

Manage a node remotely using the SP/BMC ONTAP 9

NetApp September 28, 2022

This PDF was generated from https://docs.netapp.com/us-en/ontap/system-admin/manage-node-remotely-sp-bmc-concept.html on September 28, 2022. Always check docs.netapp.com for the latest.

Table of Contents

Manage a node remotely using the SP/BMC	1
Manage a node remotely using the SP/BMC overview	1
About the SP	1
What the Baseboard Management Controller does	3
Configure the SP/BMC network	4
Methods of managing SP/BMC firmware updates	9
When the SP/BMC uses the network interface for firmware updates	11
Access the SP/BMC	11
Use online help at the SP/BMC CLI	16
Commands for managing a node remotely	18
About the threshold-based SP sensor readings and status values of the system sensors comma	ınd
output	23
About the discrete SP sensor status values of the system sensors command output	25
Commands for managing the SP from ONTAP	28
ONTAP commands for BMC management	32
BMC CLI commands	33

Manage a node remotely using the SP/BMC

Manage a node remotely using the SP/BMC overview

You can manage a node remotely using an onboard controller, called a Service Processor (SP) or Baseboard Management Controller (BMC). This remote management controller is included in all current platform models. The controller stays operational regardless of the operating state of the node.

The following platforms support BMC instead of SP:

- FAS 8700
- FAS 8300
- FAS27x0
- AFF A800
- AFF A700s
- AFF A400
- AFF A320
- AFF A220
- AFF C190

About the SP

The Service Processor (SP) is a remote management device that enables you to access, monitor, and troubleshoot a node remotely.

The key capabilities of the SP include the following:

• The SP enables you to access a node remotely to diagnose, shut down, power-cycle, or reboot the node, regardless of the state of the node controller.

The SP is powered by a standby voltage, which is available as long as the node has input power from at least one of its power supplies.

You can log in to the SP by using a Secure Shell client application from an administration host. You can then use the SP CLI to monitor and troubleshoot the node remotely. In addition, you can use the SP to access the serial console and run ONTAP commands remotely.

You can access the SP from the serial console or access the serial console from the SP. The SP enables you to open both an SP CLI session and a separate console session simultaneously.

For instance, when a temperature sensor becomes critically high or low, ONTAP triggers the SP to shut down the motherboard gracefully. The serial console becomes unresponsive, but you can still press Ctrl-G on the console to access the SP CLI. You can then use the system power on or system power cycle command from the SP to power on or power-cycle the node.

• The SP monitors environmental sensors and logs events to help you take timely and effective service actions.

The SP monitors environmental sensors such as the node temperatures, voltages, currents, and fan speeds. When an environmental sensor has reached an abnormal condition, the SP logs the abnormal readings, notifies ONTAP of the issue, and sends alerts and "down system" notifications as necessary through an AutoSupport message, regardless of whether the node can send AutoSupport messages.

The SP also logs events such as boot progress, Field Replaceable Unit (FRU) changes, events generated by ONTAP, and SP command history. You can manually invoke an AutoSupport message to include the SP log files that are collected from a specified node.

Other than generating these messages on behalf of a node that is down and attaching additional diagnostic information to AutoSupport messages, the SP has no effect on the AutoSupport functionality. The AutoSupport configuration settings and message content behavior are inherited from ONTAP.



The SP does not rely on the -transport parameter setting of the system node autosupport modify command to send notifications. The SP only uses the Simple Mail Transport Protocol (SMTP) and requires its host's AutoSupport configuration to include mail host information.

If SNMP is enabled, the SP generates SNMP traps to configured trap hosts for all "down system" events.

• The SP has a nonvolatile memory buffer that stores up to 4,000 events in a system event log (SEL) to help you diagnose issues.

The SEL stores each audit log entry as an audit event. It is stored in onboard flash memory on the SP. The event list from the SEL is automatically sent by the SP to specified recipients through an AutoSupport message.

The SEL contains the following information:

- Hardware events detected by the SP—for example, sensor status about power supplies, voltage, or other components
- Errors detected by the SP—for example, a communication error, a fan failure, or a memory or CPU error
- Critical software events sent to the SP by the node—for example, a panic, a communication failure, a
 boot failure, or a user-triggered "down system" as a result of issuing the SP system reset or
 system power cycle command
- The SP monitors the serial console regardless of whether administrators are logged in or connected to the console.

When messages are sent to the console, the SP stores them in the console log. The console log persists as long as the SP has power from either of the node power supplies. Because the SP operates with standby power, it remains available even when the node is power-cycled or turned off.

- Hardware-assisted takeover is available if the SP is configured.
- The SP API service enables ONTAP to communicate with the SP over the network.

The service enhances ONTAP management of the SP by supporting network-based functionality such as using the network interface for the SP firmware update, enabling a node to access another node's SP functionality or system console, and uploading the SP log from another node.

You can modify the configuration of the SP API service by changing the port the service uses, renewing the SSL and SSH certificates that are used by the service for internal communication, or disabling the service

entirely.

