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 cimc**	Enters the Cisco IMC command mode.
Step 2	Server /cimc # **scope tech-support**	Enters the tech-support command mode.

	Command or Action	Purpose
Step 3	Server /cimc/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 4	Server /cimc/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 5	Server /cimc/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 6	Server /cimc/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 7	Server /cimc/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 8	Server /cimc/tech-support # **commit**	Commits the transaction to the system configuration.
Step 9	Server /cimc/tech-support # **start**	Begins the transfer of the data file to the remote server.

	Command or Action	Purpose
Step 10	Server /cimc/tech-support # **show detail**	(Optional) Displays the progress of the transfer of the data file to the remote server.
Step 11	Server /cimc/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 cimc
Server /cimc # scope tech-support
Server /cimc/tech-support # set remote-ip 192.0.20.41
Server /cimc/tech-support* # set remote-protocol tftp
Server /cimc/tech-support *# set remote-path /user/user1/default.tar.gz
Server /cimc/tech-support *# commit
Server /cimc/tech-support # start
Tech Support upload started.

Server /cimc/tech-support # show detail

Tech Support:
  Server Address: 192.0.20.41
  Path: default.tar.gz
  Protocol: tftp
  Username:
  Password: *******
  Progress (%): 5
  Status: Collecting

Server /cimc/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 cimc**	Enters the Cisco IMC command mode.

	Command or Action	Purpose
Step 2	Server /cimc # **reboot**	The Cisco IMC reboots.

This example reboots the Cisco IMC:

```
Server# scope cimc
Server /cimc # 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 bios**	Enters the bios command mode.
Step 2	Server /bios # **clear-cmos**	After a prompt to confirm, clears the CMOS memory.

This example clears the BIOS CMOS memory:

```
Server# scope bios
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 /bios #
```

Recovering from a Corrupted BIOS

Note This procedure is not available in some server models.

In addition to this procedure, there are three other methods for recovering from a corrupted BIOS:

- Use the Cisco Host Upgrade Utility (HUU). This is the recommended method.
- Use the Cisco IMC GUI interface.
- If your server model supports it, use the BIOS recovery function of the hardware jumper on the server motherboard. For instructions, see the Cisco UCS Server Installation and Service Guide for your server model.

Before You Begin

- You must be logged in as admin to recover from a corrupted BIOS.
- Have the BIOS recovery ISO image ready. You will find the BIOS recovery ISO image under the Recovery folder of the firmware distribution package.
- Schedule some down time for the server because it will be power cycled at the end of the recovery procedure.

Procedure

	Command or Action	Purpose
Step 1	Server# **scope bios**	Enters the bios command mode.
Step 2	Server# **recover**	Launches a dialog for loading the BIOS recovery image.

This example shows how to recover from a corrupted BIOS:

```
Server# scope bios
Server /bios # recover
This operation will automatically power on the server to perform BIOS FW recovery.
Continue?[y|N]y
```

What to Do Next

Power cycle or reset the server.

Resetting the Cisco IMC to Factory Defaults

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

When you upgrade from version 1.5(1) to version 1.5(2), the hostname in the Cisco IMC interface is retained as is. However, after upgrading to version 1.5(2), if you do a factory reset, the hostname changes to CXXX-YYYYYY format, where XXX is the model number and YYYYYY is the serial number of the server.

When you downgrade from version 1.5(2) to version 1.5(1), the hostname is retained as is. However, if you do a factory reset, the hostname changes to ucs-cxx-mx format.

Note If you reset Cisco IMC 1.5(x), 2.0, and 2.0(3) versions to factory defaults, **Shared LOM** mode is configured by default. For C3160 servers, if you reset Cisco IMC to factory defaults, **Dedicated** mode is configured to **Full** duplex with 100 Mbps speed by default.

Procedure

	Command or Action	Purpose
Step 1	Server# **scope cimc**	Enters the Cisco IMC command mode.
Step 2	Server /cimc # **factory-default**	After a prompt to confirm, the Cisco IMC resets to factory defaults.

The Cisco IMC 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 Cisco IMC to factory defaults:

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

Exporting and Importing the Cisco IMC Configuration

Exporting the Cisco IMC 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 cimc**	Enters the Cisco IMC command mode.
Step 2	Server /cimc # **scope import-export**	Enters the import-export command mode.
Step 3	Server /cimc/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.
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 cimc
Server /cimc # scope import-export
Server /cimc/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 /cimc/import-export # show detail
Import Export:
    Operation: EXPORT
    Status: COMPLETED
    Error Code: 100 (No Error)
    Diagnostic Message: NONE

Server /cimc/import-export #
```

Exporting and Importing the Cisco IMC Configuration

To perform a backup of the Cisco IMC configuration, you take a snapshot of the system configuration and export the resulting Cisco IMC configuration file to a location on your network. The export operation saves information from the management plane only; it does not back up data on the servers. Sensitive configuration information such as user accounts and the server certificate are not exported.

