

Junos® OS Evolved

Junos® OS Evolved Software Installation and Upgrade Guide

Published
2021-09-16

Juniper Networks, Inc.
1133 Innovation Way
Sunnyvale, California 94089
USA
408-745-2000
www.juniper.net

Juniper Networks, the Juniper Networks logo, Juniper, and Junos are registered trademarks of Juniper Networks, Inc. in the United States and other countries. All other trademarks, service marks, registered marks, or registered service marks are the property of their respective owners.

Juniper Networks assumes no responsibility for any inaccuracies in this document. Juniper Networks reserves the right to change, modify, transfer, or otherwise revise this publication without notice.

Junos® OS Evolved Junos® OS Evolved Software Installation and Upgrade Guide
Copyright © 2021 Juniper Networks, Inc. All rights reserved.

The information in this document is current as of the date on the title page.

YEAR 2000 NOTICE

Juniper Networks hardware and software products are Year 2000 compliant. Junos OS has no known time-related limitations through the year 2038. However, the NTP application is known to have some difficulty in the year 2036.

END USER LICENSE AGREEMENT

The Juniper Networks product that is the subject of this technical documentation consists of (or is intended for use with) Juniper Networks software. Use of such software is subject to the terms and conditions of the End User License Agreement ("EULA") posted at <https://support.juniper.net/support/eula/>. By downloading, installing or using such software, you agree to the terms and conditions of that EULA.

Table of Contents

1

Overview of Junos OS Evolved

Junos OS Evolved Overview | 2

Junos OS Evolved Overview | 2

Understand Graceful Routing Engine Switchover for Junos OS Evolved | 5

Nonstop Active Routing Concepts for Junos OS Evolved | 9

Directories for Junos OS Evolved File Storage | 11

Default Directories for Junos OS Evolved File Storage | 11

Writable Directories for Junos OS Evolved | 12

2

Install, Upgrade, and Downgrade Software

Software Installation and Upgrade Overview | 16

Software Installation and Upgrade Overview (Junos OS Evolved) | 16

Junos OS Evolved Installation Packages | 23

Junos OS Evolved Installation Packages | 23

Prepare to Install and Upgrade Software | 27

Ensure Sufficient Disk Space for Upgrades | 27

Before You Upgrade or Reinstall Junos OS Evolved | 33

Validate the Configuration against the Installation Image | 48

Upgrade and Downgrade Software | 50

Install, Upgrade, and Downgrade Software | 50

Prepare to Install Software | 51

Prepare both Routing Engines to Join the System | 53

Install the Software Package on a Device with Redundant Routing Engines | 59

Install the Software Package on a Device with a Single Routing Engine | 63

Recover from a Failed Installation Attempt If the CLI Is Working | 65

Replace a Routing Engine in a Dual-RE System | 67

Not Enough Disk Space for Software Installation | 69

Install Third-Party Software | 71

How to Install Third-Party Software on Devices Running Junos OS Evolved | 71

System Backup and Recovery

Boot Junos OS Evolved from a USB Drive | 75

Boot Junos OS Evolved by Using a Bootable USB Drive | 75

Create a Bootable USB Drive Using a Windows Device | 75

Create a Bootable USB Drive Using a MAC OS X | 76

Create a Bootable USB Drive Using a Switch or Router Running Junos OS Evolved | 77

Boot Junos OS Evolved from a Bootable USB Drive Using the CLI | 78

Recover Junos OS Evolved Using USB Scratch Install | 79

Boot Junos OS Evolved from a Bootable USB Drive Using the Shell | 80

Back Up an Installation with Snapshots | 86

Back up and Recover Software with Snapshots | 86

Understand Snapshots | 86

Create a Snapshot on the Secondary SSD and Use It to Recover the Software Installation | 87

Roll Back the Software to a Previous Version | 90

Roll Back the Software to a Previous Version | 90

Backup and Recover the Configuration File | 92

Back up and Recover the Configuration | 92

Save a Rescue Configuration | 93

Validate a Rescue Configuration | 93

Roll Back to a Rescue Configuration | 93

Fix the Failed Configuration | 94

Delete the Rescue Configuration | 95

Copy either the Configuration File or the Rescue Configuration to a Remote Server | 95

Roll Back to a Prior Configuration | 96

Synchronize the Rescue Configuration to the Secondary RE after the Current Configuration Is Synchronized | 96

Restore the Configuration from a Backup Copy after a USB Software Installation | 97

Revert to the Default Factory Configuration | 99

Storage Media and Routing Engines

Storage Media and Routing Engines | 102

Storage Media and Routing Engines | 102

Routing Engines and Storage Media | 102

Zero Touch Provisioning

Zero Touch Provisioning | 105

Zero Touch Provisioning | 105

Zero Touch Provisioning Overview | 105

Zero Touch Provisioning Using DHCP Options | 114

Zero Touch Provisioning Using DHCPv6 Options | 122

Zero Touch Provisioning on SRX Series Devices | 129

Understanding Zero Touch Provisioning on SRX Series Devices | 129

Configuring Zero-Touch Provisioning on an SRX Series Device | 133

Understanding Factory-Default Configuration on SRX Series Device for Zero Touch Provisioning | 137

Monitoring Zero Touch Provisioning | 138

Using the Console to Monitor Zero Touch Provisioning | 139

Using System Log Alerts to Monitor Zero Touch Provisioning | 139

Using Error Messages to Monitor Zero Touch Provisioning | 140

Using System Log Files to Monitor Zero Touch Provisioning in Junos OS Using DHCP Options | 141

Using System Log Files to Monitor Zero Touch Provisioning in Junos OS Using DHCPv6 Options | 142

Using the Console to Monitor Zero Touch Provisioning in Junos OS Evolved | 143

Using the show dhcp client binding Command | 145

Using the show dhcpv6 client binding Command | 147

Using the show dhcp client statistics Command | 148

Using the show dhcpv6 client statistics Command | 149

Zero Touch Provisioning DHCP Options | 155

Zero Touch Provisioning DHCP Options for Junos OS Evolved | 155

Configuration Statements and Operational Commands

Configuration Statements | 161

auto-sw-sync | 161

license | 163

Operational Commands | 166

request node halt (Junos OS Evolved) | **167**

request node (offline | online) (Junos OS Evolved) | **170**

request node power-off (Junos OS Evolved) | **172**

request node power-on (Junos OS Evolved) | **174**

request node reboot (re0 | re1) (Junos OS Evolved) | **176**

request system application (Junos OS Evolved) | **178**

request system configuration rescue delete | **179**

request system configuration rescue save | **181**

request system firmware upgrade | **182**

request system snapshot (Junos OS Evolved) | **186**

request system software add (Junos OS Evolved) | **188**

request system software delete (Junos OS Evolved) | **200**

request system software rollback (Junos OS Evolved) | **204**

request system software sync | **207**

request system software validate (Junos OS Evolved) | **212**

request system storage cleanup (Junos OS Evolved) | **214**

request system zeroize (Junos OS Evolved) | **225**

restart (Junos OS Evolved) | **227**

rollback | **229**

show system applications (Junos OS Evolved) | **230**

show system core dumps (Junos OS Evolved) | **239**

show system errors | **241**

show system errors active | **246**

show system errors count | **253**

show system errors error-id | **255**

show system errors fru | **258**

show system errors inactive | **264**

show system errors history | **272**

show system rollback | **275**

show system snapshot (Junos OS Evolved) | **277**

show system software add-restart (Junos OS Evolved) | **279**

show system software list | **282**

show system ztp | **286**

show version (Junos OS Evolved) | **291**

1

PART

Overview of Junos OS Evolved

[Junos OS Evolved Overview](#) | 2

[Directories for Junos OS Evolved File Storage](#) | 11

CHAPTER 1

Junos OS Evolved Overview

IN THIS CHAPTER

- [Junos OS Evolved Overview | 2](#)
- [Understand Graceful Routing Engine Switchover for Junos OS Evolved | 5](#)
- [Nonstop Active Routing Concepts for Junos OS Evolved | 9](#)

Junos OS Evolved Overview

IN THIS SECTION

- [Benefits | 2](#)
- [Native Linux Base | 3](#)
- [Central Database for State | 4](#)
- [Modular Design | 4](#)

Junos OS Evolved is a unified, end-to-end network operating system that provides reliability, agility, and open programmability for successful cloud-scale deployments. With Junos OS Evolved, you can enable higher availability, accelerate your deployments, innovate more rapidly, and operate your network more efficiently. We've aligned Junos OS Evolved with Junos OS so that you can seamlessly continue to manage and to automate your network.

Benefits

Junos OS Evolved provides several benefits to Juniper Networks customers:

- It runs natively on Linux, providing direct access to all the Linux utilities and operations. With Linux integration, you can use standard Linux and open-source tools to speed up onboarding, accelerate

feature adoption with a smooth upgrade process, and enjoy enhanced debugging capabilities for streamlined qualification and deployment.

- Support for 3rd party applications and tools. You can run Linux applications directly on Junos OS Evolved using Docker containers, or create custom applications for advanced networking solutions. You can use existing Linux tools and procedures to create custom functions on a developer-friendly platform with a short learning curve. This versatility allows you to create the solution that best fits your needs through simple third-party application integration and the ability to implement the components required for specific use cases.
- You can install multiple different Junos OS Evolved software releases on a device, with support for rolling back to previous versions. This gives you the flexibility to try out different software releases and easily revert back to your preferred version if necessary.
- Enhanced security at all OS layers. Junos OS Evolved uses an integrity solution called Integrity Measurement Architecture (IMA), and a companion mechanism called the Extended Verification Module (EVM). These open source protections are part of a set of Linux Security Modules that are industry-standard and consistent with the trust mechanisms specified by the Trusted Computing Group. Junos OS Evolved also supports other security features such as TPM infrastructure, hardened secure BIOS, and secure boot. Security is a core design principle for Junos OS Evolved. Juniper Networks is committed to maintaining a strong security infrastructure to keep your network safe and protected.
- Nearly all of the CLI and user interfaces are identical to those provided in Junos OS, meaning you can pick up Junos OS Evolved with a minimal learning curve. These similarities provide simplicity and operational consistency, minimizing the effort required to implement, maintain, and customize your end-to-end solution.

Native Linux Base

Whereas Junos OS runs over an instance of the FreeBSD operating system on a specific hardware element (for example, the CPU on the Routing Engine), Junos OS Evolved runs over a native Linux system. Having Linux as a base leverages a much wider, dynamic, and active development community. The Linux system also contains multiple third-party applications and tools developed for Linux that Junos OS Evolved can integrate with minimal effort.

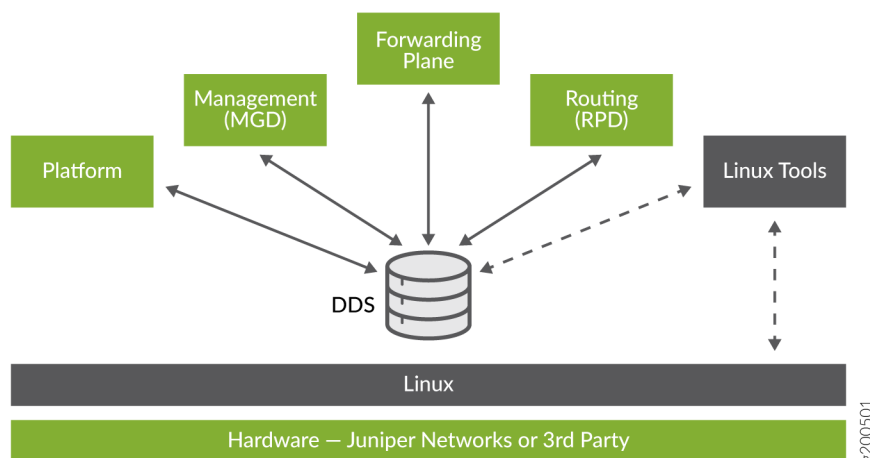
The Junos OS Evolved infrastructure is a horizontal software layer that decouples the application processes from the hardware on which the processes run. Effectively, this decoupling creates a general-purpose software infrastructure spanning all the different compute resources on the system (Routing Engine CPUs, line card CPUs, and possibly others). Application processes (protocols, services, and so on) run on top of this infrastructure and communicate with each other by publishing and consuming (that is, subscribing to) state.

Central Database for State

State is the retained information or status about physical or logical entities that the system preserves and shares across the system, and supplies during restarts. State includes both operational and configuration state, including committed configuration, interface state, routes, and hardware state. In Junos OS Evolved, state can be held in a central database called the Distributed Data Store (DDS).

The DDS does not interpret state. Its only job is to hold state received from subscribers and propagate state to consumers. It implements the publish-subscribe messaging pattern for communicating state between applications that are originators of a state to applications that are consumers of that state (see [Figure 1 on page 4](#)). Each application publishes state to and subscribes to state from the DDS directly, making applications independent of each other.

Figure 1: Publish-Subscribe Model



Decoupling applications in this manner isolates the failure of one application from others. The failing application can restart using the last known state of the system held in the state database.

Modular Design

Junos OS Evolved is composed of components with well-defined interfaces. Applications can be individually restarted without requiring a system reboot. Restarted applications reload the state that is preserved in the DDS.

Understand Graceful Routing Engine Switchover for Junos OS Evolved

IN THIS SECTION

- Graceful Routing Engine Switchover Concepts | 5
- Effects of a Routing Engine Switchover | 7

Graceful Routing Engine Switchover Concepts

The *graceful Routing Engine switchover* (GRES) feature in Junos OS Evolved enables a router with redundant Routing Engines to continue forwarding packets, even if one Routing Engine fails. GRES preserves interface information. Traffic is not interrupted.

NOTE: On PTX10004 and PTX10008 platforms running Junos OS Evolved, GRES is enabled by default and cannot be disabled.

Neighboring routers detect that the router has experienced a restart and react to the event in a manner prescribed by individual routing protocol specifications.

To preserve routing during a switchover, GRES must be combined with either:

- Graceful restart protocol extensions
- *Nonstop active routing* (NSR)

Any updates to the primary Routing Engine during GRES are replicated to the backup Routing Engine as soon as they occur.

NOTE: Because of its synchronization requirements and logic, NSR/GRES performance is limited by the slowest Routing Engine in the system.

The primary role switches to the backup Routing Engine if:

- The primary Routing Engine kernel stops operating.
- The primary Routing Engine experiences a hardware failure.
- The administrator initiates a manual switchover.

NOTE: To quickly restore or to preserve routing protocol state information during a switchover, GRES must be combined with graceful restart or nonstop active routing, respectively. For more information about nonstop active routing, see ["Nonstop Active Routing Concepts" on page 9](#).

If the backup Routing Engine does not receive a keepalive from the primary Routing Engine after 2 seconds, it determines that the primary Routing Engine has failed, and assumes the primary role.

The Packet Forwarding Engine:

- Seamlessly disconnects from the old primary Routing Engine
- Reconnects to the new primary Routing Engine
- Does not reboot
- Does not interrupt traffic

The new primary Routing Engine and the Packet Forwarding Engine then become synchronized. If the new primary Routing Engine detects that the Packet Forwarding Engine state is not up to date, it re-sends state update messages.

NOTE: Successive Routing Engine switchover events must be a minimum of 240 seconds (4 minutes) apart after both Routing Engines have come up.

If the router or switch displays a warning message similar to Standby Routing Engine is not ready for graceful switchover. Packet Forwarding Engines that are not ready for graceful switchover might be reset, do not attempt switchover. If you choose to proceed with switchover, only the Packet Forwarding Engines that were not ready for graceful switchover are reset. None of the FPCs should spontaneously restart. We recommend that you wait until the warning no longer appears and then proceed with the switchover.

NOTE: Check GRES readiness by issuing both:

- The request chassis routing-engine master switch check command from the primary Routing Engine.
- The show system switchover command from the backup Routing Engine.

The switchover preparation process for GRES is as follows:

1. The primary Routing Engine starts.

2. The routing platform processes start.
3. The Packet Forwarding Engine starts and connects to the primary Routing Engine.
4. All state information is updated in the system.
5. The backup Routing Engine starts.
6. The system determines whether GRES has been enabled.
7. The backup Routing Engine is synchronized with the primary Routing Engine.
8. State information and the forwarding table are updated.

A switchover process comprises the following steps:

1. When keepalives from the primary Routing Engine are lost, the system switches over gracefully to the backup Routing Engine.
2. The Packet Forwarding Engine connects to the backup Routing Engine, which becomes the new primary.
3. Routing platform processes that are not part of GRES (such as the routing protocol process (rpd)) restart.
4. State information learned from the point of the switchover is updated in the system.
5. If configured, graceful restart protocol extensions collect and restore routing information from neighboring peer *helper* routers.

Effects of a Routing Engine Switchover

[Table 1 on page 8](#) describes the effects of a Routing Engine switchover when different features are enabled:

- Graceful Routing Engine switchover only
- GRES plus nonstop active routing (NSR)
- GRES plus graceful restart

Table 1: Effects of a Routing Engine Switchover

Feature	Benefits	Considerations
GRES enabled	<ul style="list-style-type: none"> • During the switchover, interface information is preserved. • The switchover is faster because the Packet Forwarding Engines are not restarted. 	<ul style="list-style-type: none"> • The new primary Routing Engine restarts the routing protocol process (rpd). • All adjacent systems are aware of the router's change in state.
GRES <i>and</i> NSR enabled	<ul style="list-style-type: none"> • Traffic is not interrupted during the switchover. • Interface information is preserved. 	<ul style="list-style-type: none"> • Unsupported protocols must be refreshed using the normal recovery mechanisms inherent in each protocol.
GRES <i>and</i> graceful restart enabled	<ul style="list-style-type: none"> • Traffic is not interrupted during the switchover. • Interface information is preserved. • Graceful restart protocol extensions quickly collect and restore routing information from the neighboring routers. 	<ul style="list-style-type: none"> • Neighbors are required to support graceful restart, and a wait interval is required. • The routing protocol process (rpd) restarts. • For certain protocols, a significant change in the network can cause graceful restart to stop.

RELATED DOCUMENTATION

Nonstop Active Routing Concepts for Junos OS Evolved

Nonstop active routing (NSR) uses the same infrastructure as *graceful Routing Engine switchover* (GRES) to preserve interface and kernel information. However, NSR also synchronizes routing protocol information by running the routing protocol process (rpd) on the backup Routing Engine. By synchronizing this additional information, NSR is self-contained and does not rely on helper routers (or switches) to assist the routing platform in restoring routing protocol information. NSR is advantageous in networks in which neighbor routers (or switches) do not support graceful restart protocol extensions. As a result of this enhanced functionality, NSR is a natural replacement for graceful restart.

To activate NSR, use the `set routing-options nonstop-routing` configuration statement.

The switchover preparation process for NSR comprises the following steps:

1. The primary Routing Engine starts.
2. The routing platform processes on the primary Routing Engine (such as the routing protocol process [rpd]) start.
3. The Packet Forwarding Engine starts and connects to the primary Routing Engine.
4. All state information is updated in the system.
5. The backup Routing Engine starts, including the routing protocol process (rpd).
6. The system determines whether GRES and NSR have been enabled.
7. The backup Routing Engine is synchronized with the primary Routing Engine.
8. For supported protocols, state information is updated directly between the routing protocol processes on the primary and backup Routing Engines.

The switchover process comprises the following steps:

1. When keepalives from the primary Routing Engine are lost, the system switches over gracefully to the backup Routing Engine.
2. The Packet Forwarding Engine connects to the backup Routing Engine, which becomes the new primary. Because the routing protocol process (rpd) is already running, this processes do not need to restart.
3. State information learned from the point of the switchover is updated in the system. Forwarding and routing are continued during the switchover, resulting in minimal packet loss.
4. Peer routers or switches continue to interact with the routing platform as if no change had occurred. Routing adjacencies and session state relying on underlying routing information are preserved and not reset.



CAUTION: We recommend that you do not restart the routing protocol process (rpd) on the primary Routing Engine after enabling NSR, as it disrupts the protocol adjacency/peering sessions, resulting in traffic loss.

RELATED DOCUMENTATION

[Understand Graceful Routing Engine Switchover for Junos OS Evolved | 5](#)

Directories for Junos OS Evolved File Storage

IN THIS CHAPTER

- [Default Directories for Junos OS Evolved File Storage | 11](#)
- [Writable Directories for Junos OS Evolved | 12](#)

Default Directories for Junos OS Evolved File Storage

Junos OS Evolved files are stored in the following directories on the device:

- **/boot**—This directory contains the boot loader and associated files.
- **/config**—This directory contains the current operational router or switch configuration and the last three committed configurations, in the files **juniper.conf**, **juniper.conf.1**, **juniper.conf.2**, and **juniper.conf.3**, respectively. The **/config/scripts** directory contains all stored scripts.
- **/data**—This is the directory for all mutable copies of mutable directories. It contains the following subdirectories:
 - **/config**—Contains version-specific Juniper configuration files. This directory is bind mounted to **/config**, meaning that changes in either directory will be reflected in both directories.
 - **/etc**—Contains version-specific Linux configuration files. This directory is bind mounted to **/etc**.
 - **/var**—Shared writable directory for all software versions. This directory is bind mounted to **/var**.
 - **/var_db**—Contains version-specific **/var/db** files. This directory is bind mounted to **/var/db**.
 - **/var_db/scripts**—Contains subdirectories for various script types. Scripts are stored in and executed from these directories. This directory is bind mounted to **/var/db/scripts**.
 - **/var/db/scripts/commit**—Contains SLAX scripts.
 - **/var/db/scripts/op**—Contains op scripts.
 - **/var/db/scripts/event**—Contains event scripts.
 - **/var/db/scripts/snmp**—Contains SNMP scripts.

- **/var/db/scripts/lib**—Contains imported scripts.
- **/var_etc**—Contains version-specific **/var/etc** files. This directory is bind mounted to **/var/etc**.
- **/var_pfe**—Contains version-specific PFE configuration files. This directory is bind mounted to **/var/pfe**.
- **/var_rundb**—Contains UI-related runtime-generated database files that are shared across versions. This directory is bind mounted to **/var/rundb**.
- **/soft**—This directory is the software install area. All software versions are installed here.
- **/u**—This directory is a read-only file system for the running version of Junos OS Evolved.
- **/var**—This directory contains the following subdirectories:
 - **/home**—Contains users' home directories, which are created when you create user access accounts. For users using SSH authentication, their **.ssh** file, which contains their SSH key, is placed in their home directory. When a user saves or loads a configuration file, that file is loaded from the current working directory unless the user specifies a full pathname.
 - **/db/config**—Contains up to 46 previous versions of committed configurations, which are stored in the files **juniper.conf.4.gz** through **juniper.conf.49.gz**.
 - **/log**—Contains system log and tracing files.
 - **/core**—Contains core files. The software saves up to five core files, numbered from 0 through 4. File number 0 is the oldest core file and file number 4 is the newest core file. To preserve the oldest core files, the software overwrites the newest core file, number 4, with any subsequent core file.

RELATED DOCUMENTATION

[Junos OS Evolved Overview](#) | 2

Writable Directories for Junos OS Evolved

IN THIS SECTION

- [How the System Handles Writable Directories](#) | 13

The various versions of software share the same disk and partitions. The run-time environment enables a clean separation of the version's private state while also enabling the sharing of common directories, such as the log files and the core files. The final run-time filesystem topology is read-only by default. The system contains two kinds of writable directories:

- **Shared**—All software versions installed on the device use these directories. These directories hold files such as the log files and core files. For example, **/var** is a shared writable directory.
- **Private**—The individual software versions own these directories. Each version gets a pristine set of these directories and files, based on packaging content, and gets the opportunity to synchronize these files with whatever is the current file version, by peeking under the **/curroot** directory prefix. The system creates these directories in the **/data** partition and uses the name of the directory, with '/' replaced by '_' (slashes replaced with underscores). These directories are bind-mounted during boot up; the files contained within the directory are specific to that software version. The private directory list differs according to the capabilities of the nodes (for example, RE or FPC) and the products (for example, PTX10003 or PTX10008).

How the System Handles Writable Directories

Shared writable directories do not need special handling during software upgrades or rollbacks, because the contents are common across software versions. During software synchronization for dual-RE systems, only the user home directories in **/var/home** for the current software version synchronize to the backup RE from the primary RE. No other contents of the shared writable directories synchronize.

For private writable directories, because these directories are version-specific, the directories need special handling during software upgrades, rollbacks, and synchronizations:

- **Software upgrades**—During the post-install stage of the upgrade to a new version, the system creates a chroot environment for the new version, and the previous version mounts as **/curroot**. The post-install scripts of the new version merge the contents of the previous version's private directories into the new version. Therefore, any user scripts or configurations that are part of the previous version's private writable directories carry forward to the new version.
- **Software rollbacks when you specify the `with-old-snapshot-config` option on the `request system software rollback` command**—The system does not copy over any contents of the running version's private writable directories to the rollback version's private writable directories. After reboot, the system comes up with the contents that were present at the stage when the software upgrade was done from the previous (rollback) version to the currently running version.
- **Software rollbacks without the `with-old-snapshot-config` option**—During the roll back from the running version to the previous version, the system merges the contents of the running version's private writable directories with the previous version's private writable directories, similarly to what happens during a software upgrade.

- Software synchronization (Dual-RE systems only)—The system synchronizes the contents of the private writable directories from the primary RE to the backup RE for the software versions, based upon the option you specify on the `request system software sync` command: `current`, `rollback` or `all-versions`. When you configure the `auto-sw-sync` statement at the `[edit system]` hierarchy level, the system synchronizes all contents of the private writable directories from the primary RE to the backup RE for all software versions.

2

PART

Install, Upgrade, and Downgrade Software

[Software Installation and Upgrade Overview](#) | 16

[Junos OS Evolved Installation Packages](#) | 23

[Prepare to Install and Upgrade Software](#) | 27

[Upgrade and Downgrade Software](#) | 50

[Install Third-Party Software](#) | 71

CHAPTER 3

Software Installation and Upgrade Overview

IN THIS CHAPTER

- [Software Installation and Upgrade Overview \(Junos OS Evolved\) | 16](#)

Software Installation and Upgrade Overview (Junos OS Evolved)

SUMMARY

A Juniper Networks device is delivered with the Juniper Networks operating system (Junos OS Evolved) already installed. When you power on the device, it starts (boots) using the installed software. As new features and software fixes become available, you must upgrade your software to use them.

IN THIS SECTION

- [Types of Junos OS Evolved Installation | 17](#)
- [Multiple Software Versions Available | 17](#)
- [Node Software Synchronization for Dual-RE Systems | 18](#)
- [Back up the Current System's Files | 19](#)
- [Determine the Software Installation Package | 20](#)
- [Connect to the Console | 20](#)
- [Validate the Installation Package with the Current Configuration | 20](#)
- [Upgrade Method Impacts on Internal Media | 21](#)
- [Boot Sequence | 21](#)

Before installing software, you must back up the system, including the configuration. You upgrade (or downgrade) the version of the operating system on a device by copying a software installation package to your device and then use the CLI to install the new software on the device. You then reboot the device, which boots from the newly installed software. After a successful upgrade, back up the new software and configuration. See ["Back up and Recover Software with Snapshots" on page 86](#).

NOTE: Before installing software on a device that has one or more custom YANG data models added to it, back up and remove the configuration data corresponding to the custom YANG data models from the active configuration. For more information see [Managing YANG Packages and Configurations During a Software Upgrade or Downgrade](#).

To understand more about Junos OS Evolved Software Licensing, see the [Juniper Licensing Guide](#). Please refer to the product Data Sheets accessible from [Products & Services](#) for details, or contact your Juniper Account Team or Juniper Partner.

The following sections introduce the overall considerations in upgrading and downgrading the software:

Types of Junos OS Evolved Installation

The two types of installations used to upgrade or downgrade your device are standard installation and recovery. The standard installation is the standard method of upgrading and downgrading the software. You perform a recovery installation when the software on the device is damaged or otherwise unable to accommodate a software upgrade or downgrade.

Standard Installation	A standard installation is the typical method used to upgrade or downgrade software on the server. This method uses the installation package that matches the installation package already installed on the system. For information on the different installation packages available, see " Junos OS Evolved Installation Packages " on page 23.
Recovery Installation	A recovery installation is the method used to repair a device with damaged software or a condition that prevents the upgrade or downgrade of the software.

Multiple Software Versions Available

Junos OS Evolved stores multiple versions of software on the storage media. To see the software packages installed on the system, use the `show system software list operational mode` command. Junos OS Evolved also allows you to roll back to any of the releases already stored on the system with the `request system software rollback operational mode` command.

Each version also stores the last configuration file that was running when that release was running. Junos OS Evolved supports a roll back to an alternate image with either the current configuration file or with the configuration snapshot from when the alternate image was last running, using the `request system software rollback image-name with-old-snapshot-config operational mode` command.

Node Software Synchronization for Dual-RE Systems

Junos OS Evolved ensures all nodes in a system are running the same software version.

If you insert an RE that has the same current software version as the primary RE into the system, the new RE joins the system. The system automatically synchronizes the configurations and the other software versions from the existing RE to the new RE, even if you have not configured the `auto-sw-sync` statement.

If you insert an RE that has a different software version into the system, the RE is kept outside the system and the system generates a software mismatch alarm. The alarm specifies the RE name and the version of software on the newly-inserted RE, similar to the following: `Software Version Mismatch on re1:junos-evo-install-ptx-x86-64-20.4R2.6-EV0`. You need to manually synchronize the REs to bring RE1 back into the system.

```
user@host-re0> show system alarms
2 alarms currently active
Alarm time          Class  Description
2021-04-19 16:02:26 PDT  Major  Re1 Node unreachable
2021-04-19 16:04:46 PDT  Major  Software Version Mismatch on re1:junos-evo-install-ptx-
x86-64-20.4R2.6-EV0
```

You can either manually or automatically synchronize the software versions and configurations to the new RE. Automatic software synchronization is disabled by default. We recommend that you enable automatic software synchronization.

- To automatically always synchronize the software versions and configurations to the new RE, configure the `auto-sw-sync` enable statement at the `[edit system]` hierarchy level. When you configure the `auto-sw-sync` statement, the system detects the new RE, synchronizes all of the images to the new RE, and reboots the new RE so that the new RE boots up with the same software and the same configuration version as the primary RE and joins the system. Each software image contains the configuration running when that software image was last active.
- To manually synchronize the software versions and configurations to the new RE, use the `request system software sync all-versions operational` mode command. All software images and configurations stored with the images are synchronized to the new RE and the system reboots the new RE. When the new RE comes back up, the new RE joins the system.

For a dual-RE system, when the secondary RE boots with a different current image than the primary RE's current image and you have configured the `auto-sw-sync` enable statement, the primary RE synchronizes the current image to the secondary RE. The primary RE also synchronizes the rollback software image and the other images to the secondary RE. If the current configuration file (`juniper.conf.gz`) from the primary RE matches the current configuration file on the secondary RE, then the primary RE does not synchronize the rescue configuration (`rescue.conf.gz`) to the secondary RE.

To synchronize the rescue configuration from the primary RE to the secondary RE, issue the `file copy` command on the primary RE:

```
user@host-re0> file copy /config/rescue.conf.gz re1:/config/
```

For more information on replacing REs, see ["Replace a Routing Engine in a Dual-RE System" on page 67](#).

Back up the Current System's Files

Creating a backup of the current system on your device has the following advantages:

- The device can boot from a backup and come back online in case a component fails or a power failure during an upgrade corrupts the primary boot device.
- The backup copy of the system saves your active configuration files and log files.
- The device can recover from a known, stable environment in case of an unsuccessful upgrade.

During a successful upgrade, the upgrade package completely re-installs the existing operating system. It retains the **juniper.conf**, **rescue.conf**, SNMP ifIndexes, **/var/home**, **/config/scripts**, SSH files, and other filesystem files. The upgrade process removes all other information. Therefore, you should back up your existing system in case you need to return to it after running the installation program.

You create copies of both the software and the configuration running on a device using the `request system snapshot` command. The `request system snapshot` command takes a "snapshot" of the files currently used to run the device—the complete contents of the **/root**, **/soft**, and **/config** file systems, which include the current and all rollback software images, the active configuration, and the rescue configuration—and copies all of these files into an alternate (internal solid-state drive) memory source. You can then use this snapshot to boot the device at the next boot up or as a backup boot option. When the backup completes, the current and backup software installations are identical. For a dual-RE system, you should create a snapshot on both the primary and the secondary RE, ensuring a snapshot is available, no matter which RE you use to reboot the device.

NOTE: When you issue the `request system snapshot` command, the system backs up the **/root** file system and the **/config** file system to the secondary solid-state drive (SSD). The **/root** and **/config** file systems are on the device's primary SSD. The snapshot **/root** and **/config** file systems are on the device's secondary SSD.

Determine the Software Installation Package

Juniper Networks delivers software releases in signed packages that contain digital signatures to ensure official Juniper Networks software. To see the information about the software packages currently running on the device, use the `show version` operational mode command at the top level of the command-line interface (CLI).

NOTE: The `show version` command does not show the software edition, only the release number of the software.

You download software to the `/var/tmp` directory of your device from the [Juniper Networks Software Downloads](#) webpage.

For more information about software packages, see "[Junos OS Evolved Installation Packages](#)" on page 23.

Connect to the Console

We recommend that you upgrade all individual software packages using an out-of-band connection from the console or the management Ethernet interface, because in-band connections can drop during the upgrade process.

Console ports allow root access to devices through a terminal or laptop interface, regardless of the state of the device, unless the device is off. By connecting to the console port, you can access the root level of the device, without using the network to which the device might or might not be connected. Connecting to the console port creates a secondary path to the device without relying on the network.

Using the terminal interface provides a technician, who is usually sitting in a NOC a long distance away, the ability to restore a device or perform an initialization configuration securely, using a modem, even if the primary network has failed. Without a connection to the console port, a technician must visit the site to perform repairs or initialization. A remote connection to the device through a modem requires the cable and connector (provided in the device accessory box), plus a DB-9 to DB-25 (or similar) adapter for your modem, which you must purchase separately. For more information about connecting to the console port, see the hardware guide for your particular device.

Validate the Installation Package with the Current Configuration

When you upgrade or downgrade software, we recommend that you validate the configuration with the `request system software add` operational mode command, to check that the candidate software is compatible with the current configuration. By default, when you add a package with a different release number, the system automatically performs the validation check.

Upgrade Method Impacts on Internal Media

Installation from the boot loader using a USB storage device re-formats the internal media before installation.

Installation using the CLI retains the existing partitioning scheme.



CAUTION: Upgrade methods that re-format the internal media before installation wipe out the existing contents of the media and the configuration files. You must back up all configuration files in the **/config** directory and any important data before starting the installation process.

Boot Sequence

Juniper Networks devices start using the installed Junos OS Evolved software. Boot-able copies of the software are stored in two locations: the internal solid-state drive and the removable media (USB). The following subsections discuss the order of the locations the system checks for a valid boot-able operating system.

Boot Order

Junos OS Evolved devices attempt to boot from these storage media in the following order:

1. Dual, internal SSD devices. First, the system tries to boot from the primary SSD device. If that SSD fails to boot, then the system attempts to boot from the secondary SSD device.
2. USB device. (If you insert a USB emergency boot device, select **USB00** from the Grub menu to boot from the USB device.)

Boot from an Alternate Boot Device

If the device boots from an alternate boot device, when you log in to the device, a message displays indicating the alternate boot device. For example, the following message shows that the software booted from the secondary SSD (**/dev/sdb**):

```
login: username
Password: password
[...output truncated...]
--- NOTICE: System is running on alternate media device (/dev/sdb).
```

NOTE: Do not select an emergency boot device during reboot under normal operations. The router does not operate normally when booted from an emergency boot device. Selecting the USB00 option on the Grub menu installs the image from the USB onto the SSD. You must then apply the user configuration.

The system boots from an alternate boot device when the system detects a problem with the primary boot device—usually the primary SSD (**/dev/sda**)—that prevents the device from booting. Consequently, the system boots from the alternate boot device (the secondary SSD, **/dev/sdb**). When the system boots from the alternate boot device, the system removes the primary boot device from the list of candidate boot devices. The problem is usually a serious hardware error. We recommend you contact the Juniper Networks Technical Assistance Center (JTAC).

When the device boots from the alternate boot device, the software and the configuration are only as current as the most recent snapshot (taken with the `request system snapshot operational mode` command).

RELATED DOCUMENTATION

[Before You Upgrade or Reinstall Junos OS Evolved](#) | 33

Junos OS Evolved Installation Packages

IN THIS CHAPTER

- [Junos OS Evolved Installation Packages | 23](#)

Junos OS Evolved Installation Packages

SUMMARY

The installation package is used to upgrade or downgrade from one Junos OS Evolved release to another. When added, the installation package completely re-installs the software, rebuilds the file system, and can erase system logs and other auxiliary information from the previous installation. The system does, however, retain the configuration files from the previous installation.

IN THIS SECTION

- [Junos OS Evolved Installation Package Prefixes | 23](#)
- [Junos OS Evolved Release Numbers | 25](#)
- [Junos OS Evolved Editions | 26](#)

The names of the Junos OS Evolved installation packages have the following general pattern:

- *prefix-release-edition.iso*

Juniper Networks delivers the Junos OS Evolved software in signed packages that contain digital signatures. The system only installs a package if the checksum within it matches the hash recorded in its corresponding file.

Junos OS Evolved Installation Package Prefixes

The first part of the installation package filename is a combination of a standard prefix and a product designation.

Table 2: Installation Package Prefixes

Prefix	Description
junos-evo-install* or junos-evo-install-media*	<p>Introduced as of Junos OS Evolved Release 18.3R1. For Junos OS Evolved, there is a single image for all fixed form (versus chassis) platforms, and a platform image name can also be distinguished as merchant silicon (ms). Starting in Junos OS Evolved Release 20.3R1, install packages are available in limited editions. See "Junos OS Evolved Editions" on page 26. Here are some examples:</p> <ul style="list-style-type: none"> • junos-evo-install-acx-qfx-7k-x86-64-release.iso—A single ISO image for the ACX7100 platforms. • junos-evo-install-acx-t-x86-64-release.iso—A single ISO image for the ACX6160 platforms. • junos-evo-install-acx-x86-64-release.iso—A single ISO image for ACX chassis platforms. • junos-evo-install-ptx-fixed-x86-32-release.iso—All fixed PTX platform variants (that is, PTX10001-36MR, and so on) have a single ISO image. • junos-evo-install-ptx-fixed-x86-64-release.iso—All fixed PTX platform variants (that is, PTX10003, and so on) have a single ISO image. For PTX orders, this image is installed as factory default. • junos-evo-install-ptx-chassis-x86-64-release.iso—One single ISO image for PTX chassis platforms. • junos-evo-install-qfx-ms-fixed-x86-64-release.iso—Single image for all QFX platforms based on merchant silicon. It could be the Broadcom family or any other vendor. • junos-evo-install-qfx-fixed-x86-64-release.iso—All fixed QFX platform variants have a single ISO image. For QFX orders, this image is installed as factory default. • junos-evo-install-qfx-chassis-x86-64-release.iso—One single ISO image for QFX chassis platforms.

Junos OS Evolved Release Numbers

NOTE: Junos OS Evolved uses the same release numbering system as Junos OS.

Each release has certain new features that complement the software processes that support Internet routing protocols, control the device's interfaces and the device chassis, and allow for device system management. From the web page for [Juniper Networks Software Downloads](#), you download software for a particular release number.

In this example, we dissect the format of the software release number in the installation package to show what it indicates. The generalized format is as follows:

Given the format of:

- *m.nZb.s-EVO*

The software release number 20.4R1.17-EVO, for example, maps to this format as follows:

- *m* is the main release number of the product, for example, 20.
- *n* is the minor release number of the product, for example, 4.
- *Z* is the type of software release, for example, R for an FRS or a maintenance release.

For types of software releases, see [Table 3 on page 25](#).

- *b* is the build number of the product, for example, 1, indicating the FRS rather than a maintenance release.
- *s* is the spin number of the product, for example, 17.
- -EVO means that it is a Junos OS Evolved package.

Table 3: Software Release Types

Release Type	Description
R	First revenue ship (FRS) or maintenance release software. R1 is FRS. R2 is a maintenance release.
B	Beta release software.

Table 3: Software Release Types *(Continued)*

Release Type	Description
I	Internal release software. These packages are private software releases for verifying fixes.
S	Service release software, released to customers to solve a specific problem—Juniper Networks will maintain this release along with the life span of the underlying release. The service release number is after the R number; for example, 20.3R1-S2.12. Here, S2 represents the 2nd service release on top of 20.3R1 and is the 12th re-spin.

Junos OS Evolved Editions

Edition names show up in the installation package name between the release number string and the extension.

For Junos OS Evolved:

- A null (empty) edition field denotes the standard image for Junos OS Evolved.
- **limited**—Starting in Junos OS Evolved 20.3R1, limited packages are available. Limited packages do not have cryptographic support and are intended for countries in the Eurasian Customs Union (EACU). These countries have import restrictions on software containing data-plane encryption. An example of a limited package image for a PTX router is **junos-evo-install-ptx-fixed-x86-64-20.4R1.17-EVO-limited.iso**.

RELATED DOCUMENTATION

[show version \(Junos OS Evolved\)](#) | 291

Prepare to Install and Upgrade Software

IN THIS CHAPTER

- [Ensure Sufficient Disk Space for Upgrades | 27](#)
- [Before You Upgrade or Reinstall Junos OS Evolved | 33](#)
- [Validate the Configuration against the Installation Image | 48](#)

Ensure Sufficient Disk Space for Upgrades

SUMMARY

The amount of free disk space necessary to upgrade a device with a new version of Junos OS Evolved can vary from one release to another. Check the software version you are installing to determine the free disk space requirements, and then clear enough disk space for the upgrade.

If the `/soft`, `/var`, or `/data` directories are at 90% capacity or more, the device does not have enough storage space to install a software package. If the amount of storage space on a device is insufficient for installing Junos OS Evolved, you might receive a warning similar to the following messages, that a file system is low on free disk space:

```
WARNING: The /soft filesystem is low on free disk space.
```

```
WARNING: This package requires 1075136k free, but there is only 666502k available.
```

When the system file storage space on the device is full, rebooting the device does not solve the problem. The following error message displays during a typical operation on the device after the file storage space is full: `user@host> configure /soft: write failed, filesystem is full`

1. To determine the amount of free disk space on the device, issue the `show system storage` command. The command output displays statistics about the amount of free disk space in the device's file system.

For example:

```
user@host> show system storage
```

```
fpc0:
```

```
-----
Filesystem      Size      Used      Avail  Capacity  Mounted on
/dev/root        30M       30M        0      100%    /run/initramfs
/dev/ram1p2      4.9G     586M      4.0G     13%    /soft
/dev/ram1p5       93M       19M       68M     22%    /data
/dev/ram1p7      2.7G      66M      2.4G      3%    /var
/dev/loop0       379M      2.3M     353M      1%    /data/var/external
devtmpfs         16G        0       16G      0%    /dev
[...output truncated...]
```

```
fpc1:
```

```
-----
Filesystem      Size      Used      Avail  Capacity  Mounted on
/dev/root        30M       30M        0      100%    /run/initramfs
/dev/ram1p2      4.9G     586M      4.0G     13%    /soft
/dev/ram1p5       93M       19M       68M     22%    /data
/dev/ram1p7      2.7G      42M      2.5G      2%    /var
/dev/loop0       379M      2.3M     353M      1%    /data/var/external
devtmpfs         16G        0       16G      0%    /dev
[...output truncated...]
```

```
re0:
```

```
-----
Filesystem      Size      Used      Avail  Capacity  Mounted on
/dev/root        34M       34M        0      100%    /run/initramfs
/dev/sda2        32G      10G      21G     34%    /soft
/dev/sda5        3.0G     179M      2.6G      7%    /data
/dev/sda7       145G     4.5G     134G      4%    /var
/dev/loop0       15G      38M      14G      1%    /data/var/external
devtmpfs         32G        0      32G      0%    /dev
/tmp             32G        0      32G      0%    /run/initramfs/uswitch/tmp
/dev/loop1       517M     517M        0     100%    /run/initramfs/uswitch/data/
hashes/8e6065a478c593473cd390245274128f1a5885e8
/dev/loop2        29M      29M        0     100%    /run/initramfs/uswitch/data/
hashes/244e2161887b001792709ec078f864c966baca88
/dev/loop3        36M      36M        0     100%    /run/initramfs/uswitch/data/
hashes/4cad203feb9c1bd4a903f03503a6777509e4031d
/dev/loop4        10M      10M        0     100%    /run/initramfs/uswitch/data/
```

```

hashes/5f9454b8d26e33715373f621d16c9c752e3ff57b
/dev/loop5          46M      46M      0      100% /run/initramfs/switch/data/
hashes/182901abd18cfe6f63397bcb6f2a8238d38a9b
/dev/loop6          9.8M      9.8M      0      100% /run/initramfs/switch/data/
hashes/c08bb2c69ae7ff2446bdb32011a03a4a53c5585
/dev/loop7          58M      58M      0      100% /run/initramfs/switch/data/
hashes/c92e70dc394c01bf5a2a9d06ffcc25ba673286d1
/dev/loop8          34M      34M      0      100% /run/initramfs/switch/data/
hashes/90fdfeec1bab47c19641d636598a4205bbb7949d
/dev/loop9          8.2M      8.2M      0      100% /run/initramfs/switch/data/
hashes/3874cf9fea904b2d5d3f6920671864bdc05130a2
/dev/loop10         34M      34M      0      100% /run/initramfs/switch/data/
hashes/35afa8ff63aded42bd23444b672dcd33b922898c
/dev/loop11         7.0M      7.0M      0      100% /run/initramfs/switch/data/
hashes/15684de48b2a621a98afaf9619026dd81cdf74bd
/dev/loop12         4.5M      4.5M      0      100% /run/initramfs/switch/data/
hashes/2d75968c5d882c86b38015fc93fe9e148e226407
/dev/loop13         148M     148M      0      100% /run/initramfs/switch/data/
hashes/ccb0c8af3d4b26bdf9ccc047aa7e76d34e31387
switchd             7.0M      7.0M      0      100% /run/initramfs/switch/data/
junos-evo-install-ptx-x86-64-21.2I20210315015050-EVO__cd-builder/switch
unionfs             3.0G      186M      2.6G      7% /
/dev/sda1            196M      19M      178M     10% /boot
/dev/sda6            984M      1.5M      916M      1% /data/config
/tmp                 32G       68K      32G      1% /tmp
tmpfs                32G       28M      32G      1% /run
tmpfs                32G      123M      32G      1% /dev/shm
tmpfs                32G        0      32G      0% /sys/fs/cgroup
tmpfs                6.3G        0      6.3G      0% /run/user/0

re1:
-----
Filesystem      Size      Used      Avail  Capacity  Mounted on
/dev/root        34M       34M        0     100% /run/initramfs
/dev/sda2        32G      10G       21G     34% /soft
/dev/sda5        3.0G     321M     2.5G     12% /data
/dev/sda7        145G     3.0G    135G      3% /var
/dev/loop0       15G       38M       14G      1% /data/var/external
devtmpfs         32G        0       32G      0% /dev
[...output truncated...]

```

2. If the amount of free disk space on a device is insufficient for installing Junos OS Evolved, you can clean up the file storage on the device by deleting the system files or unnecessary software images.

You can use either the request system storage cleanup or the request system software delete operational mode command, or both, depending on where you need to clear space.

- a. Issue the request system storage cleanup operational mode command on the primary RE to delete system files in the **/var** directory for all REs in a system, usually system-log and trace files.

The list of files to be deleted displays:

```
user@host> request system storage cleanup
List of files to delete:
```

Size	Date	Name
11B	Oct 28 23:40	/var/jail/tmp/alarmd.ts
92.4K	Jan 11 17:12	/var/log/chassisd.0.gz
92.4K	Jan 11 06:06	/var/log/chassisd.1.gz
92.5K	Jan 10 19:00	/var/log/chassisd.2.gz
92.5K	Jan 10 07:53	/var/log/chassisd.3.gz
92.2K	Jan 10 15:00	/var/log/hostlogs/auth.log.1.gz
92.2K	Jan 1 18:45	/var/log/hostlogs/auth.log.2.gz
92.1K	Jan 4 17:30	/var/log/hostlogs/auth.log.3.gz
92.2K	Jan 1 18:45	/var/log/hostlogs/auth.log.4.gz
79.0K	Jan 12 01:59	/var/log/hostlogs/daemon.log.1.gz
78.8K	Jan 11 23:15	/var/log/hostlogs/daemon.log.2.gz
78.7K	Jan 11 20:30	/var/log/hostlogs/daemon.log.3.gz
79.1K	Jan 11 17:44	/var/log/hostlogs/daemon.log.4.gz
59.1K	Jan 11 21:59	/var/log/hostlogs/debug.1.gz
59.2K	Jan 11 17:44	/var/log/hostlogs/debug.2.gz
59.2K	Jan 11 13:29	/var/log/hostlogs/debug.3.gz
59.3K	Jan 11 09:14	/var/log/hostlogs/debug.4.gz
186.6K	Oct 20 16:31	/var/log/hostlogs/kern.log.1.gz
238.3K	Jan 11 23:15	/var/log/hostlogs/lcmd.log.1.gz
238.4K	Jan 11 17:30	/var/log/hostlogs/lcmd.log.2.gz
238.6K	Jan 11 11:45	/var/log/hostlogs/lcmd.log.3.gz
238.5K	Jan 11 06:00	/var/log/hostlogs/lcmd.log.4.gz
372.5K	Jan 11 17:00	/var/log/hostlogs/syslog.1.gz
372.5K	Jan 11 04:45	/var/log/hostlogs/syslog.2.gz
371.9K	Jan 10 16:30	/var/log/hostlogs/syslog.3.gz
372.7K	Jan 10 04:15	/var/log/hostlogs/syslog.4.gz
10.1K	Jan 12 02:03	/var/log/messages.0.gz
55.1K	Jan 6 21:25	/var/log/messages.1.gz
81.5K	Dec 1 21:30	/var/log/messages.2.gz

Delete these files ? [yes,no] (no)

Enter the option **yes** to delete the files.

