Cisco IOS Resilient Configuration

First Published: May 17, 2004
Last Updated: October 19, 2009

The Cisco IOS Resilient Configuration feature enables a router to secure and maintain a working copy of the running image and configuration so that those files can withstand malicious attempts to erase the contents of persistent storage (NVRAM and flash).

Finding Feature Information

Your software release may not support all the features documented in this module. For the latest feature information and caveats, see the release notes for your platform and software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the "Feature Information for Cisco IOS Resilient Configuration" section on page 9.

Use Cisco Feature Navigator to find information about platform support and Cisco IOS and Catalyst OS software image support. To access Cisco Feature Navigator, go to http://tools.cisco.com/ITDIT/CFN/jsp/index.jsp. An account on Cisco.com is not required.

Contents

Americas Headquarters:
Cisco Systems, Inc., 170 West Tasman Drive, San Jose, CA 95134-1706 USA

Restrictions for Cisco IOS Resilient Configuration

- This feature is available only on platforms that support a Personal Computer Memory Card International Association (PCMCIA) Advanced Technology Attachment (ATA) disk. There must be enough space on the storage device to accommodate at least one Cisco IOS image (two for upgrades) and a copy of the running configuration. IOS Files System (IFS) support for secure file systems is also needed by the software.
- It may be possible to force removal of secured files using an older version of Cisco IOS software that does not contain file system support for hidden files.
- This feature can be disabled only by using a console connection to the router. With the exception of the upgrade scenario, feature activation does not require console access.
- You cannot secure a bootset with an image loaded from the network. The running image must be loaded from persistent storage to be secured as primary.
- Secured files will not appear on the output of a **dir** command issued from an executive shell because the IFS prevents secure files in a directory from being listed. ROM monitor (ROMMON) mode does not have any such restriction and can be used to list and boot secured files. The running image and running configuration archives will not be visible in the Cisco IOS **dir** command output. Instead, use the **show secure bootset** command to verify archive existence.

Information About Cisco IOS Resilient Configuration

Before using Cisco IOS Resilient Configuration, you should understand the following concept:

- Feature Design of Cisco IOS Resilient Configuration, page 2

Feature Design of Cisco IOS Resilient Configuration

A great challenge of network operators is the total downtime experienced after a router has been compromised and its operating software and configuration data erased from its persistent storage. The operator must retrieve an archived copy (if any) of the configuration and a working image to restore the router. Recovery must then be performed for each affected router, adding to the total network downtime.

The Cisco IOS Resilient Configuration feature is intended to speed up the recovery process. The feature maintains a secure working copy of the router image and the startup configuration at all times. These secure files cannot be removed by the user. This set of image and router running configuration is referred to as the primary bootset.

The following factors were considered in the design of Cisco IOS Resilient Configuration:

- The configuration file in the primary bootset is a copy of the running configuration that was in the router when the feature was first enabled.
- The feature secures the smallest working set of files to preserve persistent storage space. No extra space is required to secure the primary Cisco IOS image file.
- The feature automatically detects image or configuration version mismatch.
- Only local storage is used for securing files, eliminating scalability maintenance challenges from storing multiple images and configurations on TFTP servers.
- The feature can be disabled only through a console session.

How to Use Cisco IOS Resilient Configuration

This section contains the following procedures:

- Archiving a Router Configuration, page 3
- Restoring an Archived Router Configuration, page 4

Archiving a Router Configuration

This task describes how to save a primary bootset to a secure archive in persistent storage.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **secure boot-image**
4. **secure boot-config**
5. **end**
6. **show secure bootset**

DETAILED STEPS

	Command or Action	Purpose

Step 1	**`enable`**
	Example:
	`Router> enable`
		Enables privileged EXEC mode.
		• Enter your password if prompted.

Step 2	**`configure terminal`**
	Example:
	`Router# configure terminal`
		Enters global configuration mode.

Step 3	**`secure boot-image`**
	Example:
	`Router(config)# secure boot-image`
		Enables Cisco IOS image resilience.

Step 4	**`secure boot-config`**
	Example:
	`Router(config)# secure boot-config`
		Stores a secure copy of the primary bootset in persistent storage.

	Command or Action	Purpose

Step 5	**end**
	Example:
	`Router(config)# end`
		Exits to privileged EXEC mode.

Step 6	**show secure bootset** **Example:** `Router# show secure bootset`	(Optional) Displays the status of configuration resilience and the primary bootset filename.

Examples

This section provides the following output example:

- Sample Output for the show secure bootset Command, page 4

Sample Output for the show secure bootset Command

The following example displays sample output from the **show secure bootset** command:

```
Router# show secure bootset

IOS resilience router id JMX0704L5GH

IOS image resilience version 12.3 activated at 08:16:51 UTC Sun Jun 16 2002
Secure archive slot0:c3745-js2-mz type is image (elf) []
  file size is 25469248 bytes, run size is 25634900 bytes
  Runnable image, entry point 0x80008000, run from ram

IOS configuration resilience version 12.3 activated at 08:17:02 UTC Sun Jun 16 2002
Secure archive slot0:.runcfg-20020616-081702.ar type is config
configuration archive size 1059 bytes
```

Restoring an Archived Router Configuration

This task describes how to restore a primary bootset from a secure archive after the router has been tampered with (by an NVRAM erase or a disk format).