The following diagram illustrates access to ONTAP and the SP of a node. The SP interface is accessed through the Ethernet port (indicated by a wrench icon on the rear of the chassis):



What the Baseboard Management Controller does

Beginning with ONTAP 9.1, on certain hardware platforms, software is customized to support a new onboard controller in called the Baseboard Management Controller (BMC). The BMC has command-line interface (CLI) commands you can use to manage the device remotely.

The BMC works similarly to the Service Processor (SP) and uses many of the same commands. The BMC allows you to do the following:

- · Configure the BMC network settings.
- Access a node remotely and perform node management tasks such as diagnose, shut down, power-cycle, or reboot the node.

There are some differences between the SP and BMC:

- The BMC completely controls the environmental monitoring of power supply elements, cooling elements, temperature sensors, voltage sensors, and current sensors. The BMC reports sensor information to ONTAP through IPMI.
- Some of the high-availability (HA) and storage commands are different.
- The BMC does not send AutoSupport messages.

Automatic firmware updates are also available when running ONTAP 9.2 GA or later with the following requirements:

• BMC firmware revision 1.15 or later must be installed.



A manual update is required to upgrade BMC firmware from 1.12 to 1.15 or later.

• BMC automatically reboots after a firmware update is completed.



Node operations are not impacted during a BMC reboot.

Configure the SP/BMC network

Isolate management network traffic

It is a best practice to configure SP/BMC and the e0M management interface on a subnet dedicated to management traffic. Running data traffic over the management network can cause performance degradation and routing problems.

The management Ethernet port on most storage controllers (indicated by a wrench icon on the rear of the chassis) is connected to an internal Ethernet switch. The internal switch provides connectivity to SP/BMC and to the e0M management interface, which you can use to access the storage system via TCP/IP protocols like Telnet, SSH, and SNMP.



If you plan to use both the remote management device and e0M, you must configure them on the same IP subnet. Since these are low-bandwidth interfaces, the best practice is to configure SP/BMC and e0M on a subnet dedicated to management traffic.

If you cannot isolate management traffic, or if your dedicated management network is unusually large, you should try to keep the volume of network traffic as low as possible. Excessive ingress broadcast or multicast traffic may degrade SP/BMC performance.



Some storage controllers, such as the AFF A800, have two external ports, one for BMC and the other for e0M. For these controllers, there is no requirement to configure BMC and e0M on the same IP subnet.

Considerations for the SP/BMC network configuration

You can enable cluster-level, automatic network configuration for the SP (recommended). You can also leave the SP automatic network configuration disabled (the default) and manage the SP network configuration manually at the node level. A few considerations exist for each case.



This topic applies to both the SP and the BMC.

The SP automatic network configuration enables the SP to use address resources (including the IP address, subnet mask, and gateway address) from the specified subnet to set up its network automatically. With the SP automatic network configuration, you do not need to manually assign IP addresses for the SP of each node. By default, the SP automatic network configuration is disabled; this is because enabling the configuration requires that the subnet to be used for the configuration be defined in the cluster first.

If you enable the SP automatic network configuration, the following scenarios and considerations apply:

- If the SP has never been configured, the SP network is configured automatically based on the subnet specified for the SP automatic network configuration.
- If the SP was previously configured manually, or if the existing SP network configuration is based on a different subnet, the SP network of all nodes in the cluster are reconfigured based on the subnet that you specify in the SP automatic network configuration.

The reconfiguration could result in the SP being assigned a different address, which might have an impact on your DNS configuration and its ability to resolve SP host names. As a result, you might need to update your DNS configuration.

- A node that joins the cluster uses the specified subnet to configure its SP network automatically.
- The system service-processor network modify command does not enable you to change the SP IP address.

When the SP automatic network configuration is enabled, the command only allows you to enable or disable the SP network interface.

- If the SP automatic network configuration was previously enabled, disabling the SP network interface results in the assigned address resource being released and returned to the subnet.
- If you disable the SP network interface and then reenable it, the SP might be reconfigured with a different address.

If the SP automatic network configuration is disabled (the default), the following scenarios and considerations apply:

If the SP has never been configured, SP IPv4 network configuration defaults to using IPv4 DHCP, and IPv6 is disabled.

A node that joins the cluster also uses IPv4 DHCP for its SP network configuration by default.

• The system service-processor network modify command enables you to configure a node's SP IP address.

A warning message appears when you attempt to manually configure the SP network with addresses that are allocated to a subnet. Ignoring the warning and proceeding with the manual address assignment might result in a scenario with duplicate addresses.

If the SP automatic network configuration is disabled after having been enabled previously, the following scenarios and considerations apply:

- If the SP automatic network configuration has the IPv4 address family disabled, the SP IPv4 network defaults to using DHCP, and the system service-processor network modify command enables you to modify the SP IPv4 configuration for individual nodes.
- If the SP automatic network configuration has the IPv6 address family disabled, the SP IPv6 network is also disabled, and the system service-processor network modify command enables you to

enable and modify the SP IPv6 configuration for individual nodes.

Enable the SP/BMC automatic network configuration

Enabling the SP to use automatic network configuration is preferred over manually configuring the SP network. Because the SP automatic network configuration is cluster wide, you do not need to manually manage the SP network for individual nodes.