- b. Before you can clean up unnecessary software images in the **/soft** and **/data** directories for all REs in a system, you must first find out what images exist on the device, using the `show system software list operational` mode command.

```

-----
node: fpc0
-----
Active boot device is primary: /dev/ram1
List of installed version(s) :

    '-' running version
    '>' next boot version after upgrade/downgrade
    '<' rollback boot version

-   junos-evo-install-ptx-x86-64-20.4-202103151929.0-EVO - [2021-03-17 12:18:07]
-----
node: re0
-----
Active boot device is primary: /dev/sda
List of installed version(s) :

    '-' running version
    '>' next boot version after upgrade/downgrade
    '<' rollback boot version

<   junos-evo-install-ptx-x86-64-20.4-202103121629.0-EVO - [2021-03-17 11:22:40]
-   junos-evo-install-ptx-x86-64-20.4-202103151929.0-EVO - [2021-03-17 10:50:39]
    junos-evo-install-ptx-x86-64-20.4-202103131143.0-EVO - [2021-03-16 16:12:38]
    junos-evo-install-ptx-x86-64-20.4-202103141559.0-EVO - [2021-03-15 17:26:42]
-----
node: re1
-----
Active boot device is primary: /dev/sda
List of installed version(s) :

    '-' running version
    '>' next boot version after upgrade/downgrade
    '<' rollback boot version

```

```
< junos-evo-install-ptx-x86-64-20.4-202103121629.0-EVO - [2021-03-17 11:25:03]
- junos-evo-install-ptx-x86-64-20.4-202103151929.0-EVO - [2021-03-17 10:50:39]
  junos-evo-install-ptx-x86-64-20.4-202103131143.0-EVO - [2021-03-16 16:14:55]
  junos-evo-install-ptx-x86-64-20.4-202103141559.0-EVO - [2021-03-15 17:57:05]
```

You can delete software images one at a time or you can delete all software images except for the current and rollback images. These commands delete the images on all REs in the system.

- To delete the software images one at a time, issue the request `system software delete image-name` operational mode command for each image you need to delete. If you delete this image, you cannot downgrade to this particular version of the software. You cannot delete the currently running software version. Use the force option to delete the rollback software image.
- Starting in Junos OS Evolved Release 20.4R2, to delete all software images except for the current and rollback images, issue the request `system software delete archived` operational mode command. This command fails when a next-boot software image is on the RE; a new software image was installed, but the device has not yet been rebooted to finish the installation process.

```
user@host-re0> request system software delete archived
ALERT: This command will delete all archived SW versions except current and rollback.
       Do you want to proceed? [yes,no] (no) yes

Software delete in progress...
re0: Executing Software delete...
re0: Cannot delete junos-evo-install-ptx-x86-64-20.4-202103141559.0-EVO - It is the
current version
re0: Rollback or scratch install
re0: Removing version junos-evo-install-ptx-x86-64-20.4-202103150459.0-EVO...
re0: Removing version junos-evo-install-ptx-x86-64-20.4-202103111254.0-EVO...
re1: Removing version junos-evo-install-ptx-x86-64-20.4-202103150459.0-EVO...
re1: Removing version junos-evo-install-ptx-x86-64-20.4-202103111254.0-EVO...
Image deletion succeeded.
```

RELATED DOCUMENTATION

[request system software delete \(Junos OS Evolved\)](#) | 200

Before You Upgrade or Reinstall Junos OS Evolved

SUMMARY

Before you upgrade or reinstall Junos OS Evolved, you must save some system information, ensure enough disk space is available, and back up the current software and configuration.

You need to gather and to save information about the current state of the system so that you can compare the state before and after the upgrade to make sure the system is correctly configured and operating. You also need to take a snapshot of the system software and configuration before you upgrade, so that you are able to recover the system if necessary.

- 1. To check if enough disk space is available for the installation, use the `show system storage` operational mode command.

Various directories store the installed software versions and the data files, such as the log and core files. If the (`/soft`, `/var`, or `/data`) directories are at 90% capacity or more, the device does not have enough storage space to install a software package. A software installation could fail if these directories do not have sufficient space.

We recommend that you store no more than 5 versions of software on the device. Please use the `request system software delete` operational mode command to delete older or unused versions of software. To delete all but the current and the rollback versions of the software, use the `request system software delete archived` operational mode command.

Use the `request system storage cleanup` operational mode command if your storage area (the `/var` directory) is full. We recommend that you issue this command before you copy the new image into the `/var/tmp` directory as this command could remove the image if the `/var` partition is low on space.

For more information, see ["Ensure Sufficient Disk Space for Upgrades" on page 27](#).

The sample output displays statistics about the amount of free disk space in the device's file system for the FPCs and REs.

```
user@host> show system storage
fpc0:
-----
Filesystem      Size      Used      Avail  Capacity  Mounted on
/dev/root        30M       30M         0      100%  /run/initramfs
/dev/ram1p2      4.9G     586M     4.0G       13%  /soft
```



```

/dev/ram1p5          93M      19M      68M      22% /data
/dev/ram1p7          2.7G      66M      2.4G       3% /var
/dev/loop0           379M      2.3M     353M       1% /data/var/external
devtmpfs             16G        0      16G        0% /dev
[...output truncated...]

```

fpc1:

```

-----
Filesystem      Size      Used      Avail  Capacity  Mounted on
/dev/root        30M       30M        0      100% /run/initramfs
/dev/ram1p2      4.9G     586M      4.0G      13% /soft
/dev/ram1p5      93M       19M       68M      22% /data
/dev/ram1p7      2.7G      42M      2.5G       2% /var
/dev/loop0       379M      2.3M     353M       1% /data/var/external
devtmpfs         16G        0      16G        0% /dev
[...output truncated...]

```

re0:

```

-----
Filesystem      Size      Used      Avail  Capacity  Mounted on
/dev/root        34M       34M        0      100% /run/initramfs
/dev/sda2        32G       10G       21G      34% /soft
/dev/sda5        3.0G     179M      2.6G       7% /data
/dev/sda7        145G      4.5G     134G       4% /var
/dev/loop0       15G       38M       14G       1% /data/var/external
devtmpfs         32G        0      32G        0% /dev
/tmp             32G        0      32G        0% /run/initramfs/uswitch/tmp
/dev/loop1       517M     517M        0      100% /run/initramfs/uswitch/data/
hashes/8e6065a478c593473cd390245274128f1a5885e8
/dev/loop2        29M       29M        0      100% /run/initramfs/uswitch/data/
hashes/244e2161887b001792709ec078f864c966baca88
/dev/loop3        36M       36M        0      100% /run/initramfs/uswitch/data/
hashes/4cad203feb9c1bd4a903f03503a6777509e4031d
/dev/loop4        10M       10M        0      100% /run/initramfs/uswitch/data/
hashes/5f9454b8d26e33715373f621d16c9c752e3ff57b
/dev/loop5        46M       46M        0      100% /run/initramfs/uswitch/data/
hashes/182901abd18cefe6f63397bcbb6f2a8238d38a9b
/dev/loop6        9.8M      9.8M        0      100% /run/initramfs/uswitch/data/
hashes/c08bb2c69ae7ff2446bdbcb32011a03a4a53c5585
/dev/loop7        58M       58M        0      100% /run/initramfs/uswitch/data/
hashes/c92e70dc394c01bf5a2a9d06ffcc25ba673286d1
/dev/loop8        34M       34M        0      100% /run/initramfs/uswitch/data/
hashes/90fdfeec1bab47c19641d636598a4205bbb7949d

```

```

/dev/loop9          8.2M      8.2M      0      100% /run/initramfs/switch/data/
hashes/3874cf9fea904b2d5d3f6920671864bdc05130a2
/dev/loop10         34M       34M      0      100% /run/initramfs/switch/data/
hashes/35afa8ff63aded42bd23444b672dcd33b922898c
/dev/loop11         7.0M      7.0M      0      100% /run/initramfs/switch/data/
hashes/15684de48b2a621a98afaf9619026dd81cdf74bd
/dev/loop12         4.5M      4.5M      0      100% /run/initramfs/switch/data/
hashes/2d75968c5d882c86b38015fc93fe9e148e226407
/dev/loop13         148M      148M      0      100% /run/initramfs/switch/data/
hashes/ccb0c8af3d4b26bdf9ccc047aa7e76d34e31387
switchd             7.0M      7.0M      0      100% /run/initramfs/switch/data/
junos-evo-install-ptx-x86-64-21.2I20210315015050-EVO__cd-builder/switch
unionfs             3.0G      186M      2.6G      7% /
/dev/sda1           196M      19M      178M     10% /boot
/dev/sda6           984M      1.5M     916M      1% /data/config
/tmp                32G       68K      32G      1% /tmp
tmpfs               32G       28M      32G      1% /run
tmpfs               32G      123M      32G      1% /dev/shm
tmpfs               32G        0      32G      0% /sys/fs/cgroup
tmpfs               6.3G        0      6.3G      0% /run/user/0

rel:
-----
Filesystem      Size      Used      Avail  Capacity  Mounted on
/dev/root        34M       34M        0     100% /run/initramfs
/dev/sda2        32G       10G       21G     34% /soft
/dev/sda5        3.0G      321M       2.5G     12% /data
/dev/sda7        145G      3.0G      135G      3% /var
/dev/loop0       15G       38M       14G      1% /data/var/external
devtmpfs         32G        0      32G      0% /dev
[...output truncated...]

```

2. To save the system software information, use the `show version detail | save filename` and the `show system software list operational mode` commands.

The `save filename` option saves the information in a file for you to look at later, after you upgrade the system, to compare to the current state.

- a. Issue the `show version detail | save filename` command.

```

user@host> show version detail | save /var/tmp/swversion.old
Wrote 3274 lines of output to '/var/tmp/swversion.old'

```

The sample output shows the contents of the saved file: the hostname, device model, current software package name, and the various Junos OS Evolved processes and their release numbers.

```

Hostname: host-02-re0
Model: ptx10008
Junos: junos-evo-install-ptx-x86-64-20.4R1.17-EV0.iso
Yocto: 2.2.1
Linux Kernel: 4.8.28-WR2.2.1_standard-g65c1491
JUNOS-EVO OS 64-bit [junos-evo-install-ptx-x86-64-20.4R1.17-EV0.iso]
aapl_25x release 67
accountd release 20
accountd-app-config release 20
accountd-policy release 4
accounting_module release 95
accounting_module-evl release 95
action-scripts release 1
addrwatch_module release 34
addrwatch_module-evl release 34
aft-sysinfo-policy release 3
[...output truncated...]

```

- b. Issue the `show system software list | save filename` command.

```

user@host> show system software list | save /var/tmp/swlist.old
Wrote 39 lines of output to '/var/tmp/swlist.old'

```

The sample output shows the contents of the saved file: all the software versions in the persistent storage on the Routing Engines in the system and the current software version running on the FPCs. FPCs cannot store more than one version, because FPCs do not contain any persistent storage media.

```

-----
node: fpc0
-----
Active boot device is primary: /dev/ram1
List of installed version(s) :

    '-' running version
    '>' next boot version after upgrade/downgrade

```

```

'<' rollback boot version

- junos-evo-install-ptx-x86-64-20.4-202103151929.0-EVO - [2021-03-17 12:18:07]
-----
node: re0
-----
Active boot device is primary: /dev/sda
List of installed version(s) :

'-' running version
'>' next boot version after upgrade/downgrade
'<' rollback boot version

< junos-evo-install-ptx-x86-64-20.4-202103121629.0-EVO - [2021-03-17 11:22:40]
- junos-evo-install-ptx-x86-64-20.4-202103151929.0-EVO - [2021-03-17 10:50:39]
  junos-evo-install-ptx-x86-64-20.4-202103131143.0-EVO - [2021-03-16 16:12:38]
  junos-evo-install-ptx-x86-64-20.4-202103141559.0-EVO - [2021-03-15 17:26:42]
-----
node: re1
-----
Active boot device is primary: /dev/sda
List of installed version(s) :

'-' running version
'>' next boot version after upgrade/downgrade
'<' rollback boot version

< junos-evo-install-ptx-x86-64-20.4-202103121629.0-EVO - [2021-03-17 11:25:03]
- junos-evo-install-ptx-x86-64-20.4-202103151929.0-EVO - [2021-03-17 10:50:39]
  junos-evo-install-ptx-x86-64-20.4-202103131143.0-EVO - [2021-03-16 16:14:55]
  junos-evo-install-ptx-x86-64-20.4-202103141559.0-EVO - [2021-03-15 17:57:05]

```

3. To save the active configuration on the device, which is the last committed configuration, use the `show configuration | save filename operational` mode command.

If you need to make changes to the configuration before you install the software package, now is a good time to do so, before you capture any further information about your system. After you change the configuration and commit it, save a copy of it in the `/var/tmp` directory.

```

user@host> show configuration | save /var/tmp/config.old
Wrote 345 lines of output to '/var/tmp/config.old'

```

4. To save information about the system alarms, use the `show system alarms | save filename` operational mode command.

```
user@host> show system alarms | save /var/tmp/alarms.old
Wrote 14 lines of output to '/var/tmp/alarms.old'
```

The sample output shows the contents of the saved file: information about the active alarms.

Alarm time	Class	Description
2021-03-31 17:22:10 PDT	Minor	CB 0 Temp Sensor Fail
2021-04-01 10:51:01 PDT	Minor	FAN 1 Power Sensor Fail
2021-03-31 01:36:38 PDT	Major	PSM 0 Input1 Failed
2021-03-31 01:36:38 PDT	Major	PSM 0 Input2 Failed
2021-03-31 01:36:13 PDT	Major	PSM 1 Input2 Failed
2021-03-31 01:36:38 PDT	Major	PSM 2 Input1 Failed
2021-03-31 01:36:38 PDT	Major	PSM 2 Input2 Failed
2021-03-31 01:36:13 PDT	Major	PSM 3 Input2 Failed
2021-03-31 01:36:13 PDT	Major	PSM 4 Input2 Failed
2021-03-31 01:36:13 PDT	Major	PSM 5 Input2 Failed
2021-04-01 10:22:58 PDT	Minor	RE 0 Secure boot disabled or not enforced
2021-03-31 01:35:52 PDT	Minor	RE 1 Secure boot disabled or not enforced
2021-04-01 10:46:18 PDT	Major	chassis No Redundant Power

5. To save information about the nodes in the system, use the `show system nodes | save filename` operational mode command.

```
user@host> show system nodes | save /var/tmp/nodes.old
Wrote 47 lines of output to '/var/tmp/nodes.old'
```

The sample output shows the contents of the saved file: node information about the FPCs and REs in the system.

```
Node: fpc0
Node Id      : 2201170739216
Node Nonce   : 3051624042
Status       : online, apps-ready
Attributes   : ASICS (Active), BT (Active), FABRIC_PFE (Active), FPC (Active), PIC
              (Active), TIMINGD_FPC (Active), MSVCSD (Active), SFLOWD (Active)
```

```

Node: fpc1
  Node Id    : 2201170739217
  Node Nonce : 524098764
  Status     : online, apps-ready
  Attributes : ASICS (Active), BT (Active), FABRIC_PFE (Active), FPC (Active), PIC
               (Active), TIMINGD_FPC (Active), MSVCSD (Active), SFLOWD (Active)
[...output truncated...]
Node: re0
  Node Id    : 2201170739204
  Node Nonce : 1409607325
  Status     : online
  Attributes : FABRIC_CONTROL (Active), FABRIC_FCHIP_PARALLEL (Active), RE (Active),
               TIMINGD_RE (Active), MasterRE (Active), GlobalIPOwner (Active)
Node: re1
  Node Id    : 2201170739205
  Node Nonce : 4092367597
  Status     : online, apps-ready
  Attributes : FABRIC_CONTROL (Spare), FABRIC_FCHIP_PARALLEL (Spare), RE (Spare),
               TIMINGD_RE (Spare), BackupRE (Active)

```

6. To save the hardware component information, use the `show chassis hardware | save filename` operational mode command.

You will need the hardware information if the device cannot successfully reboot after the upgrade and so you cannot access the serial number for the Routing Engine. The Routing Engine serial number is necessary for the Juniper Networks Technical Assistance Center (JTAC) to issue a return to manufacturing authorization (RMA). Without the Routing Engine serial number, JTAC must dispatch an on-site technician to issue the RMA.

```

user@host> show chassis hardware | save /var/tmp/hwinventory.old
Wrote 32 lines of output to '/var/tmp/hwinventory.old'

```

You should then upload this file to an off-box location using `scp`.

```

user@host> file copy scp:///var/tmp/hwinventory.old user@remotehost.com:filename

```

The output varies depending on the chassis components of the device. Refer to the hardware guides for information about the different chassis components. The sample output shows the contents of the saved file: the hardware inventory for a PTX10008 router.

Hardware inventory:

Item	Version	Part number	Serial number	Description
Chassis			AA100	JNP10008 [PTX10008]
Midplane 0	REV 16	750-086802	AAAA1001	Midplane 8
FPM 0	REV 02	711-086964	AAAA2002	Front Panel Display
PSM 0	Rev 03	740-069994	1B21B000001	JNP10K 5500W AC/HVDC Power Supply
Unit				
PSM 1	Rev 03	740-069994	1B21B000002	JNP10K 5500W AC/HVDC Power Supply
Unit				
PSM 2	Rev 03	740-069994	1B21B000003	JNP10K 5500W AC/HVDC Power Supply
Unit				
Routing Engine 0		BUILTIN	BUILTIN	JNP10K-RE1-E
Routing Engine 1		BUILTIN	BUILTIN	JNP10K-RE1-E
CB 0	REV 06	750-101345	AAAA3001	Control Board
CB 1	REV 06	750-101345	AAAA3002	Control Board
FPC 0	REV 38	750-093524	BBBB0001	JNP10K-LC1201
CPU	REV 10	750-087304	CCCC0001	JNP10K-LC1201 PMB Board
PIC 0		BUILTIN	BUILTIN	JNP10K-36QDD-LC-PIC
Xcvr 0	REV 01	740-061405	1AAQ00000AA	QSFP-100GBASE-SR4-T2
Xcvr 1	REV 01	740-061405	1AAQ00001AA	QSFP-100GBASE-SR4-T2
Xcvr 2	REV 01	740-058734	1AAQ00002AA	QSFP-100GBASE-SR4
Xcvr 3	REV 01	740-061405	1AAQ00003AA	QSFP-100GBASE-SR4-T2
Xcvr 4	REV 01	740-067443	QA0001AA	QSFP+-40G-SR4
Xcvr 5	REV 01	740-054053	QA0002AA	QSFP+-4X10G-SR
MEZZ 0	REV 10	711-084968	DDDD0001	JNP10K-LC1201 MEZZ Board
FPC 1	REV 38	750-093524	BBBB0002	JNP10K-LC1201
CPU	REV 10	750-087304	CCCC0002	JNP10K-LC1201 PMB Board
PIC 0		BUILTIN	BUILTIN	JNP10K-36QDD-LC-PIC
MEZZ 0	REV 10	711-084968	DDDD0002	JNP10K-LC1201 MEZZ Board
SIB 0	REV 30	750-083423	EEEE0001	SIB-JNP10008
SIB 1	REV 30	750-083423	EEEE0002	SIB-JNP10008
FTC 0	REV 18	750-083435	FFFF0001	Fan Controller 8
FTC 1	REV 18	750-083435	FFFF0002	Fan Controller 8
Fan Tray 0	REV 08	750-103312	FFFF1001	Fan tray 8
Fan Tray 1	REV 08	750-103312	FFFF1002	Fan tray 8

7. To save the chassis environment information, use the `show chassis environment | save filename` operational mode command.

```
user@host> show chassis environment | save /var/tmp/hwenvironment.old
Wrote 162 lines of output to '/var/tmp/hwenvironment.old'
```

The sample output shows the contents of the saved file: environmental information about the chassis, including the temperature and status for the various chassis components as well as the fan speeds.

Class	Item	Status	Measurement
Temp	PSM 0	Ok	26 degrees C / 78 degrees F
	PSM 1	Ok	38 degrees C / 100 degrees F
	PSM 2	Ok	31 degrees C / 87 degrees F
	CB 0 Intake A Temp Sensor	Ok	23 degrees C / 73 degrees F
	CB 0 Intake B Temp Sensor	Ok	23 degrees C / 73 degrees F
	CB 0 Exhaust A Temp Sensor	Ok	26 degrees C / 78 degrees F
	CB 0 Exhaust B Temp Sensor	Ok	29 degrees C / 84 degrees F
	CB 0 Middle Temp Sensor	Ok	28 degrees C / 82 degrees F
	CB 1 Intake A Temp Sensor	Ok	23 degrees C / 73 degrees F
	CB 1 Intake B Temp Sensor	Ok	23 degrees C / 73 degrees F
	CB 1 Exhaust A Temp Sensor	Ok	26 degrees C / 78 degrees F
	CB 1 Exhaust B Temp Sensor	Ok	29 degrees C / 84 degrees F
	CB 1 Middle Temp Sensor	Ok	28 degrees C / 82 degrees F
	Fan Tray 0 Inlet Temp Sensor	Ok	24 degrees C / 75 degrees F
	Fan Tray 0 Outlet Temp Sensor	Ok	27 degrees C / 80 degrees F
	Fan Tray 1 Inlet Temp Sensor	Ok	23 degrees C / 73 degrees F
	Fan Tray 1 Outlet Temp Sensor	Ok	28 degrees C / 82 degrees F
	FPC 0 BT-0 HBM-0 Temperature	Ok	54 degrees C / 129 degrees F
	FPC 0 BT-0 HBM-1 Temperature	Ok	54 degrees C / 129 degrees F
[...output truncated...]			
Fan	Fan Tray 0 Fan 0	Ok	4650 RPM
	Fan Tray 0 Fan 1	Ok	5400 RPM
	Fan Tray 0 Fan 2	Ok	4500 RPM
	Fan Tray 0 Fan 3	Ok	5400 RPM
	Fan Tray 0 Fan 4	Ok	4500 RPM
	Fan Tray 0 Fan 5	Ok	5250 RPM
	Fan Tray 0 Fan 6	Ok	4500 RPM
	Fan Tray 0 Fan 7	Ok	5400 RPM
	Fan Tray 0 Fan 8	Ok	4650 RPM
[...output truncated...]			

8. To save the system boot-message information, use the `show system boot-messages | save filename` operational mode command.

```
user@host> show system boot-messages | save /var/tmp/bootmessages.old
Wrote 7201 lines of output to '/var/tmp/bootmessages.old'
```

The sample output shows the contents of the saved file: the initial messages generated by the system kernel upon boot for FPCs and the REs; the contents of the `/var/run/dmesg.boot` file.

```
-----
node: fpc0
-----

[ 1.630132] pci 0000:ff:13.5: [8086:6fad] type 00 class 0x088000
[ 1.630204] pci 0000:ff:13.6: [8086:6fae] type 00 class 0x088000
[ 1.630274] pci 0000:ff:13.7: [8086:6faf] type 00 class 0x088000
[ 1.630352] pci 0000:ff:14.0: [8086:6fb0] type 00 class 0x088000
[ 1.630426] pci 0000:ff:14.1: [8086:6fb1] type 00 class 0x088000
[ 1.630499] pci 0000:ff:14.2: [8086:6fb2] type 00 class 0x088000
[ 1.630572] pci 0000:ff:14.3: [8086:6fb3] type 00 class 0x088000
[ 1.630644] pci 0000:ff:14.4: [8086:6fbc] type 00 class 0x088000
[ 1.630713] pci 0000:ff:14.5: [8086:6fbd] type 00 class 0x088000
[ 1.630781] pci 0000:ff:14.6: [8086:6fbe] type 00 class 0x088000
[ 1.630851] pci 0000:ff:14.7: [8086:6fbf] type 00 class 0x088000
[ 1.630921] pci 0000:ff:15.0: [8086:6fb4] type 00 class 0x088000
[ 1.630994] pci 0000:ff:15.1: [8086:6fb5] type 00 class 0x088000
[ 1.631067] pci 0000:ff:15.2: [8086:6fb6] type 00 class 0x088000
[ 1.631140] pci 0000:ff:15.3: [8086:6fb7] type 00 class 0x088000
[ 1.631225] pci 0000:ff:1e.0: [8086:6f98] type 00 class 0x088000
[ 1.631295] pci 0000:ff:1e.1: [8086:6f99] type 00 class 0x088000
[ 1.631371] pci 0000:ff:1e.2: [8086:6f9a] type 00 class 0x088000
[ 1.631441] pci 0000:ff:1e.3: [8086:6fc0] type 00 class 0x088000
[ 1.631495] pci 0000:ff:1e.4: [8086:6f9c] type 00 class 0x088000
[ 1.631566] pci 0000:ff:1f.0: [8086:6f88] type 00 class 0x088000
[ 1.631635] pci 0000:ff:1f.2: [8086:6f8a] type 00 class 0x088000
[ 1.632456] ACPI: Enabled 6 GPEs in block 00 to 3F
[ 1.632624] vgaarb: loaded
[ 1.632683] SCSI subsystem initialized
[ 1.632737] libata version 3.00 loaded.
[ 1.632765] ACPI: bus type USB registered
[...output truncated...]
-----
```

```

node: re0
-----
[ 0.000000] x86/fpu: xstate_offset[2]: 576, xstate_sizes[2]: 256
[ 0.000000] x86/fpu: Enabled xstate features 0x7, context size is 832 bytes, using
'standard' format.
[ 0.000000] x86/fpu: Using 'eager' FPU context switches.
[ 0.000000] e820: BIOS-provided physical RAM map:
[ 0.000000] BIOS-e820: [mem 0x0000000000000000-0x0000000000007dfff] usable
[ 0.000000] BIOS-e820: [mem 0x000000000007e000-0x000000000007ffff] reserved
[ 0.000000] BIOS-e820: [mem 0x0000000000080000-0x000000000009ffff] usable
[ 0.000000] BIOS-e820: [mem 0x00000000000a0000-0x00000000000ffff] reserved
[ 0.000000] BIOS-e820: [mem 0x0000000000100000-0x0000000000678defff] usable
[ 0.000000] BIOS-e820: [mem 0x0000000000678df000-0x000000000067bdefff] type 20
[ 0.000000] BIOS-e820: [mem 0x000000000067bdf000-0x00000000006b69efff] reserved
[ 0.000000] BIOS-e820: [mem 0x00000000006b69f000-0x00000000006b69efff] ACPI NVS
[ 0.000000] BIOS-e820: [mem 0x00000000006b69f000-0x00000000006b7fefff] ACPI data
[ 0.000000] BIOS-e820: [mem 0x00000000006b7ff000-0x00000000006b7fffff] usable
[ 0.000000] BIOS-e820: [mem 0x00000000006b800000-0x00000000008ffffff] reserved
[ 0.000000] BIOS-e820: [mem 0x0000000000feb00000-0x0000000000feb03fff] reserved
[ 0.000000] BIOS-e820: [mem 0x0000000000fec00000-0x0000000000fec0ffff] reserved
[ 0.000000] BIOS-e820: [mem 0x0000000000fed18000-0x0000000000fed19fff] reserved
[ 0.000000] BIOS-e820: [mem 0x0000000000fed1c000-0x0000000000fed1ffff] reserved
[ 0.000000] BIOS-e820: [mem 0x0000000000ff800000-0x0000000000ffffffff] reserved
[ 0.000000] BIOS-e820: [mem 0x00000000100000000-0x00000000107ffffff] usable
[...output truncated...]

```

9. To save information about the interfaces on the device, use the `show interfaces terse | save filename` operational mode command.

```

user@host> show interfaces terse | save /var/tmp/interfaces.old
Wrote 176 lines of output to '/var/tmp/interfaces.old'

```

The sample output shows the contents of the saved file: summary information about the physical and logical interfaces on the device.

Interface	Admin	Link	Proto	Local	Remote
et-0/0/0	up	down			
et-0/0/0.16386	up	down	multiservice		
pfh-0/0/0	up	up			
pfh-0/0/0.16383	up	up	inet		
et-0/0/1	up	up			

```

et-0/0/1.0      up    up    inet    10.1.1.1/24
                  multiservice

et-0/0/2        up    down

et-0/0/2.16386  up    down multiservice

et-0/0/3        up    down

et-0/0/3.0      up    down inet    10.0.0.1/24
                  multiservice

et-0/0/4        up    down

et-0/0/4.16386  up    down multiservice

[...output truncated...]

et-1/0/0        up    down

et-1/0/0.16386  up    down multiservice

pfh-1/0/0       up    up

pfh-1/0/0.16383 up    up    inet

et-1/0/1        up    down

et-1/0/1.16386  up    down multiservice

et-1/0/2        up    down

et-1/0/2.16386  up    down multiservice

[...output truncated...]

re0:mgmt-0      up    up

re0:mgmt-0.0    up    up    inet    10.48.20.100/22

re1:mgmt-0      up    up

re1:mgmt-0.0    up    up    inet    10.48.20.115/22

dsc             up    up

esi            up    up

fti0           up    up

fti1           up    up

fti2           up    up

fti3           up    up

fti4           up    up

fti5           up    up

fti6           up    up

fti7           up    up

irb            up    up

lo0            up    up

lo0.0          up    up    inet    10.255.9.9      --> 0/0
                  127.0.0.1      --> 0/0
                  127.0.0.64    --> 0/0

                  iso

47.0005.80ff.f800.0000.0108.0001.0102.5500.9009.00
                  inet6    2001:db8::10:255:9:9    -->
                  2001:db8::8603:28f0:db:6a6d-->

lsi            up    up

```

```

pip0          up    up
vtep          up    up

```

10. To save protocol information, use the `show` operational mode commands with the `save filename` option for the protocols configured for the device. To discover for which categories `show` commands are available, type `show ?` at the CLI operational mode prompt, and the system responds with a list of the available categories. Then choose a category, for example, `bgp`. Entering `show bgp ?` displays the list of `show` commands available for that category.

```

user@host> show bgp ?
Possible completions:
  bmp                Show BGP Monitoring Protocol information
  group              Show the BGP group database
  neighbor           Show the BGP neighbor database
  output-scheduler   Show BGP output queue scheduler configuration
  replication         BGP NSR replication state between master and backup
  source-packet-routing Show BGP source-packet-routing
  summary            Show overview of BGP information
  tunnel-attribute   Show Tunnel attributes advertised/received

```

This example shows the commands to save useful information about the Border Gateway Protocol (BGP), Intermediate System-to-Intermediate System (IS-IS), and Open Shortest Path First (OSPF) protocols. If you have other protocols configured, such as Address Resolution Protocol (ARP), Bidirectional Forwarding Detection (BFD), Link Layer Discovery Protocol (LLDP), MPLS, Resource Reservation Protocol (RSVP), or Protocol Independent Multicast (PIM), you also should save summary information for these protocols.

```

user@host> show bgp summary | save /var/tmp/bgp.old
Wrote 17 lines of output to '/var/tmp/bgp.old'

```

The sample output shows the contents of the saved file: summary information about BGP.

```

Threading mode: BGP I/O
Default eBGP mode: advertise - accept, receive - accept
Groups: 4 Peers: 4 Down peers: 0
Table      Tot Paths  Act Paths Suppressed    History Damp State   Pending
inet.0
          600000    600000         0         0         0         0
inet6.0
          200000    200000         0         0         0         0

```

Peer	AS	InPkt	OutPkt	OutQ	Flaps	Last Up/Dwn	State #Active/Received/Accepted/Damped...
192.0.2.2	64496	933	1007	0	0	4:40:24	Establ
inet.0: 300000/300000/300000/0							
198.51.100.2	64497	933	1055	0	0	4:40:20	Establ
inet.0: 300000/300000/300000/0							
2001:db8::119:2	64498	963	1068	0	0	4:40:30	Establ
inet6.0: 100000/100000/100000/0							
2001:db8::120:2	64499	962	1083	0	0	4:40:26	Establ
inet6.0: 100000/100000/100000/0							

```
user@host> show isis adjacency brief | save /var/tmp/isis.old
Wrote 383 lines of output to '/var/tmp/isis.old'
```

The sample output shows the contents of the saved file: brief information about the IS-IS adjacencies.

Interface	System	L State	Hold (secs)	SNPA
ae0.1	host-101	1 Up	6	78:4f:9b:ff:19:83
ae0.1	host-101	2 Up	8	78:4f:9b:ff:19:83
ae0.10	host-101	1 Up	6	78:4f:9b:ff:19:83
ae0.10	host-101	2 Up	8	78:4f:9b:ff:19:83
ae0.100	host-101	1 Up	8	78:4f:9b:ff:19:83
ae0.100	host-101	2 Up	7	78:4f:9b:ff:19:83
ae0.11	host-101	1 Up	8	78:4f:9b:ff:19:83
ae0.11	host-101	2 Up	8	78:4f:9b:ff:19:83
ae0.12	host-101	1 Up	8	78:4f:9b:ff:19:83
ae0.12	host-101	2 Up	6	78:4f:9b:ff:19:83

[...output truncated...]

```
user@host> show ospf neighbor brief | save /var/tmp/ospf.old
Wrote 428 lines of output to '/var/tmp/ospf.old'
```

The sample output shows the contents of the saved file: brief information about the OSPF neighbors.

Address	Interface	State	ID	Pri	Dead
---------	-----------	-------	----	-----	------

10.1.1.2	ae0.1	Full	10.255.2.135	128	38
10.1.10.2	ae0.10	Full	10.255.2.135	128	37
10.1.100.2	ae0.100	Full	10.255.2.135	128	35
10.1.11.2	ae0.11	Full	10.255.2.135	128	39
10.1.12.2	ae0.12	Full	10.255.2.135	128	32
10.1.13.2	ae0.13	Full	10.255.2.135	128	35
10.1.14.2	ae0.14	Full	10.255.2.135	128	36
10.1.15.2	ae0.15	Full	10.255.2.135	128	37
10.1.16.2	ae0.16	Full	10.255.2.135	128	35
10.1.17.2	ae0.17	Full	10.255.2.135	128	36
10.1.18.2	ae0.18	Full	10.255.2.135	128	39
11.1.19.2	ae0.19	Full	10.255.2.135	128	34

[...output truncated...]

11. To check if you have a recent-enough backup copy of your software, file system, and configuration, use the `show system snapshot | save filename` operational mode command.

```
user@host> show system snapshot | save /var/tmp/snapshot.old
Wrote 27 lines of output to '/var/tmp/snapshot.old'
```

The sample output shows the contents of the saved file: information about the snapshots saved on the system.

```
-----
node: re0
-----

Current snapshot device: /dev/sdb
Snapshot boot device: sdb
List of installed version(s) in Snapshot boot device sdb:

[1]  < junos-evo-install-ptx-x86-64-20.4-202103151803.0-EVO - [2021-03-16 15:09:46]
[2]   junos-evo-install-ptx-x86-64-20.4-202103111254.0-EVO - [2021-03-16 15:10:32]
[3] -> junos-evo-install-ptx-x86-64-20.4-202103150459.0-EVO - [2021-03-16 15:07:49]
[4]   junos-evo-install-ptx-x86-64-20.4-202103141559.0-EVO - [2021-03-16 15:11:52]

    '-' running version
    '>' next boot version after upgrade/downgrade
    '<' rollback boot version
-----
node: re1
```

```

-----
Current snapshot device: /dev/sdb
Snapshot boot device: sdb
List of installed version(s) in Snapshot boot device sdb:

[1] -> junos-evo-install-ptx-x86-64-20.4-202103051234.0-EVO - [2021-03-05 01:10:31]

    '-' running version
    '>' next boot version after upgrade/downgrade
    '<' rollback boot version

```

We recommend that if you do not have a snapshot that is the version currently running on the system or one that is recent enough to have the latest configuration for the system, that you back up the currently running software, file system, and configuration. Use the request system snapshot operational mode command, using the instructions at ["Back up and Recover Software with Snapshots" on page 86](#).

Once you have a snapshot of your system and collected information about the system, you need to validate the configuration image before upgrading or downgrading your software. See ["Validate the Configuration against the Installation Image" on page 48](#).

RELATED DOCUMENTATION

[Install, Upgrade, and Downgrade Software](#) | 50

Validate the Configuration against the Installation Image

SUMMARY

When you upgrade or downgrade the Junos OS Evolved image on a device, the system validates that the existing configuration is compatible with the new image before the actual upgrade or downgrade commences.

Before you upgrade or downgrade Junos OS Evolved on your device, you should validate the device's current configuration against the installation image you've downloaded from [Juniper Networks Support](#).

Validation is on by default. You do not need to configure it or issue any command to start it on a device.

When you upgrade or downgrade the Junos OS Evolved image on a device, the system validates that the existing configuration is compatible with the new image before the actual upgrade or downgrade commences.

Benefits of validation—If validation fails, the new image is not loaded and an error message provides information about the failure. If you upgrade or downgrade the software on a system without validation, configuration incompatibilities between the existing and new image or insufficient memory to load the new image might cause the system to lose its current configuration or go offline.

To invoke validation manually, do one of the following:

- Issue the `request system software add image-name` operational mode command to install the package with validation.
- Issue the `request system software validate` operational mode command to just validate the configuration.

RELATED DOCUMENTATION

| [request system software validate \(Junos OS Evolved\)](#) | 212

Upgrade and Downgrade Software

IN THIS CHAPTER

- [Install, Upgrade, and Downgrade Software | 50](#)

Install, Upgrade, and Downgrade Software

SUMMARY

Devices are delivered with Junos OS Evolved already installed on them. As new features and software fixes become available, you must upgrade Junos OS Evolved to use them. You can install software on devices that have either single or redundant routing engines. Before you install a software release on a device, you should make any necessary changes to the configuration and back up the current system.

IN THIS SECTION

- [Prepare to Install Software | 51](#)
- [Prepare both Routing Engines to Join the System | 53](#)
- [Install the Software Package on a Device with Redundant Routing Engines | 59](#)
- [Install the Software Package on a Device with a Single Routing Engine | 63](#)
- [Recover from a Failed Installation Attempt If the CLI Is Working | 65](#)
- [Replace a Routing Engine in a Dual-RE System | 67](#)
- [Not Enough Disk Space for Software Installation | 69](#)

Junos OS Evolved ensures that all Routing Engines (REs) and FPCs in the system are running the same software version. When you issue the request `system software add image-name` operational mode command on the primary RE, the system installs the new version of software on both REs. Once you reboot the system after a software package installation, all the REs and FPCs in the system run the new version of the software.

Junos OS Evolved supports storing multiple versions of software on the storage media. You can view the installed versions on the device with the `show system software list operational mode` command. Each version of the software is stored in a distinct area in the `/soft` directory, ensuring that a software package installation does not impact the other software versions installed in the system. We recommend you keep no more than 5 versions of software in the system.

In Junos OS, you must first upgrade the software on the standby RE and then switch control to the standby RE to run the new software version. After you are sure the software upgrade on the original standby RE is successful, you can upgrade the original primary RE to the new software version and switch control back to the original primary RE. However, with Junos OS Evolved, you do not need to upgrade the standby RE first. You upgrade both REs using a single command issued on the primary RE.

During a successful installation, the installation package completely re-installs the existing software. It retains configuration files and similar information, such as secure shell and host keys, from the previous version. The previous software package is preserved in a separate disk partition, and you can manually roll back to it if necessary. If the software installation fails for any reason, such as loss of power during the installation process, the system returns to the originally active installation when you reboot. For more background information on software installation, see ["Software Installation and Upgrade Overview \(Junos OS Evolved\)" on page 16](#).

Junos OS Evolved allows you to roll back to any of the releases stored in the system with the `request system software rollback image-name operational mode` command. The system also stores with each release the last configuration that was running when the release was running. Junos OS Evolved supports rolling back to an alternate image with the currently-running configuration or with the saved configuration that corresponds to the rollback software image, with the `request system software rollback with-old-snapshot-config operational mode` command.

If the system does not function properly after the upgrade and reboot, the previous version can be restored by rolling back to the previous version. See the roll back step in the ["Recover from a Failed Installation Attempt If the CLI Is Working" on page 65](#) procedure.

For dual-RE devices, if an RE inserted into the device has a different software version, the new RE is kept out of the system. We recommend that you configure the software to synchronize automatically to the new RE, by configuring the `auto-sw-sync enable` statement at the `[edit system]` hierarchy level. When this configuration is present, the RE that is in the system copies over all the images to the new RE and reboots the new RE so that it automatically comes up with the correct software. You can also choose to synchronize the software to the new RE manually each time you have to replace an RE, by using the `request system software sync all-versions operational mode` command, which synchronizes the software versions and configurations. For more information about replacing REs, see ["Replace a Routing Engine in a Dual-RE System" on page 67](#).

Prepare to Install Software

Follow these steps to prepare to install your Junos OS Evolved software:

1. Using a Web browser, navigate to the **All Junos Platforms** software download URL on the Juniper Networks webpage: <https://www.juniper.net/support/downloads/>
2. In the **Find a Product** box, enter the Junos OS platform for the software that you want to download.
3. Select **Junos Evolved** from the OS drop-down list.
4. Select the relevant release number from the **Version** drop-down list.
5. In the **Install Package** section, select the software package for the release.
6. Log in to the Juniper Networks authentication system using the username (generally your e-mail address) and password supplied by a Juniper Networks representative.
7. Review and accept the End User License Agreement.
8. Download the software to a local host.

NOTE: Download the Services Profile 1 image to use the lean rpd profile. For more information about the types of Junos OS installation package prefixes, see ["Junos OS Evolved Installation Package Prefixes" on page 23](#).

9. For a dual-RE device, ensure that both REs are participating in the system, and are running the same software. See ["Prepare both Routing Engines to Join the System" on page 53](#).
10. Ensure enough disk space is available to install the package, ensure that a system backup is available, and gather information about the system and how it is currently handling traffic by following the procedure in ["Before You Upgrade or Reinstall Junos OS Evolved" on page 33](#).
11. Copy the software image to the `/var/tmp/` directory of the device running Junos OS Evolved using the scp command.

```
user@host> file copy scp://filename /var/tmp/filename
```

12. Validate the configuration against the installation image before upgrading or downgrading your software by following the procedure in ["Validate the Configuration against the Installation Image" on page 48](#).
13. Install the new package on the device.
Choose one of the following procedures:
 - ["Install the Software Package on a Device with a Single Routing Engine" on page 63](#)
 - ["Install the Software Package on a Device with Redundant Routing Engines" on page 59](#)

NOTE: We recommend that you upgrade all software packages out of band using the console port, because in-band connections are lost during the installation process.

For more information about EOL releases and to review a list of EOL releases, see the [Junos OS Evolved Dates and Milestones](#) webpage.

Prepare both Routing Engines to Join the System

For dual-RE devices, both REs must be participating in the system to be able to install software on both REs. You must verify that both REs are in the system and which software versions are currently running in the system. You use the `show system software list`, `show system nodes`, and `show system alarms` operational mode commands to do so and to determine what course of action to take if one of the REs is not participating in the system.

Issue the `show system software list` and `show system nodes` commands on the primary RE to check the status of the REs. If information about both `re0` and `re1` appear in the output, and show a status of `Status : online, apps-ready` in the output of the `show system nodes` command, both REs are operational, part of the system, and are running the same software version. You can proceed to install the software. See "[Install the Software Package on a Device with Redundant Routing Engines](#)" on page 59. For example:

```
user@host-re0> show system software list
[...output truncated...]
-----
node: re0
-----
Active boot device is primary: /dev/sda
List of installed version(s) :

    '-' running version
    '>' next boot version after upgrade/downgrade
    '<' rollback boot version

-   junos-evo-install-ptx-x86-64-20.4R2.13-EVO - [2021-05-05 09:19:16]
<   junos-evo-install-ptx-x86-64-20.4R2.14-EVO - [2021-05-05 09:03:23]
-----
node: re1
-----
Active boot device is primary: /dev/sda
List of installed version(s) :

    '-' running version
    '>' next boot version after upgrade/downgrade
    '<' rollback boot version

-   junos-evo-install-ptx-x86-64-20.4R2.13-EVO - [2021-05-05 09:22:09]
```

```
< junos-evo-install-ptx-x86-64-20.4R2.14-EVO - [2021-05-05 09:06:50]
user@host-re0> show system nodes
Node: fpc0
  Node Id      : 2201170739216
  Node Nonce   : 2632845278
  Status       : online, apps-ready
  Attributes   : ASICS (Active), BT (Active), FABRIC_PFE (Active), FPC (Active), PIC (Active),
TIMINGD_FPC (Active), MSVCSD (Active)

Node: re0
  Node Id      : 2201170739204
  Node Nonce   : 1829978227
  Status       : online, apps-ready
  Attributes   : FABRIC_CONTROL (Active), FABRIC_FCHIP_PARALLEL (Active), RE (Active), TIMINGD_RE
(Active), MasterRE (Active), GlobalIPOwner (Active)

Node:
re1
  Node Id      : 2201170739205
  Node Nonce   : 3166228206
  Status       : online, apps-ready
  Attributes   : FABRIC_CONTROL (Spare), FABRIC_FCHIP_PARALLEL (Spare), RE (Spare), TIMINGD_RE
(Spare), BackupRE (Active)
```

If both REs are present, but the status of one RE is not Status : online, apps-ready, you need to take action to bring that RE into the system. In these examples, re0 is the RE in the system and re1 is the other RE that needs to join the system:

- **If the status is Status : offline, configured-offline**, issue the request node online *node-name* operational mode command on the RE in the system to bring the other RE back online. For example:

```
user@host-re0> request node online re1
This may take a few minutes. Online the node ? [yes,no] (no) yes

Node re1 is set to be online
```

Issue the show system nodes command to verify the RE has joined the system (both REs show Status : online, apps-ready).

```
user@host-re0> show system nodes
Node: fpc0
  Node Id      : 2201170739216
```

```

Node Nonce : 4089726524
Status      : online, apps-ready
Attributes  : ASICS (Active), BT (Active), FABRIC_PFE (Active), FPC (Active), PIC (Active),
TIMINGD_FPC (Active)
[...output truncated...]
Node: re0
Node Id     : 2201170739204
Node Nonce  : 4290191371
Status      : online, apps-ready
Attributes  : FABRIC_CONTROL (Active), FABRIC_FCHIP_PARALLEL (Active), RE (Active),
TIMINGD_RE (Active), MasterRE (Active), GlobalIPOwner (Active)
Node: re1
Node Id     : 2201170739205
Node Nonce  : 237744170
Status      : online, apps-ready
Attributes  : FABRIC_CONTROL (Spare), FABRIC_FCHIP_PARALLEL (Spare), RE (Spare), TIMINGD_RE
(Spare), BackupRE (Active)

```

If the status is still Status : offline, configured-offline, the other RE is configured to be offline and you need to delete that part of the configuration and commit it. Use the `show configuration system node operational mode` command to check the configuration. Delete the configuration, and issue the `show system nodes` command to check the status. The REs should both be online.

```

user@host-re0> show configuration system node
offline re1;

{master}
user@host-re0> edit

{master}[edit]
user@host-re0# delete system node offline re1

{master}[edit]
user@host-re0# commit
commit complete

{master}[edit]
user@host-re0# exit

{master}
user@host-re0>

```

- If the status is Status : offline, configured-powered-off, the other RE has either been powered off or halted. Issue the request chassis cb slot *slot-number* offline operational mode command from the RE in the system to determine which is the case. For example:
- If the RE was halted, the status message says Offline initiated:

```
user@host-re0> request chassis cb slot 1 offline
Offline initiated
```

- If the RE was powered-off, the status message says CB is already Offline:

```
user@host-re0> request chassis cb slot 1 offline
CB is already Offline
```

In either case, you need to bring the other RE back online and verify the RE has joined the system:

- Issue the request chassis cb slot *slot-number* online operational mode command on the RE in the system to bring the other RE online:

After issuing the command, please wait a few minutes for the other RE to come back online.

```
user@host-re0> request chassis cb slot 1 online
Online initiated
```

- Issue the show system software list operational mode command to verify that the RE has joined the system and that both REs are running the same software version:

```
user@host-re0> show system software list
-----
node: fpc0
-----
Active boot device is primary: /dev/ram1
List of installed version(s) :

    '-' running version
    '>' next boot version after upgrade/downgrade
    '<' rollback boot version

- junos-evo-install-ptx-x86-64-20.4R2.13-EV0 - [2021-05-05 16:27:34]
-----
node: re0
```

```

-----
Active boot device is primary: /dev/sda
List of installed version(s) :

    '-' running version
    '>' next boot version after upgrade/downgrade
    '<' rollback boot version

-   junos-evo-install-ptx-x86-64-20.4R2.13-EVO - [2021-05-05 09:19:16]
<   junos-evo-install-ptx-x86-64-20.4R2.14-EVO - [2021-05-05 09:03:23]
-----

node: re1
-----
Active boot device is primary: /dev/sda
List of installed version(s) :

    '-' running version
    '>' next boot version after upgrade/downgrade
    '<' rollback boot version

-   junos-evo-install-ptx-x86-64-20.4R2.13-EVO - [2021-05-05 14:24:37]
<   junos-evo-install-ptx-x86-64-20.4R2.14-EVO - [2021-05-05 13:59:46]

```

- If the output of the `show system software list` and `show system nodes operational mode` commands do not contain information for re1 and the `show system alarms operational mode` command shows that the software versions do not match (Software Version Mismatch on re1:*package-name*), issue the `request system software sync all-versions` operational mode command on the RE in the system to bring the other RE into the system and synchronize the software from the RE in the system to the other RE.

```

user@host-re0> request system software sync all-versions
warning: Erase software versions present on the other RE node and sync software versions from
Master RE node
Erase software versions on the other RE and sync from Master RE? [yes,no] (no) ...yes

Cleanup old software versions on re1
The current version on master RE - junos-evo-install-ptx-x86-64-20.4R2.13-EVO
The current version on other RE - junos-evo-install-ptx-x86-64-20.4R2.14-EVO
Sync in progress for /soft/junos-evo-install-ptx-x86-64-20.4R2.13-EVO...
The rollback version on master RE - junos-evo-install-ptx-x86-64-20.4R2.14-EVO
The rollback version on other RE - junos-evo-install-ptx-x86-64-20.4R2.13-EVO
Sync in progress for /soft/junos-evo-install-ptx-x86-64-20.4R2.14-EVO...

```


Software sync completed for all versions

Warning: Rebooting re1

Please run 'show system software list' to see SW versions installed in all nodes

Issue the show system software list operational mode command to verify that both REs are in the system and the REs are running the same software version:

```

user@host-re0> show system software list
-----
node: fpc0
-----
Active boot device is primary: /dev/ram1
List of installed version(s) :

    '-' running version
    '>' next boot version after upgrade/downgrade
    '<' rollback boot version

-   junos-evo-install-ptx-x86-64-20.4R2.13-EVO - [2021-05-05 16:27:34]
-----
node: re0
-----
Active boot device is primary: /dev/sda
List of installed version(s) :

    '-' running version
    '>' next boot version after upgrade/downgrade
    '<' rollback boot version

-   junos-evo-install-ptx-x86-64-20.4R2.13-EVO - [2021-05-05 09:19:16]
<   junos-evo-install-ptx-x86-64-20.4R2.14-EVO - [2021-05-05 09:03:23]
-----
node: re1
-----
Active boot device is primary: /dev/sda
List of installed version(s) :

    '-' running version
    '>' next boot version after upgrade/downgrade
    '<' rollback boot version

```

```
- junos-evo-install-ptx-x86-64-20.4R2.13-EVO - [2021-05-05 14:24:37]
< junos-evo-install-ptx-x86-64-20.4R2.14-EVO - [2021-05-05 13:59:46]
```

Install the Software Package on a Device with Redundant Routing Engines

Unlike Junos OS, Junos OS Evolved ensures all nodes in a system are running the same software version. In Junos OS Evolved, the device can contain multiple releases of the software simultaneously if enough space exists. If the device does not have enough space, you must delete an older image of the software before installing a new one. We recommend that you store no more than 5 versions of software on the device.

