



Configurazione NDMP

ONTAP 9

NetApp
January 08, 2026

Sommario

- Configurazione NDMP 1
 - Informazioni sulla configurazione NDMP di ONTAP 1
 - Scopri di più sul flusso di lavoro di configurazione NDMP di ONTAP 1
 - Preparare le configurazioni ONTAP NDMP 2
 - Verificare le connessioni del dispositivo a nastro ONTAP NDMP 5
 - Abilitare le prenotazioni dei nastri per le operazioni di backup ONTAP NDMP 6
 - Configurare NDMP con ambito SVM 7
 - Abilitare NDMP con ambito SVM sul cluster ONTAP 7
 - Abilitare gli utenti di backup per l'autenticazione ONTAP NDMP 8
 - Configurare ONTAP LIF per NDMP con ambito SVM 9
 - Configurare NDMP con ambito nodo 16
 - Abilita NDMP con ambito nodo sul cluster ONTAP 16
 - Configurare ONTAP LIF per NDMP con ambito nodo 17
 - Configurare le applicazioni di backup per la configurazione ONTAP NDMP 22

Configurazione NDMP

Informazioni sulla configurazione NDMP di ONTAP

È possibile configurare rapidamente un cluster ONTAP 9 in modo che utilizzi il protocollo di gestione dei dati di rete (NDMP) per eseguire il backup dei dati direttamente su nastro utilizzando un'applicazione di backup di terze parti.

Se l'applicazione di backup supporta Cluster Aware Backup (CAB), è possibile configurare NDMP come *SVM-scoped* o *node-scoped*:

- SVM-scope a livello di cluster (admin SVM) consente di eseguire il backup di tutti i volumi ospitati su diversi nodi del cluster. Se possibile, si consiglia di utilizzare NDMP con ambito SVM.
- NDMP con ambito nodo consente di eseguire il backup di tutti i volumi ospitati su quel nodo.

Se l'applicazione di backup non supporta CAB, è necessario utilizzare NDMP con ambito nodo.

Gli NDMP con ambito SVM e nodo si escludono a vicenda e non possono essere configurati sullo stesso cluster.



NDMP con ambito del nodo è obsoleto in ONTAP 9.

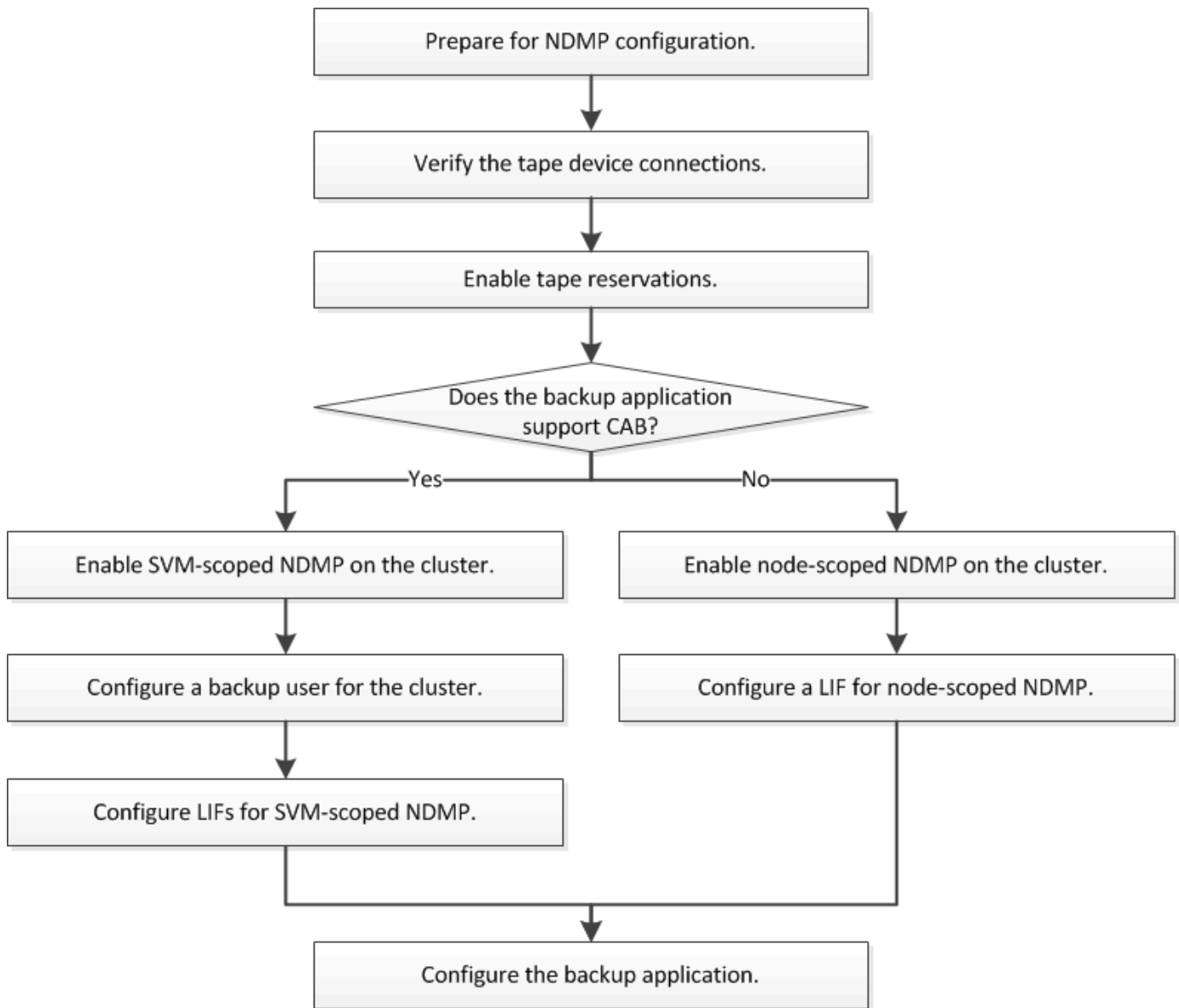
Ulteriori informazioni su "[Backup cluster-aware \(CAB\)](#)".

