Gestión de conexiones de soporte

Element Software

NetApp
October 01, 2024

Tabla de contenidos

Gestión de conexiones de soporte

Acceder a nodos de almacenamiento mediante SSH para solución de problemas básica

A partir de Element 12.5, puede utilizar la cuenta del sistema sfreadonly en los nodos de almacenamiento para la solución de problemas básica. También permite habilitar y acceder al túnel de soporte remoto para el soporte de NetApp para la solución de problemas avanzada.

La cuenta del sistema sfreadonly permite el acceso para ejecutar comandos básicos de solución de problemas de red y sistema Linux, incluidos `ping`.

> A menos que el soporte de NetApp indique lo contrario, cualquier modificación de este sistema no será compatible, anulando su contrato de soporte y podría dar lugar a inestabilidad o inaccesibilidad a los datos.

Antes de empezar

- **Escribir permisos**: Compruebe que tiene permisos de escritura en el directorio de trabajo actual.
- **(Opcional) Generar su propio par de claves**: Ejecutar `ssh-keygen` desde Windows 10, macOS o distribución de Linux. Se trata de una acción única que permite crear un par de claves de usuario y volver a utilizarla para futuras sesiones de solución de problemas. Es posible que desee utilizar certificados asociados a cuentas de empleados, que también funcionarán en este modelo.
- **Habilitar la capacidad SSH en el nodo de administración**: Para habilitar la funcionalidad de acceso remoto en el modo de administración, consulte "este tema". Para los servicios de gestión 2.18 y posteriores, la funcionalidad para el acceso remoto se deshabilita en el nodo de gestión de manera predeterminada.
- **Habilitar la capacidad SSH en el clúster de almacenamiento**: Para habilitar la funcionalidad de acceso remoto en los nodos del clúster de almacenamiento, consulte "este tema".
- **Configuración del firewall**: Si el nodo de gestión está detrás de un servidor proxy, se necesitan los siguientes puertos TCP en el archivo sshd.config:

Puerto TCP	Descripción	Dirección de conexión
443	Llamadas API/HTTPS para un reenvío de puertos inverso a través de un túnel de soporte abierto a la interfaz de usuario web	Del nodo de gestión a los nodos de almacenamiento
22	Acceso de inicio de sesión SSH	Del nodo de gestión a los nodos de almacenamiento o desde los nodos de almacenamiento al nodo de gestión

Opciones de solución de problemas

- Solucionar los problemas de un nodo de clúster
- Solucione problemas de un nodo de clúster con el soporte de NetApp

- Solucione el problema de un nodo que no forme parte del clúster

Solucionar los problemas de un nodo de clúster

Puede realizar la solución de problemas básica utilizando la cuenta del sistema sfreadonly:

Pasos

1. SSH al nodo de gestión con las credenciales de inicio de sesión de su cuenta seleccionadas al instalar la máquina virtual del nodo de gestión.
2. En el nodo de gestión, vaya a `/sf/bin`.
3. Busque la secuencia de comandos adecuada para el sistema:
   - SignSshKeys.ps1
   - SignSshKeys.py
   - SignSshKeys.sh

   > SignSshKeys.ps1 depende de PowerShell 7 o posterior y SignSshKeys.py depende de Python 3.6.0 o posterior y el "módulo solicitudes".
   >
   > El `SignSshKeys` archivo de comandos escribe `user`, `user.pub` y `user-cert.pub` archivos en el directorio de trabajo actual, que posteriormente se utiliza con el `ssh` comando. Sin embargo, cuando se proporciona un archivo de clave pública al script, solo se escribe en el directorio un `<public_key>` archivo (con `<public_key>` el prefijo del archivo de clave pública que se pasa al script).

4. Ejecute el script en el nodo de gestión para generar la cadena de claves SSH. La secuencia de comandos permite el acceso SSH mediante la cuenta del sistema sfreadonly en todos los nodos del clúster.

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

   a. Sustituya el valor entre corchetes [ ] (incluidos los corchetes) para cada uno de los parámetros siguientes:

      > Puede utilizar el parámetro de formulario abreviado o completo.

      - **--ip | -i [dirección ip]**: Dirección IP del nodo de destino en el que se ejecuta la API.
      - **--user | -u [username]**: Usuario de cluster utilizado para ejecutar la llamada de API.
      - **(opcional) --duración | -d [horas]**: La duración que una clave firmada debe seguir siendo válida como un número entero en horas. El valor predeterminado es 24 horas.
      - **(opcional) --publickey | -k [ruta de acceso de clave pública]**: La ruta a una clave pública, si el usuario decide proporcionarla.

   b. Compare los datos introducidos con el siguiente comando de ejemplo. En este ejemplo, `10.116.139.195` es la IP del nodo de almacenamiento, `admin` es el nombre de usuario del clúster y la duración de la validez de la clave es de dos horas:

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

c. Ejecute el comando.

