Release Notes

Published
2024-04-18

Junos OS Release 22.3R2®

Juniper Networks | 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, Junos Fusion Enterprise, Junos Fusion Provider Edge, MX Series, NFX Series, PTX Series, QFX Series, SRX Series, vMX, vRR, and vSRX. These release notes accompany Junos OS Release 22.3R1. 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.

Junos OS Release Notes for ACX Series

IN THIS SECTION

These release notes accompany Junos OS Release 22.3R2 for the ACX Series. They describe new and changed features, limitations, and known and resolved problems in the hardware and software.

You can also find these release notes on the Juniper Networks Junos OS Documentation webpage, located at https://www.juniper.net/documentation/product/en_US/junos-os.

What's New

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

What's Changed

IN THIS SECTION

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

Junos XML API and Scripting

- **The `file copy` command supports only text-formatted output in the CLI (ACX Series, EX Series, MX Series, PTX Series, QFX Series, SRX Series, vMX, and vSRX)**—The `file copy` command does not emit output when the operation is successful and supports only text-formatted output when an error occurs. The `file copy` command does not support using the `| display xml` filter or the `| display json` filter to display command output in XML or JSON format in any release. We've removed these options from the CLI.

Software Installation and Upgrade

- **New options for the `request system snapshot` command (ACX Series, EX Series, MX Series, PTX Series, QFX Series, and SRX Series)**—The `request system snapshot` command includes new options for non-recovery snapshots. You can include the `name` option to specify a user-defined name for the snapshot, and you can include the `configuration` or `no-configuration` option to include or exclude configuration files in the snapshot. By default, the snapshot saves the configuration files, which include the contents of the **/config** and **/var** directories and certain SSH files.

  [See request system snapshot (Junos OS with Upgraded FreeBSD).]

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.

General Routing

- IFD based CFM sessions are not supported. PR1660086

Infrastructure

- When upgrading from releases before Junos OS Release 21.2 to Release 21.2 and onward, validation and upgrade might fail. The upgrading requires using of `no-validate` configuration statement.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

- The VXLAN VNI (mcast) scaling causes traffic issue. PR1462548
- Due to BRCM KBP issue route lookup might fail. PR1533513
- Service MIC does not work on ACX500 running Junos OS Release 20.4 or higher. PR1569103
- On all Junos and Evolved platforms, the hosts will not receive multicast traffic when snooping is configured in a Ethernet Virtual Private Network - Multiprotocol Label Switching (EVPN-MPLS) enabled broadcast domain. PR1613462
- For ACX5448, MX204 and MX2008 "VM Host-based" platforms, starting with Junos 21.4R1 or later, ssh and root login is required for copying line card image (chspmb.elf for MX2008) from Junos VM to Linux host during installation. The ssh and root login are required during installation. Use `deny-password` instead of `deny` as default root-login option under ssh config to allow internal trusted communication. Ref https://kb.juniper.net/TSB18224 PR1629943
- On Junos ACX platforms (ACX1100, ACX2100 and ACX2200) the Forwarding Engine Board (FEB) crash might occur. This might only occur when the system has encountered a dual parity error on MPLS entry memory in the hardware. There might be an impact on services when the FEB crashes, however, it returns to normal functionality after the crash.PR1632043
- A vulnerability in class-of-service (CoS) queue management in Juniper Networks Junos OS on the ACX2000 Series devices allows an unauthenticated network-based attacker to cause a Denial of Service (DoS). Refer to https://kb.juniper.net/JSA70187 for more information.PR1637615
- In an interop scenario, when using 1G SFP Optic on PIC-2, auto-negotiation should be disabled on the peer. PR1657766
- 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 hardware. 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 ACX5000 series devices.PR1665178
- When there are more than 1 dhcp server connected to the device and zeroize in initiated then multiple route are added and the file server is not reachable after the zeroize if it is not reachable through the default route.PR1675011

- `dc-pfe: HEAP malloc(0) detected!` when a VPLS instance is deactivated in ACX5048. This are informational messages. PR1692400
- Convergance time might be more than 60ms for OSPF TILFA Node protection testing. PR1695292
- FIPS mode is not supported in this release for SRXSME devices. PR1697999

Resolved Issues

IN THIS SECTION

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

General Routing

- The Layer 3 packets with the destination as IPv6 Link Local address will not work. PR1638642
- jdhcpd core is seen on boot. PR1658327
- SSH non-default port configuration causes FPC offline after upgrade to Junos OS Release 21.4. PR1660446
- The rpd core might be seen when there is a synchronization issue. PR1663050
- Inline BFDv6 Sessions might go DOWN and stay in that state on ACX5448 and ACX710 platforms. PR1666746
- Traffic loss is observed when the VRRP is configured over the AE interface. PR1666853
- New BFD sessions will not come up on ACX5448/ACX710 due to continuous flaps. PR1670684
- PIC core file is seen when a CPCD service is modified. PR1675990
- The LLDP packets will not be transmitted over l2circuit on the ACX platform. PR1678752

- Memory leak is seen on ACX710/5448 when the core link flaps. PR1681980
- ACX5448 DNX PFE incorrectly spelled as QUMARN instead of Qumran. PR1682819
- The traffic drop would be observed with inter-vlan configuration when deactivating and activating the EVPN routing instance. PR1683321
- jnxOperatingDescr.1.1.0.0 returns blank, but jnxOperatingState.1.1.0.0 returns value. PR1683753
- On Junos ACX the IP packets with VLAN tags do not get an ICMP response when sent out on the IRB interface. PR1683770
- ACX5448: ACX710 L2Circuit traffic drop with control-word enabled or control-word configuration change. PR1683900
- ACX710 : Auto-mdix is not working in ACX710. PR1685431
- subscriber-management-helper is thrashing, not restarted, messages are seen on ACX5448. PR1688107
- The jdchpd core file is seen with dhcp-snooping persistent configuration. PR1688644
- The LACP would get stuck in a continuous update loop in the MC-LAG scenario. PR1688958
- EVPN Packets might go to incorrect queues due to the incorrect classification and might lead to packets drop during congestion. PR1689604
- Packet forwarding fails on specific ACX Junos platforms due to flapping of core interface member link in the MPLS-EVPN environment. PR1690590
- PCS errors and framing errors on 100GE interfaces on certain Juniper platforms. PR1692063

Routing Protocols

- Incorrect SR-TE secondary path weight makes the secondary path active in forwarding table. PR1696598

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.

Starting in Junos OS release 21.2R1, all Junos OS products which were previously running on FreeBSD 11.x based Junos OS are migrated to FreeBSD 12.x based Junos OS, except EX4400. Starting with Junos OS release 21.3R1, EX4400 platforms are migrated to FreeBSD 12.x based Junos OS.

