Gestire le connessioni di supporto

Element Software

NetApp
October 01, 2024

Sommario

Gestire le connessioni di supporto

Accesso ai nodi storage tramite SSH per troubleshooting di base

A partire da Element 12,5, è possibile utilizzare l'account di sistema sfreadonly sui nodi di storage per il troubleshooting di base. È inoltre possibile attivare e aprire l'accesso remoto al tunnel di supporto per il supporto NetApp per la risoluzione avanzata dei problemi.

L'account di sistema sfreadonly consente l'accesso per eseguire i comandi di base per la risoluzione dei problemi di rete e di sistema Linux, tra cui `ping`.

> Se non richiesto dall'assistenza NetApp, eventuali modifiche al sistema non sono supportate, annullano il contratto di assistenza e potrebbero causare instabilità o inaccessibilità dei dati.

Prima di iniziare

- **Autorizzazioni di scrittura**: Verificare di disporre delle autorizzazioni di scrittura per la directory di lavoro corrente.
- **(opzionale) genera la tua coppia di chiavi**: Esegui `ssh-keygen` da Windows 10, MacOS o Linux. Si tratta di un'azione singola per creare una coppia di chiavi utente e può essere riutilizzata per future sessioni di risoluzione dei problemi. È possibile utilizzare i certificati associati agli account dipendenti, che funzionerebbero anche in questo modello.
- **Abilitare la funzionalità SSH sul nodo di gestione**: Per abilitare la funzionalità di accesso remoto nella modalità di gestione, vedere "in questo argomento". Per i servizi di gestione 2.18 e versioni successive, la funzionalità di accesso remoto è disattivata per impostazione predefinita nel nodo di gestione.
- **Abilitare la funzionalità SSH sul cluster di archiviazione**: Per abilitare la funzionalità di accesso remoto sui nodi del cluster di archiviazione, vedere "in questo argomento".
- **Configurazione firewall**: 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

Opzioni di risoluzione dei problemi

- Eseguire il troubleshooting di un nodo del cluster
- Eseguire il troubleshooting di un nodo del cluster con il supporto NetApp
- Eseguire il troubleshooting di un nodo che non fa parte del cluster

Eseguire il troubleshooting di un nodo del cluster

È possibile eseguire la risoluzione dei problemi di base utilizzando l'account di sistema sfreadonly:

Fasi

1. SSH al nodo di gestione utilizzando le credenziali di accesso dell'account selezionate durante l'installazione della VM del nodo di gestione.
2. Sul nodo di gestione, andare a `/sf/bin`.
3. Individuare lo script appropriato per il sistema:
   - SignSshKeys.ps1
   - SignSshKeys.py
   - SignSshKeys.sh

   SignSshKeys.ps1 dipende da PowerShell 7 o versione successiva e SignSshKeys.py dipende da Python 3.6.0 o versione successiva e da "modulo richieste" .

   `SignSshKeys`Lo script scrive i `user` file , , `user.pub` e `user-cert.pub` nella directory di lavoro corrente, che vengono successivamente utilizzati dal `ssh` comando. Tuttavia, quando un file di chiave pubblica viene fornito allo script, solo un `<public_key>` file (`<public_key>`sostituito dal prefisso del file di chiave pubblica passato nello script) viene scritto nella directory.

4. Eseguire lo script sul nodo di gestione per generare il portachiavi SSH. Lo script abilita l'accesso SSH utilizzando l'account di sistema sfreadonly in tutti i nodi del cluster.

```
SignSshKeys --ip [ip address] --user [username] --duration [hours]
--publickey [public key path]
```

   a. Sostituire il valore tra parentesi [ ] (comprese le parentesi) per ciascuno dei seguenti parametri:

      È possibile utilizzare il parametro forma abbreviata o completa.

