Release Notes

Published

2026-02-04

Junos OS Release 23.4R2®

Introduction

Junos OS runs on the following Juniper Networks® hardware: ACX Series, cSRX, EX Series, JRR Series, Juniper Secure Connect, MX Series, NFX Series, QFX Series, SRX Series Firewalls, vRR, and vSRX Virtual Firewall. These release notes accompany Junos OS Release 23.4R2. They describe new and changed features, limitations, and known and resolved problems in the hardware and software.

You can find release notes for all Junos OS releases at https://www.juniper.net/documentation/product/us/en/junos-os#cat=release_notes.

Engineering Simplicity

Table of Contents

Introduction

Junos OS runs on the following Juniper Networks® hardware: ACX Series, cRPD, cSRX, EX Series, JRR Series, Juniper Secure Connect, MX Series, NFX Series, QFX Series, SRX Series Firewall, vRR, and vSRX Virtual Firewall. These release notes accompany Junos OS Release 23.4R2. They describe new and changed features, limitations, and known and resolved problems in the hardware and software.

Junos OS Release Notes for ACX Series

IN THIS SECTION

What's New

There are no new features or enhancements to existing features in this release for ACX Series routers.

To view features supported on the ACX platforms, view the Feature Explorer using the following links. To see which features were added in Junos OS Release 23.4R2, click the Group by Release link. You can collapse and expand the list as needed.

- ACX710
- ACX5448-D
- ACX5448-M
- ACX5448

What's Changed

IN THIS SECTION

Learn about what changed in this release for ACX Series routers.

EVPN

- **Limit on number of IP address associations per MAC address per bridge domain in EVPN MAC-IP database**—By default, devices can associate a maximum of 200 IP addresses with a single MAC address per bridge domain. We provide a new CLI statement to customize this limit, `mac-ip-limit` statement at the `[edit protocols evpn]` hierarchy level. In most use cases, you do not need to change the default limit. If you want to change the default limit, we recommend that you do not set this limit to more than 300 IP addresses per MAC address per bridge domain. Otherwise, you might see very high CPU usage on the device, which can degrade system performance.

  [See mac-ip-limit.]

General Routing

- **MTU and TCP MSS not available on service interfaces (MX Series routers)**—You cannot configure the media MTU or TCP MSS on service interfaces (ms, vms, or ams).

  [See mtu (interfaces).]

- **Change in options and generated configuration for the EZ-LAG configuration IRB subnet-address statement**—With the EZ-LAG `subnet-address inet` or `subnet-address inet6` options at the `[edit services evpn evpn-vxlan irb *irb-instance*]` hierarchy, you can now specify multiple IRB subnet addresses in a single statement using the list syntax `addr1 addr2 ...` . Also, in the generated configuration for IRB interfaces, the commit script now includes default `router-advertisement` statements at the `[edit protocols]` hierarchy level for that IRB interface.

[See subnet-address (Easy EVPN LAG Configuration).]

- Starting from Junos 21.4R1 platforms with the following Routing Engines which have Intel CPUs with microcode version 0x35 observe the error warning, "000: **Firmware Bug**: TSC_DEADLINE disabled due to Errata; please update microcode to version: 0x3a (or later)" on the console. RE-S-X6-64G RE-S-X6-128G REMX2K-X8-64G RE-PTX-X8-64G RE-MX2008-X8-64G RE-MX2008-X8-128G

- For MPC5E line card with flexible-queuing-mode enabled, queue resources are shared between scheduler block 0 and 1. Resource monitor CLI output displays an equal distribution of the total available and used queues between scheduler blocks. This correctly represents the queue availability to the routing engine.

  [See https://uat.juniper.net/documentation/test/us/en/junos-24.2/software/junos/cli-reference/topics/ref/command/show-system-resource-monitor-summary.html and https://uat.juniper.net/documentation/test/us/en/junos-24.2/software/junos/cli-reference/topics/ref/command/show-system-resource-monitor-ifd-cos-queue-mapping-fpc.html]

- The topics in CVBC-Documented-In field have been updated to mention range.

Infrastructure

- **Option to disable path MTU discovery**—Path MTU discovery is enabled by default. To disable it for IPv4 traffic, you can configure the no-path-mtu-discovery statement at the [edit system internet-options] hierarchy level. To reenable it, use the `path-mtu-discovery` statement.

  [See Path MTU Discovery.]

Routing Protocols

- **Optimized mesh group routes (QFX5110, QFX5120, QFX5130, QFX5700 and ACX Series)**— `show route snooping` for inet.1/inet6.1 table and `show route snooping table inet.1/inet6.1` will display only CE mesh group routes for platforms that support EVPN-MPLS or EVPN-VXLAN multicast. In earlier releases, other mesh groups like the VE mesh group were also displayed.

VPNs

- **Increase in revert-delay timer range**— The `revert-delay` timer range is increased to 600 seconds from 20 seconds.

  [See min-rate.]

- **Configure min-rate for IPMSI traffic explicitly**— In a source-based MoFRR scenario, you can set a min-rate threshold for IPMSI traffic explicitly by configuring `ipmsi-min-rate` under `set routing-instances protocols mvpn hot-root-standby min-rate`. If not configured, the existing `min-rate` will be applicable to both IPMSI and SPMSI traffic.

  [See min-rate.]

Known Limitations

IN THIS SECTION

Learn about known limitations in this release for ACX Series routers.

For the most complete and latest information about known Junos OS defects, use the Juniper Networks online Junos Problem Report Search application.

Infrastructure

- When upgrading from releases before Junos OS Release 21.2 to Release 21.2 and later, validation and upgrade might fail. The upgrade requires using the `no-validate` option to complete successfully. PR1568757

Open Issues

IN THIS SECTION

Learn about open issues in this release for ACX Series routers.

For the most complete and latest information about known Junos OS defects, use the Juniper Networks online Junos Problem Report Search application.

General Routing

- In VPLS MH cases, the standby UNI ifl in backup router will be programmed in disable state, by adding the UNI interface to invalid vpn id in HW. During switch over the UNI ifl will be deleted and will be added under the VPLS instance VPN id. In issue case, UNI interface added under invalid VPN id in backup router is tried to deleted by passing the VPLS instance vpn id, causing the issue. This issue is applicable only for ACX5k series.PR1665178
- On ACX1K/2K platforms, when a lo0.x filter is configured under a vrf type routing-instance, any IPv4 transit traffic that makes ARP request to generate to the CE-facing interfaces will fail in ARP resolution due to the ARP request packets are discard by lo0.x filter if no specific term to accept the IPv4 packets. PR1737999
- On Junos ACX2200, the PTP(Precision Time Protocol) packets are not processed over GE (Gigabit Ethernet) interfaces after a reboot due to error in initialisation sequence of PTP. This impacts all functionalities associated with PTP as PTP packets are dropped.PR1755852
- Some Junos OS Releases from 21.4R3 to 22.4R3, might display the Remote fault state as 'Offline' in show interface by default. PR1764243
- On Junos ACX5448 device with SFP-T optics, speed displays wrong in CLI when executing `show interface` *`interface-name`* CLI command will display "Unspecified" speed. Speed value will not be updated properly. There is no traffic impact.PR1764303

- When restart chassis-control trigged on M/MX router has config with ccc instance, syslog is error out " Err] ACX_ASIC_PROGRAMMING_ERROR: pfe_dnx_translation_set: Error, bcm_vlan_port_translation_set rv:Entry not found ".PR1764966
- On ACX5048/ACX5096 platform, after the device is upgraded, disabling an interface and then rebooting the device will cause a critical issue. All interfaces will go down, resulting in a complete traffic drop. There is no known workaround to prevent this service interruption during the upgrade process.PR1786687
- ACX1100 PTP(enterprise profile) is stuck at freerun state after upgrading junos to 21.2R3PR1789694
- ACX710 does not recognize GPON OLT 740-124448 reports NON-JNPR after ACX power cycle. The same error state NON-JNPR can be observed when GPON OLT SFP is installed into ACX router.PR1801112
- Multicast route is reset every 5 mins with igmp receiver on acx2200 with small traffic loss. Multicast route that are not active would get reset after 5 minutes due to cahce timeout. This was happening even for active routes that had traffic.PR1805017

MPLS

- The default behavior of local reversion has changed from Junos OS Release 16.1 and that impacts the LSPs for which the ingress does not perform make-before-break. Junos OS does not perform make-before-break for no-cspf LSPs. PR1401800

Resolved Issues

IN THIS SECTION

Learn about the issues fixed in this release for ACX Series routers.

For the most complete and latest information about known Junos OS defects, use the Juniper Networks online Junos Problem Report Search application.

General Routing

- Packet Forwarding Engine may crash on ACX710 during init. PR1604346
- We may encounter jdhcpd core during initialization. The core in rare, and there is no service impact because of this core (as the process recovers immediately). PR1730717
- The rewrite rule stops working when classifier is attached to wildcard logical interface. PR1753411
- On a L3 interface default classifier is ipprec-compatibility, but after reboot another default classifier is taking effect - ieee8021p-default. PR1754547
- Interface flaps leading to Packet Forwarding Engine crash due to FPC heap corruption. PR1764083
- LACP packets are not forwarded after the reboot. PR1765478
- Traffic convergence is longer than usual after the CoS rewrite. PR1770491
- On ACX710/5448 with hierarchical-scheduler EVPN ETREE (Ethernet virtual private network Etree feature) leaf-to-leaf communication is allowed. PR1772177
- DHCP packets are getting relayed even after deleting the dhcp relay configuration from the leaf. PR1775275
- Link remains down after upgrading Junos image or changing the interface speed on Junos based ACX5448 platform. PR1775279
- Routing Engine CPLD firmware version displayed in ACX5448 is corrected. PR1776650
- Impact of Terrapin SSH Attack (CVE-2023-48795). PR1781732
- SyncE clock get stuck in 'none' or 'abort' state and impact PTP performance. PR1783632
- ACX710 CFM asynchronous-notification feature driven on CCC-down is not supported. PR1784447
- The KRT queue will be stuck on Junos ACX710 platform. PR1787707
- The egress ports on ACX710 incorrectly tagging traffic expected to be untagged over CCC/VPLS interfaces. PR1789949
- PICD core file can be seen during FPC is off-line/on-line, HA switch over, and system restart. PR1793824
- l2cricuit interface ccc "with Native-VLAN" configured do not add vlan-ID when receiving untag packet. PR1793829
- ACX node acting as ASBR+PE in MPLS Inter-AS Option B/C is not imposing VPN labels. PR1794718

- On ACX7059 and ACX7348 routers, jdhcpd core file is seen along with dfwd-junos-relay core file. PR1794843

- Port goes down after adding interface configuration and changing the port from 1g copper to 10g fiber. PR1794939

- Commit check failure will be reported when family ethernet-switching is configured on a EVPN ETREE/EVPN ELAN interface. PR1798425

- Acx-arm-feb core may be triggered if IGMP snooping is enabled and IGMP Query is received on the same port as IGMP join. PR1799619

Migration, Upgrade, and Downgrade Instructions

IN THIS SECTION

This section contains the upgrade and downgrade support policy for Junos OS for ACX Series routers. Upgrading or downgrading Junos OS might take several minutes, depending on the size and configuration of the network.

For information about software installation and upgrade, see the https://www.juniper.net/documentation/en_US/junos/information-products/pathway-pages/software-installation-and-upgrade/software-installation-and-upgrade.html Installation and Upgrade Guide.

Upgrade and Downgrade Support Policy for Junos OS Releases and Extended End-Of-Life Releases

We have two types of releases, standard EOL and EEOL:

- Standard End of Life (EOL) releases have engineering support for twenty four months after the first general availability date and customer support for an additional six more months.

- Extended End of Life (EEOL) releases have engineering support for sixty months after the first general availability date and customer support for an additional six more months.

NOTE: The sixty months of support for EEOL releases is introduced in Junos OS 23.2 release and is available for all later releases. For releases prior to 23.2, the support for EEOL releases continues to be thirty six months.

For both standard EOL and EEOL releases, you can upgrade to the next three subsequent releases or downgrade to the previous three releases.

For EEOL releases only, you have an additional option - you can upgrade directly from one EEOL release to the next two subsequent EEOL releases, even if the target release is beyond the next three releases. Likewise, you can downgrade directly from one EEOL release to the previous two EEOL releases, even if the target release is beyond the previous three releases.

Table 1: EOL and EEOL Releases

Release Type	End of Engineering (EOE)	End of Support (EOS)	Upgrade/ Downgrade to subsequent 3 releases	Upgrade/ Downgrade to subsequent 2 EEOL releases
Standard End of Life (EOL)	24 months	End of Engineering + 6 months	Yes	No
Extended End of Life (EEOL)	60 months	End of Engineering + 6 months	Yes	Yes

For more information about standard EOL and EEOL releases, see https://www.juniper.net/support/eol/junos.html.

For information about software installation and upgrade, see the Installation and Upgrade Guide.

Junos OS Release Notes for cSRX

IN THIS SECTION

What's New

There are no new features or enhancements to existing features in this release for cSRX.

What's Changed

There are no changes in behavior and syntax in this release for cSRX.

Known Limitations

There are no known limitations in hardware or software in this release for cSRX.

For the most complete and latest information about known Junos OS defects, use the Juniper Networks online Junos Problem Report Search application.

Open Issues

There are no known issues in hardware or software in this release for cSRX.

For the most complete and latest information about known Junos OS defects, use the Juniper Networks online Junos Problem Report Search application.

Resolved Issues

There are no resolved issues in this release for cSRX.

For the most complete and latest information about known Junos OS defects, use the Juniper Networks online Junos Problem Report Search application.

Junos OS Release Notes for EX Series

IN THIS SECTION

What's New in 23.4R2-S4

IN THIS SECTION

Learn about new features introduced in Junos OS 23.4R2-S4 release for EX Series.

Authentication and Access Control

GRES support for 802.1X protocol—You can ensure uninterrupted traffic flow during a Routing Engine failure using Graceful Routing Engine Switchover (GRES) support for the 802.1X protocol. The feature maintains client authentication states, preventing traffic loss and MAC learning disruptions. Use the CLI command show dot1x sync-pending-sessions to view unsynced authenticated sessions post-switchover and ensure proper session synchronization. This enhancement allows seamless transitions without client disconnections, ensuring continuous network access and stability.

[See https://www.juniper.net/documentation/us/en/software/junos/user-access/understanding-graceful-routing-engine-switchover-support-for-802.1X.html.]

What's New in 23.4R2

IN THIS SECTION

Learn about new features introduced in Junos OS 23.4R2 release for EX Series.

To view features supported on the EX platforms, view the Feature Explorer using the following links. To see which features were added in Junos OS Release 23.4R2, click the Group by Release link. You can collapse and expand the list as needed.

- EX2300
- EX2300-VC
- EX2300 Multigigabit
- EX3400
- EX3400-VC
- EX4100
- EX4100-F
- EX4300 Multigigabit
- EX4400
- EX4400 Multigigabit
- EX4400-24X
- EX4650-48Y
- EX9200

EVPN

- Enhanced OISM in EVPN-VXLAN ERB overlay networks with an IPv6 underlay (EX4100-48MP, EX4100-24MP, EX4100-48P, EX4100-48T, EX4100-24P, EX4100-24T, EX4100-F-48P, EX4100-F-24P, EX4100-F-48T, EX4100-F-24T, EX4100-F-12P, EX4100-F-12T, EX4400-24MP, EX4400-24P,

EX4400-24T, EX4400-24X, EX4400-48F, EX4400-48MP, EX4400-48P, EX4400-48T, EX4650, QFX5120-32C, QFX5120-48T, QFX5120-48Y, and QFX5120-48YM)—Starting in Junos OS Release 23.4R2, you can configure enhanced optimized intersubnet multicast (OISM) for IPv4 and IPv6 multicast data traffic with an Ethernet VPN–Virtual Extensible LAN (EVPN-VXLAN) edge-routed bridging (ERB) overlay network that has an IPv6 underlay. To configure this feature:

- Set up the EVPN-VXLAN fabric with an IPv6 underlay:

  - You can use either external BGP (EBGP) or OSPFv3 with IPv6 addressing for the IPv6 underlay.

  - Use the `inet6` option when you set the VXLAN tunnel endpoint (VTEP) source interface to the device loopback interface in the EVPN instance (EVI):

    ```
    set routing-instances evpn-instance-name vtep-source-interface lo0.0 inet6
    ```

- Configure the enhanced OISM elements for your multicast EVPN-VXLAN environment in the same way you would configure these elements in an EVPN-VXLAN network with an IPv4 underlay.

  You can configure any of the supported platforms as enhanced OISM server leaf devices, and only EX4650 and QFX5120 switches as enhanced OISM border leaf devices.

[See EVPN-VXLAN with an IPv6 Underlay and Optimized Intersubnet Multicast in EVPN Networks.]

Software Installation and Upgrade

- **In-band ZTP management in campus fabrics (EX4100-24MP, EX4100-48MP, EX4100-48P, EX4100-48T, EX4100-24P, EX4100-24T, EX4100-F-48P, EX4100-F-24P, EX4100-F-48T, EX4100-F-24T, EX4100-F-12P, EX4100-F-12T, EX4400-24MP, EX4400-24P, EX4400-24T, EX4400-24X, EX4400-48F, EX4400-48MP, EX4400-48P, EX4400-48T, EX4650, EX9204, EX9208, EX9214, MX304, QFX5120-32C, QFX5120-48T, QFX5120-48Y, and QFX5120-48YM)**—Starting in Junos OS Release 23.4R2, you can simplify the provisioning process for campus fabrics. Already provisioned upstream devices, such as core and distribution devices, that are capable of detecting downstream Day 0 devices can provide Layer 3 (L3) connectivity. With L3 connectivity, the downstream Day 0 devices can proceed with secure zero-touch provisioning (SZTP).

  To configure in-band ZTP management, include the `in-band-ztp` statement at the `[edit system services]` hierarchy level on your core and distribution devices. Optionally, your cloud controller can provide the `in-band-ztp` configuration as part of the provisioning process for your core and distribution devices.

  [See Zero Touch Provisioning.]

What's Changed

IN THIS SECTION

Learn about what changed in this release for EX Series switches.

General Routing

- **Change in options and generated configuration for the EZ-LAG configuration IRB subnet-address statement**—With the EZ-LAG `subnet-address inet` or `subnet-address inet6` options at the `edit services evpn evpn-vxlan irb` *`irb-instance`* hierarchy, you can now specify multiple IRB subnet addresses in a single statement using the list syntax `addr1 addr2 ...` . Also, in the generated configuration for IRB interfaces, the commit script now includes default `router-advertisement` statements at the `edit protocols` hierarchy level for that IRB interface.

  [See subnet-address (Easy EVPN LAG Configuration).]

VPNs

- **Increase in revert-delay timer range**— The `revert-delay` timer range is increased to 600 seconds from 20 seconds.

  [See min-rate.]

User Interface and Configuration

- **Detection of legacy PD (PoE)**—The detection of legacy PD (powered device) is disabled by default in EX4400-24MP, EX4400-48MP, EX4400-48MXP, EX4400-48XP, EX4400-24P, and EX4400-48P models. To enable a legacy PD in a port for these models, see Enabling Legacy Powered Device

Known Limitations

IN THIS SECTION

Learn about known limitations in this release for EX Series switches.

For the most complete and latest information about known Junos OS defects, use the Juniper Networks online Junos Problem Report Search application.

General Routing

- In EX2300, transit ARP requests entering a port can get trapped to the CPU even if no IRB is configured on the VLAN. This can result in unnecessary ARP requests to the CPU and in extreme cases result in drops of genuine ARP requests in the ARP queue to CPU. PR1365642
- On EX2300, EX3400,:EX4300-48MP and EX4300 , Pause frames counters does not get incremented when pause frames are sent. PR1580560
- This is a Broadcom limitation and Day 1 issue affecting broadcom chipsets such as EX4650's, QFX5ks, EX4300. One VLAN can be mapped to only on ERPS ring. For example, VLAN 100 can be mapped to only one ERPS ring. This same VLAN 100 cannot be part of another ERPS ring on the same switch. PR1732885
- [interface] [all] EX4400-48F :: JUNOS_REG: EX4400 : input-vlan-tagged-frames are not in the expected range while verifying Vlan Tagged Frames. PR1749391

Infrastructure

- When upgrading from releases before Junos OS Release 21.2 to Release 21.2 and onward, validation and upgrade might fail. The upgrade requires using the 'no-validate' option to complete successfully. https://kb.juniper.net/TSB18251. PR1568757

Open Issues

IN THIS SECTION

Learn about open issues in this release for EX Series switches.

For the most complete and latest information about known Junos OS defects, use the Juniper Networks online Junos Problem Report Search application.

