



Access the cluster by using the CLI (cluster administrators only)

ONTAP 9

NetApp
January 11, 2023

Table of Contents

- Access the cluster by using the CLI (cluster administrators only) 1
 - Access the cluster by using the serial port. 1
 - Access the cluster by using SSH 1
 - SSH login security 4
 - Enable Telnet or RSH access to the cluster 5
 - Access the cluster by using Telnet 6
 - Access the cluster by using RSH 7

Access the cluster by using the CLI (cluster administrators only)

Access the cluster by using the serial port

You can access the cluster directly from a console that is attached to a node’s serial port.

Steps

- 1. At the console, press Enter.

The system responds with the login prompt.
- 2. At the login prompt, do one of the following:

| To access the cluster with... | Enter the following account name... |
|--|-------------------------------------|
| The default cluster account | admin |
| An alternative administrative user account | <i>username</i> |

The system responds with the password prompt.

- 3. Enter the password for the admin or administrative user account, and then press Enter.

Access the cluster by using SSH

You can issue SSH requests to the cluster to perform administrative tasks. SSH is enabled by default.

What you’ll need

- You must have a user account that is configured to use `ssh` as an access method.

The `-application` parameter of the `security login` commands specifies the access method for a user account. The `security login man` pages contain additional information.

- If you use an Active Directory (AD) domain user account to access the cluster, an authentication tunnel for the cluster must have been set up through a CIFS-enabled storage virtual machine (SVM), and your AD domain user account must also have been added to the cluster with `ssh` as an access method and `domain` as the authentication method.
- If you use IPv6 connections, IPv6 must already be configured and enabled on the cluster, and firewall policies must already be configured with IPv6 addresses.

The network options `ipv6 show` command displays whether IPv6 is enabled. The `system services firewall policy show` command displays firewall policies.

About this task

- You must use an OpenSSH 5.7 or later client.

- Only the SSH v2 protocol is supported; SSH v1 is not supported.
- ONTAP supports a maximum of 64 concurrent SSH sessions per node.

If the cluster management LIF resides on the node, it shares this limit with the node management LIF.

If the rate of incoming connections is higher than 10 per second, the service is temporarily disabled for 60 seconds.

- ONTAP supports only the AES and 3DES encryption algorithms (also known as *ciphers*) for SSH.

AES is supported with 128, 192, and 256 bits in key length. 3DES is 56 bits in key length as in the original DES, but it is repeated three times.

- When FIPS mode is on, SSH clients should negotiate with Elliptic Curve Digital Signature Algorithm (ECDSA) public key algorithms for the connection to be successful.
- If you want to access the ONTAP CLI from a Windows host, you can use a third-party utility such as PuTTY.
- If you use a Windows AD user name to log in to ONTAP, you should use the same uppercase or lowercase letters that were used when the AD user name and domain name were created in ONTAP.

AD user names and domain names are not case-sensitive. However, ONTAP user names are case-sensitive. Case mismatch between the user name created in ONTAP and the user name created in AD results in a login failure.

- Beginning with ONTAP 9.3, you can enable SSH multifactor authentication for local administrator accounts.

When SSH multifactor authentication is enabled, users are authenticated by using a public key and a password.

- Beginning with ONTAP 9.4, you can enable SSH multifactor authentication for LDAP and NIS remote users.

Steps

1. From an administration host, enter the `ssh` command in one of the following formats:

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

If you are using an AD domain user account, you must specify *username* in the format of *domainname\AD_accountname* (with double backslashes after the domain name) or "*domainname\AD_accountname*" (enclosed in double quotation marks and with a single backslash after the domain name).

hostname_or_IP is the host name or the IP address of the cluster management LIF or a node management LIF. Using the cluster management LIF is recommended. You can use an IPv4 or IPv6 address.

command is not required for SSH-interactive sessions.