Before you install a new software release on a device, you should back up the current system. See ["Back up and Recover Software with Snapshots" on page 86](#).

Before you upgrade the software, you must prepare for the installation. See ["Prepare to Install Software" on page 51](#).

The request `system software add` operational mode command installs the software on both the Routing Engines (REs). This command does not modify the currently running software stack. This command validates the current configuration using the new version of the software. Once validation succeeds, the install process checks for sufficient storage on both REs. Once the storage checks pass, the new software is installed on both REs. You need to reboot the system to run the new software. The software installation process only affects traffic for a short while; for more information, see [Table 4 on page 59](#).

Table 4: Software Installation Tasks and their Traffic Impact

Tasks	Actions	Traffic Impact
Add the software	Validate the configuration, check for sufficient storage, install on both REs	None
Verify the software installation	Show image that will be the current image after the system reboots	None
Reboot the system	Reboot all REs and FPCs at the same time	Impacted; resumes after the system reboots
Verify which software image is running	Show image running after reboot	None

To upgrade the software on a device:

1. Install the new software package using the `request system software add installation-package` operational mode command on the primary RE:

The variable *installation-package* is the name of the installation package. Specify the absolute path on the local disk; for example, `/var/tmp/ptx.iso`. In this example, the package `junos-evo-install-ptx-x86-64-20.4R2.13-EVO` was downloaded onto the local disk as `/var/tmp/ptx.iso`. To understand package name prefixes, see ["Junos OS Evolved Installation Packages" on page 23](#).

```
user@host-re0> request system software add /var/tmp/ptx.iso
Adding software images. This process can take several minutes. Please be patient...
Download and Validate in Progress
re0: Starting upgrade : /var/tmp/ptx.iso
re0: Upgrade version : junos-evo-install-ptx-x86-64-20.4R2.13-EVO
re0: Running pre-checks for 'junos-evo-install-ptx-x86-64-20.4R2.13-EVO'
re0: Pre-checks pass successfully, copying files to software
area                                re0: Running post install
commands...
re0: Post install sequence was successful.
re0: Validating existing configs. See /var/log/validation_config.log for config validation
logs.
re0: Validation Passed
re0: Going ahead with Installation
re0: Boot version is now 'junos-evo-install-ptx-x86-64-20.4R2.13-EVO'
re0: Updating all nodes...
re1: Running pre-checks for 'junos-evo-install-ptx-x86-64-20.4R2.13-EVO'
re1: Pre-checks pass successfully, copying files to software area
re1: Running post install commands...
re1: Post install sequence was successful.
re1: Boot version is now 'junos-evo-install-ptx-x86-64-20.4R2.13-EVO'
re1: Config fetch successful
re0: Other nodes have been updated successfully
re0: Cluster wide installation was successful
Image validation and installation succeeded.
WARNING: NOTE: A reboot is required to start using the new software.
WARNING: Use the 'request system reboot' command when ready.
```

NOTE: Do not change the configuration before you reboot the device. If you make any configuration changes at this time, the system discards the changes.

2. Use the `show system software list` operational mode command on the primary RE to verify the newly-added software package is now the next-boot version on both REs:

In the example, the next-boot version on both REs is now junos-evo-install-ptx-x86-64-20.4R2.13-EV0. Note that junos-evo-install-ptx-x86-64-20.4R2.14-EV0 is still the currently running version.

```

user@host-re0> show system software list
[...output truncated...]
-----
node: re0
-----
Active boot device is primary: /dev/sda
List of installed version(s) :
    '-' running version
    '>' next boot version after upgrade/downgrade
    '<' rollback boot version

> junos-evo-install-ptx-x86-64-20.4R2.13-EV0 - [2021-05-05 09:19:16]
- junos-evo-install-ptx-x86-64-20.4R2.14-EV0 - [2021-05-05 09:03:23]
-----
node: re1
-----
Active boot device is primary: /dev/sda
List of installed
version(s) :

    '-' running version
    '>' next boot version after upgrade/downgrade
    '<' rollback boot version

> junos-evo-install-ptx-x86-64-20.4R2.13-EV0 - [2021-05-05 09:22:09]
- junos-evo-install-ptx-x86-64-20.4R2.14-EV0 - [2021-05-05 09:06:50]

```

3. Reboot the device from the primary RE to start the new software:

The system reboots all nodes at the same time.

```

user@host-re0> request system reboot
The entire system (all nodes) will reboot causing traffic loss, do you wish to continue?
[yes,no] (no) yes

*** System shutdown message from user@host-re0 ***

```

reboot the system at Wed May 5 09:24:06 2021

Verify the system is running the new version.

NOTE: You must reboot the device to load the new software release on the device.

To prevent the newly added package from becoming the currently running software, do not reboot the device. Instead, answer no, and then issue the `request system software delete package-name` command. This prompt gives you the opportunity to stop the installation from finishing.

The software is loaded when you reboot the system. Installation can take between 5 and 10 minutes. The device then reboots from the boot device on which the software was just installed. When the reboot is complete, the device displays the login prompt. After the reboot, Junos OS Evolved automatically saves the previous image of the software and configuration to create the rollback image.

During the reboot, the RE on which you are performing the installation does not route traffic.

4. Log in to the primary RE and verify the release of the software installed on both REs, using the `show system software list operational mode` command:

The current version on both REs is now `junos-evo-install-ptx-x86-64-20.4R2.13-EV0`. `junos-evo-install-ptx-x86-64-20.4R2.14-EV0` is now the rollback version.

```
user@host> show system software list
[...output truncated...]
-----
node: re0
-----
Active boot device is primary: /dev/sda
List of installed version(s) :

    '-' running version
    '>' next boot version after upgrade/downgrade
    '<' rollback boot version

- junos-evo-install-ptx-x86-64-20.4R2.13-EV0 - [2021-05-05 09:19:16]
< junos-evo-install-ptx-x86-64-20.4R2.14-EV0 - [2021-05-05 09:03:23]
-----
node: re1
-----
Active boot device is primary: /dev/sda
```

List of installed version(s) :

```
'-' running version
'>' next boot version after upgrade/downgrade
'<' rollback boot version

- junos-evo-install-ptx-x86-64-20.4R2.13-EVO - [2021-05-05 09:22:09]
< junos-evo-install-ptx-x86-64-20.4R2.14-EVO - [2021-05-05 09:06:50]
```

5. Verify that the system is running properly and correctly handling traffic by repeating the steps in the procedure in ["Before You Upgrade or Reinstall Junos OS Evolved" on page 33](#) and compare the information to what you collected before you installed the software package.
6. If you need to make any changes to the configuration as a result of the verification step, don't forget to back up the software and configuration using the `request system snapshot operational mode` command. See ["Back up and Recover Software with Snapshots" on page 86](#).

Install the Software Package on a Device with a Single Routing Engine

Before you install a new software release on a device, you should back up the current system. See ["Back up and Recover Software with Snapshots" on page 86](#).

In Junos OS Evolved, the device can contain multiple releases of the software simultaneously as long as the system has enough space. If the system does not have enough space, you must delete an older image of the software before installing a new one. We recommend that you store no more than 5 versions of software on the device.

Before you upgrade the software, you must prepare for the installation. See ["Prepare to Install Software" on page 51](#).

To upgrade the software on a device:

1. Install the new software package using the `request system software add` operational mode command:

```
user@host> request system software add /var/tmp/installation-package
```

The variable *installation-package* is the name of the installation package. Specify the absolute path on the local disk; for example, `/var/tmp/junos-evo-install-ptx.iso`. To understand package name prefixes, see ["Junos OS Evolved Installation Packages" on page 23](#).

NOTE: Do not change the configuration before you reboot the device. If you make any configuration changes at this time, the system discards the changes.

2. Use the `show system software list` operational mode command to verify the newly-added software package is now the next-boot version:

In the example, the next-boot version is now `junos-evo-install-ptx-x86-64-20.4R2.13-EV0`. Note that `junos-evo-install-ptx-x86-64-20.4R2.14-EV0` is still the currently running version.

```
user@host-re0> show system software list
[...output truncated...]
-----
node: re0
-----
Active boot device is primary: /dev/sda
List of installed version(s) :
    '-' running version
    '>' next boot version after upgrade/downgrade
    '<' rollback boot version

> junos-evo-install-ptx-x86-64-20.4R2.13-EV0 - [2021-05-05 09:19:16]
- junos-evo-install-ptx-x86-64-20.4R2.14-EV0 - [2021-05-05 09:03:23]
```

3. Reboot the device to start the new software:

```
user@host> request system reboot
Reboot the system ? [yes,no] (no) yes
```

NOTE: You must reboot the device to load the new software release on the device.

To prevent the newly added package from becoming the currently running software, do not reboot the device. Instead, answer no, and then issue the `request system software delete package-name` command. This prompt gives you the opportunity to stop the installation from finishing.

The software is loaded when you reboot the system. Installation can take between 5 and 10 minutes. The device then reboots from the boot device on which the software was just installed. When the reboot is complete, the device displays the login prompt. After the reboot, Junos OS Evolved automatically saves the previous image of the software and configuration to create the rollback image.

During the reboot, the RE does not route traffic.

4. Log in and verify the release of the software installed, using the `show system software list` operational mode command:

```

user@host> show system software list
[...output truncated...]
-----
node: re0
-----
Active boot device is primary: /dev/sda
List of installed version(s) :

    '-' running version
    '>' next boot version after upgrade/downgrade
    '<' rollback boot version

> junos-evo-install-ptx-x86-64-20.4R2.13-EV0 - [2021-05-05 09:19:16]
- junos-evo-install-ptx-x86-64-20.4R2.14-EV0 - [2021-05-05 09:03:23]

```

5. Verify that the system is running properly and correctly handling traffic by repeating the steps in the procedure in ["Before You Upgrade or Reinstall Junos OS Evolved" on page 33](#) and compare the information to what you collected before you installed the software package.
6. If you need to make any changes to the configuration as a result of the verification step, don't forget to back up the software and configuration using the `request system snapshot` operational mode command. See ["Back up and Recover Software with Snapshots" on page 86](#).

SEE ALSO

[request system software add \(Junos OS Evolved\) | 188](#)

[request system software delete \(Junos OS Evolved\) | 200](#)

Recover from a Failed Installation Attempt If the CLI Is Working

If a Junos OS Evolved installation fails, and the CLI is working, use one of these procedures to install Junos OS Evolved, depending upon the situation:

- Roll back to the previous version of software.

Devices running Junos OS Evolved save the previous running image. The first time you upgrade the device, the new software package installs in next-boot position. When you finish the installation and reboot, the new image becomes the current image. The previous image becomes the rollback image. For early initialization failures, the Routing Engine automatically switches to the secondary SSD.

You can rollback to the previously saved software version and configuration that was active when that version was running.

```
user@host> request system software rollback with-old-snapshot-config
```

- For early initialization failures, use the software stored on the inactive solid-state drive (SSD) to repair the software on the active SSD of the affected RE. If the active SSDs on both REs have failed, you must perform these steps on both REs.
 - a. Reboot from the inactive SSD, typically the secondary SSD (disk2) on the primary RE (RE0).
If the active SSD on the other RE has also failed, you must repeat this step for the other RE, typically RE1.

```
user@host> request node reboot re0 disk2
```

- b. Create a snapshot to install the rollback image onto the primary SSD.
To restore the primary SSD, perform a snapshot to install the rollback image from the secondary SSD onto the primary SSD.

```
user@host> request system snapshot
```

- c. Boot from the primary SSD, typically disk1 on the primary RE (re0).
The system is now operational using the rollback software image.

```
user@host> request node reboot re0 disk1
```

- If neither one of the previous steps is successful, then install the Image from a USB drive.
The USB installation process deletes all configuration and other files. Therefore, after the USB installation process completes:
 - If your system contains only one RE, you need to re-create the configuration file. Hopefully, you previously stored a configuration file on a remote server or other off-box location. If you did not, you must start with the initial configuration steps as described in the hardware guide for your product, and then continue to add the configuration statements you need.
 - If your system contains two REs, the secondary RE boots up, but does not join the system formed by the primary RE and the FPCs, because the current software versions are different. To synchronize the software and configurations from the primary RE to the secondary RE, use the

request system software sync all-versions operational mode command. The secondary RE then reboots and joins the system.

If you have already created a USB drive with the correct software package, follow the instructions in ["Boot Junos OS Evolved from a Bootable USB Drive Using the CLI" on page 78](#) to install an image on the RE and boot the device. If you have not yet created a USB drive, then follow the instructions at ["Boot Junos OS Evolved by Using a Bootable USB Drive" on page 75](#) to create a USB drive using either a Windows or a Mac OS X device. Then use that USB drive to install the image.

Replace a Routing Engine in a Dual-RE System

Junos OS Evolved ensures all nodes in a system are running the same software version.

If you insert an RE that has the same current software version as the primary RE into the system, the new RE joins the system, and the configurations and the other software versions automatically synchronize from the existing RE to the new RE, even if you have not configured the auto-sw-sync statement.

If you insert an RE that has a different software version into the system and you have not configured the auto-sw-sync enable statement, the RE is kept outside the system and the system generates a software mismatch alarm. The alarm message displays the RE name and the version of software on the newly-inserted RE, similar to the following: Software Version Mismatch on re1:junos-evo-install-ptx-x86-64-20.4R2.6-EV0..

```
user@host-re0> show system alarms
2 alarms currently active
Alarm time          Class  Description
2021-04-19 16:02:26 PDT  Major  Re1 Node unreachable
2021-04-19 16:04:46 PDT  Major  Software Version Mismatch on re1:junos-evo-install-ptx-
x86-64-20.4R2.6-EV0
```

To clear the alarms and bring the RE into the system, manually synchronize the primary RE to the new RE with the request system software sync all-versions operational mode command.

We recommend that you configure the auto-sw-sync enable configuration statement at the [edit system] hierarchy level before inserting a new RE into the system. When you do so, the RE in the system detects the newly-inserted RE and automatically synchronizes the software to the new RE. All images are synchronized to the new RE and the system reboots the newly-inserted RE. When the newly-inserted RE comes back up, it joins the system. Each software image has the configuration used when the image ran stored with it. The configuration associated with the current running image is synchronized from the primary RE to the backup RE. Configurations stored with the rollback and other images are also synchronized to the backup RE when you configure the auto-sw-sync enable statement on the primary RE.

To replace an RE in a dual-RE system:

1. Configure the `auto-sw-sync enable` statement.

Enter configuration mode, configure the `auto-sw-sync enable` statement, commit the configuration, and exit configuration mode to get back to operational mode:

```
user@host-re0> edit
user@host-re0# set system software auto-sw-sync enable
user@host-re0# commit
commit complete
user@host-re0# exit
user@host-re0>
```

2. Replace the RE.

3. Allow several minutes for the software and configurations to synchronize and for the newly-inserted RE to reboot.

4. Verify that the newly-inserted RE is now part of the system and that the software versions on both REs are the same, by issuing the `show system software list` operational mode command.

You must make sure that the system has finished synchronizing all of the images in the background before you switch control to the newly-inserted RE to ensure that the newly-inserted RE does not remove any images from the existing RE.

```
user@host-re0> show system software list
[...output truncated...]
-----
node: re0
-----
Active boot device is primary: /dev/sda
List of installed version(s) :

    '-' running version
    '>' next boot version after upgrade/downgrade
    '<' rollback boot version

- junos-evo-install-ptx-x86-64-20.4R2.13-EVO - [2021-05-05 09:19:16]
< junos-evo-install-ptx-x86-64-20.4R2.14-EVO - [2021-05-05 09:03:23]
-----
node: re1
-----
Active boot device is primary: /dev/sda
List of installed version(s) :
```

```

    '-' running version
    '>' next boot version after upgrade/downgrade
    '<' rollback boot version

- junos-evo-install-ptx-x86-64-20.4R2.13-EVO - [2021-05-05 09:22:09]
< junos-evo-install-ptx-x86-64-20.4R2.14-EVO - [2021-05-05 09:06:50]

```

5. If the software was not automatically synchronized or if you decided not to configure the `auto-sw-sync enable` statement, manually synchronize the software versions and configurations to the newly-inserted RE, by issuing the `request system software sync all-versions` operational mode command from the primary RE.

All software images and configurations stored with the images are synchronized to the new RE and the new RE is rebooted. When the new RE comes back up, it joins the system.

6. (Required if you have a rescue configuration) Synchronize the rescue configuration from the primary RE to the secondary RE with the `file copy rescue-config-filename secondary-re-name:/config/` command on the primary RE.

For a dual-RE system, when the secondary RE boots with a different current image than the primary RE's current image and the `auto-sw-sync enable` statement is configured, the primary RE synchronizes the current image to the secondary RE. The primary RE also synchronizes the rollback software image and the other images to the secondary RE. If the current configuration file (**juniper.conf.gz**) from the primary RE matches the current configuration file on the secondary RE, then the primary RE does not synchronize the rescue configuration (**rescue.conf.gz**) to the secondary RE. For example:

```
user@host-re0> file copy /config/rescue.conf.gz re1:/config/
```

7. Verify that the newly-inserted RE can function properly with the `request chassis routing-engine master release` operational mode command on the primary RE to release control to the newly-inserted RE.

If the newly-inserted RE then does not become the primary RE, issue the `request chassis routing-engine master release` command on the newly-inserted RE to release control, remove the newly-inserted RE, get a different RE and insert it, and repeat this procedure.

For more information about node synchronization, see ["request system software sync" on page 207](#) and ["auto-sw-sync" on page 161](#).

Not Enough Disk Space for Software Installation

The software installation process requires a certain amount of unused disk space. If the system does not have enough space, you receive an error message similar to the following:

WARNING: The /soft filesystem is low on free disk space.

WARNING: This package requires 1075136k free, but there is only 666502k available.

If you need to create enough disk space for the software installation to be successful, you can do the following:

- Identify and delete older images by using the `show system software list` and `request system software delete operational mode` commands.
- Identify and delete unnecessary files by using the `show system storage` and `request system storage cleanup operational mode` commands.

For more information on how to create enough disk space for a software installation, see ["Ensure Sufficient Disk Space for Upgrades" on page 27](#).

Install Third-Party Software

IN THIS CHAPTER

- [How to Install Third-Party Software on Devices Running Junos OS Evolved | 71](#)

How to Install Third-Party Software on Devices Running Junos OS Evolved

Third-party software is software that is not part of the normal release cadence for a given target chassis. In the case of Junos OS Evolved, third-party software refers to the following types of software delivered to a node or a cluster of nodes running Junos OS Evolved:

- Private software developed by customers and partners
- Software or tools developed by Juniper

Third parties package their software as **.tgz** files. The package filename contains the component name and its version as well as the architecture and the SDK version. You install the third-party software package on a device running Junos OS Evolved using the `request system software add filename` command. This command is the same command you use to install different releases of the Junos OS Evolved software on a device. The only difference is that third-party software filenames use the **.tgz** filename extension, not the **.iso** filename extension used by the Junos OS Evolved software files.

The procedure is the same as installing software on any device running Junos OS. You back up the current system and you place the software on the device, usually in the **/var/tmp** directory of the active Routing Engine.

For example, if you have third-party software developed by Acme with the filename **acmeMonitor-1.2.3_Wr1_9.0_x86_64.tgz**, use the following command to install it on a device running Junos OS Evolved:

```
user@host> request system software add /var/tmp/acmeMonitor-1.2.3_Wr1_9.0_x86_64.tgz
```

NOTE: You do not need to use the `reboot` command to install third-party applications on devices running Junos OS Evolved.

NOTE: For Junos OS Evolved, if you are trying to reinstall an already installed application, use the `force` option. The `force` option will cause the program to remove the existing application before reinstalling it.

The program detects third-party components already installed in the current version that collide with new components in **acmeMonitor-1.2.3_Wrl_9.0_x86_64.tgz**. Without using the `force` option, a reinstall of a third-party application fails.

Use the `show version` command to see a list of the current components installed that are not part of the released BOM. The list is tagged as “External Software” and gives the name of each third-party component name and version, as well as the SDK version that was used to create it.

```
user@host> show version
Model: ptx10003-160c
Junos: 20.1-201910240713.0-EVO
Junos Package: junos-evo-install-ptx-fixed-x86-64-20.1-201910240713.0-EVO.iso
Yocto: 2.2.1
Linux Kernel: 4.8.28-WR2.2.1_standard-g21fb4b9
SDK version: 5.6.7
External Software:
    acmeMonitor-1.2.3 [sdk 5.6.7]
    acmeLoadShare-3.4.5 [sdk 5.6.8]
```

You remove third-party software the same way you remove versions of Junos OS Evolved. For example, to remove the Acme software, use this command:

```
user@host> request system software delete acmeMonitor
```

If you want to delete all third-party software, use the `request system software delete all-third-party-packages` command.

RELATED DOCUMENTATION

[request system software add \(Junos OS Evolved\) | 188](#)

[request system software delete \(Junos OS Evolved\) | 200](#)

[show version \(Junos OS Evolved\) | 291](#)

3

PART

System Backup and Recovery

[Boot Junos OS Evolved from a USB Drive | 75](#)

[Back Up an Installation with Snapshots | 86](#)

[Roll Back the Software to a Previous Version | 90](#)

[Backup and Recover the Configuration File | 92](#)

CHAPTER 8

Boot Junos OS Evolved from a USB Drive

IN THIS CHAPTER

- [Boot Junos OS Evolved by Using a Bootable USB Drive | 75](#)

Boot Junos OS Evolved by Using a Bootable USB Drive

SUMMARY

You can boot Junos OS Evolved from a USB device. Booting from the USB device reformats the disk and reinstalls the software without prompting you. After the installation is done, you can either remove the USB drive from the USB port or reboot the device.

IN THIS SECTION

- [Create a Bootable USB Drive Using a Windows Device | 75](#)
- [Create a Bootable USB Drive Using a MAC OS X | 76](#)
- [Create a Bootable USB Drive Using a Switch or Router Running Junos OS Evolved | 77](#)
- [Boot Junos OS Evolved from a Bootable USB Drive Using the CLI | 78](#)
- [Recover Junos OS Evolved Using USB Scratch Install | 79](#)
- [Boot Junos OS Evolved from a Bootable USB Drive Using the Shell | 80](#)

You can use several ways to create the Junos OS Evolved image on the USB drive. Also included are both a procedure for booting from the USB drive and a procedure for how to recover if the boot process from the USB drive goes bad.

Create a Bootable USB Drive Using a Windows Device

You need the following items to perform this procedure:

- Windows desktop or laptop with a USB port.

- Version 2.0 or version 3.0 USB device with the following features:
 - USB device is big enough to hold the ISO image.
 - USB device must have no security features, such as a keyed boot partition.
- Junos OS Evolved ISO image

For a virtual Windows desktop you must map a physical USB of the host to the guest virtual machine (VM).

To create a bootable USB drive using a Windows device:

1. Install Win32 Disk Imager on your laptop or computer.
You can download it from <https://sourceforge.net/projects/win32diskimager/>.
2. Download the required Junos OS image from the Downloads page to the Documents directory of your laptop or computer.
3. Insert a USB flash drive into the USB port of your laptop or computer.
4. Open the win32diskimager application and, in the **Image File** box, type the path to the Documents directory (or click the folder icon to navigate to the Documents directory) and select the install media image.
5. Under Device, select the USB flash-drive and click **Write and Confirm**. The Progress box shows the progress.
6. Remove the USB flash drive once it is complete.

The USB flash-drive is now ready to use as a bootable disk.

Create a Bootable USB Drive Using a MAC OS X

You need the following items to perform this procedure:

- A MAC OS X desktop or laptop with a USB port.
- Version 2.0 or version 3.0 USB device with following features:
 - USB device is big enough to hold the ISO image.

To create a bootable USB using MAC OS X:

1. Copy the install media (.img format) to the `/var/tmp/` directory of the MAC OS device using the `scp` command.

For example:

```
$ scp user@server:/var/tmp/image-name /var/tmp/
password:
```

2. To get the list of devices on the MAC OS X device, run the `diskutil list` command.
3. Insert the USB flash drive into the USB port of the MAC OS X.
4. Run the `diskutil list` command again to determine the device node assigned to USB flash-drive (for example, `/dev/disk3`).
5. Run the `diskutil unmountDisk /dev/diskN` command.

Replace *N* with the disk number from the last command. (In this example, *N* would be 3.)

For example:

```
$ diskutil unmountDisk /dev/disk3
Unmount of all volumes on disk3 was successful
```

6. Execute the command `sudo dd if=/var/tmp/junos-evo-install-ptx-fixed-x86-64-19.2R1.31-EV0.img of=/dev/rdiskN bs=1m`

For example:

```
$ sudo dd if=/var/tmp/usb.img of=/dev/rdisk3 bs=1m
Password:
965+0 records in
965+0 records out
1011875840 bytes transferred in 82.891882 secs (12207177 bytes/sec)
```

7. The USB with image is created and ready for installation. Safely remove the USB drive and use it as a bootable USB drive on the device on which you plan to run Junos OS Evolved.

Create a Bootable USB Drive Using a Switch or Router Running Junos OS Evolved

You need the following items to perform this procedure:

- A switch or router with a USB port that is running Junos OS Evolved.
- Version 2.0 or version 3.0 USB device with following features:
 - USB device is big enough to hold the ISO image.
 - USB device must have no security features, such as a keyed boot partition.
 - USB device label should be JUNOS.

To create a bootable USB using a switch or router running Junos OS Evolved:

1. Download **.img** image from Downloads site and copy it to the `/var/tmp/` directory of the switch or router running Junos OS Evolved using the `scp` command.

2. Enter the shell as root:

```
user@host> start shell user root
Password:
```

3. Before inserting the USB device, list the contents of `/dev/`.

```
root@host-re0:~#ls /dev/sd*
/dev/sda /dev/sda3 /dev/sda6 /dev/sdb1 /dev/sdb4 /dev/sdb7
/dev/sda1 /dev/sda4 /dev/sda7 /dev/sdb2 /dev/sdb5
/dev/sda2 /dev/sda5 /dev/sdb /dev/sdb3 /dev/sdb6
root@host-re0:~#
```

4. Insert the USB drive in the USB port.
5. Repeat the command to list the contents of `/dev/`.

```
root@host-re0:~#ls /dev/sd*
/dev/sda /dev/sda3 /dev/sda6 /dev/sdb1 /dev/sdb4 /dev/sdb7
/dev/sda1 /dev/sda4 /dev/sda7 /dev/sdb2 /dev/sdb5 /dev/sdc
/dev/sda2 /dev/sda5 /dev/sdb /dev/sdb3 /dev/sdb6 /dev/sdc1
root@host-re0:~#
```

NOTE: `/dev/sdc` is the USB drive.

6. Execute the following command, where `$USB` identifies the device for that USB (typically `sdc` in Linux):

```
root@host-re0:~# dd if=/var/tmp/usb.img of=/dev/$USB bs=100000
```

7. The USB with image is created and ready for installation. Safely remove the USB drive and use it as a bootable USB drive on the device on which you plan to run Junos OS Evolved.

Boot Junos OS Evolved from a Bootable USB Drive Using the CLI

Before you perform this procedure, you must create a USB drive with the Junos OS Evolved software image installed on it. For instructions, see ["Create a Bootable USB Drive Using a Windows Device" on page 75](#) ["Create a Bootable USB Drive Using a MAC OS X" on page 76](#) or ["Create a Bootable USB Drive Using a Switch or Router Running Junos OS Evolved" on page 77](#).

To install Junos OS Evolved on a device that runs Junos OS Evolved using a USB drive:

1. Connect to the console.
2. Insert the USB drive with the Junos OS Evolved package in the **USB0** port on the routing device.
3. Reboot the routing device from the CLI:

```
user@host> request system shutdown reboot usb
```

When the reboot and loading of the Junos OS Evolved package is complete, you have a choice as to running a snapshot or not:

```
Installation of image junos-evo-install-ptx-fixed-x86-64-19.2R1.31-EV0 done.  
Boot version is now 'junos-evo-install-ptx-fixed-x86-64-19.2R1.31-EV0'  
Do you want to run snapshot on secondary ssd? (Y/N)
```

4. Enter N to skip taking a snapshot. The system keeps the previous snapshot.

```
Do you want to run snapshot on secondary ssd? (Y/N)N  
Setting next_boot  
Booting from 0000
```

5. Reboot the device to finish the installation.

```
user@host-re0~# reboot
```

Recover Junos OS Evolved Using USB Scratch Install

IN THIS SECTION

- Problem | 80
- Solution | 80

Problem

Description

If, while you are trying to boot Junos OS Evolved from a USB device, the device goes to a bad state, follow this procedure.

Solution

To recover using a USB scratch install:

1. Insert the bootable USB device into the device.
2. Access the BIOS manager to check the USB selection:
 - a. Reboot the routing device.

```
user@host> request system shutdown reboot usb
```

- b. To access the BIOS boot manager, press ESC while the system reboots.
3. In the BIOS boot manager, select one of the following:
 - For PTX10003 devices, select **EFI USB**.
 - For QFX5200 devices, select **USB: *model-name***.

The scratch installation starts automatically and the operating system loads.

4. Reboot the device to finish the installation.

```
user@host-re0~# reboot
```

Boot Junos OS Evolved from a Bootable USB Drive Using the Shell

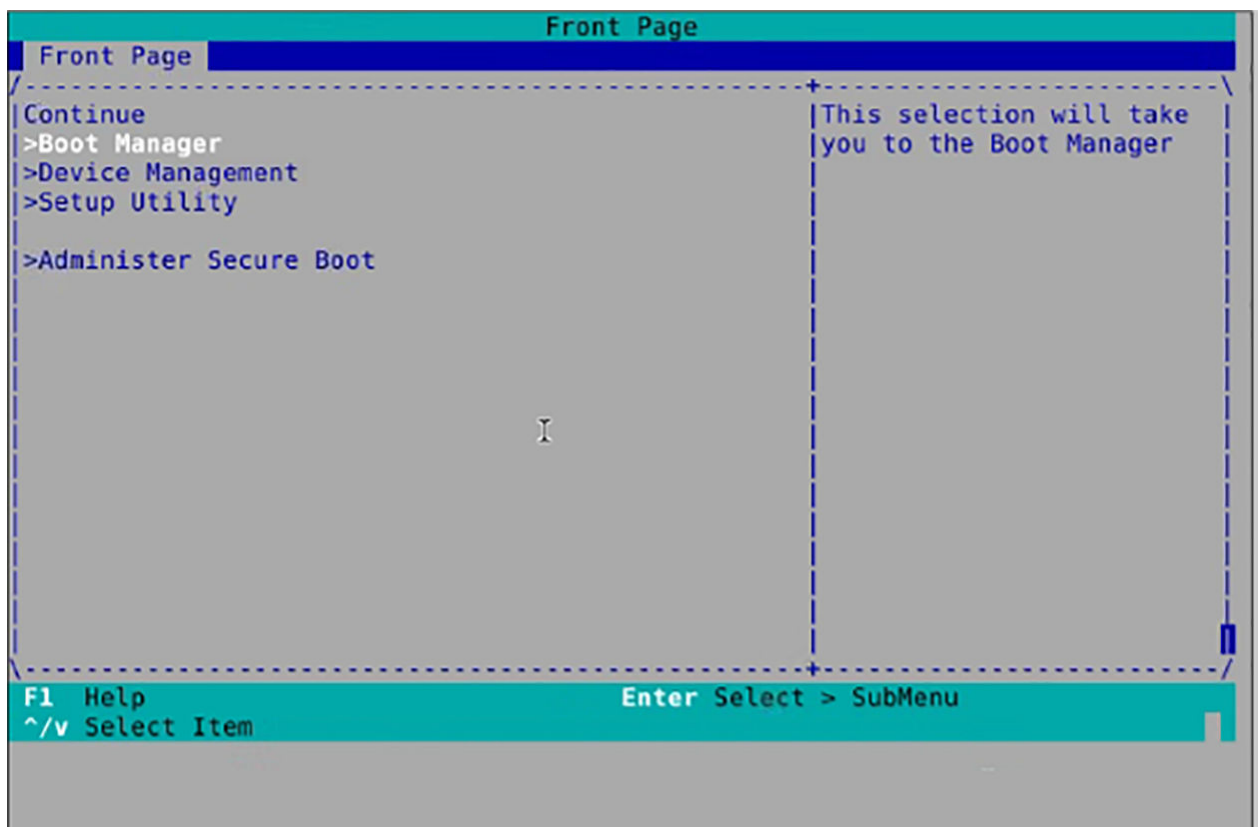
The USB installation process deletes all configuration and other files. Therefore, after the USB installation process completes:

- If your system contains only one RE, you need to re-create the configuration file. Hopefully, you previously stored a configuration file on a remote server or other off-box location. See ["Restore the Configuration from a Backup Copy after a USB Software Installation" on page 97](#). If you do not have a previously-stored configuration file, you must start with the initial configuration steps as described in the hardware guide for your product and then continue to add the configuration statements that you need.

- If your system contains two REs, the secondary RE boots up, but does not join the system formed by the primary RE and the FPCs, because the current software versions are different. To synchronize the software and configurations from the primary RE to the secondary RE, use the request system software sync all-versions operational mode command. The secondary RE then reboots and joins the system.

If you have not yet created a USB drive, follow the instructions at ["Create a Bootable USB Drive Using a Windows Device" on page 75](#) or ["Create a Bootable USB Drive Using a MAC OS X" on page 76](#) to create a USB drive using either a Microsoft Windows or a Mac OS X device and then use that USB drive to install the image.

1. Power on or reboot the device. The device boots from RE0.
2. Press the **ESC** key multiple times until the Front Page menu appears.



3. Using the arrow keys, move the cursor to the **Boot Manager** option, and press **Enter** to select that option. The Boot Manager menu appears:


```
+-----+
```

```

Use the ^ and v keys to select which entry is highlighted.
Press enter to boot the selected OS, `e' to edit the commands
before booting or `c' for a command-line. ESC to return
previous menu.
The highlighted entry will be executed automatically in 1s.

```

5. Because the USB device can contain only one image, you do not need to select the image. GRUB starts the installation automatically.

```

Booting `Evo ISO installation media
[junos-evo-install-ptx-x86-64-20.4R2.14-EV0]'

Version is junos-evo-install-ptx-x86-64-20.4R2.14-EV0, Product is ptx[re].
IMA is 1
Loading kernel ...ok
Loading initrd ...ok
Booting ...
error: no suitable video mode found.
Booting in blind mode
error: no suitable video mode found.
Booting in blind mode
Trying sdc...sdc1...Found!
[ 7.624873] jnx-cbd-fpga jnx-cbd-fpga.10: jnx_cbc_probe: FRU not handled by jnx-connector:
-22!
[ 7.736740] jnx-cbd-fpga jnx-cbd-fpga.8: jnx_cbc_probe: FRU not handled by jnx-connector:
-22!
Watchdog set to 500 seconds
[ 8.205691] watchdog: watchdog0: watchdog did not stop!
Found 186 gig (195360984 kbytes) Vendor ATA, Model SFSA200GM3AA4T0-
Writing new partitioning table to disk sda -
    boot - 204800K
    soft - 32768M
    swap - 4096M
    data - 3072M
    conf - 1024M
    var - 149622M
    user - 0M
Done
Installing/Mounting on disk /dev/sda mapped to device ata1
Processing /dev/sda2 for mount on /soft ...[creating]..

```

```

data - 3072M
conf - 1024M
var - 149622M
user - 0M
Done
Installing/Mounting on disk /dev/sda mapped to device ata1
Processing /dev/sda2 for mount on /soft ...[creating]..ok [mounting]..done
Processing /dev/sda5 for mount on /data ...[creating]..ok [mounting]..done
Processing /dev/sda6 for mount on /data/config ...[creating]..ok [mounting]..done
Processing /dev/sda7 for mount on /data/var ...[creating]..ok [mounting]..done
Processing /data/var/opt_fs for mount on /data/var/external ...[creating]..ok [mounting]..done
mkswap: /dev/sda3: warning: wiping old swap signature.
Setting up swapspace version 1, size = 4 GiB (4294963200 bytes)
no label, UUID=66495c63-a79e-496a-ba60-853417d76edb
Processing /dev/sda1 for mount on /boot ...[creating]..ok [mounting]..done
Done with local filesystems setup.
Cleanup check done.
Installation on re node for version junos-evo-install-ptx-x86-64-20.4R2.14-EVO started.
[...output truncated...]
Installation of image junos-evo-install-ptx-x86-64-20.4R2.14-EVO done.
Boot version is now 'junos-evo-install-ptx-x86-64-20.4R2.14-EVO'
Do you want to run snapshot on secondary ssd? (Y/N)n
Setting next_boot
Booting from 0000
NOTE: Now 9 keys in keyring: %keyring:.ima
Scratch install done.
BootCurrent: 0003
Timeout: 5 seconds
BootOrder: 0003,0000,0001,0002
Boot0000* HDD00 (SFSA200GM3AA4T0-C-HC-646-JUN)
Boot0001* HDD01 (SFSA200GM3AA4T0-C-HC-646-JUN)
Boot0002* ETH00 (B8-C2-53-32-91-63)
Boot0003* USB00 (JetFlashTranscend 16GB)
Booting from 0000
Scratch install done.

### To Reboot : #####
#      Pull out the USB stick      #
# Or -                             #
#      Type 'reboot' and hit <return>      #
#####

```

6. Issue the reboot command to finish the installation.

```
user@host-re0:~# reboot
```

7. The action you take next depends on whether your system has one or two REs.

- If your system has one RE, either copy a known-good configuration file to the RE, as explained in ["Restore the Configuration from a Backup Copy after a USB Software Installation" on page 97](#), or start creating a new configuration file with the steps contained in the hardware guide for your product.
- If your system has two REs, use the `request system software sync all-versions operational mode` command to synchronize the software and configurations from the primary RE to the secondary RE and enable the secondary RE to join the system and use the most-recent configuration that was stored on the primary RE. Because the current software versions do not match, the secondary RE does not join the system, which comprises the primary RE and the FPCs.

```
[vrf:none] user@host-re1:~# cli
{master}
user@host-re1> request system software sync all-versions
warning: Erase software versions present on the other RE node and sync software versions
from Master RE node
Erase software versions on the other RE and sync from Master RE? [yes,no] (no)
yes
Cleanup old software versions on re0
The current version on master RE - junos-evo-install-ptx-x86-64-20.4-202102141059.0-EVO
The current version on other RE - junos-evo-install-ptx-x86-64-19.4R1-S1.18-EVO
Transfer software version files for junos-evo-install-ptx-x86-64-20.4-202102141059.0-EVO
to node re0...
[...output truncated...]
```

Back Up an Installation with Snapshots

IN THIS CHAPTER

- [Back up and Recover Software with Snapshots | 86](#)

Back up and Recover Software with Snapshots

SUMMARY

The installation process removes all stored files on the device except for files such as the `juniper.conf`, `SNMP ifIndexes`, and `SSH` files. Therefore, you should back up your current configuration in case you need to return to the current software installation after running the installation program. You can also recover the configuration file and the Junos OS Evolved software, if required.

IN THIS SECTION

- [Understand Snapshots | 86](#)
- [Create a Snapshot on the Secondary SSD and Use It to Recover the Software Installation | 87](#)

Understand Snapshots

You can create copies of the software running on a device using the `request system snapshot operational` mode command. The command takes a “snapshot” of the files currently used to run the device—the complete contents of the `/soft` and `/config` directories, which include the running version of Junos OS Evolved, the active configuration, and the rescue configuration—and copies all of these files onto the alternate solid-state drive (SSD). You can then use this snapshot to boot the device at the next boot up or as a backup boot option. The snapshot also contains copies of user data as well as any content from the `/root`, `/var`, and `/var/home` directories.

NOTE: We recommend that you take a snapshot after every software upgrade or downgrade.

System snapshots have the following limitations:

- You cannot use snapshots to move files to any destination outside of the device, including an installed external USB flash drive.
- Snapshot commands always run on a local Routing Engine (RE) and snapshot to the secondary SSD on the local RE.

Restoring from a snapshot is especially effective as a boot-up option after a disk corruption, as it is the only recovery option that allows you to completely restore the software and configuration in the event of a corrupted disk.

After an upgrade, if the installation fails during early boot, the RE automatically reverts to booting from the secondary SSD, where snapshots are stored. You can then reboot the RE using the snapshot saved on the secondary SSD.

Create a Snapshot on the Secondary SSD and Use It to Recover the Software Installation

To create a snapshot on the secondary SSD (`/dev/sdb`) of the primary (or only) RE:

1. Issue the request `system snapshot operational mode` command.

```
user@host> request system snapshot
-----
node: re0
-----
.....
Starting Snapshot in device /dev/sdb
List of software versions getting copied to Snapshot...
[1] junos-evo-install-ptx-x86-64-20.4-202103151803.0-EVO
[2] junos-evo-install-ptx-x86-64-20.4-202103111254.0-EVO
[3] junos-evo-install-ptx-x86-64-20.4-202103150459.0-EVO
[4] junos-evo-install-ptx-x86-64-20.4-202103141559.0-EVO
.....
.....
[...output truncated...]
.....
.....
Software Snapshot completed.
```



```

** Backup RE: **
** 1) Run cli command "request system software sync all-versions" from **
**    the Master RE. **
** 2) Post RE reboot, login to RE  and run cli command "request system snapshot" **
**    to recover primary device **
** 3) Then run cli command "request node reboot re0 disk1" to boot **
**    from the primary device. **
** **
*****

```

SEE ALSO

[request system snapshot \(Junos OS Evolved\) | 186](#)

[show system snapshot \(Junos OS Evolved\) | 277](#)

Roll Back the Software to a Previous Version

IN THIS CHAPTER

- [Roll Back the Software to a Previous Version | 90](#)

Roll Back the Software to a Previous Version

SUMMARY

Junos OS Evolved maintains multiple versions of the software and configuration files on the primary solid-state drive (SSD) on the Routing Engine (RE). Each time you issue the `request system software add` operational mode command, the previous software image and configuration is preserved automatically. The last running software image and corresponding configuration file is the default rollback image. Older images, along with the configuration present when the older image was running, are preserved as well.

You use the rollback image and configuration preserved by default to revert to a prior image on the same disk as the current image.

After an upgrade or a roll back, if the software is unable to use the current configuration, the RE is often still reachable using the current management interface configuration. If the management interface does not come up, use the console to connect to the device to roll back the software and configuration.

After an upgrade, if the installation fails during early boot, the RE automatically reverts to booting from the secondary SSD, where snapshots are stored. You can then reboot the RE using the snapshot saved on the secondary SSD. You can then roll back the software version, especially if the snapshot version is not a recent-enough version of the software and configuration.

For a dual-RE device, the `request system rollback` operational mode command reverts both REs to the rollback software version. For all devices, the command rolls back the software version on the FPCs as well.

- To see which software images are available for rollback, use the `show system software list` operational mode command.
- To roll back to any image with the current configuration (the snapshot configuration), use the `request system software rollback package-name` operational mode command.
- To roll back to the last running image with its corresponding configuration from when the software was last running, use the `request system software rollback with-old-snapshot-config` operational mode command.
- To roll back to any image and its corresponding configuration, use the `request system software rollback package-name with-old-snapshot-config` operational mode command.

RELATED DOCUMENTATION

| [request system software rollback \(Junos OS Evolved\)](#) | 204

Backup and Recover the Configuration File

IN THIS CHAPTER

- [Back up and Recover the Configuration | 92](#)

Back up and Recover the Configuration

SUMMARY

During a successful upgrade, the upgrade package completely re-installs the existing operating system. It retains the **juniper.conf**, **rescue.conf**, SNMP ifIndexes, **/var/home**, **/config/scripts**, SSH files, and other filesystem files. Other information is removed. Therefore, you should back up your current configuration in case you need to return to the current software installation after running the installation program.

IN THIS SECTION

- [Save a Rescue Configuration | 93](#)
- [Validate a Rescue Configuration | 93](#)
- [Roll Back to a Rescue Configuration | 93](#)
- [Fix the Failed Configuration | 94](#)
- [Delete the Rescue Configuration | 95](#)
- [Copy either the Configuration File or the Rescue Configuration to a Remote Server | 95](#)
- [Roll Back to a Prior Configuration | 96](#)
- [Synchronize the Rescue Configuration to the Secondary RE after the Current Configuration Is Synchronized | 96](#)
- [Restore the Configuration from a Backup Copy after a USB Software Installation | 97](#)
- [Revert to the Default Factory Configuration | 99](#)

Save a Rescue Configuration

In the event of software failure, having a rescue configuration helps to load a known working configuration. No need to remember or look up the rollback number; if you save a rescue configuration, you can use it anytime.

A rescue configuration file is helpful if your device's configuration file has been misconfigured. A rescue configuration allows you to define a known working configuration or a configuration with a known state to which you can roll back at any time. You can restore the device to this rescue configuration to bring the device back online. If you save this file off the device, you can use the rescue configuration to restore your device in the event of a software failure.

To save a current device configuration as a rescue configuration file:

1. Edit the configuration file on the device to reflect the configuration you wish to save.
2. In the CLI operational mode, save this edited configuration as the rescue configuration file:

```
user@host> request system configuration rescue save
```

The system automatically saves rescue configuration file in the `/config` directory as `rescue.conf.gz`. If the device has redundant REs, the system saves the rescue configuration file on both REs.

Validate a Rescue Configuration

You can verify that the syntax of a configuration file is correct and check for commit check errors by using the test configuration *filename* command.

To verify if a rescue configuration file is correct:

- Issue the test configuration *filename* operational mode command.

```
user@host> test configuration /config/rescue.conf.gz  
configuration check succeeds
```

If the configuration contains any syntax or commit check errors, a message displays to indicate the line number and column number in which the error was found. This command only accepts text files.

Roll Back to a Rescue Configuration

1. Log in to the device through the console.

2. Issue the `rollback rescue` command from the configuration mode of the CLI.

```
user@host# rollback rescue  
load complete
```

3. Commit the configuration.

```
user@host# commit
```

4. Fix the failed configuration.

Fix the Failed Configuration

Your rescue configuration might not be the configuration you want or need on your system. Therefore, you need to fix the failed configuration and re-commit it.

To fix the failed configuration:

1. Log into the device through the management interface, or the console port (if permitted).
2. Load the failed configuration.

```
[edit]  
user@host# rollback 1
```

3. Make corrections to the configuration.
4. Use the check option on the `commit configuration mode` command.

The check option points out errors in the candidate configuration, giving you the opportunity to fix the errors. If the configuration contains syntax errors, a message indicates the location of the error and the system does not activate the configuration.

```
[edit]  
user@host# commit check
```

5. If you have other corrections to make, make them. Keep using the `commit check configuration mode` command until the system does not find any more errors.
6. Issue the `commit configuration mode` command to commit the configuration.

```
[edit]  
user@host# commit  
commit complete
```

After fixing the failed configuration, we recommend that you back up this configuration either by saving it as a rescue configuration or by saving it to a remote server or other off-box location. See ["Save a Rescue Configuration" on page 93](#) or ["Copy either the Configuration File or the Rescue Configuration to a Remote Server" on page 95](#).

Delete the Rescue Configuration

To delete the existing rescue configuration:

- Issue the request system configuration rescue delete command:

```
user@host> request system configuration rescue delete
```

Copy either the Configuration File or the Rescue Configuration to a Remote Server

This task is optional but recommended.

To copy either the currently running configuration or the rescue configuration file to a remote server:

1. Log into the device through the management interface, or the console port (if permitted).
2. Start the device shell.

```
user@host> start shell
```

3. Go to the **/config** directory and list the configuration files.

The currently running configuration file is **juniper.conf.gz** and the rescue configuration file is **rescue.conf.gz**.

```
user@host-re0:~# cd /config
user@host-re0:~# ls /config
commit-sync-status juniper.conf.2.gz juniper.conf.gz
juniper.conf.1.gz juniper.conf.3.gz license rescue.conf.gz
```

4. FTP the configuration file to the remote host.

```
user@host-re0:~# ftp host2
Name: user2
Password: password
User user2 logged in.
ftp> cd /var/tmp
ftp> lcd /config
ftp> bin
```

```

ftp> put rescue.conf.gz
local: rescue.conf.gz remote: rescue.conf.gz

Transfer complete.
ftp> put juniper.conf.gz
local: juniper.conf.gz remote: juniper.conf.gz

Transfer complete.
ftp> bye
Goodbye.

```

Roll Back to a Prior Configuration

To return to a configuration prior to the most recently committed one, include the configuration number, 0 through 49, in the rollback configuration mode command. The most recently saved configuration is number 0 (the default configuration to which the system returns), and the oldest saved configuration is number 49. To display a list of the previously committed configurations, including the rollback number, date, time, the name of the user who committed changes, and the method of commit, use the rollback ? configuration mode command.

To rollback to a prior configuration:

1. Issue the rollback *number* configuration mode command.

The rollback configuration becomes the candidate configuration.

```

[edit]
user@host# rollback 1
load complete

```

2. To activate the candidate configuration, issue the commit configuration mode command.

```

[edit]
user@host# commit

```

Synchronize the Rescue Configuration to the Secondary RE after the Current Configuration Is Synchronized

When the system boots up, if the system finds the current configuration file to be incompatible with the software, then the system fails to commit the configuration file (`/config/juniper.conf.gz`). If you previously saved a rescue configuration on the system, the system then commits the rescue configuration and saves it as the current configuration file `/config/juniper.conf.gz`.

For a dual-RE system, when the secondary RE boots with a different current image than the primary RE's current image and you have configured the `auto-sw-sync enable` statement, the primary RE synchronizes the current image to the secondary RE. The primary RE also synchronizes the rollback software image and the other images to the secondary RE. If the current configuration file (**juniper.conf.gz**) from the primary RE matches the current configuration file on the secondary RE, then the primary RE does not synchronize the rescue configuration (**rescue.conf.gz**) to the secondary RE.