Prima di configurare NDMP, verificare quanto segue:

- Si dispone di un'applicazione di backup di terze parti (chiamata anche Data Management Application o DMA).
- Sei un amministratore del cluster.
- Sono installati i dispositivi a nastro e un server multimediale opzionale.
- I dispositivi a nastro sono connessi al cluster tramite uno switch Fibre Channel (FC) o collegato localmente.
- Almeno un dispositivo a nastro ha un numero di unità logica (LUN) pari a 0.

Scopri di più sul flusso di lavoro di configurazione NDMP di ONTAP

L'impostazione del backup su nastro su NDMP richiede la preparazione della configurazione NDMP, la verifica delle connessioni dei dispositivi a nastro, l'attivazione delle prenotazioni su nastro, la configurazione di NDMP a livello di SVM o di nodo, l'abilitazione di NDMP sul cluster, la configurazione di un utente di backup, la configurazione di LIF e la configurazione dell'applicazione di backup.



Preparare le configurazioni ONTAP NDMP

Prima di configurare l'accesso al backup su nastro tramite NDMP (Network Data Management Protocol), è necessario verificare che la configurazione pianificata sia supportata, verificare che le unità a nastro siano elencate come unità qualificate su ciascun nodo, verificare che tutti i nodi dispongano di LIF intercluster, E identificare se l'applicazione di backup supporta l'estensione CAB (Cluster Aware Backup).

Fasi

1. Fare riferimento alla matrice di compatibilità del provider di applicazioni di backup per il supporto ONTAP (NetApp non qualifica le applicazioni di backup di terze parti con ONTAP o NDMP).

Verificare che i seguenti componenti NetApp siano compatibili:

- La versione di ONTAP 9 in esecuzione sul cluster.
- Il vendor e la versione dell'applicazione di backup: Ad esempio, Veritas NetBackup 8.2 o CommVault.

- I dettagli dei dispositivi a nastro, come il produttore, il modello e l'interfaccia delle unità a nastro, ad esempio IBM Ultrium 8 o HPE StoreEver Ultrium 30750 LTO-8.
- Le piattaforme dei nodi nel cluster, ad esempio FAS8700 o A400.



Le matrici di supporto per la compatibilità ONTAP legacy per le applicazioni di backup sono disponibili in ["Tool di matrice di interoperabilità NetApp"](#).

2. Verificare che le unità a nastro siano elencate come unità qualificate nel file di configurazione del nastro integrato di ciascun nodo:

- a. Nell'interfaccia della riga di comando, visualizzare il file di configurazione del nastro integrato utilizzando `storage tape show-supported-status` comando.

```
cluster1::> storage tape show-supported-status

Node: cluster1-1

Tape Drives                                Is
-----                                -
Certance Ultrium 2                        true      Dynamically Qualified
Certance Ultrium 3                        true      Dynamically Qualified
Digital DLT2000                          true      Qualified
```

- b. Confrontare le unità a nastro con l'elenco delle unità qualificate nell'output.