      - **--ip | -i [indirizzo ip]**: Indirizzo IP del nodo di destinazione per l'esecuzione dell'API.
      - **--user | -u [username]**: Utente cluster utilizzato per eseguire la chiamata API.
      - **(opzionale) --duration | -d [ore]**: La durata per la quale una chiave firmata deve rimanere valida come numero intero in ore. L'impostazione predefinita è 24 ore.
      - **(opzionale) --chiave pubblica | -k [percorso chiave pubblica]**: Il percorso verso una chiave pubblica, se l'utente sceglie di fornirne una.

   b. Confrontare l'input con il seguente comando di esempio. In questo esempio, `10.116.139.195` è l'IP del nodo di archiviazione, `admin` è il nome utente del cluster e la durata della validità della chiave è di due ore:

```
sh /sf/bin/SignSshKeys.sh --ip 10.116.139.195 --user admin --duration
2
```

c. Eseguire il comando.

5. SSH agli IP del nodo:

```
ssh -i user sfreadonly@[node_ip]
```

Sarà possibile eseguire comandi di base per la risoluzione dei problemi di rete e di sistema Linux, come `ping`, e altri comandi di sola lettura.

6. (Facoltativo) disattivare "funzionalità di accesso remoto" nuovamente al termine della risoluzione dei problemi.

> SSH rimane attivato sul nodo di gestione se non viene disattivato. La configurazione abilitata SSH persiste sul nodo di gestione tramite aggiornamenti e aggiornamenti fino a quando non viene disattivata manualmente.

Eseguire il troubleshooting di un nodo del cluster con il supporto NetApp

Il supporto NetApp può eseguire un troubleshooting avanzato con un account di sistema che consente a un tecnico di eseguire una diagnostica più approfondita degli elementi.

Fasi

1. SSH al nodo di gestione utilizzando le credenziali di accesso dell'account selezionate durante l'installazione della VM del nodo di gestione.
2. Eseguire il comando rst con il numero di porta inviato dall'assistenza NetApp per aprire il tunnel di supporto:

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

   L'assistenza NetApp effettuerà l'accesso al nodo di gestione utilizzando il tunnel di supporto.

3. Sul nodo di gestione, andare a `/sf/bin`.
4. Individuare lo script appropriato per il sistema:
   - SignSshKeys.ps1
   - SignSshKeys.py
   - SignSshKeys.sh

SignSshKeys.ps1 dipende da PowerShell 7 o versione successiva e SignSshKeys.py dipende da Python 3.6.0 o versione successiva e da "modulo richieste" .

`SignSshKeys`Lo script scrive i `user` file , , `user.pub` e `user-cert.pub` nella directory di lavoro corrente, che vengono successivamente utilizzati dal `ssh` comando. Tuttavia, quando un file di chiave pubblica viene fornito allo script, solo un `<public_key>` file (`<public_key>`sostituito dal prefisso del file di chiave pubblica passato nello script) viene scritto nella directory.

5. Eseguire lo script per generare il portachiavi SSH con il `--sfadmin` flag. Lo script abilita SSH in tutti i nodi.

```
SignSshKeys --ip [ip address] --user [username] --duration [hours]
--sfadmin
```

Per SSH come `--sfadmin` nodo cluster, è necessario generare il portachiavi SSH utilizzando un `--user` con `supportAdmin` accesso sul cluster.

Per configurare l' `supportAdmin`accesso per gli account degli amministratori del cluster, è possibile utilizzare l'interfaccia utente o le API di Element:

- "Configurare l'accesso "supportAdmin" utilizzando l'interfaccia utente di Element"
- Configurare `supportAdmin` l'accesso utilizzando le API e aggiungendo `"supportAdmin"` come `"access"` tipo nella richiesta API:
  - "Configurare l'accesso "supportAdmin" per un nuovo account"
  - "Configurare l'accesso "supportAdmin" per un account esistente"

    Per ottenere il `clusterAdminID`, è possibile utilizzare l'"ListClusterAdmins"API.