5. SSH a las IP del nodo:

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

Podrá ejecutar comandos básicos de solución de problemas del sistema Linux y de la red, `ping` como , y otros comandos de sólo lectura.

6. (Opcional) Deshabilite "función de acceso remoto" de nuevo una vez finalizada la solución de problemas.

> SSH sigue estando habilitado en el nodo de gestión si no se la deshabilita. La configuración habilitada para SSH continúa en el nodo de gestión a través de actualizaciones y renovaciones hasta que se deshabilita manualmente.

Solucione problemas de un nodo de clúster con el soporte de NetApp

El soporte de NetApp puede llevar a cabo una solución de problemas avanzada con una cuenta del sistema, lo que permite a un técnico ejecutar diagnósticos de elementos más profundos.

Pasos

1. SSH al nodo de gestión con las credenciales de inicio de sesión de su cuenta seleccionadas al instalar la máquina virtual del nodo de gestión.
2. Ejecute el comando rst con el número de puerto enviado por el soporte de NetApp para abrir el túnel de soporte:

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

   El soporte de NetApp inicia sesión en su nodo de gestión por medio del túnel de soporte.

3. En el nodo de gestión, vaya a `/sf/bin`.
4. Busque la secuencia de comandos adecuada para el sistema:
   - SignSshKeys.ps1
   - SignSshKeys.py
   - SignSshKeys.sh

> SignSshKeys.ps1 depende de PowerShell 7 o posterior y SignSshKeys.py depende de Python 3.6.0 o posterior y el "módulo solicitudes".
>
> El `SignSshKeys` archivo de comandos escribe `user`, `user.pub` y `user-cert.pub` archivos en el directorio de trabajo actual, que posteriormente se utiliza con el `ssh` comando. Sin embargo, cuando se proporciona un archivo de clave pública al script, solo se escribe en el directorio un `<public_key>` archivo (con `<public_key>` el prefijo del archivo de clave pública que se pasa al script).

5. Ejecute el script para generar el llavero SSH con el `--sfadmin` indicador. El script habilita SSH en todos los nodos.

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

> Para SSH como `--sfadmin` nodo almacenado en clúster, debe generar el llavero SSH mediante a `--user` con `supportAdmin` acceso en el clúster.
>
> Para configurar `supportAdmin` el acceso para las cuentas de administrador de clúster, pueden usarse las API o la interfaz de usuario de Element:
>
> - "Configure el acceso "supportAdmin" mediante la interfaz de usuario de Element"
> - Configure `supportAdmin` el acceso utilizando las API y agregando `"supportAdmin"` como `"access"` el tipo en la solicitud de API:
>   - "Configure el acceso "supportAdmin" para una nueva cuenta"
>   - "Configure el acceso "supportAdmin" para una cuenta existente"
>
>   Para obtener el `clusterAdminID`, puede utilizar "ListClusterAdmins"la API.
>
> Para añadir `supportAdmin` acceso, debe tener Privileges de administrador del clúster o administrador.

a. Sustituya el valor entre corchetes [ ] (incluidos los corchetes) para cada uno de los parámetros siguientes:

   > Puede utilizar el parámetro de formulario abreviado o completo.

   - **--ip | -i [dirección ip]**: Dirección IP del nodo de destino en el que se ejecuta la API.
   - **--user | -u [username]**: Usuario de cluster utilizado para ejecutar la llamada de API.
   - **(opcional) --duración | -d [horas]**: La duración que una clave firmada debe seguir siendo válida como un número entero en horas. El valor predeterminado es 24 horas.

b. Compare los datos introducidos con el siguiente comando de ejemplo. En este ejemplo, `192.168.0.1` es la IP del nodo de almacenamiento, `admin` es el nombre de usuario del clúster, la duración de la validez de la clave es de dos horas y `--sfadmin` permite el acceso al nodo de soporte de NetApp para la solución de problemas:

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

c. Ejecute el comando.

6. SSH a las IP del nodo:

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

7. Para cerrar el túnel de soporte remoto, introduzca lo siguiente:

```
rst --killall
```

8. (Opcional) Deshabilite "función de acceso remoto" de nuevo una vez finalizada la solución de problemas.

> SSH sigue estando habilitado en el nodo de gestión si no se la deshabilita. La configuración habilitada para SSH continúa en el nodo de gestión a través de actualizaciones y renovaciones hasta que se deshabilita manualmente.

