Server Utilities

This chapter includes the following sections:

Exporting Technical Support Data

Perform this task when requested by the Cisco Technical Assistance Center (TAC). This utility creates a summary report containing configuration information, logs and diagnostic data that will help TAC in troubleshooting and resolving a technical issue.

Important If any firmware or BIOS updates are in progress, do not export the technical support data until those tasks are complete.

SUMMARY STEPS

1. Server # **scope chassis**
2. Server /chassis # **scope tech-support**
3. Server /chassis/tech-support # **set collect-from** {**all** | **cmc** | **peercmc** | **bmc1** | **bmc2**}
4. Server /chassis/tech-support # **set remote-ip** *ip-address*
5. Server /chassis/tech-support # **set remote-path** *path/filename*
6. Server /chassis/tech-support # **set remote-protocol** *protocol*
7. Server /chassis/tech-support # **set remote-username** *name*
8. Server /chassis/tech-support # **set remote-password** *password*

9. Server /chassis/tech-support # **commit**
10. Server /chassis/tech-support # **start**
11. (Optional) Server /chassis/tech-support # **show detail**
12. (Optional) Server /chassis/tech-support # **cancel**

DETAILED STEPS

	Command or Action	Purpose
Step 1	Server # **scope chassis**	Enters chassis command mode.
Step 2	Server /chassis # **scope tech-support**	Enters the tech-support command mode.
Step 3	Server /chassis/tech-support # **set collect-from** {**all** | **cmc** | **peercmc** | **bmc1** | **bmc2**}	Specifies the component for which the technical support data has to be exported.
Step 4	Server /chassis/tech-support # **set remote-ip** *ip-address*	Specifies the IP address of the remote server on which the technical support data file should be stored.
Step 5	Server /chassis/tech-support # **set remote-path** *path/filename*	Specifies the file name in which the support data should be stored on the remote server. When you enter this name, include the relative path for the file from the top of the server tree to the desired location. **Tip** To have the system auto-generate the file name, enter the file name as `default.tar.gz`.
Step 6	Server /chassis/tech-support # **set remote-protocol** *protocol*	Specifies the protocol to connect to the remote server. It can be of the following types: • TFTP • FTP • SFTP • SCP • HTTP

	Command or Action	Purpose
		Note The Cisco UCS C-Series server now supports fingerprint confirmation of the server when you update firmware through a remote server. This option is available only if you choose SCP or SFTP as the remote server type. If you chose SCP or SFTP as the remote server type while performing this action, a prompt with the message Server (RSA) key fingerprint is <server_finger_print _ID> Do you wish to continue? Click y or n depending on the authenticity of the server fingerprint. The fingerprint is based on the host's public key and helps you to identify or verify the host you are connecting to.
Step 7	Server /chassis/tech-support # **set remote-username** *name*	Specifies the user name on the remote server on which the technical support data file should be stored. This field does not apply if the protocol is TFTP or HTTP.
Step 8	Server /chassis/tech-support # **set remote-password** *password*	Specifies the password on the remote server on which the technical support data file should be stored. This field does not apply if the protocol is TFTP or HTTP.
Step 9	Server /chassis/tech-support # **commit**	Commits the transaction to the system configuration.
Step 10	Server /chassis/tech-support # **start**	Begins the transfer of the data file to the remote server.
Step 11	(Optional) Server /chassis/tech-support # **show detail**	Displays the progress of the transfer of the data file to the remote server.
Step 12	(Optional) Server /chassis/tech-support # **cancel**	Cancels the transfer of the data file to the remote server.

Example

This example creates a technical support data file and transfers the file to a TFTP server:

```
Server# scope chassis
Server /chassis # scope tech-support
Server /chassis/tech-support # set collect-from all
Server /chassis/tech-support* # set remote-ip 192.0.20.41
Server /chassis/tech-support* # set remote-protocol tftp
Server /chassis/tech-support *# set remote-path /user/user1/default.tar.gz
Server /chassis/tech-support *# commit
Server /chassis/tech-support # start
Tech Support upload started.

Server /chassis/tech-support # show detail

Tech Support:
 Server Address: 192.0.20.41
    Path('default' for auto-naming): default.tar.gz
    Protocol: tftp
    Username:
    Password: ******
    Collect from: all
    Progress(%): 100
    Status: COMPLETED

Server /chassis/tech-support #
```

What to do next

Provide the generated report file to Cisco TAC.