Examples of SSH requests

The following examples show how the user account named "joe" can issue an SSH request to access a cluster whose cluster management LIF is 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.
```

The following examples show how the user account named “john” from the domain named “DOMAIN1” can issue an SSH request to access a cluster whose cluster management LIF is 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.
```

The following example shows how the user account named “joe” can issue an SSH MFA request to access a cluster whose cluster management LIF is 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.
```

Related information

[Administrator authentication and RBAC](#)

SSH login security

Beginning with ONTAP 9.5, you can view information about previous logins, unsuccessful attempts to log in, and changes to your privileges since your last successful login.

Security-related information is displayed when you successfully log in as an SSH admin user. You are alerted about the following conditions:

- The last time your account name was logged in.
- The number of unsuccessful login attempts since the last successful login.
- Whether the role has changed since the last login (for example, if the admin account's role changed from "admin" to "backup.")
- Whether the add, modify, or delete capabilities of the role were modified since the last login.



If any of the information displayed is suspicious, you should immediately contact your security department.

To obtain this information when you login, the following prerequisites must be met:

- Your SSH user account must be provisioned in ONTAP.
- Your SSH security login must be created.
- Your login attempt must be successful.

Restrictions and other considerations for SSH login security

The following restrictions and considerations apply to SSH login security information:

- The information is available only for SSH-based logins.
- For group-based admin accounts, such as LDAP/NIS and AD accounts, users can view the SSH login information if the group of which they are a member is provisioned as an admin account in ONTAP.

However, alerts about changes to the role of the user account cannot be displayed for these users. Also, users belonging to an AD group that has been provisioned as an admin account in ONTAP cannot view the count of unsuccessful login attempts that occurred since the last time they logged in.

- The information maintained for a user is deleted when the user account is deleted from ONTAP.
- The information is not displayed for connections to applications other than SSH.

Examples of SSH login security information

The following examples demonstrate the type of information displayed after you login.

- This message is displayed after each successful login:

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

- These messages are displayed if there have been unsuccessful attempts to login since the last successful login:

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

- These messages are displayed if there have been unsuccessful attempts to login and your privileges were modified since the last successful login:

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

Enable Telnet or RSH access to the cluster

As a security best practice, Telnet and RSH are disabled in the predefined management firewall policy (`mgmt`). To enable the cluster to accept Telnet or RSH requests, you must create a new management firewall policy that has Telnet or RSH enabled, and then associate the new policy with the cluster management LIF.

About this task

ONTAP prevents you from changing predefined firewall policies, but you can create a new policy by cloning the predefined `mgmt` management firewall policy, and then enabling Telnet or RSH under the new policy. However, Telnet and RSH are not secure protocols, so you should consider using SSH to access the cluster. SSH provides a secure remote shell and interactive network session.

Perform the following steps to enable Telnet or RSH access to the clusters:

Steps

1. Enter the advanced privilege mode:
`set advanced`
2. Enable a security protocol (RSH or Telnet):
`security protocol modify -application security_protocol -enabled true`

3. Create a new management firewall policy based on the `mgmt` management firewall policy:
`system services firewall policy clone -policy mgmt -destination-policy policy-name`
4. Enable Telnet or RSH in the new management firewall policy:
`system services firewall policy create -policy policy-name -service security_protocol -action allow -ip-list ip_address/netmask`
To allow all IP addresses, you should specify `-ip-list 0.0.0.0/0`
5. Associate the new policy with the cluster management LIF:
`network interface modify -vserver cluster_management_LIF -lif cluster_mgmt -firewall-policy policy-name`

Access the cluster by using Telnet

You can issue Telnet requests to the cluster to perform administrative tasks. Telnet is disabled by default.

What you'll need

The following conditions must be met before you can use Telnet to access the cluster:

- You must have a cluster local user account that is configured to use Telnet as an access method.

The `-application` parameter of the `security login` commands specifies the access method for a user account. For more information, see the `security login` man pages.

- Telnet must already be enabled in the management firewall policy that is used by the cluster or node management LIFs so that Telnet requests can go through the firewall.

By default, Telnet is disabled. The `system services firewall policy show` command with the `-service telnet` parameter displays whether Telnet has been enabled in a firewall policy. For more information, see the `system services firewall policy` man pages.

- If you use IPv6 connections, IPv6 must already be configured and enabled on the cluster, and firewall policies must already be configured with IPv6 addresses.

The `network options ipv6 show` command displays whether IPv6 is enabled. The `system services firewall policy show` command displays firewall policies.

About this task

- Telnet is not a secure protocol.

You should consider using SSH to access the cluster. SSH provides a secure remote shell and interactive network session.

- ONTAP supports a maximum of 50 concurrent Telnet sessions per node.

If the cluster management LIF resides on the node, it shares this limit with the node management LIF.

If the rate of in-coming connections is higher than 10 per second, the service is temporarily disabled for 60 seconds.

- If you want to access the ONTAP CLI from a Windows host, you can use a third-party utility such as

PuTTY.

Steps

1. From an administration host, enter the following command:

```
telnet hostname_or_IP
```

hostname_or_IP is the host name or the IP address of the cluster management LIF or a node management LIF. Using the cluster management LIF is recommended. You can use an IPv4 or IPv6 address.

Example of a Telnet request

The following example shows how the user named “joe”, who has been set up with Telnet access, can issue a Telnet request to access a cluster whose cluster management LIF is 10.72.137.28:

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

Access the cluster by using RSH

You can issue RSH requests to the cluster to perform administrative tasks. RSH is not a secure protocol and is disabled by default.

What you'll need

The following conditions must be met before you can use RSH to access the cluster:

- You must have a cluster local user account that is configured to use RSH as an access method.

The `-application` parameter of the `security login` commands specifies the access method for a user account. For more information, see the `security login` man pages.

- RSH must already be enabled in the management firewall policy that is used by the cluster or node management LIFs so that RSH requests can go through the firewall.

By default, RSH is disabled. The `system services firewall policy show` command with the `-service rsh` parameter displays whether RSH has been enabled in a firewall policy. For more information, see the `system services firewall policy` man pages.

- If you use IPv6 connections, IPv6 must already be configured and enabled on the cluster, and firewall policies must already be configured with IPv6 addresses.

The `network options ipv6 show` command displays whether IPv6 is enabled. The `system services firewall policy show` command displays firewall policies.

About this task

- RSH is not a secure protocol.

You should consider using SSH to access the cluster. SSH provides a secure remote shell and interactive network session.

- ONTAP supports a maximum of 50 concurrent RSH sessions per node.

If the cluster management LIF resides on the node, it shares this limit with the node management LIF.

If the rate of in-coming connections is higher than 10 per second, the service is temporarily disabled for 60 seconds.

Steps

1. From an administration host, enter the following command:

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

hostname_or_IP is the host name or the IP address of the cluster management LIF or a node management LIF. Using the cluster management LIF is recommended. You can use an IPv4 or IPv6 address.

command is the command you want to execute over RSH.

Example of an RSH request

The following example shows how the user named “joe”, who has been set up with RSH access, can issue an RSH request to run the `cluster show` command:

```
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$
```

Copyright information

Copyright © 2023 NetApp, Inc. All Rights Reserved. Printed in the U.S. No part of this document covered by copyright may be reproduced in any form or by any means—graphic, electronic, or mechanical, including photocopying, recording, taping, or storage in an electronic retrieval system—without prior written permission of the copyright owner.

Software derived from copyrighted NetApp material is subject to the following license and disclaimer:

THIS SOFTWARE IS PROVIDED BY NETAPP “AS IS” AND WITHOUT ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE, WHICH ARE HEREBY DISCLAIMED. IN NO EVENT SHALL NETAPP BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

NetApp reserves the right to change any products described herein at any time, and without notice. NetApp assumes no responsibility or liability arising from the use of products described herein, except as expressly agreed to in writing by NetApp. The use or purchase of this product does not convey a license under any patent rights, trademark rights, or any other intellectual property rights of NetApp.

The product described in this manual may be protected by one or more U.S. patents, foreign patents, or pending applications.

LIMITED RIGHTS LEGEND: Use, duplication, or disclosure by the government is subject to restrictions as set forth in subparagraph (b)(3) of the Rights in Technical Data -Noncommercial Items at DFARS 252.227-7013 (FEB 2014) and FAR 52.227-19 (DEC 2007).

Data contained herein pertains to a commercial product and/or commercial service (as defined in FAR 2.101) and is proprietary to NetApp, Inc. All NetApp technical data and computer software provided under this Agreement is commercial in nature and developed solely at private expense. The U.S. Government has a non-exclusive, non-transferrable, nonsublicensable, worldwide, limited irrevocable license to use the Data only in connection with and in support of the U.S. Government contract under which the Data was delivered. Except as provided herein, the Data may not be used, disclosed, reproduced, modified, performed, or displayed without the prior written approval of NetApp, Inc. United States Government license rights for the Department of Defense are limited to those rights identified in DFARS clause 252.227-7015(b) (FEB 2014).

Trademark information

NETAPP, the NETAPP logo, and the marks listed at <http://www.netapp.com/TM> are trademarks of NetApp, Inc. Other company and product names may be trademarks of their respective owners.