e la porta base.

Utilizzare IPspaces personalizzati per isolare il traffico di replica

È possibile utilizzare IPspaces personalizzati per separare le interazioni di un cluster con i peer. Detta *connettività intercluster designata*, questa configurazione consente ai service provider di isolare il traffico di replica in ambienti multi-tenant.

Si supponga, ad esempio, di voler separare il traffico di replica tra il cluster A e il cluster B dal traffico di replica tra il cluster A e il cluster C. A tale scopo, è possibile creare due IPspaces sul cluster A.

Un IPspace contiene le LIF intercluster utilizzate per comunicare con il cluster B. L'altro contiene le LIF di intercluster utilizzate per comunicare con il cluster C, come mostrato nell'illustrazione seguente.



Per una configurazione IPspace personalizzata, consultare la *Guida alla gestione di rete*.

Configurare le LIF tra cluster

Configurare le LIF tra cluster su porte dati condivise

È possibile configurare le LIF di intercluster sulle porte condivise con la rete dati. In questo modo si riduce il numero di porte necessarie per la rete tra cluster.

Fasi

1. Elencare le porte nel cluster:

```
network port show
```

Per la sintassi completa dei comandi, vedere la pagina man.

L'esempio seguente mostra le porte di rete in `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. Creazione di LIF intercluster da una SVM di amministrazione (IPSpace predefinito) o da una SVM di sistema (IPSpace personalizzato):

Opzione	Descrizione
In ONTAP 9.6 e versioni successive:	<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 e versioni precedenti:	<code>network interface create -vserver system_SVM -lif LIF_name -role intercluster -home-node node -home -port port -address port_IP -netmask netmask</code>

Per la sintassi completa dei comandi, vedere la pagina man.

Nell'esempio seguente vengono create le LIF tra cluster `cluster01_ic101` e `cluster01_ic102`:


```

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. Verificare che le LIF dell'intercluster siano state create:

Opzione	Descrizione
In ONTAP 9.6 e versioni successive:	<code>network interface show -service-policy default-intercluster</code>
In ONTAP 9.5 e versioni precedenti:	<code>network interface show -role intercluster</code>

Per la sintassi completa dei comandi, vedere la pagina `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. Verificare che le LIF dell'intercluster siano ridondanti:

Opzione	Descrizione
In ONTAP 9.6 e versioni successive:	network interface show -service-policy default-intercluster -failover
In ONTAP 9.5 e versioni precedenti:	network interface show -role intercluster -failover

Per la sintassi completa dei comandi, vedere la pagina man.

L'esempio seguente mostra che le LIF dell'intercluster `cluster01_icl01` e `cluster01_icl02` su `e0c` viene eseguito il failover della porta su `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
```

Configurare le LIF di intercluster su porte dedicate

È possibile configurare le LIF tra cluster su porte dedicate. In genere, aumenta la larghezza di banda disponibile per il traffico di replica.

Fasi

1. Elencare le porte nel cluster:

```
network port show
```

Per la sintassi completa dei comandi, vedere la pagina man.

L'esempio seguente mostra le porte di rete in `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. Determinare quali porte sono disponibili per la comunicazione tra cluster:

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

Per la sintassi completa dei comandi, vedere la pagina man.

L'esempio seguente mostra le porte e0e e. e0f Non sono stati assegnati LIF:

```
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. Creare un gruppo di failover per le porte dedicate:

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

Nell'esempio seguente vengono assegnati i port e0e e. e0f al gruppo di failover intercluster01 Sul sistema 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. Verificare che il gruppo di failover sia stato creato:

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

Per la sintassi completa dei comandi, vedere la pagina man.

```
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. Creare LIF intercluster sulla SVM di sistema e assegnarle al gruppo di failover.

Opzione	Descrizione
In ONTAP 9.6 e versioni successive:	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

Opzione	Descrizione
In ONTAP 9.5 e versioni precedenti:	<code>network interface create -vserver system_SVM -lif LIF_name -role intercluster -home-node node -home-port port -address port_IP -netmask netmask -failover-group failover_group</code>

Per la sintassi completa dei comandi, vedere la pagina man.