Rebooting the Cisco IMC

On rare occasions, such as an issue with the current running firmware, troubleshooting a server may require you to reboot the . This procedure is not part of the normal maintenance of a server. After you reboot the , you are logged off and the will be unavailable for a few minutes.

Note If you reboot the while the server is performing power-on self test (POST) or is operating in the Extensible Firmware Interface (EFI) shell, the server will be powered down until the reboot is complete.

SUMMARY STEPS

1. Server # **scope server** {**1** | **2**}
2. Server /server # **scope bmc**
3. Server /server/bmc # **reboot**

DETAILED STEPS

	Command or Action	Purpose
Step 1	Server # **scope server** {**1** | **2**}	Enters server command mode of server 1 or 2.
Step 2	Server /server # **scope bmc**	Enters bmc command mode.
Step 3	Server /server/bmc # **reboot**	The reboots.

Example

This example reboots the :

```
Server# scope server 1
Server /server # scope bmc
Server /server/bmc # reboot
```

Clearing the BIOS CMOS

On rare occasions, troubleshooting a server may require you to clear the server's BIOS CMOS memory. This procedure is not part of the normal maintenance of a server.

SUMMARY STEPS

1. Server # **scope server** {**1** | **2**}
2. Server /server # **scope bios**
3. Server /server/bios # **clear-cmos**

DETAILED STEPS

	Command or Action	Purpose
Step 1	Server # **scope server** {**1** | **2**}	Enters server command mode of server 1 or 2.
Step 2	Server /server # **scope bios**	Enters the bios command mode.
Step 3	Server /server/bios # **clear-cmos**	After a prompt to confirm, clears the CMOS memory.

Example

This example clears the BIOS CMOS memory:

```
Server# scope server 2
Server/server # scope bios
Server /server/bios # clear-cmos

This operation will clear the BIOS CMOS.
Note: Server should be in powered off state to clear CMOS.
Continue?[y|n] y

Server /server/bios #
```

Resetting the BMC to factory Defaults

On rare occasions, such as an issue with the current running firmware, troubleshooting a server may require you to reset the BMC to the factory default. When this happens, all user-configurable settings are reset.

This procedure is not part of the normal server maintenance. After you reset the BMC, you are logged off and must log in again. You may also lose connectivity and may need to reconfigure the network settings.

SUMMARY STEPS

1. Server # **scope server** {**1** | **2**}
2. Server /server # **scope bmc**
3. Server /server/bmc # **factory-default**

DETAILED STEPS

	Command or Action	Purpose
Step 1	Server # **scope server** {**1** | **2**}	Enters server command mode of server 1 or 2.
Step 2	Server /server # **scope bmc**	Enters bmc command mode. **Note** Depending on the server number you have chosen, enters the BMC1 or BMC2 mode.
Step 3	Server /server/bmc # **factory-default**	After a prompt to confirm, the BMC resets to factory defaults. All your BMC configuration is lost and some of the inventory information may not be available until the server is powered on or power cycled.

Example

This example resets BMC1 to factory defaults:

```
Server# scope server 1
Server /server # scope bmc
Server /server/bmc # factory-default
This operation will reset the Server BMC configuration to factory default.
All your configuration will be lost. Some inventory information may
not be available until the server is powered on or power cycled.
Continue?[y|N] y
```

Resetting to Factory Defaults

Before you begin

You must log in with admin privileges to perform this task.

SUMMARY STEPS

1. Server# **scope chassis**
2. Server /chassis # **factory-default** {**storage** | **vic** | **bmc1** | **bmc2** | **cmc** | **all**}
3. (Optional) Server /chassis # **show factory-reset-status**

DETAILED STEPS

	Command or Action	Purpose
Step 1	Server# **scope chassis**	Enters the chassis command mode.
Step 2	Server /chassis # **factory-default** {**storage** | **vic** | **bmc1** | **bmc2** | **cmc** | **all**}	Depending on the component that you choose to rest to factory default, the configuration parameters of that component is restored to factory defaults. You can choose one of the following components:

	Command or Action	Purpose
		• **all**—Resets the storage controllers, VIC, BMC1, BMC2, and CMCs settings to factory defaults. • **bmc1** —Resets the BMC1 settings to factory defaults. • **bmc2** —Resets the BMC2 settings to factory defaults. • **cmc** —Resets the CMCs settings to factory defaults. • **storage** —Resets the storage controller settings to factory default. • **vic** —Resets the VICs settings to factory default. Enter **y** at the confirmation prompt to reset the chosen component to default. **Note** When you reset the CMC to defaults, all your CMC configuration is lost and the network configuration mode is set to **Cisco Card** mode by default. The CMCs factory defaults include the following conditions: • SSH is enabled for access to the CLI. Telnet is disabled. • HTTPS is enabled for access to the GUI. • A single user account exists (user name is **admin** , password is **password**). • DHCP is enabled on the management port. • KVM and vMedia are enabled. • USB is enabled. • SoL is disabled.
Step 3	(Optional) Server /chassis # **show factory-reset-status**	Displays the factory defaults status.

