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.

Procedure

	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.

	Command or Action	Purpose
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 **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.

	Command or Action	Purpose
Step 10	Server /chassis/tech-support # **start**	Begins the transfer of the data file to the remote server.
Step 11	Server /chassis/tech-support # **show detail**	(Optional) Displays the progress of the transfer of the data file to the remote server.
Step 12	Server /chassis/tech-support # **cancel**	(Optional) Cancels the transfer of the data file to the remote server.

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 Cisco IMC. This procedure is not part of the normal maintenance of a server. After you reboot the Cisco IMC, you are logged off and the Cisco IMC will be unavailable for a few minutes.

Note If you reboot the Cisco IMC 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 Cisco IMC reboot is complete.

Procedure

	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 Cisco IMC reboots.

This example reboots the Cisco IMC:

```
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.

Procedure

	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.

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.

Procedure

	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.

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 CMCs to Factory Defaults

On rare occasions, such as an issue with the current running firmware, troubleshooting a server may require you to reset the CMCs 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 CMC, you are logged off and must log in again. You may also lose connectivity and may need to reconfigure the network settings.

Procedure

	Command or Action	Purpose
Step 1	Server# **scope chassis**	Enters the chassis command mode.
Step 2	Server /chassis # **factory-default**	After a prompt to confirm, the CMCs resets to factory 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 Cisco IMC CLI. Telnet is disabled.

- HTTPS is enabled for access to the Cisco IMC GUI.
- A single user account exists (user name is **admin** , password is **password**).
- DHCP is enabled on the management port.
- The previous actual boot order is retained.
- KVM and vMedia are enabled.
- USB is enabled.
- SoL is disabled.

This example resets the CMCs to factory defaults:

```
Server# scope chassis
Server /chassis # factory-default
This operation will reset the CMC configuration to factory default.
All your configuration will be lost.
Continue?[y|N]
```

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 Cisco IMC configuration until those tasks are complete.

Procedure

	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.
Step 4	Enter the Username, Password and Pass Phrase.	Sets the username, password and the pass phrase for the file being imported. 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.

This example shows how to import a Cisco IMC configuration:

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

Importing BMC Configuration

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

Procedure

	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.

	Command or Action	Purpose
Step 3	Server /server/bmc # **scope import-export**	Enters the import-export command mode.
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.
Step 5	Enter the Username and Password.	Sets the username and password for the file being imported. 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.

This example shows how to import a Cisco IMC configuration:

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

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 Cisco IMC configuration until those tasks are complete.

Before You Begin

Obtain the backup remote server IP address.

Procedure

	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.

	Command or Action	Purpose
Step 5	Enter the Username and Password.	Sets the username, password and the pass phrase for the file being exported. Starts the backup operation.

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

This example shows how to back up the Cisco IMC 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 Cisco IMC configuration until those tasks are complete.

Before You Begin

Obtain the backup remote server IP address.

Procedure

	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: • TFTP

	Command or Action	Purpose
		• 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.
Step 4	Enter the Username, Password and Pass Phrase.	Sets the username, password and the pass phrase for the file being exported. Starts the backup operation.

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

This example shows how to back up the Cisco IMC 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 #
```

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.

Procedure

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

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

Procedure

	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	Server /chassis # **show-banner**	(Optional) The banner that you have added displays.

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 #
```