You can restore an exported Cisco IMC configuration file to the same system or you can import it to another Cisco IMC system, provided that the software version of the importing system is the same as or is configuration-compatible with the software version of the exporting system. When you import a configuration file to another system as a configuration template, you must modify system-specific settings such as IP addresses and host names. An import operation modifies information on the management plane only.

The Cisco IMC configuration file is an XML text file whose structure and elements correspond to the Cisco IMC command modes.

When performing an export or import operation, consider these guidelines:

- You can perform an export or an import while the system is up and running. While an export operation has no impact on the server or network traffic, some modifications caused by an import operation, such as IP address changes, can disrupt traffic or cause a server reboot.
- You cannot execute an export and an import simultaneously.

You can perform an import or an export operation on the following features:

- Cisco IMC version

Note You can only export this information.

- Network settings
- Technical support
- Logging control for local and remote logs
- Power policies
- BIOS - BIOS Parameters

Note Precision boot is not supported.

- Communication services
- Remote presence
- User management - LDAP
- Event management
- SNMP

Exporting the Cisco IMC 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 cimc**	Enters the Cisco IMC command mode.
Step 2	Server /cimc # **scope import-export**	Enters the import-export command mode.
Step 3	Server /cimc/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.
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 cimc
Server /cimc # scope import-export
Server /cimc/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 /cimc/import-export # show detail
Import Export:
    Operation: EXPORT
    Status: COMPLETED
    Error Code: 100 (No Error)
    Diagnostic Message: NONE

Server /cimc/import-export #
```

Importing a Cisco IMC 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 cimc**	Enters the Cisco IMC command mode.
Step 2	Server /cimc # **scope import-export**	Enters the import-export command mode.
Step 3	Server /cimc/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 cimc
Server /cimc # scope import-export
Server /cimc/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 /cimc/import-export # show detail
Import Export:
    Operation: Import
    Status: COMPLETED
    Error Code: 100 (No Error)
    Diagnostic Message: NONE
Server /cimc/import-export #
```

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.

	Command or Action	Purpose
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 #
```

Deleting Cisco IMC Banner

Procedure

	Command or Action	Purpose
Step 1	Server # **scope chassis**	Enters chassis command mode.
Step 2	Server /chassis # **delete-banner**	At the prompt, enter y. This results in a loss of the current session, when you log back on again, the banner is deleted.
Step 3	Server /chassis # **show-banner**	(Optional) The banner that you have added displays.

This example shows how to delete the Cisco IMC banner:

```
Server # scope chassis
Server /chassis # delete-banner
This will terminate all open SSH session to take an immediate action.
Do you wish to continue? [y/N] yy
Server /chassis # show-banner

Server /chassis #
```

Enabling Secure Adapter Update

Before You Begin

You must log in as a user with admin privileges to perform this action.

Procedure

	Command or Action	Purpose
Step 1	Server# **scope cimc**	Enters the Cisco IMC command mode.
Step 2	Server /cimc # **scope adapter-secure-update**	Enters the adapter-secure-update command mode.
Step 3	Server /cimc/adapter-secure-update # **enable-security-version-check** {**yes** | **no**}	Enter yes at the prompt. **Note** If you enter no at the prompt, secure adapter update is disabled.
Step 4	Server /cimc/adapter-secure-update # **enable-security-version-check status**	(Optional) Displays the secure update status.

This example shows how to enable the secure adapter update:

```
Server# scope cimc
Server /cimc # scope adapter-secure-update
Server /cimc/adapter-secure-update # enable-security-version-check yes
Server /cimc/adapter-secure-update # enable-security-version-check status
enable-security-version-check: Enabled
Server /cimc/adapter-secure-update #
```