Example

This example resets to factory defaults:

```
Server# scope chassis
Server /chassis # factory-default vic
his factory-default operation does the following on these components without any back-up:
VIC – all user configured data will deleted and controller properties reset to default
values
(Host power-cycle is required for it to be effective)
Storage – all user configured data (including OS VD/drive if any) will be deleted,
controller properties and zoning settings reset to default values (Host power-cycle is
required for it to be effective)
```

```
BMC -  all Server BMC configuration reset to factory default values
CMC - all user configured data (including admin password) will be deleted and CMC settings
 reset to default values
Continue?[y|N]y
factory-default for ' vic' started. Please check the status using "show factory-reset-status".
Server /chassis # show factory-reset-status
Factory Reset Status:
    Storage: NA
    VIC: Pending
    BMC1: NA
    BMC2: NA
    CMC: NA
Server /chassis #
```

Resetting to Factory Defaults

Before you begin

You must log in with admin privileges to perform this task.

SUMMARY STEPS

1. Server# **scope chassis**
2. Server /chassis # **factory-default** {**storage** | **vic** | **bmc1** | **bmc2** | **cmc** | **all**}
3. (Optional) Server /chassis # **show factory-reset-status**

DETAILED STEPS

	Command or Action	Purpose
Step 1	Server# **scope chassis**	Enters the chassis command mode.
Step 2	Server /chassis # **factory-default** {**storage** | **vic** | **bmc1** | **bmc2** | **cmc** | **all**}	Depending on the component that you choose to rest to factory default, the configuration parameters of that component is restored to factory defaults. You can choose one of the following components: • **`all`**—Resets the storage controllers, VIC, BMC1, BMC2, and CMCs settings to factory defaults. • **`bmc1`** —Resets the BMC1 settings to factory defaults. • **`bmc2`** —Resets the BMC2 settings to factory defaults. • **`cmc`** —Resets the CMCs settings to factory defaults. • **`storage`** —Resets the storage controller settings to factory default. • **`vic`** —Resets the VICs settings to factory default. Enter **`y`** at the confirmation prompt to reset the chosen component to default.

	Command or Action	Purpose
		Note When you reset the CMC to defaults, all your CMC configuration is lost and the network configuration mode is set to **Cisco Card** mode by default. The CMCs factory defaults include the following conditions: • SSH is enabled for access to the CLI. Telnet is disabled. • HTTPS is enabled for access to the GUI. • A single user account exists (user name is **admin** , password is **password**). • DHCP is enabled on the management port. • KVM and vMedia are enabled. • USB is enabled. • SoL is disabled.
Step 3	(Optional) Server /chassis # **show factory-reset-status**	Displays the factory defaults status.

Example

This example resets to factory defaults:

```
Server# scope chassis
Server /chassis # factory-default vic
his factory-default operation does the following on these components without any back-up:
VIC – all user configured data will deleted and controller properties reset to default
values
(Host power-cycle is required for it to be effective)
Storage – all user configured data (including OS VD/drive if any) will be deleted,
controller properties and zoning settings reset to default values (Host power-cycle is
required for it to be effective)
BMC –  all Server BMC configuration reset to factory default values
CMC – all user configured data (including admin password) will be deleted and CMC settings
 reset to default values
Continue?[y|N]y
factory-default for ' vic' started. Please check the status using "show factory-reset-status".
Server /chassis # show factory-reset-status
Factory Reset Status:
    Storage: NA
    VIC: Pending
    BMC1: NA
    BMC2: NA
    CMC: NA
Server /chassis #
```

Exporting and Importing the Cisco IMC and BMC Configuration

Importing a CMC Configuration

> **Important** If any firmware or BIOS updates are in progress, do not import the configuration until those tasks are complete.

