Manage support connections

Element Software

NetApp
October 01, 2024

Table of Contents

Manage support connections

Accessing storage nodes using SSH for basic troubleshooting

Beginning with Element 12.5, you can use the sfreadonly system account on the storage nodes for basic troubleshooting. You can also enable and open remote support tunnel access for NetApp Support for advanced troubleshooting.

The sfreadonly system account enables access to run basic Linux system and network troubleshooting commands, including `ping`.

Unless advised by NetApp Support, any alterations to this system are unsupported, voiding your support contract, and might result in instability or inaccessibility of data.

Before you begin

- **Write permissions**: Verify that you have write permissions to the current working directory.
- **(Optional) Generate your own key pair**: Run `ssh-keygen` from Windows 10, MacOS, or Linux distribution. This is a one-time action to create a user key pair and can be reused for future troubleshooting sessions. You might want to use certificates associated with employee accounts, which would also work in this model.
- **Enable SSH capability on the management node**: To enable remote access functionality on the management mode, see this topic. For management services 2.18 and later, the capability for remote access is disabled on the management node by default.
- **Enable SSH capability on the storage cluster**: To enable remote access functionality on the storage cluster nodes, see this topic.
- **Firewall configuration**: If your management node is behind a proxy server, the following TCP ports are required in the sshd.config file:

TCP port	Description	Connection direction
443	API calls/HTTPS for reverse port forwarding via open support tunnel to the web UI	Management node to storage nodes
22	SSH login access	Management node to storage nodes or from storage nodes to management node

Troubleshooting options

- Troubleshoot a cluster node
- Troubleshoot a cluster node with NetApp Support
- Troubleshoot a node that is not part of cluster

Troubleshoot a cluster node

You can perform basic troubleshooting using the sfreadonly system account:

Steps

1. SSH to the management node using your account login credentials you selected when installing the management node VM.
2. On the management node, go to `/sf/bin`.
3. Find the appropriate script for your system:
   - SignSshKeys.ps1
   - SignSshKeys.py
   - SignSshKeys.sh

   SignSshKeys.ps1 is dependent on PowerShell 7 or later and SignSshKeys.py is dependent on Python 3.6.0 or later and the requests module.

   The `SignSshKeys` script writes `user`, `user.pub`, and `user-cert.pub` files into the current working directory, which are later used by the `ssh` command. However, when a public key file is provided to the script, only a `<public_key>` file (with `<public_key>` replaced with the prefix of the public key file passed into the script) is written out to the directory.

4. Run the script on the management node to generate the SSH keychain. The script enables SSH access using the sfreadonly system account across all nodes in the cluster.

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

   a. Replace the value in [ ] brackets (including the brackets) for each of the following parameters:

      You can use either the abbreviated or full form parameter.

      - **--ip | -i [ip address]**: IP address of the target node for the API to run against.
      - **--user | -u [username]**: Cluster user used to run the API call.
      - **(Optional) --duration | -d [hours]**: The duration a signed key should remain valid as an integer in hours. The default is 24 hours.
      - **(Optional) --publickey | -k [public key path]**: The path to a public key, if the user chooses to provide one.

   b. Compare your input against the following sample command. In this example, `10.116.139.195` is the IP of the storage node, `admin` is the cluster username, and the duration of key validity is two hours:

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

   c. Run the command.

5. SSH to the node IPs:

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

You will be able to run basic Linux system and network troubleshooting commands, such as `ping`, and other read-only commands.

6. (Optional) Disable remote access functionality again after troubleshooting is complete.

> SSH remains enabled on the management node if you do not disable it. SSH enabled configuration persists on the management node through updates and upgrades until it is manually disabled.

Troubleshoot a cluster node with NetApp Support

NetApp Support can perform advanced troubleshooting with a system account that allows a technician to run deeper Element diagnostics.

Steps

1. SSH to the management node using your account login credentials you selected when installing the management node VM.
2. Run the rst command with the port number sent by NetApp Support to open the support tunnel:

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

   NetApp Support will log in to your management node using the support tunnel.