This task applies to both the SP and the BMC.

• The subnet you want to use for the SP automatic network configuration must already be defined in the cluster and must have no resource conflicts with the SP network interface.

The network subnet show command displays subnet information for the cluster.

The parameter that forces subnet association (the -force-update-lif-associations parameter of the network subnet commands) is supported only on network LIFs and not on the SP network interface.

• If you want to use IPv6 connections for the SP, IPv6 must already be configured and enabled for ONTAP.

The network options ipv6 show command displays the current state of IPv6 settings for ONTAP.

Steps

- 1. Specify the IPv4 or IPv6 address family and name for the subnet that you want the SP to use by using the system service-processor network auto-configuration enable command.
- 2. Display the SP automatic network configuration by using the system service-processor network auto-configuration show command.
- 3. If you subsequently want to disable or reenable the SP IPv4 or IPv6 network interface for all nodes that are in quorum, use the system service-processor network modify command with the -address -family [IPv4|IPv6] and -enable [true|false] parameters.

When the SP automatic network configuration is enabled, you cannot modify the SP IP address for a node that is in quorum. You can only enable or disable the SP IPv4 or IPv6 network interface.

If a node is out of quorum, you can modify the node's SP network configuration, including the SP IP address, by running system service-processor network modify from the node and confirming that you want to override the SP automatic network configuration for the node. However, when the node joins the quorum, the SP automatic reconfiguration takes place for the node based on the specified subnet.

Configure the SP/BMC network manually

If you do not have automatic network configuration set up for the SP, you must manually configure a node's SP network for the SP to be accessible by using an IP address.

What you'll need

If you want to use IPv6 connections for the SP, IPv6 must already be configured and enabled for ONTAP. The network options ipv6 commands manage IPv6 settings for ONTAP.



This task applies to both the SP and the BMC.

You can configure the SP to use IPv4, IPv6, or both. The SP IPv4 configuration supports static and DHCP addressing, and the SP IPv6 configuration supports static addressing only.

If the SP automatic network configuration has been set up, you do not need to manually configure the SP network for individual nodes, and the system service-processor network modify command allows you to only enable or disable the SP network interface.

Steps

- 1. Configure the SP network for a node by using the system service-processor network modify command.
 - The -address-family parameter specifies whether the IPv4 or IPv6 configuration of the SP is to be modified.
 - The -enable parameter enables the network interface of the specified IP address family.
 - The -dhcp parameter specifies whether to use the network configuration from the DHCP server or the network address that you provide.

You can enable DHCP (by setting -dhcp to v4) only if you are using IPv4. You cannot enable DHCP for IPv6 configurations.

• The -ip-address parameter specifies the public IP address for the SP.

A warning message appears when you attempt to manually configure the SP network with addresses that are allocated to a subnet. Ignoring the warning and proceeding with the manual address assignment might result in a duplicate address assignment.

- The -netmask parameter specifies the netmask for the SP (if using IPv4.)
- The -prefix-length parameter specifies the network prefix-length of the subnet mask for the SP (if using IPv6.)
- The -gateway parameter specifies the gateway IP address for the SP.
- 2. Configure the SP network for the remaining nodes in the cluster by repeating the step 1.
- 3. Display the SP network configuration and verify the SP setup status by using the system service-processor network show command with the -instance or -field setup-status parameters.

The SP setup status for a node can be one of the following:

- ° not-setup Not configured
- ° succeeded Configuration succeeded
- ° in-progress Configuration in progress
- ° failed Configuration failed

Example of configuring the SP network

The following example configures the SP of a node to use IPv4, enables the SP, and displays the SP network configuration to verify the settings:

```
cluster1::> system service-processor network modify -node local
-address-family IPv4 -enable true -ip-address 192.168.123.98
-netmask 255.255.255.0 -gateway 192.168.123.1
cluster1::> system service-processor network show -instance -node local
                               Node: node1
                       Address Type: IPv4
                  Interface Enabled: true
                     Type of Device: SP
                             Status: online
                        Link Status: up
                        DHCP Status: none
                         IP Address: 192.168.123.98
                        MAC Address: ab:cd:ef:fe:ed:02
                            Netmask: 255.255.255.0
       Prefix Length of Subnet Mask: -
         Router Assigned IP Address: -
              Link Local IP Address: -
                 Gateway IP Address: 192.168.123.1
                  Time Last Updated: Thu Apr 10 17:02:13 UTC 2014
                        Subnet Name: -
Enable IPv6 Router Assigned Address: -
            SP Network Setup Status: succeeded
    SP Network Setup Failure Reason: -
1 entries were displayed.
cluster1::>
```

Modify the SP API service configuration

The SP API is a secure network API that enables ONTAP to communicate with the SP over the network. You can change the port used by the SP API service, renew the certificates the service uses for internal communication, or disable the service entirely. You need to modify the configuration only in rare situations.

About this task

• The SP API service uses port 50000 by default.

You can change the port value if, for example, you are in a network setting where port 50000 is used for communication by another networking application, or you want to differentiate between traffic from other applications and traffic generated by the SP API service.

• The SSL and SSH certificates used by the SP API service are internal to the cluster and not distributed externally.