To synchronize the rescue configuration from the primary RE to the secondary RE, issue the `file copy` command on the primary RE:

```
user@host-re0> file copy /config/rescue.conf.gz re1:/config/
```

Restore the Configuration from a Backup Copy after a USB Software Installation

If you install Junos OS Evolved from a USB drive onto a single-RE device, the installation process deletes the configuration files. Therefore, you need to re-configure the device. Also, if you have used the `request system zeroize` command to reset the device to the factory defaults, you also need to re-configure the device. If you have already saved a configuration file on a remote server or another off-box location, you can copy that configuration file onto the device to save time when re-configuring the device.

To restore the configuration from a backup copy:

1. Connect to the device through the console port.
2. Power on the device and wait for it to boot.
Junos OS Evolved boots automatically. When the boot process is complete, you'll see the `login:` prompt on the console.
3. Log in as the user `root`.
You won't need a password for the root user account, because the device is using the factory-default configuration. The device prompt `root@#` indicates that you are the root user. You must configure the management interface address and the password for the root user account before you are able to copy a configuration file to the device.
4. Issue the `cli` command to start the Junos OS Evolved CLI.
5. Issue the `configure` command to access configuration mode.
6. Configure the `interfaces` statement at the `[edit]` hierarchy level to configure the IP address and prefix length for the management address on RE0.

```
[edit]
root@# set interfaces re0:mgmt-number unit 0 family inet address address/prefix-length
```

7. Configure the root password. Use the password that you would usually configure for the root user account.

Enter a plain-text password that the system will encrypt, an already-encrypted password, or an SSH public key string. Configure the system root-authentication statement at the [edit] hierarchy level, and type or paste in the password or string when prompted.

- To enter a plain-text password:

```
[edit]
root@# set system root-authentication plain-text-password
New password: password
Retype new password: password
```

- To enter an already-encrypted password, paste the password into the command after the encrypted-password option:

```
[edit]
root@# set system root-authentication encrypted-password encrypted-password
```

- To enter an SSH public key string, paste the key string into the command after the ssh-rsa option:

```
[edit]
root@# set system root-authentication ssh-rsa key
```

8. Commit the configuration.

```
[edit]
root@# commit

commit complete
```

9. Exit configuration mode.

```
root@# exit
root@>
```

10. To copy the configuration file onto the router, use the file copy command.

Place the file in the `/var/tmp` directory.

```
root@> file copy scp://filename var/tmp/filename
```

11. Start configuration mode.

```
root@# configure
Entering configuration mode

[edit]
root@#
```

12. Load the file into the current configuration and override the existing file.

```
root@# load override /var/tmp/filename
load complete
```

13. Commit the configuration.

```
root@# commit
commit complete
```

14. Exit configuration mode.

```
root@host# exit
root@host>
```

15. After you are satisfied that the new configuration is successfully running, issue the `request system snapshot operational mode` command to back up the system. We also recommend that you create a rescue configuration; for more information, see ["Save a Rescue Configuration" on page 93](#).

If you do not issue the `request system snapshot` command, the configuration on the secondary solid-state drive (SSD) will be out of sync with the configuration on the primary SSD.

Revert to the Default Factory Configuration

The `request system zeroize` command is an operational mode command that removes all configuration information and resets all key values. The operation unlinks all user-created data files, including the configuration and log files, from their directories. The device then reboots and reverts to the factory-default configuration.



CAUTION: Before issuing the `request system zeroize operational mode` command, use the `request system snapshot operational mode` command to back up the files currently used to run the device to the secondary SSD.

To revert to the factory-default configuration by using the `request system zeroize` command:

1. Issue the `request system zeroize operational mode` command.

```
user@host> request system zeroize
warning: System will be rebooted and may not boot without configuration
Erase all data, including configuration and log files? [yes,no] (yes)
```

2. Type **yes** to remove configuration and log files and revert to the factory default configuration.
3. Complete the initial configuration of the device. See either the hardware guide for your product or the [Initial Configuration](#) page in the Junos OS Evolved Day One + Guide. You can also copy a configuration file from a remote server or other off-box location to the device. See ["Restore the Configuration from a Backup Copy after a USB Software Installation"](#) on page 97.

4

PART

Storage Media and Routing Engines

Storage Media and Routing Engines | 102

Storage Media and Routing Engines

IN THIS CHAPTER

- [Storage Media and Routing Engines | 102](#)

Storage Media and Routing Engines

SUMMARY

IN THIS SECTION

- [Routing Engines and Storage Media | 102](#)

The Routing Engine and Packet Forwarding Engine (PFE) are the two primary components of Juniper Networks platforms. Junos OS Evolved software is installed on the routing engine and it is stored in storage media.

Routing Engines and Storage Media

IN THIS SECTION

- [Storage Media | 103](#)

Juniper Networks routing platforms are made up of two basic routing components:

- **Routing Engine**—The Routing Engine controls the routing updates and system management.
- **Packet Forwarding Engine (PFE)**—The Packet Forwarding Engine performs Layer 2 and Layer 3 packet switching, route lookups, and packet forwarding.

From a system administration perspective, you install the software onto the Routing Engine and during the installation, the appropriate software is forwarded to other components as necessary. Routing Engines include two solid-state drives that store Junos OS Evolved.

Storage Media

Junos OS Evolved devices use the following storage media components:

- Solid-state drives—Junos OS Evolved devices use two SATA based solid-state drives (SSDs) as the primary storage devices. The two SSDs are designated as primary and secondary. The primary SSD acts as the default boot device.
- Emergency boot device—You can use an external USB drive as the emergency boot device for Junos OS Evolved devices. For more information on creating an emergency boot device, see ["Boot Junos OS Evolved by Using a Bootable USB Drive" on page 75](#)

5

PART

Zero Touch Provisioning

[Zero Touch Provisioning | 105](#)

[Zero Touch Provisioning DHCP Options | 155](#)

Zero Touch Provisioning

IN THIS CHAPTER

- [Zero Touch Provisioning | 105](#)

Zero Touch Provisioning

IN THIS SECTION

- [Zero Touch Provisioning Overview | 105](#)
- [Zero Touch Provisioning Using DHCP Options | 114](#)
- [Zero Touch Provisioning Using DHCPv6 Options | 122](#)
- [Zero Touch Provisioning on SRX Series Devices | 129](#)
- [Monitoring Zero Touch Provisioning | 138](#)

Zero Touch Provisioning installs or upgrades the software automatically on your new Juniper Networks devices with minimal manual intervention.

Zero Touch Provisioning Overview

IN THIS SECTION

- [ZTP Workflow | 109](#)
- [Provisioning a Device Using a Script | 110](#)
- [Zero Touch Provisioning Restart Process Triggers | 111](#)
- [Caveats Relating to ZTP | 112](#)

- [Zero Touch Provisioning Using WAN Interfaces on PTX1000 Routers | 113](#)
- [Zero Touch Provisioning on PTX10008 Routers | 114](#)

Zero Touch Provisioning (ZTP) allows you to provision new Juniper Networks devices in your network automatically, with minimal manual intervention. You can use either management ports or network ports, depending on your device, to connect to the network. When you physically connect a device to the network and boot it with a default factory configuration, the device upgrades (or downgrades) the Junos OS release and autoinstalls a configuration file from the network. The configuration file can be a Junos OS configuration or a script. Using scripts, you can create device-specific configuration files and perform HTTP request operations to web servers to download specific configuration files or Junos OS releases.

To locate the necessary software image and configuration files on the network, the device uses information that you have configured on a Dynamic Host Configuration Protocol (DHCP) server. If you do not configure the DHCP server to provide this information, the device boots with the preinstalled software and default factory configuration.

Originally (as of Junos OS release 12.2), the only devices that supported ZTP (or EZ Touchless Provisioning as it was previously known) were EX Series switches and only configuration files could be used to provision configuration.

Over subsequent Junos OS releases, ZTP support has expanded:

- Starting in Junos OS Release 16.1R1, you can provision supported devices by using either a script to be executed or a configuration file to be loaded.
- Starting in Junos OS Release 17.2R1, ZTP can automate the provisioning of the device configuration and software image on VM host platforms that use PTX1000 routers.
- Starting in Junos OS Release 18.1R1, ZTP can automate the provisioning of the device configuration and software image on VM host platforms that use QFX10002-60C switches.
- Starting in Junos OS Release 18.2R1, ZTP can automate the provisioning of the device configuration and software image on VM host platforms that use PTX5000, PTX3000, PTX10008, PTX10016, PTX10002-60C routers.
- Starting in Junos OS Release 18.2R1, ZTP can automate the provisioning of the device configuration and software image on VM host platforms that use QFX10008 and QFX10016 switches.
- Starting in Junos OS Release 18.3R1, ZTP, which automates the provisioning of the device configuration and software image with minimal manual intervention, is supported on MX Series VM hosts.

- Starting in Junos OS Release 19.2R1, ZTP can automate the provisioning of the device configuration and software image on management interface emo for ACX5448 switches.

Starting in Junos OS Evolved Release 19.1R1, ZTP can automate the provisioning of the device configuration and software image on the management interface for QFX5220 and PTX10003 devices. The management interfaces for PTX10003 devices are re0:mgmt-0 and re0:mgmt-1. The management interface for QFX5220 devices is vmb0.

- Starting in Junos OS Release 19.4R1, ZTP can automate the provisioning of the device configuration and software image on Juniper Route Reflector (JRR). ZTP supports self image upgrades and automatic configuration updates using ZTP DHCP options. In this release, ZTP supports revenue ports em2 thru em9, in addition to management port em0 which is supported in Junos OS Releases before 19.4R1.
- Starting in Junos OS Evolved Release 20.1R1 on PTX10003 devices, Zero Touch Provisioning (ZTP) dynamically detects the port speed of WAN interfaces and uses this information to create ZTP server ports with the same speed.
- Starting in Junos OS Evolved Release 20.1R1, PTX10008 devices support automation of the device configuration and software upgrade over the management interface of Routing Engine 0 (RE0).
- Starting in Junos OS Release 20.2R1-S1 on the MX-Series, EX3400, EX4300, QFX5100, and QFX5200 devices, ZTP supports the DHCPv6 client. During the bootstrap process, the device first uses the DHCPv4 client to request for information regarding image and configuration file from the DHCP server. The device checks the DHCPv4 bindings sequentially. If there is a failure with one of the DHCPv4 bindings, the device will continue to check for bindings until provisioning is successful. If there are no DHCPv4 bindings, however, the device will check for DHCPv6 bindings and follow the same process as for DHCPv4 until the device can be provisioned successfully. The DHCP server uses DHCPv6 options 59 and 17 and applicable sub-options to exchange ZTP-related information between itself and the DHCP client.
- Starting in Junos OS Release 20.2R1 on SRX300, SRX320, SRX340, SRX345, SRX550 HM, and SRX1500 devices, you can use Zero Touch Provisioning with DHCP options or the phone-home client to provision your device.
- Starting in Junos OS Release 20.4R1 on the MX-Series, EX3400, EX4300, QFX5100, and QFX5200 devices, ZTP supports the DHCPv6 client. During the bootstrap process, the device first uses the DHCPv4 client to request for information regarding image and configuration file from the DHCP server. The device checks the DHCPv4 bindings sequentially. If there is a failure with one of the DHCPv4 bindings, the device will continue to check for bindings until provisioning is successful. If there are no DHCPv4 bindings, however, the device will check for DHCPv6 bindings and follow the same process as for DHCPv4 until the device can be provisioned successfully. The DHCP server uses DHCPv6 options 59 and 17 and applicable sub-options to exchange ZTP-related information between itself and the DHCP client.

- Starting in Junos OS Release 20.4R1 on the EX4600, EX4650, EX9200 with RE-S-EX9200-2X00X6, QFX5110, QFX5200, QFX5210, QFX5120-32C, and QFX5120-48Y devices, you can use either the legacy DHCP-options-based ZTP or the phone-home client (PHC) to provision software for the switch. When the switch boots up, if there are DHCP options that have been received from the DHCP server for ZTP, ZTP resumes. If DHCP options are not present, PHC is attempted. PHC enables the switch to securely obtain bootstrapping data, such as a configuration or software image, with no user intervention other than having to physically connect the switch to the network. When the switch first boots up, PHC connects to a redirect server, which redirects to a phone home server to obtain the configuration or software image. .
- Starting in Junos OS Evolved Release 20.4R1, PTX10004 devices support automation of the device configuration and software upgrade over the management interface of Routing Engine 0 (RE0).
- Starting in Junos OS Evolved Release 20.4R1, ACX5448 and QFX5120-48YM devices support the ability for either WAN interfaces or management interfaces to automatically download and install the appropriate software and the configuration file on your device during the ZTP bootstrap process.
- Starting in Junos OS Release 21.1R1, Starting in Junos OS Release 21.1R1, during the bootstrapping process, the phone-home client (PHC) can access the redirect server or phone-home server through a proxy server. The DHCP server uses DHCP option 43 suboption 8 or DHCP option 17 suboption 8 to deliver the details of both IPv4 and IPv6 proxy servers to the PHC. The DHCP daemon running on the target switch learns about the proxy servers in the initial DHCP cycle and then populates either the `phc_vendor_specific_info.xml` files or the `phc_v6_vendor-specific_info.xml` files located in the `/var/etc/` directory with the vendor-specific information.
- Starting in Junos OS Release 21.1R1, on EX2300, EX2300-VC, EX3400, EX3400-VC, EX4400-24T, EX4400-48F, EX4400-48T, and EX4600 devices, when the phone-home client (PHC) receives information regarding the HTTP proxy server through either DHCP option 43 suboption 8 or DHCP option 17 suboption 8, it creates an HTTPS transparent tunnel with the proxy server. After the tunnel is established, the PHC uses the tunnel as a proxy for the phone-home server or redirect server. The phone-home client downloads the software image and configuration file through the tunnel onto the device. When bootstrapping is complete, the device reboots and the tunnel quits.
- Starting in Junos OS Release 21.2R1 on QFX10002 devices, Zero Touch Provisioning (ZTP) dynamically detects the port speed of WAN interfaces and uses this information to create ZTP server ports with the same speed.
- Starting in Junos OS Evolved Release 21.2R1 on PTX10008 devices, Zero Touch Provisioning (ZTP) dynamically detects the port speed of WAN interfaces and uses this information to create ZTP server ports with the same speed.
- Starting in Junos OS Evolved Release 21.2R1, QFX5700 devices support the ability for either WAN interfaces or management interfaces to automatically download and install the appropriate software and the configuration file on your device during the ZTP bootstrap process.

- Starting in Junos OS Release 21.2R1, on EX2300-C, EX2300-MP, EX4300, EX4300-MP, EX4300-VC, EX4400-24MP, EX4400-48MP, EX4600-VC, EX4650, and EX4650-48Y-VC devices, during the bootstrapping process, the phone-home client can access the redirect server through a proxy server. The DHCP server uses DHCP option 43 suboption 8 to deliver the details of IPv4 and/or IPv6 proxy servers to the phone-home client. The DHCP daemon running on the target switch learns about the proxy servers in the initial DHCP cycle and then populates either the `phc_vendor_specific_info.xml` or the `phc_v6_vendor_specific_info.xml` files located in the `/var/etc/` directory with the vendor-specific information.
- Starting in Junos OS Release 21.2R1, on EX2300-C, EX2300-MP, EX4300, EX4300-MP, EX4300-VC, EX4400-24MP, EX4400-48MP, EX4600-VC, EX4650, and EX4650-48Y-VC devices, you can use a DHCPv6 client and ZTP to provision a switch. During the bootstrap process, the device first uses the DHCPv4 client to request for information regarding the image and configuration file from the DHCP server. The device checks the DHCPv4 bindings sequentially. If there is a failure with one of the DHCPv4 bindings, the device continues to check for bindings until provisioning is successful. However, if there are no DHCPv4 bindings, the device checks for DHCPv6 bindings and follows the same process as for DHCPv4 until the device is provisioned successfully. Both DHCPv4 and DHCPv6 clients are included as part of the default configuration on the device. The DHCP server uses DHCPv6 options 59 and 17 and applicable suboptions to exchange ZTP-related information between itself and the DHCP client.
- Starting in Junos OS Evolved Release 21.3R1, on PTX10001-36MR, PTX10003, PTX10004, PTX10008, and PTX10016 devices, ZTP now supports DHCP options 61 and 77. DHCP option 61 is used to specify the chassis serial number, and DHCP option 77 is used to specify the make, model, and software version of the chassis.

NOTE: To see which platforms support ZTP, in a browser, go to [Feature Explorer](#). In the **Explore Features** section of the Feature Explorer page, select **All Features**. In the **Features Grouped by Feature Family** box, select Zero Touch Provisioning. You can also type the name of the feature in the **Search for Features** edit box.

ZTP Workflow

When a device boots up with the default configuration, the following events take place:

1. DHCP client is enabled on supported interfaces.
2. DHCP server provisions an IP address and includes several DHCP options in the reply related to the ZTP process.
3. The device processes the DHCP options and locates configuration files, executes scripts, and upgrades and/or downgrades software.

4. If both the image and configuration files are present, the image is installed and the configuration is applied.
5. If only the image file is present, the image is installed on the device.
6. If the image is the same as the image already installed on the device, ZTP continues and skips the installation step.
7. If the image was unable to be fetched by the device, ZTP will try to fetch the image again.
8. If the image is corrupted, installation fails.

If installation fails for any reason, the ZTP will restart.

9. If only the configuration file is present, the configuration is downloaded.

If the first line of the file consists of the `#!` characters followed by an interpreter path, then the file is considered a script, and the script is executed by the interpreter. If the script returns an error, the ZTP state machine will refetch the script and attempt to execute the script again.

If the configuration file is unable to be downloaded, the ZTP process will try to download it again.

If the configuration file is corrupted, has syntax errors, or includes commands that are unsupported by the device, the device will be unable to commit, and the retry mechanism will restart.

10. If there is no image or configuration file, the ZTP process starts again.
11. If there is no file server information, the ZTP process starts again.
12. Once the configuration is committed, the ZTP process is deemed successful and terminates.

Provisioning a Device Using a Script

During the ZTP process, when you connect and boot a new networking device, the device requests an IP address from the DHCP server. The server provides the IP address, and if configured, the filenames and locations for the software image and configuration file for the device. The configuration file can be a Junos OS configuration or a script.

If a configuration file is provided, Junos OS determines if the file is a script based on the first line of the file. If the first line contains the characters `#!` followed by an interpreter path, Junos OS treats the file as a script and executes it with the specified interpreter. If the script returns an error (that is, a nonzero value), the ZTP state machine refetches the script and attempts to execute it again. This continues until the script executes successfully.

[Table 5 on page 111](#) outlines the supported script types, the corresponding interpreter path, and the platforms that support that script type during the ZTP process.

Table 5: Scripts Supported During ZTP

Script Type	Interpreter Path	Platform Support
Shell script	<code>#!/bin/sh</code>	All devices
SLAX script	<code>#!/usr/libexec/ui/cscript</code>	All devices
Python script	<code>#!/usr/bin/python</code>	Devices running Junos OS with Enhanced Automation Devices running Junos OS Evolved

NOTE: For security reasons, Junos OS has strict requirements for running unsigned Python scripts on devices running Junos OS. Only devices running Junos OS with Enhanced Automation and devices running Junos OS Evolved support using unsigned Python scripts in DHCP option 43 suboption 01.

If Junos OS does not find the characters `#!` followed by an interpreter path, it treats the file as a Junos OS configuration in text format and loads the configuration on the device.

Zero Touch Provisioning Restart Process Triggers

ZTP restarts when any of the following events occur:

- Request for configuration file, script file, or image file fails.
- Configuration file is incorrect, and commit fails.
- No configuration file and no image file is available.
- Image file is corrupted, and installation fails.
- No file server information is available.
- DHCP server does not have valid ZTP parameters configured.
- When none of the DHCP client interfaces goes to a bound state.
- ZTP transaction fails after six attempts to fetch configuration file or image file.

NOTE: On devices running Junos OS Evolved, if downloading a file fails, ZTP restarts.

When any of these events occur, ZTP resets the DHCP client state machine on all of the DHCP client-configured interfaces (management and network) and then restarts the state machine. Restarting the state machine enables the DHCP client to get the latest DHCP server-configured parameters.

Before ZTP restarts, approximately 15 to 30 seconds must elapse to allow enough time to build a list of bound and unbound DHCP client interfaces.

The list of bound and unbound DHCP client interfaces can contain:

- No entries.
- Multiple DHCP client interfaces.

Priority is given to the DHCP client interfaces that have received all ZTP parameters (software image file, configuration file, and file server information) from the DHCP server.

After the lists of bound and unbound client interfaces are created, and a DHCP client gets selected for ZTP activity, any existing default route is deleted and the DHCP client interface that was selected adds a new default route. In order to add a new default route, only one ZTP instance can be active.

After ZTP restarts, the DHCP client attempts fetching files from the DHCP server for up to six times, with ten to fifteen seconds elapsing between attempts. Every attempt, whether successful or not, is logged and can be seen on the console.

If there is a failure, or the number of attempts exceeds the limit, ZTP stops. ZTP then clears the DHCP client bindings and restarts state machine on the DHCP-configured interfaces.

The ZTP restart process continues until there is either a successful software upgrade, or an operator manually commits a user configuration and deletes the ZTP configuration.

Caveats Relating to ZTP

There are two downgrade limitations for EX Series switches:

- If you downgrade to a software version earlier than Junos OS Release 12.2, in which ZTP is not supported, the configuration file autoinstall phase of the zero touch provisioning process does not happen.
- To downgrade to a software version that does not support resilient dual-root partitions (Junos OS Release 10.4R2 or earlier), you must perform some manual work on the device. For more information, see *Configuring Dual-Root Partitions*.

The following are caveats for QFX Series switches:

- On QFX3500 and QFX3600 switches running the original CLI, you cannot use ZTP to upgrade from Junos OS Release 12.2 or later to Junos OS Release 13.2X51-D15 or later.
- QFX5200 switches only work with HTTP in 15.1X53-D30. FTP and TFTP protocols are not supported.
-
- If you are performing Zero Touch Provisioning (ZTP) with a Junos OS image that contains enhanced automation for the QFX5100 switch, configure root authentication, and the provider name, license type, and deployment scope for Chef and Puppet at the [edit system] hierarchy in the configuration file that is fetched from the server:

```
{ master:0}
root# set root-authentication (encrypted-password password | plain-text-password password |
ssh-dsa public-key | ssh-rsa public-key)
root# set extensions providers juniper license-type customer deployment-scope commercial
root# set extensions providers chef license-type customer deployment-scope commercial
```

- In Junos OS Release 18.1R1, if you are upgrading the software, you must perform a full software upgrade. A full upgrade includes upgrading both the Junos OS software and the host software packages.

There are no caveats for Junos OS Evolved platforms.

Zero Touch Provisioning Using WAN Interfaces on PTX1000 Routers

Zero Touch Provisioning (ZTP) allows you to provision your router in your network automatically, with minimal manual intervention. Starting in Junos OS Release 19.3R1, you can use either WAN interfaces or management interfaces, to automatically download and install the appropriate software and the configuration file on your router during the ZTP bootstrap process.

When you connect the router to the network at the first time, you can choose any available WAN port on the router to connect the optics. The ZTP automatically configures WAN interfaces based on the optics type, and then connects your device to the Dynamic Host Configuration Protocol (DHCP) server to perform the bootstrap process.

The WAN interfaces created based on the optics type you connected to the device and the WAN interface speed auto-transitions through all possible supported port speeds until the ZTP gets completed successfully. The speed auto-transition ensures to establish physical link of the WAN port with the optics you connected and the peer end device connectivity to the DHCP server.

[PTX1000 Port Mapping](#) shows the available combinations for the ports on the PTX1000 routers.

Zero Touch Provisioning on PTX10008 Routers

Zero Touch Provisioning (ZTP) allows you to provision your router in your network automatically, with minimal manual intervention. Starting in Junos OS Evolved Release 20.1R1, the PTX10008 devices support automation of the device configuration and software upgrade over the management interface of Routing Engine 0 (RE0).

ZTP is enabled on the PTX10008 device in the factory default mode. You can connect the management interface (re0:mgmt-0) to a network with a Dynamic Host Configuration Protocol (DHCP) server, and then add ZTP configuration to the DHCP server. Use the `show interfaces re0:mgmt-0` command on the PTX10008 device to find the MAC address of the interface to use on the DHCP server configuration.

When the PTX10008 device is able to contact the DHCP server and retrieve ZTP parameters, it performs the following ZTP operations based on these parameters:

1. Fetches the specified image and/or configuration file using the specified protocol.
2. If an image is specified, ZTP installs the image on both Routing Engines and reboots the device.
3. If a configuration file is specified:
 - If the file is a Junos configuration, ZTP applies the configuration on the device.
 - If the file is a script, ZTP execute the script on the device.

SEE ALSO

| *Configuring Dual-Root Partitions*

Zero Touch Provisioning Using DHCP Options

Zero Touch Provisioning (ZTP) allows for automatic provisioning of Juniper Network devices that you add to your network. You can provision any supported device by using either a script to be executed or a configuration file to be loaded. You will also need to configure a DHCP server with required information, which is provided in this procedure, to use ZTP.

Optionally, you can configure an HTTP proxy server for either the phone-home server or redirect server. When the phone-home client receives information regarding the HTTP proxy server via DHCP option 43 suboption 8, it will create an HTTPS transparent tunnel with the proxy server. Once the tunnel is established, the phone-home client uses the tunnel as a proxy for the phone-home server or redirect server. The phone-home client downloads the software image and configuration file through the tunnel onto the device. Once bootstrapping is complete, the device reboots and the tunnel quits.

ZTP requires that your device is in a factory default state. The device from the factory boots with preinstalled software and factory default configuration. On a device that does not currently have the factory default configuration, you can issue the `request system zeroize` command.

NOTE: The request `system zeroize` command is not supported on PTX1000, PTX10001-20C, QFX10002-60C, PTX10002-60C devices. You must issue the request `vmhost zeroize` command (instead of `request system zeroize`) for factory default configuration on PTX1000 routers.

NOTE: On PTX10001-20C devices, after you issue the `request vmhost zeroize` command, you will see the following message twice: VMHost Zeroization : Erase all data, including configuration and log files ? [yes,no] (no) yes warning: Vmhost will reboot and may not boot without configuration Erase all data, including configuration and log files? [yes,no] (no) yes

Before you begin:

- Ensure that the device has access to the following network resources:
 - The DHCP server that provides the location of the software image and configuration files on the network

Refer to your DHCP server documentation for configuration instructions.

- The File Transfer Protocol (anonymous FTP), Hypertext Transfer Protocol (HTTP), or Trivial File Transfer Protocol (TFTP) server on which the software image and configuration files are stored

NOTE: Although TFTP is supported, we recommend that you use FTP or HTTP instead, because these transport protocols are more reliable.



CAUTION: HTTP URLs are limited to 256 characters in length.

- A Domain Name System (DNS) server to perform reverse DNS lookup (not supported).
 - (Optional) An NTP server to perform time synchronization on the network
 - (Optional) A system log (syslog) server to manage system log messages and alerts.
- Syslog messages will be forwarded to this syslog server during ZTP.
- (Optional) An HTTP proxy server for either the phone-home server or redirect server.
 - Locate and record the MAC address for your device.

On PTX10008 devices, the management MAC addresses are located on routing engines.



CAUTION: You cannot commit a configuration while the device is performing the software update process. If you commit a configuration while the device is performing the configuration file autoinstallation process, the process stops, and the configuration file is not downloaded from the network.

To enable zero touch provisioning for a device using DHCP options:

1. Boot the device.
2. Make sure the device has the default factory configuration installed.

Issue the request `system zeroize` command on the device that you want to provision.

NOTE: The request `system zeroize` command is not supported on PTX1000 devices. You must issue the request `vmhost zeroize` command (instead of request `system zeroize`) for factory default configuration on PTX1000 devices.

Starting in Junos OS Evolved Release 19.3R1, on QFX5220-128C device, in Zero Touch Provisioning (ZTP), you can use either WAN interfaces or management interfaces, to automatically download and install the appropriate software and the configuration file on your device during the bootstrap process. ZTP automatically configures on WAN port that has default port speed of 100-Gbps, and then connects your device to the Dynamic Host Configuration Protocol (DHCP) server to perform the bootstrap process:

- If multiple DHCP replies arrive, the ZTP chooses the best set of arguments.
- If multiple interfaces provide the same arguments, ZTP chooses one of the interfaces.
- If there is an error while connecting to DHCP server, ZTP retry to connect DHCP server, and if multiple interfaces again provide same arguments, ZTP choose one of the interfaces.

We recommend you to provision the DHCP server and save the software and configuration file in the specified DHCP server path on the file server.

3. Download the software image file and/or the configuration file to the FTP, HTTP, or TFTP server from which the device will download these files.

NOTE: If you are performing zero touch provisioning with a Junos OS image that contains enhanced automation for the QFX5100 device, configure root authentication and the provider name, license type, and deployment scope for Chef and Puppet at the `[edit system]` hierarchy in the configuration file that is fetched from the server:

```
{ master:0}
root# set root-authentication (encrypted-password password | plain-text-password
password | ssh-dsa public-key | ssh-rsa public-key)
root# set extensions providers juniper license-type customer deployment-scope commercial
root# set extensions providers chef license-type customer deployment-scope commercial
```

4. Configure the DHCP server to provide the necessary information to the device.

Configure IP address assignment.

You can configure dynamic or static IP address assignment for the management address of the device. To determine the management MAC address for static IP address mapping, add 1 to the last byte of the MAC address of the device, which you noted before you began this procedure.

NOTE: This address can be any address from the pool.

5. Define the format of the vendor-specific information for DHCP option 43 in the **dhcpd.conf** file.

Here is an example of an ISC DHCP 4.2 server **dhcpd.conf** file:

```
option space NEW_OP; option;
option NEW_OP.image-file-name code 0 = text;
option NEW_OP.config-file-name code 1 = text;
option NEW_OP.image-file-type code 2 = text;
option NEW_OP.transfer-mode code 3 = text;
option NEW_OP.alt-image-file-name code 4= text;
option NEW_OP.http-port code 5= text;
option NEW_OP-encapsulation code 43 = encapsulate NEW_OP;
option NEW_OP.proxyv4-info code 8 = text;
```

NOTE: Starting in Junos OS Release 18.2R1, a new DHCP option is introduced to set the timeout value for the file downloads over FTP. If the transfer-mode is set as FTP, the default value for the timeout is automatically set as 120 minutes, that is, in case the FTP session gets interrupted due to loss of connectivity in the middle of a file transfer, it will timeout after 120 minutes and ZTP will attempt to retry the file fetching process. This value can be overridden using the DHCP option as follows:

```
option NEW_OP.ftp-timeout code 7 = text;
```

```
option NEW_OP.ftp-timeout "val";
```

where “val” is the user configurable timeout value in seconds and must be provided within quotes (like, "val").

6. Configure the following DHCP option 43 suboptions:

- Suboption 00: The name of the software image file to install.

NOTE: When the DHCP server cannot use suboption 00, configure the software image filename using suboption 04. If both suboption 00 and suboption 4 are defined, suboption 04 is ignored.

```
option NEW_OP.image-file-name "/dist/images/jinstall-ex-4200-13.2R1.1-domestic-  
signed.tgz";
```

- Suboption 01: The name of the script or configuration file to install.

```
option NEW_OP.config-file-name "/dist/config/jn-switch35.config";
```

NOTE: ZTP determines if the file is a script file based on the first line of the file. If the first line contains the characters `#!` followed by an interpreter path, ZTP treats the file as a script and executes it with the specified interpreter path. In order for a script to execute, the script file must provide the ability to fetch and load a valid configuration file on the device during the ZTP process.

The following list provides the types of scripts and their associated interpreter paths:

- Shell script interpreter path: `#!/bin/sh`
- SLAX script interpreter path: `#!/usr/libexec/ui/cscript`
- Python script interpreter path: `#!/usr/bin/python`

For security reasons, Junos OS has strict requirements for running unsigned Python scripts on devices running Junos OS. Only devices running Junos OS with Enhanced Automation and devices running Junos OS Evolved support running unsigned Python scripts as part of the ZTP process.

If the file does not contain special characters (!) , ZTP determines that the file is a configuration file and loads the configuration file.

NOTE: Starting in Junos OS Release 21.1R1, ZTP Python scripts that are fetched from the ZTP server should be migrated to use Python 3 because Python 2.7 is no longer supported. In other words, the interpreter directive line should point to Python 3 and also the script's code needs to be migrated to Python 3.

- Suboption 02: The symbolic link to the software image file to install.

```
option NEW_OP.image-file-type "symlink";
```

NOTE: If you do not specify suboption 2, the ZTP process handles the image filename as a filename, not a symbolic link.

- Suboption 03: The transfer mode that the device uses to access the TFTP, FTP, or HTTP server. If you select FTP as the transfer mode, Junos OS uses the anonymous FTP login to download files from the FTP server.

```
option NEW_OP.transfer-mode "ftp";
```

NOTE: If suboption 03 is not configured, TFTP becomes the transfer mode by default.

- Suboption 04: The name of the software image file to install.

NOTE: If the DHCP server does not support suboption 00, configure the image file using suboption 04. If both suboption 00 and suboption 4 are defined, suboption 04 is ignored.

```
option NEW_OP.alt-image-file-name "/dist/images/jinstall-ex-4200-13.2R1.1-domestic-signed.tgz";
```

- Suboption 05: The HTTP port that the device uses to download either the image or configuration file or both instead of the default HTTP port.

```
option NEW_OP.http-port code 5= 8080;
```

7. (Mandatory) Configure either option 150 or option 66.

NOTE: You must configure either option 150 or option 66. If you configure both option 150 and option 66, option 150 takes precedence, and option 66 is ignored. Also, make sure you specify an IP address, not a hostname, because name resolution is not supported.

- Configure DHCP option 150 to specify the IP address of the FTP, HTTP, or TFTP server.

```
option option-150 code 150={ ip-address};
option option-150 10.100.31.71;
```

- Configure DHCP option 66 to specify the IP address of the FTP, HTTP, or TFTP server.

```
option tftp-server-name "10.100.31.71";
```

8. (Optional) Configure DHCP option 7 to specify one or more system log (syslog) servers.

```
option log-servers 10.100.31.72;
```

9. (Optional) Configure DHCP option 42 to specify one or more NTP servers.

List each NTP server separated by a space.

```
option ntp-servers 10.100.31.73;
```

10. (Optional) Configure DHCP option 12 to specify the hostname of the device.

```
option hostname "jn-switch35";
```

The following sample configuration shows the DHCP options you just configured in this procedure:

```
host jn-switch35 {
    hardware ethernet ac:4b:c8:29:5d:02;
```

```

fixed-address 10.100.31.36;

option tftp-server-name "10.100.31.71";
  option NEW_OP.ftp-timeout " val";
option host-name "jn-switch35";
option log-servers 10.100.31.72;
option ntp-servers 10.100.31.73;
option NEW_OP.image-file-name "/dist/images/jinstall-ex-4200-13.2R1.1-domestic-
signed.tgz";
option NEW_OP.transfer-mode "ftp";
option NEW_OP.http-port code 5= 8080;
option NEW_OP.config-file-name "/dist/config/jn-switch35.config";
}

```

Based on the DHCP options configured in this example, the following items are added to the [edit system] hierarchy:

```

system {
  host-name jn-switch35;

  syslog {
    host 10.100.31.72 {
      any any;
    }
  }
  ntp {
    server 10.100.31.73;
  }
}

```

11. Connect the device to the network that includes the DHCP server and the FTP, HTTP, or TFTP server.
12. Power on the device.
13. Monitor the ZTP process by looking at the console.

NOTE: When SLAX scripts are executed, the `op-script.log` and `event-script.log` files are produced.

You can use these log files to troubleshoot in case something goes wrong.

- `/var/log/dhcp_logfile`

Use this file to check DHCP client logs.

- /var/log/event-script.log

Use this file to check configuration commit status.

- /var/log/image_load_log

Use this file to check software image and configuration file fetch and installation status.

- /var/log/messages

Use this file to check system-level logs.

- /var/log/op-script.log

Use this file to check configuration commit status.

- /var/log/script_output

Use this file to check script execution output.

For Junos OS Evolved, use the **/var/log/ztp.log** file to troubleshoot.

You can also monitor the ZTP process by looking at error messages and issuing operational commands. See ["Monitoring Zero Touch Provisioning" on page 138](#) for more information.

Zero Touch Provisioning Using DHCPv6 Options

The DHCPv6 protocol doesn't have a subnet option for the IA_NA (identity association for non-temporary addresses) to learn and install subnet routes. Instead, the subnet route is installed through Neighbor Discovery Protocol.

In IPv6, devices periodically advertise IPv6 prefixes along with other link parameters using Router Advertisement (RA) messages. On the client (Juniper device running ZTP), once the DHCPv6 client is bound, the Neighbor Discovery Protocol (NDP) will learn these prefixes and installs the prefix routes via the client interface, with the next hop as the link to the local address of the gateway device.

On the client device, router advertisement configuration is enabled by default along with the DHCPv6 configuration.

- Ensure that the device has access to the following network resources:
 - The DHCP server that provides the location of the software image and configuration files on the network

Refer to your DHCP server documentation for configuration instructions.

- On the MX Series, the File Transfer Protocol (anonymous FTP), Trivial File Transfer Protocol (TFTP), Hypertext Transfer Protocol (HTTP), or Hypertext Transfer Protocol Secure (HTTPS) server on which the software image and configuration files are stored.



CAUTION: HTTP URLs are limited to 256 characters in length.

- On the EX3400, EX4300, QFX5100, and QFX5200 devices, the Hypertext Transfer Protocol (HTTP) or Hypertext Transfer Protocol Secure (HTTPS) server on which the software image and configuration files are stored.



CAUTION: HTTP URLs are limited to 256 characters in length.

- (Optional) An HTTP proxy server for either the phone-home server or redirect server.
- Locate and record the MAC address printed on the device.

Zero Touch Provisioning (ZTP) allows for automatic provisioning of Juniper Network devices that you add to your network. You can provision any supported device by using either a script to be executed or a configuration file to be loaded.

To use ZTP, you configure a DHCP server to provide the required information. If you do not configure the DHCP server to provide this information, the device boots with the preinstalled software and default factory configuration. If your device is not in a factory default state, you can issue the `request system zeroize` command.

Optionally, you can configure an HTTP proxy server for either the phone-home server or redirect server. When the phone-home client receives information regarding the HTTP proxy server via DHCP option 17 suboption 8, it will create an HTTPS transparent tunnel with the proxy server. Once the tunnel is established, the phone-home client uses the tunnel as a proxy for the phone-home server or redirect server. The phone-home client downloads the software image and configuration file through the tunnel onto the device. Once bootstrapping is complete, the device reboots and the tunnel quits.

NOTE: Starting in Junos OS Release 20.2R1-S1, the DHCPv6 client is supported the MX-Series, EX3400, EX4300, QFX5100, and QFX5200 switches. Both DHCPv4 and DHCPv6 clients are included as part of the default configuration. During the bootstrap process, the device first uses the DHCPv4 client to request for information regarding image and configuration file from the DHCP server. The device checks the DHCPv4 bindings sequentially. If there is a failure with one of the DHCPv4 bindings, the device will continue to check for bindings until provisioning is successful. If there are no DHCPv4 bindings, however, the device will check for DHCPv6

bindings and follow the same process as for DHCPv4 until the device can be provisioned successfully. The DHCP server uses DHCPv6 options 59 and 17 and applicable sub-options to exchange ZTP-related information between itself and the DHCP client.



CAUTION: You cannot commit a configuration while the device is performing the software update process. If you commit a configuration while the device is performing the configuration file autoinstallation process, the process stops, and the configuration file is not downloaded from the network.

To use zero touch provisioning for a device using DHCPv6 options:

1. Boot the device.
2. Make sure the device has the default factory configuration installed.
 - If multiple DHCP replies arrive, the ZTP chooses the best set of arguments.
 - If multiple interfaces provide the same arguments, ZTP chooses one of the equal interfaces.
 - If there is an error while connecting to the DHCP server, ZTP tries again to connect to the DHCP server. If multiple interfaces again provide the same arguments, ZTP chooses one of the interfaces.

We recommend you to provision the DHCP server and save the software and configuration file in the specified DHCP server path on the file server.

3. Download the software image file and the configuration file to the FTP, HTTP, HTTPS, or TFTP server from which the device will download these files.
4. Configure the DHCP server to provide the necessary information to the device.
5. Configure IP address assignment.

You can configure dynamic or static IP address assignment for the management address of the device. To determine the management MAC address for static IP address mapping, add 1 to the last byte of the MAC address of the device, which you noted before you began this procedure.

6. Define the format of the DHCPv6 option 59 (OPT_BOOTFILE_URL) in the **dhcpcd6.conf** file, so the server can send information about URLs to images to the client.

NOTE: Only the HTTP and HTTPS transport protocols are supported on the EX3400, EX4300, QFX5100, and QFX5200 devices.

Here's the format for this option:

```
transfer-mode://[<ipv6-address>]:<port-number>/<path/image-file-name>
```

For example:

```
ftp://[2001:db8::40]:21/ZTP/bootimage.tgz
tftp://[2001:db8::40]:69/ZTP/bootimage.tgz
http://[2001:db8::40]:80/ZTP/bootimage.tgz
https://[2001:db8::40]:443/ZTP/bootimage.tgz
```

The transfer mode and IPv6 address are required, but the port number is optional. If you do not specify the port number, the default port number of the transfer mode is used. If you specify the port number in options 17 and 59, then the port number mentioned in option 17 vendor-specific information option is used.

You can specify the image file name in either option 59 or option 17. If the image file name is mentioned in both options 59 and 17, then the image name mentioned in option 17 vendor-specific information option is used.

7. Define the format of the vendor-specific information for the following DHCP option 17 suboptions:

Here is an example of an ISC DHCP 4.2 server `dhcdd6.conf` file:

```
option space NEW_OP_V6 code width 2 length width 2;
option NEW_OP_V6.image-file-name code 0 = text;
option NEW_OP_V6.config-file-name code 1 = text;
option NEW_OP_V6. image-file-type code 2 = text;
option NEW_OP_V6.transfer-mode code 3 = text;
option NEW_OP_V6. alt-image-file-name code 4 = text;
option NEW_OP_V6.port-number code 5 = text;
option NEW_OP_V6. jloader-file code 6 = text;
option NEW_OP_V6. ftp-timeout code 7 = text;
option NEW_OP_V6.proxyv6-info code 8 = text;
option vsio.NEW_OP_V6 code 2636 = encapsulate NEW_OP_V6;
```

- Suboption 00: The name of the software image file to install.

NOTE: When the DHCP server cannot use suboption 00, configure the software image filename using suboption 04. If both suboption 00 and suboption 4 are defined, suboption 04 is ignored.

```
option NEW_OP_V6.image-file-name "ZTP_IMAGES/jinstall-qfx-5-20.2-img.tgz";
```

- Suboption 01: The name of the script or configuration file to install.

```
option NEW_OP_V6.config-file-name "ZTP_FILES/baseline_config";
```

NOTE: ZTP determines if the file is a script file based on the first line of the file. If the first line contains the characters `#!` followed by an interpreter path, ZTP treats the file as a script and executes it with the specified interpreter path. In order for a script to execute, the script file must provide the ability to fetch and load a valid configuration file on the device during the ZTP process.

The following list provides the types of scripts and their associated interpreter paths:

- Shell script interpreter path: `#!/bin/sh`
- SLAX script interpreter path: `#!/usr/libexec/ui/cscript`
- Python script interpreter path: `#!/usr/bin/python`

For security reasons, Junos OS has strict requirements for running unsigned Python scripts on devices running Junos OS. Only devices running Junos OS with Enhanced Automation and devices running Junos OS Evolved support running unsigned Python scripts as part of the ZTP process.

If the file does not contain special characters (`#!`), ZTP determines that the file is a configuration file and loads the configuration file.

NOTE: Starting in Junos OS Release 21.1R1, ZTP Python scripts that are fetched from the ZTP server should be migrated to use Python 3 because Python 2.7 is no longer supported. In other words, the interpreter directive line should point to Python 3 and also the script's code needs to be migrated to Python 3.

- Suboption 02: The image type.

```
option NEW_OP_V6.image-file-type symlink;
```

NOTE: If you do not specify suboption 2, the ZTP process handles the software image as a filename, not a symbolic link.

- Suboption 03: The transfer mode that the device uses to access the TFTP, FTP, HTTP, or HTTPS server.

```
option NEW_OP_V6.transfer-mode "https";
```

NOTE: If suboption 03 is not configured, the transfer mode mentioned in option 59 for the boot image URL is used.

- Suboption 04: The name of the software image file to install.

NOTE: When the DHCP server cannot use suboption 00, configure the image file using suboption 04. If both suboption 00 and suboption 4 are defined, suboption 04 is ignored.

```
option NEW_OP_V6.alt-image-file-name "ZTP_IMAGES/jinstall-qfx-5-20.2-alternate-img.tgz";
```

- Suboption 05: The port that the device uses to download either the image or configuration file or both instead of the default port.

```
option NEW_OP_V6.port-number 8080;
```

- Suboption 06: The JLoader package file name (supported only on QFX5100 devices)

```
option NEW_OP_V6."jloader.tgz";
```

- Suboption 07: FTP timeout code.

```
option NEW_OP_V6. ftp-timeout "val";
```

- The DHCPv6 protocol defines the Vendor-specific Information Option ("VSIO") in order to send vendor options encapsulated in a standard DHCP option.

```
option vsio.NEW_OP_V6 code 2636 = encapsulate NEW_OP_V6;
```

The following sample configuration shows the DHCPv6 options you've just configured:

```
subnet6 2001:db8::/32 {
    range6 2001:db8::10 2001:db8::40;
}
host chocolate {
    option host-name chocolate;
    hardware ethernet 00:a0:a5:7b:cd:38;
    fixed-address6 2001:db8::11;
    option dhcp6.bootfile-url "https://[2001:db8::1]";

    option NEW_OP_V6.image-file-name "ZTP_IMAGES/jinstall-qfx-5-20.2I-img.tgz";
    option NEW_OP_V6.port-number 8080;
    option NEW_OP_V6.config-file-name "ZTP_FILES/baseline_config";
    option NEW_OP_V6.image-file-type symlink;
    option NEW_OP_V6.transfer-mode "https";
    option NEW_OP_V6.jloader-file "jloader.tgz ";
    option dhcp6.vendor-opts code 17 = string
    option NEW_OP.proxyv6-info "http://[2001::1]:3128";
}
```

8. Power on the device with the default configuration.
9. Monitor the ZTP process by looking at the the console.

NOTE: When SLAX scripts are executed, the `op-script.log` and `event-script.log` files are produced.

You can also use these log files to troubleshoot in case something goes wrong.

- `/var/log/dhcp_logfile`

Use this file to check DHCP client logs.

- /var/log/event-script.log

Use this file to check configuration commit status.

- /var/log/image_load_log

Use this file to check software image and configuration file fetch and installation status.

- /var/log/messages

Use this file to check system-level logs.

- /var/log/op-script.log

Use this file to check configuration commit status.

- /var/log/script_output

Use this file to check script execution output.

You can also monitor the ZTP process by looking at error messages and issuing operational commands. See ["Monitoring Zero Touch Provisioning" on page 138](#) for more information.

Zero Touch Provisioning on SRX Series Devices

IN THIS SECTION

- [Understanding Zero Touch Provisioning on SRX Series Devices | 129](#)
- [Configuring Zero-Touch Provisioning on an SRX Series Device | 133](#)
- [Understanding Factory-Default Configuration on SRX Series Device for Zero Touch Provisioning | 137](#)

Understanding Zero Touch Provisioning on SRX Series Devices

IN THIS SECTION

- [Understanding ZTP on SRX Series Devices | 130](#)
- [Network Activator Overview | 130](#)
- [Limitations | 133](#)

This topic includes following sections:

Understanding ZTP on SRX Series Devices

Zero Touch Provisioning (ZTP) enables you to provision and configure devices automatically, minimizing most of the manual intervention required for adding devices to a network. ZTP is supported on SRX300, SRX320, SRX340, SRX345, SRX550M, and SRX1500 devices.

Starting in Junos OS Release 20.2R1 on SRX300, SRX320, SRX340, SRX345, SRX550 HM, and SRX1500 devices, you can use Zero Touch Provisioning with DHCP options to provision your device. See ["Zero Touch Provisioning Using DHCP Options" on page 114](#) for more information.

ZTP on SRX Series devices is responsible for the initial bootup and configuration of the device when the device is powered on. This functionality includes:

- Providing the bare-minimum bootstrapping of the device. The SRX Series device is shipped with a factory-default configuration. The factory-default configuration includes the URL of the redirect server, that is used to connect to the central server by using a secure encrypted connection.
- Automatically connecting to the server over the Internet, and downloading the configuration and Junos OS image as specified by the customer or user from the server when the SRX Series device boots up with the factory-default configuration. The new image is installed first and then the initial configuration is applied and committed on the SRX Series device.

ZTP offers the following advantages:

- Simplified and faster deployment
- Increased configuration accuracy
- Support for scaling of network without additional resources

The ZTP process uses Network Activator to initially provision SRX Series devices.

Network Activator Overview

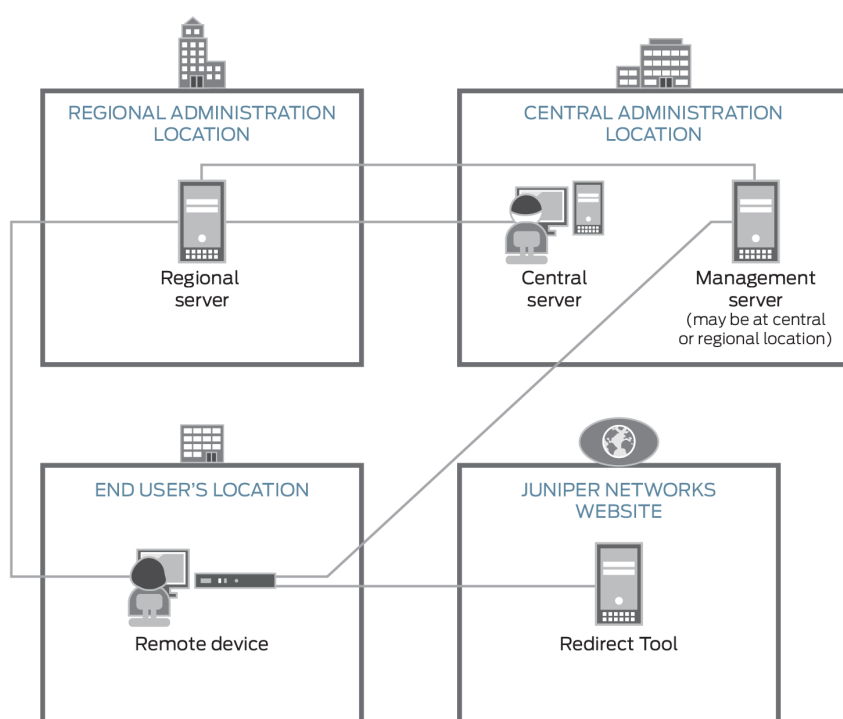
Network Service Activator enables fast device discovery and provisioning for automated configuration to eliminate complex device setup.