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 thirty six months after the first general availability date and customer support for an additional six more 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 example, you can upgrade from 20.4 to the next three releases – 21.1, 21.2 and 21.3 or downgrade to the previous three releases – 20.3, 20.2 and 20.1.

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. For example, 20.4 is an EEOL release. Hence, you can upgrade from 20.4 to the next two EEOL releases – 21.2 and 21.4 or downgrade to the previous two EEOL releases – 20.2 and 19.4.

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)	36 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

These release notes accompany Junos OS Release 22.3R2 for the cSRX Container Firewall, a containerized version of the SRX Series Services Gateway. They describe new and changed features, limitations, and known and resolved problems in the hardware and software.

You can also find these release notes on the Juniper Networks Junos OS Documentation webpage, located at https://www.juniper.net/documentation/product/en_US/junos-os.

What's New

There are no new features or enhancements to existing features in Junos OS Release 22.3R2 for cSRX.

What's Changed

There are no changes in behavior and syntax in Junos OS Release 22.3R2 for cSRX.

Known Limitations

There are no known limitations in hardware and software in Junos OS 22.3R2 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 and software in Junos OS Release 22.3R2 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

IN THIS SECTION

Resolved Issues

There are no resolved issues in Junos OS Release 22.3R2 for cSRX.

Junos OS Release Notes for EX Series

IN THIS SECTION

These release notes accompany Junos OS Release 22.3R2 for the EX Series. They describe new and changed features, limitations, and known and resolved problems in the hardware and software.

You can also find these release notes on the Juniper Networks Junos OS Documentation webpage, located at https://www.juniper.net/documentation/product/en_US/junos-os.

What's New

There are no new features or enhancements to existing features in this release for EX Series Switches.

What's Changed

IN THIS SECTION

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

Junos XML API and Scripting

- **The `file copy` command supports only text-formatted output in the CLI (ACX Series, EX Series, MX Series, PTX Series, QFX Series, SRX Series, vMX, and vSRX)**—The `file copy` command does not emit output when the operation is successful and supports only text-formatted output when an error occurs. The `file copy` command does not support using the `| display xml` filter or the `| display json` filter to display command output in XML or JSON format in any release. We've removed these options from the CLI.

Software Installation and Upgrade

- **New options for the `request system snapshot` command (ACX Series, EX Series, MX Series, PTX Series, QFX Series, and SRX Series)**—The `request system snapshot` command includes new options for non-recovery snapshots. You can include the `name` option to specify a user-defined name for the snapshot, and you can include the `configuration` or `no-configuration` option to include or exclude configuration files in the snapshot. By default, the snapshot saves the configuration files, which include the contents of the **/config** and **/var** directories and certain SSH files.

  [See request system snapshot (Junos OS with Upgraded FreeBSD).]

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

- Unified ISSU on EX4650 switches will not be supported if there is a change in the vendor versions of the chipset SDKs between the releases. This is a product limitation as change in the vendor firmware leads to the chip reset and hence ISSU is impacted. The vendor versions in the chipset SDKs should be the same between two JUNOS OS releases for unified ISSU to work. PR1634695
- EX4100 48P/T SKUs: On changing interface speed change, the interface stats are retained on ports 24-to-47 but cleared on ports 0-23. PR1657995
- On EX4100 and EX4100-F series SKU PIC0 ports (except EX4100-24MP first 8 ports [mge 0-7]), Jabber frames are dropped as oversized frames. PR1663992
- EX4100 series and EX4100-F series: VC (PIC1) 4x1G ports in network-mode will need auto-neg off on the peer-device. PR1665640
- MVRP on PVLAN promiscuous port is not supported. If you configure MVRP on promiscuous port, then hosts connected to secondary VLAN ports will not be able to reach external world through promiscuous port carrying primary VLAN tags. PR1693345

Virtual Chassis

- EX4400 supports multiple uplink modules. Some supports VC port conversion and some does not and hence, the recommended procedure is to convert VC port to NW port first and then make sure uplink module is made offline using `request chassis pic <> fpc <>` command before removal.PR1665242

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.

Class of Service (CoS)

- On all Junos platforms, in a scaled scenario when some of the ge/xe/et interfaces are members of Aggregated Ethernet (AE) and the Class of Service (CoS) forwarding-class-set configuration is applied with a wildcard for all the physical interfaces and AE, it would trigger a Flexible PIC Concentrators (FPC) crash which leads to traffic loss. PR1688455

General Routing

- When you add VLAN as an action for changing the VLAN in both ingress and egress filters, the filter does not ge installed. PR1362609
- runt, fragment and jabber counters are not incrementing on EX4300-MPsPR1492605
- On EX4300-48MPdevices, if POE is enabled, a primary Routing Engine might reconnect 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
- On EX4400 family of devices, sometimes login prompt is not shown after the login session ends. PR1582754
- On EX4600 devices, the Virtual-chassis goes in to the `Unstable` state for 3 to 7 minutes causing traffic loss. PR1661349
- On EX4100 and EX4100-F devices, PIC 1 ports with 1G optic displays AN enabled but it is not enabled in the hardware. PR1666227
- On the EX4600 device with SFP-LX10/SFP-SX, after a power cycle/software reboot, all ports are initialized and links are up with auto-negotiation enabled. Few ports are up and traffic flows whereas few ports are up but no traffic flow through them. PR1672583
- On EX4100 and EX4100-F Virtual Chassis, non-existing PIC ports (example, PIC0:PORT100 and PIC2:PORT102) while running the jvision query. PR1681673

- If MVRP is enabled on an MSTP enabled interface, the interface will be made part of all the existing instances on the switch, So, if there are two interfaces between R1 and R2 as below: R1(et-0/0/1 and et-0/0/2)======(et-0/0/1 and et-0/0/2)R2 And one interface is MVRP enabled (say et-0/0/1), and et-0/0/2 is not MVRP enabled. By configuration et-0/0/1 is part of MSTI-1 and et-0/0/2 is part of MSTI-2. MSTI-1 is running on vlan-100 and MSTI-2 is running on Vlan-200. R2 in this case, is advertising only vlan-100. The MVRP enabled interface will become part of all the MSTIs(MSTI-1 and MSTI-2 both) configured on the device and it will take part in the FSM of all the MSTIs. Although et-0/0/1 is not member interface of vlan-200(correspnding to MSTI-2). This potentially can cause a problem where et-0/0/1 although not a vlan-200 member, will go into FWD state and et-0/0/2, genuine member of vlan-200 goes into BLK state for MSTI-2. So, when traffic is received in vlan-200 it will be sent out of et-0/0/1, it gets dropped. PR1686596
- When a sfp gets unplugged or plugged in, the sfp might not be recognized. PR1696444
- Traffic loss could be seen in case config changes lead to switching from fallback to primary or vice-versa are committed, while SAK rollover from current live session is in progress. The issue is dependent on sequence of event at specific time. Example - MACsec session is live with primary key and at non-keyserver CAK for primary is changed this will lead to switching to fallback session, in case at same instance SAK rollover was triggered by Key-server then traffic loss will be observed. PR1698687