In the unlikely event that the certificates are compromised, you can renew them.

• The SP API service is enabled by default.

You only need to disable the SP API service in rare situations, such as in a private LAN where the SP is not configured or used and you want to disable the service.

If the SP API service is disabled, the API does not accept any incoming connections. In addition, functionality such as network-based SP firmware updates and network-based SP "down system" log collection becomes unavailable. The system switches to using the serial interface.

Steps

- 1. Switch to the advanced privilege level by using the set -privilege advanced command.
- 2. Modify the SP API service configuration:

If you want to	Use the following command
Change the port used by the SP API service	system service-processor api-service modify with the -port {4915265535} parameter
Renew the SSL and SSH certificates used by the SP API service for internal communication	 For ONTAP 9.5 or later use system service-processor api-service renewinternal-certificate For ONTAP 9.4 and earlier use system service-processor api-service renew-certificates If no parameter is specified, only the host certificates (including the client and server certificates) are renewed. If the -renew-all true parameter is specified, both the host certificates and the root CA certificate are renewed.
comm	
Disable or reenable the SP API service	system service-processor api-service modify with the -is-enabled {true false} parameter

3. Display the SP API service configuration by using the system service-processor api-service show command.

Methods of managing SP/BMC firmware updates

ONTAP includes an SP firmware image that is called the *baseline image*. If a new version of the SP firmware becomes subsequently available, you have the option to download it

and update the SP firmware to the downloaded version without upgrading the ONTAP version.



This topic applies to both the SP and the BMC.

ONTAP offers the following methods for managing SP firmware updates:

- The SP automatic update functionality is enabled by default, allowing the SP firmware to be automatically updated in the following scenarios:
 - When you upgrade to a new version of ONTAP

The ONTAP upgrade process automatically includes the SP firmware update, provided that the SP firmware version bundled with ONTAP is newer than the SP version running on the node.



ONTAP detects a failed SP automatic update and triggers a corrective action to retry the SP automatic update up to three times. If all three retries fail, see the Knowledge Base article xref:./system-admin/ Health Monitor SPAutoUpgradeFailedMajorAlert SP upgrade fails - AutoSupport Message.

- When you download a version of the SP firmware from the NetApp Support Site and the downloaded version is newer than the one that the SP is currently running
- When you downgrade or revert to an earlier version of ONTAP

The SP firmware is automatically updated to the newest compatible version that is supported by the ONTAP version you reverted or downgraded to. A manual SP firmware update is not required.

You have the option to disable the SP automatic update functionality by using the <code>system service-processor image modify</code> command. However, it is recommended that you leave the functionality enabled. Disabling the functionality can result in suboptimal or nonqualified combinations between the ONTAP image and the SP firmware image.

• ONTAP enables you to trigger an SP update manually and specify how the update should take place by using the system service-processor image update command.

You can specify the following options:

The SP firmware package to use (-package)

You can update the SP firmware to a downloaded package by specifying the package file name. The advance system image package show command displays all package files (including the files for the SP firmware package) that are available on a node.

• Whether to use the baseline SP firmware package for the SP update (-baseline)

You can update the SP firmware to the baseline version that is bundled with the currently running version of ONTAP.



If you use some of the more advanced update options or parameters, the BMC's configuration settings may be temporarily cleared. After reboot, it can take up to 10 minutes for ONTAP to restore the BMC configuration.

• ONTAP enables you to display the status for the latest SP firmware update triggered from ONTAP by using the system service-processor image update-progress show command.

Any existing connection to the SP is terminated when the SP firmware is being updated. This is the case whether the SP firmware update is automatically or manually triggered.

Related information

NetApp Downloads: System Firmware and Diagnostics

When the SP/BMC uses the network interface for firmware updates

An SP firmware update that is triggered from ONTAP with the SP running version 1.5, 2.5, 3.1, or later supports using an IP-based file transfer mechanism over the SP network interface.



This topic applies to both the SP and the BMC.

An SP firmware update over the network interface is faster than an update over the serial interface. It reduces the maintenance window during which the SP firmware is being updated, and it is also nondisruptive to ONTAP operation. The SP versions that support this capability are included with ONTAP. They are also available on the NetApp Support Site and can be installed on controllers that are running a compatible version of ONTAP.

When you are running SP version 1.5, 2.5, 3.1, or later, the following firmware upgrade behaviors apply:

- An SP firmware update that is *automatically* triggered by ONTAP defaults to using the network interface for the update; however, the SP automatic update switches to using the serial interface for the firmware update if one of the following conditions occurs:
 - The SP network interface is not configured or not available.
 - The IP-based file transfer fails.
 - The SP API service is disabled.

Regardless of the SP version you are running, an SP firmware update triggered from the SP CLI always uses the SP network interface for the update.

Related information

NetApp Downloads: System Firmware and Diagnostics

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 <code>-application</code> parameter of the <code>security login create</code> command set to <code>service-processor</code> and the <code>-authmethod</code> parameter set to <code>password</code>. 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 <code>-application</code> parameter of the security <code>login</code> create command set to <code>service-processor</code> and the <code>-authmethod</code> parameter set to <code>password</code>.