Network Activator initially provisions SRX Series devices (henceforth referred to as *remote devices* in this documentation), which reside at end users' sites. The remote devices download a boot image and initial configuration files from servers hosting Network Activator, using a process that provides full authorization and authentication for all interactions. When initial provisioning is complete, the remote device communicates with a management server, which then starts to manage and monitor the remote device.

Network Activator uses a distributed architecture to support remote devices. Network Activator is installed on one central administration server (central server) and multiple regional administration servers (regional servers). A device communicates directly with its assigned regional server. The distributed architecture optimizes the efficiency of the initial provisioning process, contributing to high performance and scaling of the network.

Figure 2 on page 131 illustrates the distributed architecture and the components involved in the initial provisioning process.

Figure 2: Components Involved in Initial Provisioning of Remote Device



The roles of the components in the initial provisioning process are as follows:

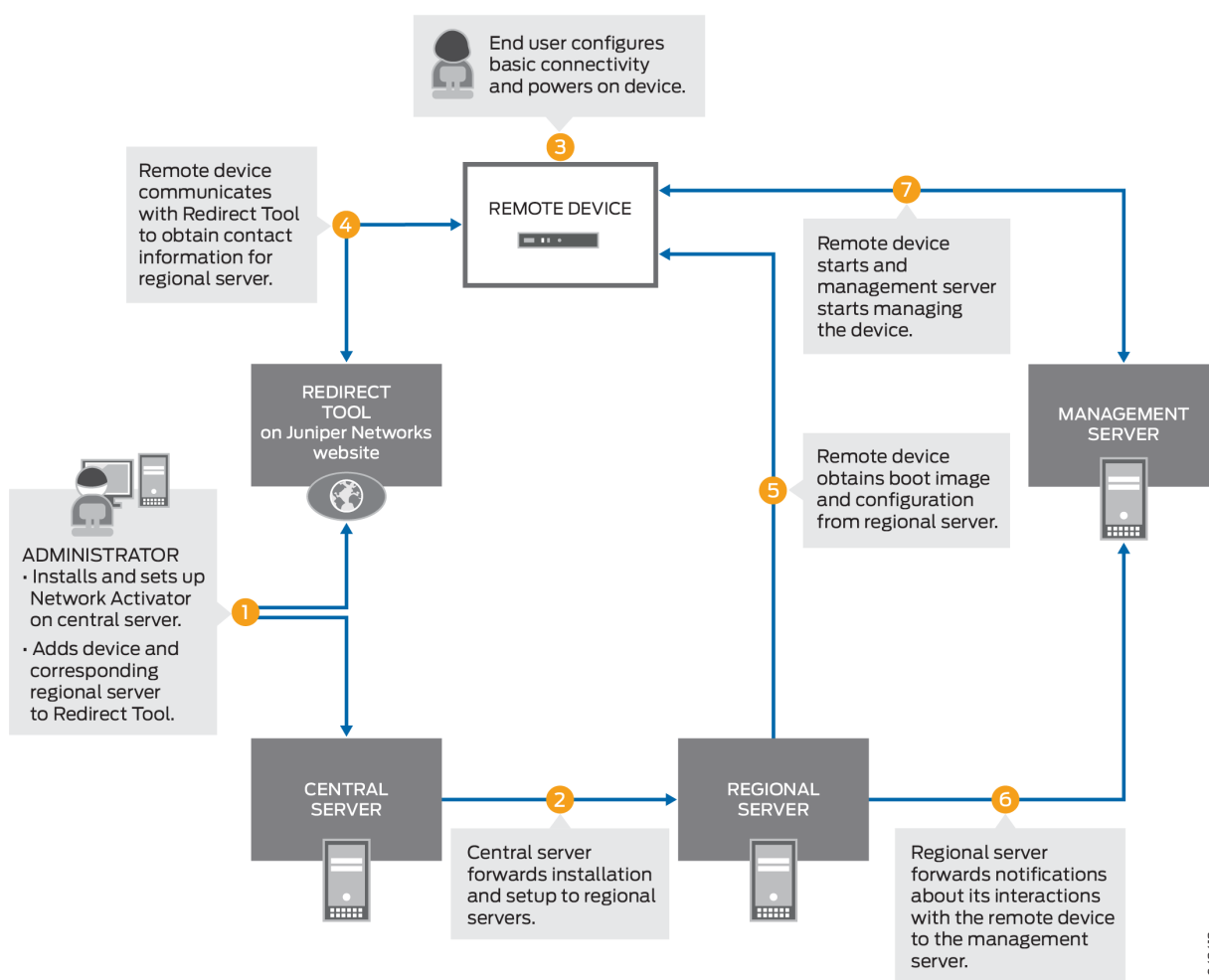
- The remote device sends requests for initial provisioning. The remote device resides at the end user's location.
- The Redirect Tool provides authentication and authorization for remote devices to access their assigned regional servers through use of ITU-T X.509 private key infrastructure (PKI) digital certificates. Redirect service is hosted on Amazon Web Services (AWS), operated and maintained by Juniper Networks.
- The central server hosts Network Activator and communicates with the regional activator servers. Administrators at a service provider or central enterprise location interact with this server to install

and set up Network Activator. The central server is located at a central geographic location for the service provider.

- The regional server also hosts Network Activator. This server stores information about its assigned remote devices and communicates directly with those devices. This server typically resides at a regional administrative location the provider designates for the end user.

Figure 3 on page 132 illustrates the initial provisioning workflow.

Figure 3: Workflow for Initial Provisioning



In detail, the provisioning workflow proceeds as follows:

1. The administrator at the service provider:
 - Installs and sets up Network Activator on the central server.
 - Adds remote devices and regional servers in the Redirect Tool.

2. The central server forwards the installation to the regional servers.
3. The end user powers on the remote device, connects it to a computer, and enters the authentication code in the webpage to send a request for initial provisioning.
4. The device transmits its X.509 certificate and fully qualified domain name (FQDN) as a provisioning request to the Redirect Tool.
5. The Redirect Tool searches its data store for the regional server that the administrator specified for this device, and confirms that the device's request corresponds to the X.509 certificate specified for the server.
6. The Redirect Tool sends contact information for the regional server to the device.
7. The device sends a request to the regional server for the URL of the boot image and the location of the initial configuration.
8. The regional server sends the information to the device.
9. The device obtains the boot image and configuration from the regional server.
10. The device uses the boot image and configuration to start and become operational.

Limitations

- There are no restrictions on the number of attempts for entering the correct activation code.
- If the remote device is not able to reach the server (because the configured address in the factory-default configuration is not correct or the server is down, and so on), the remote device attempts to connect to an alternative server (if configured in the factory-default configuration). If there is only one server configured, then you can reattempt to connect. In such scenarios, we recommend that you configure the device manually through the console.
- Captive portal redirection, required for automatically redirecting users to the authentication webpage for entering the activation code, is not supported. You must manually navigate to the activation page after connecting to the device.

Configuring Zero-Touch Provisioning on an SRX Series Device

Before you begin:

- Unpack the device, install it, complete the necessary cabling, connect a laptop or any other terminal device, and power on the device. See the *Hardware installation Guide* for your device for more information.
- For SRX300, SRX320, SRX340, SRX345, and SRX550M devices, connect the management device and access the J-Web interface.

For more information, see Quick Start guides of respective devices at [SRX300](#), [SRX320](#), [SRX340](#), [SRX345](#), and [SRX550M](#).

You are provided with an option to use ZTP; you can use this option or skip it and continue with J-Web wizards.

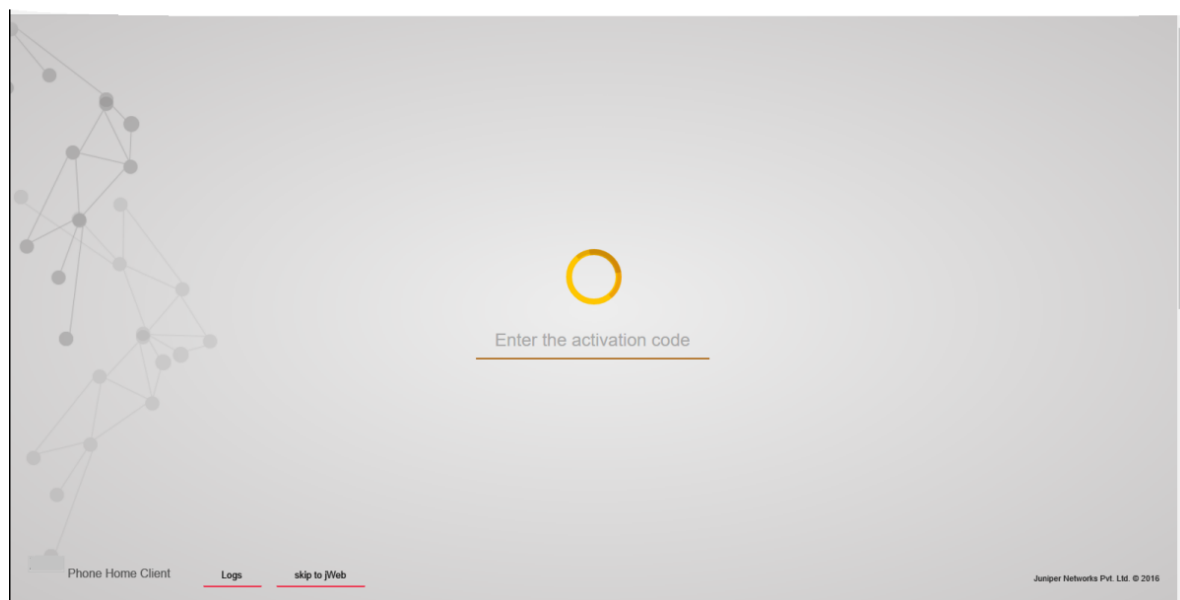
- For SRX1500 devices, before you can use J-Web to configure your device, you must access the CLI to configure the root authentication and the management interface. For more information, see [How to Set Up Your SRX1500 Services Gateway](#).

This section provides step-by-step instructions on how to use ZTP on an SRX Series device for initial provisioning of the device.

To provision an SRX Series device by using ZTP:

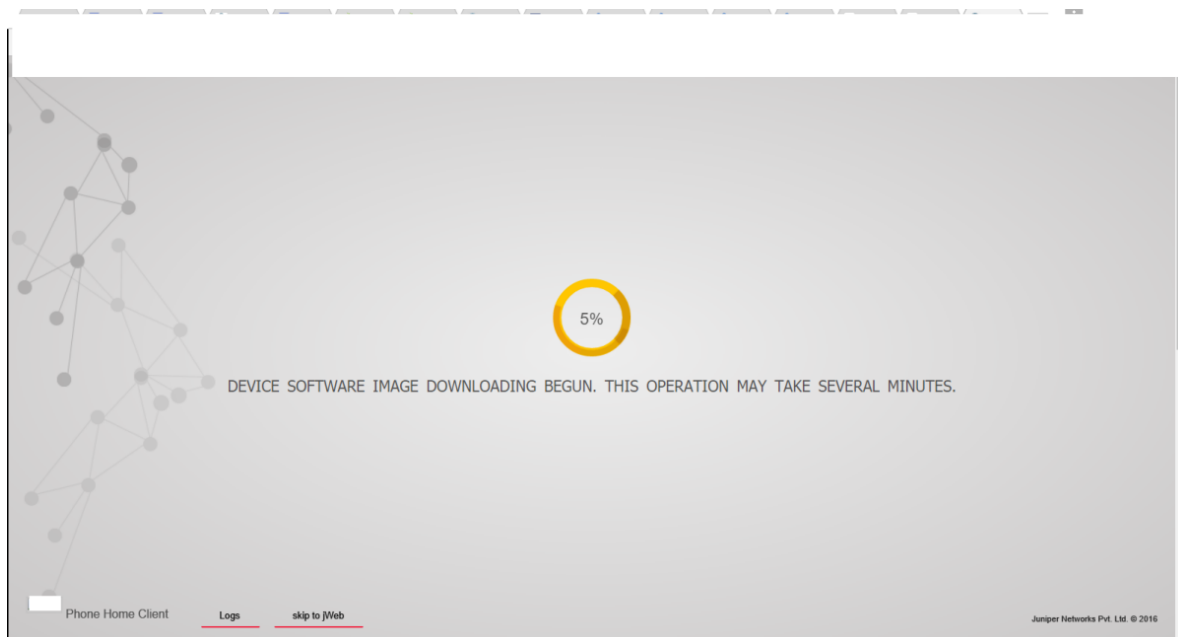
1. Connect a management device (PC or laptop) to any front panel Ethernet port (WAN port) of the SRX Series device.
2. Launch a Web browser from the management device and enter the authentication code in the webpage as shown in [Figure 4 on page 134](#).

Figure 4: Entering Activation Code for ZTP



After the device is successfully authenticated, it starts downloading the software image and initial configuration from the server as shown in [Figure 5 on page 135](#).

Figure 5: Initiating ZTP Process (Software Image Downloading)

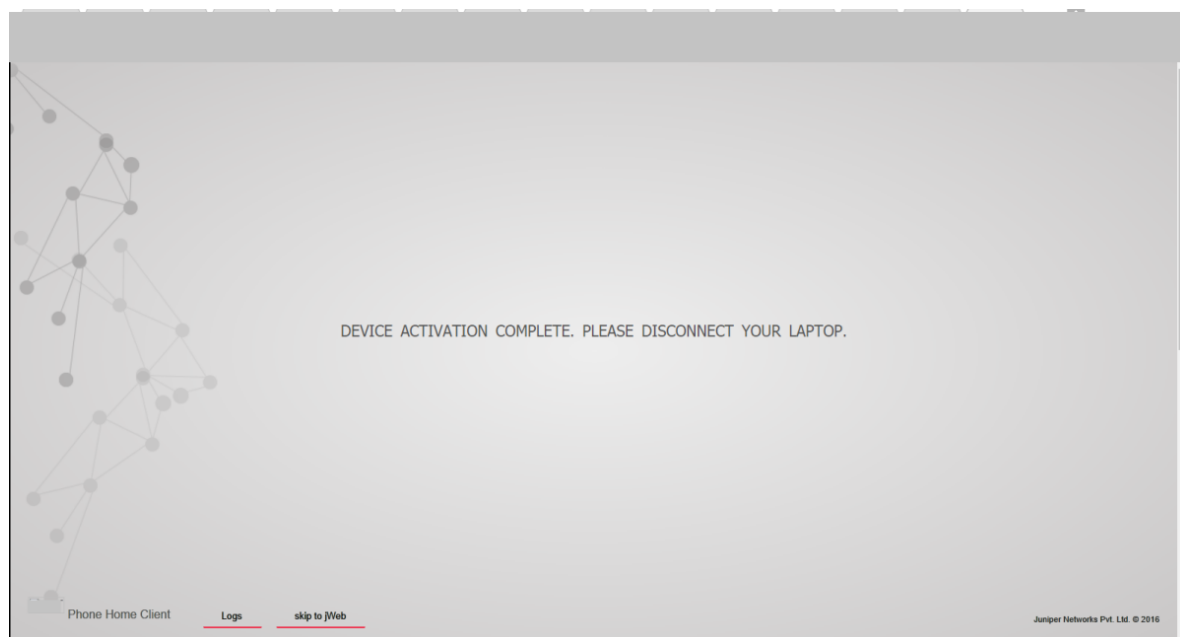


At this step:

- The activation code is sent to the server, and if the authentication is successful, the server pushes the initial configuration to the device. If the authentication is unsuccessful, you are asked to provide the correct code.
- The server can optionally push a new software image on the SRX Series device. In that case, the new image is installed first and then the initial configuration is applied and committed on the device.

The new image is installed and then the initial configuration is applied and committed on the device. When the process is complete, a confirmation message is displayed, as shown in [Figure 6 on page 136](#).

Figure 6: Completing ZTP Process



3. Click **Logs** to display details of the bootstrapping process.

After successfully installing the new software image and configuration on the system, the client sends the bootstrap-complete notification to the server that provided the image and the configuration. After the notification is sent, the configuration that includes the names of servers is deleted from the system. When you use ZTP the next time, you must explicitly configure the URL of the redirect server.

NOTE: In case of failure at any stage, the procedure is started all over again.

NOTE: The ZTP process either upgrades or downgrades the Junos OS version. During a downgrade on an SRX Series device, if you downgrade to a software version earlier than Junos OS Release 15.1X49-D100, in which ZTP is not supported, the autoinstallation phase of the ZTP process does not happen.

For SRX300, SRX320, SRX340, SRX345, and SRX550M devices, ZTP is the default method for provisioning the devices. However, if you want to use J-Web-based provisioning (J-Web setup wizards

supported for the SRX300 line of devices and SRX550M devices), then instead of ZTP, you can use the option provided in the client portal to skip to J-Web setup wizards for performing the initial software configuration of your device.

If you select the **Skip to JWeb** option, you must configure the system root authentication password as shown in [Figure 7 on page 137](#).

Figure 7: Configuring System Root-Authentication Password

NOTE: For SRX1500 devices, the **Skip to JWeb** option is not supported. To access J-Web, the ZTP client configuration must be deleted during the initial setup of SRX1500 through CLI.

Understanding Factory-Default Configuration on SRX Series Device for Zero Touch Provisioning

Your services gateway is shipped with a factory-default configuration. Following is a sample of the default configuration that includes configuration for ZTP:

```
system {
  phone-home {
    rfc-compliant;
    server https://redirect.juniper.net;
```



```
}
}
```

Note that, in this configuration:

- `server` indicates the name or IP address of the server. The factory-default configuration on an SRX Series device might include IP addresses of more than one servers.
- `rfc-compliant` indicates that after an upgrade, the server enforces certain behaviors that are compliant with RFC standards.

NOTE: By default, the system autoinstallation configuration is part of the factory-default configuration of the device. So, the administrator must ensure that the configuration file sent from the regional server to the remote device (SRX series device) must include the `delete system autoinstallation` option in the factory-default configuration.

Monitoring Zero Touch Provisioning

IN THIS SECTION

- [Using the Console to Monitor Zero Touch Provisioning | 139](#)
- [Using System Log Alerts to Monitor Zero Touch Provisioning | 139](#)
- [Using Error Messages to Monitor Zero Touch Provisioning | 140](#)
- [Using System Log Files to Monitor Zero Touch Provisioning in Junos OS Using DHCP Options | 141](#)
- [Using System Log Files to Monitor Zero Touch Provisioning in Junos OS Using DHCPv6 Options | 142](#)
- [Using the Console to Monitor Zero Touch Provisioning in Junos OS Evolved | 143](#)
- [Using the `show dhcp client binding` Command | 145](#)
- [Using the `show dhcpv6 client binding` Command | 147](#)
- [Using the `show dhcp client statistics` Command | 148](#)
- [Using the `show dhcpv6 client statistics` Command | 149](#)

Starting in Junos OS Release 12.2, you can use the console and operational commands to monitor Zero Touch Provisioning.

Starting in Junos OS Evolved Release 19.1R1, to monitor zero touch provisioning on Junos OS Evolved, use the `show system ztp` command.

Using the Console to Monitor Zero Touch Provisioning

The following Zero Touch Provisioning (ZTP) activities are displayed on the console during the ZTP process:

- Starting and ending times of ZTP process.
- Lists of bound and unbound DHCP client interfaces.
- DHCP options that DHCP servers send to DHCP clients.
- Logs indicating which interfaces are used for ZTP.
- ZTP parameters that DHCP clients obtain from DHCP servers.
- Filenames of configuration and image files, names of file servers, protocols used to fetch files, and times when DHCP servers fetch configuration and image files.
- Failure states caused by files not being on servers, or unreachable servers, and time outs.
- Number of attempts made, and number of attempts remaining, for retry in current ZTP cycle.
- Completion of file transfers.
- Installation, reboot, and state of ZTP process.
- Internal state errors and termination of ZTP process.
- Logs for when default routes were added or deleted.

Using System Log Alerts to Monitor Zero Touch Provisioning

IN THIS SECTION

- [Purpose | 139](#)
- [Action | 140](#)
- [Meaning | 140](#)

Purpose

In this example, the system log alert alerts you that the auto-image upgrade will start.

Action

Use the following system log alert to monitor the auto-image upgrade process.

```
"ALERT:Auto-image upgrade will start. This can terminate config CLI session(s). Modified
configuration will be lost. To stop Auto-image, in CLI do the
following: 'edit; delete chassis auto-image-upgrade; commit'."
```

```
"Checking whether image upgrade is already invoked"
```

Meaning

This system log alert indicates that the auto-image upgrade will start, and provides information on how to stop the auto-image upgrade process.

Using Error Messages to Monitor Zero Touch Provisioning**IN THIS SECTION**

- [Purpose | 140](#)
- [Action | 140](#)
- [Meaning | 141](#)

Purpose

Error messages provide information on which DHCP options are not configured.

Action

Use the information in the following error message to find out which DHCP options are not configured.

```
"DHCP Log Server Option"
"DHCP Host Name Option"
"DHCP NTP Server Option"
```

Meaning

The error message indicates that the DHCP log server, hostname, and NTP server options are not configured.

Using System Log Files to Monitor Zero Touch Provisioning in Junos OS Using DHCP Options

IN THIS SECTION

- Purpose | 141
- Action | 141
- Meaning | 142

Purpose

System log files provide information on the state of the auto-upgrade process, lists of bound and unbound DHCP client interfaces, IP addresses of file servers, names and locations of image and configuration files, and successful and failed attempts at fetching configuration and image files.

Action

Use the information in the following system log files to monitor the auto-upgrade process.

```
Auto Image Upgrade: Start fetching config-file file from server 10.1.1.1 through irb using ftp
```

```
Auto Image Upgrade: Tried [2] attempts to fetch config-file file from server 10.1.1.1 through
irb. Summary: "Retrieving /config-file
:: Failed to open file.". To retry [4] times.
```

```
Auto Image Upgrade: Tried [4] attempts to fetch config-file file from server 10.1.1.1 through
irb. Summary: "Retrieving /config-fileconfig-file
:: Failed to open file.". To retry [2] times.
```

```
Auto Image Upgrade: Tried [6] attempts to fetch config-file file from server 10.1.1.1 through
irb. Summary: "Retrieving /config-file
:: Failed to open file.". To retry [0] times.
```

```
Auto Image Upgrade: All [6] attempts to fetch config-file file from server 10.1.1.1 through irb
FAILED. Start retry again in few minutes.
```

Meaning

These system log files indicate that there were six failed attempts to fetch the configuration file from the file server, the IP address of the file server, the DHCP client interface name, and the number of times the retry process occurred.

Using System Log Files to Monitor Zero Touch Provisioning in Junos OS Using DHCPv6 Options

IN THIS SECTION

- Purpose | 142
- Action | 142
- Meaning | 143

Purpose

System log files provide information on the state of the auto-upgrade process, lists of bound and unbound DHCP client interfaces, IP addresses of file servers, names and locations of image and configuration files, and successful and failed attempts at fetching configuration and image files.

Action

Use the information in the following system log files to monitor the auto-upgrade process.

```
Auto Image Upgrade: Tried [2] attempts to fetch junos-vmhost-install
-20.2.tgz file from server 2001:db8::1 through et-0
/0/0:2. Summary: "fetch-secure: https://[2001:*: Connection refused". To retry
[4] times.
```

```
Auto Image Upgrade: Tried [4] attempts to fetch junos-vmhost-install
-20.2.tgz file from server 2001:db8::1 through et-0
```

```
/0/0:2. Summary: "fetch-secure: https://[2001*: Connection refused". To retry
[2] times.
```

```
Auto Image Upgrade: Tried [6] attempts to fetch junos-vmhost-install-
20.2.tgz file from server 2001:db8::1 through et-0
```

```
/0/0:2. Summary: "fetch-secure: https://[2001*: Connection refused". To retry
[0] times.
```

Meaning

These system log files indicate that there were six failed attempts to fetch the image file from the file server, the IP address of the file server, the DHCPv6 client interface name, and the number of times the retry process occurred.

Using the Console to Monitor Zero Touch Provisioning in Junos OS Evolved

IN THIS SECTION

- Purpose | 143
- Action | 143
- Meaning | 145

Purpose

System log files provide information on the state of the auto-upgrade process, lists of bound and unbound DHCP client interfaces, IP addresses of file servers, names and locations of image and configuration files, and successful and failed attempts at fetching configuration and image files.

Action

Use the information in the console to monitor the auto-upgrade process.

Here is an example of output for Junos OS Evolved.

```
164.319243] ztp.py[15456]: 2019-07-11 17:54:25 INFO: ZTP: Booted with factory settings set auto-
image-upgrade
ztp.py[15456]: 2019-07-11 17:54:26 INFO: ZTP: loading config
[ 184.456977] ztp.py[15456]: 2019-07-11 17:54:45 INFO: ZTP: Releasing prior dhcp state
```

```

[ 184.520075] ztp.py[15456]: 2019-07-11 17:54:46 INFO: ZTP: initializing
[ 184.520736] ztp.py[15456]: 2019-07-11 17:54:46 INFO: ZTP: Interface vmb0 Watching
path /var/db/scripts/ztp/ztpopt.vmb0
[ 184.566657] ztp.py[15456]: 2019-07-11 17:54:46 INFO: ZTP: Interface vmb0v6 Watching
path /var/db/scripts/ztp/ztpopt6.vmb0
[ 184.603976] ztp.py[15456]: 2019-07-11 17:54:46 INFO: ZTP: remove "chassis auto-image-upgrade"
from config to abort ZTP
[ 184.605897] ztp.py[15456]: 2019-07-11 17:54:46 INFO: ZTP: send DHCP discover on interface vmb0
[ 184.606083] ztp.py[15456]: 2019-07-11 17:54:46 INFO: ZTP: send DHCP discover on interface
vmb0v6
[ 205.043925] ztp.py[15456]: 2019-07-11 17:55:06 INFO: ZTP: loading options config
[ 225.528749] ztp.py[15456]: 2019-07-11 17:55:27 INFO: ZTP:(vmb0) Running: ['/sbin/dhclient',
'-1', '-v', 'vmb0', '-cf', '/var
/db/scripts/ztp/dhclient.conf', '-pf', '/var/db/scripts/ztp/vmb0.pid4']
[ 227.349638] ztp.py[15456]: 2019-07-11 17:55:28 INFO: ZTP: loading options config
[ 248.512666] ztp.py[15456]: 2019-07-11 17:55:50 INFO: ZTP:(vmb0) Running: ['/sbin/dhclient',
'-6', '-D', 'LL', '-1', '-v', 'v
mb0', '-cf', '/var/db/scripts/ztp/dhclient6.conf', '-pf', '/var/db/scripts/ztp/vmb0.pid6']
[ 309.448411] ztp.py[15456]: 2019-07-11 17:56:50 ERROR: ZTP:(vmb0v6) Unable to get DhcpInfo
[ 309.452340] ztp.py[15456]: 2019-07-11 17:56:50 INFO: ZTP: intf vmb0 ipaddr is 10.10.213.111
[ 309.453114] ztp.py[15456]: 2019-07-11 17:56:50 INFO: ZTP: intf vmb0 subnetmask is
255.255.255.0
[ 309.453379] ztp.py[15456]: 2019-07-11 17:56:50 INFO: ZTP: intf vmb0 option150addr is
10.10.213.1
[ 309.453619] ztp.py[15456]: 2019-07-11 17:56:50 INFO: ZTP: intf vmb0 option66addr is
10.10.213.1
[ 309.453836] ztp.py[15456]: 2019-07-11 17:56:50 INFO: ZTP: intf vmb0 host-name is sw-s3-u8-07
[ 309.454093] ztp.py[15456]: 2019-07-11 17:56:50 INFO: ZTP: intf vmb0 ntp server is
['10.129.255.62']
[ 309.454267] ztp.py[15456]: 2019-07-11 17:56:50 INFO: ZTP: intf vmb0 ntp server is
['10.129.255.62', '10.129.255.63']
[ 309.454451] ztp.py[15456]: 2019-07-11 17:56:50 INFO: ZTP: intf vmb0 log server is 10.10.213.1
[ 309.454673] ztp.py[15456]: 2019-07-11 17:56:50 INFO: ZTP: intf vmb0 image path is /ZTP_IMAGES/
junos-evo-install-ptx-chassis-x
86-64-19.4EVO.iso
[ 309.454886] ztp.py[15456]: 2019-07-11 17:56:50 INFO: ZTP: intf vmb0 config path is /
ZTP_CONFIG/sw-s3-u8-07.cfg
[ 309.455217] ztp.py[15456]: 2019-07-11 17:56:50 INFO: ZTP: intf vmb0 transfertype is tftp
[ 309.457209] ztp.py[15456]: 2019-07-11 17:56:50 INFO: ZTP: Chose interface vmb0:
[ 309.633177] ztp.py[15456]: 2019-07-11 17:56:51 INFO: ZTP: loading options config
[ 333.584288] ztp.py[15456]: 2019-07-11 17:57:15 INFO: ZTP: downloading image file/ZTP_IMAGES/
junos-evo-install-ptx-chassis-x86
-64-19.4-20190708.2-EVO.iso

```

```
[ 333.584840] ztp.py[15456]: 2019-07-11 17:57:15 INFO: ZTP: downloading image file
local /var/tmp/junos-evo-install-ptx-chassis
-x86-64-19.4-20190708.2-EVO.iso
[ 554.625986] ztp.py[15456]: No such vrf (None)
[ 554.628523] ztp.py[15456]: 2019-07-11 18:00:56 INFO: ZTP: Downloaded image file
[ 554.629289] ztp.py[15456]: 2019-07-11 18:00:56 INFO: ZTP: Downloading config file /
ZTP_CONFIG/sw-s3-u8-07.cfg
[ 555.198176] ztp.py[15456]: No such vrf (None)
[ 555.200076] ztp.py[15456]: 2019-07-11 18:00:56 INFO: ZTP: Downloaded config file
[ 555.201882] ztp.py[15456]: 2019-07-11 18:00:56 INFO: ZTP: loading options config
577.427218] ztp.py[15456]: 2019-07-11 18:01:18 INFO: ZTP: Upgrading image
[ 577.427770] ztp.py[15456]: 2019-07-11 18:01:18 INFO: ZTP: Upgraded image localpath
is /var/tmp/junos-evo-install-ptx-chassis-x86-64-19.4EVO.iso
[ 577.483927] ztp.py[15456]: 2019-07-11 18:01:19 INFO: ZTP: Installing via CLI (/var/tmp/junos-
evo-install-ptx-chassis-x86-64-19.4-20190708.2-EVO.iso)
[ 577.484271] ztp.py[15456]: 2019-07-11 18:01:19 INFO: ZTP: Running: ['/usr/sbin/cli', '-c',
'show chassis hardware | display xml | match <name> | match "CB" | count']
[ 577.775918] ztp.py[15456]: 2019-07-11 18:01:19 INFO: ZTP: Dual-RE setup detected
[ 577.776130] ztp.py[15456]: 2019-07-11 18:01:19 INFO: ZTP: Checking for second RE
[ 577.776894] ztp.py[15456]: 2019-07-11 18:01:19 INFO: ZTP: Running: ['/usr/sbin/cli', '-c',
'show chassis hardware | display xml | match <name> | match "Routing Engine" | count']
[ 577.987278] ztp.py[15456]: 2019-07-11 18:01:19 INFO: Running: ['/usr/sbin/cli', '-c',
'request system software add /var/tmp/junos-evo-install-ptx-chassis-x86-64-19.4EVO.iso | display
xml']
[ 738.153925] ztp.py[15456]: 2019-07-11 18:03:59 INFO: ZTP: wait returns: 0
[ 738.154148] ztp.py[15456]: 2019-07-11 18:03:59 INFO: ZTP: Return Code: 0
[ 738.154281] ztp.py[15456]: 2019-07-11 18:03:59 INFO: ZTP: Upgraded image status is 0
[ 738.154749] ztp.py[15456]: 2019-07-11 18:03:59 INFO: ZTP: Upgrade succeeded Rebooting
[ 738.155372] ztp.py[15456]: 2019-07-11 18:03:5          Stopping Ethernet Bridge Filtering
Tables...
```

Meaning

The console shows the progress of ZTP.

Using the show dhcp client binding Command

IN THIS SECTION

 Purpose | 146

- [Action | 146](#)
- [Meaning | 146](#)

Purpose

Issue the `show dhcp client binding` command to display DHCP client binding information

NOTE: This command does not apply to Junos OS Evolved.

Action

Issue the `show dhcp client binding` command to display the IP address of the DHCP client, the hardware address of the DHCP client, number of seconds in which the DHCP client's IP address lease expires, state of the DHCP client IP address in the binding table, and the name of the interface that has active client bindings.

show dhcp client binding

```
user@device# show dhcp client binding
```

IP address	Hardware address	Expires	State	Interface
10.0.0.0	00:22:83:2a:db:dc	0	SELECTING	irb.0
10.6.6.13	00:22:83:2a:db:dd	49201	BOUND	vme.0
10.0.0.0	00:22:83:2a:db:df	0	SELECTING	xe-0/0/0.0
10.0.0.0	00:22:83:2a:db:e0	0	SELECTING	xe-0/0/1.0

Meaning

The output of this command shows that there is one client interface that is bound, and that there are three interfaces that are receiving DHCP offers from the DHCP server.

Using the show dhcpv6 client binding Command

IN THIS SECTION

- Purpose | 147
- Action | 147
- Meaning | 148

Purpose

Issue the show dhcpv6 client binding command to display DHCP client binding information

NOTE: This command does not apply to Junos OS Evolved.

Action

Issue the show dhcpv6 client binding command to display the IP address of the DHCPv6 client, the hardware address of the DHCPv6 client, number of seconds in which the DHCPv6 client's IP address lease expires, state of the DHCPv6 client IP address in the binding table, and the name of the interface that has active client bindings.

show dhcpv6 client binding

user@device# show dhcpv6 client binding						
IP/prefix	Expires	State	ClientType		Interface	Client
DUID						
2001:db8::10		57	SELECTING	STATEFUL	em0.0	
LL0x3-54:4b:8c:d3:a2:34						
2001:db8::10		46	SELECTING	STATEFUL	em2.0	
LL0x3-54:4b:8c:d3:a2:35						
2001:db8::10		38	SELECTING	STATEFUL	et-0/0/0:0.0	
LL0x3-54:4b:8c:d3:a2:3b						
2001:db8::10		530	BOUND	STATEFUL	et-0/0/0:1.0	
LL0x3-54:4b:8c:d3:a2:3c						

Meaning

The output of this command shows that there is one client interface that is bound, and that there are three interfaces that are receiving DHCPv6 offers from the DHCP server.

Using the show dhcp client statistics Command

IN THIS SECTION

Purpose | 148

Action | 148

Meaning | 149

Purpose

Issue the `show dhcp client statistics` command to display DHCP client statistics.

Action

Issue the `show dhcp client statistics` command to display DHCP client statistics, such as the number of packets dropped, and the number DHCP and BOOTP messages sent and received.

show dhcp client statistics

```
user@device# show dhcp client statistics
Packets dropped:
  Total          14
  Send error     14
Messages received:
  BOOTREPLY      5
  DHCPOFFER      1
  DHCPACK        4
  DHCPNAK        0
  DHCPFORCERENEW 0
Messages sent:
  BOOTREQUEST    6751
  DHCPDECLINE    0
  DHCPDISCOVER   6747
```

DHCPREQUEST	4
DHCPINFORM	0
DHCPRELEASE	0
DHCPRENEW	0
DHCPREBIND	0

Meaning

The output of this command displays how many packets were dropped with errors, the number of BOOTREPLY and DHCPOFFER messages that were received, and the number of BOOTREQUEST and DHCPREQUEST messages that were sent.

Using the show dhcpv6 client statistics Command

IN THIS SECTION

- Purpose | 149
- Action | 149
- Meaning | 150

Purpose

Issue the `show dhcpv6 client statistics` command to display DHCPv6 client statistics.

Action

Issue the `show dhcpv6 client statistics` command to display DHCPv6 client statistics, such as the number of packets dropped, and the number of DHCPv6 messages sent and received.

show dhcpv6 client statistics

```
user@device# show dhcpv6 client statistics
```

```
Dhcpv6 Packets dropped:
```

Total	20323
Bad Send	7580
Bad Options	12743

```
Messages received:
```

```

DHCPV6_ADVERTISE      13
DHCPV6_REPLY          109
DHCPV6_RECONFIGURE    0

```

Messages sent:

```

DHCPV6_DECLINE        0
DHCPV6_SOLICIT        879
DHCPV6_INFORMATION_REQUEST 0
DHCPV6_RELEASE        0
DHCPV6_REQUEST        9
DHCPV6_CONFIRM        0
DHCPV6_RENEW          61
DHCPV6_REBIND         41

```

Meaning

The output of this command displays how many packets were dropped with errors, and the number of DHCPV6 messages that were received and sent.

Release History Table

Release	Description
19.1-Evo	Starting in Junos OS Evolved Release 19.1R1, to monitor zero touch provisioning on Junos OS Evolved, use the show system ztp command.
12.2	Starting in Junos OS Release 12.2, you can use the console and operational commands to monitor Zero Touch Provisioning.

Release History Table

Release	Description
21.3R1-EVO	Starting in Junos OS Evolved Release 21.3R1, on PTX10001-36MR, PTX10003, PTX10004, PTX10008, and PTX10016 devices, ZTP now supports DHCP options 61 and 77. DHCP option 61 is used to specify the chassis serial number, and DHCP option 77 is used to specify the make, model, and software version of the chassis.
21.2R1-EVO	Starting in Junos OS Evolved Release 21.2R1 on PTX10008 devices, Zero Touch Provisioning (ZTP) dynamically detects the port speed of WAN interfaces and uses this information to create ZTP server ports with the same speed.

21.2R1-EVO	Starting in Junos OS Evolved Release 21.2R1, QFX5700 devices support the ability for either WAN interfaces or management interfaces to automatically download and install the appropriate software and the configuration file on your device during the ZTP bootstrap process.
21.2R1	Starting in Junos OS Release 21.2R1 on QFX10002 devices, Zero Touch Provisioning (ZTP) dynamically detects the port speed of WAN interfaces and uses this information to create ZTP server ports with the same speed.
21.2R1	Starting in Junos OS Release 21.2R1, on EX2300-C, EX2300-MP, EX4300, EX4300-MP, EX4300-VC, EX4400-24MP, EX4400-48MP, EX4600-VC, EX4650, and EX4650-48Y-VC devices, during the bootstrapping process, the phone-home client can access the redirect server through a proxy server. The DHCP server uses DHCP option 43 suboption 8 to deliver the details of IPv4 and/or IPv6 proxy servers to the phone-home client. The DHCP daemon running on the target switch learns about the proxy servers in the initial DHCP cycle and then populates either the <code>phc_vendor_specific_info.xml</code> or the <code>phc_v6_vendor-specific_info.xml</code> files located in the <code>/var/etc/</code> directory with the vendor-specific information.
21.2R1	Starting in Junos OS Release 21.2R1, on EX2300-C, EX2300-MP, EX4300, EX4300-MP, EX4300-VC, EX4400-24MP, EX4400-48MP, EX4600-VC, EX4650, and EX4650-48Y-VC devices, you can use a DHCPv6 client and ZTP to provision a switch. During the bootstrap process, the device first uses the DHCPv4 client to request for information regarding the image and configuration file from the DHCP server. The device checks the DHCPv4 bindings sequentially. If there is a failure with one of the DHCPv4 bindings, the device continues to check for bindings until provisioning is successful. However, if there are no DHCPv4 bindings, the device checks for DHCPv6 bindings and follows the same process as for DHCPv4 until the device is provisioned successfully. Both DHCPv4 and DHCPv6 clients are included as part of the default configuration on the device. The DHCP server uses DHCPv6 options 59 and 17 and applicable suboptions to exchange ZTP-related information between itself and the DHCP client.
21.1R1	Starting in Junos OS Release 21.1R1, on EX2300, EX2300-VC, EX3400, EX3400-VC, EX4400-24T, EX4400-48F, EX4400-48T, and EX4600 devices, when the phone-home client receives information regarding the HTTP proxy server via DHCP option 43 suboption 8, it will create an HTTPS transparent tunnel with the proxy server. Once the tunnel is established, the phone-home client uses the tunnel as a proxy for the phone-home server or redirect server. The phone-home client downloads the software image and configuration file through the tunnel onto the device. Once bootstrapping is complete, the device reboots and the tunnel quits.
21.1R1	Starting in Junos OS Release 21.1R1, on EX2300, EX2300-VC, EX3400, EX3400-VC, EX4400-24T, EX4400-48F, EX4400-48T, and EX4600 devices, during the bootstrapping process, the phone-home client can access the redirect server through a proxy server. The DHCP server uses DHCP option 43 suboption 8 to deliver the details of IPv4 and/or IPv6 proxy servers to the phone-home client. The DHCP daemon running on the target switch learns about the proxy servers in the initial DHCP cycle and then populates either the <code>phc_vendor_specific_info.xml</code> or the <code>phc_v6_vendor-specific_info.xml</code> files located in the <code>/var/etc/</code> directory with the vendor-specific information.

20.4R1-EVO	Starting in Junos OS Evolved Release 20.4R1, PTX10004 devices support automation of the device configuration and software upgrade over the management interface of Routing Engine 0 (RE0).
20.4R1-EVO	Starting in Junos OS Evolved Release 20.4R1, ACX5448 and QFX5120-48YM devices support the ability for either WAN interfaces or management interfaces to automatically download and install the appropriate software and the configuration file on your device during the ZTP bootstrap process.
20.4R1	Starting in Junos OS Release 20.4R1 on the MX-Series, EX3400, EX4300, QFX5100, and QFX5200 devices, ZTP supports the DHCPv6 client. During the bootstrap process, the device first uses the DHCPv4 client to request for information regarding image and configuration file from the DHCP server. The device checks the DHCPv4 bindings sequentially. If there is a failure with one of the DHCPv4 bindings, the device will continue to check for bindings until provisioning is successful. If there are no DHCPv4 bindings, however, the device will check for DHCPv6 bindings and follow the same process as for DHCPv4 until the device can be provisioned successfully. The DHCP server uses DHCPv6 options 59 and 17 and applicable sub-options to exchange ZTP-related information between itself and the DHCP client.
20.4R1	Starting in Junos OS Release 20.4R1 on the EX4600, EX4650, EX9200 with RE-S-EX9200-2X00X6, QFX5110, QFX5200, QFX5210, QFX5120-32C, and QFX5120-48Y devices, you can use either the legacy DHCP-options-based ZTP or the phone-home client (PHC) to provision software for the switch. When the switch boots up, if there are DHCP options that have been received from the DHCP server for ZTP, ZTP resumes. If DHCP options are not present, PHC is attempted. PHC enables the switch to securely obtain bootstrapping data, such as a configuration or software image, with no user intervention other than having to physically connect the switch to the network. When the switch first boots up, PHC connects to a redirect server, which redirects to a phone home server to obtain the configuration or software image.
20.2R1-S1	Starting in Junos OS Release 20.2R1-S1 on the MX-Series, EX3400, EX4300, QFX5100, and QFX5200 devices, ZTP supports the DHCPv6 client. During the bootstrap process, the device first uses the DHCPv4 client to request for information regarding image and configuration file from the DHCP server. The device checks the DHCPv4 bindings sequentially. If there is a failure with one of the DHCPv4 bindings, the device will continue to check for bindings until provisioning is successful. If there are no DHCPv4 bindings, however, the device will check for DHCPv6 bindings and follow the same process as for DHCPv4 until the device can be provisioned successfully. The DHCP server uses DHCPv6 options 59 and 17 and applicable sub-options to exchange ZTP-related information between itself and the DHCP client.
20.2R1	Starting in Junos OS Release 20.2R1 on SRX300, SRX320, SRX340, SRX345, SRX550 HM, and SRX1500 devices, you can use Zero Touch Provisioning with DHCP options or the phone-home client to provision your device.

20.1R1-EVO	Starting in Junos OS Evolved Release 20.1R1 on PTX10003 devices, Zero Touch Provisioning (ZTP) dynamically detects the port speed of WAN interfaces and uses this information to create ZTP server ports with the same speed.
20.1R1-EVO	Starting in Junos OS Evolved Release 20.1R1, PTX10008 devices support automation of the device configuration and software upgrade over the management interface of Routing Engine 0 (RE0).
19.4R1	Starting in Junos OS Release 19.4R1, ZTP can automate the provisioning of the device configuration and software image on Juniper Route Reflector (JRR). ZTP supports self image upgrades and automatic configuration updates using ZTP DHCP options. In this release, ZTP supports revenue ports em2 thru em9, in addition to management port em0 which is supported in Junos OS Releases before 19.4R1.
19.3R1-Evo	Starting in Junos OS Evolved Release 19.3R1, on QFX5220-128C device, in Zero Touch Provisioning (ZTP), you can use either WAN interfaces or management interfaces, to automatically download and install the appropriate software and the configuration file on your device during the bootstrap process.
19.3R1	Starting in Junos OS Release 19.3R1, you can use either WAN interfaces or management interfaces, to automatically download and install the appropriate software and the configuration file on your router during the ZTP bootstrap process.
19.2R1	Starting in Junos OS Release 19.2R1, ZTP can automate the provisioning of the device configuration and software image on management interface emo for ACX5448 switches.
19.1-Evo	Starting in Junos OS Evolved Release 19.1R1, ZTP can automate the provisioning of the device configuration and software image on the management interface for QFX5220 and PTX10003 devices.
19.1-Evo	Starting in Junos OS Evolved Release 19.1R1, to monitor zero touch provisioning on Junos OS Evolved, use the show system ztp command.
18.3R1	Starting in Junos OS Release 18.3R1, ZTP, which automates the provisioning of the device configuration and software image with minimal manual intervention, is supported on MX Series VM hosts.
18.2R1	Starting in Junos OS Release 18.2R1, ZTP can automate the provisioning of the device configuration and software image on VM host platforms that use PTX5000, PTX3000, PTX10008, PTX10016, PTX10002-60C routers.
18.2R1	Starting in Junos OS Release 18.2R1, ZTP can automate the provisioning of the device configuration and software image on VM host platforms that use QFX10008 and QFX10016 switches.

18.1R1	Starting in Junos OS Release 18.1R1, ZTP can automate the provisioning of the device configuration and software image on VM host platforms that use QFX10002-60C switches.
17.2R1	Starting in Junos OS Release 17.2R1, ZTP can automate the provisioning of the device configuration and software image on VM host platforms that use PTX1000 routers.
16.1R1	Starting in Junos OS Release 16.1R1, you can provision supported devices by using either a script to be executed or a configuration file to be loaded
12.2	Starting in Junos OS Release 12.2, you can use the console and operational commands to monitor Zero Touch Provisioning.

Zero Touch Provisioning DHCP Options

IN THIS CHAPTER

- [Zero Touch Provisioning DHCP Options for Junos OS Evolved | 155](#)

Zero Touch Provisioning DHCP Options for Junos OS Evolved

IN THIS SECTION

- [IPv4 DHCP Options | 156](#)
- [IPv6 DHCP Options | 157](#)

With Zero Touch Provisioning (ZTP), you can provision Juniper Networks devices in your network automatically, with minimal manual intervention. You can use either the management interface (re0:mgmt-0 for all devices; additionally re0:mgmt-1 for PTX10003) or WAN interface ports, depending on your device, to connect to the network. You use a Dynamic Host Configuration Protocol (DHCP) server on the network to control provisioning. You configure DHCP options for provisioning in the DHCP configuration file [dhcpd.conf (for IPv4 addressing) or dhcpd6.conf (for IPv6 addressing).]

When you physically connect a device to the network and boot the device with a factory-default configuration, ZTP starts and detects that the device has a factory-default configuration. ZTP then uses the DHCP client on the device to request provisioning information from the DHCP server. The DHCP server reads the parameters from the DHCP configuration file and sends the provisioning information to the device. ZTP uses this information to install the configured version of the Junos OS Evolved software image and the configuration file. The configuration file installed can be either a Junos OS Evolved configuration file or a script. With scripts, you can create device-specific configuration files and perform HTTP request operations to web servers to download specific configuration files or software images. After a reboot, ZTP applies the configuration to the device. You can monitor progress by issuing the `show system ztp operational mode` command.

DHCP option parameters are used in priority order if the same parameter is specified in two places in the DHCP configuration file.

IPv4 DHCP Options

The base DHCP packet contains the IPv4 address of the management or WAN interface.

For DHCP option 43 (vendor-specific options), you can configure the following parameters in the DHCP configuration file (`dhcpd.conf`) on the DHCP server:

- `image-file-name` (Junos OS Evolved software package name)
- `configuration-file-name` (Junos OS Evolved configuration file name)
- `image-file-type` (symbolic link)
- `transfer-type` (for example, FTP, HTTP, HTTPS, TFTP)
- `ftp-ip` (IP address of the FTP server)
- `alt-image` (If you do not configure the `image-file-name` parameter, ZTP uses the file name specified for the `alt-image` parameter.)

DHCP options sent by ZTP to the DHCP server, which are derived from the hardware information encoded on the device:

- Option 60 (vendor class identifier)—`make-serial_num-sw_version` (For example, `Juniper-serial-number-software-version`; uses the character - as a delimiter.)
- Option 61 (DHCP client identifier)—serial number
- Option 77 (user class)—`make:model:sw_version` (For example, `Juniper:qfx5220-128c-sw-version`; uses the character : as a delimiter.)

DHCP options received from the DHCP server, which you configure in the DHCP configuration file (`dhcpd.conf`) on the DHCP server:

- Option 1—subnet mask
- Option 3—device's subnet address
- Option 7—log server
- Option 12—host name
- Option 42—NTP server arguments
- Option 150—FTP server IP address

- Option 66—TFTP server or FTP server IP address
- Option 67—URL for the bootfile name

Order of Priority for Configuration and Script Management

In general, for configuring location, port, and transfer method, option 67 is primary and option 43 is secondary, except if the transfer type is HTTP. If the transfer type is HTTP, the port chosen for HTTP is configured from the information specified with option 43. If option 43 does not specify an HTTP port, the port is configured from the information specified with option 67.

Management Interface Address Configuration

The management interface address is configured based on the value for `ip_address` in the DHCP packet. The management interface address can be configured as one of the following:

- A fixed address for a device in the device-specific configuration, matched on the device's MAC address.
- An address from the specified subnet pool specified by the `range` parameter.