General Routing

- Runt, fragment and jabber counters are not incrementing on EX4300-MPs.PR1492605

- On EX4300-48MP platform, if POE is enabled, a master RE reconnect might be seen which could cause traffic impact. PR1499771

- On EX2300, EX3400,:EX4300-48MP and EX4300 , Pause frames counters does not get incremented when pause frames are sent. PR1580560

- When the remote end server/system reboots, QFX5100 platform ports with SFP-T 1G inserted might go into a hung state and remain in that state even after the reboot is complete. This may affect traffic after the remote end system comes online and resumes traffic transmission. PR1665800

- On all EX platforms, whenever beacon LED functionality is enabled, there is a mismatch between the physical LED status and the output of the CLI command ?show chassis led? showing incorrect port LED status for interfaces as LED up instead of off. PR1697678

- When TISSU upgrade is done from 22.4 release onwards, the box come up as backup RE.PR1703229

- On EX4650 and QFX5120-48Y, the SFP-LX interface will not be UP when different Small Form-factor Pluggable(SFP-10GBASE-T and SFP-LX) are plugged in within the same 4 port group. The presence of the 10GE-T SFP resets the speed of the quad back to 10G even if the quad port speed is set to 1G. Normally 10G interface by itself will be up when set to 1G if no other SFP is plugged in. PR1714833

- EX4400-48F: Carrier transitions is not setting properly for channelized ports on non-DUT Lagavulin for QSFP28-100G-AOC-30M 740-064980 of FINISAR. PR1723924

- During device reboot, mge connected ports on the peer goes up after 90s into reboot. PR1767347

- EX2300 VC: Dot1x authentication flapping in multiple supplicant mode with 100 user scale. PR1767706

- After rebooting a mixed Virtual Chassis (VC) of EX4300-P and EX4300-MP switches or rebooting a EX4300-P member, interfaces with Power over Ethernet (PoE) configured won`t come up on EX4300-P members. PR1782445

- EX-Hardening:Local/Remote fault insertion from TG is failing. PR1789999

Interfaces and Chassis

- You can configure the routing platform to track IPv6-specific packets and bytes passing through the router. To enable IPv6 accounting, include the route-accounting statement at the `[edit forwarding-options family inet6]` hierarchy level: `[edit forwarding-options family inet6]` route-accounting; By default, IPv6 accounting is disabled. If IPv6 accounting is enabled, it remains enabled after a reboot of the router. To view IPv6 statistics, issue the show interface statistics operational mode command. Can be found here: Configuring IPv4 and IPv6 Accounting PR717316

MPLS

- On Junos QFX5100 and EX4600 platforms in Layer 2 Virtual Private Network (L2VPN) scenarios, when an access port flaps or the port related configuration is deactivated and activated, the traffic ingressing or egressing out of that port gets dropped. PR1775553

Platform and Infrastructure

- On Junos OS EX4300 and EX4300-VC platforms, if zeroize or interface configuration deletion performed, PFEX process crash will se seen when interface/device comes up and there will be traffic loss during the PFE restart.PR1714117

- In a rare scenario, due to timing issues, the Packet Forwarding Engine (PFE) crash is observed on Junos EX4300 platforms. This causes traffic loss until the PFE comes up.PR1720219

- On EX4300 platforms, when the firewall filter applied on the loopback interface is configured with default action as a discard on the DHCP-Relay and a client is connected to a VLAN with DHCP-security and DHCP-Relay enabled, then the DHCP lease renewal unicast packet sent by the DHCP client will be dropped by the loopback filter on the DHCP-Relay. This will eventually lead to service impact as the DHCP client loses the IP address. PR1730903

- On EX4300-VC, the Online Insertion and Removal (OIR) of Quad Small Form-factor Pluggable (QSFP) may result in a PFE crash under near-zero idle CPU conditions.PR1733339

- After an upgrade, the SFP modules are not detected in case of EX4300 platforms and the ports remain down impacting traffic. PR1747374

- On EX4300, "Error requesting CMTFPC SET INTEGER" and "Error requesting SET BOOLEAN" logs may be seen after device boot up. There is no functional impact for the error messages. PR1749289

- On all EX4300 platforms, traffic is sent on an AE interface and sent to the removed child interface from AE (Aggregated Ethernet) where the traffic is lost. PR1749406

- On EX switches, if 40G DAC(Direct Attach Copper) cables with PN(Part Number) 740-038624 (QSFP+-40G-CU3M) and 740-044512 (QSFP+-40G-CU50CM) are used, links might not come up after software upgrade to Junos 21.4R3-S3 or after a switch reboot (if the switch is running Junos 21.4R3-S3). The switch ports that use these DAC cables are observed to go down after a reboot. PR1752611

- An Incorrect Behavior Order vulnerability in the Packet Forwarding Engine (PFE) of Juniper Networks Junos OS on EX4300 Series allows an unauthenticated, network-based attacker to cause an integrity impact to networks downstream of the vulnerable device. Please refer to https://supportportal.juniper.net/JSA79185 for more information.PR1770410

- An Improper Check for Unusual or Exceptional Conditions vulnerability in the Packet Forwarding Engine (PFE) of Juniper Networks Junos OS on EX4300 Series allows a locally authenticated attacker with low privileges to cause a Denial-of-Service (Dos). Please refer to https://supportportal.juniper.net/JSA79186 for more information.PR1774634

- On EX4300 or EX4300-VC, removal of a Physical Interface Card (PIC), or if the software fails to detect a PIC that is installed, it can cause a crash in the pfex process. This crash can lead to high CPU usage and potentially disrupt network traffic. PR1779410

- On EX4300 Platforms, Packet Forwarding Engine (PFE) crash will be seen due to an unexpected switchover after committing interface configuration. PR1785058

Routing Protocols

- On all Junos and Junos Evolved platforms, when the shortest-path-first (SPF) algorithm for IS-IS is triggered frequently, CPU usage might increase and impact the device performance and traffic.PR1667575

Virtual Chassis

- On EX4600-VC, when "request system reboot all members" is executed, post-reboot one of the VC member/Flexible PIC Concentrator(FPC) might disconnect and join the VC back due to Packet Forwarding Engine (PFE) restart. Traffic loss is seen when FPC is disconnected.PR1700133

Resolved Issues

IN THIS SECTION

Learn about the issues fixed in this release for EX Series switches.

For the most complete and latest information about known Junos OS defects, use the Juniper Networks online Junos Problem Report Search application.

General Routing

- LTS19: MX960: 000: [Firmware Bug]: TSC_DEADLINE disabled due to Errata; please update microcode to version: 0x3a (or later) seen upon upgrade to 21.4. PR1608045
- Mac entry not ageout in RTG in EX4600-VC after VCP port reconnect. PR1707878
- When FAN tray is inserted, insertion SNMP TRAP message is not printed. PR1711653
- New option to allow operator to configure a power source alarm if power is not received on PD ports. PR1722976
- Transition Junos OS kernel random number generator from hashing algorithm SHA-256 to SHA-512. PR1723499
- In virtual-chassis(VC), swapping routing-engine member-id and role with linecard will lead to physical interface down. PR1740024
- EX4400 Platforms Virtual Chassis (VC) - HGOE enabled causes system crash when system memory becomes unavailable for cumulative protocol daemons traffic. PR1754344
- The VC port stays down after backup becomes master. PR1754838
- Multicast traffic may be dropped if both bpdu-block-on-edge and igmp-snooping are configured. PR1757160
- EX-hardening: EX4400: set chassis config-button no-clear is not working. PR1758042
- An unnecessary traffic load on the peer boxes. PR1767190
- [EX46/QFX5K]MTU Errors are counted when receiving packets up to 4 bytes in MTU. PR1770448
- EX4100/4400 : Error message 'COS default: IEEE 802.1ad defaults not specified' upon commit operation. PR1771111
- Memory leak observed on non-local FPC for Junos QFX5K and EX platforms. PR1771183
- Dynamic VLAN change on one port is affecting forwarding plane traffic on other ports to which no changes were done. PR1771222
- License missing on VC member after reboot. PR1771376
- Turning port beacon LED on or OFF may not change the LED status. PR1772477
- TDR link status not consistent in CLI. PR1773103
- The DHCP client will not be able to get the IP address. PR1774202

- The RE goes into amnesiac mode upon license check validation failure. PR1775463
- Peer device ports connected to Gigabit Physical ports of EX4100 transition to up state momentarily during reboot of EX4100. PR1775479
- On MX and EX platform replacing the line-cards may trigger FPC to be offlined due to unreachable destinations. PR1777534
- Core files for pfex and dot1x seen due to dot1x authentication. PR1778056
- In Virtual-Chassis mode, the EX4100 switch might not boot up upon triggering a manual reboot. PR1778873
- Error is shown on system when pvidb variable is accessed. PR1781317
- Junos OS and Junos OS Evolved: Impact of Terrapin SSH Attack (CVE-2023-48795). PR1781732
- A few AE interfaces will drop traffic when a large number of AE interfaces are deleted and added back. PR1781955
- MPC line card crashes while ISSU to Junos OS Release 24.1 or later, displays "ISSU PREPARE TIMEOUT" error. PR1785960
- Interface configured with BPDU-disable goes down during VC mastership switchover. PR1787892
- Traffic loss after PIC restart if the packet has a VLAN tag of 4095. PR1788573
- On EX2300/EX3400 series SFP-SX interface is not come up due to auto-negotiation failure. PR1789617
- The l2ald process will crash, with rapid configuration changes followed by rpd and l2ald restart process PR1790064
- The access port is dropping a VLAN-tagged packet of which the interface is a VLAN-member. PR1790316
- Warning message 'Too many VLAN-IDs on untagged interface' is seen when more than 1025 vlans on the same LAG interface are configured. PR1791053
- With any configuration change or interface up/down with MACsec protocol configured with or without Dot1x, dot1xd process core is observed in the device. PR1792507
- Dot1x process crash will be seen in the system with "server-timeout" and "server-fail use-cache" configuration. PR1794778
- On all Junos EX platforms rewrite rules does not work properly when multiple interfaces are configured. PR1795545

- Cos rewrite rules does not work properly when input/output-vlan-map swap are configured. PR1795807

- DHCP IP assignment will fail on VoIP phone connected to a VXLAN access port. PR1797422

- Intermittent alarms related to fan overspeed value can be observed on EX4100 platform. PR1797727

- [EX2300]"Ethernet Link Down" would not be generated when me0 was down. PR1799093

- ARP won't be forwarded in VLAN associated VNI in VxLAN Fabric. PR1801237

- CPU usage gets spiked for eventd due to flooding of pfe_khms_spurious_wakeup log. PR1801535

- The `set chassis config-button no-clear` support not added on EX4100. PR1802614

-

Interfaces and Chassis

- The ifinfo process crash is seen on Junos platforms. PR1786555

Layer 2 Ethernet Services

- DNS received through DHCP is lost after a commit and not able to ping internet. PR1743611

- DHCP clients not receiving IP address. PR1776451

Platform and Infrastructure

- In EVPN-MPLS/EVPN-VxLAN Multi-Home Active/Active scenario, random packet drops are observed. PR1772733

Routing Protocols

- In a scaled setup mcsnoopd is taking high CPU causing traffic drop. PR1710565

User Interface and Configuration

- After the device reboot BGP sessions configured with authentication will be down. PR1726731
- High storage is reported in **/var/jail/log** due to http.log and http-trace.log on all Junos platforms. PR1776688

Migration, Upgrade, and Downgrade Instructions

IN THIS SECTION

This section contains the upgrade and downgrade support policy for Junos OS for EX Series switches. Upgrading or downgrading Junos OS might take several minutes, depending on the size and configuration of the network.

For information about software installation and upgrade, see the Installation and Upgrade Guide.

Upgrade and Downgrade Support Policy for Junos OS Releases and Extended End-Of-Life Releases

We have two types of releases, standard EOL and EEOL:

- Standard End of Life (EOL) releases have engineering support for twenty four months after the first general availability date and customer support for an additional six more months.
- Extended End of Life (EEOL) releases have engineering support for sixty months after the first general availability date and customer support for an additional six more months.

> **NOTE**: The sixty months of support for EEOL releases is introduced in Junos OS 23.2 release and is available for all later releases. For releases prior to 23.2, the support for EEOL releases continues to be thirty six months.

For both standard EOL and EEOL releases, you can upgrade to the next three subsequent releases or downgrade to the previous three releases.

For EEOL releases only, you have an additional option - you can upgrade directly from one EEOL release to the next two subsequent EEOL releases, even if the target release is beyond the next three releases. Likewise, you can downgrade directly from one EEOL release to the previous two EEOL releases, even if the target release is beyond the previous three releases.

Table 2: EOL and EEOL Releases

Release Type	End of Engineering (EOE)	End of Support (EOS)	Upgrade/ Downgrade to subsequent 3 releases	Upgrade/ Downgrade to subsequent 2 EEOL releases
Standard End of Life (EOL)	24 months	End of Engineering + 6 months	Yes	No
Extended End of Life (EEOL)	60 months	End of Engineering + 6 months	Yes	Yes

For more information about standard EOL and EEOL releases, see https://www.juniper.net/support/eol/junos.html.

For information about software installation and upgrade, see the Installation and Upgrade Guide.

Junos OS Release Notes for JRR Series

IN THIS SECTION

NOTE: Junos OS Release 23.4R2 is the last-supported release for the following SKUs:

Product Line	SKUs	Junos OS Release
JRR200	JRR200-AC	Junos OS Release 23.4R2
JRR200	JRR200-CHAS	Junos OS Release 23.4R2
JRR200	JRR200-DC	Junos OS Release 23.4R2

What's New

There are no new features or enhancements to existing features in this release for JRR Series Route Reflectors.

What's Changed

There are no changes in behavior and syntax in this release for JRR Series Route Reflectors.

Known Limitations

There are no known limitations in hardware or software in this release for JRR Series Route Reflectors.

For the most complete and latest information about known Junos OS defects, use the Juniper Networks online Junos Problem Report Search application.

Open Issues

There are no known issues in hardware or software in this release for JRR Series Route Reflectors.

For the most complete and latest information about known Junos OS defects, use the Juniper Networks online Junos Problem Report Search application.

Resolved Issues

There are no resolved issues in this release for JRR Series Route Reflectors.

For the most complete and latest information about known Junos OS defects, use the Juniper Networks online Junos Problem Report Search application.

Migration, Upgrade, and Downgrade Instructions

IN THIS SECTION

This section contains the upgrade and downgrade support policy for Junos OS for the JRR Series Route Reflector. Upgrading or downgrading Junos OS might take several minutes, depending on the size and configuration of the network.

NOTE: Junos OS Release 23.4R2 is the last-supported release for the following SKUs:

Product Line	SKUs	Junos OS Release
JRR200	JRR200-AC	Junos OS Release 23.4R2

(Continued)

Product Line	SKUs	Junos OS Release
JRR200	JRR200-CHAS	Junos OS Release 23.4R2
JRR200	JRR200-DC	Junos OS Release 23.4R2

For information about software installation and upgrade, see the JRR200 Route Reflector Quick Start and Installation and Upgrade Guide.

Upgrade and Downgrade Support Policy for Junos OS Releases and Extended End-Of-Life Releases

We have two types of releases, standard EOL and EEOL:

- Standard End of Life (EOL) releases have engineering support for twenty four months after the first general availability date and customer support for an additional six more months.

- Extended End of Life (EEOL) releases have engineering support for sixty months after the first general availability date and customer support for an additional six more months.

NOTE: The sixty months of support for EEOL releases is introduced in Junos OS 23.2 release and is available for all later releases. For releases prior to 23.2, the support for EEOL releases continues to be thirty six months.

For both standard EOL and EEOL releases, you can upgrade to the next three subsequent releases or downgrade to the previous three releases.

For EEOL releases only, you have an additional option - you can upgrade directly from one EEOL release to the next two subsequent EEOL releases, even if the target release is beyond the next three releases. Likewise, you can downgrade directly from one EEOL release to the previous two EEOL releases, even if the target release is beyond the previous three releases.

Table 3: EOL and EEOL Releases

Release Type	End of Engineering (EOE)	End of Support (EOS)	Upgrade/ Downgrade to subsequent 3 releases	Upgrade/ Downgrade to subsequent 2 EEOL releases
Standard End of Life (EOL)	24 months	End of Engineering + 6 months	Yes	No
Extended End of Life (EEOL)	60 months	End of Engineering + 6 months	Yes	Yes

For more information about standard EOL and EEOL releases, see https://www.juniper.net/support/eol/junos.html.

For information about software installation and upgrade, see the Installation and Upgrade Guide.

Junos OS Release Notes for Juniper Secure Connect

IN THIS SECTION

What's New

There are no new features or enhancements to existing features in this release for Juniper Secure Connect.

What's Changed

There are no changes in behavior and syntax in this release for Juniper Secure Connect.

Known Limitations

There are no known limitations in hardware or software in this release for Juniper Secure Connect.

For the most complete and latest information about known Junos OS defects, use the Juniper Networks online Junos Problem Report Search application.

Open Issues

There are no known issues in hardware or software in this release for Juniper Secure Connect.

For the most complete and latest information about known Junos OS defects, use the Juniper Networks online Junos Problem Report Search application.

Resolved Issues

There are no resolved issues in this release for Juniper Secure Connect.

For the most complete and latest information about known Junos OS defects, use the Juniper Networks online Junos Problem Report Search application.

Junos OS Release Notes for MX Series

IN THIS SECTION

What's New

IN THIS SECTION

Learn about new features introduced in this release for the MX Series routers.

Software Installation and Upgrade

- **In-band ZTP management in campus fabrics (EX4100-24MP, EX4100-48MP, EX4100-48P, EX4100-48T, EX4100-24P, EX4100-24T, EX4100-F-48P, EX4100-F-24P, EX4100-F-48T, EX4100-F-24T, EX4100-F-12P, EX4100-F-12T, EX4400-24MP, EX4400-24P, EX4400-24T, EX4400-24X, EX4400-48F, EX4400-48MP, EX4400-48P, EX4400-48T, EX4650, EX9204, EX9208, EX9214, MX304, QFX5120-32C, QFX5120-48T, QFX5120-48Y, and QFX5120-48YM)**—Starting in Junos OS Release 23.4R2, you can simplify the provisioning process for campus fabrics. Already provisioned upstream devices, such as core and distribution devices, that are capable of detecting downstream Day 0 devices can provide Layer 3 (L3) connectivity. With L3 connectivity, the downstream Day 0 devices can proceed with secure zero-touch provisioning (SZTP).

  To configure in-band ZTP management, include the `in-band-ztp` statement at the `[edit system services]` hierarchy level on your core and distribution devices. Optionally, your cloud controller can provide the `in-band-ztp` configuration as part of the provisioning process for your core and distribution devices.

  [See Zero Touch Provisioning.]

What's Changed

IN THIS SECTION

Learn about what changed in this release for MX Series routers.

Infrastructure

- **Option to disable path MTU discovery**— Path MTU discovery is enabled by default. To disable it for IPv4 traffic, you can configure the `no-path-mtu-discovery` statement at the `[edit system internet-options]` hierarchy level. To reenable it, use the `path-mtu-discovery` statement.

  [See Path MTU Discovery.]

VPNs

- **Increase in revert-delay timer range**— The `revert-delay` timer range is increased to 600 seconds from 20 seconds.

  [See min-rate.]

- **Configure min-rate for IPMSI traffic explicitly**— In a source-based MoFRR scenario, you can set a min-rate threshold for IPMSI traffic explicitly by configuring `ipmsi-min-rate` under `set routing-instances protocols mvpn hot-root-standby min-rate`. If not configured, the existing `min-rate` will be applicable to both IPMSI and SPMSI traffic.

  [See min-rate.]

Known Limitations

IN THIS SECTION

Learn about known limitations in this release for MX Series routers.

For the most complete and latest information about known Junos OS defects, use the Juniper Networks online Junos Problem Report Search application.

General Routing

- On the MX2000 line of routers, you might see RPD usage hit 100% when you start running OCST polling. The spike in RPD usage is expected because of the very large scale and OCST in general. This issue should not affect any RPD functionality if that is the concern since telemetry streaming is the lowest priority task in RPD. PR1614978
- Core will will not be generated on RE when RE disk space is greater than 85%PR1695408
- It is recommended to use IGP shortcut with strict SPF SIDs in SRTE path. if Strict SPF SIDs are used then this issue would not occur. This issue will occur only if regular ISIS SIDs are used in SRTE path and IGP shortcut is enabled. with this, if customer perform multiple times deactivate/activate for SRTE telemetry. PR1697880
- On Older MPC Cards (e.g., MPC6) that have PPC as the host CPU, the CPU usage can exceed 95% whenever the host-bound traffic rate is more than 5k-6k PPS. SNMP polling consumes a significant amount of CPU resources; disabling it will allow the system to handle some amount of additional PPS host-bound traffic. In current PR context, disabling SNMP allowed the system to handle an additional 2k-3k PPS of host-bound traffic. When the CPU usage > 95%, host-bound routing protocol packets (e.g., BGP, ISIS) may not be drained fast enough, which may result in flaps. PR1749829
- Currently streaming lcmd logs on the vmhost side towards junos /var/log/messages is unavailable. PR1762097
- On Junos MX304 and MX platforms with LC9600 linecards, With the current error handling mechanism upon receiving fatal error on Flexible pic concentrators(FPC), leads to disable both the

Packet Forwarding Engine(PFE) on a Physical Interface Cards(PIC) card and seen traffic impact. PR1765394

- `PEM I2C Failure` alarm expected to appear and quickly vanish, during the PEM FW upgrade process. As the PEM is expected to upgrade and reboot itself, during which it will not respond to i2c requests. PR1766248

Infrastructure

- When upgrading from releases prior Junos OS Release 21.2 to Release 21.2 and later, validation and upgrade might fail. The upgrade requires using the 'no-validate' option to complete successfully. PR1568757

Open Issues

IN THIS SECTION

Learn about open issues in this release for MX Series routers.

For the most complete and latest information about known Junos OS defects, use the Juniper Networks online Junos Problem Report Search application.

