Accedere al cluster utilizzando la CLI (solo amministratori del cluster)

ONTAP 9

NetApp
September 12, 2024

Sommario

Accedere al cluster utilizzando la CLI (solo amministratori del cluster)

Accedere al cluster utilizzando la porta seriale

È possibile accedere al cluster direttamente da una console collegata alla porta seriale di un nodo.

Fasi

1. Nella console, premere Invio.

   Il sistema risponde con la richiesta di accesso.

2. Al prompt di accesso, eseguire una delle seguenti operazioni:

Per accedere al cluster con…	Immettere il seguente nome account…
L'account cluster predefinito	**`admin`**
Un account utente amministrativo alternativo	*`username`*

   Il sistema risponde con la richiesta della password.

3. Immettere la password per l'account amministratore o amministrativo, quindi premere Invio.

Accedere al cluster utilizzando SSH

È possibile inviare richieste SSH a un cluster ONTAP per eseguire task amministrativi. SSH è attivato per impostazione predefinita.

Prima di iniziare

- È necessario disporre di un account utente configurato per l'utilizzo `ssh` come metodo di accesso.

  Il `-application` del parametro `security login` commands specifica il metodo di accesso per un account utente. Il `security login` "pagine man" contengono informazioni aggiuntive.

- Se si utilizza un account utente di dominio Active Directory (ad) per accedere al cluster, è necessario configurare un tunnel di autenticazione per il cluster tramite una VM di storage abilitata CIFS e aggiungere anche l'account utente di dominio ad al cluster con `ssh` come metodo di accesso e. `domain` come metodo di autenticazione.

A proposito di questa attività

- È necessario utilizzare un client OpenSSH 5.7 o successivo.
- È supportato solo il protocollo SSH v2; SSH v1 non è supportato.
- ONTAP supporta un massimo di 64 sessioni SSH simultanee per nodo.

  Se la LIF di gestione del cluster risiede nel nodo, condivide questo limite con la LIF di gestione del nodo.

Se la velocità delle connessioni in entrata è superiore a 10 al secondo, il servizio viene temporaneamente disattivato per 60 secondi.

- ONTAP supporta solo gli algoritmi di crittografia AES e 3DES (noti anche come *cifrari*) per SSH.

  AES è supportato con 128, 192 e 256 bit di lunghezza della chiave. 3DES ha una lunghezza della chiave di 56 bit come nel DES originale, ma viene ripetuto tre volte.

- Quando la modalità FIPS è attiva, i client SSH devono negoziare con gli algoritmi a chiave pubblica ECDSA (Elliptic Curve Digital Signature Algorithm) per consentire la connessione.
- Se si desidera accedere all'interfaccia utente di ONTAP da un host Windows, è possibile utilizzare un'utility di terze parti, ad esempio putty.
- Se si utilizza un nome utente Windows ad per accedere a ONTAP, utilizzare le stesse lettere maiuscole o minuscole utilizzate al momento della creazione del nome utente e del nome di dominio ad in ONTAP.

  I nomi utente E i nomi di dominio AD non sono sensibili al maiuscolo/minuscolo. Tuttavia, i nomi utente ONTAP distinguono tra maiuscole e minuscole. La mancata corrispondenza tra il nome utente creato in ONTAP e il nome utente creato in ad comporta un errore di accesso.

Opzioni di autenticazione SSH

- A partire da ONTAP 9.3, è possibile "Abilitare l'autenticazione a più fattori SSH" per gli account dell'amministratore locale.

  Quando l'autenticazione a più fattori SSH è attivata, gli utenti vengono autenticati utilizzando una chiave pubblica e una password.