I nomi dei dispositivi a nastro nell'output potrebbero variare leggermente rispetto ai nomi sull'etichetta del dispositivo o nella matrice di interoperabilità. Ad esempio, Digital DLT2000 può anche essere noto come DLT2k. È possibile ignorare queste differenze di denominazione minori.

- c. Se un dispositivo non è elencato come qualificato nell'output anche se il dispositivo è qualificato secondo la matrice di interoperabilità, scaricare e installare un file di configurazione aggiornato per il dispositivo utilizzando le istruzioni sul sito del supporto NetApp.

["Download NetApp: File di configurazione dei dispositivi su nastro"](#)

Un dispositivo qualificato potrebbe non essere elencato nel file di configurazione del nastro integrato se il dispositivo a nastro è stato qualificato dopo la spedizione del nodo.

3. Verificare che ogni nodo del cluster disponga di una LIF intercluster:

- a. Visualizzare le LIF di intercluster sui nodi utilizzando `network interface show -role intercluster` comando.

```
cluster1::> network interface show -role intercluster
```

	Logical	Status	Network	Current
Current Is				
Vserver	Interface	Admin/Oper	Address/Mask	Node
Port	Home			
-----	-----	-----	-----	-----
-----	-----	-----	-----	-----
cluster1	IC1	up/up	192.0.2.65/24	cluster1-1
e0a	true			

Ulteriori informazioni su `network interface show` nella ["Riferimento al comando ONTAP"](#).

- b. Se non esiste una LIF di intercluster su un nodo, creare una LIF di intercluster utilizzando `network interface create` comando.

```
cluster1::> network interface create -vserver cluster1 -lif IC2 -role  
intercluster  
-home-node cluster1-2 -home-port e0b -address 192.0.2.68 -netmask  
255.255.255.0  
-status-admin up -failover-policy local-only -firewall-policy  
intercluster
```

```
cluster1::> network interface show -role intercluster
```

	Logical	Status	Network	Current
Current Is				
Vserver	Interface	Admin/Oper	Address/Mask	Node
Port	Home			
-----	-----	-----	-----	-----
-----	-----	-----	-----	-----
cluster1	IC1	up/up	192.0.2.65/24	cluster1-1
e0a	true			
cluster1	IC2	up/up	192.0.2.68/24	cluster1-2
e0b	true			

Ulteriori informazioni su `network interface create` nella ["Riferimento al comando ONTAP"](#).

"Gestione della rete"

4. Identificare se l'applicazione di backup supporta Cluster Aware Backup (CAB) utilizzando la documentazione fornita con l'applicazione di backup.

Il supporto CAB è un fattore chiave per determinare il tipo di backup che è possibile eseguire.

Informazioni correlate

- ["spettacolo di nastri di archiviazione"](#)
- ["nastro di archiviazione mostra-stato-supportato"](#)

Verificare le connessioni del dispositivo a nastro ONTAP NDMP

Assicurarsi che tutti i dischi e i media changer siano visibili in ONTAP come dispositivi.

Fasi

1. Visualizzare le informazioni su tutti i dischi e i media changer utilizzando `storage tape show` comando.

```
cluster1::> storage tape show
```

```
Node: cluster1-01
```

Device ID	Device Type	Description
-----------	-------------	-------------

Status		
--------	--	--

-----	-----	-----
-------	-------	-------

sw4:10.11	tape drive	HP LTO-3
-----------	------------	----------

normal		
--------	--	--

0b.125L1	media changer	HP MSL G3 Series
----------	---------------	------------------

normal		
--------	--	--

0d.4	tape drive	IBM LTO 5 ULT3580
------	------------	-------------------

normal		
--------	--	--

0d.4L1	media changer	IBM 3573-TL
--------	---------------	-------------

normal		
--------	--	--

...		
-----	--	--

...		
-----	--	--

2. Se non viene visualizzata un'unità a nastro, risolvere il problema.
3. Se non viene visualizzato un media changer, visualizzare le informazioni sui media changer utilizzando `storage tape show-media-changer` e risolvere il problema.

```
cluster1::> storage tape show-media-changer
```

```
Media Changer: sw4:10.11L1
```

```
Description: PX70-TL
```

```
WWNN: 2:00a:000e11:10b919
```

```
WWPN: 2:00b:000e11:10b919
```

```
Serial Number: 00FRU7800000_LL1
```

```
Errors: -
```

```
Paths:
```

```
Node Initiator Alias Device State
```

```
Status
```

```
-----
```

```
cluster1-01 2b mc0 in-use
```

```
normal
```

```
...
```

Informazioni correlate

- ["nastro di archiviazione mostra-supporto-cambia-nastro"](#)

Abilitare le prenotazioni dei nastri per le operazioni di backup ONTAP NDMP

È necessario assicurarsi che le unità a nastro siano riservate all'utilizzo da parte delle applicazioni di backup per le operazioni di backup NDMP.