SUMMARY STEPS

1. Server# **scope chassis**
2. Server /chassis # **scope import-export**
3. Server /chassis/import-export # **import-config** *protocol ip-address path-and-filename*

DETAILED STEPS

	Command or Action	Purpose
Step 1	Server# **scope chassis**	Enters the chassis command mode.
Step 2	Server /chassis # **scope import-export**	Enters the import-export command mode.
Step 3	Server /chassis/import-export # **import-config** *protocol ip-address path-and-filename*	The configuration file at the specified path and file name on the remote server at the specified IPv4 or IPv6 address or a hostname will be imported. The remote server can be one of the following: • TFTP • FTP • SFTP • SCP • HTTP

	Command or Action	Purpose
		Note The Cisco UCS C-Series server now supports fingerprint confirmation of the server when you update firmware through a remote server. This option is available only if you choose SCP or SFTP as the remote server type. If you chose SCP or SFTP as the remote server type while performing this action, a prompt with the message Server (RSA) key fingerprint is <server_finger_print _ID> Do you wish to continue? Click y or n depending on the authenticity of the server fingerprint. The fingerprint is based on the host's public key and helps you to identify or verify the host you are connecting to.

To determine whether the import operation has completed successfully, use the **show detail** command. To abort the operation, type CTRL+C.

Example

This example shows how to import a configuration:

Importing BMC Configuration

Important If any firmware or BIOS updates are in progress, do not import the configuration until those tasks are complete.

SUMMARY STEPS

1. Server # **scope server** {**1** | **2**}
2. Server /server # **scope bmc**
3. Server /server/bmc # **scope import-export**
4. Server /server/bmc/import-export # **import-config** *protocol ip-address path-and-filename*

DETAILED STEPS

	Command or Action	Purpose
Step 1	Server # **scope server** {**1** | **2**}	Enters server command mode of server 1 or 2.
Step 2	Server /server # **scope bmc**	Enters bmc command mode.
Step 3	Server /server/bmc # **scope import-export**	Enters the import-export command mode.

	Command or Action	Purpose
Step 4	Server /server/bmc/import-export # **import-config** *protocol ip-address path-and-filename*	The configuration file at the specified path and file name on the remote server at the specified IPv4 or IPv6 address or a hostname will be imported. The remote server can be one of the following: • TFTP • FTP • SFTP • SCP • HTTP **Note** The Cisco UCS C-Series server now supports fingerprint confirmation of the server when you update firmware through a remote server. This option is available only if you choose SCP or SFTP as the remote server type. If you chose SCP or SFTP as the remote server type while performing this action, a prompt with the message Server (RSA) key fingerprint is <server_finger_print _ID> Do you wish to continue? Click y or n depending on the authenticity of the server fingerprint. The fingerprint is based on the host's public key and helps you to identify or verify the host you are connecting to.

To determine whether the import operation has completed successfully, use the **show detail** command. To abort the operation, type CTRL+C.

Example

This example shows how to import a configuration:

Exporting the BMC Configuration

Note For security reasons, this operation does not export user accounts or the server certificate.

Important If any firmware or BIOS updates are in progress, do not export the configuration until those tasks are complete.

Before you begin

Obtain the backup remote server IP address.

SUMMARY STEPS

1. Server # **scope server** {**1** | **2**}
2. Server /server # **scope bmc**
3. Server /server/bmc # **scope import-export**
4. Server /server/bmc/import-export # **export-config** *protocol ip-address path-and-filename*

DETAILED STEPS

	Command or Action	Purpose
Step 1	Server # **scope server** {**1** | **2**}	Enters server command mode of server 1 or 2.
Step 2	Server /server # **scope bmc**	Enters bmc command mode.
Step 3	Server /server/bmc # **scope import-export**	Enters the import-export command mode.
Step 4	Server /server/bmc/import-export # **export-config** *protocol ip-address path-and-filename*	The configuration file will be stored at the specified path and file name on a remote server at the specified IPv4 or IPv6 address or a hostname. The remote server could be one of the following types: • TFTP • FTP • SFTP • SCP • HTTP **Note** The Cisco UCS C-Series server now supports fingerprint confirmation of the server when you update firmware through a remote server. This option is available only if you choose SCP or SFTP as the remote server type. If you chose SCP or SFTP as the remote server type while performing this action, a prompt with the message Server (RSA) key fingerprint is <server_finger_print _ID> Do you wish to continue? Click y or n depending on the authenticity of the server fingerprint. The fingerprint is based on the host's public key and helps you to identify or verify the host you are connecting to.

To determine whether the export operation has completed successfully, use the **show detail** command. To abort the operation, type CTRL+C.