Interfaces and Chassis

- On EX46000 Virtual Chassis (VC), if a primary member gets unplugged or forced to power off, the unicast traffic drops due to `mac-persistence-timer` expiry difference in MAC addresses between logical aggregated parent interface and member aggregated ethernet(ae) interface. PR1695663

Platform and Infrastructure

- On EX4400-48MP devices, VM file generates core files and Virtual Chassis might split with multicast scale scenario. PR1614145
- On EX4300 devices, if you configure `encapsulation ethernet-bridge`, the interface gets programmed as trunk instead of access in VLAN membership. This leads to untagged traffic drop. PR1665785
- On EX4300-24T, EX4300-48P, EX4300-VC, EX430024P, EX430032F and EX430048T devices, when a VSTP (VLAN Spanning Tree Protocol) BPDU (Bridge Protocol Data Unit) arrives with a VLAN ID that is not configured in the switch, but that matches with an HW Token of any other configured VLAN, the VLAN ID of the BPDU will be changed to the VLAN ID corresponding to the matched HW

Token and flooded. This disrupts STP convergence on the configured VLAN because some ports can incorrectly go into the `Blocking` state. PR1673000

Virtual Chassis

- On EX4600 Virtual Chassis (VC), the primary Routing Engine reboot and all-members reboot leads to the Packet Forwarding Engine Manager hogging logs when you install SFP-T pluggables. The Packet Forwarding Engine Manager hogging logs has no functionality impact. PR1685067
- On EX4600 Virtual Chassis (VC), when the `request system reboot all members` command gets executed, post-reboot one of the VC member/Flexible PIC Concentrator(FPC) might disconnect and join the VC back due to Packet Forwarding Engine restart. Traffic loss occurs when you disconnect FPC. 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

- DHCP packets might get looped in a VXLAN setup. PR1657597
- In the EVPN-VXLAN scenario, the DHCP packets will get dropped when the DHCP relay agent is configured. PR1662524

- EX4100 and EX4100-F series: On device reboot in scaled PoE scenario with perpetual PoE configured, it takes some time (a few minutes) for the CLI to reflect the correct status for LLDP enabled ports. PR1671311
- On EX4100 MACsec interface statistics of encrypted/decrypted bytes do not increment further after reaching a 40-bit limit. PR1658584
- Aggregate Ethernet interface will receive unknown unicast traffic on FPC3 reboot of a VC. PR1678430
- DHCP binding will fail for the clients (Clients connected on an AE interface with 2 or more VLANs) on a VLAN where DHCP security is not configured. PR1679094
- Firewall functions will not work as expected when egress firewall filter is configured. PR1679574
- On EX2300 and EX3400, `set system ports console log-out-on-disconnect` does not allow user to log in through console. PR1680408
- Multicast traffic loss is seen with **igmp-snooping** running on EX4100. PR1681478
- EX4100-24mp/48mp/48p/48t/24p/24t: Activity LED is lit on some ports if 1G optic is inserted without link being present or up. PR1682633
- The l2cpd process crash might be observed when disabling RSTP on an interface. PR1684072
- Licenses on the device might become invalid when the device is upgraded from a legacy licensing-based release to an Agile licensing-based release. PR1684842
- MAC address learning might not happen on specific EX platforms. PR1685938
- The l2ald core seen after zeroize. PR1686097
- EX4300-48MP, factory Reset/Mode button cannot toggle status mode LED (SPD, DX, EN, and PoE). PR1687407
- EX4400 SNMP : FRU removal/insertion trap may not be generated when Fan try or PIC is removed and inserted. PR1687848
- On EX4100 and EX4400 platform, alarm **PEM is not supported** might be seen. PR1690674
- The factory default configuration does not have xe-0/2/0. PR1691174
- Few uplink ports of EX2300-48MP are not coming up. PR1692579
- The dot1x reauthentication will not work for a port with VoIP VLAN. PR1693640
- PFE crash is seen on all Junos OS EX4600 platforms with L2PT configuration. PR1694076
- On a PVLAN with DAI ARP packets will be forwarded between isolated ports. PR1694800

- The dot1x authentication will not be enabled on interfaces with specific configuration combination. PR1696906
- Dot1x authentication failure for EVPN VXLAN enabled port. PR1697995
- TCAM space might be exhausted when learning DHCP snooping entries on a trusted port. PR1699777
- Traffic drops observed with hierarchal overlay ECMP configuration. PR1704470

Platform and Infrastructure

- Traffic drop seen and filter not hitting as expected for match condition traffic class with FLT option configured. PR1573350
- EX9000 platforms do not relay a DHCP offer with a broadcast flag under EVPN-VXLAN scenario. PR1670923

Virtual Chassis

- Instability observed after mastership switchover on members with SFP-T pluggable installed on EX4600-VC. PR1689946

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.

Starting in Junos OS release 21.2R1, all Junos OS products which were previously running on FreeBSD 11.x based Junos OS are migrated to FreeBSD 12.x based Junos OS, except EX4400. Starting with Junos OS release 21.3R1, EX4400 platforms are migrated to FreeBSD 12.x based Junos OS.

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 thirty six months after the first general availability date and customer support for an additional six more 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 example, you can upgrade from 20.4 to the next three releases – 21.1, 21.2 and 21.3 or downgrade to the previous three releases – 20.3, 20.2 and 20.1.

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. For example, 20.4 is an EEOL release. Hence, you can upgrade from 20.4 to the next two EEOL releases – 21.2 and 21.4 or downgrade to the previous two EEOL releases – 20.2 and 19.4.

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)	36 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

These release notes accompany Junos OS Release 22.3R2 for the JRR Series. They describe new and changed features, limitations, and known and resolved problems in the hardware and software.

You can also find these release notes on the Juniper Networks Junos OS Documentation webpage, located at https://www.juniper.net/documentation/product/en_US/junos-os.

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 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

IN THIS SECTION

Learn about the issues fixed in this release for JRR Series Route Reflectors.

General Routing

- A 802.1Q tagged Ethernet traffic with an expected VLAN ID and with a non-zero 802.1P value ingressing a JRR200 VLAN enabled interface is dropped. PR1691694

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.

Starting in Junos OS release 21.2R1, all Junos OS products which were previously running on FreeBSD 11.x based Junos OS are migrated to FreeBSD 12.x based Junos OS, except EX4400. Starting with Junos OS release 21.3R1, EX4400 platforms are migrated to FreeBSD 12.x based Junos OS.