- A partire da ONTAP 9.4, è possibile "Abilitare l'autenticazione a più fattori SSH" Per utenti remoti LDAP e NIS.
- A partire da ONTAP 9.13.1, è possibile aggiungere facoltativamente la convalida del certificato al processo di autenticazione SSH per migliorare la sicurezza di accesso. A tal fine, "Associare un certificato X.509 alla chiave pubblica" utilizzato da un account. Se si accede utilizzando SSH sia con una chiave pubblica SSH che con un certificato X.509, ONTAP verifica la validità del certificato X.509 prima di autenticarsi con la chiave pubblica SSH. L'accesso SSH viene rifiutato se il certificato è scaduto o revocato e la chiave pubblica SSH viene disattivata automaticamente.
- A partire da ONTAP 9.14.1, gli amministratori di ONTAP possono farlo "Aggiungere l'autenticazione a due fattori Cisco Duo al processo di autenticazione SSH" per migliorare la protezione dell'accesso. Al primo accesso dopo aver attivato l'autenticazione Cisco Duo, gli utenti dovranno registrare un dispositivo per fungere da autenticatore per le sessioni SSH.
- A partire da ONTAP 9.15.1, gli amministratori possono farlo "Configurare l'autorizzazione dinamica" Fornire un'autenticazione adattiva aggiuntiva agli utenti SSH in base al punteggio di attendibilità dell'utente.

Fasi

1. Da un host con accesso alla rete del cluster ONTAP, immettere il `ssh` comando in uno dei seguenti formati:

   - **`ssh` *`username@hostname_or_IP`* `[`*`command`*`]`**
   - **`ssh -l` *`username hostname_or_IP`* `[`*`command`*`]`**

Se si utilizza un account utente di dominio ad, è necessario specificare *`username`* nel formato di *`domainname\\AD_accountname`* (con barre rovesciate doppie dopo il nome di dominio) o. **"***`domainname\AD_accountname`***"** (racchiuso tra virgolette doppie e con una barra rovesciata singola dopo il nome di dominio).

hostname_or_IP È il nome host o l'indirizzo IP della LIF di gestione del cluster o di una LIF di gestione dei nodi. Si consiglia di utilizzare la LIF di gestione del cluster. È possibile utilizzare un indirizzo IPv4 o IPv6.

command Non è richiesto per le sessioni interattive SSH.

Esempi di richieste SSH

I seguenti esempi mostrano come l'account utente "joe" può emettere una richiesta SSH per accedere a un cluster la cui LIF di gestione del cluster è 10.72.137.28:

```
$ ssh joe@10.72.137.28
Password:
cluster1::> cluster show
Node                  Health  Eligibility
--------------------- ------- ------------
node1                 true    true
node2                 true    true
2 entries were displayed.
```

```
$ ssh -l joe 10.72.137.28 cluster show
Password:
Node                  Health  Eligibility
--------------------- ------- ------------
node1                 true    true
node2                 true    true
2 entries were displayed.
```

I seguenti esempi mostrano come l'account utente "john" del dominio "DOMAIN1" può emettere una richiesta SSH per accedere a un cluster la cui LIF di gestione del cluster è 10.72.137.28:

```
$ ssh DOMAIN1\\john@10.72.137.28
Password:
cluster1::> cluster show
Node                  Health  Eligibility
--------------------- ------- ------------
node1                 true    true
node2                 true    true
2 entries were displayed.
```

```
$ ssh -l "DOMAIN1\john" 10.72.137.28 cluster show
Password:
Node                  Health  Eligibility
--------------------- ------- ------------
node1                 true    true
node2                 true    true
2 entries were displayed.
```

L'esempio seguente mostra come l'account utente "joe" può inviare una richiesta SSH MFA per accedere a un cluster la cui LIF di gestione del cluster è 10.72.137.32:

```
$ ssh joe@10.72.137.32
Authenticated with partial success.
Password:
cluster1::> cluster show
Node                  Health  Eligibility
--------------------- ------- ------------
node1                 true    true
node2                 true    true
2 entries were displayed.
```

Informazioni correlate

"Autenticazione amministratore e RBAC"

Sicurezza di accesso SSH

A partire da ONTAP 9.5, è possibile visualizzare le informazioni sugli accessi precedenti, i tentativi di accesso non riusciti e le modifiche ai privilegi dall'ultimo accesso riuscito.