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 \mid 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
```

Use online help at the SP/BMC CLI

The online help displays the SP/BMC CLI commands and options.

About this task

This task applies to both the SP and the BMC.

Steps

1. To display help information for the SP/BMC commands, enter the following:

To access SP help	To access BMC help
Type help at the SP prompt.	Type system at the BMC prompt.

The following example shows the SP CLI online help.

```
SP> help
date - print date and time
exit - exit from the SP command line interface
events - print system events and event information
help - print command help
priv - show and set user mode
sp - commands to control the SP
system - commands to control the system
version - print SP version
```

The following example shows the BMC CLI online help.

```
BMC> system
system acp - acp related commands
system battery - battery related commands
system console - connect to the system console
system core - dump the system core and reset
system cpld - cpld commands
system log - print system console logs
system power - commands controlling system power
system reset - reset the system using the selected firmware
system sensors - print environmental sensors status
system service-event - print service-event status
system fru - fru related commands
system watchdog - system watchdog commands

BMC>
```

To display help information for the option of an SP/BMC command, enter help before or after the SP/BMC command.

The following example shows the SP CLI online help for the SP events command.

```
SP> help events
events all - print all system events
events info - print system event log information
events newest - print newest system events
events oldest - print oldest system events
events search - search for and print system events
```

The following example shows the BMC CLI online help for the BMC system power command.