A proposito di questa attività

Le impostazioni di prenotazione variano in diverse applicazioni di backup e devono corrispondere all'applicazione di backup e ai nodi o ai server che utilizzano gli stessi dischi. Consultare la documentazione del fornitore dell'applicazione di backup per le impostazioni di prenotazione corrette.

Fasi

1. Attivare le prenotazioni utilizzando `options -option-name tape.reservations -option-value persistent` comando.

Il seguente comando consente di attivare le prenotazioni con `persistent` valore:

```
cluster1::> options -option-name tape.reservations -option-value  
persistent  
2 entries were modified.
```

2. Verificare che le prenotazioni siano attivate su tutti i nodi utilizzando `options tape.reservations e`

quindi esaminare l'output.

```
cluster1::> options tape.reservations

cluster1-1
  tape.reservations                persistent

cluster1-2
  tape.reservations                persistent
2 entries were displayed.
```

Configurare NDMP con ambito SVM

Abilitare NDMP con ambito SVM sul cluster ONTAP

Se il DMA supporta l'estensione CAB (Cluster Aware Backup), è possibile eseguire il backup di tutti i volumi ospitati su diversi nodi di un cluster attivando NDMP con ambito SVM, attivando il servizio NDMP sul cluster (SVM amministrativa) e configurando i LIF per la connessione dati e di controllo.

Prima di iniziare

L'estensione DELLA CABINA deve essere supportata dal DMA.

A proposito di questa attività

La disattivazione della modalità NDMP con ambito nodo attiva la modalità NDMP con ambito SVM sul cluster.

Fasi

1. Abilita la modalità NDMP SVM-scoped:

```
cluster1::> system services ndmp node-scope-mode off
```

La modalità NDMP SVM-scoped è abilitata.

2. Attivare il servizio NDMP sulla SVM di amministrazione:

```
cluster1::> vserver services ndmp on -vserver cluster1
```

Il tipo di autenticazione è impostato su `challenge` per impostazione predefinita, l'autenticazione in chiaro è disattivata.



Per una comunicazione sicura, è necessario disattivare l'autenticazione in chiaro.

3. Verificare che il servizio NDMP sia abilitato:

```
cluster1::> vserver services ndmp show
```

Vserver	Enabled	Authentication type
-----	-----	-----
cluster1	true	challenge
vs1	false	challenge

Abilitare gli utenti di backup per l'autenticazione ONTAP NDMP

Per autenticare NDMP con ambito SVM dall'applicazione di backup, è necessario disporre di un utente amministrativo con privilegi sufficienti e di una password NDMP.

A proposito di questa attività

È necessario generare una password NDMP per gli utenti amministratori del backup. È possibile abilitare gli utenti amministratori di backup a livello di cluster o SVM e, se necessario, creare un nuovo utente. Per impostazione predefinita, gli utenti con i seguenti ruoli possono eseguire l'autenticazione per il backup NDMP:

- A livello di cluster: `admin` oppure `backup`
- SVM individuali: `vsadmin` oppure `vsadmin-backup`

Se si utilizza un utente NIS o LDAP, l'utente deve esistere sul rispettivo server. Non è possibile utilizzare un utente Active Directory.

Fasi

1. Visualizza gli utenti e i permessi di amministrazione correnti:

```
security login show
```

Ulteriori informazioni su `security login show` nella ["Riferimento al comando ONTAP"](#).

2. Se necessario, creare un nuovo utente di backup NDMP con `security login create` E il ruolo appropriato per i privilegi SVM a livello di cluster o singoli.

È possibile specificare un nome utente per il backup locale o un nome utente NIS o LDAP per `-user-or-group-name` parametro.

Il seguente comando crea l'utente di backup `backup_admin1` con `backup` ruolo per l'intero cluster:

```
cluster1::> security login create -user-or-group-name backup_admin1  
-application ssh -authmethod password -role backup
```

Il seguente comando crea l'utente di backup `vsbackup_admin1` con `vsadmin-backup` Ruolo di una singola SVM:

```
cluster1::> security login create -user-or-group-name vsbackup_admin1  
-application ssh -authmethod password -role vsadmin-backup
```

Inserire una password per il nuovo utente e confermare.