Solucione el problema de un nodo que no forme parte del clúster

Puede realizar la solución de problemas básica de un nodo que aún no se ha añadido a un clúster. Puede utilizar la cuenta del sistema sfreadonly con este fin, con o sin la ayuda del soporte de NetApp. Si tiene configurado un nodo de gestión, puede usarlo para SSH y ejecutar el script proporcionado para esta tarea.

1. Desde un equipo Windows, Linux o Mac que tiene instalado un cliente SSH, ejecute el script adecuado para el sistema proporcionado por el soporte de NetApp.
2. SSH a la IP del nodo:

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

3. (Opcional) Deshabilite "función de acceso remoto" de nuevo una vez finalizada la solución de problemas.

> SSH sigue estando habilitado en el nodo de gestión si no se la deshabilita. La configuración habilitada para SSH continúa en el nodo de gestión a través de actualizaciones y renovaciones hasta que se deshabilita manualmente.

Obtenga más información

- "Plugin de NetApp Element para vCenter Server"
- "Página de recursos de NetApp HCI"

Inicie una sesión de soporte remota de NetApp

Si necesita soporte técnico para su sistema de almacenamiento all-flash SolidFire, el soporte de NetApp puede conectarse de forma remota con su sistema. Para iniciar una sesión y tener acceso remoto, el soporte de NetApp puede abrir una conexión de Secure Shell (SSH) inversa a su entorno.

Puede abrir un puerto TCP para una conexión de túnel SSH inverso con el soporte de NetApp. Gracias a esta conexión, el soporte de NetApp puede iniciar sesión en su nodo de gestión.

Antes de empezar

- Para los servicios de gestión 2.18 y posteriores, la funcionalidad para el acceso remoto se deshabilita en el nodo de gestión de manera predeterminada. Para activar la función de acceso remoto, consulte "Gestione la funcionalidad SSH en el nodo de gestión".
- Si el nodo de gestión está detrás de un servidor proxy, se necesitan los siguientes puertos TCP en el archivo sshd.config:

Puerto TCP	Descripción	Dirección de conexión
443	Llamadas API/HTTPS para un reenvío de puertos inverso a través de un túnel de soporte abierto a la interfaz de usuario web	Del nodo de gestión a los nodos de almacenamiento
22	Acceso de inicio de sesión SSH	Del nodo de gestión a los nodos de almacenamiento o desde los nodos de almacenamiento al nodo de gestión

Pasos

- Inicie sesión en su nodo de almacenamiento y abra una sesión de terminal.
- En un símbolo del sistema, introduzca lo siguiente:

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

- Para cerrar el túnel de soporte remoto, introduzca lo siguiente:

```
rst --killall
```

- (Opcional) Vuelva a deshabilitar "función de acceso remoto".

> SSH sigue estando habilitado en el nodo de gestión si no se la deshabilita. La configuración habilitada para SSH continúa en el nodo de gestión a través de actualizaciones y renovaciones hasta que se deshabilita manualmente.

Obtenga más información

- "Plugin de NetApp Element para vCenter Server"
- "Documentación de SolidFire y el software Element"

Gestione la funcionalidad SSH en el nodo de gestión

Es posible deshabilitar, volver a habilitar o determinar el estado de la funcionalidad SSH en el nodo de gestión (mNode) mediante la API DE REST. La funcionalidad de SSH que proporciona "Acceso a la sesión del túnel de soporte remoto (RST) de NetApp Support"está deshabilitada de manera predeterminada en los nodos de gestión que ejecutan los servicios de gestión 2,18 o posterior.

A partir de los servicios de gestión 2.20.69, puede habilitar y deshabilitar la funcionalidad SSH en el nodo de gestión mediante la interfaz de usuario de control de cloud híbrido de NetApp.

Lo que necesitará

- **Permisos de control del cloud híbrido de NetApp**: Tiene permisos como administrador.
- **Permisos de administrador de clúster**: Tiene permisos como administrador en el clúster de almacenamiento.
- **Software Element**: El clúster ejecuta el software NetApp Element 11.3 o posterior.
- **Nodo de gestión**: Ha implementado un nodo de gestión que ejecuta la versión 11.3 o posterior.
- **Actualizaciones de servicios de administración**:
  - Para utilizar la IU de control de nube híbrida de NetApp, ha actualizado el "paquete de servicios de gestión" a la versión 2.20.69 o posterior.
  - Para utilizar la interfaz de usuario de la API de REST, actualizó el "paquete de servicios de gestión" a la versión 2,17.