```
BMC> system power help
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

BMC>
```

Commands for managing a node remotely

You can manage a node remotely by accessing its SP and running SP CLI commands to perform node-management tasks. For several commonly performed remote node-management tasks, you can also use ONTAP commands from another node in the cluster. Some SP commands are platform-specific and might not be available on your platform.

If you want to	Use this SP command	Use this BMC command	Or this ONTAP command
Display available SP commands or subcommands of a specified SP command	help[command]		
Display the current privilege level for the SP CLI	priv show		
Set the privilege level to access the specified mode for the SP CLI	<pre>priv set {admin advanced diag}</pre>		
Display system date and time	date		date

If you want to	Use this SP command	Use this BMC command	Or this ONTAP command
Display events that are logged by the SP	events {all info newest number oldest number search keyword}		
Display SP status and network configuration information	sp status [-v -d] The -v option displays SP statistics in verbose form. The -d option adds the SP debug log to the display.	bmc status [-v -d] The -v option displays SP statistics in verbose form. The -d option adds the SP debug log to the display.	system service- processor show
Display the length of time the SP has been up and the average number of jobs in the run queue over the last 1, 5, and 15 minutes	sp uptime	bmc uptime	
Display system console logs	system log		
Display the SP log archives or the files in an archive	<pre>sp log history show [-archive {latest all archive-name}][-dump {all file- name}]</pre>	<pre>bmc log history show[-archive {latest all archive-name}][-dump {all file-name}]</pre>	
Display the power status for the controller of a node	system power status		system node power show
Display battery information	system battery show		
Display ACP information or the status for expander sensors	system acp[show sensors show]		
List all system FRUs and their IDs	system fru list		
Display product information for the specified FRU	system fru show fru_id		

If you want to	Use this SP command	Use this BMC command	Or this ONTAP command
Display the FRU data history log	system fru log show (advanced privilege level)		
Display the status for the environmental sensors, including their states and current values	system sensors or system sensors show		system node environment sensors show
Display the status and details for the specified sensor	system sensors get sensor_name You can obtain sensor_name by using the system sensors or the system sensors show command.		
Display the SP firmware version information	version		system service- processor image show
Display the SP command history	sp log audit (advanced privilege level)	bmc log audit	
Display the SP debug information	sp log debug (advanced privilege level)	bmc log debug (advanced privilege level)	
Display the SP messages file	sp log messages (advanced privilege level)	bmc log messages (advanced privilege level)	
Display the settings for collecting system forensics on a watchdog reset event, display system forensics information collected during a watchdog reset event, or clear the collected system forensics information	system forensics [show log dump log clear]		
Log in to the system console	system console		system node run- console
	You should press Ctrl-D to	exit the system console ses	sion.

If you want to	Use this SP command	Use this BMC command	Or this ONTAP command
Turn the node on or off, or perform a power-cycle (turning the power off and then back on)	system power on		system node power on (advanced privilege level)
	system power off		
	system power cycle		
	Using these concause an improshutdown) and	on to keep the SP running wing use occurs before power is to the second of the node (I is not a substitute for a gradem node halt command.	turned back on. r-cycle the node might also called a <i>dirty</i>
Create a core dump and reset the node	system core [-f] The -f option forces the creation of a core dump and the reset of the node.		system node coredump trigger (advanced privilege level)
	(NMI) button on a node, ca of the core files when haltin ONTAP on the node is hun node shutdown. The ger the system node cored	e same effect as pressing the using a dirty shutdown of the ng the node. These commands or does not respond to concreted core dump files are always show command. The state node is not interrupted.	e node and forcing a dump nds are helpful when mmands such as system displayed in the output of
Reboot the node with an optionally specified BIOS firmware image (primary, backup, or current) to recover from issues such as a corrupted image of the node's boot device	<pre>system reset {primary backup current}</pre>		system node reset with the -firmware {primary backup current} parameter(advanced privilege level) system node reset
		causes a dirty shutdown of	
		is specified, the current ima as long as the input power to	

If you want to	Use this SP command	Use this BMC command	Or this ONTAP command
Display the status of battery firmware automatic update, or enable or disable battery firmware automatic update upon next SP boot	system battery auto_update[status enable disable] (advanced privilege level)		
Compare the current battery firmware image against a specified firmware image	system battery verify [image_URL] (advanced privilege level) If image_URL is not specified, the default battery firmware image is used for comparison.		
Update the battery firmware from the image at the specified location	system battery flash image_URL (advanced privilege level) You use this command if the automatic battery firmware upgrade process has failed for some reason.		
Update the SP firmware by using the image at the specified location	sp update image_URL image_URL must not exceed 200 characters.	bmc update image_URL image_URL must not exceed 200 characters.	system service- processor image update
Reboot the SP	sp reboot		system service- processor reboot-sp
Erase the NVRAM flash content	system nvram flash clear (advanced privilege level) This command cannot be initiated when the controller power is off (system power off).		
Exit the SP CLI	exit		

About the threshold-based SP sensor readings and status values of the system sensors command output

Threshold-based sensors take periodic readings of a variety of system components. The SP compares the reading of a threshold-based sensor against its preset threshold limits that define a component's acceptable operating conditions.

Based on the sensor reading, the SP displays the sensor state to help you monitor the condition of the component.

Examples of threshold-based sensors include sensors for the system temperatures, voltages, currents, and fan speeds. The specific list of threshold-based sensors depends on the platform.

Threshold-based sensors have the following thresholds, displayed in the output of the SP system sensors command:

- Lower critical (LCR)
- Lower noncritical (LNC)
- Upper noncritical (UNC)
- Upper critical (UCR)

A sensor reading between LNC and LCR or between UNC and UCR means that the component is showing signs of a problem and a system failure might occur as a result. Therefore, you should plan for component service soon.

A sensor reading below LCR or above UCR means that the component is malfunctioning and a system failure is about to occur. Therefore, the component requires immediate attention.

The following diagram illustrates the severity ranges that are specified by the thresholds:



You can find the reading of a threshold-based sensor under the Current column in the system sensors command output. The system sensors get sensor_name command displays additional details for the specified sensor. As the reading of a threshold-based sensor crosses the noncritical and critical threshold ranges, the sensor reports a problem of increasing severity. When the reading exceeds a threshold limit, the sensor's status in the system sensors command output changes from ok to nc (noncritical) or cr (critical) depending on the exceeded threshold, and an event message is logged in the SEL event log.

Some threshold-based sensors do not have all four threshold levels. For those sensors, the missing thresholds show na as their limits in the system sensors command output, indicating that the particular sensor has no limit or severity concern for the given threshold and the SP does not monitor the sensor for that threshold.

Example of the system sensors command output

The following example shows some of the information displayed by the system sensors command in the SP CLI:

Sensor Name Current	1	IIni+	1	C+ 2+110	T CD	1	TNC
UNC UCR	1	OHIL	ı	Status	LCK	1	LINC
	+-		-+-	+		-+	
CPU0_Temp_Margin -55.000		degrees C	-	ok	na		na
-5.000 0.000							
CPU1_Temp_Margin -56.000		degrees C		ok	na		na
-5.000	1	do amondo a		-1-	0 000		10 000
In_Flow_Temp 32.000 42.000 52.000		degrees C	ı	OK	0.000	-	10.000
Out Flow Temp 38.000		dearees C	ı	ok	0.000	ı	10.000
59.000 68.000		4091000 0		012	J. 550	1	10.000
CPU1 Error 0x0		discrete		0x0180	na		na
na na							
CPU1_Therm_Trip 0x0		discrete		0x0180	na		na
na na							
CPU1_Hot 0x0		discrete		0x0180	na		na
na na		_		_			
IO_Mid1_Temp 30.000		degrees C		ok	0.000		10.000
55.000 64.000		dogmood C		م ا -	0 000		10.000
IO_Mid2_Temp 30.000 55.000 64.000		degrees C	ı	OK	0.000	١	10.000
CPU VTT 1.106		Volts	I	ok	1.028	ı	1.048
1.154 1.174					0		
CPU0_VCC 1.154		Volts		ok	0.834		0.844
1.348 1.368							
3.3V 3.323	- 1	Volts		ok	3.053	-	3.116
3.466 3.546							
5V 5.002		Volts		ok	4.368	-	4.465
5.490 5.636							. = 0 =
STBY_1.8V 1.794		Volts		ok	1.678		1.707
1.892 1.911							

Example of the system sensors sensor_name command output for a threshold-based sensor

The following example shows the result of entering system sensors get sensor_name in the SP CLI for the threshold-based sensor 5V:

```
SP node1> system sensors get 5V
Locating sensor record...
              : 5V (0x13)
Sensor ID
Entity ID
                   : 7.97
Sensor Type (Analog) : Voltage
Sensor Reading : 5.002 (+/- 0) Volts
Status
                   : ok
Lower Non-Recoverable : na
Lower Critical : 4.246
Lower Non-Critical : 4.490
                   : 5.490
Upper Non-Critical
Upper Critical : 5.758
Upper Non-Recoverable : na
Assertion Events
Assertions Enabled : lnc-lcr-ucr+
Deassertions Enabled : lnc-lcr-ucr+
```

About the discrete SP sensor status values of the system sensors command output

Discrete sensors do not have thresholds. Their readings, displayed under the Current column in the SP CLI system sensors command output, do not carry actual meanings and thus are ignored by the SP. The Status column in the system sensors command output displays the status values of discrete sensors in hexadecimal format.

Examples of discrete sensors include sensors for the fan, power supply unit (PSU) fault, and system fault. The specific list of discrete sensors depends on the platform.

You can use the SP CLI system sensors get sensor_name command for help with interpreting the status values for most discrete sensors. The following examples show the results of entering system sensors get sensor name for the discrete sensors CPU0 Error and IO Slot1 Present:

```
SP node1> system sensors get CPU0_Error
Locating sensor record...

Sensor ID : CPU0_Error (0x67)