Ulteriori informazioni su security login create nella ["Riferimento al comando ONTAP"](#).

3. Generare una password per la SVM amministrativa utilizzando `vserver services ndmp generate password` comando.

La password generata deve essere utilizzata per autenticare la connessione NDMP dall'applicazione di backup.

```
cluster1::> vserver services ndmp generate-password -vserver cluster1  
-user backup_admin1
```

```
Vserver: cluster1  
User: backup_admin1  
Password: qG5CqQHYxw7tE57g
```

Configurare ONTAP LIF per NDMP con ambito SVM

È necessario identificare le LIF che verranno utilizzate per stabilire una connessione dati tra le risorse di dati e nastro e per controllare la connessione tra la SVM amministrativa e l'applicazione di backup. Dopo aver identificato le LIF, devi verificare che siano impostati i criteri di servizio e failover.



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 ["Gestione del traffico supportato"](#).

ONTAP 9.10.1 o versione successiva

Fasi

1. Identificare la LIF intercluster nei nodi usando il comando `network interface show` il `-service-policy` parametro.

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

Ulteriori informazioni su `network interface show` nella ["Riferimento al comando ONTAP"](#).

2. Identifica la LIF di gestione ospitata sui nodi usando il `network interface show` comando insieme al `-service-policy` parametro.

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

3. Assicurarsi che la intercluster LIF includa il `backup-ndmp-control` servizio:

```
network interface service-policy show
```

Ulteriori informazioni su `network interface service-policy show` nella ["Riferimento al comando ONTAP"](#).

4. Assicurarsi che la policy di failover sia impostata correttamente per tutte le LIF:

- a. Verificare che il criterio di failover per la LIF di gestione del cluster sia impostato su `broadcast-domain-wide` E il criterio per le LIF di gestione di intercluster e nodi è impostato su `local-only` utilizzando `network interface show -failover` comando.

Il seguente comando visualizza il criterio di failover per le LIF di gestione del cluster, dell'intercluster e dei nodi:

```
cluster1::> network interface show -failover
```

Vserver	Logical Interface	Home Node:Port	Failover Policy	Failover Group
cluster	cluster1_clus1	cluster1-1:e0a	local-only	cluster Failover
Targets:				
cluster1	cluster_mgmt	cluster1-1:e0m	broadcast-domain-wide	Default Failover
Targets:				
	IC1	cluster1-1:e0a	local-only	Default Failover
Targets:				
	IC2	cluster1-1:e0b	local-only	Default Failover
Targets:				
cluster1-1	c1-1_mgmt1	cluster1-1:e0m	local-only	Default Failover
Targets:				
cluster1-2	c1-2_mgmt1	cluster1-2:e0m	local-only	Default Failover
Targets:				

- a. Se i criteri di failover non sono impostati correttamente, modificare il criterio di failover utilizzando `network interface modify` con il `-failover-policy` parametro.

```
cluster1::> network interface modify -vserver cluster1 -lif IC1
-failover-policy local-only
```

Ulteriori informazioni su `network interface modify` nella ["Riferimento al comando ONTAP"](#).

5. Specificare le LIF richieste per la connessione dati utilizzando `vserver services ndmp modify` con il `preferred-interface-role` parametro.

```
cluster1::> vserver services ndmp modify -vserver cluster1
-preferred-interface-role intercluster,cluster-mgmt,node-mgmt
```

6. Verificare che il ruolo di interfaccia preferito sia impostato per il cluster utilizzando `vserver services ndmp show` comando.

```
cluster1::> vserver services ndmp show -vserver cluster1

Vserver: cluster1
NDMP Version: 4
.....
.....
Preferred Interface Role: intercluster, cluster-mgmt, node-mgmt
```

ONTAP 9.9 o versioni precedenti

Fasi

1. Identificare le LIF di gestione di intercluster, cluster e nodi utilizzando `network interface show` con il `-role` parametro.