EVPN

- A few duplicate packets might be seen in an A/A EVPN scenario when the remote PE device sends a packet with an IM label due to MAC not learned on the remote PE device, but learned on the A/A local PE device. The nondesignated forwarder sends the IM-labeled encapsulated packet to the PE-CE interface after MAC lookup instead of dropping the packet, which causes duplicate packets to be seen on the CE side. PR1245316

- After GRES, VPWS Switchover occurs only after NSR Phantom Timer expires. The NSR Phantom timer is configurable. This can result in packet loss for that duration. This needs to be fixed in DCB. PR1765052

Flow-based and Packet-based Processing

- The subscription path for flow sensor shall be changed from /junos/security/spu/flow/usage to /junos/security/spu/flow/statistics. This change is done to maintain uniform format for subscription path in request and response data. PR1738832

General Routing

- With Next Generation Routing Engine (NG-RE), in some race conditions, the following interrupts messages might be seen on master RE: kernel: interrupt storm detected on "irq11:"; throttling interrupt. source PR1386306

- This log is harmless: Feb 27 20:26:40 xolo fpc3 Cannot scan phys_mem_size.out. Please collect /var/log/*.out (0;0xdd3f6ea0;-1) (posix_interface_get_ram_size_info): Unknown error: -1. PR1548677

- Due to a race condition, the 'show multicast route extensive instance instance-name output can display the session status as Invalid. Such an output is a cosmetic defect and not indicative of a functional issue. PR1562387

- The output of show network agent command should be null, which shows statistic per component after GRES. PR1610325

- Percentage physical-interface policer is not working on the aggregated Ethernet after switching between baseline config to policer configuration. PR1621998

- There will be drop of syslog packets seen for RT_FLOW: RT_FLOW_SESSION_CREATE_USF logs until this is fixed. This will not impact the functionality. PR1678453

- Current stack and display is correctly set to 128 ports that is qualified on all MX10K8 line cards. PR1706376
- When LAG is configured with mixed speed interfaces switching to a secondary interface of different port speed, results in a few packet drops for a very short duration. PTP remains lock and there is no further functional impact. PR1707944
- On MX2020 devices, the chassisd process generates core file during feature test as Retaining the SLC name modify the CPU nos in configuration. PR1713626
- fec-codeword-rate data with render type decimal64 is rendered as string in grpc python decoder. PR1717520
- Segmentation fault on grpc timer thread (might be related to keepalive) #32085 grpc issue https://github.com/grpc/grpc/issues/32085 grpc stack needs to be upgraded to 1.53 or later. PR1722414
- As a part of recent logging enhancement in cRPD. This will be applicable only for file configured under [edit system syslog hierarchy].We have shipped logrotate binary to rotate the syslog file in junos-osbase-ub22-hooks.sh.https://opengrok.juniper.net/source/xref/DEV_COM MON_BRANCH/junos/ddl/action-impl/junos/junos_foreign.c?r=1350442#3629.Below are the parameter related to logrotate for syslog file defined in container_logrotate file.crontab is scheduled default for 15min to rotate files configured under [edit system syslog hierarchy].based on requirement you can configure on below CLI knob.[edit system syslog log-rotate-frequency 1..59min] root@crpd3:/var# cat /etc/logrotate.d/container_logrotate. PR1727111
- In Junos OS Release 23.4 nfx-3, high CPU utilization by vcpu thread of vjunos0. Same behavior may be observed with the vcpu thread of any VNF. PR1727654
- Telemetry Stats are not visible for MPLS LSP(RSVP Based) when the core interface is MPC11/MPC10. PR1731587
- When class-of-service with shaping rate is configured on Aggregate Ethernet interfaces, and the firewall policer queries the aggregated Ethernet member and not the aggregated Ethernet interface, the shaping rate or the policy configuration does not take effect as the shaping rate is not configured in the aggregated Ethernet member. PR1735087
- On all Junos devices, the time needed to commit increases when a Trusted Platform Module (TPM) is configured. PR1738193
- There must be at least one minute spacing between consecutive key rollovers. This includes key rollovers triggered by key chain, sak_key_interval, primary/fallback, packet count rollovers. PR1739933
- On MXVC , Due to some timing issue when RPD is restarted, It will not be spawned again. This issue is rarely reproducible. PR1740083

- Even though Source and Feed Redundancy are mutually exclusive, they appear as suggestions to each of them in Config CLI. This is due to the way, these commands are ordered in the DDL to simplify the use of them. However, commit will be blocked if user tries to enable both Source and Feed Redundancy in config. Hence No impact for feature usage and operation. PR1741630

- On MX platforms with MS-MPC/MS-DPC, when the system is busy in the creation/deletion of sessions results in the picd process crashes for executing the CLI command "show service sessions/ flows" or "clear service sessions/flows" aggressively (executing CLI command in 5-10 secs iteration). PR1743031

- Session synchronization does not work on standby even after replication-threshold timer (150 seconds) is complete with SRD configuration. PR1744420

- Error message might get generated once in a while with full scale during negative scenarios like 'clear bgp neighbor all' with all the services like EVPN, vrf etc being present. PR1744815

- Traces on line cards with no SSDs are not available on line cards as well as Routing Engine. There is no infra to transport the traces to Routing Engine. PR1747957

- On MX960 devices, the core-vmcore-ms2 process generates core files. PR1750581

- Problem Statement: When Feed redundancy is configured and existing load does not support the Feed redundancy, Feed Redundancy will be deactivated with an Alarm "Feed redundancy unsupported". In MX Chasssis running Junos this alarm is raised at the system level instead of the individial PEM. This behaviour of alarm is different from EVO where the feed redundancy is deactivated at the individial PEM level. Reason: The implemenation of the power budgeting in Junos and EVO is different. In case of Juons the functional split between Junos and LCMD is the constraint in handling the power bugdting. It is handled at the Junos chassisd and hence this limiation for the Junos. Customer Impact: None. Except that there is a difference in Alarm behaviour between EVO and Junos. Since the "Feed redundancy unsupported" alarm is becuse of not able to support feed-redundancy for the exising load conditions, end user has to disable the feed reduncy or increase the power with additonal PEM or additional feeds on any PEM. PR1754234

- SRv6 TE with logical-systems is not qualified in any release. A test only RLI may be required to qualify the same. PR1760727

- For certain releases, performing ISSU on MPC10 or MPC11 can cause an FPC core. PR1766307

- Removing PEM FRU from the chassis during its firmware upgrade is currenlty not allowed due to firmware upgrade limitations, leading to undefined software behaviour in such situations. PR1773895

- On MX10008 devices, PLD is higher than 2000 msec on ungraceful removal of a Fabric board. PR1776054

- The following network overrides will not be supported in a CUPS model: set system services subscriber-management overrides no-gratuitous-arp set system services subscriber-management overrides force-show-arp-no-resolve set system services subscriber-management overrides interfaces family inet receive-gratuitous-arp set system services subscriber-management overrides interfaces family inet receive-gratuitous-arp-reply set system services subscriber-management overrides interfaces family inet ipoe-dynamic-arp-enable set system nd-override-preferred-src set system services subscriber-management overrides no-gratuitous-nd. PR1781731

- Even after "request vmhost power-off" LEDs keep lighting on. The LEDs state should be off because routing-engine doesn't have power in case of "request vmhost power-off". PR1781815

- On AFT(Advanced Forwarding Toolkit) based MX platforms, default ARP(Address Resolution Protocol) policer fails because of which ARP resolution fails on the interface and hence the traffic gets impacted. PR1795940

- We might observe repd core (in the "from" release) during ISSU. There are no functional impact due to this repd core. PR1797189

- IKE is not coming up with dhgroup19 and dhgroup20. The below Junos releases are impacted. junos:21.2R3-S7 junos:21.4R3-S6 junos:22.1R3-S5 junos:22.2R3-S3 junos:22.3R3-S2 junos:22.4R3-S1 junos:24.1R1. So previous to these releases dhgroup19 and dhgroup20 should be working. PR1801201

- On MX platforms with SCBE3-MX (MX240, MX480 and MX960) due to a hardware failure of the Control Board, the Routing Engine(RE) switchover might not happen. This will result in the 19.4Mhz clock failure and has potential risk for chassis wide traffic impact. In worst case all revenue ports will be impacted. If the RE switchover is done in a timely manner then the device will recover because FPCs will try using the 19.4Mhz clock from the new master. PR1801284

Interfaces and Chassis

- You can configure the routing platform to track IPv6-specific packets and bytes passing through the router. To enable IPv6 accounting, include the route-accounting statement at the [edit forwarding-options family inet6] hierarchy level: [edit forwarding-options family inet6] route-accounting; By default, IPv6 accounting is disabled. If IPv6 accounting is enabled, it remains enabled after a reboot of the router. To view IPv6 statistics, issue the show interface statistics operational mode command. Can be found here: http://www.juniper.net/techpubs/en_US/junos10.4/topics/usage-guidelines/policy-configuring-ipv6-accounting.html. PR717316

- IFL counter has a counter named "IPv6 transit statistics". It can be confirmed on "show interfaces extensive" command output. However, this counter is originally for IPv6 total statistics(transit + local) and the counter name was wrong from the first. On older releases like 19.1R1, as the support for IPv6 local stats was not available the local stats was always zero. So, the meaning of the counter name was the same to the counting content coincidentally. In latest releases support for IPv6 local stats has been added but the counter name was not changed. As the local stats will not be zero the difference between the meaning of the counter name and the counting content started being visible. PR1631200

- The LAG (Link Aggregation Group) member links may flap on all Junos platforms except MX when the configuration of any interface is changed/modified. The flap is not seen always. PR1679952
- On Junos and Junos OS Evolved platform, In a system with scaled interface config, when deleting entire config via openconfig at interfaces hierarchy, changes got fails because translation module takes more time to process to delete the entire configuration. PR1785035

J-Web

- PHP software included with Junos OS J-Web has been updated from 7.4.30 to 8.2.0 to resolve multiple vulnerabilities. Please refer to https://supportportal.juniper.net/JSA71653 for more information. PR1698386

MPLS

- On all Junos and Junos OS Evolved platforms, when MPLS (Multiprotocol Label Switching) statistics is configured without LSP (Label-Switched Path) configuration, the rpd process crashes and impacts the routing protocols. This leads to traffic disruption due to the loss of routing information. PR1698889

Network Management and Monitoring

- In some NAPT44 and NAT64 scenarios, Duplicate SESSION_CLOSE Syslog gets generated. PR1614358

Platform and Infrastructure

- On MX960 devices, JUNOS_REG:MX960:bgp stats convergence time is 76 and not within accepted limit of 70 Secs after restart routing. PR1734760

- Firewall filter counters are not incremented as expected when filter is applied to IRB interface in the ingress/egress direction via forwarding table. PR1766471

Routing Protocols

- Certain BGP traceoption flags (for example, "open", "update", and "keepalive") might result in (trace) logging of debugging messages that do not fall within the specified traceoption category, which results in some unwanted BGP debug messages being logged to the BGP traceoption file. PR1252294

- LDP OSPF are in synchronization state because the IGP interface is down with ldp-synchronization enabled for OSPF. user@host> show ospf interface ae100.0 extensive Interface State Area DR ID BDR ID Nbrs ae100.0 PtToPt 0.0.0.0 0.0.0.0 0.0.0.0 1 Type: P2P, Address: 10.0.60.93, Mask: 255.255.255.252, MTU: 9100, Cost: 1050 Adj count: 1 Hello: 10, Dead: 40, ReXmit: 2, Not Stub Auth type: MD5, Active key ID: 1, Start time: 1970 Jan 1 00:00:00 UTC Protection type: None Topology default (ID 0) -> Cost: 1050 LDP sync state: in sync, for: 00:04:03, reason: IGP interface down config holdtime: infinity. As per the current analysis, the IGP interface goes down because although LDP notified OSPF that LDP synchronization was achieved, OSPF is not able to take note of the LDP synchronization notification, because the OSPF neighbor is not up yet. PR1256434

- On MX platforms, unexpected log message will appear if the CLI command 'show version detail' or 'request support information' is executed: test@test> show version detail *** messages *** Oct 12 12:11:48.406 re0 mcsnoopd: INFO: krt mode is 1 Oct 12 12:11:48.406 re0 mcsnoopd: JUNOS SYNC private vectors set. PR1315429

- On all Junos and Junos Evolved platforms, when the shortest-path-first (SPF) algorithm for IS-IS is triggered frequently, CPU usage might increase and impact the device performance and traffic. PR1667575

- On Junos platforms and Junos Evolved platforms, if a BGP peer goes down and stays down, the system might take an extremely long time to complete removing the BGP routes. The issue is observed when a BGP peer sends many routes, only a small number of routes are selected as the active routes in the routing information base (RIB, also known as the routing table), and if the BGP delete job gets only a small part of the CPU time because other work in the routing process is utilizing the CPU. PR1695062

- When rib (Routing Information Base) contains IPv4 routes with IPv6 next-hops, these routes do not get re-advertised by IPv4 EBGP sessions unless export policy is configured to change it to IPv4 next-hop. PR1712406

- On all Junos and Junos Evolved platforms with TI-LFA (Topology-Independent Loop-Free Alternate) feature enabled, when IP address is removed from one interface and is assigned to another interface in the same commit, the rpd process crashes affecting routing control plane. PR1723172

- The BFD sessions bounce during ISSU if authentication is used. PR1723992

- The openconfig-local-routing.yang from "1.0.0" to "2.0.0" in which this module is deprecated now. As we upgraded yang model for local-routes, it deprecated few xpaths that were previously supported: / local-routes/static-routes/static/ /local-routes/local-aggregates/aggregate/. PR1735926

- With BGP sharding and NSR configured, rpd core is hit in master RE after repeated deactivate/ activate routing-instances and interfaces. PR1742915

- There are streaming Discrepancies for /adjacency-sids/adjacency-sid in /network-instances/network-instance/protocols/protocol/isis between Junos OS Releases 22.3R2-S1 and 20.X75-D51. There is a OC YANG version difference between the two releases and the OC YANG versions are not backwards compatible. The YANG version is tightly coupled with the release. PR1750314

- Configuration of a global AS number is necessary when route target filter is enabled. Currently JUNOS cli does not enforce configuring a global AS number and it has been the behavior for a long time. Many unexpected issues may be seen without a global AS number. It's been a recommended practice to configure a global AS number in the field. PR1783375

Services Applications

- On Junos MX80, MX240, MX480, MX960 platforms with Multiservices Modular Interfaces Card (MS-MIC), Multiservices Modular Port Concentrators (MS-MPC) service cards, in an issue where an old dynamic security association_configuration (sa_cfg) for a tunnel is present and trying to establish new sets of Internet Protocol Security Security Association (IPSec SAs) using a new Internet Key Exchange (IKE) SA established for the same remote device but with a different request. This can happen, if for some reason old sa_cfg is not cleaned (failed in clean-up). On crash, the Key Management Daemon (kmd) restarts but fails because of kernel instance mismatch present in the kernel database. So all the IPsec tunnels will be impacted. PR1771009

VPNs

- This happens only when MVPN protocol has separate route targets configured and then both the address families are disabled. rpd (Routing process daemon) infra parsing does not check if MVPN protocol is disabled and hence will create the auto policies for route-targets if configured. So if those policies are not marked as active in MVPN configuration flow, it does not get resolved and thereby the policy object may not be valid thus leading to the core. PR1700345

- On all Junos and Junos Evolved platforms with Dual RE and MVPN ((Multicast Virtual Private Network) enabled, when the user initiates a GRES (Graceful Routing Engine Switchover) switchover, it triggers a route change from the MVPN . During this process, there's a gap where traffic loss is observed because the flood next hop pointed to by the route gets deleted. PR1747703

Resolved Issues

IN THIS SECTION

Learn about the issues fixed in this release for MX Series routers.

For the most complete and latest information about known Junos OS defects, use the Juniper Networks online Junos Problem Report Search application.

Class of Service (CoS)

- The CoS scheduler map will not get attached to the sub-interface correctly when shaping-rate and scheduler-map are configured on it. PR1734013
- "load override" followed by ISSU will introduce incorrect class-of-service FC(Forwarding Class)-to-Q(queue) table mapping. PR1755540
- Change in the cosd behaviour due to the CoS interface specific wildcards. PR1760817

EVPN

- SRv6 locator change results in rpd crash. PR1724845
- EVPN-VXLAN interconnection DCI forwarding problem was observed when one of the AGW IRB interfaces failed in data centers spine . PR1732414
- While doing a migration from VPLS to EVPN, when any changes are done like FPC restart or device reboot, the crash is observed. PR1734686
- After switchover EVPN-VPWS SID is not allocated. PR1735856
- The rpd crash on EVPN VPWS environment. PR1738032
- Evpn-VXLAN comp nh is not installed in pfe after peer reboot. PR1739686
- ARP/FIB are added even if IRB in EVPN is disabled. PR1743529
- BGP NH resolution should happen using locator and without extra policy at egress. PR1745991
- The user will be unable to configure the interface having stacked outer VLAN and a list of inner VLANs. PR1746787
- Intermittent packet loss can be observed in evpn-vpws local switching scenario. PR1747706
- Re-ARP is not sent before MAC entry expires in EVPN environment on Junos OS MX Series platforms. PR1751386
- EVPN AD per EVI route might not carry SRv6 sid post GRES switchover. PR1756536
- MAC addresses programming failure resulting in traffic flooding. PR1758677
- The rpd can crash on all Junos platforms in Seamless DCI scenario. PR1761852

- [EVPN/MPLS] Color related LSPs for next-hop will disappear from EVPN routes on mpls.0 routing-table by changing 'fallback none' option in 'transport-class' configuration. PR1764126

- Migrating from Layer 2 Circuit to EVPN results in rpd crash. PR1767914

- In EVPN-VXLAN scenario, arp flag may not be set properly due to mac-ip entry age out not handled properly. PR1773734

Forwarding and Sampling

- Traffic not hitting the policer after configuring macroflow filter. PR1718147

- FPC cards restart unexpectedly. PR1743032

- High CPU utilization of the mib2d process will be observed with error messages due to stale SNMP requests. PR1749092

- Traffic loss observed when using ingress-queuing-filter on non zero PFE interface. PR1751494

General Routing

- The mustd process may crash on all platforms. PR1562848

- Inter vlan ipv6 traffic loss for some hosts after configuration remove and restore. PR1629345

- Delegated BFD sessions configured on routing-instance may fail to come up. PR1633395

- Continuous error logs and Telemetry data might not be populated. PR1661423

- Telemetry data is not being captured. PR1666714

- IFL packet counters does not work on show AMS interface extensive for sub interfaces. PR1673337

- LC9600 line card not booting-up [BIOS corruption]. PR1677757

- A new command has been introduced that will display the differences between the destroute entries learned within l2ald and present in the kernel. PR1677996

- The PFE will get disabled for underrun cmerrors observed when traffic ingressing over the AF interface. PR1681428

- The xml validation failure seen for "show security macsec connections | display xml validate" with ERROR: Duplicate data element. PR1691435

- RPD may restart during Multi-Feature-Test with BGP-MP, L3VPN/L2VPN, over RSVP/LDP transport, as well as colored SRTE, and SRv6 tunnel transport along with BGP CT. PR1699773
- Alarms for PEMs are still seen when PEM are removed from the chassis. PR1703566
- Interface flaps are seen after PTP GM changes to a different FPC slot. PR1704633
- Next Hop counts are not as expected. PR1710274
- The dcpfe process will crash due to memory fragmentation. PR1711860
- The agentd would become unresponsive on all Junos platforms. PR1715377
- Inconsistent RPD crash found in rt_walk, task_job_run_job_bg, task_scheduler. PR1715599
- BMP station will not receive the RIBs as expected. PR1715886
- Same MAC address is assigned to cbp and physical interfaces instead of being unique on MX304 devices. PR1719084
- The subscribers will be stuck in a terminated state when an FPC is taken offline. PR1719427
- Continuous messages indicating duplicate IP address L2ALM_DUPLICATE_IP_ADDR will be seen in MCLAG and VRRP scenario. PR1719868
- Removing a PEM that doesn't have power feed does not generate the SNMP TRAP for "Power Supply Removed". PR1719915
- The ES-IS route does not get installed in the (instance-name).iso.0 routing table. PR1720303
- Reachability loss between Master and backup Routing Engine in certain condition on MX2008 platform. PR1720407
- The bbe-statsd process crash is observed on the backup Routing Engine immediate after GRES was disabled. PR1720978
- The "no-reduced-srh" SRV6 encap mode is not working as expected on MX304 devices. PR1721404
- L2alm sends IPv6 NS with IRB link local address even though target IP is global address. PR1722102
- BNG CUPS Controller: authd core after enabling a configured SGRP and subscriber-group-default-tags. PR1722802
- The FPC crash is observed on Junos MX10008 platform when connected to non-Juniper SFP. PR1722823
- PADT response will not be sent for an incoming PPPoE/PPP data Packet from an unknown session ID. PR1722945

- PS interface remains up while LT or RLT interface is down. PR1724298
- Help string "Display information for a specified VLAN" is changed to "Display information for a specified bridge domain". PR1724489
- gNMI native Junos configuration push commit fails if configuration has special character. PR1724746
- Memory initialization and scrub operation using PFE's fails. PR1724841
- The entPhysicalSoftwareRev MIB object returns Junos OS version value for components which do not run Junos OS. PR1725078
- The "show network-access address-assignment address-pool-manager status" command reports APM not connected when in fact it is connected. PR1725143
- The error logs "fpc0 expr_hostbound_packet_handler: Receive pe 254?" would be generated. PR1725716
- Root user is unable to login using public key authentication after reboot or upgrade. PR1726621
- Upgrading the i40e NVM Firmware on Routing Engines with VM Host Support. PR1726775
- The EVPN-VXLAN proxy-arp will respond with the wrong MAC when no-mac-learning gets configured. PR1727119
- "/lib/systemd/system/docker.socket is marked executable" logs flood after system reboot. PR1727524
- On all Junos and Junos Evolved platforms the l2ald process memory usage is seen to increase over time. PR1727954
- A panic reboot will be observed due to deadlock on VMhost platforms. PR1727985
- DHCP subscribers are stuck in DHCP-renew state when 'overrides always-write-giaddr' gets enabled. PR1729913
- MX304 Major Alarm "Host 0 detected AER correctable error" after Routing Engine switchover. PR1731237
- IPv6 to IPv4 translation is not happening for traceroutev6 traffic. PR1731341
- Auto-sw-sync doesn't trigger upgrade/restart of rRuting Engine. PR1731877
- Traffic drop will be observed when RIPv2 is enabled on IPv4 interface. PR1732673
- The xmlproxyd crash might be observed when there are multiple collectors. PR1732763
- Error logs are seen with a non-vxlan dot1x enabled port. PR1733365

- 23.2R1 :USF_DNSF:log messages are not generated when Sending MX query with domain name in black list with action as report after configure the web filtering with one/morep profile and template. PR1733435

- Traffic loss is seen when "lacp force-up" command gets configured. PR1733543

- PTP gets stuck in acquiring state which leads to improper time synchronization after system reboot. PR1734235

- Script is failing when trying to verify Radius ngs_pppoev4_dynamic accounting stop status. PR1734608

- The jkdsd process crashes due to multiple telemetry requests. PR1734718

- The bbe-smgd process crashes in a certain scenario. PR1735560

- Control plane flap, data drop, unexpected behavior of PFE or device is observed when file storage is impacted in a continuous ksyncd process crash scenario. PR1735685

- Crash on all Junos VMhost platforms due to deadlock panic. PR1735843

- Unexpected VLAN tagging behavior would be observed in the EVPN-VXLAN scenario. PR1736954

- ICMP Response not coming properly for downstream traceroute UDP traffic. PR1736972

- The CLI command "show class-of-service classifier" hangs intermittently. PR1737009

- BGP sessions flap due to license updates. PR1737035

- The traffic blackhole will be observed when the SRTE shortcut gets configured. PR1737119

- Traffic drop can be seen in the MPLS traffic Engineering scenario. PR1737594

- URL-Filtering few HTTP sites are getting bypassed and redirect does not occur. PR1737670

- PSoRLT Aggregate Stats: ipv4 leaf elements for ps transpfort ifl are exported , since ps is l2 interface no stats under ipv4 should be exported. PR1737935

- After picd restart, traffic was not recovered on MACsec enabled ports. PR1738038

- JV DB is missing leaf: /interfaces/interface[name=\'ae0\']/state/counters/out-octets, out-pkts, out-unicast-pkts, out-broadcast-pkts, out-multicast-pkts, in-errors, out-errors, in-discards ,out-discards ,in-pause-pkts, out-pause-pkts. PR1738395