Le informazioni relative alla sicurezza vengono visualizzate quando si effettua l'accesso come utente amministratore SSH. L'utente viene avvisato delle seguenti condizioni:

- L'ultima volta in cui è stato effettuato l'accesso al nome dell'account.
- Il numero di tentativi di accesso non riusciti dall'ultimo accesso riuscito.
- Se il ruolo è cambiato dall'ultimo accesso (ad esempio, se il ruolo dell'account admin è cambiato da "admin" a "backup").
- Se le funzionalità di aggiunta, modifica o eliminazione del ruolo sono state modificate dall'ultimo accesso.

> Se una delle informazioni visualizzate è sospetta, contattare immediatamente il reparto di sicurezza.

Per ottenere queste informazioni al momento dell'accesso, devono essere soddisfatti i seguenti prerequisiti:

- Il provisioning dell'account utente SSH deve essere eseguito in ONTAP.

- È necessario creare l'accesso di sicurezza SSH.
- Il tentativo di accesso deve essere riuscito.

Restrizioni e altre considerazioni per la sicurezza dell'accesso SSH

Le seguenti restrizioni e considerazioni si applicano alle informazioni di sicurezza per l'accesso SSH:

- Le informazioni sono disponibili solo per gli accessi basati su SSH.
- Per gli account admin basati su gruppo, come ad esempio gli account LDAP/NIS e ad, gli utenti possono visualizzare le informazioni di accesso SSH se il gruppo di cui fanno parte è configurato come account admin in ONTAP.

  Tuttavia, gli avvisi relativi alle modifiche al ruolo dell'account utente non possono essere visualizzati per questi utenti. Inoltre, gli utenti appartenenti a un gruppo ad che è stato fornito come account admin in ONTAP non possono visualizzare il numero di tentativi di accesso non riusciti che si sono verificati dall'ultimo accesso.

- Le informazioni conservate per un utente vengono eliminate quando l'account utente viene cancellato da ONTAP.
- Le informazioni non vengono visualizzate per le connessioni ad applicazioni diverse da SSH.

Esempi di informazioni di sicurezza per l'accesso SSH

I seguenti esempi mostrano il tipo di informazioni visualizzate dopo l'accesso.

- Questo messaggio viene visualizzato dopo ogni accesso riuscito:

  ```
  Last Login : 7/19/2018 06:11:32
  ```

- Questi messaggi vengono visualizzati se si sono verificati tentativi di accesso non riusciti dall'ultimo accesso riuscito:

  ```
  Last Login : 4/12/2018 08:21:26
  Unsuccessful login attempts since last login - 5
  ```

- Questi messaggi vengono visualizzati se si sono verificati tentativi di accesso non riusciti e i privilegi sono stati modificati dall'ultimo accesso riuscito:

  ```
  Last Login : 8/22/2018 20:08:21
  Unsuccessful login attempts since last login - 3
  Your privileges have changed since last login
  ```

Abilitare l'accesso Telnet o RSH al cluster

Come procedura consigliata per la protezione, Telnet e RSH sono disattivati per

impostazione predefinita. Per consentire al cluster di accettare le richieste Telnet o RSH, è necessario abilitare il servizio nella politica del servizio di gestione predefinita.

Con il passare del tempo, il modo in cui ONTAP gestisce il tipo di traffico supportato dalle LIF è cambiato.

- Le versioni ONTAP 9.5 e precedenti utilizzano i ruoli LIF e i servizi firewall
- Le versioni ONTAP 9.6 e successive utilizzano i criteri di servizio LIF
  - La versione ONTAP 9.5 ha introdotto le politiche di servizio LIF
  - ONTAP 9.6 ha sostituito i ruoli LIF con le politiche di servizio LIF
  - ONTAP 9.10,1 ha sostituito i servizi firewall con le policy di servizio LIF

Il metodo configurato dipende dal rilascio di ONTAP in uso.

Ulteriori informazioni su:

- Criteri firewall, fare riferimento a. "Comando: Firewall-policy-show"
- Ruoli LIF, fare riferimento a. "Ruoli LIF (ONTAP 9,5 e versioni precedenti)"
- Policy di servizio LIF, fare riferimento a. "LIF e policy di servizio (ONTAP 9,6 e versioni successive)"

Telnet e RSH non sono protocolli sicuri, è consigliabile utilizzare SSH per accedere al cluster. SSH offre una shell remota sicura e una sessione di rete interattiva. Per ulteriori informazioni, fare riferimento a. "Accedere al cluster utilizzando SSH"

ONTAP 9,6 o versione successiva

A proposito di questa attività

- RSH non è un protocollo sicuro.