3. On the management node, go to `/sf/bin`.
4. Find the appropriate script for your system:
   - SignSshKeys.ps1
   - SignSshKeys.py
   - SignSshKeys.sh

   > SignSshKeys.ps1 is dependent on PowerShell 7 or later and SignSshKeys.py is dependent on Python 3.6.0 or later and the requests module.
   >
   > The `SignSshKeys` script writes `user`, `user.pub`, and `user-cert.pub` files into the current working directory, which are later used by the `ssh` command. However, when a public key file is provided to the script, only a `<public_key>` file (with `<public_key>` replaced with the prefix of the public key file passed into the script) is written out to the directory.

5. Run the script to generate the SSH keychain with the `--sfadmin` flag. The script enables SSH across all nodes.

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

To SSH as `--sfadmin` to a clustered node, you must generate the SSH keychain using a `--user` with `supportAdmin` access on the cluster.

To configure `supportAdmin` access for cluster administrator accounts, you can use the Element UI or APIs:

- Configure "supportAdmin" access using the Element UI
- Configure `supportAdmin` access by using APIs and adding `"supportAdmin"` as the `"access"` type in the API request:
  - Configure "supportAdmin" access for a new account
  - Configure "supportAdmin" access for an existing account

    To get the `clusterAdminID`, you can use the ListClusterAdmins API.

To add `supportAdmin` access, you must have cluster administrator or administrator privileges.

a. Replace the value in [ ] brackets (including the brackets) for each of the following parameters:

   You can use either the abbreviated or full form parameter.

   - **--ip | -i [ip address]**: IP address of the target node for the API to run against.
   - **--user | -u [username]**: Cluster user used to run the API call.
   - **(Optional) --duration | -d [hours]**: The duration a signed key should remain valid as an integer in hours. The default is 24 hours.

b. Compare your input against the following sample command. In this example, `192.168.0.1` is the IP of the storage node, `admin` is the cluster username, duration of key validity is two hours, and `--sfadmin` allows NetApp Support node access for troubleshooting:

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

c. Run the command.

6. SSH to the node IPs:

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

7. To close the remote support tunnel, enter the following:

```
rst --killall
```

8. (Optional) Disable remote access functionality again after troubleshooting is complete.

SSH remains enabled on the management node if you do not disable it. SSH enabled configuration persists on the management node through updates and upgrades until it is manually disabled.

Troubleshoot a node that is not part of cluster

You can perform basic troubleshooting of a node that has not yet been added to a cluster. You can use the sfreadonly system account for this purpose with or without the help of NetApp Support. If you have a management node set up, you can use it for SSH and run the script provided for this task.

1. From a Windows, Linux, or Mac machine that has an SSH client installed, run the appropriate script for your system provided by NetApp Support.
2. SSH to the node IP:

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

3. (Optional) Disable remote access functionality again after troubleshooting is complete.

SSH remains enabled on the management node if you do not disable it. SSH enabled configuration persists on the management node through updates and upgrades until it is manually disabled.

Find more information

- NetApp Element Plug-in for vCenter Server
- NetApp HCI Resources Page

Start a remote NetApp Support session

If you require technical support for your SolidFire all-flash storage system, NetApp Support can connect remotely with your system. To start a session and gain remote access, NetApp Support can open a reverse Secure Shell (SSH) connection to your environment.

You can open a TCP port for an SSH reverse tunnel connection with NetApp Support. This connection enables NetApp Support to log in to your management node.

Before you begin

- For management services 2.18 and later, the capability for remote access is disabled on the management node by default. To enable remote access functionality, see Manage SSH functionality on the management node.
- If your management node is behind a proxy server, the following TCP ports are required in the sshd.config file:

TCP port	Description	Connection direction
443	API calls/HTTPS for reverse port forwarding via open support tunnel to the web UI	Management node to storage nodes
22	SSH login access	Management node to storage nodes or from storage nodes to management node

Steps

- Log in to your management node and open a terminal session.
- At a prompt, enter the following:

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

- To close the remote support tunnel, enter the following:

```
rst --killall
```

- (Optional) Disable remote access functionality again.

> SSH remains enabled on the management node if you do not disable it. SSH enabled configuration persists on the management node through updates and upgrades until it is manually disabled.