Order of Priority for Transfer Address

ZTP prefers to choose the transfer address from option 150. If not specified in option 150, ZTP chooses the address specified in option 66 instead. If not specified in either of these options, ZTP chooses the address specified for the `ftp-ip` parameter in option 43.

Order of Priority for Transfer Type

ZTP prefers to choose the transfer type from option 43. If not specified in option 43, ZTP uses the transfer type in option 67.

Order of Priority for Port Number

ZTP uses the HTTP or HTTPS port number from the option 43 `image-file-name` parameter for the image type and from the `alt-image-file-name` parameter for the alternate image type. For the `configuration-file-name` parameter, ZTP prefers to read the port number from the configuration file argument in option 43. However, if not specified in option 43, ZTP reads the port number from the image URL in option 67.

IPv6 DHCP Options

The base DHCP packet contains both the IPv6 address of the management or WAN interface and the IPv6 prefix length.

For DHCP option 17 (vendor-specific options), you can configure the following parameters in the DHCP configuration file (`dhcpd6.conf`) on the DHCP server:

- image-file (Junos OS Evolved software package name, URL, or path)
- configuration-file (Junos OS Evolved configuration file name, URL, or path)
- image-file-type (symbolic link)
- transfer-type (for example, FTP, HTTP, HTTPS, TFTP)
- alt-image (If you do not configure the image-file-name parameter, ZTP uses the file name specified for the alt-image parameter.)
- port-number (configuration port number)

DHCP options sent by ZTP to the DHCP server, which are derived from the hardware information encoded on the device: `dhcp6.vendor-class-identifier` (For example, Juniper: *platform_type:serial_num:sw_version*, uses the character : as a delimiter.)

DHCP options received from the DHCP server, which you configure in the DHCP configuration file (`dhcpd6.conf`) on the DHCP server:

- Option 59—`bootfile-url` parameter. This parameter can be configured in one of two formats:
 - `<TransferMode>://<FTP Server IP>.<PortNumber>/<ImagePath/ConfigPath/ScriptPath>`
 - `<TransferMode>://<FTP Server IP>`
- IPv6 address—`IP6ADDR`
- IPv6 prefix length—`IP6PREFIXLEN`

Order of Priority for Configuration and Script Management

ZTP prefers to use the fully-formed URL specified in option 17; otherwise it uses the other configuration and script parameters specified in option 17. If these parameters are not specified in option 17, ZTP uses the URL specified in option 59.

Management Interface Address Configuration

The management interface address is configured based on the value for `ip6_address` in the DHCP packet.

Order of Priority for Transfer Address

ZTP prefers to use the vendor-specific URL from option 17. If not specified in option 17, ZTP uses the URL specified with the `bootfile-url` parameter in option 59.

Order of Priority for Transfer Type

ZTP prefers to use the transfer type from option 17. If not specified there, ZTP uses the transfer type from the argument for the `bootfile-url` parameter in option 59.

Order of Priority for Port Number

ZTP prefers to read the port number from the `portnum` parameter in option 17. If not specified there, ZTP uses the port number from the argument for the `bootfile-url` parameter in option 59.

RELATED DOCUMENTATION

| [Zero Touch Provisioning](#) | 105



Configuration Statements and Operational Commands

Configuration Statements | 161

Operational Commands | 166

CHAPTER 15

Configuration Statements

IN THIS CHAPTER

- [auto-sw-sync](#) | 161
- [license](#) | 163

auto-sw-sync

IN THIS SECTION

- [Syntax](#) | 161
- [Hierarchy Level](#) | 161
- [Description](#) | 162
- [Default](#) | 162
- [Options](#) | 162
- [Required Privilege Level](#) | 162
- [Release Information](#) | 163

Syntax

```
auto-sw-sync node node-name (disable | enable);
```

Hierarchy Level

```
[edit system]
```


Description

(Junos OS Evolved only) When you add a new Routing Engine (RE) to the device and the new RE has a different software version than the rest of the system, by default the RE is kept out of the system. If you want a new RE's software and configuration to be automatically upgraded and synchronized with that of the cluster, configure this statement. Once configured for the device, if an RE fails and you replace the RE, the software and the configuration from the primary RE in the system automatically installs on the new RE.

When you configure this statement, the primary Routing Engine of the system copies over all the images (software and configuration) to the new Routing Engine and reboots the new Routing Engine so it runs the same software version and configuration as the primary Routing Engine. Each software image also contains the configuration running when the software image was last active.

When the chassis first comes up, the Routing Engines elect a "primary" node based on several factors, including which Routing Engine was "primary" last, which Routing Engine is the current hardware primary RE, and the slot position (0 versus 1).

Default

Disabled: When you insert a new Routing Engine with a different software version than the rest of the system and you have not already configured this statement on the system, the Routing Engine is kept out of the system. Thereafter, the newly-inserted RE does not respond to any software event and remains in its original software version.

Options

disable | enable (Required) Specify whether to disable or enable automatic software synchronization from the primary node to the new Routing Engine.

- Default: Disable

node *node-name* Specify the node to be synchronized (fpc0 | re0 | re1). Deprecated as of Junos OS Evolved Release 20.4R2.

Required Privilege Level

system—To view this statement in the configuration.

system-control—To add this statement to the configuration.

Release Information

Statement introduced in Junos OS Evolved Release 20.2R1.

node option deprecated as of Junos OS Evolved Release 20.4R2.

RELATED DOCUMENTATION

[Node Software Synchronization for Dual-RE Systems | 18](#)

[Replace a Routing Engine in a Dual-RE System | 67](#)

license

IN THIS SECTION

- [Syntax | 163](#)
- [Hierarchy Level | 164](#)
- [Description | 164](#)
- [Options | 164](#)
- [Required Privilege Level | 165](#)
- [Release Information | 165](#)

Syntax

```
license {  
  autoupdate {  
    url url <password password>;  
  }  
  keys {  
    key key  
  }  
  renew {  
    before-expiration number;  
    interval interval-hours;
```

```

    }
    traceoptions {
        file {
            filename;
            files number;
            match regular-expression;
            size maximum-file-size;
            (world-readable | no-world-readable);
        }
        flag flag;
        no-remote-trace;
    }
}

```

Hierarchy Level

[edit system]

Description

Specify license information for the device.

Options

autoupdate	Autoupdate license keys from license servers.
before-expiration <i>number</i>	License renewal lead time before expiration, in days. <ul style="list-style-type: none"> • Range: 0 through 60 days
interval <i>interval-hours</i>	License checking interval, in hours. <ul style="list-style-type: none"> • Range: 1 through 336 hours
keys key <i>key</i>	Configure one or more license keys. For example,

```

[edit]
user@device# set system license keys key "key_1"
user@device# set system license keys key "key_2"
user@device# set system license keys key "key_3"

```

```
user@device# set system license keys key "key_4"  
user@device# commit  
commit complete
```

renew License renewal lead time and checking interval.

url URL of a license server.

The remaining statements are explained separately. See [CLI Explorer](#).

Required Privilege Level

system—To view this statement in the configuration.

system-control—To add this statement to the configuration.

Release Information

Statement introduced in Junos OS Release 8.5.

Options **keys** introduced in Junos OS Release 14.1X53-D10.

Operational Commands

IN THIS CHAPTER

- request node halt (Junos OS Evolved) | 167
- request node (offline | online) (Junos OS Evolved) | 170
- request node power-off (Junos OS Evolved) | 172
- request node power-on (Junos OS Evolved) | 174
- request node reboot (re0 | re1) (Junos OS Evolved) | 176
- request system application (Junos OS Evolved) | 178
- request system configuration rescue delete | 179
- request system configuration rescue save | 181
- request system firmware upgrade | 182
- request system snapshot (Junos OS Evolved) | 186
- request system software add (Junos OS Evolved) | 188
- request system software delete (Junos OS Evolved) | 200
- request system software rollback (Junos OS Evolved) | 204
- request system software sync | 207
- request system software validate (Junos OS Evolved) | 212
- request system storage cleanup (Junos OS Evolved) | 214
- request system zeroize (Junos OS Evolved) | 225
- restart (Junos OS Evolved) | 227
- rollback | 229
- show system applications (Junos OS Evolved) | 230
- show system core dumps (Junos OS Evolved) | 239
- show system errors | 241
- show system errors active | 246
- show system errors count | 253
- show system errors error-id | 255
- show system errors fru | 258

- [show system errors inactive | 264](#)
- [show system errors history | 272](#)
- [show system rollback | 275](#)
- [show system snapshot \(Junos OS Evolved\) | 277](#)
- [show system software add-restart \(Junos OS Evolved\) | 279](#)
- [show system software list | 282](#)
- [show system ztp | 286](#)
- [show version \(Junos OS Evolved\) | 291](#)

request node halt (Junos OS Evolved)

IN THIS SECTION

- [Syntax | 167](#)
- [Description | 167](#)
- [Options | 168](#)
- [Required Privilege Level | 168](#)
- [Sample Output | 168](#)
- [Release Information | 169](#)

Syntax

```
request node halt node-name
<(at time | in minutes)>
<message message>
```

Description

Use this command to halt a Routing Engine (RE). Halt instructs the hardware to stop all CPU functions but leave the node in a powered-on, standby state. To un-halt the node, do one of the following:

- Issue the request `chassis cb slot slot-number` online operational mode command from the primary RE.
- Log in to the console port for that node and press any key to reboot the node.

NOTE: We do not recommend leaving a node halted for a long period of time, because the node is not available as a backup in case something happens to the primary RE.

Options

- node-name*** Specify the Routing Engine node to halt. You cannot halt the primary RE.
- (at *time* | in *minutes*)** (Optional) Specify when the action should occur, either in time, in *hh:mm* format, or in number of minutes.
- message *message*** (Optional) Message to display to all users.

Required Privilege Level

view

Sample Output

request node halt re1

On the primary RE:

```
user@host-re0> request node halt re1
Halt the node ? [yes,no] (no) yes
*** System shutdown message from user@host-re0***

Shutdown at Thu Apr 29 16:31:01 2021
.
{master}
user@host-re0>
```

When logged into the console port on the node during the halt:

```
[...output truncated, processes stopped...]
Shutdown target is 'halt'
Checking on root FS daemon .....Done
Cleaning up root FS daemon...done
/sbin/bom.sh: line 1242: /tmp/mp_aid: Read-only file system
/sbin/bom.sh: line 1793: /tmp/sku_mode_log: Read-only file system
/sbin/bom.sh: line 1242: /tmp/mp_aid: Read-only file system
/sbin/bom.sh: line 1793: /tmp/sku_mode_log: Read-only file system
Clearing linux_up bit
warning - 'debugfs' was not mounted
Deactivating swap...
Putting SSD devices in standby mode...

/dev/sdb:
    issuing standby command

/dev/sdc:
    issuing standby command
SG_IO: bad/missing sense data, sb[]:  70 00 05 00 00 00 00 14 00 00 00 00 20 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00

/dev/sda:
    issuing standby command
The operating system has halted.

Please press any key to reboot...
```

Release Information

Command introduced in Junos OS Evolved Release 18.3R1.

RELATED DOCUMENTATION

request node (offline / online) (Junos OS Evolved)

[request node power-off \(Junos OS Evolved\) | 172](#)

[request node power-on \(Junos OS Evolved\) | 174](#)

request node reboot (re0 / re1) (Junos OS Evolved)

request node (offline | online) (Junos OS Evolved)

IN THIS SECTION

- [Syntax | 170](#)
- [Description | 170](#)
- [Options | 171](#)
- [Required Privilege Level | 171](#)
- [Sample Output | 171](#)
- [Release Information | 171](#)

Syntax

```
request node (offline | online) node-name
```

Description

Use this command to change the node status to offline or online.

- To add a node to the system, set the node status to online.
- To remove a node from the system, set the node status to offline.

You can use the `offline` option to stop all applications on the node and move them to other nodes if applicable. The node is not allowed to join the system until the node is brought online using the `request node online` command.

NOTE: We do not recommend leaving the secondary RE offline for a long period of time, because the secondary RE is not available as a backup in case something happens to the primary RE.

When you use the `request node offline` command for FPC nodes, the node is powered off. When used for an RE node, the node just reboots.

Options

<i>node-name</i>	Specify the node name. You cannot take the primary RE (re0) offline. The backup or secondary node is re1. For a device that supports only one RE, you can only specify FPC node names in this command.
(offline online)	Change the node status to online or offline. When you specify the online option, the node reboots, which can take a few minutes.

Required Privilege Level

view

Sample Output

request node offline re1

```
user@host-re0> request node offline re1
This may take a few minutes. Offline the node ? [yes,no] (no) yes

Node re1 is set to be offline
```

request node online re1

```
user@host-re0> request node online re1
This may take a few minutes. Online the node ? [yes,no] (no) yes

Node re1 is set to be online
```

Release Information

Statement introduced in Junos OS Evolved Release 18.3R1.

RELATED DOCUMENTATION

[request node halt \(Junos OS Evolved\) | 167](#)

[request node power-off \(Junos OS Evolved\) | 172](#)

[request node power-on \(Junos OS Evolved\) | 174](#)

request node reboot (re0 / re1) (Junos OS Evolved)

[request system application \(Junos OS Evolved\) | 178](#)

request node power-off (Junos OS Evolved)

IN THIS SECTION

- [Syntax | 172](#)
- [Description | 172](#)
- [Options | 173](#)
- [Required Privilege Level | 173](#)
- [Sample Output | 173](#)
- [Release Information | 174](#)

Syntax

```
request node power-off node-name  
<(at time | in minutes)>  
<message message>
```

Description

Use this command to power off a Routing Engine, stopping the CPU and commencing a complete shutdown.

NOTE: We do not recommend leaving a node powered off for a long period of time, because the node is not available as a backup in case something happens to the primary RE.

Options

- node-name*** Specify the Routing Engine node to shut down. You cannot shut down the primary RE.
- (at time | in minutes)*** (Optional) Specify when the action should occur, either in time, in *hh:mm* format, or in number of minutes.
- message message*** (Optional) Message to display to all users.

Required Privilege Level

view

Sample Output

request node power-off re1

On the primary RE:

```
user@host-re0> request node power-off re1
Power-off the node ? [yes,no] (no) yes

*** System shutdown message from user@host-re0***

Shutdown at Fri Apr 30 10:47:01 2021
.

{master}
user@host-re0>
```

When logged in to the console port on the node:

```
[...output truncated, stopping processes...]

Shutdown target is 'poweroff'
Checking on root FS daemon .....Done
Cleaning up root FS daemon...done
```

```
Powering off.
[ 285.750267] reboot: Power down
```

Release Information

Command introduced in Junos OS Evolved Release 18.3R1.

RELATED DOCUMENTATION

[request node halt \(Junos OS Evolved\) | 167](#)

request node (offline | online) (Junos OS Evolved)

[request node power-on \(Junos OS Evolved\) | 174](#)

request node reboot (re0 | re1) (Junos OS Evolved)

request node power-on (Junos OS Evolved)

IN THIS SECTION

- [Syntax | 174](#)
- [Description | 175](#)
- [Options | 175](#)
- [Required Privilege Level | 175](#)
- [Sample Output | 175](#)
- [Release Information | 175](#)

Syntax

```
request node power-on node-name
<(at time | in minutes)>
<message message>
```

Description

Use this command to power on a Routing Engine. The node reboots, which can take a few minutes.

Options

- node-name*** Specify the Routing Engine node to power on.
- (at time | in minutes)*** (Optional) Specify when the action should occur, either in time, in *hh:mm* format, or in number of minutes.
- message message*** (Optional) Message to display to all users.

Required Privilege Level

view

Sample Output

request node power-on re1

```
user@host-re0> request node power-on re1
Power-on the node ? [yes,no] (no) yes
OK
```

Release Information

Command introduced in Junos OS Evolved Release 18.3R1.

RELATED DOCUMENTATION

[request node halt \(Junos OS Evolved\) | 167](#)

[request node \(offline | online\) \(Junos OS Evolved\)](#)

[request node power-off \(Junos OS Evolved\) | 172](#)

[request node reboot \(re0 | re1\) \(Junos OS Evolved\)](#)

request node reboot (re0 | re1) (Junos OS Evolved)

IN THIS SECTION

- [Syntax | 176](#)
- [Description | 176](#)
- [Options | 176](#)
- [Required Privilege Level | 177](#)
- [Sample Output | 177](#)
- [Release Information | 177](#)

Syntax

```
request node reboot (re0 | re1)
<(at time | in minutes)>
<(disk1 | disk2)>
<message message>
<usb>
```

Description

Use this command to reboot one of the Routing Engines in a system. You cannot reboot the primary RE with this command. To reboot all nodes at once, use the `request system reboot` command.

Options

(at <i>time</i> in <i>minutes</i>)	(Optional) Specify when the reboot is performed, either at a particular time, in <i>hh:mm</i> format, or in number of minutes.
(disk1 disk2)	(Optional) Boot from the primary solid-state drive (SSD) (disk1) or the secondary SSD (disk2). Default: disk1
message <i>message</i>	(Optional) Message to display to all users.

(re0 re1)	Specify which Routing Engine to reboot. You cannot reboot the primary RE using this command.
usb	(Optional) Boot from the USB device.

Required Privilege Level

view

Sample Output

request node reboot re1

On the primary RE:

```
user@host-re0> request node reboot re1
This may affect traffic in system. Proceed ? [yes,no] (no) yes

*** System shutdown message from user@host-re0***

Shutdown at Fri Apr 30 10:47:01 2021
.
```

Release Information

Command introduced in Junos OS Evolved Release 18.3R1.

RELATED DOCUMENTATION

[request node halt \(Junos OS Evolved\) | 167](#)

[request node \(offline | online\) \(Junos OS Evolved\)](#)

[request node power-off \(Junos OS Evolved\) | 172](#)

[request node power-on \(Junos OS Evolved\) | 174](#)

[request system application \(Junos OS Evolved\) | 178](#)

request system application (Junos OS Evolved)

IN THIS SECTION

- [Syntax | 178](#)
- [Description | 178](#)
- [Options | 178](#)
- [Required Privilege Level | 178](#)
- [Sample Output | 179](#)
- [Release Information | 179](#)

Syntax

```
request system application app application-name node node-name restart
```

Description

Use this command to stop and then start (restart) an application on the specified node. Use the `show system applications` command to verify if an application is started or stopped.

Options

- | | |
|--|---|
| <code>app <i>application-name</i></code> | Specify the application you want started or stopped. |
| <code>node <i>node-name</i></code> | Specify the name of the node on which to start or stop the application. |
| <code>restart</code> | Restart the application. |

Required Privilege Level

view

Sample Output

request system application app application-name node node-name restart

```
user@host> request system application app cmd node fpc0 restart
This may affect traffic in the system. Proceed ? [yes,no] (no) yes

App cmd on node fpc0 restart request is submitted
```

Release Information

Statement introduced in Junos OS Evolved Release 18.3R1.

RELATED DOCUMENTATION

[request node halt \(Junos OS Evolved\) | 167](#)

request node (offline / online) (Junos OS Evolved)

[request node power-off \(Junos OS Evolved\) | 172](#)

[request node power-on \(Junos OS Evolved\) | 174](#)

request node reboot (re0 / re1) (Junos OS Evolved)

[show system applications \(Junos OS Evolved\) | 230](#)

request system configuration rescue delete

IN THIS SECTION

- [Syntax | 180](#)
- [Description | 180](#)
- [Options | 180](#)
- [Required Privilege Level | 180](#)
- [Output Fields | 180](#)
- [Sample Output | 180](#)

Syntax

```
request system configuration rescue delete
```

Description

Delete an existing rescue configuration.

NOTE: The [edit system configuration] hierarchy is not available on QFabric systems.

Options

This command has no options.

Required Privilege Level

maintenance

Output Fields

This command produces no output.

Sample Output

```
request system configuration rescue delete
```

```
user@host> request system configuration rescue delete
```

Release Information

Command introduced before Junos OS Release 7.4.

Command introduced in Junos OS Evolved Release 20.4R2.

request system configuration rescue save

IN THIS SECTION

- [Syntax | 181](#)
- [Description | 181](#)
- [Options | 181](#)
- [Required Privilege Level | 182](#)
- [Output Fields | 182](#)
- [Sample Output | 182](#)
- [Release Information | 182](#)

Syntax

```
request system configuration rescue save
```

Description

Save the most recently committed configuration as the rescue configuration so that you can return to it at any time by using the `rollback` command. If saved on a device with redundant REs, the rescue configuration file is saved on both REs.

NOTE: The `[edit system configuration]` hierarchy is not available on QFabric systems.

Options

This command has no options.

Required Privilege Level

maintenance

Output Fields

This command produces no output.

Sample Output

request system configuration rescue save

```
user@host> request system configuration rescue save
```

Release Information

Command introduced before Junos OS Release 7.4.

Command introduced in Junos OS Evolved Release 20.4R2.

request system firmware upgrade

IN THIS SECTION

- [Syntax | 183](#)
- [Description | 183](#)
- [Options | 183](#)
- [Required Privilege Level | 184](#)
- [Output Fields | 184](#)
- [Sample Output | 184](#)
- [Release Information | 185](#)

Syntax

```
request system firmware upgrade
<cb>
<fpc>
<psm>
<re>
<vcpu>
<optics [fpc-slot fpc-slot-number | pic-slot pic-slot-number | port port-number]>
<pem>
```

Description

Use this command to upgrade firmware and optics module on a system running either Junos OS or Junos OS Evolved.

Options

cb (Junos OS Evolved only, for ACX7100 Series routers) Upgrade baseboard FPGA.

- **fancpld**—(Optional) Upgrade fanboard CPLD.
- **optics**—(Optional) Upgrade optics CPLD.

fpc Upgrade FPC ROM monitor.

- **bcm-pfe**—(Optional) Upgrade BCM PFE chip.
- **slot *slot-number***—(Optional) Upgrade a particular FPC slot.

pic (Junos OS only) Upgrade PIC firmware.

pem Upgrade PEM firmware.

psm Upgrade power supply module firmware.

- **slot *slot-number***—(Optional) Upgrade a particular power supply module.

re Upgrade baseboard BIOS/FPGA. There is an active BIOS image and a backup BIOS image.

- **bios**—(Optional) Upgrade BIOS.

- `fpga`—(Optional) Upgrade baseboard FPGA.
- `i210`—(Optional) Upgrade baseboard i210 GbE NIC.
- `i40nvme`—(Optional) Upgrade baseboard i40.

Starting in Junos OS Release 19.3R1, you can upgrade the i40e NVM firmware on routers with VM Host support.

- `ssd`—(Optional) Upgrade Routing Engine solid-state drive (SSD) firmware.
 - `disk1`—Upgrade SSD disk1 firmware.
 - `disk2`—Upgrade SSD disk2 firmware.

Starting in Junos OS Release 17.2R1, you can upgrade the SSD firmware on routers with the VM Host support.

- `xmcfpga`—(Optional) Upgrade XMC FPGA.

`vcpu`—Upgrade VCPU ROM monitor.

`optics`—Upgrade optics firmware.

- `fpc-slot` *fpc-slot-number*—Upgrade optics firmware for a specific FPC slot.
- `pic-slot` *pic-slot-number*—Upgrade optics firmware for a specific PIC slot.
- `port` *port-number*—Upgrade optics firmware for a specific port.

Required Privilege Level

maintenance

Output Fields

When you enter this command, you are provided feedback on the status of your request.

Sample Output

request system firmware upgrade

```
user@host> request system firmware upgrade re bios
```

Part	Type	Tag	Current version	Available version	Status

```

Routing Engine 0 RE BIOS      0  1.5      1.9      OK
Routing Engine 0 RE BIOS Backup 1  1.7      1.9      OK
Perform indicated firmware upgrade ? [yes,no] (no) yes
user@host> request system firmware upgrade re bios backup
Part          Type          Tag Current  Available Status
                        version version
Routing Engine 0 RE BIOS      0  1.5      1.9      OK
Routing Engine 0 RE BIOS Backup 1  1.7      1.9      OK
Perform indicated firmware upgrade ? [yes,no] (no) yes

user@host> request system firmware upgrade re ssd disk1
Part   Type   Tag                Current  Available  Status
                        version  version
Routing Engine 0 RE SSD1    4      12028    12029     OK
Perform indicated firmware upgrade ? [yes,no] (no) yes

Firmware upgrade initiated, use "show system firmware" to monitor status.

user@host> request system firmware upgrade pem slot 0
...
...
Firmware upgrade initiated, use "show system firmware" to monitor status.

user@host> request system firmware upgrade optics fpc-slot 0
...
...
Firmware optics upgrade initiated, use "show system firmware" to monitor status.

```

Release Information

Command introduced in Junos OS Release 10.2.

cb option added in Junos OS Evolved Releases 21.1R2 and 21.2R1.

pem option introduced in Junos OS Release 21.2R1.

optics option introduced in Junos OS Release 21.2R2.

RELATED DOCUMENTATION

request system halt

watchdog (PSM)

request system snapshot (Junos OS Evolved)

IN THIS SECTION

- [Syntax | 186](#)
- [Description | 186](#)
- [Options | 186](#)
- [Additional Information | 187](#)
- [Required Privilege Level | 187](#)
- [Output Fields | 187](#)
- [Sample Output | 187](#)
- [Release Information | 188](#)

Syntax

```
request system snapshot
```

Description

On devices running Junos OS Evolved, take a snapshot of the contents of the **/soft** directory, which includes the running version of Junos OS Evolved.

Starting with Junos OS Evolved 21.2, for dual-RE systems, this command only runs on the local RE, and not on both REs in the system. Any data in the **/var/home** directory of the secondary disk is no longer overwritten.



CAUTION: After you run the `request system snapshot` command, you cannot return to the previous version of the software, because the running and backup copies of the software are identical.

Options

This command has no options.

Additional Information

Before you upgrade the software on the router or replace one of the Routing Engines, when you have a known stable system, issue the `request system snapshot` command to back up the software, including the configuration, to the `/soft` directory. After you have upgraded the software or have replaced one of the Routing Engines, and are satisfied that the software packages are successfully installed and running, issue the `request system snapshot` command again to back up the software to the `/soft` directory.

Required Privilege Level

view

Output Fields

When you enter this command, the system provides feedback on the status of your request.

Sample Output

`request system snapshot (Junos OS Evolved)`

```
user@host> request system snapshot
```

```
-----
node: re0
-----
.....
Starting Snapshot in device /dev/sdb
List of software versions getting copied to Snapshot...
[1] junos-evo-install-ptx-x86-64-20.4-202103111254.0-EVO
[2] junos-evo-install-ptx-x86-64-20.4-202103150459.0-EVO
[3] junos-evo-install-ptx-x86-64-20.4-202103141559.0-EVO
.....
.....
.....
.....
.....
.....
.....
.....
.....
```

```

.....
.....
.....
.....
.....
.....
.....
Software Snapshot completed.

```

Release Information

Command introduced in Junos OS Evolved Release 20.4R2.

RELATED DOCUMENTATION

[show system snapshot \(Junos OS Evolved\) | 277](#)

[Back up and Recover Software with Snapshots | 86](#)

request system software add (Junos OS Evolved)

IN THIS SECTION

- [Syntax | 189](#)
- [Description | 189](#)
- [Options | 189](#)
- [Additional Information | 190](#)
- [Required Privilege Level | 191](#)
- [Output Fields | 191](#)
- [Sample Output | 191](#)
- [Release Information | 200](#)

Syntax

```
request system software add package-name
<force>
<validate | no-validate>
<reboot>
<restart>
```

Description

Install a software package on all REs in a cluster, as seen in the output of the `show system nodes` operational mode command. The default option is `validate`. We recommend that you always download the software image to `/var/tmp` only. For another way to validate the configuration before trying to install the software package (rather than at the same time), see ["request system software validate \(Junos OS Evolved\)" on page 212](#).

For Junos OS Evolved, the `request system software add` command has a built-in feature to not start the upgrade if a reboot is pending after an upgrade or rollback.

Any configuration changes you perform after inputting the `request system software add` command are lost when the system reboots with an upgraded version of Junos OS Evolved.

NOTE: Software packages from unidentified providers cannot be loaded. To authorize providers, include the `provider-id` statement at the `[edit system extensions provider]` hierarchy level.

For information on the valid filename and URL formats, see [Format for Specifying Filenames and URLs in Junos OS CLI Commands](#).

Options

package-name Location from which the software package or bundle is to be installed. Junos OS Evolved does not support a remote `.iso` file for upgrade, so specify the pathname of a package to be installed from a local directory on the router or switch (for example, `/var/tmp/package-name`).

Use the `file copy` command to copy the software package or bundle from the remote location to the `/var/tmp` directory on the hard disk:

```
file copy scp://package-name /var/tmp
```

Then install the software package or bundle using the `request system software add` command:

`request system software add /var/tmp/package-name`

- force** (Optional) Force the addition of the software package or bundle (ignore warnings). The `force` option automatically removes software versions until there is enough space for the new software install.
- For Junos OS Evolved, if you are trying to reinstall an already installed application, use the `force` option. The `force` option will cause the program to remove the existing application before reinstalling it.
- no-validate** (Optional) When loading a software package or bundle with a different release, suppress the default behavior of the `validate` option and skip the validation of the configuration. A subsequent reboot can cause the system to lose its configuration if the configuration is not compatible with the new software package. The `no-validate` option should only be used if you have previously issued the `request system software validate operational mode` command on the same target version and target configuration.
- reboot** (Optional) After installing the software package, reboot the system.
- The `reboot` command is not needed to install third-party applications on devices running Junos OS Evolved.
- restart** (Optional) This option allows you to upgrade the system using an application-level restart without requiring a reboot when possible. First, the system determines how many applications need to restart (start with a new version), and then, after sending output to the CLI session, the system restarts those applications. Restarted applications re-synchronize their state from the system. You can use the `request system software validate` command before using the `request system software add restart` command to determine if you can upgrade to the new image by application restart or if the system requires a reboot.
- validate** (Default) When loading a software package or bundle with a different release, validate the candidate software against the current configuration of the node.

Additional Information

Before you upgrade the software on the router or replace one of the Routing Engines, when you have a known stable system, issue the `request system snapshot` command to back up the software, including the configuration, to the `/soft` directory. After you have upgraded the software or have replaced one of the Routing Engines, and are satisfied that the software packages are successfully installed and running, issue the `request system snapshot` command again to back up the software to the `/soft` directory.

After you run the `request system snapshot` command, you cannot return to the previous version of the software because the running and backup copies of the software are identical.

Before installing software on a device that has one or more custom YANG data models added to it, back up and remove the configuration data corresponding to the custom YANG data models from the active configuration. For more information see [Managing YANG Packages and Configurations During a Software Upgrade or Downgrade](#).

Required Privilege Level

maintenance

Output Fields

When you enter this command, the system provides feedback on the status of your request.

Sample Output

request system software add restart (Junos OS Evolved for Fixed-Form Platforms)

```
user@device> request system software add restart
/var/tmp/qfx-ms-fixed-1-target1-ifmanarpcos.iso
Adding software images. This process can take several minutes. Please be patient...
Download and Validate in Progress
re0: Starting upgrade : /var/tmp/qfx-ms-fixed-1-target1-ifmanarpcos.iso
re0: Single RE upgrade detected.
re0: Installing IMA keys of the incoming ISO image...
re0: Validating existing configs. See /var/log/validation_config.log for config validation logs.
re0: Validation Passed. Going ahead with Installation
re0: Starting the installation...
re0: Copying files to //soft/junos-evo-install-qfx-ms-fixed-x86-64-19.2R1-20190522.4-
EVOI20190523235333-1...
re0: Running post install commands...
re0: Post install sequence was successful.
re0: Installation of image junos-evo-install-qfx-ms-fixed-x86-64-19.2R1-20190522.4-
EVOI20190523235333-1 done.
re0: Boot version is now 'junos-evo-install-qfx-ms-fixed-x86-64-19.2R1-20190522.4-
EVOI20190523235333-1'
Image validation and installation succeeded. Restarting Applications.

*** Restart Apps list ***
```

```

arpd
ifmand
cosd
Activating active instance of app arpd on node re0
Activating active instance of app ifmand on node re0
Activating active instance of app cosd on node re0
Image activation succeeded for arpd on node re0
Stopping active instance of app arpd on node re0
Image activation succeeded for ifmand on node re0
Stopping active instance of app ifmand on node re0
Image activation succeeded for cosd on node re0
Stopping active instance of app cosd on node re0
App arpd stopped on node re0
Starting active instance of app arpd on node re0
App ifmand stopped on node re0
Starting active instance of app ifmand on node re0
App cosd stopped on node re0
Starting active instance of app cosd on node re0
App cosd started/restarted on node re0
App ifmand started/restarted on node re0
App arpd started/restarted on node re0
*** Restart Summary ***
    *** Restart Success ***
    arpd
    ifmand
    cosd
Please check the status of applications using 'show system alarms'

```

request system software add restart (Junos OS Evolved for Fixed-Form Platforms)

```

user@device> request system software add restart
/var/tmp/qfx-ms-fixed-1-target2-ifmanarpcossysman.iso
Adding software images. This process can take several minutes. Please be patient...
Download and Validate in Progress
re0: Starting upgrade : /var/tmp/qfx-ms-fixed-1-target2-ifmanarpcossysman.iso
re0: Single RE upgrade detected.
re0: Installing IMA keys of the incoming ISO image...
re0: Validating existing configs. See /var/log/validation_config.log for config validation logs.
re0: Validation Passed. Going ahead with Installation
re0: Starting the installation...
re0: Copying files to //soft/junos-evo-install-qfx-ms-fixed-x86-64-19.2R1-20190522.4-

```

```

EVOI20190523235731-1...
re0: Running post install commands...
re0: Post install sequence was successful.
re0: Installation of image junos-evo-install-qfx-ms-fixed-x86-64-19.2R1-20190522.4-
EVOI20190523235731-1 done.
re0: Boot version is now 'junos-evo-install-qfx-ms-fixed-x86-64-19.2R1-20190522.4-
EVOI20190523235731-1'
Image validation and installation succeeded. Restarting Applications.

```

```

*** Restart Apps list ***

```

```

sysman
arpd
ifmand
cosd
Activating active instance of app sysman on node re0
Image activation succeeded for sysman on node re0
Restarting active instance of app sysman on node re0
App sysman started/restarted on node re0
Activating active instance of app arpd on node re0
Activating active instance of app ifmand on node re0
Activating active instance of app cosd on node re0
Image activation succeeded for arpd on node re0
Stopping active instance of app arpd on node re0
Image activation succeeded for ifmand on node re0
Stopping active instance of app ifmand on node re0
Image activation succeeded for cosd on node re0
Stopping active instance of app cosd on node re0
App cosd stopped on node re0
Starting active instance of app cosd on node re0
App ifmand stopped on node re0
Starting active instance of app ifmand on node re0
App arpd stopped on node re0
Starting active instance of app arpd on node re0
App cosd started/restarted on node re0
App ifmand started/restarted on node re0
App arpd started/restarted on node re0

```

```

*** Restart Summary ***

```

```

    *** Restart Success ***

```

```

    sysman
    arpd
    ifmand

```



```
cosd
Please check the status of applications using 'show system alarms'
```

request system software add restart (Junos OS Evolved for Fixed-Form Platforms)

```
user@device> request system software add restart
/var/tmp/qfx-ms-fixed-1-target3-ifmanarpcossysmanimgdorcd.iso
ifmanarpcossysmanimgdor
Adding software images. This process can take several minutes. Please be patient...
Download and Validate in Progress
re0: Starting upgrade : /var/tmp/qfx-ms-fixed-1-target3-ifmanarpcossysmanimgdorcd.iso
re0: Single RE upgrade detected.
re0: Installing IMA keys of the incoming ISO image...
re0: Validating existing configs. See /var/log/validation_config.log for config validation logs.
re0: Validation Passed. Going ahead with Installation
re0: Starting the installation...
re0: Copying files to //soft/junos-evo-install-qfx-ms-fixed-x86-64-19.2R1-20190522.4-
EVOI20190524000025...
re0: Running post install commands...
re0: Post install sequence was successful.
re0: Installation of image junos-evo-install-qfx-ms-fixed-x86-64-19.2R1-20190522.4-
EVOI20190524000025-gsanka-1 done.
re0: Boot version is now 'junos-evo-install-qfx-ms-fixed-x86-64-19.2R1-20190522.4-
EVOI20190524000025'
Image validation and installation succeeded. Restarting Applications.

*** Restart Apps list ***
sysman
arpd
ifmand
cosd
imgd
orchestrator
Activating active instance of app sysman on node re0
Image activation succeeded for sysman on node re0
Restarting active instance of app sysman on node re0
App sysman started/restarted on node re0
Activating active instance of app arpd on node re0
Activating active instance of app ifmand on node re0
Activating active instance of app cosd on node re0
Image activation succeeded for arpd on node re0
```

```

Stopping active instance of app arpd on node re0
Image activation succeeded for ifmand on node re0
Stopping active instance of app ifmand on node re0
Image activation succeeded for cosd on node re0
Stopping active instance of app cosd on node re0
App arpd stopped on node re0
Starting active instance of app arpd on node re0
App ifmand stopped on node re0
Starting active instance of app ifmand on node re0
App cosd stopped on node re0
Starting active instance of app cosd on node re0
App cosd started/restarted on node re0
App arpd started/restarted on node re0
App ifmand started/restarted on node re0
Activating active instance of app imgd on node re0
Activating active instance of app orchestrator on node re0
Image activation succeeded for imgd on node re0
Image activation succeeded for orchestrator on node re0
Restarting active instance of app imgd on node re0
Restarting active instance of app orchestrator on node re0

```

request system software add restart (Junos OS Evolved for Chassis-based Platforms)

```

user@device> request system software add a.iso restart
Adding software images. This process can take several minutes. Please be patient...

*** List of Offlined FPCs ***
FPC0
FPC1
FPC2

Perform online for above FPCs (y/n) ? y

*** Incompatible FPCs ***

FPC0
FPC1

Warning: Perform offline for above incompatible FPCs

```

```
Perform offline for above incompatible FPCs (y/n) ? n
```

```
Aborting Software Upgrade
```

```
user@host>
```

request system software add restart (Junos OS Evolved for Chassis-based Platforms)

```
user@device> request system software add a.iso restart
```

```
Adding software images. This process can take several minutes. Please be patient...
```

```
*** Unsupported frus list ***
```

```
fpc0
```

```
Perform offline for above unsupported FPCs
```

```
Offline the incompatible FRUs before proceeding for upgrade?
```

```
Enter yes to proceed with offline for incompatible frus or no to abort the upgrade.. Proceed?
```

```
[yes,no] (no) yes
```

```
*** Restart Apps list ***
```

```
sysman
```

```
arpd
```

```
mgd
```

```
orchestratord
```

```
*** Offlining of Unsupported frus may take few mins ***
```

```
fpc0 has been successfully offlined
```

```
*** Offlining of Unsupported frus are done ***
```

```
Activating active instance of app sysman on node re0
```

```
Activating active instance of app sysman on node re1
```

```
Activating active instance of app sysman on node fpc0
```

```
Image activation succeeded for sysman on node re0
```

```
Restarting active instance of app sysman on node re0
```

```
Image activation succeeded for sysman on node re1
```

```
Restarting active instance of app sysman on node re1
```

```
Image activation failed on node fpc0
```

```
App does not exist sysman on node fpc0
```

```
App sysman started/restarted on node re0
```

```

App sysman started/restarted on node re1
Activating active instance of app arpd on node re0
Image activation succeeded for arpd on node re0
Stopping active instance of app arpd on node re0
App arpd stopped on node re0
Starting active instance of app arpd on node re0
App arpd started/restarted on node re0
Activating active instance of app mgd on node re0
Activating active instance of app mgd on node re1
Activating active instance of app orchestrator on node re0
Image activation succeeded for mgd on node re0
Image activation succeeded for mgd on node re1
Image activation succeeded for orchestrator on node re0
Activating new version of the software on node fpc0
Activating new version of the software on node re0
Activating new version of the software on node re1
Image activation failed on node fpc0
Image activation succeeded on node re0
Image activation succeeded on node re1

*** Onlining of Unsupported frus may take few mins ***
fpc0 could not to be onlined

*** Onlining of Unsupported frus are done ***
Restarting active instance of app mgd on node re0
Restarting active instance of app mgd on node re1
Restarting active instance of app orchestrator on node re0
*** Restart Summary ***
  *** Restart Success ***
  sysman
  sysman
  arpd
  *** Restart Failure ***
  sysman
Please restart the failed applications
Please check the status of applications using 'show system alarms'

WARNING: cli has been replaced by an updated version:
CLI release 20190916.173330_rbu-builder.r1055817 built by rbu-builder on 2019-09-16 18:02:02 UTC
Restart cli using the new version ? [yes,no] (yes) yes

Restarting cli ...

```

```
{master}
user@host
```

request system software add

```
user@host-re0> request system software add /var/tmp/ptxinstall.iso
Adding software images. This process can take several minutes. Please be patient...
Download and Validate in Progress
re0: Starting upgrade : /var/tmp/ptxinstall.iso
re0: Upgrade version : junos-evo-install-ptx-x86-64-20.4-202103131143.0-EVO
re0: Running pre-checks for 'junos-evo-install-ptx-x86-64-20.4-202103131143.0-EVO'
re0: Pre-checks pass successfully, copying files to software area
re0: Running post install commands...
re0: Post install sequence was successful.
re0: Validating existing configs. See /var/log/validation_config.log for config validation logs.
re0: Validation Passed
re0: Going ahead with Installation
re0: Boot version is now 'junos-evo-install-ptx-x86-64-20.4-202103131143.0-EVO'
re0: Updating all nodes...
re1: Running pre-checks for 'junos-evo-install-ptx-x86-64-20.4-202103131143.0-EVO'
re1: Pre-checks pass successfully, copying files to software area
re1: Running post install commands...
re1: Post install sequence was successful.
re1: Boot version is now 'junos-evo-install-ptx-x86-64-20.4-202103131143.0-EVO'
re0: Other nodes have been updated successfully
re0: Cluster wide installation was successful
Image validation and installation succeeded.
WARNING: NOTE: A reboot is required to start using the new software.
WARNING: Use the 'request system reboot' command when ready.
```

request system software add restart (Junos OS Evolved with Support for Hotfix and JSU Upgrade)

```
user@device> request system software add restart /var/tmp/ptx-J2.iso
Adding software images. This process can take several minutes. Please be patient...
Download and Validate in Progress
re0: Starting upgrade : /var/tmp/ptx-J2.iso
re0: Upgrade version : junos-evo-install-ptx-x86-64-21.2I20210510171915-EVO_20210510171915
re0: Running prechecks for JSU image...
```

```

re0: JSU base release 21.2I20210510171915-EV0_20210510171915 matches with Current Release:
21.2I20210510171915-EV0_20210510171915.
re0: Starting JSU package installation...
re0: Copying Files from base version junos-evo-install-ptx-x86-64-21.2I20210510171915-
EV0_20210510171915-J1.1 ...
re0: Copying Files from JSU image...
re0: Signing files...
re0: Running pre-checks for 'junos-evo-install-ptx-x86-64-21.2I20210510171915-EV0_20210510171915-
J2'
re0: Pre-checks pass successfully, copying files to software area
re0: Running post install commands...
re0: Post install sequence was successful.
re0: Validating existing configs. See /var/log/validation_config.log for config validation logs.
re0: Validation Passed
re0: Going ahead with Installation
re0: Boot version is now 'junos-evo-install-ptx-x86-64-21.2I20210510171915-EV0_20210510171915-J2'
re1: Running pre-checks for 'junos-evo-install-ptx-x86-64-21.2I20210510171915-EV0_20210510171915-
J2'
re1: Pre-checks pass successfully, copying files to software area
re1: Running post install commands...
re1: Post install sequence was successful.
re1: Boot version is now 'junos-evo-install-ptx-x86-64-21.2I20210510171915-EV0_20210510171915-J2'
re0: Updating all nodes...
re0: Other nodes have been updated successfully
re0: Gathering impact report...
re0: Installation was successful
Image validation and installation succeeded. Restarting Applications.

*** Restart Apps list ***
arpd
Activating active instance of app arpd on node re0
Activating active instance of app arpd on node re1
Image activation succeeded for arpd on node re0
Stopping active instance of app arpd on node re0
Image activation succeeded for arpd on node re1
Stopping active instance of app arpd on node re1
App arpd stopped on node re1
Starting active instance of app arpd on node re1
App arpd stopped on node re0
Starting active instance of app arpd on node re0
App arpd started/restarted on node re1
App arpd started/restarted on node re0
Activating new version of the software on node fpc0

```

```
Image activation succeeded on node fpc0
*** Restart Summary ***
    *** Restart Success ***
    arpd (re0)
    arpd (re1)
Please check the status of applications using 'show system alarms'
```

Release Information

The following options are deprecated in Junos OS Evolved Release 18.3R1: best-effort-load, delay-restart, no-copy, on-primary, (re0 | re1), set, unlink, validate, validate-on-host, and validate-on-routing-engine.

RELATED DOCUMENTATION

- [request system snapshot \(Junos OS Evolved\) | 186](#)
- [request system software delete \(Junos OS Evolved\) | 200](#)
- [request system software rollback \(Junos OS Evolved\) | 204](#)
- [request system software sync | 207](#)
- [request system software validate \(Junos OS Evolved\) | 212](#)

request system software delete (Junos OS Evolved)

IN THIS SECTION

- [Syntax | 201](#)
- [Description | 201](#)
- [Options | 201](#)
- [Additional Information | 202](#)
- [Required Privilege Level | 202](#)
- [Output Fields | 202](#)
- [Sample Output | 202](#)

Syntax

```
request system software delete  
<force>  
<package-name>  
<archived>  
<all-third-party-packages>
```

Description

Use this command to remove a software package from the device, as long as it is not the software version currently running on the system. The force option is required if the requested version is the rollback version.



CAUTION: Before removing a software package, make sure that you have already placed the new software package that you intend to load onto the device, in the `/var/tmp` directory.

Options

<i>package-name</i>	Name of the Junos OS Evolved package running on the device. Type the package-name explicitly and do not use the tab key to auto-complete the command. You can see this package name by issuing the <code>show system software list operational mode</code> command.
<i>all-third-party-packages</i>	(Optional) Delete all third-party software on the device.
<i>archived</i>	(Optional) Delete all archived software versions except the current and the rollback versions. When there is a pending next-boot software version, you must reboot the system to finish installing that version, or delete just that version, before you can delete any versions with this option. If the other RE in the system has more images than the one from which you are issuing the command, the older versions are deleted from the current RE and the current and the rollback versions are synchronized to the other RE.

force (Optional) Ignore warnings and force removal of the software. The force option is required if the requested version is the rollback version.

Additional Information

Before you upgrade the software on the router or replace one of the Routing Engines, when you have a known stable system, issue the `request system snapshot` command to back up the software, including the configuration, to the `/soft` directory. After you have upgraded the software or have replaced one of the Routing Engines, and are satisfied that the software packages are successfully installed and running, issue the `request system snapshot` command again to back up the software to the `/soft` directory.

After you run the `request system snapshot` command, you cannot return to the previous version of the software because the running and backup copies of the software are identical.

Required Privilege Level

maintenance

Output Fields

When you enter this command, the system provides feedback on the status of your request.

Sample Output

request system software delete (Junos OS Evolved)

```
user@host> request system software delete junos-evo-install-qfx-fixed-
x86-64-18.3I20180911102422
Removing version 'junos-evo-install-qfx-fixed-x86-64-18.3I20180911102422'.
Software ... done.
Data ... done.
Version 'junos-evo-evo-qfx-fixed-x86-64-18.3I20180911102422' removed successfully.
```

request system software delete archived

```
user@host-re0> request system software delete archived
ALERT: This command will delete all archived SW versions except current and rollback.
Do you want to proceed? [yes,no] (no) yes
```

```

Software delete in progress...
re0: Executing Software delete...
re0: Cannot delete junos-evo-install-ptx-x86-64-20.4-202103141559.0-EVO - It is the current
version
re0: Rollback or scratch install
re0: Removing version junos-evo-install-ptx-x86-64-20.4-202103150459.0-EVO...
re0: Removing version junos-evo-install-ptx-x86-64-20.4-202103111254.0-EVO...
re1: Removing version junos-evo-install-ptx-x86-64-20.4-202103150459.0-EVO...
re1: Removing version junos-evo-install-ptx-x86-64-20.4-202103111254.0-EVO...
Image deletion succeeded.

```

request system software delete archived (with Next-boot Software Version in System)

```

user@host-re0> request system software delete archived
ALERT: This command will delete all archived SW versions except current and rollback.
Do you want to proceed? [yes,no] (no) yes

re0: Software delete cannot proceed as reboot is pending after upgrade/rollback to junos-evo-
install-ptx-x86-64-20.4I20210212000536-EVO.
re0: Please reboot before doing delete operation.
re0: Or Delete junos-evo-install-ptx-x86-64-20.4I20210212000536-EVO using 'request system
software delete'.
re0: Run 'show system software list' to get all installed software versions
Image deletion failed.

```

request system software delete archived (with Only a Current and Rollback Version Available)

```

user@host-re0> request system software delete archived
ALERT: This command will delete all archived SW versions except current and rollback.
Do you want to proceed? [yes,no] (no) yes

re0: Only minimal set of software versions exists. Cannot delete Current or Rollback versions.
Image deletion failed.

```

Release Information

all-third-party-packages option introduced in Junos OS Evolved Release 19.4R2.

archived option added in Junos OS Evolved Release 20.4R2.

RELATED DOCUMENTATION

[request system software add \(Junos OS Evolved\) | 188](#)

[request system software rollback \(Junos OS Evolved\) | 204](#)

[request system software sync | 207](#)

[request system software validate \(Junos OS Evolved\) | 212](#)

show system software list

request system software rollback (Junos OS Evolved)

IN THIS SECTION

- [Syntax | 204](#)
- [Description | 204](#)
- [Options | 205](#)
- [Required Privilege Level | 205](#)
- [Output Fields | 205](#)
- [Sample Output | 206](#)
- [Release Information | 207](#)

Syntax

```
request system software rollback reboot
<no-validate>
<package-name version>
<with-old-snapshot-config>
```

Description

Use this command to revert to the last successfully installed package before the last-issued `request system software (add | delete)` command. By default, once the software is rolled back, the device uses the current configuration file. You can use this command on either Routing Engine (RE) in a dual-RE system.

On Junos OS Evolved, the reboot option is required in order to complete the rollback.