Nell'esempio seguente vengono create le LIF tra cluster `cluster01_icl01` e `cluster01_icl02` nel gruppo di 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. Verificare che le LIF dell'intercluster siano state create:

Opzione	Descrizione
In ONTAP 9.6 e versioni successive:	<code>network interface show -service-policy default-intercluster</code>
In ONTAP 9.5 e versioni precedenti:	<code>network interface show -role intercluster</code>

Per la sintassi completa dei comandi, vedere la pagina 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. Verificare che le LIF dell'intercluster siano ridondanti:

Opzione	Descrizione
In ONTAP 9.6 e versioni successive:	<code>network interface show -service-policy default-intercluster -failover</code>
In ONTAP 9.5 e versioni precedenti:	<code>network interface show -role intercluster -failover</code>

Per la sintassi completa dei comandi, vedere la pagina `man`.

L'esempio seguente mostra che le LIF dell'intercluster `cluster01_icl01` e `cluster01_icl02` Su SVM `e0e` viene eseguito il failover della porta su `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

```

Configurare le LIF di intercluster in spazi IPpersonalizzati

È possibile configurare le LIF di intercluster in spazi IPpersonalizzati. In questo modo è possibile isolare il traffico di replica in ambienti multitenant.

Quando si crea un IPspace personalizzato, il sistema crea una SVM (System Storage Virtual Machine) che funge da contenitore per gli oggetti di sistema in tale IPspace. È possibile utilizzare la nuova SVM come container per qualsiasi LIF di intercluster nel nuovo IPspace. Il nuovo SVM ha lo stesso nome dell'IPspace personalizzato.

Fasi

1. Elencare le porte nel cluster:

```
network port show
```

Per la sintassi completa dei comandi, vedere la pagina man.

L'esempio seguente mostra le porte di rete in `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. Creare spazi IP personalizzati sul cluster:

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

Nell'esempio seguente viene creato l'IPspace personalizzato `ip-space-IC1`:

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

3. Determinare quali porte sono disponibili per la comunicazione tra cluster:

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

Per la sintassi completa dei comandi, vedere la pagina man.

L'esempio seguente mostra le porte e0e e. e0f Non sono stati assegnati LIF:

```
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. Rimuovere le porte disponibili dal dominio di trasmissione predefinito:

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

Una porta non può trovarsi in più di un dominio di trasmissione alla volta. Per la sintassi completa dei comandi, vedere la pagina man.

Nell'esempio seguente vengono rimosse le porte e0e e. e0f dal dominio di trasmissione predefinito:

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

5. Verificare che le porte siano state rimosse dal dominio di trasmissione predefinito:

```
network port show
```

Per la sintassi completa dei comandi, vedere la pagina man.

L'esempio seguente mostra le porte e0e e. e0f sono stati rimossi dal dominio di trasmissione predefinito:


```
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. Creare un dominio di broadcast nell'IPSpace personalizzato:

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

Nell'esempio seguente viene creato il dominio di trasmissione `ipspace-IC1-bd` In 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. Verificare che il dominio di trasmissione sia stato creato:

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

Per la sintassi completa dei comandi, vedere la pagina man.

```

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. Creare LIF di intercluster sulla SVM di sistema e assegnarle al dominio di trasmissione:

Opzione	Descrizione
In ONTAP 9.6 e versioni successive:	<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>
In ONTAP 9.5 e versioni precedenti:	<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>

La LIF viene creata nel dominio di trasmissione a cui è assegnata la porta home. Il dominio di broadcast dispone di un gruppo di failover predefinito con lo stesso nome del dominio di broadcast. Per la sintassi completa dei comandi, vedere la pagina man.

Nell'esempio seguente vengono create le LIF tra cluster cluster01_ic101 e cluster01_ic102 nel dominio di broadcast ipspace-IC1-bd:

```
cluster01::> network interface create -vserver ipspace-IC1 -lif
cluster01_ic101 -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_ic102 -service-
policy default-intercluster -home-node cluster01-02 -home-port e0e
-address 192.168.1.202
-netmask 255.255.255.0
```

9. Verificare che le LIF dell'intercluster siano state create:

Opzione	Descrizione
In ONTAP 9.6 e versioni successive:	network interface show -service-policy default-intercluster
In ONTAP 9.5 e versioni precedenti:	network interface show -role intercluster

