



Gestire le connessioni di supporto

HCI

NetApp
October 11, 2024

Sommario

- Gestire le connessioni di supporto 1
 - Avviare una sessione remota di NetApp Support 1
 - Gestire la funzionalità SSH sul nodo di gestione 1

Gestire le connessioni di supporto

Avviare una sessione remota di NetApp Support

Se hai bisogno di supporto tecnico per il tuo sistema NetApp HCI, il supporto NetApp può connetterti in remoto con il tuo sistema. Per avviare una sessione e ottenere l'accesso remoto, il supporto NetApp può aprire una connessione Secure Shell (SSH) inversa al proprio ambiente.

A proposito di questa attività

Con il supporto NetApp è possibile aprire una porta TCP per una connessione a tunnel inverso SSH. Questa connessione consente al supporto NetApp di accedere al nodo di gestione. Se il nodo di gestione si trova dietro un server proxy, nel file `sshd.config` sono necessarie le seguenti porte TCP:

Porta TCP	Descrizione	Direzione di connessione
443	Chiamate API/HTTPS per l'inoltro inverso delle porte all'interfaccia utente Web tramite tunnel di supporto aperto	Nodo di gestione ai nodi di storage
22	Accesso SSH	Nodo di gestione per nodi di storage o da nodi di storage a nodi di gestione



Per impostazione predefinita, la capacità di accesso remoto è attivata nel nodo di gestione. Per disattivare la funzionalità di accesso remoto, vedere ["Gestire la funzionalità SSH sul nodo di gestione"](#). Se necessario, è possibile abilitare nuovamente la funzionalità di accesso remoto.

Fasi

- Accedere al nodo di gestione e aprire una sessione terminale.
- Quando richiesto, immettere quanto segue:

```
rst -r sfsupport.solidfire.com -u element -p <port_number>
```

- Per chiudere il tunnel di supporto remoto, immettere quanto segue:

```
rst --killall
```

Trova ulteriori informazioni

- ["Plug-in NetApp Element per server vCenter"](#)
- ["Pagina delle risorse NetApp HCI"](#)

Gestire la funzionalità SSH sul nodo di gestione

È possibile disattivare, riattivare o determinare lo stato della funzionalità SSH sul nodo di gestione (mNode) utilizzando l'API REST. La capacità SSH fornita da ["Accesso alla"](#)

[sessione del NetApp Support Remote Support Tunnel \(RST\)](#)" è attivata sul nodo di gestione per impostazione predefinita.

A partire da Management Services 2.20.69, è possibile attivare e disattivare la funzionalità SSH sul nodo di gestione utilizzando l'interfaccia utente di NetApp Hybrid Cloud Control.

Di cosa hai bisogno

- **NetApp Hybrid Cloud Control Permissions:** Hai le autorizzazioni di amministratore.
- **Cluster Administrator permissions** (autorizzazioni amministratore cluster): Si dispone delle autorizzazioni di amministratore per il cluster di storage.
- **Software Element:** Il cluster esegue il software NetApp Element 11.3 o versione successiva.
- **Nodo di gestione:** È stato distribuito un nodo di gestione che esegue la versione 11,3 o successiva.
- **Aggiornamenti dei servizi di gestione:**
 - Per utilizzare l'interfaccia utente di controllo cloud ibrido NetApp, hai aggiornato ["bundle di servizi di gestione"](#) alla versione 2.20.69 o successiva del.
 - Per utilizzare l'interfaccia utente delle API REST, è stata aggiornata la ["bundle di servizi di gestione"](#) alla versione 2,17.

Opzioni

- [Disattivare o attivare la funzionalità SSH sul nodo di gestione utilizzando l'interfaccia utente di NetApp Hybrid Cloud Control](#)

È possibile eseguire una delle seguenti operazioni dopo di che ["autenticare"](#):

- [Disattivare o attivare la funzionalità SSH sul nodo di gestione utilizzando le API](#)
- [Determinare lo stato della funzionalità SSH sul nodo di gestione utilizzando le API](#)

Disattivare o attivare la funzionalità SSH sul nodo di gestione utilizzando l'interfaccia utente di NetApp Hybrid Cloud Control

È possibile disattivare o riattivare la funzionalità SSH sul nodo di gestione. La capacità SSH che fornisce ["Accesso alla sessione del NetApp Support Remote Support Tunnel \(RST\)"](#) è disattivata per impostazione predefinita nei nodi di gestione che eseguono servizi di gestione 2,18 o successivi. La disattivazione di SSH non interrompe o disconnette le sessioni client SSH esistenti al nodo di gestione. Se si disattiva SSH e si sceglie di riattivarlo in un secondo momento, è possibile farlo utilizzando l'interfaccia utente di NetApp Hybrid Cloud Control.