Per aggiungere `supportAdmin` l'accesso è necessario disporre di un Privileges dell'amministratore del cluster o dell'amministratore.

a. Sostituire il valore tra parentesi [ ] (comprese le parentesi) per ciascuno dei seguenti parametri:

   È possibile utilizzare il parametro forma abbreviata o completa.

   - **--ip | -i [indirizzo ip]**: Indirizzo IP del nodo di destinazione per l'esecuzione dell'API.
   - **--user | -u [username]**: Utente cluster utilizzato per eseguire la chiamata API.
   - **(opzionale) --duration | -d [ore]**: La durata per la quale una chiave firmata deve rimanere valida come numero intero in ore. L'impostazione predefinita è 24 ore.

b. Confrontare l'input con il seguente comando di esempio. In questo esempio, `192.168.0.1` è l'IP del

nodo storage, `admin` è il nome utente del cluster, la durata di validità della chiave è di due ore e `--sfadmin` consente l'accesso al nodo supporto NetApp per il troubleshooting:

```
sh /sf/bin/SignSshKeys.sh --ip 192.168.0.1 --user admin --duration 2
--sfadmin
```

c. Eseguire il comando.

6. SSH agli IP del nodo:

```
ssh -i user sfadmin@[node_ip]
```

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

```
rst --killall
```

8. (Facoltativo) disattivare "funzionalità di accesso remoto" nuovamente al termine della risoluzione dei problemi.

> SSH rimane attivato sul nodo di gestione se non viene disattivato. La configurazione abilitata SSH persiste sul nodo di gestione tramite aggiornamenti e aggiornamenti fino a quando non viene disattivata manualmente.

Eseguire il troubleshooting di un nodo che non fa parte del cluster

È possibile eseguire il troubleshooting di base di un nodo non ancora aggiunto a un cluster. A tale scopo, è possibile utilizzare l'account di sistema sfreadonly con o senza l'aiuto del supporto NetApp. Se è stato configurato un nodo di gestione, è possibile utilizzarlo per SSH ed eseguire lo script fornito per questa attività.

1. Da una macchina Windows, Linux o Mac su cui è installato un client SSH, eseguire lo script appropriato per il sistema fornito dal supporto NetApp.
2. SSH all'IP del nodo:

```
ssh -i user sfreadonly@[node_ip]
```

3. (Facoltativo) disattivare "funzionalità di accesso remoto" nuovamente al termine della risoluzione dei problemi.

> SSH rimane attivato sul nodo di gestione se non viene disattivato. La configurazione abilitata SSH persiste sul nodo di gestione tramite aggiornamenti e aggiornamenti fino a quando non viene disattivata manualmente.

Trova ulteriori informazioni

- "Plug-in NetApp Element per server vCenter"
- "Pagina delle risorse NetApp HCI"

Avviare una sessione remota di NetApp Support

Se hai bisogno di supporto tecnico per il tuo sistema storage all-flash SolidFire, 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.

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.

Prima di iniziare

- Per i servizi di gestione 2.18 e versioni successive, la funzionalità di accesso remoto è disattivata per impostazione predefinita nel nodo di gestione. Per abilitare la funzionalità di accesso remoto, vedere "Gestire la funzionalità SSH sul 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

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
```

- (Facoltativo) disattivare "funzionalità di accesso remoto" nuovamente.

> SSH rimane attivato sul nodo di gestione se non viene disattivato. La configurazione abilitata SSH persiste sul nodo di gestione tramite aggiornamenti e aggiornamenti fino a quando non viene disattivata manualmente.

Trova ulteriori informazioni

- "Plug-in NetApp Element per server vCenter"
- "Documentazione software SolidFire ed Element"

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 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.

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 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 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 disabilitare SSH o `true` per riabilitare la funzionalità

SSH precedentemente disabilitata.

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 disattivato per impostazione predefinita sui nodi di gestione che eseguono i servizi di gestione 2.18 o versioni successive.

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"

- "Documentazione software SolidFire ed Element"

Informazioni sul copyright

Informazioni sul marchio commerciale