Entity ID : 7.97

Sensor Type (Discrete): Temperature

States Asserted : Digital State

[State Deasserted]
```

SP node1> system sensors get IO Slot1 Present

Locating sensor record...

Sensor ID : IO Slot1 Present (0x74)

Entity ID : 11.97

Sensor Type (Discrete): Add-in Card

States Asserted : Availability State

[Device Present]

Although the system sensors get sensor_name command displays the status information for most discrete sensors, it does not provide status information for the System_FW_Status, System_Watchdog, PSU1_Input_Type, and PSU2_Input_Type discrete sensors. You can use the following information to interpret these sensors' status values.

System_FW_Status

The System_FW_Status sensor's condition appears in the form of <code>0xAABB</code>. You can combine the information of <code>AA</code> and <code>BB</code> to determine the condition of the sensor.

AA can have one of the following values:

Values	Condition of the sensor
01	System firmware error
02	System firmware hang
04	System firmware progress

BB can have one of the following values:

Values	Condition of the sensor
00	System software has properly shut down
01	Memory initialization in progress
02	NVMEM initialization in progress (when NVMEM is present)
04	Restoring memory controller hub (MCH) values (when NVMEM is present)
05	User has entered Setup
13	Booting the operating system or LOADER

Values	Condition of the sensor
1F	BIOS is starting up
20	LOADER is running
21	LOADER is programming the primary BIOS firmware. You must not power down the system.
22	LOADER is programming the alternate BIOS firmware. You must not power down the system.
2F	ONTAP is running
60	SP has powered off the system
61	SP has powered on the system
62	SP has reset the system
63	SP watchdog power cycle
64	SP watchdog cold reset

For instance, the System_FW_Status sensor status 0x042F means "system firmware progress (04), ONTAP is running (2F)."

System_Watchdog

The System_Watchdog sensor can have one of the following conditions:

• 0x0080

The state of this sensor has not changed

Values	Condition of the sensor
0x0081	Timer interrupt
0x0180	Timer expired
0x0280	Hard reset
0x0480	Power down
0x0880	Power cycle

For instance, the System_Watchdog sensor status 0x0880 means a watchdog timeout occurs and causes a system power cycle.

PSU1_Input_Type and PSU2_Input_Type

For direct current (DC) power supplies, the PSU1_Input_Type and PSU2_Input_Type sensors do not apply. For alternating current (AC) power supplies, the sensors' status can have one of the following values:

Values	Condition of the sensor
0x01 xx	220V PSU type
0x02 xx	110V PSU type

For instance, the PSU1_Input_Type sensor status 0x0280 means that the sensor reports that the PSU type is 110V.

Commands for managing the SP from ONTAP

ONTAP provides commands for managing the SP, including the SP network configuration, SP firmware image, SSH access to the SP, and general SP administration.

Commands for managing the SP network configuration

If you want to	Run this ONTAP command
Enable the SP automatic network configuration for the SP to use the IPv4 or IPv6 address family of the specified subnet	system service-processor network auto- configuration enable
Disable the SP automatic network configuration for the IPv4 or IPv6 address family of the subnet specified for the SP	system service-processor network auto- configuration disable
Display the SP automatic network configuration	system service-processor network auto- configuration show

If you want to	Run this ONTAP command
Manually configure the SP network for a node, including the following:	system service-processor network modify
The IP address family (IPv4 or IPv6)	
Whether the network interface of the specified IP address family should be enabled	
 If you are using IPv4, whether to use the network configuration from the DHCP server or the network address that you specify 	
The public IP address for the SP	
The netmask for the SP (if using IPv4)	
 The network prefix-length of the subnet mask for the SP (if using IPv6) 	
The gateway IP address for the SP	
Display the SP network configuration, including the following:	system service-processor network show
 The configured address family (IPv4 or IPv6) and whether it is enabled 	Displaying complete SP network details requires the -instance parameter.
The remote management device type	
The current SP status and link status	
 Network configuration, such as IP address, MAC address, netmask, prefix-length of subnet mask, router-assigned IP address, link local IP address, and gateway IP address 	
The time the SP was last updated	
The name of the subnet used for SP automatic configuration	
 Whether the IPv6 router-assigned IP address is enabled 	
SP network setup status	
Reason for the SP network setup failure	
Modify the SP API service configuration, including the following:	system service-processor api-service modify
Changing the port used by the SP API service	(advanced privilege level)
Enabling or disabling the SP API service	

If you want to	Run this ONTAP command
Display the SP API service configuration	system service-processor api-service show (advanced privilege level)
Renew the SSL and SSH certificates used by the SP API service for internal communication	• For ONTAP 9.5 or later: system service- processor api-service renew-internal- certificates
	• For ONTAP 9.4 or earlier: system service- processor api-service renew- certificates
	(advanced privilege level)

Commands for managing the SP firmware image

If you want to	Run this ONTAP command
Display the details of the currently installed SP firmware image, including the following: • The remote management device type • The image (primary or backup) that the SP is booted from, its status, and firmware version • Whether the firmware automatic update is enabled and the last update status	System service-processor image show The -is-current parameter indicates the image (primary or backup) that the SP is currently booted from, not if the installed firmware version is most current.
Enable or disable the SP automatic firmware update	By default, the SP firmware is automatically updated with the update of ONTAP or when a new version of the SP firmware is manually downloaded. Disabling the automatic update is not recommended because doing so can result in suboptimal or nonqualified combinations between the ONTAP image and the SP firmware image.

If you want to	Run this ONT	AP command
Manually download an SP firmware image on a node	system node image get	
	im pri	efore you run the system node nage commands, you must set the ivilege level to advanced (set privilege advanced), entering you nen prompted to continue.
	do not need to unless you waı	are image is packaged with ONTAP. You download the SP firmware manually, nt to use an SP firmware version that is the one packaged with ONTAP.
Display the status for the latest SP firmware update triggered from ONTAP, including the following information:	system serv progress sh	vice-processor image update- now
The start and end time for the latest SP firmware update		
Whether an update is in progress and the percentage that is complete		

Commands for managing SSH access to the SP

If you want to	Run this ONTAP command
Grant SP access to only the specified IP addresses	system service-processor ssh add- allowed-addresses
Block the specified IP addresses from accessing the SP	system service-processor ssh remove- allowed-addresses
Display the IP addresses that can access the SP	system service-processor ssh show

Commands for general SP administration

If you want to	Run this ONTAP command
Display general SP information, including the following:	system service-processor show Displaying complete SP information requires the -instance parameter.
The remote management device type	parameter.
The current SP status	
 Whether the SP network is configured 	
 Network information, such as the public IP address and the MAC address 	
The SP firmware version and Intelligent Platform Management Interface (IPMI) version	
Whether the SP firmware automatic update is enabled	
Reboot the SP on a node	system service-processor reboot-sp
Generate and send an AutoSupport message that includes the SP log files collected from a specified node	system node autosupport invoke-splog
Display the allocation map of the collected SP log files in the cluster, including the sequence numbers for the SP log files that reside in each collecting node	system service-processor log show- allocations

Related information

ONTAP 9 Commands

ONTAP commands for BMC management

These ONTAP commands are supported on the Baseboard Management Controller (BMC).

The BMC uses some of the same commands as the Service Processor (SP). The following SP commands are supported on the BMC.

If you want to	Use this command
Display the BMC information	system service-processor show
Display/modify the BMC network configuration	system service-processor network show/modify
Reset the BMC	system service-processor reboot-sp

If you want to	Use this command
Display/modify the details of the currently installed BMC firmware image	<pre>system service-processor image show/modify</pre>
Update BMC firmware	system service-processor image update
Display the status for the latest BMC firmware update	system service-processor image update- progress show
Enable the automatic network configuration for the BMC to use an IPv4 or IPv6 address on the specified subnet	system service-processor network auto- configuration enable
Disable the automatic network configuration for an IPv4 or IPv6 address on the subnet specified for the BMC	system service-processor network auto- configuration disable
Display the BMC automatic network configuration	system service-processor network auto- configuration show

For commands that are not supported by the BMC firmware, the following error message is returned.

::> Error: Command not supported on this platform.

BMC CLI commands

You can log into the BMC using SSH. The following commands are supported from the BMC command line.

Command	Function
system	Display a list of all commands.
system console	Connect to the system's console. Use Ctrl+D to exit the session.
system core	Dump the system core and reset.
system power cycle	Power the system off, then on.
system power off	Power the system off.
system power on	Power the system on.

Command	Function
system power status	Print system power status.
system reset	Reset the system.
system log	Print system console logs
system fru show [id]	Dump all/selected field replaceable unit (FRU) info.

Copyright Information

Copyright © 2022 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.

RESTRICTED RIGHTS LEGEND: Use, duplication, or disclosure by the government is subject to restrictions as set forth in subparagraph (c)(1)(ii) of the Rights in Technical Data and Computer Software clause at DFARS 252.277-7103 (October 1988) and FAR 52-227-19 (June 1987).

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.