Per abilitare o disabilitare l'accesso al supporto utilizzando SSH per un cluster di archiviazione, è necessario utilizzare ["Pagina delle impostazioni del cluster dell'interfaccia utente Element"](#) .

Fasi

1. Dalla dashboard, selezionare il menu delle opzioni in alto a destra e selezionare **Configura**.
2. Nella schermata **Support Access for Management Node** (accesso supporto per nodo di gestione), attivare lo switch per attivare il nodo di gestione SSH.
3. Una volta completata la risoluzione dei problemi, nella schermata **Support Access for Management Node** (accesso supporto per nodo di gestione), impostare lo switch su **Disable Management Node SSH** (Disattiva SSH nodo di gestione).

Disattivare o attivare la funzionalità SSH sul nodo di gestione utilizzando le API

È possibile disattivare o riattivare la funzionalità SSH sul nodo di gestione. La capacità SSH fornita da "Accesso alla sessione del NetApp Support Remote Support Tunnel (RST)" è attivata sul nodo di gestione per impostazione predefinita. La disattivazione di SSH non interrompe o disconnette le sessioni client SSH esistenti al nodo di gestione. Se si disattiva SSH e si sceglie di riattivarlo in un secondo momento, è possibile utilizzare la stessa API.

Comando API

Per i servizi di gestione 2.18 o versioni successive:

```
curl -k -X PUT
"https://<<ManagementNodeIP>/mnode/2/settings/ssh?enabled=<false/true>" -H
"accept: application/json" -H "Authorization: Bearer ${TOKEN}"
```

Per i servizi di gestione 2.17 o precedenti:

```
curl -X PUT
"https://<ManagementNodeIP>/mnode/settings/ssh?enabled=<false/true>" -H
"accept: application/json" -H "Authorization: Bearer ${TOKEN}"
```



È possibile trovare il bearer `${TOKEN}` utilizzato dal comando API quando si "autorizzare". Il bearer `${TOKEN}` è nella risposta curl.

FASI DELL'INTERFACCIA UTENTE API REST

1. Accedere all'interfaccia utente API REST per il servizio API del nodo di gestione immettendo l'indirizzo IP del nodo di gestione seguito da `/mnode/`:

```
https://<ManagementNodeIP>/mnode/
```

2. Selezionare **autorizzare** e completare le seguenti operazioni:
 - a. Inserire il nome utente e la password del cluster.
 - b. Immettere l'ID client come `mnode-client`.
 - c. Selezionare **autorizzare** per avviare una sessione.
 - d. Chiudere la finestra.
3. Dall'interfaccia utente dell'API REST, selezionare **PUT /settings/ssh**.
 - a. Selezionare **Provalo**.
 - b. Impostare il parametro **Enabled** su `false` per disattivare SSH o `true` per riattivare la funzionalità SSH precedentemente disattivata.
 - c. Selezionare **Esegui**.

Determinare lo stato della funzionalità SSH sul nodo di gestione utilizzando le API

È possibile determinare se la funzionalità SSH è attivata sul nodo di gestione utilizzando un'API di servizio del nodo di gestione. SSH è attivato per impostazione predefinita sul nodo di gestione.

Comando API

Per i servizi di gestione 2.18 o versioni successive:

```
curl -k -X PUT
"https://<ManagementNodeIP>/mnode/2/settings/ssh?enabled=<false/true>" -H
"accept: application/json" -H "Authorization: Bearer ${TOKEN}"
```

Per i servizi di gestione 2.17 o precedenti:

```
curl -X PUT
"https://<ManagementNodeIP>/mnode/settings/ssh?enabled=<false/true>" -H
"accept: application/json" -H "Authorization: Bearer ${TOKEN}"
```



È possibile trovare il bearer `${TOKEN}` utilizzato dal comando API quando si ["autorizzare"](#). Il bearer `${TOKEN}` è nella risposta curl.

FASI DELL'INTERFACCIA UTENTE API REST

1. Accedere all'interfaccia utente API REST per il servizio API del nodo di gestione immettendo l'indirizzo IP del nodo di gestione seguito da `/mnode/`:

```
https://<ManagementNodeIP>/mnode/
```

2. Selezionare **autorizzare** e completare le seguenti operazioni:
 - a. Inserire il nome utente e la password del cluster.
 - b. Immettere l'ID client come `mnode-client`.
 - c. Selezionare **autorizzare** per avviare una sessione.
 - d. Chiudere la finestra.
3. Dall'interfaccia utente dell'API REST, selezionare **GET /settings/ssh**.
 - a. Selezionare **Provalo**.
 - b. Selezionare **Esegui**.

Trova ulteriori informazioni

- ["Plug-in NetApp Element per server vCenter"](#)
- ["Pagina delle risorse NetApp HCI"](#)

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.