- VC case not handled properly while calling brcm_vxlan_port_discard_set api. PR1738404

- PTP time sync issues after release upgrade or rebooting the device. PR1738458

- DHCP offer is dropped at MX and specific EX platforms when an lt interface is used as the transport. PR1738548
- An rpd crash will be observed due to inconsistency between rpd and kernel. PR1738820
- The interface goes down and the error message floods due to the FD leak in the picd process. PR1738854
- with multiple reboot srx300 going into panic: sleeping thread. PR1739219
- The ksyncd process crash would be seen on backup Routing Engine. PR1739258
- Installation of third party package on one Routing Engine and using auto-sync to add another Routing Engine into the dual Routing Engine setup might result in app not starting on the later inserting Routing Engine. PR1739286
- Memory leak in PKID. PR1739342
- FPC generates a core file and crashes in a race condition. PR1739595
- Duplicate BUM traffic is observed after the WAN interface flaps in the EVPN-VXLAN multihomed DC scenario. PR1739632
- FTC X FTC FPGA minimum supported firmware version mismatch alarm raised by OIR FTC. PR1739842
- Major alarms will be observed on the FPC when ALB is enabled under aggregated Ethernet interface. PR1739854
- FPC crashes and remains offline after the upgrade of RE BIOS to 0.15.1 version. PR1739922
- Layer 2 traffic will be dropped on VSTP disabled interface. PR1739975
- Traffic loss is seen due to anomalies after the recreation of IFLs. PR1740561
- System not bootable after request system zeroize. PR1740989
- The traffic drop is observed due to the MAC source address being learned from the incorrect direction. PR1741316
- The BGP routes gets stuck in BMP withdraw state. PR1741732
- Fans may stop working after removal and insertion of Fan Tray. PR1742174
- SPMB process will crash and PICs will not come online. PR1742186
- Tunnel interfaces are getting bounced causing a momentary impact on traffic. PR1742510
- Race condition where FLOOD ROUTE DEL event can cause l2ald crash. PR1742613

- Traffic verification failed for DHCPv6 relay. PR1743087
- The l2ald crashes when there is recursive deletion of IFBD or when BGP neighborship is cleared in EVPN-VXLAN multi-homed configuration. PR1743282
- FTI interface status (up/down) does not sync between master and backup Routing Engine. PR1743306
- The chassisd crash is observed on Junos MX204 platforms due to Fabric request timeout. PR1743379
- pppoe subscriber over PS ifd over rlt, when rlt mode change between active-active to active-backup, core ->subscriber direction, forwarding path uses the wrong Unilist aft node. PR1743515
- After this PR fix, to enable the xSTP support in ephemeral DB, below configuration command needs to be used: "set protocols layer2-control ephemeral-db-support". PR1743632
- Due to SPMB restarts in the middle of the FPC boot process, FPC wont come up. PR1743686
- The switch-options settings on the logical-system will be not reflected after Routing Engine rebooting or Routing Engine switchover. PR1743737
- If more than 32 VLAN ranges are configured under the dynamic-profile then login issue and traffic impact can be seen with subscribers of random VLANs. PR1743903
- Traffic drop is observed after the addition or removal of the "filter-specific" command under the policer. PR1743930
- GRE over IPv6 will not work resulting in traffic impact post-upgrading the device. PR1743978
- [USF - SPC3 - LOGGING] "log-tag" is not populated in the cgnat syslogs intermittently. PR1744563
- With multiple Traffic Selectors having same remote-ip, the traffic works only for first tunnel on MX Series platforms with SPC3 cards. PR1744601
- 100G interfaces will flap due to Routing Engine switchover on Junos MX platforms with MPC3E-3D-NG/MPC-3E-3D-NG-Q line cards. PR1744883
- Enhancement of PoE controller firmware files into Junos OS Software. PR1745088
- Fans may stop working after removal and insertion of Fan . PR1745299
- MPC10E - PIC bounce/config change on a PIC with 10G QSA adaptor can cause a FPC restart. PR1745317
- Packet drops might occur in the "show network-agent statistics detail" command when subscribing to sensors using gRPC. PR1745451

- rpd core at #2 0x00007f9b2512742c in __assert_fail_base (fmt=0x7f9b2528bae8 "%s%s%s:%u: %s %sAssertion `%s' failed.\n%n", assertion=0x55be37507a48 "nh_idx_t_getval(nhid) == nh_idx_t_getval(rt_nexthops_nhid(rtnh))", file=0x55be375077e8 "../../../../../../../../src/layer3/usr.sbin/rpd/lib/krt/common/krt_ack.c", line=1306, function=optimized out) at assert.c:92. PR1745509

- The hwdre application restarted due to memory leak. PR1745749

- The rpd crashes when BGP sharding, multipath and dynamic tunnel are configured. PR1746012

- Node-segment reachability gets lost in Multitopology based IS-IS. PR1746304

- MPC10E line card crashes when it reboots after FPC firmware upgrade. PR1746541

- Traffic degradation in 25% down might be seen under high load traffic at srx4600 with fpga v1.65. PR1746567

- PTP master feature will not work as expected. PR1746984

- Traffic from subscribers will be dropped by Junos based MX platforms. PR1747009

- On MX204 devices, INLINE NAT - address-prefix any-ipv4 reporting wrong. PR1747483

- Control board is stuck in Present state. PR1747567

- On MX2000 devices, the frequent fabric plane Check state reported due to remote destination timeouts PR1747893

- The memory consumption increases due to memory leak. PR1747992

- The rpd process shuts down on all Junos OS and Junos OS Evolved platforms. PR1749252

- Connectivity fails intermittently on 802.1x enabled ports. PR1749312

- Packet Forwarding Engine Flow ID doesn't shows correct in `show subscriber extensive` output. PR1749336

- Router crashes if routing services over PS are configured. PR1749748

- The authentication algorithm hmac-sha-256-128 for IPsec SA is not working and causing interoperability issues between Junos Evolved platforms and other devices. PR1749779

- IRB interface state remains up on local-remote option on all platforms along with EVPN-VxLAN configuration. PR1750146

- SyncE stuck in holdover upon PTP slot switchover without change in PTP phase align state. PR1750316

- On MX304 devices, ssh is not enabled by default. PR1750596

- Transferring or receiving traffic is impacted for SPC3 CPU cores connected to the affected PCIe bus when the SPC3 card boots up. PR1750634
- The mspmand daemon crashes causing traffic loss. PR1750823
- The Packet Forwarding Engine process crashed while removing and applying the firewall filters. PR1750828
- MPC10E: Support of G.8275.1 PTP Hybrid mode with speed 25G and 400G. PR1750885
- ARP learning issue for dynamic ARP entry for the DVLAN stacked frame route not resolved. PR1751656
- Traffic loss with preserve-nexthop-hierarchy enabled on MX platforms with a combination of MPC1-9, LC480, LC2101, and MPC10E, MPC11E, LC9600 line cards. PR1751699
- Incorrect egress MTU errors when larger than 1500 byte packets are sent on Layer 2 ports. PR1751700
- FPC reboots observed during ISSU on the MX10008 and MX10016 devices resulting in ISSU being unsuccessful. PR1751785
- Service PIC enabled with url-filtering may crash and gets into booting loop. PR1751860
- The mspmand process crashes when MPLS VRF Route table is not present for a MPLS route and MPLS route gets deleted. PR1752132
- Firmware upgrade will fail, if "set system services ssh root-login deny" command is present in configuration. PR1752765
- Port et-0/0/4 and xe-0/0/5:0 can not be up at the same when port 4 is configured as 100g and port 5 is configured as 1x10G on MX304 devices. PR1752831
- MPC11E suddenly goes offline due to power failure causing multitude fabric stream drain failures on all other MPC11. PR1753374
- FPC reboot can cause a crash while UDP streaming of packet usage sensor path. PR1753394
- PIM neighborship, or other control protocols flaps due to host-bound queue (Q3) congestion. PR1753853
- Incorrect egress encapsulation corrupting packets of IRB interface on MPC10E with MXVC results in traffic loss. PR1753951
- Traffic impact will be seen for static VoIP VLAN on access interface if same VLAN configured as data VLAN. PR1754474
- The "set services evpn global-parameters virtual-gateway v6-mac" command is broken. PR1754493

- The interface stats interrupt may be lost resulting in stats not getting updated. PR1755161
- Users authenticated through captive portal experience a noticeable delay of atleast 2 to 5 minutes. PR1755593
- Continuous fpc0-aftd-trio coredump on MX304 devices when turning up ipv6 neighbors with LMIC 2. PR1755950
- High CPU utilization observed after a few days of operation when BGP RIB sharding is enabled. PR1765417
- HMC errors will be observed on Junos platforms with LC480. PR1756780
- Prolonged SNMP polling leads to kernel crash in SCU/DCU scenario. PR1767098
- macsec license get cleared on master member post nssu/reboot. PR1757835
- Interface using QSA adapter with 1G speed wont work after upgrade to Junos OS 21.4R3-S4.9. PR1757878
- On MX10008 devices, PLD is higher than 2000 msec on ungraceful removal of a Fabric board. PR1758348
- The mcsnoopd process generates a core file with EVPN-MPLS and VPLS with multicast configuration. PR1758659
- The remote end of the link goes down on JNP10K-LC480 line card after unified ISSU. PR1758764
- On JNP10K-LC9600, shared-bandwidth-policer may be loaded into irrelevant Packet Forwarding Engine depending on choice of member port of aggregated Ethernet. PR1758935
- AFTD crash while rollback/config delete. PR1759899
- RPD process crash is seen post Routing Engine switchover. PR1759991
- On Junos OS and Junos OS Evolved platforms the rpd crashed abnormally and later chassisd crashed as well. PR1761667
- LLDP neighborship will not be formed on all Junos devices. PR1763053
- BFD session detection time is higher than expected leading to traffic drop. PR1763667
- Interface flaps leading to PFE crash due to FPC heap corruption. PR1764083
- High RPD CPU due to BMP station configuration. PR1764911
- A warning message is seen while installing a license key with an unknown feature. PR1766515

- PFE component of /interfaces/interface/subinterfaces/subinterface/state/ sensor might send data with frequency higher than requested by collector. PR1772266
- MX2K | SFB2 | MPC8E | FI: Reorder cell timeout | FI: Cell underflow | FI: Cell jump drop error. PR1774558
- After the device reboot the interested clients will not be able to receive the inactive routes. PR1774975
- JNP10K-PWR-AC3 PSM on MX10004 and MX10008 platforms display snmp mib walk jnxFruTemp updating just inlet TEMP sensor. Updating all supported temperature sensors is necessary. PR1775383
- In the BNG CUPS system after GRES subscribers will fail to login. PR1775539

High Availability (HA) and Resiliency

- The traffic drop is observed during the graceful restart on Junos OS and Junos OS Evolved platforms. PR1727957

Interfaces and Chassis

- Physical link remains stuck in down state on certain MX Series platforms. PR1707707
- Traffic impact will be seen with mismatched speeds on the LAG interface and member interface. PR1725168
- The lt/vt/ut interfaces may not recover from the disable-pfe (admin down) state if the GRES switchover is done before restarting FPC. PR1731190
- Changing speed and adding to aggregated Ethernet in the same commit fails. PR1743461
- Out of range "Near-end loss" percentage or jnxSoamLmCurrentStatsBackwardAvgFlr. PR1754637
- High memory utilization is observed on all Junos OS platforms. PR1757801
- Backup Routing Engine reset followed by Master Routing Engine reset traffic loss will be observed on aggregated Ethernet links. PR1767397

Junos Fusion Satellite Software

- Junos Fusion Satellite device will be stuck in the SyncWait state. PR1733558

Junos XML API and Scripting

- Junos OS platform device unable to commit configuration in recovery mode. PR1717425
- OpenConfig data obtained with gNMI GetRequest in json format displays module prefix. PR1736286

Layer 2 Ethernet Services

- DHCP binding is not happening in EVPN VXLAN topology with DHCP stateless relay (forward-only). PR1722082
- DHCP ALQ no-advertise-routes-on-backup functionality does not work in VRF for Framed-Route. PR1740822
- Active bulk leasequery is not working for IPv6 DHCP local server on MX Series platforms. PR1744162

MPLS

- Static MPLS LSP (transit) stats are not incrementing post the rpd restart. PR1719162
- LDP sync not complete with NSR (stuck at Inprogress forever) when "protocols ldp strict-targeted-hellos" is enabled when LDP signalled VPLS gets configured. PR1725519
- Traffic silently drops because of an additional label when CCNH is toggled. PR1738774
- LSP with auto bandwidth enabled is not updating its Max AvgBW value, preventing the LSP from being resized. PR1740226
- rpd crash observed during Routing Engine switchover or Route Convergence. PR1747365
- In-place-lsp-update failure causing ungraceful tear down of LSP. PR1756096
- Memory exhaustion leading to FPC core with auto-policing enabled MPLS with Multicast P2MP. PR1757984

- After the switchover, auto-bandwidth functionality does not work and LSPs do not get adjusted according to the traffic in the network. PR1772634

Network Management and Monitoring

- Syslog filter not functioning with generating /etc/syslog.conf+ file after syslog config is deactivated and re-activated. PR1726925
- The mgd process crash is observed in VMhost platforms during system reboot. PR1732379
- Syslog messages modification for SNMPv3 authentication failure. PR1734549

Platform and Infrastructure

- VRRP does not work when a firewall filter is configured to accept VRRP packets with a TTL value of 255. PR1701874
- Remote EVPN router is not receiving ARP packets for double-tag VLAN when sender is sent a packet from MPC10 and MPC11 line card. PR1718372
- ksyncd core with dhcp subscribers. PR1722708
- VPLS traffic gets blackholed by qualified-bum-pruning mode. PR1731564
- Heap memory leak on MPCs used for subscriber termination. PR1732690
- Intermittent flooding of traffic every 40 seconds. PR1736667
- The CoS rewrite rules will not be working in the EVPN with IRB scenario. PR1736890
- MPC1 to MPC13E/LC2101,LC2103,LC480/T4000-FPC5/MPC built-in Trio based line card reboots when subscriber management services are configured. PR1737615
- Host communication does not work in EVPN-L2VPN-CCC setup. PR1740606
- Inline-monitoring will not work as expected when more than one instances are configured. PR1742123
- PFE will wedge for RVTEP connectivity having unilist VENH. PR1743947
- `show system connections` and `show-routing-instances` reports all routing-instances as unknown. PR1746779

- PSoRLT telemetry | UDP | oc path /qos/interfaces/interface/output/queues/queue/state/ is not exporting results for ps IFL and lt interfaces | UDP sensor will be using different yang and there was a missing dr:source for a container which impacted the streaming in UDP. PR1750995
- [MX480/MX240] Multicast ping ff02::1 cannot perform reply on MX240/480 platform from MX204 through VXLAN. PR1751846
- The ksyncd process crashes with replication error after performing restart routing. PR1752151
- TCP window scaling may be not applied to the first TCP packet sent to the client after the three-way handshake, leading to unnecessary segmentation. PR1761242
- Routing protocol session down with native VLAN configuration on MX Series platforms. PR1763706
- core-dump-AFEB core happened with heap high. PR1770750
- In EVPN-MPLS Multi-Home Active/Active scenario, random packet drops observed. PR1772733
- Cos queueing issue with tunnel interface when HCOS hierarchy is configured on it. PR1772826

Routing Policy and Firewall Filters

- The static routes are installed in the routing table even though interface routes are not present. PR1714163
- Policy change to a rib-group import-policy configured with global routing-options interface-routes causes the rpd issue on all platforms with EVPN-VXLAN configuration. PR1744449

Routing Protocols

- The mscnoopd process crash will be observed when snooping configuration gets removed. PR1696374
- A crafted BGP UPDATE message allows a remote attacker to de-peer (reset) BGP sessions. PR1709837
- The PE advertises incorrect next-hop towards CE although BGP export policy configured with next-hop under policy-statement. PR1712527
- The RPD process gets stuck at a high CPU when OSPF areas are configured at a high scale and after starting the protocol. PR1728573

- Traffic impact is seen when there is a single peer in the proxy BGP group connected to the BGP route reflector. PR1728604

- BMP leads to prolonged high rpd CPU utilization upon committing the BGP peer import policy configuration. PR1729733

- The rpd process will crash in a scaled BGP setup with traceoptions configured. PR1732087

- IP-IP tunnel traffic drop is seen when "preserve-nexthop-hierarchy" command gets enabled. PR1733803

- Enabling bgp traceoptions flags will log frequently to the trace file. PR1735189

- RPD crash when attempting to send a very long AS PATH to a non-4-byte-AS capable BGP neighbor. PR1736029

- Commit FAILs when more than one locators are configured with same prefix. PR1736746

- The rpd crash files are seen due to a use-after free of objects. PR1737679

- OSPFv3 using the VIP address on the IRB interface will not form adjacencies between peers. PR1737978

- BFD session for BGP remains down in a specific scenario. PR1738074

- RPD crashes when multiple ISIS processes are configured. PR1738222

- Traffic loss will be seen in IPv6 only IS-IS topologies. PR1738901

- The rpd process crash will be observed when the prefix-limit exceeds on the backup Routing Engine. PR1739335

- The IPv6 link local based BFD session over an AE interface will be stuck in Init state. PR1739860

- Error message for mld static group configuration is not proper. PR1741370

- Memory leak observed when reconfiguring the flow routes. PR1742147

- Partial application of BGP import policy with BMP configuration and after back-to-back commits changes BGP import policy. PR1742222

- RPD scheduler slip is observed when the BGP session flaps and subsequent configuration changes for the same peer. PR1742416

- When BGP is configured in routing-instance of type virtual-router, default MPLS table is being created for that virtual-router, unexpectedly. PR1742513

- CPU in rpd spikes and scheduler slips will be observed when the duplicate community is added. PR1745073

- Route-distinguisher change leads to the route being present in rpd, but not installed in kernel/PFE. PR1746439
- Stale IP prefixes when issuing "show isis route flex-algorithm-id". PR1746557
- With RIB sharding configuration upon rpd restart the rpd crash will be observed. PR1748152
- Multi-instance isis route leaking for inet.3 is not working as expected. PR1748223
- The device will not be reachable over the loopback interface for the IS-IS nodes even though the neighborship might exist. PR1749850
- RPD may crash when deactivate protocol ISIS. PR1751210
- ISIS export policy does not export all default routes (IPv6 and IPv4) from BGP (or any other protocol). PR1751371
- Traffic drop is seen if chained-composite-next-hop is turned on for Segment Routing. PR1752551
- Deletion of routing-instance with 3K paths per prefix takes a long time with the rpd CPU usage at 100 percent. PR1752594
- The rpd crashes on all Junos and Junos Evolved platforms with IS-IS, segment routing and flex algo configured. PR1753003
- The BFD process crash will be observed when telemetry is used. PR1754535
- BGP multipath route is not correctly applied after changing the IGP metric. PR1754935
- The BGP LU labels can have next-hops pointing to each other in multi-homed PE setup. PR1760885
- Memory spike will be observed on the system with BFD enabled for OSPF/ISIS. PR1761232
- The rpd process crashes after clearing ISIS database or restarting the rpd process. PR1759728
- An rpd crash is observed when mvpn-mode is configured as "rpt-spt" and multicast snooping is enabled. PR1769782

Services Applications

- L2TP tunnels may time out if creation of bbe-smgd core dump takes a long time. PR1720994
- Crash file is generated when local certificate keychain is missed repeatedly. PR1728605

Subscriber Access Management

- Potential memory leak in authd process. PR1729035
- Test aaa command may failure due to "Subscriber creation failed". PR1759048
- BNG Dynamic Pools JUNOS 22.4R3: Algorithm to determine prefix count for apportionment requests to APM is over aggressive. PR1768651

User Interface and Configuration

- After the device reboot BGP sessions configured with authentication will be down. PR1726731
- The 'load replace' operation might result in mustd and mgd crash. PR1740289
- Attribute GLOBALIPOWNER does not exist is reported on primary Routing Engine when commit synchronizes to secondary Routing Engine. PR1741284
- The `commit confirm` and `commit race condition` commands crashes the firewall functionality. PR1743038
- The mgd process crash is observed when 'show' is executed from the configuration mode. PR1745565
- Subsequent commits hang will be seen, when transfer-on-commit fails. PR1752374

VPNs

- In MPLS-L2VPN/BGP-VPLS setup the flow-label route update is not propagating to neighbouring devices. PR1751717

Migration, Upgrade, and Downgrade Instructions

IN THIS SECTION

This section contains the procedure to upgrade Junos OS, and the upgrade and downgrade policies for Junos OS for the MX Series. Upgrading or downgrading Junos OS might take several minutes, depending on the size and configuration of the network.

Basic Procedure for Upgrading to Release 23.4R2

NOTE: Before upgrading, back up the file system and the currently active Junos OS configuration so that you can recover to a known, stable environment in case the upgrade is unsuccessful. Issue the following command:

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

The installation process rebuilds the file system and completely reinstalls Junos OS. Configuration information from the previous software installation is retained, but the contents of log files might be erased. Stored files on the routing platform, such as configuration templates and shell scripts (the only exceptions are the juniper.conf and ssh files might be removed. To preserve the stored files, copy them to another system before upgrading or downgrading the routing platform. For more information, see the Installation and Upgrade Guide.

For more information about the installation process, see Installation and Upgrade Guide and Upgrading Junos OS with Upgraded FreeBSD.

Procedure to Upgrade to Junos OS

To download and install Junos OS:

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. Select the name of the Junos OS platform for the software that you want to download.

3. Select the release number (the number of the software version that you want to download) from the Release drop-down list to the right of the Download Software page.