Example

This example shows how to back up the configuration:

```
Server# scope server 2
Server /server# scope bmc
Server /server/bmc # scope import-export
Server /server/bmc/import-export # export-config tftp 192.0.2.34 /ucs/backups/cimc5.xml
Username:pynj
Password:****
Export config started. Please check the status using "show detail".
Server /cimc/import-export # show detail
Import Export:
    Operation: EXPORT
    Status: COMPLETED
    Error Code: 100 (No Error)
    Diagnostic Message: NONE

Server /server/bmc/import-export #
```

Exporting the CMC Configuration

Note For security reasons, this operation does not export user accounts or the server certificate.

Important If any firmware or BIOS updates are in progress, do not export the configuration until those tasks are complete.

Before you begin

Obtain the backup remote server IP address.

SUMMARY STEPS

1. Server # **scope chassis**
2. Server /chassis # **scope import-export**
3. Server /chassis/import-export # **export-config** *protocol ip-address path-and-filename*

DETAILED STEPS

	Command or Action	Purpose
Step 1	Server # **scope chassis**	Enters chassis command mode.
Step 2	Server /chassis # **scope import-export**	Enters the import-export command mode.
Step 3	Server /chassis/import-export # **export-config** *protocol ip-address path-and-filename*	The configuration file will be stored at the specified path and file name on a remote server at the specified IPv4 or IPv6 address or a hostname. The remote server could be one of the following types:

	Command or Action	Purpose
		• TFTP • FTP • SFTP • SCP • HTTP **Note** The Cisco UCS C-Series server now supports fingerprint confirmation of the server when you update firmware through a remote server. This option is available only if you choose SCP or SFTP as the remote server type. If you chose SCP or SFTP as the remote server type while performing this action, a prompt with the message Server (RSA) key fingerprint is <server_finger_print _ID> Do you wish to continue? Click y or n depending on the authenticity of the server fingerprint. The fingerprint is based on the host's public key and helps you to identify or verify the host you are connecting to.

To determine whether the export operation has completed successfully, use the **show detail** command. To abort the operation, type CTRL+C.

Example

This example shows how to back up the configuration:

```
Server# scope chassis
Server /chassis # scope import-export
Server /chassis/import-export # export-config tftp 192.0.2.34 /ucs/backups/cimc5.xml
Username:pynj
Password:****
Passphrase:***
Export config started. Please check the status using "show detail".
Server /chassis/import-export # show detail
Import Export:
    Operation: EXPORT
    Status: COMPLETED
    Error Code: 100 (No Error)
    Diagnostic Message: NONE

Server /chassis/import-export #
```

Exporting VIC Adapter Configuration

Important If any firmware or BIOS updates are in progress, do not export the VIC adapter configuration until those tasks are complete.

SUMMARY STEPS

1. Server# **scope chassis**
2. Server /chassis # **export-all-adapters** *protocol ip-address path-and-filename*

DETAILED STEPS

	Command or Action	Purpose
Step 1	Server# **scope chassis**	Enters the chassis command mode.
Step 2	Server /chassis # **export-all-adapters** *protocol ip-address path-and-filename*	The configuration file at the specified path and file name on the remote server at the specified IPv4 or IPv6 address or a hostname will be imported. The remote server can be one of the following: • TFTP • FTP • SFTP • SCP • HTTP **Note** The Cisco UCS C-Series server now supports fingerprint confirmation of the server when you update firmware through a remote server. This option is available only if you choose SCP or SFTP as the remote server type. If you chose SCP or SFTP as the remote server type while performing this action, a prompt with the message Server (RSA) key fingerprint is <server_finger_print _ID> Do you wish to continue? Click y or n depending on the authenticity of the server fingerprint. The fingerprint is based on the host's public key and helps you to identify or verify the host you are connecting to.

To determine whether the export operation has completed successfully, use the **show detail** command. To abort the operation, type CTRL+C.

Example

This example shows how to export a VIC adapter configuration:

Importing VIC Adapter Configuration

Important If any firmware or BIOS updates are in progress, do not import the VIC Adapter configuration until those tasks are complete.

SUMMARY STEPS

1. Server# **scope chassis**
2. Server /chassis # **import-all-adapters** *protocol ip-address path-and-filename*
3. Enter the username, and password.