  Si consiglia di utilizzare SSH per accedere al cluster. SSH offre una shell remota sicura e una sessione di rete interattiva.

- ONTAP supporta un massimo di 50 sessioni RSH simultanee per nodo.

  Se la LIF di gestione del cluster risiede nel nodo, condivide questo limite con la LIF di gestione del nodo.

  Se la velocità delle connessioni in entrata è superiore a 10 al secondo, il servizio viene temporaneamente disattivato per 60 secondi.

- I comandi RSH richiedono privilegi avanzati.

Fasi

1. Verificare che il protocollo di protezione RSH o Telnet sia attivato:

   ```
   security protocol show
   ```

   a. Se il protocollo di protezione RSH o Telnet è attivato, passare alla fase successiva.
   b. Se il protocollo di protezione RSH o Telnet non è attivato, utilizzare il seguente comando per attivarlo:

      ```
      security protocol modify -application <rsh/telnet> -enabled true
      ```

2. Conferma che il `management-rsh-server` servizio OR `management-telnet-server` è presente nella LIF di gestione:

   ```
   network interface show -services management-rsh-server
   ```

   oppure

   ```
   network interface show -services management-telnet-server
   ```

   a. Se il `management-rsh-server` servizio o `management-telnet-server` è presente, passare alla fase successiva.
   b. Se il `management-rsh-server` servizio o `management-telnet-server` non esiste, utilizzare il comando seguente per aggiungerlo:

      ```
      network interface service-policy add-service -vserver cluster1 -policy
      default-management -service management-rsh-server
      ```

```
network interface service-policy add-service -vserver cluster1 -policy
default-management -service management-telnet-server
```

ONTAP 9.5 o versioni precedenti

A proposito di questa attività

ONTAP non consente di modificare i criteri firewall predefiniti, ma è possibile creare un nuovo criterio

clonando il `mgmt` criterio firewall di gestione predefinito e quindi attivando Telnet o RSH nel nuovo criterio.

Fasi

1. Accedere alla modalità avanzata dei privilegi:

   ```
   set advanced
   ```

2. Abilitare un protocollo di sicurezza (RSH o Telnet):

   ```
   security protocol modify -application security_protocol -enabled true
   ```

3. Creare un nuovo criterio firewall di gestione basato sul `mgmt` criterio firewall di gestione:

   ```
   system services firewall policy clone -policy mgmt -destination-policy
   policy-name
   ```

4. Abilitare Telnet o RSH nella nuova policy del firewall di gestione:

   ```
   system services firewall policy create -policy policy-name -service
   security_protocol -action allow -ip-list ip_address/netmask
   ```

   Per consentire tutti gli indirizzi IP, occorre specificare `-ip-list 0.0.0.0/0`

5. Associare la nuova policy alla LIF di gestione del cluster:

   ```
   network interface modify -vserver cluster_management_LIF -lif cluster_mgmt
   -firewall-policy policy-name
   ```

Accedere al cluster utilizzando Telnet

È possibile inviare richieste Telnet al cluster per eseguire attività amministrative. Telnet è disattivato per impostazione predefinita.

Con il passare del tempo, il modo in cui ONTAP gestisce il tipo di traffico supportato dalle LIF è cambiato.

- Le versioni ONTAP 9.5 e precedenti utilizzano i ruoli LIF e i servizi firewall
- Le versioni ONTAP 9.6 e successive utilizzano i criteri di servizio LIF
  - La versione ONTAP 9.5 ha introdotto le politiche di servizio LIF
  - ONTAP 9.6 ha sostituito i ruoli LIF con le politiche di servizio LIF
  - ONTAP 9.10,1 ha sostituito i servizi firewall con le policy di servizio LIF

Il metodo configurato dipende dal rilascio di ONTAP in uso.