Il seguente comando visualizza le LIF dell'intercluster:

```
cluster1::> network interface show -role intercluster
```

	Logical	Status	Network	Current
Current Is				
Vserver	Interface	Admin/Oper	Address/Mask	Node
Port	Home			
-----	-----	-----	-----	-----
-----	-----			
cluster1	IC1	up/up	192.0.2.65/24	cluster1-1
e0a	true			
cluster1	IC2	up/up	192.0.2.68/24	cluster1-2
e0b	true			

Il seguente comando visualizza la LIF di gestione del cluster:

```
cluster1::> network interface show -role cluster-mgmt
```

	Logical	Status	Network	Current
Current Is				
Vserver	Interface	Admin/Oper	Address/Mask	Node
Port	Home			
-----	-----	-----	-----	-----
-----	-----			
cluster1	cluster_mgmt	up/up	192.0.2.60/24	cluster1-2
e0M	true			

Il seguente comando visualizza le LIF di gestione dei nodi:

```
cluster1::> network interface show -role node-mgmt
```

	Logical	Status	Network	Current
Current Is				
Vserver	Interface	Admin/Oper	Address/Mask	Node
Port	Home			
-----	-----	-----	-----	
-----	-----	-----	-----	
cluster1	cluster1-1_mgmt1	up/up	192.0.2.69/24	cluster1-1
e0M	true			
	cluster1-2_mgmt1	up/up	192.0.2.70/24	cluster1-2
e0M	true			

Ulteriori informazioni su `network interface show` nella ["Riferimento al comando ONTAP"](#).

2. Assicurarsi che il criterio firewall sia abilitato per NDMP sulle (`node-mgmt`interfacce LIF intercluster, cluster-(`cluster-mgmt`management) e Node-management):
 - a. Verificare che il criterio firewall sia abilitato per NDMP utilizzando `system services firewall policy show` comando.

Il seguente comando visualizza il criterio del firewall per la LIF di gestione del cluster:

```
cluster1::> system services firewall policy show -policy cluster
```

Vserver	Policy	Service	Allowed
-----	-----	-----	-----
cluster	cluster	dns	0.0.0.0/0
		http	0.0.0.0/0
		https	0.0.0.0/0
		ndmp	0.0.0.0/0
		ndmps	0.0.0.0/0
		ntp	0.0.0.0/0
		rsh	0.0.0.0/0
		snmp	0.0.0.0/0
		ssh	0.0.0.0/0
		telnet	0.0.0.0/0

10 entries were displayed.

Il seguente comando visualizza il criterio firewall per la LIF dell'intercluster:

```
cluster1::> system services firewall policy show -policy
intercluster
```

Vserver	Policy	Service	Allowed
cluster1	intercluster	dns	-
		http	-
		https	-
		ndmp	0.0.0.0/0, ::/0
		ndmps	-
		ntp	-
		rsh	-
		ssh	-
		telnet	-

9 entries were displayed.

Il seguente comando visualizza il criterio firewall per la LIF di gestione dei nodi:

```
cluster1::> system services firewall policy show -policy mgmt
```

Vserver	Policy	Service	Allowed
cluster1-1	mgmt	dns	0.0.0.0/0, ::/0
		http	0.0.0.0/0, ::/0
		https	0.0.0.0/0, ::/0
		ndmp	0.0.0.0/0, ::/0
		ndmps	0.0.0.0/0, ::/0
		ntp	0.0.0.0/0, ::/0
		rsh	-
		snmp	0.0.0.0/0, ::/0
		ssh	0.0.0.0/0, ::/0
		telnet	-

10 entries were displayed.

- b. Se il criterio del firewall non è attivato, attivare il criterio del firewall utilizzando `system services firewall policy modify` con il `-service` parametro.

Il seguente comando abilita il criterio firewall per la LIF dell'intercluster:

```
cluster1::> system services firewall policy modify -vserver cluster1
-policy intercluster -service ndmp 0.0.0.0/0
```

3. Assicurarsi che la policy di failover sia impostata correttamente per tutte le LIF:

- a. Verificare che il criterio di failover per la LIF di gestione del cluster sia impostato su broadcast-domain-wide`E il criterio per le LIF di gestione di intercluster e nodi è impostato su `local-only utilizzando network interface show -failover comando.

Il seguente comando visualizza il criterio di failover per le LIF di gestione del cluster, dell'intercluster e dei nodi:

```
cluster1::> network interface show -failover
```

Failover Vserver Group	Logical Interface	Home Node:Port	Failover Policy
-----	-----	-----	-----
cluster cluster	cluster1_clus1	cluster1-1:e0a	local-only
			Failover
Targets:		
cluster1 wide Default	cluster_mgmt	cluster1-1:e0m	broadcast-domain-
			Failover
Targets:		
Default	IC1	cluster1-1:e0a	local-only
			Failover
Targets:		
Default	IC2	cluster1-1:e0b	local-only
			Failover
Targets:		
cluster1-1 Default	cluster1-1_mgmt1	cluster1-1:e0m	local-only
			Failover
Targets:		
cluster1-2 Default	cluster1-2_mgmt1	cluster1-2:e0m	local-only
			Failover
Targets:		

- a. Se i criteri di failover non sono impostati correttamente, modificare il criterio di failover utilizzando `network interface modify` con il `-failover-policy` parametro.

```
cluster1::> network interface modify -vserver cluster1 -lif IC1  
-failover-policy local-only
```

Ulteriori informazioni su `network interface modify` nella ["Riferimento al comando ONTAP"](#).