Options

package-name <i>version</i>	Select any installed version for the rollback. The <code>request system software rollback</code> operational mode command uses the version instead of the package-name. You can see the available versions by using the <code>show system software list</code> operational mode command. If you do not specify the version, the system rolls back to the default rollback version (the one with the '<' before it on the <code>show system software list</code> command output). You can specify any previous Junos OS Evolved release as long as it is neither the one that is currently running nor the rollback version.
no-validate	Do not check compatibility with the current configuration. Default: validate
reboot	(Optional) Reboot to complete the rollback. If you do not specify the reboot option, then when this command completes, you need to issue the <code>request system reboot</code> operational mode command to reboot the system to finish the rollback process.
with-old-snapshot-config	(Optional) Rolls back the system to the specified version with the old snapshot of the configuration used in that version. Otherwise, the rollback, by default, takes the current configuration.

Required Privilege Level

maintenance

Output Fields

When you enter this command, the system provides feedback on the status of your request.

Sample Output

request system software rollback with-old-snapshot-config

```
user@host> request system software rollback junos-evo-install-ptx-x86-64-20.4-202103141559.0
with-old-snapshot-config
```

```
Starting software rollback to version junos-evo-install-ptx-x86-64-20.4-202103141559.0-EVO
Software rollback in progress...
re0: Boot version is now 'junos-evo-install-ptx-x86-64-20.4-202103141559.0-EVO'
re0: Rollback Done. Next Boot version is now 'junos-evo-install-ptx-x86-64-20.4-202103141559.0-
EVO'. Must reboot now to activate.
re0: Syncing nodes
re1: Boot version is now 'junos-evo-install-ptx-x86-64-20.4-202103141559.0-EVO'
re0: All nodes synced
Software rollback succeeded.
NOTICE: 'pending' rollback version will be activated at next reboot...
```

request system software rollback reboot

```
user@host> request system software rollback reboot
Starting software rollback to default rollback version
Software rollback in progress...
re0: Validating current config for rollback version junos-evo-install-ptx-
x86-64-20.4-202103151929.0-EVO
re0: Validating existing configs. See /var/log/validation_config.log for config validation logs.
re0: Validation Passed
re0: Validation passed for version junos-evo-install-ptx-x86-64-20.4-202103151929.0-EVO
re0: Copying current config to rollback version
re0: Boot version is now 'junos-evo-install-ptx-x86-64-20.4-202103151929.0-EVO'
re0: Rollback Done. Next Boot version is now 'junos-evo-install-ptx-x86-64-20.4-202103151929.0-
EVO'. Must reboot now to activate.
re0: Syncing nodes
re1: Config fetch successful
re1: Res Config fetch successful
re1: Boot version is now 'junos-evo-install-ptx-x86-64-20.4-202103151929.0-EVO'
re0: All nodes synced
Software rollback succeeded.
Rebooting...
```

```
{master}
user@host-re0>
System going down IMMEDIATELY

Software rollback in reboot mode succeeded. Rebooting

Connection to host closed by remote host.
Connection to host closed.
```

Release Information

validate and no-validate options introduced for Junos OS Evolved Release 18.3R1.

package-name *version* option introduced for Junos OS Evolved Release 18.3R1.

with-old-snapshot-config option introduced for Junos OS Evolved Release 18.3R1.

RELATED DOCUMENTATION

[request system snapshot \(Junos OS Evolved\) | 186](#)

[request system software add \(Junos OS Evolved\) | 188](#)

[request system software delete \(Junos OS Evolved\) | 200](#)

[request system software sync | 207](#)

[request system software validate \(Junos OS Evolved\) | 212](#)

show system software list

request system software sync

IN THIS SECTION

- [Syntax | 208](#)
- [Description | 208](#)
- [Options | 208](#)
- [Additional Information | 208](#)

- [Required Privilege Level | 209](#)
- [Sample Output | 210](#)
- [Release Information | 211](#)

Syntax

```
request system software sync (current | rollback | all-versions)
```

Description

Use this command on the primary Routing Engine (RE) of a system to synchronize the software and configurations from the primary RE to the other nodes and reboot the other nodes. The configurations are synchronized even if the images are identical. If specified on the backup RE, the command fails.

Options

- | | |
|---|---|
| current
rollback
all-
versions | <p>Specify which software version (current, rollback, or all versions) to sync to the other node:</p> <ul style="list-style-type: none"> • For the current option, the system syncs the current version from the primary RE to the other node and reboots the other node with that version. If the current version on the primary RE of the system matches the version on the other node of the system, the command fails. • For the rollback option, the system synchronizes the rollback version to the other node. If the rollback version on the primary RE of the system matches the rollback version on the other node, the command fails. • For the all-versions option, the system synchronizes all software versions and configurations from the primary RE to the other node and reboots the other node if there's a mismatch between current versions. |
|---|---|

Additional Information

For the **all-versions** option, the synchronization proceeds as follows:

1. All versions are deleted on the other node, except for the current version.

2. The current and rollback images and configurations are copied from the primary RE to the other node. Even if the software versions match, the configuration is copied and the software proceeds to the next image.
3. Any other versions and configurations are copied from the primary RE to the other node.
4. If the current version on the other node is not the same as current on the primary RE, then the other node is rebooted after warning the user.

The request `system software sync all-versions` command is successful if the first two steps of the synchronization are successful. If step 3 fails, a warning message is displayed. To make the versions match, you can delete the extra versions using the request `system software delete operational mode` command.

To see what the software versions are available on the device, use the `show system software list` command.

If an RE that has a different software version is inserted into the system, the RE is kept outside the system and a software mismatch alarm is generated, which specifies the RE name and the version of software on that RE, similar to the following: Software Version Mismatch on `re1:junos-evo-install-ptx-x86-64-20.4R2.6-EV0`. To clear this alarm, use the request `system software sync all-versions` command to synchronize the software. Once the new RE comes back up, it joins the system.

```
user@host-re0> show system alarms
2 alarms currently active
Alarm time          Class  Description
2021-04-19 16:02:26 PDT  Major  Re1 Node unreachable
2021-04-19 16:04:46 PDT  Major  Software Version Mismatch on re1:junos-evo-install-ptx-
x86-64-20.4R2.6-EV0
```

For the current option, before you switch control to a newly-inserted RE, ensure all images are synchronized to the newly-inserted RE by using the output from the `show system software list operational mode` command to compare the images installed on both REs and make sure they are the same. You must make sure that the system has finished synchronizing all of the images in the background before you switch control to the newly- inserted RE to ensure that the newly-inserted RE does not remove any images from the existing RE.

Required Privilege Level

view

Sample Output

request system software sync current

```

user@host-re0> request system software sync current
warning: Erase software versions present on the other RE node and sync software versions from
Master RE node
Erase software versions on the other RE and sync from Master RE? [yes,no] (no) yes

The current version on master RE - junos-evo-install-ptx-x86-64-20.4R2.14-EV0
The current version on other RE - junos-evo-install-ptx-x86-64-20.4R2.13-EV0
Transfer software version files for junos-evo-install-ptx-x86-64-20.4R2.14-EV0 to node re1...
Sync in progress for /soft/junos-evo-install-ptx-x86-64-20.4R2.14-EV0...
/data/var/home/root
Sync in progress for /data/junos-evo-install-ptx-x86-64-20.4R2.14-EV0...
Sync in progress for /data/config/junos-evo-install-ptx-x86-64-20.4R2.14-EV0...
Sync in progress for /data/etc/junos-evo-install-ptx-x86-64-20.4R2.14-EV0...
Sync in progress for /data/var_db/junos-evo-install-ptx-x86-64-20.4R2.14-EV0...
Sync in progress for /data/usr_conf/junos-evo-install-ptx-x86-64-20.4R2.14-EV0...
Sync in progress for /data/usr_evo_share/junos-evo-install-ptx-x86-64-20.4R2.14-EV0...
Sync in progress for /data/var_pfe/junos-evo-install-ptx-x86-64-20.4R2.14-EV0...
Sync in progress for /data/var_etc/junos-evo-install-ptx-x86-64-20.4R2.14-EV0...
Setting up software version files for junos-evo-install-ptx-x86-64-20.4R2.14-EV0 on re1
Sync in progress /data/var/home...
Software sync completed for junos-evo-install-ptx-x86-64-20.4R2.14-EV0
Warning: Rebooting re1
Please run 'show system software list' to see SW versions installed in all nodes

```

request system software sync rollback (Versions Are Already The Same)

```

user@host> request system software sync rollback
warning: Erase software versions present on the other RE node and sync software versions from
Master RE node
Erase software versions on the other RE and sync from Master RE? [yes,no] (no) yes

The rollback version on master RE - junos-evo-install-ptx-x86-64-20.4R2.14-EV0
The rollback version on other RE - junos-evo-install-ptx-x86-64-20.4R2.14-EV0
Warning: The rollback version junos-evo-install-ptx-x86-64-20.4R2.14-EV0 matches to rollback
version on other-RE. Skipping software sync
Software sync completed for junos-evo-install-ptx-x86-64-20.4R2.14-EV0

```

Please run 'show system software list' to see SW versions installed in all nodes

request system software sync all-versions

```

user@host-re0 request system software sync all-versions
warning: Erase software versions present on the other RE node and sync software versions from
Master RE node
Erase software versions on the other RE and sync from Master RE? [yes,no] (no) ...yes

Cleanup old software versions on re1
The current version on master RE - junos-evo-install-ptx-x86-64-20.4R2.14-EVO
The current version on other RE - junos-evo-install-ptx-x86-64-20.4R2.13-EVO
Sync in progress for /soft/junos-evo-install-ptx-x86-64-20.4R2.14-EVO...
The rollback version on master RE - junos-evo-install-ptx-x86-64-20.4R2.13-EVO
The rollback version on other RE - junos-evo-install-ptx-x86-64-20.4R2.14-EVO
Sync in progress for /soft/junos-evo-install-ptx-x86-64-20.4R2.13-EVO...
Software sync completed for all versions
Warning: Rebooting re1
Please run 'show system software list' to see SW versions installed in all nodes

```

Release Information

Command introduced in Junos OS Evolved Release 18.3R1.

RELATED DOCUMENTATION

show system software list

[request system software rollback \(Junos OS Evolved\) | 204](#)

[Node Software Synchronization for Dual-RE Systems | 18](#)

request system software validate (Junos OS Evolved)

IN THIS SECTION

- [Syntax | 212](#)
- [Description | 212](#)
- [Options | 212](#)
- [Required Privilege Level | 213](#)
- [Output Fields | 213](#)
- [Sample Output | 213](#)
- [Release Information | 213](#)

Syntax

```
request system software validate package-name  
<restart>
```

Description

Use this command to validate the candidate software package against the current configuration of the node. The configuration check does not change the current software or the file system.

You can use the `request system software validate` command before using the `request system software add restart` command to determine if you can upgrade to the new image with an application restart or with a reboot.

Options

package-name Name of the software bundle or package to test.

restart (Optional) Verify the new software configuration compatibility. When you issue the command with this option, the output lists those services that might be restarted.

Required Privilege Level

maintenance

Output Fields

When you enter this command, the system provides feedback on the status of your request.

Sample Output

request system software validate */var/tmp/package-name*

```
user@host-re0> request system software validate /var/tmp/ptxinstall.iso
Validating software image /var/tmp/ptxinstall.iso...
Download and Validate in Progress
re0: Starting validation : /var/tmp/ptxinstall.iso
re0: Validating version : junos-evo-install-ptx-x86-64-20.4-202103131143.0-EVO
re0: Running pre-checks for 'junos-evo-install-ptx-x86-64-20.4-202103131143.0-EVO'
re0: Pre-checks pass successfully, copying files to software area
re0: Running post install commands...
re0: Post install sequence was successful.
re0: Validating existing configs. See /var/log/validation_config.log for config validation logs.
re0: Validation Passed
re1: Running pre-checks for 'junos-evo-install-ptx-x86-64-20.4-202103131143.0-EVO'
re1: Pre-checks pass successfully, copying files to software area
re1: Running post install commands...
re1: Post install sequence was successful.
re0: Validation successful - cleaning up
re0: Removing version junos-evo-install-ptx-x86-64-20.4-202103131143.0-EVO...
re1: Removing version junos-evo-install-ptx-x86-64-20.4-202103131143.0-EVO...
Image validation succeeded.
```

Release Information

restart option added in Junos OS Evolved Release 18.3R1.

RELATED DOCUMENTATION

[request system snapshot \(Junos OS Evolved\)](#) | 186

request system software add (Junos OS Evolved) 188
request system software delete (Junos OS Evolved) 200
request system software rollback (Junos OS Evolved) 204
request system software sync 207

request system storage cleanup (Junos OS Evolved)

IN THIS SECTION

- [Syntax | 214](#)
- [Description | 214](#)
- [Options | 215](#)
- [Additional Information | 215](#)
- [Required Privilege Level | 215](#)
- [Sample Output | 216](#)
- [Release Information | 225](#)

Syntax

```
request system storage cleanup (dry-run | force-deep | no-confirm)
```

Description

Use this command to free storage space on the router or switch by rotating log files and proposing a list of files for deletion.

The Junos OS Evolved implementation of the `request system storage cleanup` command is slightly different from the implementation on Junos OS:

- The system prompts you to specify the dry-run option:

```
Please check the list of files to be deleted using the dry-run option.
Continue anyway without checking? [yes,no] (yes)
```

- When you issue the `request system storage cleanup` command, Junos OS Evolved displays the types of files to be deleted. See the Sample Output section below for an example.
- Prior to Junos OS Evolved Release 20.1R1, the command cleans up any ISO files on the system, rotates system log files, and clears trace files. It does not remove user-created files. Starting in Junos OS Evolved Release 20.1R1, this command does not remove ISO images from the system. It removes all core files, log files from `/var/log/`, and all `/var/log/*` files. To remove old images from the device, use the `request system software delete` command.
- In Junos OS Evolved, the system computes the available space and emits o/p on console for reference.

In Junos OS Evolved, the `request system storage cleanup | display xml rpc` command displays different XML tags for different file types. In Junos OS, the command displays only the `file` tag for all types of files. For more information about the differences between Junos OS and Junos OS Evolved, see [How Junos OS Evolved Differs from Junos OS](#).

Options

- dry-run** (Prompted if not specified) List the files proposed for deletion (without deleting the files).
- force-deep** (Optional) Deep clean all temporary files and rotate logs. This option cleans up all the user-created files under the `/tmp` and `/var/tmp` directories.
- no-confirm** (Optional) Do not ask for confirmation before doing the cleanup.

Additional Information

If logging is configured and being used, the `dry-run` option rotates the log files. In that case, the output displays the message “Currently rotating log files, please wait”. If no logging is currently under way, the output displays only a list of files to delete.

Required Privilege Level

maintenance

Sample Output

request system storage cleanup (Junos OS Evolved)

```

user@host-re0> request system storage cleanup
Please check the list of files to be deleted using the dry-run option.
Continue anyway without checking? [yes,no] (no) yes
-----
node: fpc0
-----
Clearing all core files

Clearing all local host core files and files from /var/log/watchdog

Clearing node specific core files

Clearing FPC log files

Clearing logical-systems log files

Clearing journal logs

Clearing all /var/log/* files

Size      Date           Name
4.0K Tue Feb  2 13:32 /var/log/beacon_getconfid.log
4.0K Tue Feb  2 13:32 /var/log/beacon_set_dhcpd.log
4.0K Tue Feb  2 13:31 /var/log/boot_init.log
556K Tue Feb  2 13:37 /var/log/evo-cda-bt.log
8.0K Tue Feb  2 13:32 /var/log/evoinit.log
  0 Tue Feb  2 13:31 /var/log/ftp_fail
4.0K Tue Feb  2 13:32 /var/log/imgd.log
  0 Tue Feb  2 13:31 /var/log/interactive-commands
  0 Tue Feb  2 13:33 /var/log/mcelog.log
4.0K Tue Feb  2 13:33 /var/log/mem_mgmt.log
  0 Tue Feb  2 13:32 /var/log/mem_monitor.dat

```

```

    0 Tue Feb  2 13:31 /var/log/messages
  4.0K Tue Feb  2 13:32 /var/log/mstr.log
  4.0K Tue Feb  2 13:32 /var/log/mstr_change.log
 292K Tue Feb  2 13:37 /var/log/ofp-packet.log
 688K Tue Feb  2 13:37 /var/log/ofp.log
 680K Tue Feb  2 13:37 /var/log/picd.log
   40K Tue Feb  2 13:32 /var/log/sinet.log
  4.0K Tue Feb  2 13:32 /var/log/ss.log
  4.0K Tue Feb  2 13:37 /var/log/storageCleanup.log
  4.0K Tue Feb  2 13:32 /var/log/sysconfig.log
   60K Tue Feb  2 13:32 /var/log/sysePOCHman.log
  4.0K Tue Feb  2 13:32 /var/log/sysstart.log
   72K Tue Feb  2 13:32 /var/log/uswitch.log
   68K Tue Feb  2 13:31 /var/log/uswitch.log.prev
  4.0K Tue Feb  2 13:32 /var/log/wtmp

```

Clearing all JSON files in /var/log/objmon

busy with previous request.

Clearing SI traces

Removing any ISO files in /data

Current space available in /soft: 4233300 K and /data: 69765 K

```

-----
node: re0
-----

```

Clearing all core files

Clearing all local host core files and files from /var/log/watchdog

Clearing node specific core files

Clearing FPC log files

Clearing logical-systems log files

Clearing journal logs

Clearing all /var/log/* files

Size	Date	Name
4.0K	Tue Feb 2 13:28	/var/log/__policy_names_rpd__
4.0K	Tue Feb 2 13:32	/var/log/__policy_names_rpdn__
8.0K	Tue Feb 2 13:32	/var/log/alarm-mgtd
4.0K	Tue Feb 2 13:28	/var/log/beacon_getconfid.log
48K	Tue Feb 2 13:27	/var/log/beacon_mountVersion.log
4.0K	Tue Feb 2 13:29	/var/log/beacon_set_dhcpd.log
4.0K	Tue Feb 2 13:28	/var/log/boot_init.log
4.0K	Tue Feb 2 13:31	/var/log/charonctl_trace.log
4.0K	Tue Feb 2 13:27	/var/log/check_restore_recovery_bios.log
4.0K	Tue Feb 2 13:32	/var/log/clksyncd.log
84K	Tue Feb 2 13:32	/var/log/configd-streamer.log
4.0K	Tue Feb 2 13:31	/var/log/copy_other_re_keys.log
4.0K	Tue Feb 2 13:37	/var/log/core_mgr.log
0	Tue Feb 2 13:28	/var/log/cscript.log
4.0K	Tue Feb 2 13:32	/var/log/ddosd.log
4.0K	Tue Feb 2 13:31	/var/log/disk_mgmt
4.0K	Tue Feb 2 13:31	/var/log/evo_dns_relay.log
8.0K	Tue Feb 2 13:28	/var/log/evoinit.log
12K	Tue Feb 2 13:36	/var/log/fibd-proxy.log
12K	Tue Feb 2 13:31	/var/log/imgd.log
32K	Tue Feb 2 13:33	/var/log/interactive-commands
28K	Tue Feb 2 13:37	/var/log/kfirewall-agent.log
0	Tue Feb 2 13:32	/var/log/mcelog.log
8.0K	Tue Feb 2 13:32	/var/log/mem_mgmt.log
0	Tue Feb 2 13:31	/var/log/mem_monitor.dat
128K	Tue Feb 2 13:37	/var/log/messages
0	Tue Feb 2 13:31	/var/log/mgd-api
4.0K	Tue Feb 2 13:28	/var/log/mgmt-ethd-helper.log
84K	Tue Feb 2 13:33	/var/log/mib2d
12K	Tue Feb 2 13:33	/var/log/mirrord.log
4.0K	Tue Feb 2 13:28	/var/log/mstr.log
4.0K	Tue Feb 2 13:28	/var/log/mstr_change.log

```

464K Tue Feb  2 13:37 /var/log/ofp-packet.log
984K Tue Feb  2 13:37 /var/log/ofp.log
 48K Tue Feb  2 13:27 /var/log/postinstall.log
4.0K Tue Feb  2 13:37 /var/log/security
4.0K Tue Feb  2 13:28 /var/log/set_mgmt_mac.log
 68K Tue Feb  2 13:28 /var/log/sinet.log
 16K Tue Feb  2 13:33 /var/log/snmpd
4.0K Tue Feb  2 13:31 /var/log/ss.log
4.0K Tue Feb  2 13:31 /var/log/ssh-key-utils.log
4.0K Tue Feb  2 13:37 /var/log/storageCleanup.log
4.0K Tue Feb  2 13:31 /var/log/sync_other_re.log
4.0K Tue Feb  2 13:28 /var/log/sysconfig.log
552K Tue Feb  2 13:32 /var/log/sysePOCHman.log
4.0K Tue Feb  2 13:28 /var/log/sysstart.log
4.0K Tue Feb  2 13:33 /var/log/system-events
 84K Tue Feb  2 13:28 /var/log/uswitch.log
 88K Tue Feb  2 13:26 /var/log/uswitch.log.prev
8.0K Tue Feb  2 13:31 /var/log/validator_debug.log
4.0K Tue Feb  2 13:33 /var/log/vrf.log
8.0K Tue Feb  2 13:36 /var/log/wtmp
4.0K Tue Feb  2 13:32 /var/log/xferlog
364K Tue Feb  2 13:37 /var/log/zookeeper--server-host-re0.log
4.0K Tue Feb  2 13:29 /var/log/zookeeper--server-host-re0.out
4.0K Tue Feb  2 13:33 /var/log/ztp.log

```

Clearing all JSON files in /var/log/objmon

Cleared traces for application all node all pid all

Clearing SI traces

Removing any ISO files in /data

Current space available in /soft: 14158432 K and /data: 2857732 K

```

-----
node: re1
-----

```

Clearing all core files

Clearing all local host core files and files from /var/log/watchdog

Clearing node specific core files

Clearing FPC log files

Clearing logical-systems log files

Clearing journal logs

Clearing all /var/log/* files

Size	Date	Name
4.0K	Tue Feb 2 13:32	/var/log/__policy_names_rpd__
4.0K	Tue Feb 2 13:31	/var/log/alarm-mgtd
4.0K	Tue Feb 2 13:29	/var/log/beacon_getconfid.log
48K	Tue Feb 2 13:27	/var/log/beacon_mountVersion.log
4.0K	Tue Feb 2 13:29	/var/log/beacon_set_dhcpd.log
4.0K	Tue Feb 2 13:28	/var/log/boot_init.log
4.0K	Tue Feb 2 13:31	/var/log/charonctl_trace.log
4.0K	Tue Feb 2 13:28	/var/log/check_restore_recovery_bios.log
12K	Tue Feb 2 13:32	/var/log/copy_other_re_keys.log
4.0K	Tue Feb 2 13:32	/var/log/core_mgr.log
0	Tue Feb 2 13:28	/var/log/cscript.log
4.0K	Tue Feb 2 13:31	/var/log/disk_mgmt
4.0K	Tue Feb 2 13:31	/var/log/evo_dns_relay.log
8.0K	Tue Feb 2 13:31	/var/log/evoinit.log
24K	Tue Feb 2 13:37	/var/log/fibd-proxy.log
4.0K	Tue Feb 2 13:29	/var/log/imgd.log
0	Tue Feb 2 13:28	/var/log/interactive-commands
24K	Tue Feb 2 13:37	/var/log/kfirewall-agent.log
0	Tue Feb 2 13:32	/var/log/mcelog.log
4.0K	Tue Feb 2 13:31	/var/log/mem_mgmt.log
0	Tue Feb 2 13:31	/var/log/mem_monitor.dat
0	Tue Feb 2 13:32	/var/log/messages
4.0K	Tue Feb 2 13:31	/var/log/mgmt-ethd-helper.log

```

4.0K Tue Feb 2 13:31 /var/log/mib2d
4.0K Tue Feb 2 13:28 /var/log/mstr.log
4.0K Tue Feb 2 13:28 /var/log/mstr_change.log
444K Tue Feb 2 13:37 /var/log/ofp-packet.log
1016K Tue Feb 2 13:37 /var/log/ofp.log
 48K Tue Feb 2 13:28 /var/log/postinstall.log
   0 Tue Feb 2 13:32 /var/log/security
4.0K Tue Feb 2 13:28 /var/log/set_mgmt_mac.log
 68K Tue Feb 2 13:28 /var/log/sinet.log
4.0K Tue Feb 2 13:31 /var/log/snmpd
4.0K Tue Feb 2 13:31 /var/log/ss.log
8.0K Tue Feb 2 13:32 /var/log/ssh-key-utils.log
4.0K Tue Feb 2 13:37 /var/log/storageCleanup.log
4.0K Tue Feb 2 13:32 /var/log/sync_other_re.log
4.0K Tue Feb 2 13:28 /var/log/sysconfig.log
204K Tue Feb 2 13:32 /var/log/sysePOCHman.log
4.0K Tue Feb 2 13:28 /var/log/sysstart.log
   0 Tue Feb 2 13:32 /var/log/system-events
 84K Tue Feb 2 13:29 /var/log/uswitch.log
 88K Tue Feb 2 13:26 /var/log/uswitch.log.prev
 12K Tue Feb 2 13:32 /var/log/validator_debug.log
4.0K Tue Feb 2 13:33 /var/log/vrf.log
8.0K Tue Feb 2 13:33 /var/log/wtmp
4.0K Tue Feb 2 13:31 /var/log/xferlog
 88K Tue Feb 2 13:37 /var/log/zookeeper--server-host-re1.log
4.0K Tue Feb 2 13:29 /var/log/zookeeper--server-host-re1.out

```

Clearing all JSON files in /var/log/objmon

Cleared traces for application all node all pid all

Clearing SI traces

Removing any ISO files in /data

Current space available in /soft: 14158432 K and /data: 2775780 K

{master}

```
user@host-re0>
```

request system storage cleanup dry-run (Junos OS Evolved)

```
user@host> request system storage cleanup dry-run
```

```
-----  
node: re0  
-----
```

```
List of all core files to be cleared:
```

```
List of local_host core files to be cleared:
```

```
List of core sub directory files to be cleared:
```

```
List of log files from FPCs to be cleared:
```

```
List of log files from logical systems to be cleared:
```

```
Clears all App logs, App traces, App SI traces and App core files from /var/log/*, /var/log/  
traces/*, /var/log/si_traces/* and /var/core/*
```

```
Clears all JSON files in /var/log/objmon/ during cleanup
```

```
List of ISO files from /data partition to be cleared:
```

```
Current list of software versions installed
```

```
Removes older software versions - Minimum two versions would be left around
```

```
Active boot device is primary : /dev/vda
```

```
List of installed version(s) :
```

```
'-' running version
```

'>' next boot version after upgrade/downgrade

'<' rollback boot version

- junos-evo-install-ptx-fixed-x86-64-20.1-201911201458.0-EVO - [2019-11-21 11:23:21]

request system storage cleanup force-deep (Junos OS Evolved)

```
user@host> request system storage cleanup force-deep
```

Please check the list of files to be deleted using the dry-run option.

Continue anyway without checking? [yes,no] (no) **yes**

```
-----
node: re0
-----
```

```
.....
```

```
===== Start cleanup now =====
```

```
=== Start removing other logs, traces, core files ===
```

```
Clearing core files
```

```
Clearing FPC logs
```

```
Clearing logical-systems logs
```

```
=== Clearing journal logs ===
```

```
Clearing log: /var/log/RE_journal.log
```

```
Clearing log: /var/log/RE_journal_boot.log
```

```
Clearing log: /var/log/alarm-mgmt
```

```
Clearing log: /var/log/appDemo_stdout
```

```
Clearing log: /var/log/charonctl_trace.log
```

```
Clearing log: /var/log/configd-streamer.log
```

```
Clearing log: /var/log/core_mgr.log
```

```
Clearing log: /var/log/cscript.log
```

```
Clearing log: /var/log/eth_linkmon.log
```

```
Clearing log: /var/log/evo-cda-zx.log
```

```
Clearing log: /var/log/evoinit.log
```

```
Clearing log: /var/log/fibd-proxy.log
```

```
Clearing log: /var/log/i2ctrace.log
```

```
Clearing log: /var/log/i2ctrace_spmbo.log
```

```
Clearing log: /var/log/i2ctrace_spmbo1.log
```

```
Clearing log: /var/log/icmpd.log
```

```
Clearing log: /var/log/ifinfo.log
```

```
Clearing log: /var/log/imgd_svr.log
```

```
Clearing log: /var/log/install
```

```
Clearing log: /var/log/interactive-commands
```

```

Clearing log: /var/log/jsd
Clearing log: /var/log/lastlog
Clearing log: /var/log/mcelog.log
Clearing log: /var/log/messages
Clearing log: /var/log/mgd-api
Clearing log: /var/log/mgmt-ethd-helper.log
Clearing log: /var/log/mib2d
Clearing log: /var/log/na-grpcd
Clearing log: /var/log/objmon_sync.json
Clearing log: /var/log/packetio-cout.log
Clearing log: /var/log/picd.log
Clearing log: /var/log/platform_mon.log
Clearing log: /var/log/policerd.log
Clearing log: /var/log/postinstall.log
Clearing log: /var/log/ptp_fpga.log
Clearing log: /var/log/reboot_node.log
Clearing log: /var/log/rollback.log
Clearing log: /var/log/security
Clearing log: /var/log/semctl.log
Clearing log: /var/log/set_mgmt_mac.log
Clearing log: /var/log/shutdown_complete.log
Clearing log: /var/log/sinet.log
Clearing log: /var/log/smartd-attr-SFSA200GM3AA4TO_C_HC_636_JUN-000060139624B1000020.log
Clearing log: /var/log/smartd-attr-SFSA200GM3AA4TO_C_HC_636_JUN-000060139624B1000022.log
Clearing log: /var/log/snmpd
Clearing log: /var/log/ss.log
Clearing log: /var/log/ssh-key-utils.log
Clearing log: /var/log/sshd_lua.log
Clearing log: /var/log/sysconfig.log
Clearing log: /var/log/sysman.conf
Clearing log: /var/log/system-events
Clearing log: /var/log/upgrade_master.log
Clearing log: /var/log/uswitch.log
Clearing log: /var/log/uswitch.log.prev
Clearing log: /var/log/validator_debug.log
Clearing log: /var/log/wtmp
Clearing log: /var/log/zookeeper--server-re.log
Clearing log: /var/log/zookeeper--server-re.out
Clearing log: /var/log/ztp.log
=== Clearing all traces ===
=== Clearing SI traces ===
=== Removing other logs, traces, core files completed ===
=== Started removing any ISO files in /data

```

```

=== Removing any ISO files in /data completed
=== Start Software versions cleanup ===
Removing older software versions except current and rollback
=== Software versions cleanup completed ===
===== Cleanup done =====
Current space available in /soft: 12372572 K
Current space available in /data: 2638752 K
Cannot delete junos-evo-install-qfx-fixed-x86-64-18.3I20180906130134_mkamil - It is the rollback
version
Cannot delete junos-evo-install-qfx-fixed-x86-64-18.3-20180906.3 - It is the current version
Removing version junos-evo-install-qfx-x86-64-16.2I20180516093649...
Done.

```

Release Information

Command introduced in Junos OS Evolved Release 20.4R2.

RELATED DOCUMENTATION

[request system software delete \(Junos OS Evolved\)](#) | 200

request system zeroize (Junos OS Evolved)

IN THIS SECTION

- [Syntax](#) | 226
- [Description](#) | 226
- [Options](#) | 226
- [Required Privilege Level](#) | 226
- [Sample Output](#) | 226
- [Release Information](#) | 226

Syntax

```
request system zeroize
```

Description

Use this command to remove all configuration information on the Routing Engines and reset all key values on the device where you run the command. If the device has two Routing Engines, the command is broadcast to both Routing Engines on the device.

This command removes all data files, including any customized configuration and log files, by unlinking the files from their directories. The command removes all user-created files from the system, including all plain-text passwords, secrets, and private keys for SSH, local encryption, local authentication, IPSec, RADIUS, TACACS+, and SNMP.

This command reboots the device and sets it to the factory default configuration. After the reboot, you cannot access the device through the management Ethernet interface. Log in through the console as root and start the CLI by typing `cli` at the prompt.

Options

This command has no options.

Required Privilege Level

maintenance

Sample Output

request system zeroize

```
user@host> request system zeroize
warning: System will be rebooted and may not boot without configuration
Erase all data, including configuration and log files? [yes,no] (yes)
```

Release Information

Command introduced in Junos OS Evolved Release 18.3R1.

restart (Junos OS Evolved)

IN THIS SECTION

- [Syntax | 227](#)
- [Description | 227](#)
- [Options | 228](#)
- [Required Privilege Level | 228](#)
- [Output Fields | 228](#)
- [Sample Output | 228](#)
- [Release Information | 229](#)

Syntax

```
restart application-name  
<gracefully | immediately | soft>
```

Description

Restart a Junos OS Evolved process.



CAUTION: Never restart a software process unless instructed to do so by a customer support engineer. A restart might cause the router or switch to drop calls and interrupt transmission, resulting in possible loss of data.

For Junos OS Evolved, the restart command also triggers a restart of the dependent applications (apps). To inform you which dependent apps restarted, the following message appears in the log whenever you use the restart command:

```
App restarting <app name>. Related apps that may be impacted - <related-app name> . For example: Jan  
14 11:42:08 RE0 sysman[5100]: SYSTEM_APP_RESTARTING_WITH_RELAPPS_EVENT: App restarting re0-ifmand.  
Related apps that may be impacted - aggd
```

Starting in Junos OS Evolved Release 20.1R1, if you specify the `restart app-name` command and the application is not supposed to run on the platform, the error message is as follows:

```
user@device> restart fabspoked-pfe
Restart failed for fabspoked-pfe on node re0. Application is not running.
```

The `restart` command expands all application names, including applications not required for the current platform. Therefore, you could try to restart an application that is not running for the current platform. This error message communicates that the restart failed because the application was not running on the system.

Options

<i>application-name</i>	Specify the name of the application you want to restart. Use the <code>show system applications operational mode</code> command for information about what applications are running.
none	Same as <code>gracefully</code> .
gracefully	(Optional) Gracefully restart the software process.
immediately	(Optional) Immediately restart the software process.
soft	(Optional) Re-read and reactivate the configuration without completely restarting the software processes. For example, BGP peers stay up and the routing table stays constant. Omitting this option results in a graceful restart of the software process.

Required Privilege Level

reset

Output Fields

When you enter this command, the system provides feedback on the status of your request.

Sample Output

restart interface-control (Junos OS Evolved)

```
user@host> restart interface-control
interface-control restart requested
```

```
Restarted aggd on re0
Restarted ifmand on re0
```

Release Information

Introduced in Junos OS Evolved Release 19.1R1.

rollback

IN THIS SECTION

- [Syntax | 229](#)
- [Description | 229](#)
- [Options | 230](#)
- [Required Privilege Level | 230](#)
- [Release Information | 230](#)

Syntax

```
rollback <number | rescue | revision revision-string>
```

Description

Return to a previously committed configuration. The software saves the last 50 committed configurations, including the rollback number, date, time, and name of the user who issued the `commit` configuration command.

The currently operational configuration is stored in the file **juniper.conf**, and the last three committed configurations are stored in the files **juniper.conf.1**, **juniper.conf.2**, and **juniper.conf.3**. These four files are located in the directory **/config**, which is on the router's flash drive. The remaining 46 previous committed configurations, the files **juniper.conf.4** through **juniper.conf.49**, are stored in the directory **/var/db/config**, which is on the router's hard disk.

During rollback, the configuration you specify is loaded from the associated file. Only objects in the rollback configuration that differ from the previously loaded configuration are marked as changed (equivalent to `load update`).

Options

none	(Optional) Return to the most recently saved configuration.
<i>number</i>	(Optional) Configuration to return to. The range of values is from 0 through 49. The most recently saved configuration is number 0, and the oldest saved configuration is number 49. The default is 0.
rescue	(Optional) Return to the rescue configuration.
revision <i>revision-string</i>	(Option) Use a configuration revision identifier to rollback to a specific configuration. Use the <i>show system commit include-configuration-revision</i> command to view the configuration revision identifier for each revision.

Required Privilege Level

rollback—To roll back to configurations other than the one most recently committed.

Release Information

Command introduced before Junos OS Release 7.4.

Option `revision` introduced in Junos OS Release 20.4R1 and Junos OS Evolved Release 20.4R1.

show system applications (Junos OS Evolved)

IN THIS SECTION

- [Syntax | 231](#)
- [Description | 231](#)
- [Options | 231](#)
- [Required Privilege Level | 231](#)
- [Output Fields | 232](#)

- [Sample Output | 235](#)
- [Release Information | 239](#)

Syntax

```
show system applications
<app app-name>
<brief>
<detail>
<node node-name>
```

Description

This command displays application summary information in one of the following forms:

- Shows all application summary information for all nodes.
- Shows the application summary information for a specific application.
- Shows the application summary information for a specific node.

Options

app <i>app-name</i>	(Optional) Specify application name for which you want to display application summary information.
brief	(Optional) Display brief output. This is the default format of display.
detail	(Optional) Display detailed output.
node <i>node-name</i>	(Optional) Specify node name for which you want to display application summary information.

Required Privilege Level

view

Output Fields

For a description of the output fields, see [Table 6 on page 232](#). Output fields are listed in the approximate order in which they appear.

Table 6: show system applications Output Fields

Field Name	Description		Level
Applications Information	Application	Name of the application.	all levels
	Node	Name of the node the application is running on.	
	App State	State of the application: online, offline, failed, or active.	
	App Weight	A relative weight for multiple instances of the application across multiple nodes. The application instance with the higher weight provides more functionality.	
	App Zookeeper Session	Zookeeper session ID.	
Object Producer details	Producer ID	Identifies which production set the object is part of.	all levels
	Epoch ID	A number that identifies the current process that owns a production set. There can only be one owning process (active producer) that owns a production set at one time. The current owning process has an Epoch ID that is larger than any previous producer.	
	Production Topic	Hierarchical string that represents the production set.	
	Producer State	active or standby: <ul style="list-style-type: none"> • active indicates the application has production rights to modify the state in the production set. • standby means that the application is waiting to get the production right for the production set. 	

Table 6: show system applications Output Fields (Continued)

Field Name	Description	Level
Description	A short description of the application, it also lists the systemd service file used for the application.	detail
Loaded	A systemd state that indicates if the application is loaded in the system or not.	detail
Run State from OS	A systemd state that indicates if the application is active or not.	detail
Main PID	Process identifier (PID) of the application.	detail
Command	Command line to launch the application.	detail
ID	Name of the application.	detail
Meta	<p>Meta data for the application includes the following fields:</p> <p>Bin path Path to application execution.</p> <p>Log file Where logs go.</p> <p>Working Dir Working directory.</p> <p>Production Set Global or local production set. Values might be shared or local.</p>	detail

Table 6: show system applications Output Fields (*Continued*)

Field Name	Description	Level
Resource	<p>Resource data for the application includes the following fields:</p> <p>all nodes Does the application run on all nodes, true or false.</p> <p>Max instances How many instances of the application are there.</p> <p>Max instances per node How many instances of the application per node are there.</p> <p>Run on startup Is the application launched at bootup, true or false.</p> <p>Node attributes Typical node attributes are RE, FPC, MasterRE. You can see the node attributes by using the <code>show system node-attributes</code> command.</p> <p>Node attribute match What is the node attribute required to launch this application on a node? For example, if this field has the output <code>re, Service file: lfmd</code>, it indicates that the process <code>lfmd</code> will be launched on a node that has the attribute RE.</p>	detail
Failure	<p>Failure data for the application includes the following fields:</p> <p>Alarm color Which alarm to be raised on failure, or none.</p> <p>Alarm ID The alarm ID.</p> <p>Restart Whether to restart the application, true or false.</p>	detail
Upgrade	<p>Upgrade parallely Options are true or false.</p> <p>Upgrade restart node Options are true or false.</p> <p>Upgrade style Option is stop-start.</p>	detail

Table 6: show system applications Output Fields (Continued)

Field Name	Description	Level
App-Exit	<p>App-Exit data for the application includes the following fields:</p> <p>Restart Supported True/false. When the application exits, should the application be restarted.</p> <p>Restart Node True/false. When the application exits, should the node be rebooted.</p> <p>Mark node spare When an application exits, should the node be marked spare.</p>	detail

Sample Output

show system applications

```

user@host> show system applications
Applications Information:
Application      : bcmd_evo
Node             : fpc0
App State        : offline
Object Producer details
Producer ID      : 0
Epoch ID        : 0

Applications Information:
Application      : ccdpfe
Node             : fpc0
App State        : online
Object Producer details
Producer ID      : 576
Epoch ID        : 65
Production Topic : /Root/fpc0/ccdpfe/100143551468101228
Producer State   : active

Applications Information:
Application      : cmd

```

```

Node           : fpc0
App State      : online
Object Producer details
Producer ID    : 570
  Epoch ID     : 66
  Production Topic : /Root/fpc0/cmd/1099227235289688912
  Producer State : active

```

...

Applications Information:

```

Application    : alarm-mgmt
Node          : re0
App State      : online
Object Producer details
Producer ID    : 26
  Epoch ID     : 1
  Production Topic : /Root/alarm-mgmt/2988563069668674039
  Producer State : active

```

Applications Information:

```

Application    : alarmd
Node          : re0
App State      : online
Object Producer details
Producer ID    : 377
  Epoch ID     : 30
  Production Topic : /Root/alarmd/6512784671716237713
  Producer State : active

```

Applications Information:

```

Application    : arpd
Node          : re0
App State      : online
Object Producer details
Producer ID    : 396
  Epoch ID     : 41
  Production Topic : /Root/arpd/14284058728950342139
  Producer State : active

```

...

Applications Information:

```

Application      : alarm-mgmt
Node             : re1
App State        : online
Object Producer details
Producer ID      : 26
  Epoch ID       : 0
  Production Topic : /Root/alarm-mgmt/2988563069668674039
  Producer State  : standby

Applications Information:
Application      : bcmd_evo
Node             : re1
App State        : offline
Object Producer details
Producer ID      : 0
  Epoch ID       : 0

Applications Information:
Application      : charonctl
Node             : re1
App State        : online
Object Producer details
Producer ID      : 25
  Epoch ID       : 4
  Production Topic : /Root/re1/charonctl/10854553120394604032
  Producer State  : active

...

```

show system applications app application-name node node-name

```

user@host> show system applications app alarm-mgmt node re1
Applications Information:
Application      : alarm-mgmt
Node             : re1
App State        : online
Object Producer details
Producer ID      : 26
  Epoch ID       : 0

```

```

Production Topic      : /Root/alarm-mgmd/2988563069668674039
Producer State       : standby

```

show system applications node node-name detail

```

user@host> show system applications app cmdd detail
Applications Information:
Application          : cmdd
Node                 : re0
App State            : online ready
App Weight           : 1
App Zookeeper Session : 1000000934d000d
Object Producer details
Producer ID          : 50331736
  Epoch ID           : 47
  Production Topic    : /Root/re0/cmdd/3158206796014561683
  Producer State      : active
Description          : cmdd.service - "Command Daemon"
Loaded               : loaded (/etc/systemd/system/cmdd.service;static;vendor preset:enabled)
Run State from OS    : active (running) (Result: success) since Mon 2018-10-29 05:02:24 PDT
Main PID             : 5814
Command              : /usr/sbin/cmdd --app-name cmdd -I object_select --shared-objects-mode 3
App Config Info
  ID                 : cmdd
  Meta
    Bin path         : /usr/sbin/cmdd
    Log file         : /var/log
    Working Dir      : /usr/sbin
    Production Set    : local
    Sysman Managed    : true
    Type Evo         : true
  Resource
    All nodes        : true
    Max instances     : 1
    Max instances per node: 1
    App Suite         : default,diags_default
    Run on startup    : true
    Node attributes   :
(Node attribute match : *, Service file : cmdd)
Failure
  Alarm color        : red

```

```

Restart Node      : false
Mark node spare   : false
Upgrade
  Upgrade parallely      : true
  Upgrade restart node   : false
  Upgrade style          : stop-start
App-Exit
  Restart Supported      : true
  Restart Node           : false
  Mark node spare        : false

```

Release Information

Command introduced in Junos OS Evolved Release 18.3R1.

RELATED DOCUMENTATION

[request node halt \(Junos OS Evolved\) | 167](#)

request node (offline / online) (Junos OS Evolved)

[request node power-off \(Junos OS Evolved\) | 172](#)

[request node power-on \(Junos OS Evolved\) | 174](#)

request node reboot (re0 / re1) (Junos OS Evolved)

show system core dumps (Junos OS Evolved)

IN THIS SECTION

- [Syntax | 240](#)
- [Description | 240](#)
- [Required Privilege Level | 240](#)
- [Output Fields | 240](#)
- [Sample Output | 240](#)

Syntax

```
show system core-dumps
<node node-name>
```

Description

Show core files on all routers or switches running Junos OS Evolved. You use this command to show a list of system core files created when the device has failed, which can be useful for diagnostic purposes. Each list item includes the file permissions, number of links, owner, group, size, modification date, and path and filename.

NOTE: For Junos OS Evolved, if dual Routing Engines are present, the command lists the core-dump files for both Routing Engines.

Required Privilege Level

view

Output Fields

The command displays a list of core-dump files. If a node does not have any core-dump files, then the command displays just the node name.

Sample Output

show system core-dumps (Dual-RE System, with Core Dump on only One RE)

```
user@host> show system core-dumps
re0:
-----

re1:
-----
-rw-r--r--  1 root  root    10389341 Mar 16 00:38 /var/core/re1/
agentd.re.re1.19293.2021_03_16.00_37_32.tar.gz
total files: 1
```

The output shows that there aren't any core-dump files on node RE0, but node RE1 has one core-dump file.

show system core-dumps (Dual-RE System, with Core Dumps on both REs)

```
user@host-re0> show system core-dumps
re0:
-----
-rw-r--r--  1 root  root    52340949 Apr 13 11:01 /var/core/fpc0/
hwdfpc.fpc_x86_64.fpc0.14522.2021_04_13.10_59_10.tar.gz
total files: 1

re1:
-----
-rw-r--r--  1 root  root    32432932 Apr 13 13:01 /var/core/re1/
imgd.re.re1.11040.2021_04_13.12_59_45.tar.gz
-rw-r--r--  1 root  root    346853497 Apr  8 10:52 /var/core/re1/
rpdagent.re.re1.17935.2021_04_08.10_46_34.tar.gz
-rw-r--r--  1 root  root    369435949 Apr  8 10:58 /var/core/re1/
rpdagent.re.re1.1908.2021_04_08.10_52_22.tar.gz
-rw-r--r--  1 root  root    192094114 Apr  8 11:00 /var/core/re1/
rpdagent.re.re1.5148.2021_04_08.10_56_18.tar.gz
-rw-r--r--  1 root  root    214337055 Apr  8 10:51 /var/core/re1/
rpdagent.re.re1.17935.2021_04_08.10_46_34/rpd-agent_trace.tar.gz
total files: 5
```

show system errors

IN THIS SECTION

- [Syntax | 242](#)
- [Description | 242](#)
- [Options | 242](#)
- [Required Privilege Level | 242](#)
- [Output Fields | 243](#)

- [Sample Output | 244](#)
- [Release Information | 246](#)

Syntax

```
show system errors
<cb slot| ccg slot | fan slot | fpc slot | psm slot | re slot | sib slot>
```

Description

Display information about faults in the system. You can display all errors or the errors for one system component. Use this command to understand about faults and their correlation with other events. First, top level root causes are listed, with board level faults followed by component level faults. Next, details for affected faults are listed.

The show output represents five faults, F1 through F5. F4 and F5 are top level faults, where F4 is affected by F1, F2, and F3; and F3 is affected by F1 and F2. The lowest level (leaf) faults, F1, F2, and F5, have no affected events.

NOTE: For Junos OS Evolved, only the QFX5200 supports this command. For all other Junos OS Evolved platforms, use the *show system errors active*, *show system errors count*, *show system errors error-id*, ["show system errors fru" on page 258](#), or ["show system errors inactive" on page 264](#) command.

Options

This command has no options.

Required Privilege Level

view

Output Fields

Table 7 on page 243 lists the output fields for the `show system errors` command. Output fields are listed in the approximate order in which they appear.

Table 7: show system errors Output Fields

Field Name	Field Description
Top level root causes	Display of the top level faults with board level faults followed by component level faults.
Fx	Fault number F1 to Fn, where F1 is the first fault and n is the last fault generated by the system.
(<i>module, error-id, board-name, component-name</i>)	Information about the fault. Component level faults include the component name.
Group	Fault severity level is Fatal, Major, or Minor.
Scope	Affected scope of fault is System, Component, Board, or Link.
Corr-enabled	Correlation with fault is always enabled, Y.
Time	Time in the format yyyy-mm-dd hh:nn:ss.lll TMZ, where nn is minutes, lll is milliseconds, and TMZ is time zone.
Desc	Description of the fault.
Actions	List of errors that caused the fault.
Root-causes	List of faults that caused this error.
Affected	List of faults that correlate to this root cause.

Table 7: show system errors Output Fields (Continued)

Field Name	Field Description
Details for affected errors	Display the affected errors listed in top level faults.