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 thirty six months after the first general availability date and customer support for an additional six more 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 example, you can upgrade from 20.4 to the next three releases – 21.1, 21.2 and 21.3 or downgrade to the previous three releases – 20.3, 20.2 and 20.1.

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. For example, 20.4 is an EEOL release. Hence, you can upgrade from 20.4 to the next two EEOL releases – 21.2 and 21.4 or downgrade to the previous two EEOL releases – 20.2 and 19.4.

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)	36 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

These release notes accompany Junos OS Release 22.3R2 for Juniper Secure Connect. They describe new and changed features, limitations, and known and resolved problems in the hardware and software.

You can also find these release notes on the Juniper Networks Junos OS Documentation webpage, located at https://www.juniper.net/documentation/product/en_US/junos-os.

What's New

There are no new features or enhancements to existing features in Junos OS Release 22.3R2 for Juniper Secure Connect.

What's Changed

There are no changes in behavior and syntax in Junos OS Release 22.3R2 for Juniper Secure Connect.

Known Limitations

There are no known limitations in hardware and software in Junos OS 22.3R2 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 and software in Junos OS Release 22.3R2 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 Junos OS Release 22.3R2 for Juniper Secure Connect.

Junos OS Release Notes for Junos Fusion for Enterprise

IN THIS SECTION

These release notes accompany Junos OS Release 22.3R2 for the Junos Fusion for enterprise. They describe new and changed features, limitations, and known and resolved problems in the hardware and software.

You can also find these release notes on the Juniper Networks Junos OS Documentation webpage, located at https://www.juniper.net/documentation/product/en_US/junos-os.

What's New

There are no new features or enhancements to existing features in Junos OS Release 22.3R2 for Junos fusion for enterprise.

What's Changed

There are no changes in behavior and syntax in Junos OS Release 22.3R2 for Junos Fusion for Enterprise.

Known Limitations

There are no known limitations in hardware or software in this release for Junos fusion for enterprise.

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 Junos Fusion for enterprise.

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 Junos Fusion for enterprise.

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 procedure to upgrade or downgrade Junos OS and satellite software for a Junos fusion for enterprise. Upgrading or downgrading Junos OS and satellite software might take several hours, depending on the size and configuration of the Junos fusion for enterprise topology.

Basic Procedure for Upgrading Junos OS on an Aggregation Device

When upgrading or downgrading Junos OS for an aggregation device, always use the `junos-install` 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 `junos-install` package and details of the installation process, see the Installation and Upgrade Guide.

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. See the Junos OS Administration Library.

To download and install Junos OS:

1. Using a Web browser, navigate to the Download Software URL on the Juniper Networks webpage:

   https://www.juniper.net/support/downloads/

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

3. Select **By Technology > Junos Platform > Junos fusion** to find the software that you want to download.

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

5. Select the **Software** tab.

6. Select the software package for the release.

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 `junos-install` package on the aggregation 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 commands, where *n* is the spin number.

```
user@host> request system software add validate reboot source/package-name.n.tgz
```

All other customers, use the following commands, where *n* is the spin number.

```
user@host> request system software add validate reboot source/package-name.n-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* (available only for Canada and U.S. version)

The `validate` option validates the software package against the current configuration as a prerequisite to adding the software package to ensure that the router reboots successfully. This is the default behavior when the software package being added is a different release.

Adding the `reboot` command reboots 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.

Upgrading an Aggregation Device with Redundant Routing Engines

If the aggregation device has two Routing Engines, perform a Junos OS installation on each Routing Engine separately to minimize disrupting network operations as follows:

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*.

Preparing the Switch for Satellite Device Conversion

There are multiple methods to upgrade or downgrade satellite software in your Junos fusion for enterprise. See Configuring or Expanding a Junos fusion for enterprise.

For satellite device hardware and software requirements, see Understanding Junos fusion for enterprise Software and Hardware Requirements.

Use the following command to install Junos OS on a switch before converting it into a satellite device:

```
user@host> request system software add validate reboot source/package-name
```

NOTE: The following conditions must be met before a Junos switch that is running Junos OS Release 14.1X53-D43 can be converted to a satellite device when the action is initiated from the aggregation device:

- The switch running Junos OS can be converted only to SNOS 3.1 and later.
- Either the switch must be set to factory-default configuration by using the `request system zeroize` command, or the following command must be included in the configuration: `set chassis auto-satellite-conversion`.

When the interim installation has completed and the switch is running a version of Junos OS that is compatible with satellite device conversion, perform the following steps:

1. Log in to the device using the console port.
2. Clear the device:

```
[edit]
user@satellite-device# request system zeroize
```

NOTE: The device reboots to complete the procedure for resetting the device.

If you are not logged in to the device using the console port connection, your connection to the device is lost after you enter the **request system zeroize** command.

If you lose connection to the device, log in using the console port.

3. (EX4300 switches only) After the reboot is complete, convert the built-in 40-Gbps QSFP+ interfaces from Virtual Chassis ports (VCPs) into network ports:

```
user@satellite-device> request virtual-chassis vc-port delete pic-slot 1 port port-number
```

For example, to convert all four built-in 40-Gbps QSFP+ interfaces on an EX4300-24P switch into network ports:

```
user@satellite-device> request virtual-chassis vc-port delete pic-slot 1 port 0
user@satellite-device> request virtual-chassis vc-port delete pic-slot 1 port 1
user@satellite-device> request virtual-chassis vc-port delete pic-slot 1 port 2
user@satellite-device> request virtual-chassis vc-port delete pic-slot 1 port 3
```

This step is required for the 40-Gbps QSFP+ interfaces that will be used as uplink interfaces in a Junos fusion topology. Built-in 40-Gbps QSFP+ interfaces on EX4300 switches are configured into VCPs by default, and the default settings are restored after the device is reset.

After this initial preparation, you can use one of three methods to convert your switches into satellite devices—autoconversion, manual conversion, or preconfiguration. See Configuring or Expanding a Junos fusion for enterprise for detailed configuration steps for each method.

Converting a Satellite Device to a Standalone Switch

If you need to convert a satellite device to a standalone device, you must install a new Junos OS software package on the satellite device and remove it from the Junos fusion topology. For more information, see Converting a Satellite Device to a Standalone Device.

Upgrade and Downgrade Support Policy for Junos OS Releases

We have two types of releases, EOL and EEOL:

- 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 thirty six months after the first general availability date and customer support for an additional six more months.

For both EOL and EEOL releases, you can upgrade to the next three subsequent releases or downgrade to the previous three releases. For example, you can upgrade from 20.4 to the next three releases – 21.1, 21.2 and 21.3 or downgrade to the previous three releases – 20.3, 20.2 and 20.1.

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. For example, 20.4 is an EEOL release. Hence, you can upgrade from 20.4 to the next two EEOL releases – 21.2 and 21.4 or downgrade to the previous two EEOL releases – 20.2 and 19.4.

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
End of Life (EOL)	24 months	End of Engineering + 6 months	Yes	No
Extended End of Life (EEOL)	36 months	End of Engineering + 6 months	Yes	Yes

For more information about 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.

Downgrading Junos OS

Junos fusion for enterprise is first supported in Junos OS Release 16.1, although you can downgrade a standalone EX9200 switch to earlier Junos OS releases.

> **NOTE**: You cannot downgrade more than three releases.
> For more information, see the Installation and Upgrade Guide.

To downgrade a Junos fusion for enterprise, follow the procedure for upgrading, but replace the `junos-install` package with one that corresponds to the appropriate release.

Junos OS Release Notes for Junos Fusion for Provider Edge

IN THIS SECTION

These release notes accompany Junos OS Release 22.3R2 for Junos Fusion for provider edge. They describe new and changed features, limitations, and known and resolved problems in the hardware and software.

You can also find these release notes on the Juniper Networks Junos OS Documentation webpage, located at https://www.juniper.net/documentation/product/en_US/junos-os.

What's New

There are no new features or enhancements to existing features in Junos OS Release 22.3R2 for Junos Fusion for Provider Edge.

What's Changed

There are no changes in behavior and syntax in Junos OS Release 22.3R2 for Junos Fusion for Provider Edge.

Known Limitations

There are no known limitations in hardware or software in this release for Junos fusion for provider edge.

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 Junos Fusion for provider edge.

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 Junos OS Release 22.3R2 for Junos Fusion for provider edge.

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 Junos fusion for provider edge. Upgrading or downgrading Junos OS might take several hours, depending on the size and configuration of the network.

Basic Procedure for Upgrading an Aggregation Device

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.

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. See the Installation and Upgrade Guide.

The download and installation process for Junos OS Release 22.3R2 is different from that for earlier Junos OS releases.

1. Using a Web browser, navigate to the Download Software URL on the Juniper Networks webpage:

   https://www.juniper.net/support/downloads/

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

3. Select **By Technology > Junos Platform > Junos fusion** to find the software that you want to download.

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 page.

5. Select the **Software** tab.

6. Select the software package for the release.

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 aggregation 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 commands.

    - For 64-bit software:

> **NOTE**: We recommend that you use 64-bit Junos OS software when implementing Junos fusion for provider edge.

```
user@host> request system software add validate reboot source/jinstall64-21.1R1.SPIN-domestic-signed.tgz
```

- For 32-bit software:

```
user@host> request system software add validate reboot source/jinstall-21.1R1.SPIN-domestic-signed.tgz
```

All other customers, use the following commands.

- For 64-bit software:

> **NOTE**: We recommend that you use 64-bit Junos OS software when implementing Junos fusion for provider edge.

```
user@host> request system software add validate reboot source/jinstall64-21.1R1.SPIN-export-signed.tgz
```

- For 32-bit software:

```
user@host> request system software add validate reboot source/jinstall-21.1R1.SPIN-export-signed.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* (available only for the Canada and U.S. version)

The `validate` option validates the software package against the current configuration as a prerequisite for adding the software package to ensure that the router reboots successfully. This is the default behavior when the software package being added is for a different release.

Adding the `reboot` command reboots 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: After you install a Junos OS Release 21.1R1 `jinstall` package, you cannot return to the previously installed software by issuing the `request system software rollback` command. Instead, you must issue the `request system software add validate` command and specify the `jinstall` package that corresponds to the previously installed software.

Upgrading an Aggregation Device with Redundant Routing Engines

If the aggregation device has two Routing Engines, perform a Junos OS installation on each Routing Engine separately as follows to minimize disrupting network operations:

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*.

Preparing the Switch for Satellite Device Conversion

Satellite devices in a Junos fusion topology use a satellite software package that is different from the standard Junos OS software package. Before you can install the satellite software package on a satellite device, you first need to upgrade the target satellite device to an interim Junos OS software version that

can be converted to satellite software. For satellite device hardware and software requirements, see Understanding Junos fusion Software and Hardware Requirements

NOTE: The following conditions must be met before a standalone switch that is running Junos OS Release 14.1X53-D43 can be converted to a satellite device when the action is initiated from the aggregation device:

- The switch can be converted to only SNOS 3.1 and later.
- Either the switch must be set to factory-default configuration by using the `request system zeroize` command, or the following command must be included in the configuration: `set chassis auto-satellite-conversion`.

Customers with EX4300 switches, use the following command:

```
user@host> request system software add validate reboot source/jinstall-ex-4300-14.1X53-D43.3-domestic-signed.tgz
```

Customers with QFX5100 switches, use the following command:

```
user@host> request system software add reboot source/jinstall-qfx-5-14.1X53-D43.3-domestic-signed.tgz
```

When the interim installation has completed and the switch is running a version of Junos and OS on one line that is compatible with satellite device conversion, perform the following steps:

1. Log in to the device by using the console port.
2. Clear the device:

```
[edit]
user@satellite-device# request system zeroize
```

NOTE: The device reboots to complete the procedure for resetting the device.

If you are not logged in to the device by using the console port connection, your connection to the device is lost after you enter the **request system zeroize** command.

If you lose your connection to the device, log in using the console port.

3. (EX4300 switches only) After the reboot is complete, convert the built-in 40-Gbps QSFP+ interfaces from Virtual Chassis ports (VCPs) into network ports:

```
user@satellite-device> request virtual-chassis vc-port delete pic-slot 1 port port-number
```

For example, to convert all four built-in 40-Gbps QSFP+ interfaces on an EX4300-24P switch into network ports:

```
user@satellite-device> request virtual-chassis vc-port delete pic-slot 1 port 0
user@satellite-device> request virtual-chassis vc-port delete pic-slot 1 port 1
user@satellite-device> request virtual-chassis vc-port delete pic-slot 1 port 2
user@satellite-device> request virtual-chassis vc-port delete pic-slot 1 port 3
```

This step is required for the 40-Gbps QSFP+ interfaces that will be used as uplink interfaces in a Junos fusion topology. Built-in 40-Gbps QSFP+ interfaces on EX4300 switches are configured into VCPs by default, and the default settings are restored after the device is reset.

After this initial preparation, you can use one of three methods to convert your switches into satellite devices—autoconversion, manual conversion, and preconfiguration. See Configuring Junos fusion for provider edge for detailed configuration steps for each method.

Converting a Satellite Device to a Standalone Device

If you need to convert a satellite device to a standalone device, you must install a new Junos OS software package on the satellite device and remove the satellite device from the Junos fusion topology.