Per la sintassi completa dei comandi, vedere la pagina man.

```
cluster01::> network interface show -service-policy default-intercluster
Logical      Status      Network      Current
Current Is
Vserver      Interface  Admin/Oper  Address/Mask  Node          Port
Home
-----
-----
ipspace-IC1
      cluster01_ic101
                up/up      192.168.1.201/24  cluster01-01  e0e
true
      cluster01_ic102
                up/up      192.168.1.202/24  cluster01-02  e0f
true
```

10. Verificare che le LIF dell'intercluster siano ridondanti:

Opzione	Descrizione
In ONTAP 9.6 e versioni successive:	network interface show -service-policy default-intercluster -failover
In ONTAP 9.5 e versioni precedenti:	network interface show -role intercluster -failover

Per la sintassi completa dei comandi, vedere la pagina man.

L'esempio seguente mostra che le LIF dell'intercluster cluster01_icl01 e cluster01_icl02 Su SVM e0e failover della porta alla 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
```

Configurare le relazioni peer

Creare una relazione peer del cluster

Prima di poter proteggere i dati replicandoli in un cluster remoto per il backup dei dati e il ripristino di emergenza, è necessario creare una relazione di peer cluster tra il cluster locale e quello remoto.

Sono disponibili diversi criteri di protezione predefiniti. Se si desidera utilizzare policy personalizzate, è necessario aver creato le policy di protezione.

Prima di iniziare

- Se stai utilizzando l'interfaccia CLI di ONTAP, devi creare una intercluster LIF in ogni nodo dei cluster a cui stai effettuando il peering usando uno dei seguenti metodi:
 - ["Configurare le LIF tra cluster su porte dati condivise"](#)
 - ["Configurare intercluster LIF su porte per dati dedicate"](#)
 - ["Configurare le LIF di intercluster in spazi IP personalizzati"](#)

- I cluster devono eseguire ONTAP 9.3 o versione successiva. Se i cluster eseguono ONTAP 9.2 o versioni precedenti, fare riferimento alle procedure descritte in "[documento archiviato](#)".)



Fasi

Eeguire questa attività utilizzando Gestione di sistema di ONTAP o l'interfaccia utente di ONTAP.

System Manager

1. Nel cluster locale, fare clic su **Cluster > Impostazioni**.
2. Nella sezione **Impostazioni di intercluster**, fare clic su **Aggiungi interfacce di rete** e immettere l'indirizzo IP e la subnet mask per aggiungere interfacce di rete intercluster per il cluster.

Ripetere questo passaggio sul cluster remoto.

3. Nel cluster remoto, fare clic su **Cluster > Impostazioni**.
4. Fare clic  nella sezione **Cluster Peers** e selezionare **generate Passphrase**.
5. Selezionare la versione del cluster ONTAP remoto.
6. Copiare la passphrase generata.
7. Nel cluster locale, in **Cluster Peers**, fare clic su  e selezionare **Peer cluster**.
8. Nella finestra **Peer cluster**, incollare la passphrase e fare clic su **Initiate cluster peering**.

CLI

1. Sul cluster di destinazione, creare una relazione peer con il cluster di origine:

```
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  
<ipspace>
```

Se si specificano entrambi `-generate-passphrase` e `-peer-addr`, Solo il cluster i cui LIF intercluster sono specificati in `-peer-addr` può utilizzare la password generata.

È possibile ignorare `-ip` Se non si utilizza un IPspace personalizzato. Per la sintassi completa dei comandi, vedere la pagina man.

Se si crea la relazione di peering in ONTAP 9.6 o versione successiva e non si desidera crittografare le comunicazioni di peering tra cluster, è necessario utilizzare `-encryption-protocol-proposed none` opzione per disattivare la crittografia.

Nell'esempio seguente viene creata una relazione peer del cluster con un cluster remoto non specificato e viene pre-autorizzata la relazione peer con le SVM `vs1` e `vs2` sul cluster locale:

```
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.
```

Nell'esempio riportato di seguito viene creata una relazione peer del cluster con il cluster remoto agli indirizzi IP LIF 192.140.112.103 e 192.140.112.104 dell'intercluster e viene pre-autorizzata una relazione peer con qualsiasi SVM sul cluster locale:

```
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.
```

Nell'esempio seguente viene creata una relazione peer del cluster con un cluster remoto non specificato e viene pre-autorizzata la relazione peer con le SVM_{vs1} e _{vs2} sul cluster locale:

```
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. Nel cluster di origine, autenticare il cluster di origine nel cluster di destinazione:

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

Per la sintassi completa dei comandi, vedere la pagina `man`.