Note To restore an archived primary bootset, Cisco IOS image resilience must have been enabled and a primary bootset previously archived in persistent storage.

SUMMARY STEPS

1. **reload**
2. **dir** [*filesystem***:**]
3. **boot** [*partition-number***:**][*filename*]
4. **no**
5. **enable**
6. **configure terminal**

7. **secure boot-config** [**restore** *filename*]
8. **end**
9. **copy** *filename* **running-config**

DETAILED STEPS

	Command or Action	Purpose

Step 1	**`reload`**
	Example:
	`Router# reload`
		(Optional) Enters ROM monitor mode, if necessary.

Step 2	**`dir`** `[`*`filesystem`***`:`**`]`
	Example:
	`rommon 1 > dir slot0:`
		Lists the contents of the device that contains the secure bootset file.
		- The device name can be found in the output of the **show secure bootset** command.

Step 3	**`boot`** `[`*`partition-number`***`:`**`][`*`filename`*`]`
	Example:
	`rommon 2 > boot slot0:c3745-js2-mz`
		Boots up the router using the secure bootset image.

Step 4	**`no`**
	Example:
	`--- System Configuration Dialog ---`
	`Would you like to enter the initial`
	`configuration dialog? [yes/no]: no`
		(Optional) Declines to enter an interactive configuration session in setup mode.
		- If the NVRAM was erased, the router enters setup mode and prompts the user to initiate an interactive configuration session.

Step 5	**`enable`**
	Example:
	`Router> enable`
		Enables privileged EXEC mode.
		- Enter your password if prompted.

Step 6	**`configure terminal`**
	Example:
	`Router# configure terminal`
		Enters global configuration mode.

Step 7	**`secure boot-config`** `[`**`restore`** *`filename`*`]`
	Example:
	`Router(config)# secure boot-config restore`
	`slot0:rescue-cfg`
		Restores the secure configuration to the supplied filename.

	Command or Action	Purpose

Step 8	**end**
	Example:
	`Router(config)# end`
		Exits to privileged EXEC mode.

Step 9	**copy** *filename* **running-config** **Example:** `Router# copy slot0:rescue-cfg running-config`	Copies the restored configuration to the running configuration.

Additional References

The following sections provide references related to Cisco IOS Resilient Configuration.

Related Documents

Related Topic	Document Title
Additional commands: complete command syntax, command mode, defaults, usage guidelines, and examples	*The Cisco IOS Configuration Fundamentals and Network Management Command Reference, Release 12.4T*

Standards

Standards	Title
No new or modified standards are supported by this feature, and support for existing standards has not been modified by this feature.	—

MIBs

MIBs	MIBs Link
No new or modified MIBs are supported by this feature, and support for existing MIBs has not been modified by this feature.	To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use Cisco MIB Locator found at the following URL: http://www.cisco.com/go/mibs

RFCs

RFCs	Title
No new or modified RFCs are supported by this feature, and support for existing RFCs has not been modified by this feature.	—

Technical Assistance

Description	Link
The Cisco Support website provides extensive online resources, including documentation and tools for troubleshooting and resolving technical issues with Cisco products and technologies. To receive security and technical information about your products, you can subscribe to various services, such as the Product Alert Tool (accessed from Field Notices), the Cisco Technical Services Newsletter, and Really Simple Syndication (RSS) Feeds. Access to most tools on the Cisco Support website requires a Cisco.com user ID and password.	http://www.cisco.com/techsupport

Feature Information for Cisco IOS Resilient Configuration

Table 1 lists the release history for this feature.

Not all commands may be available in your Cisco IOS software release. For release information about a specific command, see the command reference documentation.

Use Cisco Feature Navigator to find information about platform support and software image support. Cisco Feature Navigator enables you to determine which Cisco IOS and Catalyst OS software images support a specific software release, feature set, or platform. To access Cisco Feature Navigator, go to http://tools.cisco.com/ITDIT/CFN/jsp/index.jsp. An account on Cisco.com is not required.

Note Table 1 lists only the Cisco IOS software release that introduced support for a given feature in a given Cisco IOS software release train. Unless noted otherwise, subsequent releases of that Cisco IOS software release train also support that feature.

Table 1 Feature Information for Cisco IOS Resilient Configuration

Feature Name	Releases	Feature Information
Cisco IOS Resilient Configuration	12.3(8)T	The Cisco IOS Resilient Configuration feature enables a router to secure and maintain a working copy of the running image and configuration so that those files can withstand malicious attempts to erase the contents of persistent storage (NVRAM and flash). In 12.3(8)T this feature was introduced. The following commands were introduced or modified: **secure boot-config**, **secure boot-image**, **show secure bootset**.

Any Internet Protocol (IP) addresses and phone numbers used in this document are not intended to be actual addresses and phone numbers. Any examples, command display output, network topology diagrams, and other figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses or phone numbers in illustrative content is unintentional and coincidental.