4. Specificare le LIF richieste per la connessione dati utilizzando `vserver services ndmp modify` con il `preferred-interface-role` parametro.

```
cluster1::> vserver services ndmp modify -vserver cluster1  
-preferred-interface-role intercluster,cluster-mgmt,node-mgmt
```

5. Verificare che il ruolo di interfaccia preferito sia impostato per il cluster utilizzando `vserver services ndmp show` comando.

```
cluster1::> vserver services ndmp show -vserver cluster1  
  
Vserver: cluster1  
NDMP Version: 4  
.....  
.....  
Preferred Interface Role: intercluster, cluster-mgmt,  
node-mgmt
```

Configurare NDMP con ambito nodo

Abilita NDMP con ambito nodo sul cluster ONTAP

È possibile eseguire il backup dei volumi ospitati su un singolo nodo attivando NDMP con ambito nodo, attivando il servizio NDMP e configurando una LIF per la connessione dati e di controllo. Questa operazione può essere eseguita per tutti i nodi del cluster.



NDMP con ambito del nodo è obsoleto in ONTAP 9.

A proposito di questa attività

Quando si utilizza NDMP in modalità Node-Scope, l'autenticazione deve essere configurata per nodo. Per ulteriori informazioni, vedere ["L'articolo della Knowledge base "come configurare l'autenticazione NDMP in modalità 'node-scope'"](#).

Fasi

1. Abilita la modalità NDMP con ambito dei nodi:

```
cluster1::> system services ndmp node-scope-mode on
```

La modalità ambito-nodo NDMP è abilitata.

2. Abilitare il servizio NDMP su tutti i nodi nel cluster:

L'utilizzo del carattere jolly "*" attiva il servizio NDMP su tutti i nodi contemporaneamente.

Specificare una password per l'autenticazione della connessione NDMP da parte dell'applicazione di backup.

```
cluster1::> system services ndmp on -node *
```

```
Please enter password:
Confirm password:
2 entries were modified.
```

3. Disattivare -clear-text Opzione per la comunicazione sicura della password NDMP:

Utilizzando il carattere jolly "*" disables the -clear-text su tutti i nodi contemporaneamente.

```
cluster1::> system services ndmp modify -node * -clear-text false
```

4. Verificare che il servizio NDMP sia attivato e il -clear-text opzione disattivata:

```
cluster1::> system services ndmp show
```

Node	Enabled	Clear text	User Id
cluster1-1	true	false	root
cluster1-2	true	false	root

2 entries were displayed.

Configurare ONTAP LIF per NDMP con ambito nodo

È necessario identificare una LIF che verrà utilizzata per stabilire una connessione dati e controllare la connessione tra il nodo e l'applicazione di backup. Dopo aver identificato la LIF, è necessario verificare che i criteri di firewall e failover siano impostati per la LIF.



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 ["Gestione del traffico supportato"](#).

ONTAP 9.10.1 o versione successiva

Fasi

1. Identificare la LIF intercluster nei nodi usando il comando `network interface show` il `-service-policy` parametro.

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

2. Assicurarsi che la intercluster LIF includa il `backup-ndmp-control` servizio:

```
network interface service-policy show
```

3. Assicurarsi che il criterio di failover sia impostato correttamente per le LIF dell'intercluster:

- a. Verificare che il criterio di failover per le LIF dell'intercluster sia impostato su `local-only` utilizzando `network interface show -failover` comando.

```
cluster1::> network interface show -failover
```

	Logical	Home	Failover	
Failover				
Vserver	Interface	Node:Port	Policy	Group
-----	-----	-----	-----	

cluster1	IC1	cluster1-1:e0a	local-only	
Default				
			Failover	
Targets:				
			
	IC2	cluster1-2:e0b	local-only	
Default				
			Failover	
Targets:				
			
cluster1-1	cluster1-1_mgmt1	cluster1-1:e0m	local-only	
Default				
			Failover	
Targets:				
			

- b. Se il criterio di failover non è impostato correttamente, modificare il criterio di failover utilizzando `network interface modify` con il `-failover-policy` parametro.

```
cluster1::> network interface modify -vserver cluster1 -lif IC1  
-failover-policy local-only
```

Ulteriori informazioni su `network interface show`, `network interface service-policy`

show e network interface modify nella ["Riferimento al comando ONTAP"](#).