Opciones

- Deshabilite o habilite la funcionalidad SSH en el nodo de gestión mediante la IU de control de cloud híbrido de NetApp

Puede realizar cualquiera de las siguientes tareas después de usted"autenticar":

- Deshabilite o habilite la funcionalidad SSH en el nodo de gestión mediante las API de
- Determine el estado de la capacidad SSH en el nodo de gestión mediante las API de

Deshabilite o habilite la funcionalidad SSH en el nodo de gestión mediante la IU de control de cloud híbrido de NetApp

Es posible deshabilitar o volver a habilitar la funcionalidad SSH en el nodo de gestión. La funcionalidad de SSH que proporciona "Acceso a la sesión del túnel de soporte remoto (RST) de NetApp Support"está deshabilitada de manera predeterminada en los nodos de gestión que ejecutan los servicios de gestión 2,18 o posterior. Al deshabilitar SSH, no se finalizan ni desconectan las sesiones de cliente SSH existentes en el nodo de gestión. Si deshabilita SSH y opta por volver a habilitarla más adelante, puede hacerlo mediante la interfaz de usuario de control de cloud híbrido de NetApp.

Para habilitar o deshabilitar el acceso de soporte mediante SSH para un clúster de almacenamiento, debe usar el "Página de configuración del clúster de la interfaz de usuario de Element".

Pasos

1. En el panel de control, seleccione el menú de opciones de la parte superior derecha y seleccione **Configurar**.
2. En la pantalla **Support Access for Management Node**, cambie el conmutador para activar el SSH del nodo de administración.
3. Después de completar la solución de problemas, en la pantalla **Support Access for Management Node**, cambie el conmutador para desactivar el SSH del nodo de gestión.

Deshabilite o habilite la funcionalidad SSH en el nodo de gestión mediante las API de

Es posible deshabilitar o volver a habilitar la funcionalidad SSH en el nodo de gestión. La funcionalidad de SSH que proporciona "Acceso a la sesión del túnel de soporte remoto (RST) de NetApp Support"está deshabilitada de manera predeterminada en los nodos de gestión que ejecutan los servicios de gestión 2,18 o

posterior. Al deshabilitar SSH, no se finalizan ni desconectan las sesiones de cliente SSH existentes en el nodo de gestión. Si deshabilita SSH y opta por volver a habilitarla más adelante, puede hacerlo mediante la misma API.

Comando API

Para los servicios de gestión 2.18 o posterior:

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

Para los servicios de gestión 2.17 o anteriores:

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

Usted puede encontrar el portador `${TOKEN}` utilizado por el comando API cuando usted "autorizar". El portador `${TOKEN}` está en la respuesta de rizo.

PASOS PARA LA INTERFAZ DE USUARIO DE LA API DE REST

1. Acceda a la interfaz de usuario de API de REST del servicio API del nodo de gestión introduciendo la dirección IP del nodo de gestión seguida `/mnode/` de :

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

2. Seleccione **autorizar** y complete lo siguiente:
   a. Introduzca el nombre de usuario y la contraseña del clúster.
   b. Introduzca el ID de cliente como `mnode-client`.
   c. Seleccione **autorizar** para iniciar una sesión.
   d. Cierre la ventana.
3. En la interfaz de usuario DE LA API DE REST, seleccione **PUT /settings/ssh**.
   a. Seleccione **probar**.
   b. Establezca el parámetro **enabled** en `false` para desactivar SSH o `true` para volver a activar la capacidad SSH que se había desactivado anteriormente.
   c. Seleccione **Ejecutar**.

Determine el estado de la capacidad SSH en el nodo de gestión mediante las API de

Puede determinar si la capacidad SSH está habilitada o no en el nodo de gestión mediante una API de servicio de nodo de gestión. SSH está deshabilitado de forma predeterminada en los nodos de gestión que ejecutan servicios de gestión 2.18 o posteriores.

Comando API

Para los servicios de gestión 2.18 o posterior:

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

Para los servicios de gestión 2.17 o anteriores:

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

Usted puede encontrar el portador `${TOKEN}` utilizado por el comando API cuando usted "autorizar". El portador `${TOKEN}` está en la respuesta de rizo..

PASOS PARA LA INTERFAZ DE USUARIO DE LA API DE REST

1. Acceda a la interfaz de usuario de API de REST del servicio API del nodo de gestión introduciendo la dirección IP del nodo de gestión seguida `/mnode/` de :

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

2. Seleccione **autorizar** y complete lo siguiente:
   a. Introduzca el nombre de usuario y la contraseña del clúster.
   b. Introduzca el ID de cliente como `mnode-client`.
   c. Seleccione **autorizar** para iniciar una sesión.
   d. Cierre la ventana.
3. En la interfaz de usuario DE LA API DE REST, seleccione **GET /settings/ssh**.
   a. Seleccione **probar**.
   b. Seleccione **Ejecutar**.

Obtenga más información

- "Plugin de NetApp Element para vCenter Server"
- "Documentación de SolidFire y el software Element"

Información de copyright

Información de la marca comercial