4. Select the Software tab.

5. In the Install Package section of the Software tab, 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.

9. Copy the software to the routing platform or to your internal software distribution site.

10. Install the new jinstall package on the routing platform.

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

All customers except the customers in the Eurasian Customs Union (currently composed of Armenia, Belarus, Kazakhstan, Kyrgyzstan, and Russia) can use the following package:

- For 32-bit Routing Engine version:

```
user@host> request system software add no-validate reboot source/junos-install-mx-x86-32-23.4R2.9-signed.tgz
```

- For 64-bit Routing Engine version:

```
user@host> request system software add no-validate reboot source/junos-install-mx-x86-64-23.4R2.9-signed.tgz
```

Customers in the Eurasian Customs Union (currently composed of Armenia, Belarus, Kazakhstan, Kyrgyzstan, and Russia) can use the following package (Limited encryption Junos package):

- For 32-bit Routing Engine version:

  ```
  user@host> request system software add no-validate reboot source/junos-install-mx-x86-32-23.4R2.x-limited.tgz
  ```

- For 64-bit Routing Engine version:

  ```
  user@host> request system software add no-validate reboot source/junos-install-mx-x86-64-23.4R2.9-limited.tgz
  ```

Replace source with one of the following values:

- ***/pathname***—For a software package that is installed from a local directory on the router.
- For software packages that are downloaded and installed from a remote location:
  - **ftp://*hostname*/*pathname***
  - **http://*hostname*/*pathname***
  - **scp://*hostname*/*pathname***

Use the `reboot` command to reboot the router after the upgrade is validated and installed. When the reboot is complete, the router displays the login prompt. The loading process might take 5 to 10 minutes.

Rebooting occurs only if the upgrade is successful.

NOTE:

- You need to install the Junos OS software package and host software package on the routers with the RE-MX-X6 and RE-MX-X8 Routing Engines. For upgrading the host OS on these routers with VM Host support, use the junos-vmhost-install-x.tgz image and specify the name of the regular package in the `request vmhost software add` command. For more information, see the VM Host Installation topic in the Installation and Upgrade Guide.
- Starting in Junos OS Release 23.4R2, in order to install a VM host image based on Wind River Linux 9, you must upgrade the i40e NVM firmware on the following MX Series routers:

- MX240, MX480, MX960, MX2010, MX2020, MX2008, MX10016, and MX10008

[See https://kb.juniper.net/TSB17603.]

NOTE: Most of the existing `request system` commands are not supported on routers with the RE-MX-X6 and RE-MX-X8 Routing Engines. See the VM Host Software Administrative Commands in the Installation and Upgrade Guide.

Upgrade and Downgrade Support Policy for Junos OS Releases

We have two types of releases, standard EOL and EEOL:

- Standard End of Life (EOL) releases have engineering support for twenty four months after the first general availability date and customer support for an additional six more months.
- Extended End of Life (EEOL) releases have engineering support for sixty months after the first general availability date and customer support for an additional six more months.

NOTE: The sixty months of support for EEOL releases is introduced in Junos OS 23.2 release and is available for all later releases. For releases prior to 23.2, the support for EEOL releases continues to be thirty six months.

For both standard EOL and EEOL releases, you can upgrade to the next three subsequent releases or downgrade to the previous three releases.

For EEOL releases only, you have an additional option - you can upgrade directly from one EEOL release to the next two subsequent EEOL releases, even if the target release is beyond the next three releases. Likewise, you can downgrade directly from one EEOL release to the previous two EEOL releases, even if the target release is beyond the previous three releases.

Table 4: EOL and EEOL Releases

Release Type	End of Engineering (EOE)	End of Support (EOS)	Upgrade/ Downgrade to subsequent 3 releases	Upgrade/ Downgrade to subsequent 2 EEOL releases
Standard End of Life (EOL)	24 months	End of Engineering + 6 months	Yes	No
Extended End of Life (EEOL)	60 months	End of Engineering + 6 months	Yes	Yes

For more information about standard EOL and EEOL releases, see https://www.juniper.net/support/eol/junos.html.

For information about software installation and upgrade, see the Installation and Upgrade Guide.

Upgrading a Router with Redundant Routing Engines

If the router has two Routing Engines, perform the following Junos OS installation on each Routing Engine separately to avoid disrupting network operation:

1. Disable graceful Routing Engine switchover (GRES) on the master Routing Engine, and save the configuration change to both Routing Engines.

2. Install the new Junos OS release on the backup Routing Engine while keeping the currently running software version on the master Routing Engine.

3. After making sure that the new software version is running correctly on the backup Routing Engine, switch over to the backup Routing Engine to activate the new software.

4. Install the new software on the original master Routing Engine that is now active as the backup Routing Engine.

For the detailed procedure, see the Installation and Upgrade Guide.

Downgrading from Release 23.4R2

To downgrade from Release 23.4R2 to another supported release, follow the procedure for upgrading, but replace the 23.4R2 jinstall package with one that corresponds to the appropriate release.

NOTE: You cannot downgrade more than three releases.

For more information, see the Installation and Upgrade Guide.

Junos OS Release Notes for NFX Series

IN THIS SECTION

What's New

There are no new features or enhancements to existing features in this release for the NFX Series.

To view features supported on the NFX platforms, view the Feature Explorer using the following links. To see which features were added in Junos OS Release 23.4R2, click the Group by Release link. You can collapse and expand the list as needed.

- NFX150
- NFX250
- NFX350

What's Changed

There are no changes in behavior and syntax in this release for NFX Series devices.

Known Limitations

IN THIS SECTION

Learn about known limitations in this release for NFX Series devices.

For the most complete and latest information about known Junos OS defects, use the Juniper Networks online Junos Problem Report Search application.

General Routing

- On the NFX platforms, when one partition supports a Junos OS Release 23.4R1 image (supported on LTS19 operating sytem) and the other partition supports an image older than Junos OS Release 23.4R1 (supported on WRL8 operating system), the `request vmhost reboot disk` command is not executed as expected.

  As a workaround, upgrade both the partitions with same image versions PR1753117.

Virtual Network Functions (VNFs)

- On NFX150 devices, before reusing a VF to Layer 3 data plane interfaces (for example, ge-1/0/3), which was earlier allocated to a VNF, you must restart the system. PR1512331

Open Issues

IN THIS SECTION

Learn about open issues in this release for NFX Series devices.

For the most complete and latest information about known Junos OS defects, use the Juniper Networks online Junos Problem Report Search application.

Interfaces

- On the NFX250, the LACP subsystem does not start automatically when the dc-pfe process is restarted.

  Workaround—Deactivate and then activate the aggregated Ethernet interface.

  PR1583054.

General Routing

- On the NFXplatforms when one partition supports a Junos OS Release 23.4R1 image (supported on LTS19 operating sytem) and the other partition supports an image older than Junos OS Release 23.4R1 (supported on WRL8 operating system), the request vmhost reboot disk command is not executed as expected PR1753117..
- On the NFX350 devices, `srxpfe core` is seen.PR1792616.
- On the NFX350 devices, `libvirtMib_suba.core.tgz` is seen.PR1675919

High Availability (HA) and Resiliency

- When high availability (HA) is enabled and fabric links are configured on NFX devices (NFX150, NFX250 and NFX350 with nfx-3 software package), the fabric link monitored status is displayed as `Down` leading to an `FL` status.PR1794559

VNF

- In Junos OS Release 23.4R1, on NFX devices with nfx-3 architecture, cpu utilization by vcpu thread of vjunos0 is high. Same behavior may be observed with the vcpu thread of any VNF.PR1727654

Resolved Issues

IN THIS SECTION

Learn about the issues fixed in this release for NFX Series.

For the most complete and latest information about known Junos OS defects, use the Juniper Networks online Junos Problem Report Search application.

Interfaces

- Starting in Junos OS Release 23.4R1 release, when you run the command `show chassis alarm` on NFX 350 devices, the output displays `Major TSensor 3:Coretemp Access Failed` due to swapping of the symlinks of hwmon0 and hwmon1.PR1769699

Network Address Translation

- On the NFX devices when the NAT port number or the IP address of the peer device located behind a Network address translation (NAT) device is changed, the next Dead Peer Detection (DPD) or rekey process fails to update the port number in the existing tunnel NAT Traversal (NAT-T) flow session. The failure to update the port-number happens if the DPD is configured as `always-send`. This condition leads to communication failure over the Internet Protocol Security (IPsec) tunnel.

  PR1776216

VNFs

- On Junos NFX350 Platforms, in spite of disabling the Auto Negotiation (AN) on the interface through configuration, it stays enabled on the copper ports.This could result in mismatch of AN settings with the remote side configuration and disrupt traffic. PR1719973.
- On the NFX platforms, the `pfe` (Packet Forwarding Engine) process crashes when configured with custom mode templates like flex mode or any other custom mode due to memory exhaustion. PR1776815

Migration, Upgrade, and Downgrade Instructions

IN THIS SECTION

This section contains the procedure to upgrade Junos OS, and the upgrade and downgrade policies for Junos OS for the NFX Series. Upgrading or downgrading Junos OS might take several hours, depending on the size and configuration of the network.

NOTE: For information about NFX product compatibility, see NFX Product Compatibility.

Upgrade and Downgrade Support Policy for Junos OS Releases

We have two types of releases, standard EOL and EEOL:

- Standard End of Life (EOL) releases have engineering support for twenty four months after the first general availability date and customer support for an additional six more months.
- Extended End of Life (EEOL) releases have engineering support for sixty months after the first general availability date and customer support for an additional six more months.

NOTE: The sixty months of support for EEOL releases is introduced in Junos OS 23.2 release and is available for all later releases. For releases prior to 23.2, the support for EEOL releases continues to be thirty six months.

For both standard EOL and EEOL releases, you can upgrade to the next three subsequent releases or downgrade to the previous three releases.

For EEOL releases only, you have an additional option - you can upgrade directly from one EEOL release to the next two subsequent EEOL releases, even if the target release is beyond the next three releases. Likewise, you can downgrade directly from one EEOL release to the previous two EEOL releases, even if the target release is beyond the previous three releases.

Table 5: EOL and EEOL Releases

Release Type	End of Engineering (EOE)	End of Support (EOS)	Upgrade/ Downgrade to subsequent 3 releases	Upgrade/ Downgrade to subsequent 2 EEOL releases
Standard End of Life (EOL)	24 months	End of Engineering + 6 months	Yes	No
Extended End of Life (EEOL)	60 months	End of Engineering + 6 months	Yes	Yes

For more information about standard EOL and EEOL releases, see https://www.juniper.net/support/eol/junos.html.

For information about software installation and upgrade, see the Installation and Upgrade Guide.

For more information on EEOL releases and to review a list of EEOL releases, see https://www.juniper.net/support/eol/junos.html.

Basic Procedure for Upgrading to Release 23.4

When upgrading or downgrading Junos OS, use the `jinstall` package. For information about the contents of the `jinstall` package and details of the installation process, see the Installation and Upgrade Guide. Use other packages, such as the `jbundle` package, only when so instructed by a Juniper Networks support representative.

> **NOTE**: The installation process rebuilds the file system and completely reinstalls Junos OS. Configuration information from the previous software installation is retained, but the contents of log files might be erased. Stored files on the device, such as configuration templates and shell scripts (the only exceptions are the juniper.conf and ssh files), might be removed. To preserve the stored files, copy them to another system before upgrading or downgrading the device. For more information, see the Software Installation and Upgrade Guide.

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

To download and install Junos OS Release 23.4R2:

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. Select the name of the Junos OS platform for the software that you want to download.

3. Select the **Software** tab.

4. Select the release number (the number of the software version that you want to download) from the Version drop-down list to the right of the Download Software page.

5. In the Install Package section of the Software tab, 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 Juniper Networks representatives.

7. Review and accept the End User License Agreement.

8. Download the software to a local host.

9. Copy the software to the device or to your internal software distribution site.

10. Install the new package on the device.

Junos OS Release Notes for QFX Series

IN THIS SECTION

What's New

IN THIS SECTION

Learn about new features introduced in this release for QFX Series switches.

To view features supported on the QFX platforms, view the Feature Explorer using the following links. To see which features were added in Junos OS Release 23.4R2, click the Group by Release link. You can collapse and expand the list as needed.

- QFX10002
- QFX10008
- QFX10016
- QFX10002-60C

Hardware

EVPN

- **Enhanced OISM in EVPN-VXLAN ERB overlay networks with an IPv6 underlay (EX4100-48MP, EX4100-24MP, EX4100-48P, EX4100-48T, EX4100-24P, EX4100-24T, EX4100-F-48P, EX4100-F-24P, EX4100-F-48T, EX4100-F-24T, EX4100-F-12P, EX4100-F-12T, EX4400-24MP, EX4400-24P, EX4400-24T, EX4400-24X, EX4400-48F, EX4400-48MP, EX4400-48P, EX4400-48T, EX4650, QFX5120-32C, QFX5120-48T, QFX5120-48Y, and QFX5120-48YM)**—Starting in Junos OS Release 23.4R2, you can configure enhanced optimized intersubnet multicast (OISM) for IPv4 and IPv6 multicast data traffic with an Ethernet VPN–Virtual Extensible LAN (EVPN-VXLAN) edge-routed bridging (ERB) overlay network that has an IPv6 underlay. To configure this feature:

    - Set up the EVPN-VXLAN fabric with an IPv6 underlay:

        - You can use either external BGP (EBGP) or OSPFv3 with IPv6 addressing for the IPv6 underlay.

        - Use the `inet6` option when you set the VXLAN tunnel endpoint (VTEP) source interface to the device loopback interface in the EVPN instance (EVI):

          ```
          set routing-instances evpn-instance-name vtep-source-interface lo0.0 inet6
          ```

    - Configure the enhanced OISM elements for your multicast EVPN-VXLAN environment in the same way you would configure these elements in an EVPN-VXLAN network with an IPv4 underlay.

      You can configure any of the supported platforms as enhanced OISM server leaf devices, and only EX4650 and QFX5120 switches as enhanced OISM border leaf devices.

  [See EVPN-VXLAN with an IPv6 Underlay and Optimized Intersubnet Multicast in EVPN Networks.]

Software Installation and Upgrade

- **In-band ZTP management in campus fabrics (EX4100-24MP, EX4100-48MP, EX4100-48P, EX4100-48T, EX4100-24P, EX4100-24T, EX4100-F-48P, EX4100-F-24P, EX4100-F-48T, EX4100-F-24T, EX4100-F-12P, EX4100-F-12T, EX4400-24MP, EX4400-24P, EX4400-24T, EX4400-24X, EX4400-48F, EX4400-48MP, EX4400-48P, EX4400-48T, EX4650, EX9204, EX9208, EX9214, MX304, QFX5120-32C, QFX5120-48T, QFX5120-48Y, and QFX5120-48YM)**—Starting in Junos OS Release 23.4R2, you can simplify the provisioning process for campus fabrics. Already provisioned upstream devices, such as core and distribution devices, that are capable of detecting downstream Day 0 devices can provide Layer 3 (L3) connectivity. With L3 connectivity, the downstream Day 0 devices can proceed with secure zero-touch provisioning (SZTP).

To configure in-band ZTP management, include the `in-band-ztp` statement at the `[edit system services]` hierarchy level on your core and distribution devices. Optionally, your cloud controller can provide the `in-band-ztp` configuration as part of the provisioning process for your core and distribution devices.

[See Zero Touch Provisioning.]

Additional Features

We've extended support for the following features to these platforms.

- **Supported transceivers, optical interfaces, and DAC cables** Select your product in the Hardware Compatibility Tool (https://apps.juniper.net/hct/product/) to view supported transceivers, optical interfaces, and direct attach copper (DAC) cables for your platform or interface module. We update the HCT and provide the first supported release information when the optic becomes available.

What's Changed

IN THIS SECTION

Learn about what changed in this release for QFX Series Switches.

EVPN

- **Limit on number of IP address associations per MAC address per bridge domain in EVPN MAC-IP database**—By default, devices can associate a maximum of 200 IP addresses with a single MAC address per bridge domain. We provide a new CLI statement to customize this limit, `mac-ip-limit` statement at the **edit protocols evpn** hierarchy level. In most use cases, you do not need to change the default limit. If you want to change the default limit, we recommend that you do not set this limit to more than 300 IP addresses per MAC address per bridge domain. Otherwise, you might see very high CPU usage on the device, which can degrade system performance.

See [mac-ip-limit.]

General Routing

- **Change in options and generated configuration for the EZ-LAG configuration IRB subnet-address statement**— With the EZ-LAG `subnet-address inet` or `subnet-address inet6` options at the [`edit services evpn evpn-vxlan irb` *`irb-instance`*] hierarchy, you can now specify multiple IRB subnet addresses in a single statement using the list syntax `addr1 addr2 ...`. Also, in the generated configuration for IRB interfaces, the commit script now includes default `router-advertisement` statements at the [`edit protocols`] hierarchy level for that IRB interface.

  [See subnet-address (Easy EVPN LAG Configuration).]

Infrastructure

- **Option to disable path MTU discovery**— Path MTU discovery is enabled by default. To disable it for IPv4 traffic, you can configure the `no-path-mtu-discovery` statement at the [`edit system internet-options`] hierarchy level. To reenable it, use the `path-mtu-discovery` statement.

  [See Path MTU Discovery.]

Routing Protocols

- **Optimized mesh group routes (QFX5110, QFX5120, QFX5130, QFX5700 and ACX Series)**— The `show route snooping` for inet.1/inet6.1 table and `show route snooping table inet.1/inet6.1` will display only CE mesh group routes for platforms that support EVPN-MPLS or EVPN-VXLAN multicast. In earlier releases, other mesh groups like the VE mesh group were also displayed.

VPNs

- **Increase in revert-delay timer range**— The `revert-delay` timer range is increased to 600 seconds from 20 seconds.

[See min-rate.]

- **Configure min-rate for IPMSI traffic explicitly**— In a source-based MoFRR scenario, you can set a min-rate threshold for IPMSI traffic explicitly by configuring `ipmsi-min-rate` under `set routing-instances protocols mvpn hot-root-standby min-rate`. If not configured, the existing `min-rate` will be applicable to both IPMSI and SPMSI traffic.

  See [min-rate.]

Known Limitations

IN THIS SECTION

Learn about known limitations in this release for QFX Series switches.

For the most complete and latest information about known Junos OS defects, use the Juniper Networks online Junos Problem Report Search application.

Infrastructure

- When upgrading from releases before Junos OS Release 21.2 to Release 21.2 and onward, validation and upgrade might fail. The upgrade requires using the `no-validate` option to complete successfully. PR1568757

Open Issues

IN THIS SECTION

Learn about open issues in this release for QFX Series switches.

For the most complete and latest information about known Junos OS defects, use the Juniper Networks online Junos Problem Report Search application.

General Routing

- On QFX10002, QFX10008, and QFX10016 switches, the following error message is observed during specific steps while clearing and loading the scaled configuration again: PRDS_SLU_SAL:jprds_slu_sal_update_lrncnt(),1379: jprds_slu_sal_update_lrncnt call failed. This issue is observed in a scaled setup with scaled VLANS and traffic flowing through all VLANS. If the configuration is cleared and loaded again using the below steps: load override <base-config> rollback 1 commit Then the base configuration is loaded, all leaned MACs are aged out and the MAC entries are marked as invalid. Aging thread scans and finds SMAC ref bit transition for cleared MAC entries and gets added to a stale MAC software table. In a scaled setup where 2000 MACs are learned over a port, not all MACs are cleared at one hardware trigger. This happens in a batch of 256 entries in a MAC table at a time as per the design of the QFX10000 lines of switches. In the meantime, it is expected that IFBD on which the MACs were learned is deleted. This is the reason why Lport+IFL mapping is not found while clearing such MACs and throws an error. PR1522852

- When TISSU upgrade is done from 22.4 release onwards, the box come up as backup Routing Engine. Work-around:- To make is primary following command needs to be run again. sysctl -w hw.lc.issuboot=0 sleep 10 sysctl -w hw.re.issu_state=0 sleep 10 sysctl -w hw.re.tissu=0 sleep 10 sysctl -w hw.product.pvi.config.chasd.no_re_status_on_backup=1 sleep 60PR1703229

- Disable the VME interfaces or have the default route added properly from the shell script for the connectivity with the ZTP server to work. PR1743222

- On all Junos OS platforms, due to timing issues the PFE (Packet Forwarding Engine) /PICs (Physical Interface Card) will be slow and services will face slowness issue and error message: **Minor potential slow peers are: X** will be seen. This is rare timing issue. PR1747077

Interfaces and Chassis

- The LAG (Link Aggregation Group) member links might flap on all Junos OS platforms except MX when the configuration of any interface is changed or modified. The flap is not seen always. PR1679952

Resolved Issues

IN THIS SECTION

Learn about the issues fixed in this release for QFX Series switches.

For the most complete and latest information about known Junos OS defects, use the Juniper Networks online Junos Problem Report Search application.