ONTAP 9.9 o versioni precedenti

Fasi

1. Identificare la LIF di intercluster ospitata sui nodi utilizzando network interface show con il -role parametro.

```
cluster1::> network interface show -role intercluster
```

Current Is	Logical	Status	Network	Current
Vserver	Interface	Admin/Oper	Address/Mask	Node
Port	Home			
-----	-----	-----	-----	-----
-----	-----			
cluster1	IC1	up/up	192.0.2.65/24	cluster1-1
e0a	true			
cluster1	IC2	up/up	192.0.2.68/24	cluster1-2
e0b	true			

2. Assicurarsi che il criterio firewall sia abilitato per NDMP sulle LIF dell'intercluster:

- a. Verificare che il criterio firewall sia abilitato per NDMP utilizzando system services firewall policy show comando.

Il seguente comando visualizza il criterio firewall per la LIF dell'intercluster:

```
cluster1::> system services firewall policy show -policy
intercluster
```

Vserver	Policy	Service	Allowed
-----	-----	-----	-----
cluster1	intercluster	dns	-
		http	-
		https	-
		ndmp	0.0.0.0/0, ::/0
		ndmps	-
		ntp	-
		rsh	-
		ssh	-
		telnet	-

9 entries were displayed.

- b. Se il criterio del firewall non è attivato, attivare il criterio del firewall utilizzando system services firewall policy modify con il -service parametro.

Il seguente comando abilita il criterio firewall per la LIF dell'intercluster:

```
cluster1::> system services firewall policy modify -vserver cluster1
-policy intercluster -service ndmp 0.0.0.0/0
```

3. Assicurarsi che il criterio di failover sia impostato correttamente per le LIF dell'intercluster:

- a. Verificare che il criterio di failover per le LIF dell'intercluster sia impostato su local-only utilizzando network interface show -failover comando.

```
cluster1::> network interface show -failover
```

	Logical	Home	Failover	
Failover				
Vserver	Interface	Node:Port	Policy	Group
-----	-----	-----	-----	
cluster1	IC1	cluster1-1:e0a	local-only	
Default				
			Failover	
Targets:			
	IC2	cluster1-2:e0b	local-only	
Default				
			Failover	
Targets:			
cluster1-1	cluster1-1_mgmt1	cluster1-1:e0m	local-only	
Default				
			Failover	
Targets:			

- b. Se il criterio di failover non è impostato correttamente, modificare il criterio di failover utilizzando network interface modify con il -failover-policy parametro.

```
cluster1::> network interface modify -vserver cluster1 -lif IC1
-failover-policy local-only
```

Ulteriori informazioni su network interface show e network interface modify nella ["Riferimento al comando ONTAP"](#).

Configurare le applicazioni di backup per la configurazione ONTAP NDMP

Una volta configurato il cluster per l'accesso NDMP, è necessario raccogliere informazioni dalla configurazione del cluster e configurare il resto del processo di backup nell'applicazione di backup.

Fasi

1. Raccogliere le seguenti informazioni configurate in precedenza in ONTAP:
 - Nome utente e password richiesti dall'applicazione di backup per creare la connessione NDMP
 - Gli indirizzi IP delle LIF di intercluster richieste dall'applicazione di backup per la connessione al cluster
2. In ONTAP, visualizzare gli alias assegnati da ONTAP a ciascun dispositivo utilizzando `storage tape alias show` comando.

Gli alias sono spesso utili nella configurazione dell'applicazione di backup.

```
cluster1::> storage tape show -alias
```

```
Device ID: 2a.0
Device Type: tape drive
Description: Hewlett-Packard LTO-5
```

Node	Alias	Mapping
-----	-----	-----
stsw-3220-4a-4b-02	st2	SN[HU19497WVR]
...		

3. Nell'applicazione di backup, configurare il resto del processo di backup utilizzando la documentazione dell'applicazione di backup.

Al termine

Se si verifica un evento di mobilità dei dati, ad esempio uno spostamento del volume o una migrazione LIF, è necessario essere pronti a reinizializzare le operazioni di backup interrotte.

Informazioni correlate

- ["alias del nastro di archiviazione mostra"](#)

Informazioni sul copyright

Copyright © 2026 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.