



Access the SP/BMC

ONTAP 9

NetApp
January 25, 2023

Table of Contents

- Access the SP/BMC 1
 - Accounts that can access the SP 1
 - Access the SP/BMC from an administration host 1
 - Access the SP/BMC from the system console 2
 - Relationship among the SP CLI, SP console, and system console sessions 3
 - Manage the IP addresses that can access the SP 4

Access the SP/BMC

Accounts that can access the SP

When you try to access the SP, you are prompted for credential. Cluster user accounts that are created with the `service-processor` application type have access to the SP CLI on any node of the cluster. SP user accounts are managed from ONTAP and authenticated by password. Beginning with ONTAP 9.9.1, SP user accounts must have the `admin` role.

User accounts for accessing the SP are managed from ONTAP instead of the SP CLI. A cluster user account can access the SP if it is created with the `-application` parameter of the `security login create` command set to `service-processor` and the `-authmethod` parameter set to `password`. The SP supports only password authentication.

You must specify the `-role` parameter when creating an SP user account.

- In ONTAP 9.9.1 and later releases, you must specify `admin` for the `-role` parameter, and any modifications to an account require the `admin` role. Other roles are no longer permitted for security reasons.
 - If you are upgrading to ONTAP 9.9.1 or later releases, see [Change in user accounts that can access the Service Processor](#).
 - If you are reverting to ONTAP 9.8 or earlier releases, see [Verify user accounts that can access the Service Processor](#).
- In ONTAP 9.8 and earlier releases, any role can access the SP, but `admin` is recommended.

By default, the cluster user account named “admin” includes the `service-processor` application type and has access to the SP.

ONTAP prevents you from creating user accounts with names that are reserved for the system (such as “root” and “naroot”). You cannot use a system-reserved name to access the cluster or the SP.

You can display current SP user accounts by using the `-application service-processor` parameter of the `security login show` command.

Access the SP/BMC from an administration host

You can log in to the SP of a node from an administration host to perform node management tasks remotely.

What you'll need

The following conditions must be met:

- The administration host you use to access the SP must support SSHv2.
- Your user account must already be set up for accessing the SP.

To access the SP, your user account must have been created with the `-application` parameter of the `security login create` command set to `service-processor` and the `-authmethod` parameter

set to password.



This task applies to both the SP and the BMC.

If the SP is configured to use an IPv4 or IPv6 address, and if five SSH login attempts from a host fail consecutively within 10 minutes, the SP rejects SSH login requests and suspends the communication with the IP address of the host for 15 minutes. The communication resumes after 15 minutes, and you can try to log in to the SP again.

ONTAP prevents you from creating or using system-reserved names (such as “root” and “naroot”) to access the cluster or the SP.

Steps

1. From the administration host, log in to the SP:

```
ssh username@SP_IP_address
```

2. When you are prompted, enter the password for `username`.

The SP prompt appears, indicating that you have access to the SP CLI.

Examples of SP access from an administration host

The following example shows how to log in to the SP with a user account `joe`, which has been set up to access the SP.

```
[admin_host]$ ssh joe@192.168.123.98
joe@192.168.123.98's password:
SP>
```

The following examples show how to use the IPv6 global address or IPv6 router-advertised address to log in to the SP on a node that has SSH set up for IPv6 and the SP configured for IPv6.

```
[admin_host]$ ssh joe@fd22:8b1e:b255:202::1234
joe@fd22:8b1e:b255:202::1234's password:
SP>
```

```
[admin_host]$ ssh joe@fd22:8b1e:b255:202:2a0:98ff:fe01:7d5b
joe@fd22:8b1e:b255:202:2a0:98ff:fe01:7d5b's password:
SP>
```

Access the SP/BMC from the system console

You can access the SP from the system console (also called *serial console*) to perform monitoring or troubleshooting tasks.

About this task

This task applies to both the SP and the BMC.

Steps

1. Access the SP CLI from the system console by pressing Ctrl-G at the prompt.
2. Log in to the SP CLI when you are prompted.

The SP prompt appears, indicating that you have access to the SP CLI.

3. Exit the SP CLI and return to the system console by pressing Ctrl-D, and then press Enter.

Example of accessing the SP CLI from the system console

The following example shows the result of pressing Ctrl-G from the system console to access the SP CLI. The `help system power` command is entered at the SP prompt, followed by pressing Ctrl-D and then Enter to return to the system console.

```
cluster1::>
```

(Press Ctrl-G to access the SP CLI.)

```
Switching console to Service Processor
Service Processor Login:
Password:
SP>
SP> help system power
system power cycle - power the system off, then on
system power off - power the system off
system power on - power the system on
system power status - print system power status
SP>
```

(Press Ctrl-D and then Enter to return to the system console.)

```
cluster1::>
```

Relationship among the SP CLI, SP console, and system console sessions

You can open an SP CLI session to manage a node remotely and open a separate SP console session to access the console of the node. The SP console session mirrors output displayed in a concurrent system console session. The SP and the system console have independent shell environments with independent login authentication.