Ulteriori informazioni su:

- Criteri firewall, fare riferimento a. "Comando: Firewall-policy-show"
- Ruoli LIF, fare riferimento a. "Ruoli LIF (ONTAP 9,5 e versioni precedenti)"
- Policy di servizio LIF, fare riferimento a. "LIF e policy di servizio (ONTAP 9,6 e versioni successive)"

Telnet e RSH non sono protocolli sicuri, è consigliabile utilizzare SSH per accedere al cluster. SSH offre una shell remota sicura e una sessione di rete interattiva. Per ulteriori informazioni, fare riferimento a. "Accedere al cluster utilizzando SSH"

ONTAP 9,6 o versione successiva

Prima di iniziare

Prima di poter utilizzare Telnet per accedere al cluster, è necessario soddisfare le seguenti condizioni:

- È necessario disporre di un account utente locale del cluster configurato per utilizzare Telnet come metodo di accesso.

  Il `-application` del parametro `security login` commands specifica il metodo di accesso per un account utente. Per ulteriori informazioni, consultare `security login` pagine man.

A proposito di questa attività

- Telnet non è un protocollo sicuro.

  Si consiglia di utilizzare SSH per accedere al cluster. SSH offre una shell remota sicura e una sessione di rete interattiva.

- ONTAP supporta un massimo di 50 sessioni Telnet simultanee per nodo.

  Se la LIF di gestione del cluster risiede nel nodo, condivide questo limite con la LIF di gestione del nodo.

  Se la velocità delle connessioni in entrata è superiore a 10 al secondo, il servizio viene temporaneamente disattivato per 60 secondi.

- Se si desidera accedere all'interfaccia utente di ONTAP da un host Windows, è possibile utilizzare un'utility di terze parti, ad esempio putty.
- I comandi RSH richiedono privilegi avanzati.

Fasi

1. Verificare che il protocollo di protezione Telnet sia attivato:

   ```
   security protocol show
   ```

   a. Se il protocollo di protezione Telnet è attivato, passare alla fase successiva.
   b. Se il protocollo di protezione Telnet non è attivato, utilizzare il comando seguente per attivarlo:

      ```
      security protocol modify -application telnet -enabled true
      ```

2. Confermare l' `management-telnet-server` esistenza del servizio nelle LIF di gestione:

   ```
   network interface show -services management-telnet-server
   ```

   a. Se il `management-telnet-server` servizio è presente, passare alla fase successiva.
   b. Se il `management-telnet-server` servizio non esiste, utilizzare il seguente comando per aggiungerlo:

      ```
      network interface service-policy add-service -vserver cluster1 -policy
      default-management -service management-telnet-server
      ```

Esempio di richiesta Telnet

L'esempio seguente mostra come l'utente "joe", configurato con accesso Telnet, può inviare una richiesta Telnet per accedere a un cluster la cui LIF di gestione del cluster è 10.72.137.28:

```
admin_host$ telnet 10.72.137.28
Data ONTAP
login: joe
Password:
cluster1::>
```

ONTAP 9.5 o versioni precedenti

Prima di iniziare

Prima di poter utilizzare Telnet per accedere al cluster, è necessario soddisfare le seguenti condizioni:

- È necessario disporre di un account utente locale del cluster configurato per utilizzare Telnet come metodo di accesso.

  Il `-application` parametro dei comandi di accesso di protezione specifica il metodo di accesso per un account utente. Per ulteriori informazioni, vedere le pagine man per l'accesso di sicurezza.

- Telnet deve essere già attivato nel criterio del firewall di gestione utilizzato dalle LIF di gestione del cluster o dei nodi, in modo che le richieste Telnet possano passare attraverso il firewall.

  Per impostazione predefinita, Telnet è disattivato. La policy firewall dei servizi di sistema mostra il comando con il parametro `-service telnet `visualizza se Telnet è stato abilitato in una policy firewall. Per ulteriori informazioni, vedere le pagine man dei criteri firewall dei servizi di sistema.