Sample Output

show system errors

```

user@host> show system errors
Top level root-causes:
F4: {pciesw, 1, fpc0} Group: Fatal Scope: Board Corr-enabled: Y
Time: "2017-02-22 16:37:47.456 PST"
Desc: PCIe Switch Fatal AER Errors
Actions: Alarm: FPC_FATAL_ERRORS + FRU_FAULT
Root-causes: None
Affected:
F3: {hwd, 1, fpc0}
F1: {pechip, 1, fpc0, pechip0}
F2: {pechip, 1, fpc0, pechip3}
F5: {pfchip, 3, sib0, pfchip5} Group: Major Scope: Component Corr-enabled: Y
Time: "2017-02-22 18:37:47.456 PST"
Desc: Midplane link errors
Actions: Alarm: ASIC_FABRIC_LINK_ERRORS
Affected: None
Details for Affected Errors:
F3: {hwd, 1, fpc0}, Group: Fatal Scope: Board Corr-enabled: Y
Time: "2017-02-22 16:37:47.856 PST"
Desc: FPC Fault
Root-causes: F4 : { pciesw, 1, fpc0}
Affected:
F1: {pechip, 1, fpc0, pechip0}
F2: {pechip, 1, fpc0, pechip3}
F1: {pechip, 3, fpc0, pechip0}, Group: Fatal Scope: Component Corr-enabled: Y
Time: "2017-02-22 16:37:48.500 PST"
Desc: PIO Fault
Root-causes:
F4 : {pciesw, 1, fpc0}
Affected: None

```

```

F2: {pechip, 3, fpc0, pechip1}, Group: Fatal Scope: Component Corr-enabled: Y
Time: "2017-02-22 16:37:48.600 PST"
Desc: PIO Fault
Root-causes:
F4 : {pciesw, 1, fpc0}
Affected: None

```

show system errors fpc 0

```

user@host> show system errors fpc 0
Top level root-causes:
F4: {pciesw, 1, fpc0} Group: Fatal   Scope: Board  Corr-enabled: Y
Time:   "2017-02-22 16:37:47.456 PST"
Desc:   PCIe Switch Fatal AER Errors
Actions: Alarm: FPC_FATAL_ERRORS + FRU_FAULT
Root-causes: None
Affected:
F3:     {hwd, 1, fpc0}
F1:     {pechip, 1, fpc0, pechip0}
F2:     {pechip, 1, fpc0, pechip3}

Details for Affected Errors:
F3: {hwd, 1, fpc0}, Group: Fatal   Scope: Board  Corr-enabled: Y
Time: "2017-02-22 16:37:47.856 PST"
Desc:   FPC Fault
Root-causes: F4 : { pciesw, 1, fpc0}
Affected:
F1:     {pechip, 1, fpc0, pechip0}
F2:     {pechip, 1, fpc0, pechip3}

F1: {pechip, 3, fpc0, pechip0}, Group: Fatal   Scope: Component  Corr-enabled: Y
Time: "2017-02-22 16:37:48.500 PST"
Desc: PIO Fault
Root-causes:
F4 : {pciesw, 1, fpc0}
Affected: None
F2: {pechip, 3, fpc0, pechip1}, Group: Fatal   Scope: Component  Corr-enabled: Y
Time: "2017-02-22 16:37:48.600 PST"
Desc: PIO Fault
Root-causes:

```

```
F4 : {pciesw, 1, fpc0}
Affected: None
```

show system errors sib 0

```
user@host> show system errors sib 0
Top level root-causes:
F5: {pfchip, 3, sib0, pfchip5} Group: Major   Scope: Component  Corr-enabled: Y
Time:    "2017-02-22 18:37:47.456 PST"
Desc:    Midplane link errors
Actions: Alarm: ASIC_FABRIC_LINK_ERRORS
Affected: None
```

Release Information

Command introduced in Junos OS Evolved Release 18.3R1.

RELATED DOCUMENTATION

| [show system errors history](#) | 272

show system errors active

IN THIS SECTION

- [Syntax](#) | 247
- [Description](#) | 247
- [Options](#) | 247
- [Required Privilege Level](#) | 247
- [Output Fields](#) | 248
- [Sample Output](#) | 249
- [Release Information](#) | 252

Syntax

```
show system errors active
<detail [fru slot-number [scope error-scope] [category error-category]]>
<fru slot-number>
```

Description

Display information collected by the J-Insight fault monitoring feature. Specifically, display summary or detailed information about the active errors based on FRU, error scope, or error category.

NOTE: In PTX Series routers with Junos OS Evolved, the details of the Packet Forwarding Engine errors (reported through CMErrors), when set and cleared, are moved from the output of `show system errors active` command to the output of `show system errors inactive` command. However, the output of the `show system errors inactive detail` does not contain the details of the active FRU board errors that are cleared.

Options

none	Display a brief summary of the system error information for all applicable FRUs.
<i>category error-category</i>	(Optional) Display system error information based on error category. An error category categorizes errors into various subgroups under a specific error scope level. Values include: core, functional, io, memory, processing, storage, and switch.
detail	(Optional) Display detailed system error information.
<i>fru slot-number</i>	(Optional) Display system error information for a specific FRU. For devices running Junos OS, output displays error details for FPC FRUs. For devices running Junos OS Evolved, output displays error details for FPC and other components such as fan, PSM, CB, and chassis.
<i>scope error-scope</i>	(Optional) Display system error information based on error scope. An error scope provides a level of classification above error category. Values include: board, pfe, and scope-all.

Required Privilege Level

admin

Output Fields

Table 8 on page 248 list the output fields for the `show system errors active` command. Output fields are listed in the approximate order in which they appear.

Table 8: show system errors active Output Fields

Field Name	Field Description
Error Name	Name of error.
Identifier	Each error is uniquely identified with an error ID that is represented as a Uniform Resource Identifier (URI).
Description	Description of the error.
State	State of the error. Values are: enabled or disabled.
Scope	Scope classification to which the error belongs. Values include board and pfe.
Category	Category subgroup under the scope level to which the error belongs. Values include: core, functional, io, memory, processing, storage, and switch.
Level	Severity level of the error.
Threshold	Configured threshold value. The associated detection and recovery actions are triggered when this value is exceeded.
Error Limit	The maximum number of times the error is reported.
Support	Support details for the error type.
Occur count	Number of times errors of a specific scope, category, and severity level has occurred.

Table 8: show system errors active Output Fields (Continued)

Field Name	Field Description
Clear count	Number of times error instances have been cleared.
Last occurred (ms ago)	Amount of time (in milliseconds) passed since the error last occurred.

Sample Output

show system errors active

For devices running Junos OS, output displays error details for FPC FRUs. For devices running Junos OS Evolved, output displays error details for FPC and other components such as fan, PSM, CB, and chassis.

```
user@host> show system errors active
```

```
System Active Errors Information
```

```
CB 0
```

```
-----
```

```
Active Minor Errors      : 0
```

```
Active Major Errors      : 0
```

```
Active Fatal Errors      : 0
```

```
CHASSIS 0
```

```
-----
```

```
Active Minor Errors      : 0
```

```
Active Major Errors      : 5
```

```
Active Fatal Errors      : 0
```

```
FAN 0
```

```
-----
```

```
Active Minor Errors      : 0
```

```
Active Major Errors      : 0
```

```
Active Fatal Errors      : 0
```

```
FAN 1
```

```
-----
```

```
Active Minor Errors      : 0
```

```
Active Major Errors      : 0
```

```
Active Fatal Errors      : 0
```


FAN 2

Active Minor Errors : 0
Active Major Errors : 0
Active Fatal Errors : 0

FAN 3

Active Minor Errors : 0
Active Major Errors : 0
Active Fatal Errors : 0

FAN 4

Active Minor Errors : 0
Active Major Errors : 0
Active Fatal Errors : 0

FPC 0

Active Minor Errors : 0
Active Major Errors : 0
Active Fatal Errors : 0

FPC 1

Active Minor Errors : 0
Active Major Errors : 0
Active Fatal Errors : 0

FPC 2

Active Minor Errors : 0
Active Major Errors : 0
Active Fatal Errors : 0

FPC 3

Active Minor Errors : 0
Active Major Errors : 0
Active Fatal Errors : 0

FPM 0

Active Minor Errors : 0
Active Major Errors : 0
Active Fatal Errors : 0

PDU 0

Active Minor Errors : 0

Active Major Errors : 0

Active Fatal Errors : 0

PICS 0

Active Minor Errors : 0

Active Major Errors : 0

Active Fatal Errors : 0

PICS 1

Active Minor Errors : 0

Active Major Errors : 0

Active Fatal Errors : 0

PSM 0

Active Minor Errors : 0

Active Major Errors : 0

Active Fatal Errors : 0

PSM 1

Active Minor Errors : 0

Active Major Errors : 0

Active Fatal Errors : 0

PSM 2

Active Minor Errors : 0

Active Major Errors : 0

Active Fatal Errors : 0

PSM 3

Active Minor Errors : 0

Active Major Errors : 0

Active Fatal Errors : 0

RE 0

Active Minor Errors : 0

Active Major Errors : 0

Active Fatal Errors : 0

SIB 0

Active Minor Errors : 0

Active Major Errors : 0

Active Fatal Errors : 0

SIB 1

```

-----
Active Minor Errors      : 0
Active Major Errors      : 0
Active Fatal Errors      : 0

```

show system errors active fpc-slot

```
user@host> show system errors active fpc-slot
```

```
0
```

```
System Active Errors Information
```

```
FPC 0
```

```
-----
Active Minor Errors: 0
```

```
Active Major Errors: 1
```

```
Active Fatal Errors: 0
```

show system errors active detail

```
user@host> show system errors active detail
```

```
System Active Errors Detail Information
```

```
CHASSIS 0
```

```
-----
Error Name : fan_tray_removal
```

```
Identifier : /chassis/0/hwdre/0/cm/0/fan_tray/Fan Tray 0/fan_tray_removal
```

```
Description : Fan_tray_absent
```

```
State : disabled
```

```
Scope : board
```

```
Category : functional
```

```
Level : major
```

```
Threshold : 1
```

```
Error limit : 1
```

```
Support : No help info provided
```

```
Occur count : 1
```

```
Clear count : 0
```

```
Last occurred(ms ago) : 339112691
```

Release Information

Command introduced in Junos OS Release 18.2R1.

RELATED DOCUMENTATION

show system errors count

show system errors error-id

[show system errors fru | 258](#)

show system errors count

IN THIS SECTION

- [Syntax | 253](#)
- [Description | 253](#)
- [Options | 253](#)
- [Required Privilege Level | 254](#)
- [Output Fields | 254](#)
- [Sample Output | 254](#)
- [Release Information | 254](#)

Syntax

```
show system errors count
```

Description

Display information collected by the J-Insight fault monitoring feature. Specifically, display information about the number of detected errors and recovery actions triggered based on error severity level.

Options

This command has no options.

Required Privilege Level

admin

Output Fields

Table 9 on page 254 lists the output fields for the `show system errors count` command. Output fields are listed in the approximate order in which they appear.

Table 9: show system errors count Output Fields

Field Name	Field Description
Level	Severity level of the error. Values are: Minor, Major, or Fatal.
Occurred	Number of times errors of a specific severity level occurred.
Cleared	Number of times errors of a specific severity level were cleared.
Action-Taken	Number of times a recovery action was triggered for a specific severity level.

Sample Output

show system errors count

```

user@host> show system errors count
Level   Occurred   Cleared     Action-Taken
-----
Minor:  0         0           0
Major:   1         0           1
Fatal:   0         0           0

```

Release Information

Command introduced in Junos OS Release 18.2R1.

RELATED DOCUMENTATION

[*show system errors active*](#)

[*show system errors error-id*](#)

[show system errors fru | 258](#)

show system errors error-id

IN THIS SECTION

- [Syntax | 255](#)
- [Description | 255](#)
- [Options | 255](#)
- [Additional Information | 256](#)
- [Required Privilege Level | 256](#)
- [Output Fields | 256](#)
- [Sample Output | 257](#)
- [Release Information | 258](#)

Syntax

```
show system errors error-id error-id-uri
```

Description

Display information collected by the J-Insight fault monitoring feature. Specifically, display information about detected errors based on the error ID Uniform Resource Identifier (URI). For devices running Junos OS Evolved, output displays only errors that have occurred at least once in the system.

Options

This command has no options.

Additional Information

Required Privilege Level

admin

Output Fields

Table 10 on page 256 lists the output fields for the `show system errors error-id` command. Output fields are listed in the approximate order in which they appear.

Table 10: show system errors error-id Output Fields

Field Name	Field Description
Error Name	Name of error.
Identifier	Each error is uniquely identified with an error ID that is represented as a Uniform Resource Identifier (URI).
Description	Description of the error.
State	State of the error. Values are: enabled or disabled.
Scope	Scope classification to which the error belongs. Values include board and pfe.
Category	Category subgroup under the scope level to which the error belongs. Values include: core, functional, io, memory, processing, storage, and switch.
Level	Severity level of the error.
Threshold	Configured threshold value. The associated detection and recovery actions are triggered when this value is exceeded.
Error Limit	The maximum number of times the error is reported.

Table 10: show system errors error-id Output Fields (Continued)

Field Name	Field Description
Support	Support details for the error type.
Occur count	Number of times errors of a specific scope, category, and severity level has occurred.
Clear count	Number of times error instances have been cleared.
Last occurred (ms ago)	Amount of time (in milliseconds) passed since the error last occurred.

Sample Output

show system errors error-id

```

user@host> show system errors error-id "/chassis/0/hwdre/0/cm/0/fan_tray/Fan
Tray 0/fan_tray_removal"
System Errors Detail Information
CHASSIS 0
-----
Error Name           : fan_tray_removal
Identifier            : /chassis/0/hwdre/0/cm/0/fan_tray/Fan Tray 0/fan_tray_removal
Description          : Fan_tray_absent
State                 : enabled
Scope                 : board
Category              : functional
Level                 : major
Threshold             : 1
Error limit           : 1
Support               : No help info provided
Occur count           : 1
Clear count           : 0
Last occurred(ms ago) : 84091182

```


Release Information

Command introduced in Junos OS Release 19.1R1.

RELATED DOCUMENTATION

show system errors active

show system errors count

[show system errors fru](#) | 258

show system errors fru

IN THIS SECTION

- [Syntax](#) | 258
- [Description](#) | 258
- [Options](#) | 259
- [Required Privilege Level](#) | 259
- [Output Fields](#) | 259
- [Sample Output \(Junos OS\)](#) | 260
- [Sample Output \(Junos OS Evolved\)](#) | 262
- [Release Information](#) | 264

Syntax

```
show system errors fru detail [fru slot-number]
```

Description

Display information collected by the J-Insight fault monitoring feature. Specifically, display information about detected errors based on the FRU.

Options

none	Display a brief summary of the system error information for the FRU.
detail	(Optional) Display detailed system error information.
<i>fru slot-number</i>	(Optional) Display system error information for a specific FRU. For devices running Junos OS, output displays error details for FPC FRUs. For devices running Junos OS Evolved, output displays error details for FPC and other components such as fan, PSM, CB, and chassis.

Required Privilege Level

admin

Output Fields

[Table 11 on page 259](#) lists the output fields for the `show system errors fru` command. Output fields are listed in the approximate order in which they appear.

Table 11: show system errors fru Output Fields

Field Name	Field Description
FRU	FRU identification number.
Scope	An error scope provides a level of classification above error category. Error scope values are: pfe and board.
Category	An error category categorizes errors into various subgroups under a specific error scope level. Values include: functional, io, memory, processing, storage, and switch.
Level	Severity level of the error.
Occurred	Number of times errors of a specific scope, category, and severity level has occurred.

Table 11: show system errors fru Output Fields (Continued)

Field Name	Field Description
Cleared	Number of times errors of a specific scope, category, and severity level were cleared.
Threshold	Configured threshold value. The associated detection and recovery actions are triggered when this value is exceeded.
Action-Taken	Number of times a user-configured recovery action was triggered for errors of a specific scope, category, and severity level.
Action	Action that is triggered when the threshold value is exceeded.

Sample Output (Junos OS)**show system errors fru detail**

```
user@host> show system errors fru detail
```

Fru	Scope	Category	Level	Occurred	Cleared	Threshold	Action-Taken	Action
FPC 0								
	board							
		functional	Minor	0	0	10	0	LOG
			Major	0	0	1	0	GET
			Fatal	0	0	1	0	DISABLE
STATE CM ALARM								
PFE		memory	Minor	0	0	10	0	LOG
			Major	0	0	1	0	GET
			Fatal	0	0	1	0	DISABLE
STATE CM ALARM								
PFE		io	Minor	0	0	10	0	LOG
			Major	0	0	1	0	GET
			Fatal	0	0	1	0	DISABLE
STATE CM ALARM								
PFE								

STATE CM ALARM	storage	Minor	0	0	10	0	LOG
		Major	0	0	1	0	GET
		Fatal	0	0	1	0	DISABLE
PFE							
STATE CM ALARM	switch	Minor	0	0	10	0	LOG
		Major	0	0	1	0	GET
		Fatal	0	0	1	0	DISABLE
PFE							
STATE CM ALARM	processing	Minor	0	0	10	0	LOG
		Major	0	0	1	0	GET
		Fatal	0	0	1	0	DISABLE
PFE							
STATE CM ALARM	functional	Minor	0	0	10	0	LOG
		Major	0	0	1	0	GET
		Fatal	0	0	1	0	DISABLE
PFE							
STATE CM ALARM	memory	Minor	0	0	10	0	LOG
		Major	0	0	1	0	GET
		Fatal	0	0	1	0	DISABLE
PFE							
STATE CM ALARM	io	Minor	0	0	10	0	LOG
		Major	0	0	1	0	GET
		Fatal	0	0	1	0	DISABLE
PFE							
STATE CM ALARM	storage	Minor	0	0	10	0	LOG
		Major	0	0	1	0	GET
		Fatal	0	0	1	0	DISABLE
PFE							
STATE CM ALARM	switch	Minor	0	0	10	0	LOG
		Major	0	0	1	0	GET
		Fatal	0	0	1	0	DISABLE
PFE							
STATE CM ALARM	processing	Minor	0	0	10	0	LOG
		Major	0	0	1	0	GET
		Fatal	0	0	1	0	DISABLE

STATE CM ALARM						
	Fatal	0	0	1	0	DISABLE
PFE						

Sample Output (Junos OS Evolved)

show system errors fru detail (PTX10003)

The following output has been shortened for clarity. For each part of a FRU, the full output displays any errors in the functional, io, memory, processing, storage, and switch categories, similar to the CB 0 FRU below.

```
user@host> show system errors fru detail
```

Fru	Scope	Category	Level	Occurred	Cleared	Threshold	Action-Taken	Action
CB 0								
	board							
		functional	Minor	0	0	10	0	LOG
			Major	0	0	1	0	GET
STATE CM ALARM			Fatal	0	0	1	0	CM ALARM
RESET								
		io	Minor	0	0	10	0	LOG
			Major	0	0	1	0	GET
STATE CM ALARM			Fatal	0	0	1	0	CM ALARM
RESET								
		memory	Minor	0	0	10	0	LOG
			Major	0	0	1	0	GET
STATE CM ALARM			Fatal	0	0	1	0	CM ALARM
RESET								
		processing	Minor	0	0	10	0	LOG
			Major	0	0	1	0	GET
STATE CM ALARM			Fatal	0	0	1	0	CM ALARM
RESET								
		storage	Minor	0	0	10	0	LOG
			Major	0	0	1	0	GET
STATE CM ALARM			Fatal	0	0	1	0	CM ALARM

RESET							
	switch	Minor	0	0	10	0	LOG
		Major	0	0	1	0	GET
STATE CM ALARM							
		Fatal	0	0	1	0	CM ALARM
RESET							
CHASSIS 0							
board							
...							
FAN 0							
board							
...							
FAN 1							
board							
...							
FPC 0							
board							
...							
pfe							
...							
FPC 1							
board							
...							
pfe							
...							
FPM 0							
board							
...							
PDU 0							
board							
...							
PICS 0							
board							
...							
PICS 1							
board							
...							
PSM 0							
board							
...							
PSM 1							

```

        board
    ...
RE 0
        board
    ...
SIB 0
        board
    ...
        switch
    ...
SIB 1
        board
    ...
        switch
    ...

```

Release Information

Command introduced in Junos OS Release 18.2R1.

RELATED DOCUMENTATION

show system errors active

show system errors count

show system errors error-id

show system errors inactive

IN THIS SECTION

- [Syntax | 265](#)
- [Description | 265](#)
- [Options | 265](#)
- [Required Privilege Level | 265](#)
- [Output Fields | 265](#)

- [Sample Output | 267](#)
- [Release Information | 271](#)

Syntax

```
show system errors inactive
<detail>
```

Description

Display information collected by the J-Insight fault monitoring feature. Specifically, display summary or detailed information about the inactive errors in the system. This commands shows the information about errors that had occurred and were then cleared.

Options

- none** Display a brief summary of the system error information for all applicable FRUs.
- detail** (Optional) Display detailed system error information.

Required Privilege Level

admin

Output Fields

[Table 12 on page 265](#) list the output fields for the `show system errors inactive` command. Output fields are listed in the approximate order in which they appear.

Table 12: show system errors inactive Output Fields

Field Name	Field Description
Error Name	Name of error.

Table 12: show system errors inactive Output Fields (Continued)

Field Name	Field Description
Identifier	Each error is uniquely identified with an error ID that is represented as a Uniform Resource Identifier (URI).
Description	Description of the error.
State	State of the error. Values are: enabled or disabled.
Scope	Scope classification to which the error belongs. Values include board and pfe.
Category	Category subgroup under the scope level to which the error belongs. Values include: core, functional, io, memory, processing, storage, and switch.
Level	Severity level of the error.
Threshold	Configured threshold value. The associated detection and recovery actions are triggered when this value is exceeded.
Error Limit	The maximum number of times the error is reported.
Support	Support details for the error type.
Occur count	Number of times errors of a specific scope, category, and severity level has occurred.
Clear count	Number of times error instances have been cleared.
Last occurred (ms ago)	Amount of time (in milliseconds) passed since the error last occurred.

Sample Output

show system errors inactive

```
user@host> show system errors inactive
```

```
System Inactive Errors Information
```

```
CB 0
```

```
-----
Inactive Minor Errors      : 0
Inactive Major Errors      : 0
Inactive Fatal Errors      : 0
```

```
CB 1
```

```
-----
Inactive Minor Errors      : 0
Inactive Major Errors      : 0
Inactive Fatal Errors      : 0
```

```
CHASSIS 0
```

```
-----
Inactive Minor Errors      : 0
Inactive Major Errors      : 0
Inactive Fatal Errors      : 0
```

```
FAN 0
```

```
-----
Inactive Minor Errors      : 0
Inactive Major Errors      : 0
Inactive Fatal Errors      : 0
```

```
FAN 1
```

```
-----
Inactive Minor Errors      : 0
Inactive Major Errors      : 0
Inactive Fatal Errors      : 0
```

```
FPC 0
```

```
-----
Inactive Minor Errors      : 0
Inactive Major Errors      : 0
Inactive Fatal Errors      : 0
```

```
FPC 1
```

```
-----
Inactive Minor Errors      : 0
Inactive Major Errors      : 0
Inactive Fatal Errors      : 0
```

```
FPC 2
```

```

-----
Inactive Minor Errors      : 0
Inactive Major Errors      : 0
Inactive Fatal Errors      : 0
FPC 3

```

```

-----
Inactive Minor Errors      : 0
Inactive Major Errors      : 0
Inactive Fatal Errors      : 0
FPC 4

```

```

-----
Inactive Minor Errors      : 0
Inactive Major Errors      : 0
Inactive Fatal Errors      : 0
FPC 5

```

```

-----
Inactive Minor Errors      : 0
Inactive Major Errors      : 0
Inactive Fatal Errors      : 0
FPC 6

```

```

-----
Inactive Minor Errors      : 0
Inactive Major Errors      : 0
Inactive Fatal Errors      : 0
FPC 7

```

```

-----
Inactive Minor Errors      : 0
Inactive Major Errors      : 0
Inactive Fatal Errors      : 0
FPM 0

```

```

-----
Inactive Minor Errors      : 0
Inactive Major Errors      : 0
Inactive Fatal Errors      : 0
PICS 0

```

```

-----
Inactive Minor Errors      : 0
Inactive Major Errors      : 0
Inactive Fatal Errors      : 0
PSM 0

```

```

-----
Inactive Minor Errors      : 0
Inactive Major Errors      : 0

```

Inactive Fatal Errors : 0

PSM 1

Inactive Minor Errors : 0

Inactive Major Errors : 0

Inactive Fatal Errors : 0

PSM 2

Inactive Minor Errors : 0

Inactive Major Errors : 0

Inactive Fatal Errors : 0

PSM 3

Inactive Minor Errors : 0

Inactive Major Errors : 0

Inactive Fatal Errors : 0

PSM 4

Inactive Minor Errors : 0

Inactive Major Errors : 0

Inactive Fatal Errors : 0

PSM 5

Inactive Minor Errors : 0

Inactive Major Errors : 0

Inactive Fatal Errors : 0

RE 0

Inactive Minor Errors : 0

Inactive Major Errors : 0

Inactive Fatal Errors : 0

RE 1

Inactive Minor Errors : 0

Inactive Major Errors : 0

Inactive Fatal Errors : 0

SIB 0

Inactive Minor Errors : 0

Inactive Major Errors : 3

Inactive Fatal Errors : 0

SIB 1

```

Inactive Minor Errors      : 0
Inactive Major Errors     : 0
Inactive Fatal Errors     : 0
SIB 2
-----

```

```

Inactive Minor Errors      : 0
Inactive Major Errors     : 0
Inactive Fatal Errors     : 0
SIB 3
-----

```

```

Inactive Minor Errors      : 0
Inactive Major Errors     : 0
Inactive Fatal Errors     : 0
SIB 4
-----

```

```

Inactive Minor Errors      : 0
Inactive Major Errors     : 0
Inactive Fatal Errors     : 0
SIB 5
-----

```

```

Inactive Minor Errors      : 0
Inactive Major Errors     : 0
Inactive Fatal Errors     : 0

```

show system errors inactive detail

```
user@host> show system errors inactive detail
```

```
System Inactive Errors Detail Information
```

```
SIB 0
```

```

-----
Error Name      : Cell_drop_errors
Identifier      : /sib/0/fabspoked-fchip/0/cm/0/fchip/0/Cell_drop_errors
Description     : Cell drop errors
State          : enabled
Scope          : board
Category       : internal
Level          : major
Threshold      : 10
Error limit    : 0
Support        : No help info provided
Occur count    : 1

```

```

Clear count          : 1
Last occurred(ms ago) : 973151
System Inactive Errors Detail Information
SIB 0
-----
Error Name           : Sib_Asic_PIO_Fault
Identifier            : /sib/0/fabspoked-fchip/0/cm/0/fchip/0/Sib_Asic_PIO_Fault
Description           : Sib Asic PIO Fault
State                : enabled
Scope                : switch
Category             : internal
Level                : major
Threshold             : 10
Error limit          : 0
Support              : No help info provided
Occur count          : 1
Clear count          : 1
Last occurred(ms ago) : 777971
System Inactive Errors Detail Information
SIB 0
-----
Error Name           : sib_link_to_fpc_fault
Identifier            : /sib/0/fabspoked-fchip/0/cm/0/fchip/0/sib_link_to_fpc_fault
Description           : sib_link_to_fpc_fault
State                : enabled
Scope                : board
Category             : internal
Level                : major
Threshold             : 10
Error limit          : 0
Support              : No help info provided
Occur count          : 1
Clear count          : 1
Last occurred(ms ago) : 862333

```

Release Information

Command introduced in Junos OS Evolved Release 19.4R1.

RELATED DOCUMENTATION

[*show system errors count*](#)

[*show system errors error-id*](#)

[show system errors fru | 258](#)

show system errors history

IN THIS SECTION

- [Syntax | 272](#)
- [Description | 272](#)
- [Options | 273](#)
- [Required Privilege Level | 273](#)
- [Output Fields | 273](#)
- [Sample Output | 274](#)
- [Release Information | 275](#)

Syntax

```
show chassis errors history
<cb slot| ccg slot | fan slot | fpc slot | psm slot | re slot | sib slot>
```

Description

Display information about cleared faults in the error history buffer. You can display history for all errors or the errors for one system component. The error history is displayed in chronological order and includes a description of each PFE and FCHIP fault and when the fault was raised and cleared.

NOTE: For Junos OS Evolved, only the QFX5200 supports this command. For all other Junos OS Evolved platforms, use the [show system errors active](#), [show system errors count](#), [show system errors error-id](#), or [show system errors fru](#) command.

Options

This command has no options.

Required Privilege Level

view

Output Fields

[Table 13 on page 273](#) lists the output fields for the `show system errors history` command. Output fields are listed in the approximate order in which they appear.

Table 13: show system errors history Output Fields

Field Name	Field Description
<i>Fault (module, error-id, board-name/component-name, PFE-or-FCHIP)</i>	Information about the fault.
Group	Fault severity level is Fatal, Major, or Minor.
Scope	Affected scope of fault is System, Component, Board, or Link.
Corr-enabled	Correlation with fault is always enabled, Y.
Raised	Time the fault was raised, in the format yyyy-mm-dd hh:nn:ss.!!! TMZ, where nn is minutes, !!! is milliseconds, and TMZ is time zone.
Desc	Description of the fault.

Table 13: show system errors history Output Fields (Continued)

Field Name	Field Description
Cleared	Time the fault was cleared, in the format yyyy-mm-dd hh:nn:ss.!!! TMZ, where nn is minutes, !!! is milliseconds, and TMZ is time zone.

Sample Output

show system errors history

```

user@host> show system errors history
Fault: {pechip, 1487, /Chassis[0]/Fpc[4], Fchip[0]}
Group:  Major          Scope: Link          Corr-enabled: Y
Raised:  2017-04-19 18:18:48.652000 PDT
Desc:    Fabric Down condition on PFE
Cleared: 2017-04-19 18:18:49.474975 PDT
Fault: {pechip, 1487, /Chassis[0]/Fpc[4], Fchip[1]}
Group:  Major          Scope: Link          Corr-enabled: Y
Raised:  2017-04-19 18:18:48.653000 PDT
Desc:    Fabric Down condition on PFE
Cleared: 2017-04-19 18:18:49.474668 PDT
Fault: {pechip, 1487, /Chassis[0]/Fpc[4], Fchip[2]}
Group:  Major          Scope: Link          Corr-enabled: Y
Raised:  2017-04-19 18:18:48.654000 PDT
Desc:    Fabric Down condition on PFE
Cleared: 2017-04-19 18:18:49.474245 PDT
Fault: {pechip, 1487, /Chassis[0]/Fpc[4], Fchip[3]}
Group:  Major          Scope: Link          Corr-enabled: Y
Raised:  2017-04-19 18:18:48.654000 PDT
Desc:    Fabric Down condition on PFE
Cleared: 2017-04-19 18:18:49.210875 PDT
Fault: {pechip, 1143, /Chassis[0]/Fpc[4], Pfe[0]}
Group:  Major          Scope: Component     Corr-enabled: N
Raised:  2017-04-19 18:18:57.533000 PDT
Desc:    hostif_local_int_wnack0
Fault: {pechip, 1487, /Chassis[0]/Fpc[4], Fchip[0]}
Group:  Major          Scope: Link          Corr-enabled: Y
Raised:  2017-04-19 19:45:20.949000 PDT

```

Desc: Fabric Down condition on PFE
Cleared: Active

Release Information

Command introduced in Junos OS Evolved Release 18.3R1.

RELATED DOCUMENTATION

| [show system errors](#) | [241](#)

show system rollback

IN THIS SECTION

- [Syntax](#) | [275](#)
- [Description](#) | [275](#)
- [Options](#) | [276](#)
- [Required Privilege Level](#) | [276](#)
- [Sample Output](#) | [276](#)
- [Release Information](#) | [277](#)

Syntax

```
show system rollback number  
<compare number | configuration-revision>
```

Description

This command displays the contents of a previously committed configuration, or the differences between two previously committed configurations.

The `show system rollback` command is a operational mode command and cannot be issued with `run` from the configuration mode.

Options

<i>number</i>	Number of a configuration to view. The output displays the configuration. The range of values is 0 through 49.
<i>compare number</i>	(Optional) Number of another previously committed (rollback) configuration to compare to rollback <i>number</i> . The output displays the differences between the two configurations. The range of values is 0 through 49.
<i>configuration-revision</i>	(Optional) Display corresponding configuration revision for this rollback number.

Required Privilege Level

view

Sample Output

show system rollback compare

```
user@host> show system rollback 3 compare 1
[edit]
+ interfaces {
+   ge-1/1/1 {
+     unit 0 {
+       family inet {
+         filter {
+           input mf_plp;
+         }
+         address 10.1.1.1/10;
+       }
+     }
+   }
+   ge-1/2/1 {
+     unit 0 {
+       family inet {
+         filter {
+           input mf_plp;
```

```

+         }
+         address 10.1.1.1/10;
+     }
+ }
+ ge-1/3/0 {
+     unit 0 {
+         family inet {
+             filter {
+                 input mf_plp;
+             }
+             address 10.1.1.1/10;
+         }
+     }
+ }
+ }
+}

```

show system rollback configuration-revision

```

user@host> show system rollback 0 configuration-revision
The corresponding configuration revision is: re0-1596379942-3

```

Release Information

Command introduced before Junos OS Release 7.4.

Option configuration-revision introduced in Junos OS Release 20.4R1 and Junos OS Evolved Release 20.4R1.

show system snapshot (Junos OS Evolved)

IN THIS SECTION

- [Syntax | 278](#)
- [Description | 278](#)
- [Options | 278](#)

- [Required Privilege Level | 278](#)
- [Output Fields | 278](#)
- [Sample Output | 278](#)

Syntax

```
show system snapshot
```

Description

This command displays information about the backup software—the contents of the **/soft** directory, which includes the running version of Junos OS Evolved. When nodes are synchronized in a cluster, this command shows what versions are available on all nodes in the cluster that contain persistent storage.

To back up the software, use the `request system snapshot` command.

Options

There are no options for this command.

Required Privilege Level

view

Output Fields

When you issue this command, you see a list of the snapshots available on each node.

Sample Output

show system snapshot (Junos OS Evolved)

```
user@host-re0> show system snapshot
-----
node: re0
```

```

-----
Current snapshot device: /dev/sdb
Snapshot boot device: sdb
List of installed version(s) in Snapshot boot device sdb:

[1]  < junos-evo-install-ptx-x86-64-20.4-202103151803.0-EVO - [2021-03-16 15:09:46]
[2]   junos-evo-install-ptx-x86-64-20.4-202103111254.0-EVO - [2021-03-16 15:10:32]
[3] -> junos-evo-install-ptx-x86-64-20.4-202103150459.0-EVO - [2021-03-16 15:07:49]
[4]   junos-evo-install-ptx-x86-64-20.4-202103141559.0-EVO - [2021-03-16 15:11:52]

    '-' running version
    '>' next boot version after upgrade/downgrade
    '<' rollback boot version
-----
node: re1
-----
Current snapshot device: /dev/sdb
Snapshot boot device: sdb
List of installed version(s) in Snapshot boot device sdb:

[1] -> junos-evo-install-ptx-x86-64-20.4-202103051234.0-EVO - [2021-03-05 01:10:31]

    '-' running version
    '>' next boot version after upgrade/downgrade
    '<' rollback boot version

```

RELATED DOCUMENTATION

| [request system snapshot \(Junos OS Evolved\)](#) | 186

show system software add-restart (Junos OS Evolved)

IN THIS SECTION

- [Syntax](#) | 280
- [Description](#) | 280

- [Required Privilege Level | 280](#)
- [Output Fields | 280](#)
- [Sample Output | 280](#)

Syntax

```
show system software  
<add-restart>
```

Description

Display all console messages from the last in-service software upgrade (ISSU).

Required Privilege Level

maintenance

Output Fields

When you enter this command, the output shows a list of console messages from the last in-service software upgrade (ISSU).

Sample Output

show system software add-restart (no Log File Found)

```
user@host> show system software add-restart  
-----  
node: re0  
-----  
Software ISSU upgrade log file not found
```

show system software add-restart (with Log Information)

```

user@host-re0> show system software add-restart
-----
node: re0
-----
2021-04-10 22:31:26 Adding software images. This process can take several minutes. Please be
patient...
2021-04-10 22:31:26 Download and Validate in Progress
2021-04-10 22:33:09 re0: Starting upgrade : /var/tmp/sharat/snapshot/ptx-J4.iso
2021-04-10 22:33:09 re0: Upgrade version : junos-evo-install-ptx-x86-64-21.1I20210410155013-EVO-
J4
2021-04-10 22:33:30 re0: Running prechecks for JSU image...
2021-04-10 22:33:30 re0: JSU base release 21.1I20210410155013-EVO matches with Current Release:
21.1I20210410155013-EVO.
2021-04-10 22:33:30 re0: Starting JSU package installation...
2021-04-10 22:33:30 re0: Copying Files from base version junos-evo-install-ptx-
x86-64-21.1I20210410155013-EVO-J3 ...
2021-04-10 22:33:32 re0: Copying Files from JSU image...
2021-04-10 22:33:34 re0: Signing files...
2021-04-10 22:33:36 re0: Running pre-checks for 'junos-evo-install-ptx-
x86-64-21.1I20210410155013-EVO-J4'
2021-04-10 22:33:58 re0: Pre-checks pass successfully, copying files to software area
2021-04-10 22:34:26 re0: Running post install commands...
2021-04-10 22:34:33 re0: Post install sequence was successful.
2021-04-10 22:34:33 re0: Validating existing configs. See /var/log/validation_config.log for
config validation logs.
2021-04-10 22:35:22 re0: Validation Passed
2021-04-10 22:35:22 re0: Going ahead with Installation
2021-04-10 22:35:43 re0: Boot version is now 'junos-evo-install-ptx-x86-64-21.1I20210410155013-
EVO-J4'
2021-04-10 22:36:00 re1: Running pre-checks for 'junos-evo-install-ptx-
x86-64-21.1I20210410155013-EVO-J4'
2021-04-10 22:36:04 re1: Pre-checks pass successfully, copying files to software area
2021-04-10 22:36:43 re1: Running post install commands...
2021-04-10 22:36:51 re1: Post install sequence was successful.
2021-04-10 22:37:10 re1: Boot version is now 'junos-evo-install-ptx-x86-64-21.1I20210410155013-
EVO-J4'
2021-04-10 22:37:23 re0: Updating all nodes...
2021-04-10 22:38:23 re0: Boot version is now 'junos-evo-install-ptx-x86-64-21.1I20210410155013-
EVO-J3'
2021-04-10 22:38:23 re0: Removing version junos-evo-install-ptx-x86-64-21.1I20210410155013-EVO-

```



```

J4...
2021-04-10 22:38:24 re0: One or more remote node(s) failed updating
2021-04-10 22:38:38 re1: Boot version is now 'junos-evo-install-ptx-x86-64-21.1I20210410155013-EVO-J3'
2021-04-10 22:38:38 re1: Removing version junos-evo-install-ptx-x86-64-21.1I20210410155013-EVO-J4...
2021-04-10 22:38:51 ERROR: Upgrade failed on current RE. Node:re0 Image: re0:/var/tmp/user/snapshot/ptx-J4.iso
2021-04-10 22:38:51 Validation and download failed. Aborting upgrade.

```

show system software list

IN THIS SECTION

- [Syntax | 282](#)
- [Description | 282](#)
- [Required Privilege Level | 283](#)
- [Output Fields | 283](#)
- [Sample Output | 283](#)
- [Release Information | 285](#)

Syntax

```
show system software list
```

Description

This command displays all the software versions in the persistent storage on the Routing Engines in the system and displays the current software version running on the FPCs. FPCs cannot store more than one version, because FPCs do not contain any persistent storage media.

Required Privilege Level

view

Output Fields

For a description of the output fields, see [Table 14 on page 283](#). Output fields are listed in the approximate order in which they appear.

Table 14: show system software list Output Fields

Field Name	Description
node	Name of the node.
List of installed version(s)	<p>Ordered list of software that is or has been installed on the node:</p> <ul style="list-style-type: none">• - indicates the running software version.• > indicates the next boot software version, which occurs only after an upgrade or a downgrade. If no upgrade or downgrade has been performed, the > symbol will not appear in the list of installed versions.• < indicates the rollback boot software version if there is one.

Sample Output

show system software list

```
user@host-re0> show system software list
-----
node: fpc0
-----
Active boot device is primary: /dev/ram1
List of installed version(s) :

    '-' running version
    '>' next boot version after upgrade/downgrade
    '<' rollback boot version
```

```

- junos-evo-install-ptx-x86-64-20.4R2.4-EVO - [2021-04-14 10:33:31]
-----
node: re0
-----
Active boot device is primary: /dev/sda
List of installed version(s) :

    '-' running version
    '>' next boot version after upgrade/downgrade
    '<' rollback boot version

- junos-evo-install-ptx-x86-64-20.4R2.4-EVO - [2021-04-14 10:22:52]
< junos-evo-install-ptx-x86-64-20.4R2.5-EVO - [2021-04-14 09:49:28]
  junos-evo-install-ptx-x86-64-20.4R2.3-EVO - [2021-04-13 12:17:55]
-----
node: re1
-----
Active boot device is primary: /dev/sda
List of installed version(s) :

    '-' running version
    '>' next boot version after upgrade/downgrade
    '<' rollback boot version

- junos-evo-install-ptx-x86-64-20.4R2.4-EVO - [2021-04-14 10:24:55]
< junos-evo-install-ptx-x86-64-20.4R2.5-EVO - [2021-04-14 09:49:28]
  junos-evo-install-ptx-x86-64-20.4R2.3-EVO - [2021-04-14 10:01:58]

```

show system software list (Junos OS Evolved with Support for Hotfix and JSU Upgrade)

```

user@host-re0> show system software list | no-more
-----
node: fpc0
-----
Active boot device is primary: /dev/ram1
List of installed version(s) :

    '-' running version
    '>' next boot version after upgrade/downgrade
    '<' rollback boot version
    '*' deleted JSU version

```

```

-   junos-evo-install-ptx-x86-64-21.2I20210510171915-EVO_20210510171915-J2 - [2021-05-11
00:38:49]
-----
node: re0
-----
Active boot device is primary: /dev/vda
List of installed version(s) :

    '-' running version
    '>' next boot version after upgrade/downgrade
    '<' rollback boot version
    '*' deleted JSU version

-   junos-evo-install-ptx-x86-64-21.2I20210510171915-EVO_20210510171915-J2 - [2021-05-11
00:35:58]
<   junos-evo-install-ptx-x86-64-21.2I20210510171915-EVO_20210510171915-J1.1 - [2021-05-11
00:23:49]
    junos-evo-install-ptx-x86-64-21.2I20210510235202-EVO_20210510171915 - [2021-05-11 00:04:15]
    junos-evo-install-ptx-x86-64-21.2I20210510171915-EVO_20210510171915 - [2021-05-10 21:59:25]
-----
node: re1
-----
Active boot device is primary: /dev/vda
List of installed version(s) :

    '-' running version
    '>' next boot version after upgrade/downgrade
    '<' rollback boot version
    '*' deleted JSU version

-   junos-evo-install-ptx-x86-64-21.2I20210510171915-EVO_20210510171915-J2 - [2021-05-11
00:37:25]
<   junos-evo-install-ptx-x86-64-21.2I20210510171915-EVO_20210510171915-J1.1 - [2021-05-11
00:25:14]
    junos-evo-install-ptx-x86-64-21.2I20210510235202-EVO_20210510171915 - [2021-05-11 00:05:58]
    junos-evo-install-ptx-x86-64-21.2I20210510171915-EVO_20210510171915 - [2021-05-10 21:59:38]

```

Release Information

Command introduced in Junos OS Evolved Release 18.3R1.

show system ztp

IN THIS SECTION

- [Syntax | 286](#)
- [Description | 286](#)
- [Required Privilege Level | 286](#)
- [Output Fields | 286](#)
- [Sample Output | 290](#)
- [Release Information | 291](#)

Syntax

```
show system ztp
```

Description

This command displays the Zero Touch Provisioning (ZTP) state information.

Required Privilege Level

view

Output Fields

For a description of the output fields, see [Table 15 on page 287](#). Output fields are listed in the approximate order in which they appear. The state field can have multiple settings. The rest of the fields are self explanatory based on DHCP arguments provided by the server.

Table 15: show system ztp Output Fields

Field Name	Description
ZtpState	<p>ZTP state field values for starting:</p> <ul style="list-style-type: none"> INITIALIZED—ZTP is initializing. STARTED—ZTP started running.
	<p>ZTP state field values for image download:</p> <ul style="list-style-type: none"> IMAGE_DOWNLOADING—ZTP is downloading the next software image. IMAGE_DOWNLOADED—ZTP is finished downloading the next software image. RETRY_IMAGE_DOWNLOAD—ZTP is retrying image download. IMAGE_NOT_FOUND—ZTP could not find the image at the specified location on the server.
	<p>ZTP state field values for configuration download:</p> <ul style="list-style-type: none"> CONFIG_DOWNLOADING—ZTP is downloading the configuration. CONFIG_DOWNLOADED—ZTP is finished downloading the configuration. RETRY_CONFIG_DOWNLOAD—ZTP is retrying configuration download. CONFIG_NOT_FOUND—ZTP could not find the configuration.
	<p>ZTP state field values for upgrading configuration:</p> <ul style="list-style-type: none"> IMAGE_CONFIG_UPGRADING—ZTP got an image and a configuration from the server. CONFIG_UPGRADING—ZTP is upgrading the configuration.

Table 15: show system ztp Output Fields *(Continued)*

Field Name	Description
	<p>ZTP state field values for upgrading image:</p> <ul style="list-style-type: none"> • <code>RETRY_IMAGE_UPGRADE</code>—ZTP is retrying image upgrade. • <code>IMAGE_CONFIG_UPGRADING</code>—ZTP got an image and a configuration from the server. • <code>IMAGE_UPGRADING</code>—ZTP is downloading the image. • <code>IMAGE_UPGRADED</code>—ZTP is finished upgrading the image.
	<p>ZTP state field values for scripts:</p> <ul style="list-style-type: none"> • <code>SCRIPT_UPGRADING</code>—ZTP is running the script provided by server. • <code>SCRIPT_UPGRADED</code>—ZTP is finished upgrading the script. • <code>SCRIPT_UPGRADE_SUCCEEDED</code>—ZTP script upgrade finished with success. • <code>SCRIPT_UPGRADE_FAILED</code>—ZTP script upgrade finished with failure status.
	<p>ZTP state field values for reboot:</p> <ul style="list-style-type: none"> • <code>REBOOTING</code>—ZTP is rebooting the system. • <code>REBOOTED</code>—ZTP is finished rebooting the system.
	<p>ZTP state field values for configuration commit:</p> <ul style="list-style-type: none"> • <code>CONFIG_COMMIT_SUCCEEDED</code>—ZTP succeeded in committing user configuration. • <code>CONFIG_COMMIT_FAILED</code>—ZTP user configuration commit failed.

Table 15: show system ztp Output Fields (Continued)

Field Name	Description
	<p>ZTP state field values for finishing:</p> <ul style="list-style-type: none"> • FAILED—ZTP failed. • SUCCEEDED—ZTP succeeded.
ZtpInterface	Name of interface.
FtpIpAddr	IP address.
DefaultRouter	When the log server, NTP server, or FTP server are on a remote subnet, the value of DefaultRouter is used to configure a route to reach the servers.
LogServers	ZTP allows specification of a remote log server address. ZTP logs are then streamed to the remote log server.
NtpServers	ZTP allows specification of a remote NTP server address.
TransferMode	Options for TransferMode are ftp, tftp, http, or https
ImageFileType	It can be a symbolic link.
ConfigFileName	Configuration filename.
ConfigUrl	Configuration URL.
ConfigStatus	This field specifies whether the config file is downloading, is downloaded, or the download is being retried.

Table 15: show system ztp Output Fields (Continued)

Field Name	Description
ZtpRetryCount	If the ZTP state machine, which applies the image and configuration, fails, the number of retries attempted.
DhcpRetryCount	If the DHCP state machine, which fetches parameters for ZTP from the DHCP server, fails, the number of times it retries.
ZTP State History	Lists the last 10 state transitions by Time (date and time) and Description or which state it was in then.

Sample Output

show system ztp

```

user@host> show system ztp
Attribute      Value
-----
ZtpState       IMAGE_CONFIG_UPGRADING
ZtpInterface   vmb0
FtpIpAddr      10.10.213.1
HostName       sw-123
LogServers     [u'10.10.213.1']
NtpServers     [u'10.10.255.62', u'10.10.255.63']
TransferMode   tftp
ImageFileName  /ZTP_IMAGES/test.iso
ImageFileType  None
ImageUrl       tftp://17.17.213.1//ZTP_IMAGES/junos-evo-scapa.iso
ImageStatus    IMAGE_DOWNLOADED
ConfigFileName /ZTP_CONFIG/sw-123.cfg
ConfigUrl      tftp://10.10.213.1//ZTP_CONFIG/sw-123.cfg
ConfigStatus   CONFIG_DOWNLOADED
ZtpRetryCount  0
DhcpRetryCount 0

```

ZTP State History(last 10 transitions)

Time	Description
Fri Jun 5 22:35:40 2020	Started
Fri Jun 5 22:36:46 2020	Initialized
Fri Jun 5 22:37:08 2020	Discovering interfaces
Fri Jun 5 22:37:31 2020	Querying DHCP Server
Fri Jun 5 22:37:43 2020	DHCP query succeeded
Fri Jun 5 22:41:46 2020	Upgrading image and config

Release Information

Command introduced in Junos OS Evolved Release 19.1R1.

RELATED DOCUMENTATION

[Zero Touch Provisioning | 105](#)

show version (Junos OS Evolved)

IN THIS SECTION

- [Syntax | 292](#)
- [Description | 292](#)
- [Options | 292](#)
- [Required Privilege Level | 292](#)
- [Sample Output | 292](#)
- [Release Information | 293](#)

Syntax

```
show version

<node (all | node-name)>
```

Description

Display the hostname and the version information about the software running on the router or switch.

The output for the `show version` command for Junos OS Evolved includes a Junos field that indicates the installation package name. From the prefix of this package name, you can decode which Junos OS Evolved architecture the device is running.

Options

none	Display standard information about the hostname and version of the software running on the router or switch.
node (all <i>node-name</i>)	(Optional) Display version information for the specified node or all nodes.

Required Privilege Level

view

Sample Output

show version (with Third-party Applications Installed)

```
user@host-re0> show version
Hostname: host-re0
Model: ptx10008
Junos: 20.4R2.4-EV0
Yocto: 2.2.1
Linux Kernel: 4.8.28-WR2.2.1_standard-g4d37950
JUNOS-EVO OS 64-bit [junos-evo-install-ptx-x86-64-20.4R2.4-EV0]
SDK version: 5.6.7
External Software:
```

```
acmeMonitor-1.2.3 [sdk 5.6.7]
acmeLoadShare-3.4.5 [sdk 5.6.8]
```

show version node re0 (on a Dual-RE Device)

```
{master}
user@host-re0> show version node re0
Hostname: host-re0
Model: ptx10008
Junos: 20.4R2.4-EV0
Yocto: 2.2.1
Linux Kernel: 4.8.28-WR2.2.1_standard-g4d37950
JUNOS-EV0 OS 64-bit [junos-evo-install-ptx-x86-64-20.4R2.4-EV0]
```

show version node all

```
{master}
user@host-re0> show version node all
re0:
-----
Hostname: host-re0
Model: ptx10008
Junos: 20.4R2.4-EV0
Yocto: 2.2.1
Linux Kernel: 4.8.28-WR2.2.1_standard-g4d37950
JUNOS-EV0 OS 64-bit [junos-evo-install-ptx-x86-64-20.4R2.4-EV0]

re1:
-----
Hostname: host-re1
Model: ptx10008
Junos: 20.4R2.4-EV0
Yocto: 2.2.1
Linux Kernel: 4.8.28-WR2.2.1_standard-g4d37950
JUNOS-EV0 OS 64-bit [junos-evo-install-ptx-x86-64-20.4R2.4-EV0]
```

Release Information

node option introduced in Junos OS Evolved Release 18.3R1.