Nell'esempio seguente viene autenticato il cluster locale nel cluster remoto agli indirizzi IP LIF 192.140.112.101 e 192.140.112.102 dell'intercluster:

```
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.
```

Inserire la passphrase per la relazione peer quando richiesto.

3. Verificare che la relazione peer del cluster sia stata creata:

```
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. Verificare la connettività e lo stato dei nodi nella relazione peer:

```
cluster peer health show
```

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

Altri modi per farlo in ONTAP

Per eseguire queste attività con...	Guarda questo contenuto...
System Manager Classic (disponibile con ONTAP 9.7 e versioni precedenti)	"Panoramica sulla preparazione del disaster recovery dei volumi"

Creare una relazione peer SVM tra cluster

È possibile utilizzare `vserver peer create` Per creare una relazione peer tra SVM su cluster locali e remoti.

Prima di iniziare

- I cluster di origine e di destinazione devono essere peering.

- I cluster devono eseguire ONTAP 9.3. Se i cluster eseguono ONTAP 9.2 o versioni precedenti, fare riferimento alle procedure descritte in ["documento archiviato"](#).)
- È necessario disporre di relazioni peer "pre-autorizzate" per le SVM sul cluster remoto.

Per ulteriori informazioni, vedere ["Creazione di una relazione peer del cluster"](#).

A proposito di questa attività

In ONTAP 9,2 e versioni precedenti, puoi autorizzare una relazione di peer per una sola SVM alla volta. Ciò significa che è necessario eseguire `vserver peer accept` Comando ogni volta che autorizzi una relazione peer SVM in sospeso.

A partire da ONTAP 9.3, è possibile "pre-autorizzare" le relazioni peer per più SVM elencando le SVM in `-initial-allowed-vserver` quando si crea una relazione peer del cluster. Per ulteriori informazioni, vedere ["Creazione di una relazione peer del cluster"](#).

Fasi

1. Nel cluster di destinazione per la protezione dei dati, visualizzare le SVM pre-autorizzate per il peering:

```
vserver peer permission show
```

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

2. Sul cluster di origine per la protezione dei dati, creare una relazione peer con una SVM pre-autorizzata sul cluster di destinazione per la protezione dei dati:

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

Per la sintassi completa dei comandi, vedere la pagina `man`.

Nell'esempio seguente viene creata una relazione peer tra la SVM locale `pvs1` E la SVM remota pre-autorizzata `vs1`:

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

3. Verificare la relazione peer 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

```

Aggiungere una relazione peer SVM tra cluster

Se si crea una SVM dopo aver configurato una relazione peer del cluster, sarà necessario aggiungere manualmente una relazione peer per la SVM. È possibile utilizzare `vserver peer create` Per creare una relazione peer tra le SVM. Una volta creata la relazione peer, è possibile eseguire `vserver peer accept` sul cluster remoto per autorizzare la relazione peer.

Prima di iniziare

I cluster di origine e di destinazione devono essere peering.

A proposito di questa attività

È possibile creare relazioni peer tra le SVM nello stesso cluster per il backup dei dati locale. Per ulteriori informazioni, consultare `vserver peer create` pagina man.

Gli amministratori utilizzano occasionalmente `vserver peer reject` Comando per rifiutare una relazione peer SVM proposta. Se la relazione tra le SVM si trova in `rejected state` (stato), è necessario eliminare la relazione prima di crearne una nuova. Per ulteriori informazioni, consultare `vserver peer delete` pagina man.

Fasi

1. Nel cluster di origine per la protezione dei dati, creare una relazione peer con una SVM nel cluster di destinazione per la protezione dei dati:

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

Nell'esempio seguente viene creata una relazione peer tra la SVM locale `pvs1` E SVM remoto `vs1`

```

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

```

Se le SVM locali e remote hanno gli stessi nomi, è necessario utilizzare un *nome locale* per creare la relazione peer SVM:

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

2. Nel cluster di origine per la protezione dei dati, verificare che la relazione peer sia stata avviata:

```
vserver peer show-all
```

Per la sintassi completa dei comandi, vedere la pagina man.