- Se si utilizzano connessioni IPv6, IPv6 deve essere già configurato e abilitato sul cluster e i criteri firewall devono essere già configurati con gli indirizzi IPv6.

  Il comando delle opzioni di rete IPv6 show visualizza se IPv6 è abilitato. Il comando System Services firewall policy show visualizza i criteri firewall.

A proposito di questa attività

- Telnet non è un protocollo sicuro.

  Si consiglia di utilizzare SSH per accedere al cluster. SSH offre una shell remota sicura e una sessione di rete interattiva.

- ONTAP supporta un massimo di 50 sessioni Telnet simultanee per nodo.

  Se la LIF di gestione del cluster risiede nel nodo, condivide questo limite con la LIF di gestione del nodo.

  Se la velocità delle connessioni in entrata è superiore a 10 al secondo, il servizio viene temporaneamente disattivato per 60 secondi.

- Se si desidera accedere all'interfaccia utente di ONTAP da un host Windows, è possibile utilizzare un'utility di terze parti, ad esempio putty.

Fasi

1. Da un host di amministrazione, immettere il seguente comando:

```
telnet hostname_or_IP
```

`hostname_or_IP` È il nome dell'host o l'indirizzo IP della LIF di gestione cluster o di una LIF di gestione nodi. Si consiglia di utilizzare la LIF di gestione del cluster. È possibile utilizzare un indirizzo IPv4 o IPv6.

Esempio di richiesta Telnet

Nell'esempio seguente viene illustrato in che modo l'utente "joe", che è stato configurato con l'accesso Telnet, può inviare una richiesta Telnet per accedere a un cluster la cui LIF di gestione cluster è 10.72.137.28:

```
admin_host$ telnet 10.72.137.28

Data ONTAP
login: joe
Password:

cluster1::>
```

Accedere al cluster utilizzando RSH

È possibile inviare richieste RSH al cluster per eseguire attività amministrative. RSH non è un protocollo sicuro ed è disattivato per impostazione predefinita.

Con il passare del tempo, il modo in cui ONTAP gestisce il tipo di traffico supportato dalle LIF è cambiato.

- Le versioni ONTAP 9.5 e precedenti utilizzano i ruoli LIF e i servizi firewall
- Le versioni ONTAP 9.6 e successive utilizzano i criteri di servizio LIF
  - La versione ONTAP 9.5 ha introdotto le politiche di servizio LIF
  - ONTAP 9.6 ha sostituito i ruoli LIF con le politiche di servizio LIF
  - ONTAP 9.10,1 ha sostituito i servizi firewall con le policy di servizio LIF

Il metodo configurato dipende dal rilascio di ONTAP in uso.

Ulteriori informazioni su:

- Criteri firewall, fare riferimento a. "Comando: Firewall-policy-show"
- Ruoli LIF, fare riferimento a. "Ruoli LIF (ONTAP 9,5 e versioni precedenti)"
- Policy di servizio LIF, fare riferimento a. "LIF e policy di servizio (ONTAP 9,6 e versioni successive)"

Telnet e RSH non sono protocolli sicuri, è consigliabile utilizzare SSH per accedere al cluster. SSH offre una shell remota sicura e una sessione di rete interattiva. Per ulteriori informazioni, fare riferimento a. "Accedere al cluster utilizzando SSH"

ONTAP 9,6 o versione successiva

Prima di iniziare

Prima di poter utilizzare RSH per accedere al cluster, è necessario soddisfare le seguenti condizioni:

- È necessario disporre di un account utente locale del cluster configurato per utilizzare RSH come metodo di accesso.

  Il `-application` del parametro `security login` commands specifica il metodo di accesso per un account utente. Per ulteriori informazioni, consultare `security login` pagine man.

A proposito di questa attività

- RSH non è un protocollo sicuro.

  Si consiglia di utilizzare SSH per accedere al cluster. SSH offre una shell remota sicura e una sessione di rete interattiva.

- ONTAP supporta un massimo di 50 sessioni RSH simultanee per nodo.

  Se la LIF di gestione del cluster risiede nel nodo, condivide questo limite con la LIF di gestione del nodo.