NOTE: If the satellite device is a QFX5100 switch, you need to install a PXE version of Junos OS. The PXE version of Junos OS is software that includes *pxe* in the Junos OS package name when it is downloaded from the Software Center—for example, the PXE image for Junos OS Release 14.1X53-D43 is named install-media-pxe-qfx-5-14.1X53-D43.3-signed.tgz . If the satellite device is an EX4300 switch, you install a standard jinstall-ex-4300 version of Junos OS.

The following steps explain how to download software, remove the satellite device from Junos fusion, and install the Junos OS software image on the satellite device so that the device can operate as a standalone device.

1. Using a Web browser, navigate to the Junos OS software download URL on the Juniper Networks webpage:

https://www.juniper.net/support/downloads

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

3. Select **By Technology > Junos Platform > Junos fusion** from the drop-down list and select the switch platform series and model for your satellite device.

4. Select the Junos OS Release 14.1X53-D30 software image for your platform.

5. Review and accept the End User License Agreement.

6. Download the software to a local host.

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

8. Remove the satellite device from the automatic satellite conversion configuration.

   If automatic satellite conversion is enabled for the satellite device's member number, remove the member number from the automatic satellite conversion configuration. The satellite device's member number is the same as the FPC slot ID.

   ```
   [edit]
   user@aggregation-device# delete chassis satellite-management auto-satellite-conversion
   satellite member-number
   ```

   For example, to remove member number 101 from Junos fusion:

   ```
   [edit]
   user@aggregation-device# delete chassis satellite-management auto-satellite-conversion
   satellite 101
   ```

   You can check the automatic satellite conversion configuration by entering the `show` command at the `[edit chassis satellite-management auto-satellite-conversion]` hierarchy level.

9. Commit the configuration.

   To commit the configuration to both Routing Engines:

   ```
   [edit]
   user@aggregation-device# commit synchronize
   ```

Otherwise, commit the configuration to a single Routing Engine:

```
[edit]
user@aggregation-device# commit
```

10. Install the Junos OS software on the satellite device to convert the device to a standalone device.

```
[edit]
user@aggregation-device> request chassis satellite install URL-to-software-package fpc-slot
member-number
```

For example, to install a PXE software package stored in the **/var/tmp** directory on the aggregation device onto a QFX5100 switch acting as the satellite device using FPC slot 101:

```
[edit]
user@aggregation-device> request chassis satellite install /var/tmp/install-media-pxe-
qfx-5-14.1X53-D43.3-signed.tgz fpc-slot 101
```

For example, to install a software package stored in the **var/tmp** directory on the aggregation device onto an EX4300 switch acting as the satellite device using FPC slot 101:

```
[edit]
user@aggregation-device> request chassis satellite install /var/tmp/jinstall-
ex-4300-14.1X53-D30.3-domestic-signed.tgz fpc-slot 101
```

The satellite device stops participating in the Junos fusion topology after the software installation starts. The software upgrade starts after this command is entered.

11. Wait for the reboot that accompanies the software installation to complete.

12. When you are prompted to log back into your device, uncable the device from the Junos fusion topology. See Removing a Transceiver from a QFX Series Device or Remove a Transceiver, as needed. Your device has been removed from Junos fusion.

NOTE: The device uses a factory-default configuration after the Junos OS installation is complete.

Upgrading an Aggregation Device

When you upgrade an aggregation device to Junos OS Release 21.1R1, you must also upgrade your satellite device to Satellite Device Software version 3.1R1.

Upgrade and Downgrade Support Policy for Junos OS Releases

We have two types of releases, EOL and EEOL:

- 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 thirty six months after the first general availability date and customer support for an additional six more months.

For both EOL and EEOL releases, you can upgrade to the next three subsequent releases or downgrade to the previous three releases. For example, you can upgrade from 20.4 to the next three releases – 21.1, 21.2 and 21.3 or downgrade to the previous three releases – 20.3, 20.2 and 20.1.

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. For example, 20.4 is an EEOL release. Hence, you can upgrade from 20.4 to the next two EEOL releases – 21.2 and 21.4 or downgrade to the previous two EEOL releases – 20.2 and 19.4.

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
End of Life (EOL)	24 months	End of Engineering + 6 months	Yes	No
Extended End of Life (EEOL)	36 months	End of Engineering + 6 months	Yes	Yes

For more information about 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.

Downgrading from Junos OS Release 22.3

To downgrade from Release 22.3 to another supported release, follow the procedure for upgrading, but replace the 21.1 `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 MX Series

IN THIS SECTION

These release notes accompany Junos OS Release 22.3R2 for the MX Series. They describe new and changed features, limitations, and known and resolved problems in the hardware and software.

You can also find these release notes on the Juniper Networks Junos OS Documentation webpage, located at https://www.juniper.net/documentation/product/en_US/junos-os.

What's New

There are no new features or enhancements to existing features in this release for MX Series Routers.

What's Changed

IN THIS SECTION

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

Junos XML API and Scripting

- **The `file copy` command supports only text-formatted output in the CLI (ACX Series, EX Series, MX Series, PTX Series, QFX Series, SRX Series, vMX, and vSRX)**—The `file copy` command does not emit output when the operation is successful and supports only text-formatted output when an error occurs. The `file copy` command does not support using the `| display xml` filter or the `| display json` filter to display command output in XML or JSON format in any release. We've removed these options from the CLI.

Software Installation and Upgrade

- **New options for the `request system snapshot` command (ACX Series, EX Series, MX Series, PTX Series, QFX Series, and SRX Series)**—The `request system snapshot` command includes new options for non-recovery snapshots. You can include the `name` option to specify a user-defined name for the snapshot, and you can include the `configuration` or `no-configuration` option to include or exclude configuration files in the snapshot. By default, the snapshot saves the configuration files, which include the contents of the **/config** and **/var** directories and certain SSH files.

  [See request system snapshot (Junos OS with Upgraded FreeBSD).]