EVPN

- EVPN-VXLAN comp nh is not installed in Packet Forwarding Engine after peer reboot. PR1739686

- After deactivating or activating GBP configuration in the MH AE scenario all tag entries not getting re-learned on leaf nodes in the ethernet-switching table resulting in traffic loss. PR1739878

- ARP or FIB are added even if IRB in EVPN is disabled. PR1743529

- IRB reachability issues might be observed in the EVPN-VXLAN environment when looped ARP comes on ESI-LAG. PR1743913

- MAC addresses programming failure resulting in traffic flooding. PR1758677

General Routing

- Minor packet drops due to hardware programming issues. PR1700927

- The dcpfe process will crash due to memory fragmentation. PR1711860

- QSFP-100G-LR4-T2 optics will stay down after ISSU/TISSU. PR1713010

- The dot1x-protocol subsystem is not responding to management requests while verifying in show security mka sessions. PR1713881

- IGMP/MLD queries might get dropped if received on a port on the backup VC member when IGMP/MLD snooping is enabled. PR1716902

- Layer 2 Multicast traffic drops when PIM is configured without IGMP snooping enabled. PR1720527

- Momentary traffic loss is observed when interface with local Type-1 ESI goes down. PR1722348

- The error logs **fpc0 expr_hostbound_packet_handler: Receive pe 254?** would be generated. PR1725716

- The class of service subsystem crashed after the device is restarted or the switchover is performed. PR1726124

- The EVPN-VXLAN proxy-arp will respond with the wrong MAC when no-mac-learning is configured. PR1727119

- On all Junos OS platforms, the l2ald process memory usage is seen to increase over time. PR1727954

- [QFX] debugging command `show aq107 xxx` on VTY might generate an error on 10GBASE-T SFP if AQ index exceeds 48. PR1728452

- Traffic loss will be observed due to CRC errors with QSFP+-40G-ACU10M plugged. PR1729067

- Traffic drops when any of the VXLAN VLAN is deleted. PR1731583

- On router reboot an interface in SP style blocks all packets on **family inet/inet6** interfaces if VSTP is configured on vlan-bridge encapsulated VLANs. PR1732718

- Traffic loss is seen when `lacp force-up` configuration statement is configured. PR1733543

- Online SIBs will go down due to a faulty SIB that triggers spmbpfe crash. PR1734734
- Packet drop is observed due to SIB ASIC issue on fabric. PR1734735
- BFD session remains stuck in INIT state on certain QFX platforms. PR1736348
- Unexpected VLAN tagging behavior would be observed in the EVPN-VXLAN scenario. PR1736954
- Blackholing of l3-inject traffic on QFX10000 platforms. PR1738197
- Traffic drop observed when encapsulation ethernet-bridge is configured on the AE interface associated with VxLAN VLAN. PR1738205
- High convergence time in the EVPN-VxLAN uplink failover scenario. PR1738276
- VC case not handled properly while calling brcm_vxlan_port_discard_set api. PR1738404
- An rpd crash will be observed due to inconsistency between rpd and kernel. PR1738820
- DSCP classifier is not created on IP interfaces. PR1738981
- The ksyncd process crash would be seen on backup Routing Engine. PR1739258
- The loop-detect is not working in the VXLAN scenario. PR1740327
- Traffic loss is seen due to anomalies after the recreation of IFLs. PR1740561
- Enabling sflow triggers ddos-protection violation of protocol group resolve. PR1741461
- SPMB process will crash and PICs will not come online. PR1742186
- Traffic dropped is observed in the MPLS LDP scenario when the peer device MAC address is changing. PR1742364
- Race condition where FLOOD ROUTE DEL event can cause l2ald crash. PR1742613
- Traffic drop will be observed after extended-vni-list configuration change with EVPN-VXLAN scenario. PR1742763
- GRE over IPv6 will not work resulting in traffic impact post-upgrading the device. PR1743978
- BPDU Protection with packet-action drop support on QFX10002-60C. PR1745102
- Clear error command support for QFX10002-60c. PR1746244
- QFX10002-60c port et-0/0/30 part of a lag is dropping peer ARP reply after configuring a GRE tunnel. PR1746435
- Soft OIR of the link connected to 10GBASE-T SFP will not update the link state at the other end. PR1747277

- Alarm LED is lit due to LICENSE_EXPIRED on Virtual Chassis backup even with the valid license. PR1747720
- Traffic drop will be observed when Label MPLS traffic egressing out on the IRB interface as IPV4. PR1748500
- L3VPN traffic destined for hosts learned over IRB/VXLAN will get dropped on QFX10000 platforms. PR1750468
- The PFE process crashed while removing and applying the firewall filters. PR1750828
- Incorrect egress MTU errors when larger than 1500 byte packets are sent on Layer 2 ports. PR1751700
- PIM neighborship, or other control protocols flaps due to host-bound queue (Q3) congestion. PR1753853
- QFX: VC(virtual chassis) does not get formed when using 100G for vc port. PR1754838
- Learning stops in logical interface in QFX10000 platforms. PR1756672
- The dcpfe process crash will be seen when L2PT interfaces are configured with multiple protocols. PR1757329
- The mcsnoopd cored with EVPN-MPLS and VPLS with multicast configuration. PR1758659
- Generate an empty file whose name is secondary_vlan when executing RSI. PR1759875
- Traffic drop will be seen when packets are sent with incorrect VLAN tag. PR1760823
- ECMP traffic drop after the AE interface flap. PR1761887
- LLDP neighborship will not be formed on all Junos OS devices. PR1763053
- VPLAG information not installed correctly in hardware results in traffic flooding. PR1763116
- BFD session detection time is higher than expected leading to traffic drop. PR1763667
- A warning message is seen while installing a license key with an unknown feature. PR1766515
- The PVST BPDU packet get dropped in transparent EVPN-VXLAN on the ingress PE-CE port of SP style on Junos OS QFX platforms. PR1771739

Interfaces and Chassis

- Traffic impact will be seen with mismatched speeds on the LAG interface and member interface. PR1725168
- High memory utilization is observed on all Junos OS platforms. PR1757801
- Services using the management interface will be affected on all Junos OS platforms. PR1757936

Junos XML API and Scripting

- Junos OS platform device unable to commit configuration in recovery mode. PR1717425

Layer 2 Ethernet Services

- DHCP binding is not happening in EVPN VXLAN topology with DHCP stateless relay (forward-only). PR1722082

MPLS

- The rpd crash observed during RE switchover or Route Convergence. PR1747365

Platform and Infrastructure

- The CoS rewrite rules will not be working in the EVPN with IRB scenario. PR1736890

Routing Policy and Firewall Filters

- Policy change to a rib-group import-policy configured with global routing-options interface-routes causes the rpd issue on all platforms with EVPN-VXLAN configuration. PR1744449

Routing Protocols

- Memory leak observed when reconfiguring the flow routes. PR1742147
- Route-distinguisher change leads to the route being present in rpd, but not installed in kernel/PFE. PR1746439
- BGP multipath route is not correctly applied after changing the IGP metric. PR1754935

Migration, Upgrade, and Downgrade Instructions

IN THIS SECTION

This section contains the procedure to upgrade Junos OS, and the upgrade and downgrade policies for Junos OS. Upgrading or downgrading Junos OS can take several hours, depending on the size and configuration of the network.

Upgrading Software on QFX Series Switches

When upgrading or downgrading Junos OS, always use the jinstall package. Use other packages (such as the jbundle package) only when so instructed by a Juniper Networks support representative. For information about the contents of the jinstall package and details of the installation process, see the Installation and Upgrade Guide and Junos OS Basics in the QFX Series documentation.

If you are not familiar with the download and installation process, follow these steps:

1. In a browser, go to https://www.juniper.net/support/downloads/junos.html.

   The Junos Platforms Download Software page appears.

2. In the QFX Series section of the Junos Platforms Download Software page, select the QFX Series platform for which you want to download the software.

3. Select **23.4** in the Release pull-down list to the right of the Software tab on the Download Software page.

4. In the Install Package section of the Software tab, select the QFX Series Install Package for the 23.4 release.

   An Alert box appears.

5. In the Alert box, click the link to the PSN document for details about the software, and click the link to download it.

   A login screen appears.

6. Log in to the Juniper Networks authentication system using the username (generally your e-mail address) and password supplied by Juniper Networks representatives.

7. Download the software to a local host.

8. Copy the software to the device or to your internal software distribution site.

9. Install the new jinstall package on the device.

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

   Customers in the United States and Canada use the following command:

   ```
   user@host> request system software add source/jinstall-host-qfx-5-x86-64-23.4-R2.n-secure-
   signed.tgz reboot
   ```

   Replace *source* with one of the following values:

   - ***/pathname***—For a software package that is installed from a local directory on the switch.

- For software packages that are downloaded and installed from a remote location:
  - **ftp://*hostname/ pathname***
  - **http://*hostname/ pathname***
  - **scp://*hostname/ pathname*** (available only for Canada and U.S. version)

Adding the `reboot` command reboots the switch after the upgrade is installed. When the reboot is complete, the switch displays the login prompt. The loading process can take 5 to 10 minutes.

Rebooting occurs only if the upgrade is successful.

NOTE: After you install a Junos OS Release 23.4 `jinstall` package, you can issue the `request system software rollback` command to return to the previously installed software.

Installing the Software on QFX10002-60C Switches

This section explains how to upgrade the software, which includes both the host OS and the Junos OS. This upgrade requires that you use a VM host package—for example, a **junos-vmhost-install-*x*.tgz** .

During a software upgrade, the alternate partition of the SSD is upgraded, which will become primary partition after a reboot .If there is a boot failure on the primary SSD, the switch can boot using the snapshot available on the alternate SSD.

NOTE: The QFX10002-60C switch supports only the 64-bit version of Junos OS.

NOTE: If you have important files in directories other than /config and /var, copy the files to a secure location before upgrading. The files under /config and /var (except /var/etc) are preserved after the upgrade.

To upgrade the software, you can use the following methods:

If the installation package resides locally on the switch, execute the **request vmhost software add *<pathname><source>*** command.

For example:

```
user@switch> request vmhost software add /var/tmp/junos-vmhost-install-qfx-x86-64-20.4R1.9.tgz
```

If the Install Package resides remotely from the switch, execute the **request vmhost software add *<pathname><source>*** command.

For example:

```
user@switch> request vmhost software add ftp://ftpserver/directory/junos-vmhost-install-qfx-
x86-64-20.4R1.9.tgz
```

After the reboot has finished, verify that the new version of software has been properly installed by executing the `show version` command.

```
user@switch> show version
```

Installing the Software on QFX10002 Switches

NOTE: If you are upgrading from a version of software that does not have the FreeBSD 10 kernel (15.1X53-D30, for example), you will need to upgrade from Junos OS Release 15.1X53-D30 to Junos OS Release 15.1X53-D32. After you have installed Junos OS Release 15.1X53-D32, you can upgrade to Junos OS Release 15.1X53-D60 or Junos OS Release 18.3R1.

NOTE: On the switch, use the `force-host` option to force-install the latest version of the Host OS. However, by default, if the Host OS version is different from the one that is already installed on the switch, the latest version is installed without using the `force-host` option.

If the installation package resides locally on the switch, execute the **request system software add *<pathname><source>* reboot** command.

For example:

```
user@switch> request system software add /var/tmp/jinstall-host-qfx-10-f-x86-64-20.4R1.n-secure-
signed.tgz reboot
```

If the Install Package resides remotely from the switch, execute the **request system software add *<pathname><source>* reboot** command.

For example:

```
user@switch> request system software add ftp://ftpserver/directory/jinstall-host-qfx-10-f-
x86-64-20.4R1.n-secure-signed.tgz reboot
```

After the reboot has finished, verify that the new version of software has been properly installed by executing the `show version` command.

```
user@switch> show version
```

Upgrading Software from Junos OS Release 15.1X53-D3X to Junos OS Release 15.1X53-D60, 15.1X53-D61.7, 15.1X53-D62, and 15.1X53-D63 on QFX10008 and QFX10016 Switches

NOTE: Before you install the software, back up any critical files in **/var/home**. For more information regarding how to back up critical files, contact Customer Support at https://www.juniper.net/support.

The switch contains two Routing Engines, so you will need to install the software on each Routing Engine (re0 and re1).

If the installation package resides locally on the switch, execute the **request system software add** ***<pathname><source>*** command.

To install the software on re0:

```
user@switch> request system software add /var/tmp/jinstall-host-qfx-10-m-15.1X53-D60.n-secure-
domestic-signed.tgz re0
```

If the Install Package resides remotely from the switch, execute the **request system software add** ***<pathname><source>*** **re0** command.

For example:

```
user@switch> request system software add ftp://ftpserver/directory/jinstall-host-qfx-10-
m-15.1X53-D60.n-secure-domestic-signed.tgz re0
```

To install the software on re1:

```
user@switch> request system software add /var/tmp/jinstall-host-qfx-10-m-15.1X53-D60.n-secure-
domestic-signed.tgz re1
```

If the Install Package resides remotely from the switch, execute the **request system software add** ***<pathname><source>*** **re1** command.

For example:

```
user@switch> request system software add ftp://ftpserver/directory/jinstall-host-qfx-10-
m-15.1X53-D60.n-secure-domestic-signed.tgz re1
```

Reboot both Routing Engines.

For example:

```
user@switch> request system reboot both-routing-engines
```

After the reboot has finished, verify that the new version of software has been properly installed by executing the `show version` command.

```
user@switch> show version
```

Installing the Software on QFX10008 and QFX10016 Switches

Because the switch has two Routing Engines, perform a Junos OS installation on each Routing Engine separately to avoid disrupting network operation.

NOTE: Before you install the software, back up any critical files in **/var/home**. For more information regarding how to back up critical files, contact Customer Support at https://www.juniper.net/support.

WARNING: If graceful Routing Engine switchover (GRES), nonstop bridging (NSB), or nonstop active routing (NSR) is enabled when you initiate a software installation, the software does not install properly. Make sure you issue the CLI `delete chassis redundancy` command when prompted. If GRES is enabled, it will be removed with the `redundancy` command. By default, NSR is disabled. If NSR is enabled, remove the nonstop-routing statement from the `[edit routing-options]` hierarchy level to disable it.

1. Log in to the master Routing Engine's console.

   For more information about logging in to the Routing Engine through the console port, see the specific hardware guide for your switch.

2. From the command line, enter configuration mode:

   ```
   user@switch> configure
   ```

3. Disable Routing Engine redundancy:

   ```
   user@switch# delete chassis redundancy
   ```

4. Disable nonstop-bridging:

   ```
   user@switch# delete protocols layer2-control nonstop-bridging
   ```

5. Save the configuration change on both Routing Engines:

   ```
   user@switch# commit synchronize
   ```

6. Exit the CLI configuration mode:

   ```
   user@switch# exit
   ```

   After the switch has been prepared, you first install the new Junos OS release on the backup Routing Engine, while keeping the currently running software version on the master Routing Engine. This enables the master Routing Engine to continue operations, minimizing disruption to your network.

   After making sure that the new software version is running correctly on the backup Routing Engine, you are ready to switch routing control to the backup Routing Engine, and then upgrade or downgrade the software version on the other Routing Engine.

7. Log in to the console port on the other Routing Engine (currently the backup).

   For more information about logging in to the Routing Engine through the console port, see the specific hardware guide for your switch.

8. Install the new software package using the `request system software add` command:

   ```
   user@switch> request system software add validate /var/tmp/jinstall-host-qfx-10-f-
   x86-64-23.4R2.n-secure-signed.tgz
   ```

   For more information about the `request system software add` command, see the CLI Explorer.

9. Reboot the switch to start the new software using the `request system reboot` command:

   ```
   user@switch> request system reboot
   ```

   > **NOTE**: You must reboot the switch to load the new installation of Junos OS on the switch.
   >
   > To abort the installation, do not reboot your switch. Instead, finish the installation and then issue the `request system software delete` *<package-name>* command. This is your last chance to stop the installation.

   All the software is loaded when you reboot the switch. Installation can take between 5 and 10 minutes. The switch then reboots from the boot device on which the software was just installed. When the reboot is complete, the switch displays the login prompt.

   While the software is being upgraded, the Routing Engine on which you are performing the installation is not sending traffic.

10. Log in and issue the `show version` command to verify the version of the software installed.

    ```
    user@switch> show version
    ```

    Once the software is installed on the backup Routing Engine, you are ready to switch routing control to the backup Routing Engine, and then upgrade or downgrade the master Routing Engine software.

11. Log in to the master Routing Engine console port.

    For more information about logging in to the Routing Engine through the console port, see the specific hardware guide for your switch.

12. Transfer routing control to the backup Routing Engine:

    ```
    user@switch> request chassis routing-engine master switch
    ```

    For more information about the `request chassis routing-engine master` command, see the CLI Explorer.

13. Verify that the backup Routing Engine (slot 1) is the master Routing Engine:

    ```
    user@switch> show chassis routing-engine
    Routing Engine status:
      Slot 0:
        Current state                  Backup
        Election priority              Master (default)

    Routing Engine status:
      Slot 1:
        Current state                  Master
        Election priority              Backup (default)
    ```

14. Install the new software package using the `request system software add` command:

    ```
    user@switch> request system software add validate /var/tmp/jinstall-host-qfx-10-f-
    x86-64-23.4R2.n-secure-signed.tgz
    ```

    For more information about the `request system software add` command, see the CLI Explorer.

15. Reboot the Routing Engine using the `request system reboot` command:

    ```
    user@switch> request system reboot
    ```

    NOTE: You must reboot to load the new installation of Junos OS on the switch.

    To abort the installation, do not reboot your system. Instead, finish the installation and then issue the `request system software delete jinstall` *<package-name>* command. This is your last chance to stop the installation.

    The software is loaded when you reboot the system. Installation can take between 5 and 10 minutes. The switch then reboots from the boot device on which the software was just installed. When the reboot is complete, the switch displays the login prompt.

While the software is being upgraded, the Routing Engine on which you are performing the installation does not send traffic.

16. Log in and issue the `show version` command to verify the version of the software installed.

17. Transfer routing control back to the master Routing Engine:

    ```
    user@switch> request chassis routing-engine master switch
    ```

    For more information about the `request chassis routing-engine master` command, see the CLI Explorer.

18. Verify that the master Routing Engine (slot 0) is indeed the master Routing Engine:

    ```
    user@switch> show chassis routing-engine
    Routing Engine status:
      Slot 0:
        Current state                  Master
        Election priority              Master (default)

    outing Engine status:
      Slot 1:
        Current state                  Backup
        Election priority              Backup (default)
    ```

Performing a Unified ISSU

You can use unified ISSU to upgrade the software running on the switch with minimal traffic disruption during the upgrade.

NOTE: Unified ISSU is supported in Junos OS Release 13.2X51-D15 and later.

Perform the following tasks:

- No Link Title
- No Link Title

Preparing the Switch for Software Installation

Before you begin software installation using unified ISSU:

- Ensure that nonstop active routing (NSR), nonstop bridging (NSB), and graceful Routing Engine switchover (GRES) are enabled. NSB and GRES enable NSB-supported Layer 2 protocols to synchronize protocol information between the master and backup Routing Engines.

  To verify that nonstop active routing is enabled:

  > **NOTE**: If nonstop active routing is enabled, then graceful Routing Engine switchover is enabled.

  ```
  user@switch> show task replication
          Stateful Replication: Enabled
          RE mode: Master
  ```

  If nonstop active routing is not enabled (`Stateful Replication` is `Disabled`), see Configuring Nonstop Active Routing on Switches for information about how to enable it.

- Enable nonstop bridging (NSB). See Configuring Nonstop Bridging on EX Series Switches for information on how to enable it.

- (Optional) Back up the system software—Junos OS, the active configuration, and log files—on the switch to an external storage device with the `request system snapshot` command.

Upgrading the Software Using Unified ISSU

This procedure describes how to upgrade the software running on a standalone switch.

To upgrade the switch using unified ISSU:

1. Download the software package by following the procedure in the Downloading Software Files with a Browser section in Installing Software Packages on QFX Series Devices.

2. Copy the software package or packages to the switch. We recommend that you copy the file to the `/var/tmp` directory.

3. Log in to the console connection. Using a console connection allows you to monitor the progress of the upgrade.

4. Start the ISSU:

   - On the switch, enter:

     ```
     user@switch> request system software in-service-upgrade /var/tmp/package-name.tgz
     ```

     where *package-name*.tgz is, for example, jinstall-host-qfx-10-f-x86-64-20.4R1.n-secure-signed.tgz.

   NOTE: During the upgrade, you cannot access the Junos OS CLI.

   The switch displays status messages similar to the following messages as the upgrade executes:

```
warning: Do NOT use /user during ISSU. Changes to /user during ISSU may get lost!
ISSU: Validating Image
ISSU: Preparing Backup RE
Prepare for ISSU
ISSU: Backup RE Prepare Done
Extracting jinstall-host-qfx-5-f-x86-64-18.3R1.n-secure-signed.tgz ...
Install jinstall-host-qfx-5-f-x86-64-19.2R1.n-secure-signed.tgz completed
Spawning the backup RE
Spawn backup RE, index 0 successful
GRES in progress
GRES done in 0 seconds
Waiting for backup RE switchover ready
GRES operational
Copying home directories
Copying home directories successful
Initiating Chassis In-Service-Upgrade
Chassis ISSU Started
ISSU: Preparing Daemons
ISSU: Daemons Ready for ISSU
ISSU: Starting Upgrade for FRUs
ISSU: FPC Warm Booting
ISSU: FPC Warm Booted
ISSU: Preparing for Switchover
ISSU: Ready for Switchover
Checking In-Service-Upgrade status
  Item           Status                  Reason
  FPC 0          Online (ISSU)
Send ISSU done to chassisd on backup RE
```

```
Chassis ISSU Completed
ISSU: IDLE
Initiate em0 device handoff
```

NOTE: A unified ISSU might stop, instead of abort, if the FPC is at the warm boot stage. Also, any links that go down and up will not be detected during a warm boot of the Packet Forwarding Engine (PFE).

NOTE: If the unified ISSU process stops, you can look at the log files to diagnose the problem. The log files are located at `/var/log/vjunos-log.tgz`.

5. Log in after the reboot of the switch completes. To verify that the software has been upgraded, enter the following command:

```
user@switch> show version
```

6. Ensure that the resilient dual-root partitions feature operates correctly, by copying the new Junos OS image into the alternate root partitions of all of the switches:

```
user@switch> request system snapshot slice alternate
```

   Resilient dual-root partitions allow the switch to boot transparently from the alternate root partition if the system fails to boot from the primary root partition.

Upgrade and Downgrade Support Policy for Junos OS Releases

We have two types of releases, standard EOL and EEOL:

- Standard End of Life (EOL) releases have engineering support for twenty four months after the first general availability date and customer support for an additional six more months.
- Extended End of Life (EEOL) releases have engineering support for sixty months after the first general availability date and customer support for an additional six more months.

NOTE: The sixty months of support for EEOL releases is introduced in Junos OS 23.2 release and is available for all later releases. For releases prior to 23.2, the support for EEOL releases continues to be thirty six months.

For both standard EOL and EEOL releases, you can upgrade to the next three subsequent releases or downgrade to the previous three releases.

For EEOL releases only, you have an additional option - you can upgrade directly from one EEOL release to the next two subsequent EEOL releases, even if the target release is beyond the next three releases. Likewise, you can downgrade directly from one EEOL release to the previous two EEOL releases, even if the target release is beyond the previous three releases.

Table 6: EOL and EEOL Releases

Release Type	End of Engineering (EOE)	End of Support (EOS)	Upgrade/ Downgrade to subsequent 3 releases	Upgrade/ Downgrade to subsequent 2 EEOL releases
Standard End of Life (EOL)	24 months	End of Engineering + 6 months	Yes	No
Extended End of Life (EEOL)	60 months	End of Engineering + 6 months	Yes	Yes

For more information about standard EOL and EEOL releases, see https://www.juniper.net/support/eol/junos.html.

For information about software installation and upgrade, see the Installation and Upgrade Guide.

Junos OS Release Notes for SRX Series Firewalls

IN THIS SECTION

What's New

IN THIS SECTION

Learn about new features introduced in this release for the SRX Series Firewall devices.

To view features supported on the SRX Series Firewall, view the Feature Explorer using the following links. To see which features were added in Junos OS Release 23.4R2, click the Group by Release link. You can collapse and expand the list as needed.