Find more information

- NetApp Element Plug-in for vCenter Server
- SolidFire and Element Software Documentation

Manage SSH functionality on the management node

You can disable, re-enable, or determine the status of the SSH capability on the management node (mNode) using the REST API. SSH capability that provides NetApp Support remote support tunnel (RST) session access is disabled by default on management nodes running management services 2.18 or later.

Beginning with Management Services 2.20.69, you can enable and disable SSH capability on the management node using the NetApp Hybrid Cloud Control UI.

What you'll need

- **NetApp Hybrid Cloud Control permissions**: You have permissions as administrator.
- **Cluster administrator permissions**: You have permissions as administrator on the storage cluster.
- **Element software**: Your cluster is running NetApp Element software 11.3 or later.
- **Management node**: You have deployed a management node running version 11.3 or later.
- **Management services updates**:

- To use the NetApp Hybrid Cloud Control UI, you have updated your management services bundle to version 2.20.69 or later.
- To use the REST API UI, you have updated your management services bundle to version 2.17.

Options

- Disable or enable the SSH capability on the management node using NetApp Hybrid Cloud Control UI

You can do any of the following tasks after you authenticate:

- Disable or enable the SSH capability on the management node using APIs
- Determine status of the SSH capability on the management node using APIs

Disable or enable the SSH capability on the management node using NetApp Hybrid Cloud Control UI

You can disable or re-enable SSH capability on the management node. SSH capability that provides NetApp Support remote support tunnel (RST) session access is disabled by default on management nodes running management services 2.18 or later. Disabling SSH does not terminate or disconnect existing SSH client sessions to the management node. If you disable SSH and elect to re-enable it at a later time, you can do so using the NetApp Hybrid Cloud Control UI.

To enable or disable support access using SSH for a storage cluster, you must use the Element UI cluster settings page.

Steps

1. From the Dashboard, select the options menu on the top right and select **Configure**.
2. In the **Support Access for Management Node** screen, toggle the switch to enable management node SSH.
3. After you complete troubleshooting, in the **Support Access for Management Node** screen, toggle the switch to disable management node SSH.

Disable or enable the SSH capability on the management node using APIs

You can disable or re-enable SSH capability on the management node. SSH capability that provides NetApp Support remote support tunnel (RST) session access is disabled by default on management nodes running management services 2.18 or later. Disabling SSH does not terminate or disconnect existing SSH client sessions to the management node. If you disable SSH and elect to re-enable it at a later time, you can do so using the same API.

API command

For management services 2.18 or later:

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

For management services 2.17 or earlier:

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

You can find the bearer `${TOKEN}` used by the API command when you authorize. The bearer `${TOKEN}` is in the curl response.

REST API UI steps

1. Access the REST API UI for the management node API service by entering the management node IP address followed by `/mnode/`:

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

2. Select **Authorize** and complete the following:
   a. Enter the cluster user name and password.
   b. Enter the client ID as `mnode-client`.
   c. Select **Authorize** to begin a session.
   d. Close the window.
3. From the REST API UI, select **PUT /settings/ssh**.
   a. Select **Try it out**.
   b. Set the **enabled** parameter to `false` to disable SSH or `true` to re-enable SSH capability that was previously disabled.
   c. Select **Execute**.

Determine status of the SSH capability on the management node using APIs

You can determine whether or not SSH capability is enabled on the management node using a management node service API. SSH is disabled by default on management nodes running management services 2.18 or later.

API command

For management services 2.18 or later:

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

For management services 2.17 or earlier:

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

You can find the bearer `${TOKEN}` used by the API command when you authorize. The bearer `${TOKEN}` is in the curl response..

REST API UI steps

1. Access the REST API UI for the management node API service by entering the management node IP address followed by `/mnode/`:

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

2. Select **Authorize** and complete the following:
   a. Enter the cluster user name and password.
   b. Enter the client ID as `mnode-client`.
   c. Select **Authorize** to begin a session.
   d. Close the window.
3. From the REST API UI, select **GET /settings/ssh**.
   a. Select **Try it out**.
   b. Select **Execute**.

Find more information

- NetApp Element Plug-in for vCenter Server
- SolidFire and Element Software Documentation

Copyright information

Trademark information