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

- In a scaled setup with LDP over RSVP configuration and maximum-ecmp as 32 or 64, line card CPU usage can remain high for extended duration on link flap operation. In this duration, LACP might take 5+ minutes to converge and the AE bundle to be active. PR1624219
- On SRX4600 platform, the CPU may overrun while performing sanity check due to incompatibility issues between ukern scheduler and Linux driver which might lead to traffic loss.PR1641517
- For GNMI subscriptions, Packet Forwarding Engine does not support filtering in subscription paths. So data is streamed from Packet Forwarding Engine ignoring filtering. PR1668911
- RE-S-X6-128G-K does not support enabling encryption with GRES. You must enable encryption on each Routing Engine. PR1676928
- MVRP on PVLAN promiscuous port is not supported. If MVRP is configured on promiscuous port, then hosts connected to secondary VLAN ports will not be able to reach external world through promiscuous port carrying primary VLAN tags. PR1693345

Infrastructure

- When upgrading from releases earlier to Junos OS Release 21.2 and later, validation and upgrade might fail. The upgrading requires using of `no-validate` configuration statement.PR1568757
- Below IPC timeouts logs can be seen for statistics query to kernel (queried from CLI or daemons querying internally) when there is configuration churn, or large number of IPCs getting exchanged between kernel and Packet Forwarding Engine in the system. if_pfe_msg_handler: pfe_peer_msg_handler error: error for msg type type, msg subtype subtype, opcode op and peer index *index*. Default IPC timeout value in kernel for IPC statistics request is 10s. This can be incremented to a larger value by setting below the hidden configuration to avoid IPC timeout errors. `set system stats-timeout-lifetime 15` and `commit`. PR1629930

MPLS

- With local reversion ON, there is a possibility of transit router not informing headend of RSVP disabled link when link is flapped more than once. Work around is to remove local-reversion configuration. PR1576979

Network Management and Monitoring

- Junos OS might translate the custom YANG configuration even after disabling the custom YANG package. PR1599107

Platform and Infrastructure

- In some scenarios with MPC, major alarm and following messages are generated. This major error is triggered due to parity error, and the impacted queue might drop packets. This might impact the forwarding, to recover MPC card need to be rebooted. PR1303489
- On MX Series and EX9200 Seriesl platforms, under Ethernet VPN (EVPN) environment, packets routed using IRB interface could not be fragmented due to media maximum transmission unit (MTU) problem. PR1522896
- After a switchover event, when ppmd calls sendmsg system call to transmit the protocol packets, it gets blocked long enough that a few sendmsg calls cumulatively take up around 7 to 8 seconds. This

indirectly impacts the BFD session because the BFD session has a Routing Engine-based detect time of 7.5 seconds to expire. PR1600684

Routing Protocols

- When `routing-options transport-class fallback none` is not configured - do not configure more than 10 transport-classes. Or advertise more than 10 distinct colors in SR-TE or FlexAlgo. PR1648490

Services Applications

- Subscriber sessions on the LNS that send an ICRQ that includes RFC5515 AVPs might fail to establish a session. The client will receive a CDN error "receive-icrq-avp-missing-random-vector" in response. PR1493289

User Interface and Configuration

- On all Junos OS and Junos OS Evolved platforms configured with persist-group-inheritance, which is enabled by default from Junos OS Release 19.4R3 and later, might lead to mustd process crash in highly scaled configuration. PR1638847

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

- In Provider Backbone Bridging - Ethernet VPN (PBB-EVPN) environment, ARP suppression feature which is not supported by PBB might be enabled unexpectedly. This could cause MAC addresses of remote CEs not to be learned and hence traffic loss. PR1529940
- On all Junos OS and Junos OS Evolved platforms that support Type-2 (T-2) Integrated Routing and Bridging (IRB) symmetric routing, EVPN virtual extensible LAN symmetric type-2 route needs to be imported in L2 mac-vrf instance for IP host route to be added in Layer 3 vrf. Layer3 inter-subnet routing will fail if there is no reachability for the remote IP-host route.PR1669585
- On all platforms, MAC-IP route deletion and addition are triggered when Address Resolution Protocol (ARP) on multihoming device fails in the EVPN-MPLS multihoming scenario resulting in traffic drop. PR1691132

Forwarding and Sampling

- On all Junos OS dual-Routing Engine platforms, when activating and deactivating GRES multiple times, you will observe synchronization issues between the primary and backup dfwd process. PR1697959

General Routing

- If a vmhost snapshot is taken on an alternate disk and there is no further vmhost software image upgrade, the expectation is that if the current vmhost image gets corrupted, the system boots with the alternate disk so the user can recover the primary disk to restore the state. However, the host root file system and the node boots with the previous vmhost software instead of the alternate disk. PR1281554
- When VLAN is added as an action for changing the VLAN in both ingress and egress filters, the filter is not installed. PR1362609
- FPC crash on MX240 and MX2020 routers or Packet Forwarding Engine crash on MX104 routers might happen when the MIC-3D-8OC3-2OC12-ATM is installed and ATM interface is configured. PR1453893
- VXLAN VNI (multicast learning) scaling on QFX5110 traffic issue is seen from VXLAN tunnel to Layer 2 interface. PR1462548
- When there are HW link errors occurred on all 32 links on an FPC 11. Because of these link errors, all FPCs reported destination errors towards FPC 11 and FPC 11 was taken offline with reason "offlined due to unreachable destinations". PR1483529
- runt, fragment and jabber counters are not incrementing on EX4300-MPsPR1492605
- After backup Routing Engine halt, CB1 goes offline and comes back online; this leads to the backup Routing Engine booting up, and it shows the reboot reason as "0x1:power cycle/failure." This issue is only for the RE reboot reason, and there is no other functional impact of this. PR1497592
- * When an AMS ifd is configured for the first time or any member of the AMS bundle is removed or added, the PICs on which the members of AMS bundle are present go for a reboot. * There is a timer running in the AMS kernel which is used as a delay for the PIC reboot to complete and once that timer expires AMS assumes that the PICs might have been rebooted and it moves into next step of AMS fsm. * In scaled scenarios, this rebooting of the PIC is delayed due to DCD. This is because when a PIC goes down, DCD is supposed to delete the IFDs on that PIC and then the PIC reboot happens. * But DCD is busy processing the scaled config and the IFD deletion is delayed. This delay is much greater than the timer running in AMS kernel. * When the above timer expires, the FSM in AMS kernel wrongly assumes the PIC reboot would be completed by then, but the reboot is still pending. * By the time DCD deletes this IFD the AMS bundles are already UP. Because of this, there is a momentary flap of the bundles. PR1521929
- In Mac-OS platforms when Juniper Secure Connect client connects successfully, the client is not getting minimized to tray icon and needs to be minimized manually.PR1525889
- IPSec rekey fails when SRX is configured with kilobyte based lifetime in remote access solution. PR1527384