  Se la velocità delle connessioni in entrata è superiore a 10 al secondo, il servizio viene temporaneamente disattivato per 60 secondi.

- I comandi RSH richiedono privilegi avanzati.

Fasi

1. Verificare che il protocollo di protezione RSH sia attivato:

   ```
   security protocol show
   ```

   a. Se il protocollo di protezione RSH è attivato, passare alla fase successiva.
   b. Se il protocollo di protezione RSH non è attivato, utilizzare il comando seguente per attivarlo:

      ```
      security protocol modify -application rsh -enabled true
      ```

2. Confermare l' `management-rsh-server` esistenza del servizio nelle LIF di gestione:

   ```
   network interface show -services management-rsh-server
   ```

   a. Se il `management-rsh-server` servizio è presente, passare alla fase successiva.
   b. Se il `management-rsh-server` servizio non esiste, utilizzare il seguente comando per aggiungerlo:

      ```
      network interface service-policy add-service -vserver cluster1 -policy
      default-management -service management-rsh-server
      ```

Esempio di richiesta RSH

L'esempio seguente mostra come l'utente "joe", che è stato configurato con accesso RSH, può emettere una richiesta RSH per eseguire `cluster show` comando:

```
admin_host$ rsh 10.72.137.28 -l joe:password cluster show

Node                  Health  Eligibility
--------------------- ------- ------------
node1                 true    true
node2                 true    true
2 entries were displayed.

admin_host$
```

ONTAP 9.5 o versioni precedenti

Prima di iniziare

Prima di poter utilizzare RSH per accedere al cluster, è necessario soddisfare le seguenti condizioni:

- È necessario disporre di un account utente locale del cluster configurato per utilizzare RSH come metodo di accesso.

  Il parametro -application dei comandi di accesso di protezione specifica il metodo di accesso per un account utente. Per ulteriori informazioni, vedere le pagine man per l'accesso di sicurezza.

- RSH deve essere già abilitato nella policy del firewall di gestione utilizzata dalle LIF di gestione del cluster o dei nodi, in modo che le richieste RSH possano passare attraverso il firewall.

  Per impostazione predefinita, RSH è disattivato. Il criterio firewall dei servizi di sistema mostra il comando con il `-service rsh` parametro visualizza se RSH è stato attivato in un criterio firewall. Per ulteriori informazioni, vedere le `system services firewall policy` pagine man.

- Se si utilizzano connessioni IPv6, IPv6 deve essere già configurato e abilitato sul cluster e i criteri firewall devono essere già configurati con gli indirizzi IPv6.

  Il `network options ipv6 show` comando visualizza se IPv6 è abilitato. Il `system services firewall policy show` comando visualizza i criteri del firewall.

A proposito di questa attività

- RSH non è un protocollo sicuro.

  Si consiglia di utilizzare SSH per accedere al cluster. SSH offre una shell remota sicura e una sessione di rete interattiva.

- ONTAP supporta un massimo di 50 sessioni RSH simultanee per nodo.

  Se la LIF di gestione del cluster risiede nel nodo, condivide questo limite con la LIF di gestione del nodo.

  Se la velocità delle connessioni in entrata è superiore a 10 al secondo, il servizio viene temporaneamente disattivato per 60 secondi.

Fasi

1. Da un host di amministrazione, immettere il seguente comando:

```
rsh hostname_or_IP -l username:passwordcommand
```

`hostname_or_IP` È il nome dell'host o l'indirizzo IP della LIF di gestione cluster o di una LIF di gestione nodi. Si consiglia di utilizzare la LIF di gestione del cluster. È possibile utilizzare un indirizzo IPv4 o IPv6.

`command` È il comando che si desidera eseguire su RSH.

Esempio di richiesta RSH

Nell'esempio seguente viene illustrato come l'utente "joe", che è stato configurato con l'accesso RSH, può emettere una richiesta RSH per eseguire il comando cluster show:

```
admin_host$ rsh 10.72.137.28 -l joe:password cluster show

Node  Health Eligibility
----  ------ -----------
node1 true   true
node2 true   true

2 entries were displayed.

admin_host
```