L'esempio seguente mostra che la relazione peer tra SVM_{pvs1} E SVM_{vs1} è stato avviato:

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

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

3. Sul cluster di destinazione per la protezione dei dati, visualizzare la relazione peer SVM in sospenso:

```
vserver peer show
```

Per la sintassi completa dei comandi, vedere la pagina man.

Nell'esempio riportato di seguito sono elencate le relazioni peer in sospenso per cluster02:

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

Vserver	Peer Vserver	Peer State
vs1	pvs1	pending

4. Nel cluster di destinazione per la protezione dei dati, autorizzare la relazione peer in sospenso:

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

Per la sintassi completa dei comandi, vedere la pagina man.

Nell'esempio riportato di seguito viene autorizzata la relazione peer tra la SVM locale vs1 E SVM remoto pvs1:

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

5. Verificare la relazione peer 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
```

Abilitare la crittografia del peering del cluster su una relazione peer esistente

A partire da ONTAP 9.6, la crittografia del peering del cluster è attivata per impostazione predefinita su tutte le relazioni di peering del cluster appena create. La crittografia del peering dei cluster utilizza una chiave precondivisa (PSK) e TLS (Transport Security Layer) per proteggere le comunicazioni di peering tra cluster. Questo aggiunge un ulteriore livello di sicurezza tra i cluster peered.

A proposito di questa attività

Se si aggiornano i cluster peering a ONTAP 9.6 o versione successiva e la relazione di peering è stata creata in ONTAP 9.5 o versione precedente, la crittografia di peering dei cluster deve essere attivata manualmente dopo l'aggiornamento. Entrambi i cluster della relazione di peering devono eseguire ONTAP 9.6 o versione successiva per abilitare la crittografia di peering dei cluster.

Fasi

1. Sul cluster di destinazione, attivare la crittografia per le comunicazioni con il cluster di origine:

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

2. Quando richiesto, inserire una passphrase.
3. Nel cluster di origine per la protezione dei dati, abilitare la crittografia per la comunicazione con il cluster di destinazione per la protezione dei dati:

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

4. Quando richiesto, inserire la stessa passphrase inserita nel cluster di destinazione.

Rimuovere la crittografia di peering del cluster da una relazione peer esistente

Per impostazione predefinita, la crittografia del peering del cluster è attivata su tutte le

relazioni peer create in ONTAP 9.6 o versioni successive. Se non si desidera utilizzare la crittografia per le comunicazioni di peering tra cluster, è possibile disattivarla.

Fasi

1. Nel cluster di destinazione, modificare le comunicazioni con il cluster di origine per interrompere l'utilizzo della crittografia di peering dei cluster:

- Per rimuovere la crittografia, ma mantenere l'autenticazione, immettere:

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

- Per rimuovere crittografia e autenticazione:

i. Modificare la policy di peering del cluster per consentire l'accesso non autenticato:

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

ii. Modificare l'accesso alla crittografia e all'autenticazione:

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

2. Quando richiesto, immettere la passphrase.

3. Confermare la passphrase immettendola di nuovo.

4. Sul cluster di origine, disattivare la crittografia per la comunicazione con il cluster di destinazione:

- Per rimuovere la crittografia, ma mantenere l'autenticazione, immettere:

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

- Per rimuovere crittografia e autenticazione:

i. Modificare la policy di peering del cluster per consentire l'accesso non autenticato:

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