- SRX300
- SRX320
- SRX340
- SRX345
- SRX380
- SRX1500

- SRX1600
- SRX2300
- SRX4100
- SRX4200
- SRX4600
- SRX5400
- SRX5600
- SRX5800

Class of Service

- **Routing-instance based classification (SRX300, SRX320, SRX340, SRX345, SRX380)**—Starting in Junos OS Release 23.4R2, SRX300, SRX320, SRX340, SRX345, SRX380 Firewalls support routing-instance based classification. You use routing instance-based classifiers to classify packets based on the virtual routing and forwarding (VRF) of incoming packets. For routing instances with VRF table labels enabled, you can apply a custom MPLS EXP, DSCP, or IEEE802.1 classifier to the routing instance.

  [See classifiers (Routing Instance).]

Content Security

- **Support for intelligent web filtering profile selection (SRX300, SRX320, SRX340, SRX345, and SRX380)**—Starting in Junos OS Release 23.4R2, dynamic app information from Juniper Networks Deep Packet Inspection (JDPI) is used to retrieve policy information before the final policy match occurs.

  The Content Security profile that is retrieved based on the dynamic app information is more accurate than applying the default profile, which was the earlier approach.

  [See Web Filtering.]

- **Support for cache preload for Enhanced Web Filtering (EWF) (SRX300, SRX320, SRX340, SRX345, and SRX380)**—Starting in Junos OS Release 23.4R2, we support preloading of cache with the top-rated, frequently visited URL list along with the classification information at the system startup stage. This feature is useful if your Internet connection is slow and you experience high latency while accessing the Web due to the remote categorization service.
  Because the Web-filter policy decision is based on the URL category information that is preloaded in the cache, you do not experience a lag even when you make the first request.

  [See Enhanced Web Filtering.]

Juniper Advanced Threat Prevention Cloud (ATP Cloud)

- **Support to delete a single country code from GeoIP-based dynamic addresses (SRX300, SRX320, SRX340, SRX345, and SRX380)**—Starting in Junos OS Release 23.4R2, you can delete a single country code from an IP-based geolocation (GeoIP)-Dynamic Address Entry (DAE) configuration.

  We've also updated the `show security dynamic-address` command to display the country code appended to the IP-based geolocation name.

  [See Configure the SRX Series and Geolocation IP for Integration with ATP Appliance and show security dynamic-address.]

J-Web

- **Support for allowed groups in LDAP (SRX300, SRX320, SRX340, SRX345, and SRX380)**— Starting in Junos OS Release 23.4R2, you can use **Allowed Groups** under the **LDAP** option in this navigation path: **Security Services** > **Firewall Authentication** > **Access Profile** > **Create Access Profile** to configure groups that are allowed to sign in.

  [See Add an Access Profile.]

- **Support for LDAP (SRX300, SRX320, SRX340, SRX345, and SRX380)**— Starting in Junos OS Release 23.4R2, you can use the **LDAP** option in this navigation path: **Network** > **VPN** > **IPsec VPN** > **Create VPN** > **Remote Access** > **Juniper Secure Connect** > **Local Gateway** to configure user authentication for an access profile.

  [See Create a Remote Access VPN—Juniper Secure Connect and Add an Access Profile.]

- **Support for system logs (SRX300, SRX320, SRX340, SRX345, and SRX380)**— Starting in Junos OS Release 23.4R2, you can use **System** > **Monitor** to monitor information about system events such as routine operations, failure and error conditions, and emergency or critical conditions.

  [See Monitor System.]

- **Support for compliance rules (SRX300, SRX320, SRX340, SRX345, and SRX380)**— Starting in Junos OS Release 23.4R2 you can use:

  - **Network** > **Compliance** menu to create remote access pre-logon compliance policies in the SRX Series Firewall. You can associate only one compliance policy for a remote access connection profile. The Juniper Secure Connect application sends details to the SRX Series Firewall. The device performs pre-logon compliance checks and accepts or rejects a connection based on the pre-logon compliance rule match.

  - **Compliance** option under **Network** > **VPN** > **IPsec VPN** > **Create VPN** > **Remote Access** > **Juniper Secure Connect** > **Remote User** to associate only one compliance rule for a remote access connection profile.

[See About the Compliance Page and Create a Remote Access VPN—Juniper Secure Connect.]

- **Support for application bypass (SRX300, SRX320, SRX340, SRX345, and SRX380)**— Starting in Junos OS Release 23.4R2, you can use **Application Bypass** under **Network** > **VPN** > **IPsec VPN** > **Create VPN** > **Remote Access** > **Juniper Secure Connect** > **Remote User** to define Juniper Secure Connect remote client configuration parameters to bypass certain applications. Bypassing is based on domain names and protocols without passing through the remote access VPN tunnel. The administrator configures these parameters on the SRX Series Firewall which are pushed to client application after successful authentication.

  [See Create a Remote Access VPN—Juniper Secure Connect.]

Network Management and Monitoring

- **Support for protobuf format (SRX300, SRX320, SRX340, SRX345, and SRX380)**—Starting in Junos OS Release 23.4R2, SRX Series Firewalls support the Google protocol buffers (GBP or *protobuf*) format to encode the security logs. The device sends the encoded security log to the target. The target decodes the logs for readability.

  [See protobuf.]

Services Applications

- **Enhancement to IP-IP tunnel configuration (SRX300, SRX320, SRX340, SRX345, SRX380)**—Starting in Junos OS Release 23.4R2, when you configure an IP tunnel (ip-*x*/*y*/*z*) on the listed firewall devices at the `[edit interfaces` *`interface-name`* `unit` *`unit-number`* `tunnel]` hierarchy level, you can also configure:

  - Interface for tunnel source
  - Hostname for tunnel source
  - Hostname for tunnel destination
  - Tunnel encapsulation type

  [See tunnel.]

Additional Features

We've extended support for the following features to these platforms.

- **JIMS support Junos PKI infrastructure and FQDN as primary and secondary address** (SRX300, SRX320, SRX340, SRX345, and SRX380).

  [See identity-management.]

- **Support for dynamic update of trusted CA bundle** (SRX300, SRX320, SRX340, SRX345, and SRX380)

[See Dynamic Update of Trusted CA Certificates.]

What's Changed

IN THIS SECTION

Learn about what changed in this release for SRX Series Firewalls.

VPNs

- **Enhancements to address error in generating RSA key pair with bigger key size (SRX Series)**–In earlier Junos OS releases, when you generate RSA key pair of size 4096 or greater, the command `request security pki generate-key-pair certificate-id name type rsa size 4096`, displays the error message `error: timeout communicating with pki-service daemon` sometimes when PKID takes more time to respond. Starting in Junos OS release 23.4R1, the command runs successfully without this error message.
- **Enhancements to the output of show security ipsec security-associations detail command (SRX Series and vSRX 3.0)**–We've enhanced the output of `show security ipsec security-associations detail` when you enable `vpn-monitor` at the `[edit security ipsec vpn vpn-name]` hierarchy level, when your firewall runs IPsec VPN services with the new iked process. The output displays `threshold` and `interval` values in the command output. Starting in Junos OS Release 23.4R1, you'll notice these changes.

  [See show security ipsec security-associations.]
- **Enhancements to address certificate validation failures after RG0 failover (SRX Series)**–Following RG0 failover in the chassis cluster, you may notice that the output of the command `show services advanced-anti-malware status` displays `Requesting server certificate validation` status due to CRL download failure on the secondary node before the failover. We've made enhancements to address the issue and you?ll see the following changes:
  - If there's a repeated failure to download the CRL even after multiple retry attempts, you will notice the error message `PKID_CRL_DOWNLOAD_RETRY_FAILED: CRL download for the CA failed even after multiple retry attempts, Check CRL server connection` until the CRL downloads successfully.

- When the cluster performs a failover from the secondary to the primary node, the PKI triggers a fresh CRL download on the new primary node, resulting in successful certificate verification.

Known Limitations

Learn about known limitations in this release for SRX Series Firewalls.

For the most complete and latest information about known Junos OS defects, use the Juniper Networks online Junos Problem Report Search application.

General Routing

- The SRX300 and SRX320 uses revenue port ge-0/0/0 as management port with 150 MB bidirectional traffic of 64 byte packet size, the flowd process is occupying all the CPU1. It can't process any further traffic. Since SRX300 and SRX320 have limited CPU, the flowd process capability to process traffic is limited. PR1705627

Infrastructure

- When upgrading from before Junos OS Release 21.2 to 21.2 and after, validation and upgrade will fail. The upgrading requires using of `no-validate` configuration. PR1568757

J-Web

- Staring in Junos OS Release 23.4R1, you must remove IKED specific configurations before uninstalling the Junos-IKE package in J-Web. If not, the Junos-IKE package gets uninstalled with configuration mismatch errors and J-Web will move to the Setup wizard mode.PR1744210

VPNs

- When multiple VPNs have same TS and different st0, in on-traffic tunnel establishment, ARI routes for the same destination and different st0 gets overwritten and only the latest route will be added. As a result, traffic over only one VPN continues and other VPN is down. In case of DPD failover, when one of the VPN is down and peer initiates DPD failover to route traffic through other VPN, due to missing ARI route on responder-side, traffic will be down. As a work-around, for DPD failover to work seamlessly, configure 2 st0s in different VRFs so both routes can be installed and failover can continue to work. PR1727795

Open Issues

Learn about open issues in this release for SRX Series Firewalls.

For the most complete and latest information about known Junos OS defects, use the Juniper Networks online Junos Problem Report Search application.

Chassis Clustering

- On SRX5000 line of devices with MNHA mode, if monitor ip is configured under routing-instance and when you try to add annotate IP command both devices might move into INELIGIBLE state and complete traffic might drop during the issue. PR1632586

- On SRX5000 line of devices HA cluster in FIPS mode, repeated manual failovers of redundancy groups can result in SPC3 or IOC4 or both the cards going offline.PR1797468

Content Security

- The command request security utm web-filtering category download version version number is deprecated from Junos OS release 24.1 onwards. Instead a new command is introduced request security utm web-filtering category download rollback to download the previous category version package. PR1773869

Flow-Based and Packet-Based Processing

- On SRX5000 line of devices and SRX4600, performing ISSU to Junos OS release 21.4 and higher from earlier Junos versions can lead to a flowd process to generates core files. PR1779260

General Routing

- When non-root user tries to generate archive file for /var/log, it either fails or generates an archive with partial log files. This happens due to permission of files under /var/log/hostlogs/.PR1692516

- When input traffic is more and output traffic is expected equal to maximum capacity of egress interface, please set the shaping explicitly equal to interface maximum capacity if default shaping does not work. PR1712964

- The NSD process might generate core files. PR1716686

- Configuring the set system processes watchdog disable/timeout command causes a commit pause, and traffic loss will be observed. Watchdog related commands are unsupported.PR1747849

- On SRX380 or SRX550 devices, when different Native-VLANs are configured on the trunk interfaces between devices, there is a packet drop. PR1750521

- The repd process might generate core files during ISSU. There is no functional impact. PR1797189

Platform and Infrastructure

- Request message user throws permission message to root user.PR1731520

VPNs

- When multiple VPNs have same TS and different st0, in on-traffic tunnel establishment, ARI routes for the same destination and different st0 gets overwritten and only the latest route will be added. As a result, traffic over only one VPN continues and other VPN is down. In case of DPD failover, when one of the VPN is down and peer initiates DPD failover to route traffic through other VPN, due to missing ARI route on responder-side, traffic will be down. As a workaround, for DPD failover to work seamlessly, configure 2 st0s in different VRFs so both routes can be installed and failover can continue to work.PR1727795

Resolved Issues

Learn about the issues fixed in this release for SRX Series Firewalls.

For the most complete and latest information about known Junos OS defects, use the Juniper Networks online Junos Problem Report Search application.

Authentication and Access Control

- Clearpass auth entry is getting deleted post successful ISSU. PR1732210

Chassis Clustering

- Both primary and secondary nodes in chassis cluster go into disabled state in HA link down scenario. PR1540654

- Core files are generated on both the nodes of HA cluster setup when it is upgraded to Junos OS release 21.2 and above. PR1736985

Content Security

- Certain video streaming services continuously buffer when safe-search and HTTP persistent mode is enabled. PR1755998

- The wf_key_ng_juniper support for NG. PR1768183

- The flowd process generates core files by Web filtering. PR1772232

Flow-Based and Packet-Based Processing

- Traffic loss is observed for the existing session if there is an update for the next-hop MAC address PR1755181
- CPU utilization calculation is inaccurate. PR1756972
- In a chassis cluster setup the flowd pause and SPC cards will fail. PR1761542
- The GTPv2 create session response and packets might get dropped. PR1771176
- The NSD process goes high on primary device when the Tenant System is configured. PR1776480
- TCP sessions might get reset during MNHA traffic failover. PR1782444
- The srxpfe process pause when ATP Cloud turned on. PR1783101
- PMI sends packets to the wrong destination. PR1783595
- Packets over GRE or IPIP or GRE(PMI) might not reach destination. PR1791633
- The GTP-U packet destination port gets duplicated to the source port and subsequently discarded by policy. PR1798041
- The commit might not go through when more than 128 vrf-groups for Layer 3 VPN configuration are configured. PR1802089
- VXLAN session not created after committing FTI configuration on both devices. PR1807339

General Routing

- Update microcode to version 0x3a or later upon upgrade to Junos OS release 21.4. PR1608045
- High latency will be observed while pinging to peer device. PR1714620
- Transition Junos OS kernel random number generator from hashing algorithm SHA-256 to SHA-512. PR1723499
- Traffic drops might be observed when a BGP session comes up after the network flap. PR1732876
- SRX4100 and SRX4200 accepts the datapath-debug configuration although it does not support it. PR1739559
- ISSU upgrade pause on Junos OS release 23.2 onwards. PR1739673
- On SRX1500, PEM alarms are displayed due to hardware limitations to read I2C. PR1751496

- ARP resolution failure for lt interfaces is observed after cluster failover. PR1753191
- VM host memory exhaustion results in image installation failure and brings down the Routing Engine (RE) during the upgrade. PR1755585
- DNS proxy feature not working on logical tunnel interfaces. PR1760684
- Application package version shows as 0 after upgrade to FreeBSD12. PR1766132
- After the device reboot JSC stops accepting user connections. PR1766594
- Inter and intra VLAN traffic drops. PR1770303
- DHCP server not responding to some clients. PR1770332
- RE switchover observed in SRX5000 line of devices when Ethernet switchports failure scenario on SCB. PR1774760
- Features utilizing inactive routes might not work properly after the device reboot. PR1774975
- Traffic drop observed right after boot up on SRX4600. PR1775083
- IPsec tunnel behind NAT stops passing traffic when the NAT port number or IP address changes. PR1776216
- The Wifi Mini-PIM card will be down upon upgrading the device. PR1776400
- Interfaces stay down when 1 G SFP fiber transceiver connected to SRX380. PR1776656
- Unexpected failover will be seen when there is communication loss between CP and SPU with web-authentication or web-redirect is configured. PR1780282
- IP monitoring fail to install route after HA cluster reboot. PR1780326
- Junos OS and Junos OS Evolved: Impact of Terrapin SSH Attack (CVE-2023-48795). PR1781732
- Chassis alarm not present for if /var partition usage exceeds 100 percent. PR1784983
- Validate result is in processing state for more than 5 minutes, when the configured validator port is in incorrect. PR1786432
- The flowd process pause when the TLS 1.3 session ticket is received on SSL-I. PR1788673
- The srxpfe or flowd process might pause while trying to update the path probe statistics. PR1790782
- The ISSU fails in Layer 2 HA cluster deployment. PR1803376
- The sxrpfe and fwauthd processes pauses sometimes. PR1804149

- IPsec VPN is getting flapped due to warning messages on MIST controlled devices. PR1805493

Interfaces and Chassis

- IP-IP tunnel with hostname does not work on SRX300 line of devices. PR1755011
- The interfaces of secondary node might shows Link-mode: Unknown. PR1773597

Intrusion Detection and Prevention (IDP)

- The flowd process pause when the device is rebooted. PR1786822

J-Web

- J-Web UI cannot be launched. PR1766378
- On the J-Web, edit icon under the interface is not working. PR1772267
- Dynamic applications, Certificate Management, and NAT destination Page display errors. PR1784905
- J-Web default session limits have been aligned with CLI default values. PR1788364
- J-Web does not display address book entries properly after certain operations. PR1789466

Platform and Infrastructure

- E2E packet capture will be corrupted. PR1761928
- A flowd process pause if CP receives the packets due to some hardware memory issue. PR1775880
- Traffic loss due to PPM not offloading LACP. PR1779749
- The chassis cluster failover is seen post ISSU. PR1784775
- Insufficient power alarm observed in SRX5000 line of devices. PR1787219
- FPC reboot seen on SRX Series Firewalls with SPC3 card post RG failover. PR1793262
- The dfwd process generates core files on node1 when performing ISSU upgrade to Junos OS release 23.1 and more. PR1794303
- DNS and NTP might not be working as expected on Junos OS release 23.3 version above. PR1795068

Routing Policy and Firewall Filters

- The srxpfe process pause when the policies referring to a dynamic-address is changed. PR1769889
- Security policies might go out of sync during ISSU. PR1783249

Routing Protocols

- OSPF route flap might be observed. PR1774715

User Interface and Configuration

- SSH configuration changes do not come into affect on an existing outbound SSH client connection. PR1791814

VLAN Infrastructure

- SRX Series Firewalls with transparent mode might fail to create a new flow session for multicast traffic when VLAN has l3-interface. PR1780182
- Packet and byte counters in flow session result or traffic log are not correct for traffic uses Content Security or ALG services when SRX Series Firewalls are working as Layer 2 mode. PR1787772

VPNs

- IPsec rekey fails when kilobyte based lifetime expires. PR1527384
- ADVPN connection limit shortcut limitation not working as expected. PR1759738
- In chassis cluster setup after failover AAMW status will remain in the requesting server certificate validation state on the new primary node. PR1765321
- IPsec tunnels might not be established due to memory leak. PR1773276
- In the MNHA scenario traffic drops are observed after failover. PR1777531
- SCTP does not work correctly. PR1778106
- The ikemd process pause when IKE traceoptions is configured. PR1780468
- The kmd or iked process pause under rare circumstances. PR1783738
- Traffic loss after deleting the traffic selector from the VPN configuration. PR1785346
- Tunnel IKE and IPsec fails to come with Layer 2 HA and FIPS after switchover. PR1793207

Migration, Upgrade, and Downgrade Instructions

IN THIS SECTION

This section contains the upgrade and downgrade support policy for Junos OS for SRX Series Firewalls. Upgrading or downgrading Junos OS might take several minutes, depending on the size and configuration of the network.

For information about software installation and upgrade, see the Installation and Upgrade Guide.

For information about ISSU, see the Chassis Cluster User Guide for Security Devices.

Upgrade and Downgrade Support Policy for Junos OS Releases and Extended End-Of-Life Releases

We have two types of releases, standard EOL and EEOL:

- Standard End of Life (EOL) releases have engineering support for twenty four months after the first general availability date and customer support for an additional six more months.
- Extended End of Life (EEOL) releases have engineering support for sixty months after the first general availability date and customer support for an additional six more months.

> **NOTE**: The sixty months of support for EEOL releases is introduced in Junos OS 23.2 release and is available for all later releases. For releases prior to 23.2, the support for EEOL releases continues to be thirty six months.

For both standard EOL and EEOL releases, you can upgrade to the next three subsequent releases or downgrade to the previous three releases.

For EEOL releases only, you have an additional option - you can upgrade directly from one EEOL release to the next two subsequent EEOL releases, even if the target release is beyond the next three releases. Likewise, you can downgrade directly from one EEOL release to the previous two EEOL releases, even if the target release is beyond the previous three releases.

Table 7: EOL and EEOL Releases

Release Type	End of Engineering (EOE)	End of Support (EOS)	Upgrade/ Downgrade to subsequent 3 releases	Upgrade/ Downgrade to subsequent 2 EEOL releases
Standard End of Life (EOL)	24 months	End of Engineering + 6 months	Yes	No
Extended End of Life (EEOL)	60 months	End of Engineering + 6 months	Yes	Yes

For more information about standard EOL and EEOL releases, see https://www.juniper.net/support/eol/junos.html.

For information about software installation and upgrade, see the Installation and Upgrade Guide.

Documentation Updates

IN THIS SECTION

This section lists the errata and changes in Junos OS Release 23.4R2 for the SRX Series Firewalls documentation.

Guide Name Change

The *Authentication and Integrated User Firewalls User Guide* has been renamed *Identity Aware Firewall User Guide* in Junos OS Release 23.4R2. For more information, see Identity Aware Firewall Guide.

The following enhancements and additions apply to the Guide:

- Overview of Identity Aware Firewall
- Active Directory as Identity Source

Junos OS Release Notes for vRR

IN THIS SECTION

NOTE: Junos OS Release 23.4R1 is the last-supported release for the following SKUs:

Product Line	SKUs	Junos OS Release
vRR	S-VRR-V-L	Junos OS Release 23.4R1
vRR	S-VRR-V-L-1Y	Junos OS Release 23.4R1
vRR	S-VRR-V-L-3Y	Junos OS Release 23.4R1
vRR	S-VRR-V-M	Junos OS Release 23.4R1
vRR	S-VRR-V-M-1Y	Junos OS Release 23.4R1
vRR	S-VRR-V-M-3Y	Junos OS Release 23.4R1

(Continued)

Product Line	SKUs	Junos OS Release
vRR	S-VRR-V-S	Junos OS Release 23.4R1
vRR	S-VRR-V-S-1Y	Junos OS Release 23.4R1
vRR	S-VRR-V-S-3Y	Junos OS Release 23.4R1

What's New

There are no new features or enhancements to existing features in this release for vRR.

What's Changed

There are no changes in behavior and syntax in this release for vRR.

Known Limitations

There are no known limitations in hardware or software in this release for vRR.

For the most complete and latest information about known Junos OS defects, use the Juniper Networks online Junos Problem Report Search application.

To learn more about common BGP or routing known limitations in Junos OS 23.4R2, see "Known Limitations" on page 32 for MX Series routers.

Open Issues

There are no known issues in hardware or software in this release for vRR.

For the most complete and latest information about known Junos OS defects, use the Juniper Networks online Junos Problem Report Search application.

Resolved Issues

There are no resolved issues in this release for vRR.

For the most complete and latest information about known Junos OS defects, use the Juniper Networks online Junos Problem Report Search application.

Junos OS Release Notes for vSRX Virtual Firewall

IN THIS SECTION

What's New

There are no new features or enhancements to existing features in this release for vSRX.

What's Changed

IN THIS SECTION

Learn about what changed in this release for vSRX Virtual Firewall.