Understanding how the SP CLI, SP console, and system console sessions are related helps you manage a node remotely. The following describes the relationship among the sessions:

- Only one administrator can log in to the SP CLI session at a time; however, the SP enables you to open both an SP CLI session and a separate SP console session simultaneously.

The SP CLI is indicated with the SP prompt (`SP>`). From an SP CLI session, you can use the `SP system console` command to initiate an SP console session. At the same time, you can start a separate SP CLI session through SSH. If you press Ctrl-D to exit from the SP console session, you automatically return to the SP CLI session. If an SP CLI session already exists, a message asks you whether to terminate the existing SP CLI session. If you enter “y”, the existing SP CLI session is terminated, enabling you to return from the SP console to the SP CLI. This action is recorded in the SP event log.

In an ONTAP CLI session that is connected through SSH, you can switch to the system console of a node by running the `ONTAP system node run-console` command from another node.

- For security reasons, the SP CLI session and the system console session have independent login authentication.

When you initiate an SP console session from the SP CLI (by using the `SP system console` command), you are prompted for the system console credential. When you access the SP CLI from a system console session (by pressing Ctrl-G), you are prompted for the SP CLI credential.

- The SP console session and the system console session have independent shell environments.

The SP console session mirrors output that is displayed in a concurrent system console session. However, the concurrent system console session does not mirror the SP console session.

The SP console session does not mirror output of concurrent SSH sessions.

Manage the IP addresses that can access the SP

By default, the SP accepts SSH connection requests from administration hosts of any IP addresses. You can configure the SP to accept SSH connection requests from only the administration hosts that have the IP addresses you specify. The changes you make apply to SSH access to the SP of any nodes in the cluster.

Steps

1. Grant SP access to only the IP addresses you specify by using the `system service-processor ssh add-allowed-addresses` command with the `-allowed-addresses` parameter.

- The value of the `-allowed-addresses` parameter must be specified in the format of `address/netmask`, and multiple `address/netmask` pairs must be separated by commas, for example, `10.98.150.10/24, fd20:8b1e:b255:c09b::/64`.

Setting the `-allowed-addresses` parameter to `0.0.0.0/0, ::/0` enables all IP addresses to access the SP (the default).

- When you change the default by limiting SP access to only the IP addresses you specify, ONTAP prompts you to confirm that you want the specified IP addresses to replace the “allow all” default setting (`0.0.0.0/0, ::/0`).
- The `system service-processor ssh show` command displays the IP addresses that can access the SP.

2. If you want to block a specified IP address from accessing the SP, use the `system service-processor`

ssh remove-allowed-addresses command with the -allowed-addresses parameter.

If you block all IP addresses from accessing the SP, the SP becomes inaccessible from any administration hosts.

Examples of managing the IP addresses that can access the SP

The following examples show the default setting for SSH access to the SP, change the default by limiting SP access to only the specified IP addresses, remove the specified IP addresses from the access list, and then restore SP access for all IP addresses:

```
cluster1::> system service-processor ssh show
Allowed Addresses: 0.0.0.0/0, ::/0

cluster1::> system service-processor ssh add-allowed-addresses -allowed
-addresses 192.168.1.202/24, 192.168.10.201/24

Warning: The default "allow all" setting (0.0.0.0/0, ::/0) will be
replaced
        with your changes. Do you want to continue? {y|n}: y

cluster1::> system service-processor ssh show
Allowed Addresses: 192.168.1.202/24, 192.168.10.201/24

cluster1::> system service-processor ssh remove-allowed-addresses -allowed
-addresses 192.168.1.202/24, 192.168.10.201/24

Warning: If all IP addresses are removed from the allowed address list,
all IP
        addresses will be denied access. To restore the "allow all"
default,
        use the "system service-processor ssh add-allowed-addresses
        -allowed-addresses 0.0.0.0/0, ::/0" command. Do you want to
continue?
        {y|n}: y

cluster1::> system service-processor ssh show
Allowed Addresses: -

cluster1::> system service-processor ssh add-allowed-addresses -allowed
-addresses 0.0.0.0/0, ::/0

cluster1::> system service-processor ssh show
Allowed Addresses: 0.0.0.0/0, ::/0
```

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.