ii. Modificare l'accesso alla crittografia e all'autenticazione:

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

5. Quando richiesto, immettere e reinserire la stessa passphrase utilizzata nel cluster di destinazione.

Informazioni sul copyright

Copyright © 2024 NetApp, Inc. Tutti i diritti riservati. Stampato negli Stati Uniti d'America. Nessuna porzione di questo documento soggetta a copyright può essere riprodotta in qualsiasi formato o mezzo (grafico, elettronico o meccanico, inclusi fotocopie, registrazione, nastri o storage in un sistema elettronico) senza previo consenso scritto da parte del detentore del copyright.

Il software derivato dal materiale sottoposto a copyright di NetApp è soggetto alla seguente licenza e dichiarazione di non responsabilità:

IL PRESENTE SOFTWARE VIENE FORNITO DA NETAPP "COSÌ COM'È" E SENZA QUALSIVOGLIA TIPO DI GARANZIA IMPLICITA O ESPRESSA FRA CUI, A TITOLO ESEMPLIFICATIVO E NON ESAUSTIVO, GARANZIE IMPLICITE DI COMMERCIALIZZABILITÀ E IDONEITÀ PER UNO SCOPO SPECIFICO, CHE VENGONO DECLINATE DAL PRESENTE DOCUMENTO. NETAPP NON VERRÀ CONSIDERATA RESPONSABILE IN ALCUN CASO PER QUALSIVOGLIA DANNO DIRETTO, INDIRETTO, ACCIDENTALE, SPECIALE, ESEMPLARE E CONSEGUENZIALE (COMPRESI, A TITOLO ESEMPLIFICATIVO E NON ESAUSTIVO, PROCUREMENT O SOSTITUZIONE DI MERCI O SERVIZI, IMPOSSIBILITÀ DI UTILIZZO O PERDITA DI DATI O PROFITTI OPPURE INTERRUZIONE DELL'ATTIVITÀ AZIENDALE) CAUSATO IN QUALSIVOGLIA MODO O IN RELAZIONE A QUALUNQUE TEORIA DI RESPONSABILITÀ, SIA ESSA CONTRATTUALE, RIGOROSA O DOVUTA A INSOLVENZA (COMPRESA LA NEGLIGENZA O ALTRO) INSORTA IN QUALSIASI MODO ATTRAVERSO L'UTILIZZO DEL PRESENTE SOFTWARE ANCHE IN PRESENZA DI UN PREAVVISO CIRCA L'EVENTUALITÀ DI QUESTO TIPO DI DANNI.

NetApp si riserva il diritto di modificare in qualsiasi momento qualunque prodotto descritto nel presente documento senza fornire alcun preavviso. NetApp non si assume alcuna responsabilità circa l'utilizzo dei prodotti o materiali descritti nel presente documento, con l'eccezione di quanto concordato espressamente e per iscritto da NetApp. L'utilizzo o l'acquisto del presente prodotto non comporta il rilascio di una licenza nell'ambito di un qualche diritto di brevetto, marchio commerciale o altro diritto di proprietà intellettuale di NetApp.

Il prodotto descritto in questa guida può essere protetto da uno o più brevetti degli Stati Uniti, esteri o in attesa di approvazione.

LEGENDA PER I DIRITTI SOTTOPOSTI A LIMITAZIONE: l'utilizzo, la duplicazione o la divulgazione da parte degli enti governativi sono soggetti alle limitazioni indicate nel sottoparagrafo (b)(3) della clausola Rights in Technical Data and Computer Software del DFARS 252.227-7013 (FEB 2014) e FAR 52.227-19 (DIC 2007).

I dati contenuti nel presente documento riguardano un articolo commerciale (secondo la definizione data in FAR 2.101) e sono di proprietà di NetApp, Inc. Tutti i dati tecnici e il software NetApp forniti secondo i termini del presente Contratto sono articoli aventi natura commerciale, sviluppati con finanziamenti esclusivamente privati. Il governo statunitense ha una licenza irrevocabile limitata, non esclusiva, non trasferibile, non cedibile, mondiale, per l'utilizzo dei Dati esclusivamente in connessione con e a supporto di un contratto governativo statunitense in base al quale i Dati sono distribuiti. Con la sola esclusione di quanto indicato nel presente documento, i Dati non possono essere utilizzati, divulgati, riprodotti, modificati, visualizzati o mostrati senza la previa approvazione scritta di NetApp, Inc. I diritti di licenza del governo degli Stati Uniti per il Dipartimento della Difesa sono limitati ai diritti identificati nella clausola DFARS 252.227-7015(b) (FEB 2014).

Informazioni sul marchio commerciale

NETAPP, il logo NETAPP e i marchi elencati alla pagina <http://www.netapp.com/TM> sono marchi di NetApp, Inc. Gli altri nomi di aziende e prodotti potrebbero essere marchi dei rispettivi proprietari.