DETAILED STEPS

	Command or Action	Purpose
Step 1	Server# **scope chassis**	Enters the chassis command mode.
Step 2	Server /chassis # **import-all-adapters** *protocol ip-address path-and-filename*	The configuration file at the specified path and file name on the remote server at the specified IPv4 or IPv6 address or a hostname will be imported. The remote server can be one of the following: • TFTP • FTP • SFTP • SCP • HTTP

	Command or Action	Purpose
		Note The Cisco UCS C-Series server now supports fingerprint confirmation of the server when you update firmware through a remote server. This option is available only if you choose SCP or SFTP as the remote server type. If you chose SCP or SFTP as the remote server type while performing this action, a prompt with the message Server (RSA) key fingerprint is <server_finger_print _ID> Do you wish to continue? Click y or n depending on the authenticity of the server fingerprint. The fingerprint is based on the host's public key and helps you to identify or verify the host you are connecting to.
Step 3	Enter the username, and password.	Starts the import operation.

To determine whether the import operation has completed successfully, use the **show detail** command. To abort the operation, type CTRL+C.

Example

This example shows how to import the VIC adapter configuration:

Generating Non-Maskable Interrupts to the Host

In some situations, the server might hang and not respond to traditional debug mechanisms. By generating a non maskable interrupt (NMI) to the host, you can create and send a crash dump file of the server and use it to debug the server.

Depending on the type of operating system associated with the server, this task might restart the OS.

SUMMARY STEPS

1. Server # **scope chassis**
2. Server /chassis # **scope server** {**1** | **2**}
3. Server /chassis/server # **generate-nmi**

DETAILED STEPS

	Command or Action	Purpose
Step 1	Server # **scope chassis**	Enters chassis command mode.
Step 2	Server /chassis # **scope server** {**1** | **2**}	Enters server command mode of server 1 or 2.
Step 3	Server /chassis/server # **generate-nmi**	Generates the crash dump file for the server.

	Command or Action	Purpose
		To use this command, the server must be powered on, and you must be logged in as an administrator.

Example

This example shows how to generate NMI signals to the host:

```
Server # scope chassis
Server /chassis # scope server 2
Server /chassis/server # generate-nmi
This operation will send NMI to host and may cause reboot of OS
OS reboot depends on it's NMI configuration
Do you want to continue? [y|N] y
Server /chassis/server #
```

Adding Cisco IMC Banner

SUMMARY STEPS

1. Server # **scope chassis**
2. Server /chassis # **upload-banner**
3. Enter the banner and press CTRL+D.
4. (Optional) Server /chassis # **show-banner**

DETAILED STEPS

	Command or Action	Purpose
Step 1	Server # **scope chassis**	Enters chassis command mode.
Step 2	Server /chassis # **upload-banner**	A prompt to enter the banner displays.
Step 3	Enter the banner and press CTRL+D.	At the prompt, enter **y**. This results in a loss of the current session, when you log back on again, the new banner appears.
Step 4	(Optional) Server /chassis # **show-banner**	The banner that you have added displays.

Example

This example shows how to add the Cisco IMC banner:

```
Server # scope chassis
Server /chassis # upload-banner
Please paste your custom banner here, when finished, press enter and CTRL+D.
hello world
This will terminate all open SSH session to take an immediate action.
Do you wish to continue? [y/N] yy
Server /chassis # show-banner
```

```
hello world
Server /chassis #
```

Downloading and Viewing Inventory Details

You can retrieve and save in a file, the following inventory details from the Web UI:

- System Properties
- CPU Information
- Power supply unit inventory
- PCI adapters Cards
- Memory Details
- Trusted Platform Module information
- Disk Information
- Network interface card
- Storage adapter card
- Virtual interface card
- Fan status
- Flex flash card
- BBU Status

SUMMARY STEPS

1. Server # **scope chassis**
2. Server /chassis # **inventory-refresh**
3. Server /chassis # **inventory-all**

DETAILED STEPS

	Command or Action	Purpose
Step 1	Server # **scope chassis**	Enters chassis command mode.
Step 2	Server /chassis # **inventory-refresh**	Initiates the data collection activity and saves the data in a file.
Step 3	Server /chassis # **inventory-all**	Displays inventory information.

Example

This example shows the inventory details and the status of inventory collection :

```
Server# scope chassis
Server /chassis #inventory-refresh

Inventory data collection started.

Server /chassis #inventory-all

Hardware Inventory Information:
Status: IN-PROGRESS
Progress(%): 5
...
Progress(%): 50
sysProductName: UCS C240 M3S
sysProductID: UCSC-C240-M3S
sysSerialNum: FCH1925V21U
...
CPU
id: 1
SocketDesignation: CPU1
ProcessorManufacturer: Intel(R) Corporation
ProcessorFamily: Xeon
ThreadCount: 4
Server /chassis #
```