VPNs

- **Enhancements to the output of show security ipsec security-associations detail command (SRX Series and vSRX 3.0)**–We've enhanced the output of `show security ipsec security-associations detail` when you enable `vpn-monitor` at the `[edit security ipsec vpn *vpn-name*]` hierarchy level, when your firewall runs IPsec VPN services with the new iked process. The output displays `threshold` and `interval` values in the command output. Starting in Junos OS Release 23.4R1, you'll notice these changes.

  [See show security ipsec security-associations.]

Known Limitations

Learn about known limitations in this release for vSRX Virtual Firewall.

For the most complete and latest information about known Junos OS defects, use the Juniper Networks online Junos Problem Report Search application.

Network Address Translation (NAT)

- During session creation,if persistent NAT is configured, under a timing scenario and specific traffic profile arriving at the same time tries to create persistent NAT bindings. One of them will proceed with persistent NAT bindings and session creation whereas the other will be marked as duplicate persistent NAT bindings and release the session. Session will be created for the second traffic flow on retransmission.PR1762417

Platform and Infrastructure

- The instance type c5n.18xlarge has two sockets/NUMAs, while vSRX only supports one NUMA.PR1738330

Open Issues

Learn about open issues in this release for vSRX Virtual Firewall.

For the most complete and latest information about known Junos OS defects, use the Juniper Networks online Junos Problem Report Search application.

Content Security

- cSRX does not have CLI command to reboot the system. You need to restart srxpfe service from Linux shell using service srxpfe restart command. PR1762827
- The command request security utm web-filtering category download version version number is deprecated from Junos OS release 24.1 onwards. Instead a new command is introduced request security utm web-filtering category download rollback to download the previous category version package. PR1773869

Resolved Issues

Learn about the issues fixed in this release for vSRX Virtual Firewall.

Flow-Based and Packet-Based Processing

- The CPU utilization calculation is inaccurate on vSRX. PR1756972
- In a chassis cluster setup the flowd process pause and SPC cards might fail. PR1761542
- Unable to download a file completely from SaaS server to LAN. PR1762568
- Packet drops might be seen in GRE scenario. PR1777565
- The ipfd process generates core files when you enable ATP from IDP policy. PR1781509

J-Web

- J-Web UI cannot be launched. PR1766378

VPNs

- IPsec tunnel behind NAT stops passing traffic when the NAT port number or IP address changes. PR1776216
- Encapsulation and decapsulation might not work correctly when PMI is enabled and while using life-sizes. PR1758785
- The kmd or iked process pause under rare circumstances. PR1783738
- Traffic loss after deleting the traffic selector from the VPN configuration. PR1785346
- The Ike idle-time tears down VPN even when there is active traffic through the tunnel. PR1802145

Migration, Upgrade, and Downgrade Instructions

IN THIS SECTION

This section contains information about how to upgrade Junos OS for vSRX Virtual Firewall using the CLI. Upgrading or downgrading Junos OS can take several hours, depending on the size and configuration of the network.

You also can upgrade to Junos OS Release 23.4R2 for vSRX Virtual Firewall using J-Web (see J-Web) or the Junos Space Network Management Platform (see Junos Space).

Direct upgrade of vSRX Virtual Firewall from Junos OS 15.1X49 Releases to Junos OS Releases 17.4, 18.1, 18.2, 18.3,18.4, 19.1, 19.2 and 19.4 is supported.

The following limitations apply:

- Direct upgrade of vSRX Virtual Firewall from Junos OS 15.1X49 Releases to Junos OS Release 19.3 and higher is not supported. For upgrade between other combinations of Junos OS Releases in vSRX Virtual Firewall and vSRX Virtual Firewall 3.0, the general Junos OS upgrade policy applies.

- The file system mounted on /var usage must be below 14% of capacity.

  Check this using the following command:

  ```
  show system storage | match " /var$" /dev/vtbd1s1f
   2.7G        82M       2.4G        3%   /var
  ```

  Using the `request system storage cleanup` command might help reach that percentage.

- The Junos OS upgrade image must be placed in the directory /var/host-mnt/var/tmp/. Use the `request system software add /var/host-mnt/var/tmp/<upgrade_image>`

- We recommend that you deploy a new vSRX Virtual Firewall virtual machine (VM) instead of performing a Junos OS upgrade. That also gives you the option to move from vSRX Virtual Firewall to the newer and more recommended vSRX Virtual Firewall 3.0.

- Ensure to back up valuable items such as configurations, license-keys, certificates, and other files that you would like to keep.

> **NOTE**: For ESXi deployments, the firmware upgrade from Junos OS Release 15.1X49-Dxx to Junos OS releases 17.x, 18.x, or 19.x is not recommended if there are more than three network adapters on the 15.1X49-Dxx vSRX Virtual Firewall instance. If there are more than three network adapters and you want to upgrade, then we recommend that you either delete all the additional network adapters and add the network adapters after the upgrade or deploy a new vSRX Virtual Firewall instance on the targeted OS version.

Upgrading Software Packages

To upgrade the software using the CLI:

1. Download the **Junos OS Release 23.4R2 for vSRX .tgz** file from the Juniper Networks website. Note the size of the software image.

2. Verify that you have enough free disk space on the vSRX Virtual Firewall instance to upload the new software image.

   ```
   root@vsrx> show system storage
          Filesystem              Size       Used      Avail  Capacity   Mounted on
          /dev/vtbd0s1a           694M       433M       206M       68%  /
          devfs                   1.0K       1.0K         0B      100%  /dev
   ```

```
       /dev/md0                1.3G       1.3G         0B      100%  /junos
       /cf                     694M       433M       206M       68%  /junos/cf
       devfs                   1.0K       1.0K         0B      100%  /junos/dev/
       procfs                  4.0K       4.0K         0B      100%  /proc
       /dev/vtbd1s1e           302M        22K       278M        0%  /config
       /dev/vtbd1s1f           2.7G        69M       2.4G        3%  /var
       /dev/vtbd3s2             91M       782K        91M        1%  /var/host
       /dev/md1                302M       1.9M       276M        1%  /mfs
       /var/jail               2.7G        69M       2.4G        3%  /jail/var
       /var/jails/rest-api       2.7G        69M       2.4G      3%  /web-api/var
       /var/log                2.7G        69M       2.4G        3%  /jail/var/log
       devfs                   1.0K       1.0K         0B      100%  /jail/dev
       192.168.1.1:/var/tmp/corefiles       4.5G       125M       4.1G    3%  /var/crash/
corefiles
       192.168.1.1:/var/volatile      1.9G       4.0K       1.9G    0%  /var/log/host
       192.168.1.1:/var/log       4.5G       125M       4.1G     3%  /var/log/hostlogs
       192.168.1.1:/var/traffic-log       4.5G       125M       4.1G    3%  /var/traffic-log
       192.168.1.1:/var/local       4.5G       125M       4.1G    3%  /var/db/host
       192.168.1.1:/var/db/aamwd      4.5G       125M       4.1G    3%  /var/db/aamwd
       192.168.1.1:/var/db/secinteld       4.5G       125M       4.1G    3%  /var/db/secinteld
```

3. Optionally, free up more disk space, if needed, to upload the image.

```
root@vsrx> request system storage cleanup
       List of files to delete:
       Size Date       Name
       11B Sep 25 14:15 /var/jail/tmp/alarmd.ts
       259.7K Sep 25 14:11 /var/log/hostlogs/vjunos0.log.1.gz
       494B Sep 25 14:15 /var/log/interactive-commands.0.gz
       20.4K Sep 25 14:15 /var/log/messages.0.gz
       27B Sep 25 14:15 /var/log/wtmp.0.gz
       27B Sep 25 14:14 /var/log/wtmp.1.gz
       3027B Sep 25 14:13 /var/tmp/BSD.var.dist
       0B Sep 25 14:14 /var/tmp/LOCK_FILE
       666B Sep 25 14:14 /var/tmp/appidd_trace_debug
       0B Sep 25 14:14 /var/tmp/eedebug_bin_file
       34B Sep 25 14:14 /var/tmp/gksdchk.log
       46B Sep 25 14:14 /var/tmp/kmdchk.log
       57B Sep 25 14:14 /var/tmp/krt_rpf_filter.txt
       42B Sep 25 14:13 /var/tmp/pfe_debug_commands
       0B Sep 25 14:14 /var/tmp/pkg_cleanup.log.err
       30B Sep 25 14:14 /var/tmp/policy_status
       0B Sep 25 14:14 /var/tmp/rtsdb/if-rtsdb
       Delete these files ? [yes,no] (no) yes
<
output omitted>
```

NOTE: If this command does not free up enough disk space, see [SRX] Common and safe files to remove in order to increase available system storage for details on safe files you can manually remove from vSRX Virtual Firewall to free up disk space.

4. Use FTP, SCP, or a similar utility to upload the Junos OS Release 21.1R1 for vSRX Virtual Firewall .tgz file to **/var/crash/corefiles/** on the local file system of your vSRX Virtual Firewall VM. For example:

```
root@vsrx> file copy ftp://username:prompt@ftp.hostname.net/pathname/
junos-vsrx-x86-64-20.4-2020-10-12.0_RELEASE_20.4_THROTTLE.tgz /var/crash/corefiles/
```

5. From operational mode, install the software upgrade package.

```
root@vsrx> request system software add /var/crash/corefiles/junos-vsrx-
x86-64-20.4-2020-10-12.0_RELEASE_20.4_THROTTLE.tgz no-copy no-validate reboot
Verified junos-vsrx-x86-64-20.4-2020-10-12.0_RELEASE_20.4_THROTTLE signed by
PackageDevelopmentEc_2017 method ECDSA256+SHA256
THIS IS A SIGNED PACKAGE
WARNING:     This package will load JUNOS 20.4 software.
WARNING:     It will save JUNOS configuration files, and SSH keys
WARNING:     (if configured), but erase all other files and information
WARNING:     stored on this machine.  It will attempt to preserve dumps
WARNING:     and log files, but this can not be guaranteed.  This is the
WARNING:     pre-installation stage and all the software is loaded when
WARNING:     you reboot the system.
Saving the config files ...
Pushing Junos image package to the host...
Installing /var/tmp/install-media-srx-mr-vsrx-20.4-2020-10-12.0_RELEASE_20.4_THROTTLE.tgz
Extracting the package ...
total 975372
-rw-r--r-- 1 30426 950 710337073 Oct 19 17:31 junos-srx-mr-
vsrx-20.4-2020-10-12.0_RELEASE_20.4_THROTTLE-app.tgz
-rw-r--r-- 1 30426 950 288433266 Oct 19 17:31 junos-srx-mr-
vsrx-20.4-2020-10-12.0_RELEASE_20.4_THROTTLE-linux.tgz
Setting up Junos host applications for installation ...
```

```
============================================
Host OS upgrade is FORCED
Current Host OS version: 3.0.4
New Host OS version: 3.0.4
Min host OS version required for applications: 0.2.4
============================================
Installing Host OS ...
upgrade_platform: -------------------
upgrade_platform: Parameters passed:
upgrade_platform: silent=0
upgrade_platform: package=/var/tmp/junos-srx-mr-vsrx-20.4-2020-10-12.0_RELEASE_20.4_THROTTLE-
linux.tgz
upgrade_platform: clean install=0
upgrade_platform: clean upgrade=0
upgrade_platform: Need reboot after staging=0
upgrade_platform: -------------------
upgrade_platform:
upgrade_platform: Checking input /var/tmp/junos-srx-mr-
vsrx-20.4-2020-10-12.0_RELEASE_20.4_THROTTLE-linux.tgz ...
upgrade_platform: Input package /var/tmp/junos-srx-mr-
vsrx-20.4-2020-10-12.0_RELEASE_20.4_THROTTLE-linux.tgz is valid.
upgrade_platform: Backing up boot assets..
cp: omitting directory '.'
bzImage-intel-x86-64.bin: OK
initramfs.cpio.gz: OK
version.txt: OK
initrd.cpio.gz: OK
upgrade_platform: Checksum verified and OK...
/boot
upgrade_platform: Backup completed
upgrade_platform: Staging the upgrade package - /var/tmp/junos-srx-mr-
vsrx-20.4-2020-10-12.0_RELEASE_20.4_THROTTLE-linux.tgz..
./
./bzImage-intel-x86-64.bin
./initramfs.cpio.gz
./upgrade_platform
./HOST_COMPAT_VERSION
./version.txt
./initrd.cpio.gz
./linux.checksum
./host-version
bzImage-intel-x86-64.bin: OK
initramfs.cpio.gz: OK
```

```
version.txt: OK
upgrade_platform: Checksum verified and OK...
upgrade_platform: Staging of /var/tmp/junos-srx-mr-
vsrx-20.4-2020-10-12.0_RELEASE_20.4_THROTTLE-linux.tgz completed
upgrade_platform: System need *REBOOT* to complete the upgrade
upgrade_platform: Run upgrade_platform with option -r | --rollback to rollback the upgrade
Host OS upgrade staged. Reboot the system to complete installation!
WARNING:     A REBOOT IS REQUIRED TO LOAD THIS SOFTWARE CORRECTLY. Use the
WARNING:     'request system reboot' command when software installation is
WARNING:     complete. To abort the installation, do not reboot your system,
WARNING:     instead use the 'request system software rollback'
WARNING:     command as soon as this operation completes.
NOTICE: 'pending' set will be activated at next reboot...
Rebooting. Please wait ...
shutdown: [pid 13050]
Shutdown NOW!
*** FINAL System shutdown message from root@ ***
System going down IMMEDIATELY
Shutdown NOW!
System shutdown time has arrived\x07\x07
```

If no errors occur, Junos OS reboots automatically to complete the upgrade process. You have successfully upgraded to Junos OS Release 21.1R1 for vSRX Virtual Firewall.

> **NOTE**: Starting in Junos OS Release 17.4R1, upon completion of the vSRX Virtual Firewall image upgrade, the original image is removed by default as part of the upgrade process.

6. Log in and use the `show version` command to verify the upgrade.

```
--- JUNOS 20.4-2020-10-12.0_RELEASE_20.4_THROTTLE Kernel 64-bit
JNPR-11.0-20171012.170745_fbsd-
At least one package installed on this device has limited support.
Run 'file show /etc/notices/unsupported.txt' for details.
root@:~ # cli
root> show version
Model: vsrx
Junos: 20.4-2020-10-12.0_RELEASE_20.4_THROTTLE
JUNOS OS Kernel 64-bit  [20171012.170745_fbsd-builder_stable_11]
JUNOS OS libs [20171012.170745_fbsd-builder_stable_11]
JUNOS OS runtime [20171012.170745_fbsd-builder_stable_11]
JUNOS OS time zone information [20171012.170745_fbsd-builder_stable_11]
JUNOS OS libs compat32 [20171012.170745_fbsd-builder_stable_11]
JUNOS OS 32-bit compatibility [20171012.170745_fbsd-builder_stable_11]
JUNOS py extensions [20171017.110007_ssd-builder_release_174_throttle]
JUNOS py base [20171017.110007_ssd-builder_release_174_throttle]
JUNOS OS vmguest [20171012.170745_fbsd-builder_stable_11]
JUNOS OS crypto [20171012.170745_fbsd-builder_stable_11]
JUNOS network stack and utilities [20171017.110007_ssd-builder_release_174_throttle]
JUNOS libs [20171017.110007_ssd-builder_release_174_throttle]
JUNOS libs compat32 [20171017.110007_ssd-builder_release_174_throttle]
JUNOS runtime [20171017.110007_ssd-builder_release_174_throttle]
JUNOS Web Management Platform Package [20171017.110007_ssd-builder_release_174_throttle]
JUNOS srx libs compat32 [20171017.110007_ssd-builder_release_174_throttle]
JUNOS srx runtime [20171017.110007_ssd-builder_release_174_throttle]
JUNOS common platform support [20171017.110007_ssd-builder_release_174_throttle]
JUNOS srx platform support [20171017.110007_ssd-builder_release_174_throttle]
JUNOS mtx network modules [20171017.110007_ssd-builder_release_174_throttle]
JUNOS modules [20171017.110007_ssd-builder_release_174_throttle]
JUNOS srxtvp modules [20171017.110007_ssd-builder_release_174_throttle]
JUNOS srxtvp libs [20171017.110007_ssd-builder_release_174_throttle]
JUNOS srx libs [20171017.110007_ssd-builder_release_174_throttle]
JUNOS srx Data Plane Crypto Support [20171017.110007_ssd-builder_release_174_throttle]
JUNOS daemons [20171017.110007_ssd-builder_release_174_throttle]
JUNOS srx daemons [20171017.110007_ssd-builder_release_174_throttle]
JUNOS Online Documentation [20171017.110007_ssd-builder_release_174_throttle]
JUNOS jail runtime [20171012.170745_fbsd-builder_stable_11]
JUNOS FIPS mode utilities [20171017.110007_ssd-builder_release_174_throttle]
```

Validating the OVA Image

If you have downloaded a vSRX Virtual Firewall .ova image and need to validate it, see Validating the vSRX .ova File for VMware.

Note that only .ova (VMware platform) vSRX Virtual Firewall images can be validated. The .qcow2 vSRX Virtual Firewall images for use with KVM cannot be validated the same way. File checksums for all software images are, however, available on the download page.

Upgrade and Downgrade Support Policy for Junos OS Releases and Extended End-Of-Life Releases

We have two types of releases, standard EOL and EEOL:

- Standard End of Life (EOL) releases have engineering support for twenty four months after the first general availability date and customer support for an additional six more months.
- Extended End of Life (EEOL) releases have engineering support for sixty months after the first general availability date and customer support for an additional six more months.

> **NOTE**: The sixty months of support for EEOL releases is introduced in Junos OS 23.2 release and is available for all later releases. For releases prior to 23.2, the support for EEOL releases continues to be thirty six months.

For both standard EOL and EEOL releases, you can upgrade to the next three subsequent releases or downgrade to the previous three releases.

For EEOL releases only, you have an additional option - you can upgrade directly from one EEOL release to the next two subsequent EEOL releases, even if the target release is beyond the next three releases. Likewise, you can downgrade directly from one EEOL release to the previous two EEOL releases, even if the target release is beyond the previous three releases.

Table 8: EOL and EEOL Releases

Release Type	End of Engineering (EOE)	End of Support (EOS)	Upgrade/ Downgrade to subsequent 3 releases	Upgrade/ Downgrade to subsequent 2 EEOL releases
Standard End of Life (EOL)	24 months	End of Engineering + 6 months	Yes	No
Extended End of Life (EEOL)	60 months	End of Engineering + 6 months	Yes	Yes

For more information about standard EOL and EEOL releases, see https://www.juniper.net/support/eol/junos.html.

For information about software installation and upgrade, see the Installation and Upgrade Guide.

Licensing

In 2020, Juniper Networks introduced a new software licensing model. The Juniper Flex Program comprises a framework, a set of policies, and various tools that help unify and thereby simplify the multiple product-driven licensing and packaging approaches that Juniper Networks has developed over the past several years.

The major components of the framework are:

- A focus on customer segments (enterprise, service provider, and cloud) and use cases for Juniper Networks hardware and software products.
- The introduction of a common three-tiered model (standard, advanced, and premium) for all Juniper Networks software products.
- The introduction of subscription licenses and subscription portability for all Juniper Networks products, including Junos OS and Contrail.

For information about the list of supported products, see Juniper Flex Program.

Finding More Information

- **Feature Explorer**—Juniper Networks Feature Explorer helps you to explore software feature information to find the right software release and product for your network.

  https://apps.juniper.net/feature-explorer/

- **PR Search Tool**—Keep track of the latest and additional information about Junos OS open defects and issues resolved.

  https://prsearch.juniper.net/InfoCenter/index?page=prsearch

- **Hardware Compatibility Tool**—Determine optical interfaces and transceivers supported across all platforms.

  https://apps.juniper.net/hct/home

  > **NOTE**: To obtain information about the components that are supported on the devices and the special compatibility guidelines with the release, see the Hardware Guide for the product.

- **Juniper Networks Compliance Advisor**—Review regulatory compliance information about Common Criteria, FIPS, Homologation, RoHS2, and USGv6.

  https://pathfinder.juniper.net/compliance/

Requesting Technical Support

IN THIS SECTION

Technical product support is available through the Juniper Networks Technical Assistance Center (JTAC). If you are a customer with an active Juniper Care or Partner Support Services support contract, or are covered under warranty, and need post-sales technical support, you can access our tools and resources online or open a case with JTAC.

- JTAC policies—For a complete understanding of our JTAC procedures and policies, review the JTAC User Guide located at https://www.juniper.net/us/en/local/pdf/resource-guides/7100059-en.pdf.
- Product warranties—For product warranty information, visit https://www.juniper.net/support/warranty/.
- JTAC hours of operation—The JTAC centers have resources available 24 hours a day, 7 days a week, 365 days a year.

Self-Help Online Tools and Resources

For quick and easy problem resolution, Juniper Networks has designed an online self-service portal called the Customer Support Center (CSC) that provides you with the following features:

- Find CSC offerings: https://www.juniper.net/customers/support/
- Search for known bugs: https://prsearch.juniper.net/
- Find product documentation: https://www.juniper.net/documentation/
- Find solutions and answer questions using our Knowledge Base: https://kb.juniper.net/
- Download the latest versions of software and review release notes: https://www.juniper.net/customers/csc/software/

- Search technical bulletins for relevant hardware and software notifications: https://kb.juniper.net/InfoCenter/
- Join and participate in the Juniper Networks Community Forum: https://www.juniper.net/company/communities/

To verify service entitlement by product serial number, use our Serial Number Entitlement (SNE) Tool: https://entitlementsearch.juniper.net/entitlementsearch/

Creating a Service Request with JTAC

You can create a service request with JTAC on the Web or by telephone.

- Visit Juniper Support Portal: Case Management, Product Support & More.
- Call 1-888-314-JTAC (1-888-314-5822 toll-free in the USA, Canada, and Mexico).

For international or direct-dial options in countries without toll-free numbers, see https://support.juniper.net/support/requesting-support/.

Revision History

5 February 2026—Junos OS Release 23.4R2.

8 January 2026—Junos OS Release 23.4R2.

22 September 2025—Junos OS Release 23.4R2.

28 August 2025—Junos OS Release 23.4R2.

14 August 2025—Junos OS Release 23.4R2.

31 March 2025—Junos OS Release 23.4R2.

8 August 2024—Junos OS Release 23.4R2.

19 July 2024—Junos OS Release 23.4R2.

10 July 2024—Junos OS Release 23.4R2.