- Due to BRCM KBP issue route lookup may fail. Need to upgrade KBP to address this issue, Due to high risk KBP SDK upgrade planned for 21.1. PR1533513
- In scaled mx2020 router, with vrf localisation enabled, 4 million nexthop scale, 800k route scale. FPCs may go offline on GRES. Post GRES, router continues to report many fabric related CM_ALARMs. FPC may continue to reboot and not come online. Rebooting master and backup RE will help recover and get router back into stable state. PR1539305
- Unsupported config is being attempted by the script that then hits the maximum threshold for the given platform PTX5000PR1555159
- 5M DAC that connects QFX10002-60C and MX2010 doesn't link up. But with 1M and 3M DAC this interoperability works as expected. Also, on QFX10002-60C and ACX Series devices or on traffic generator, the same 5M DAC works seamlessly. Need to debug certain SI or link level configuration on both QFX10002-60C and MX2010 with the help from the hardware and SI teams and resolved. PR1555955
- With IPsec PMI or fat-core enabled, the CLI `show services sessions utilization` do not display the appropriate CPU utilization. PR1557751
- The Sync-E to PTP transient simulated by Calnex Paragon Test equipment is not real network scenario. In real network deployment model typically there will be two Sync-E sources (primary and secondary) and switchover occurs from one source to another source. MPCE7 would pass real network SyncE switchover and associated transient mask. PR1557999
- VE and CE mesh groups are default mesh groups created for a given routing instance. On vlan/bridge-domain add, flood tokens and routes are created for both VE and CE mesh-group/flood-group. Ideally, VE mesh-group does not require on a CE router where IGMP is enabled on CE interfaces. Trinity based CE boxes have unlimited capacity of tokens, so this would not be a major issue. PR1560588
- This is a feature enhancement and work is in progress to provide this support. This will have impact only when routing daemon crashes and will not have impact on rest of the NSR support. PR1561059
- 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
- To avoid the additional interface flap , interface hold time needs to be configured . PR1562857
- Service MIC does not work on ACX500 running Junos 20.4 or higher. PR1569103
- On PTX platforms, when Inline Jflow is configured and high sampling rate (more than 4000 per second) is set, high CPU utilization may be observed and this might result in relevant impacts on traffic analysis and billing. This issue is fixed from 21.3R1 via RLI 49464.PR1569229

- On QFX5100, Media type for SFP+-10G-CU1M and SFP-T cables are shown as Fiber. This is only a display issue and no functionality impact is observed.PR1570555
- This issue is caused by /8 pool with block size as 1, when the config is committed the block creation utilizes more memory causing NAT pool memory shortage which is currently being notified to customer with syslog tagged RT_NAT_POOL_MEMORY_SHORTAGE. PR1579627
- On MX platforms the JDM (Juniper Device Manager) server could not be created in in-chassis mode of junos node slicing, which results in mgd process crash and affects GNF's (Guest Network Function) provisioning. PR1583324
- When the active slave interface is deactivated, the PTP lock status is set to 'INITIALIZING' state in 'show ptp lock-status' output for few seconds before BMCA chooses the next best slave interface. This is the day-1 behavior and there is no functional impact. PR1585529
- On all devices running Junos 19.1R3-S5-J3, the subscriber IFL(logical interface) may be in a stuck state after the ESSM (Extensible Subscriber Services Manager) deletion. PR1591603
- On QFX5110 VC, FPC may gets disconnected with 24K DHCPv6 relay scaling, after the traffic is stopped. "pfe_listener_disconnect" error messages may be seen.PR1594748
- Pim Vxlan not working on TD3 chipsets enabling VxLAN flexflow after release 21.3R1. Customers Pim Vxlan or data plane VxLAN can use the Junos OS Release 21.3R1. PR1597276
- MX2010, MX2020: MPC11E: ISSU is not supported for software upgrades from 21.2 to 21.3 and 21.4 releases due to a flag day change PR1597728
- During RE switchover, if there is a burst of ICMP/BFD/SSH/FTP/TELNET/RSVP packets (~18K pps) you might see new backup RE restarting. PR1604299
- On MX-VC (Virtual Chassis) platforms with MS-MPC or SPC3 service cards and AMS(Aggregated Multi-Service), traffic on the line card in the backup chassis may not be load-balanced properly due to timing conditions. This works well on the line card in the master chassis. There might be traffic loss when interfaces are not properly balanced.PR1605284
- On all MX Series platforms, in a subscriber management environment, new subscribers might not connect if Class of service (CoS) CR-features (Classifier Rewrite) are used by the VBF (Variable Based Flow) service. The reference count mismatching between RE (Routing Engine) and VBF is caused by VBF flow VAR CHANGE failure. PR1607056
- When user tries to disable AMS ifd using config knob, the ipsec tunnels are not deleted. Deactivating the services will provide the desired result. PR1613432
- In some NAPT44 and NAT64 scenarios, Duplicate SESSION_CLOSE Syslog will be seen. PR1614358
- On all Junos platforms the MAC address of the 17th ae interface might be changed after the upgrade from 18.4+ to 20.4+ releases. It will lead to mac based service interruption.PR1629050

- For a topology with VSTP and VRRP configured and IPV6 traffic, if VSTP bridge priority is changed a couple of times (to trigger toggling of root bridge), it is possible that V6 traffic drop is seen on some of the streams. PR1629345
- For ACX5448, MX204 and MX2008 "VM Host-based" platforms, starting with Junos 21.4R1 or later, ssh and root login is required for copying line card image (chspmb.elf for MX2008) from Junos VM to Linux host during installation. The ssh and root login are required during installation. Use "deny-password" instead of "deny" as default root-login option under ssh config to allow internal trusted communication. Ref https://kb.juniper.net/TSB18224 PR1629943
- On MX platform with enhanced subscriber management enabled, when "host-prefix-only" is configured on the underlying-interface for subscribers, it might not work in FPC. PR1631646
- The fabric statistics counters are not displayed in the output of "show snmp mib walk ascii jnxFabricMib". PR1634372
- On all devices running Junos OS or Junos OS Evolved, where this is a high BGP scale with flapping route and the BGP Monitoring Protocol (BMP) collector/station is very slow, the rpd process might crash due to memory pressure.PR1635143
- Source MAC should nt be configured on the underlying static interface on the UP for PPPoE login to work correctly.PR1641495
- WIth PTPoIPv6 on MPC2E 3D EQ, PTP slave stays in acquiring state.PR1642890
- When CFP2-DCO is used, operator need to configure otn-option - that is the only mode supported PR1643815
- On MX10004, MX10008, and MX10016 platforms, oamd process do not start and GRE keepalives adjacency goes down. PR1644480
- Committing configuration changes during the Packet Forwarding Engine reset pause window (when Packet Forwarding Engine is disabled, yet the Packet Forwarding Engine reset proper has not started yet) has the potential of causing errors and traffic loss. In particular, config changes that result in re-allocating policers (which are HMC-based) might lead to traffic being entirely policed out (i.e. not flowing). Once the Packet Forwarding Engine reset procedure has started config changes ought to be avoided until the procedure is completely done.PR1644661
- bb device has to be manually enabled in configuration for DHCP and PPP access models for BNG CUPS. Configuration to enable bb device is as follows:: #set system subscriber-management mode force-broadband-devicePR1645075
- When per-interface egress and per-sid egress SR sensor stats are configured using the CLI commands below, the (pushed) MPLS label length does not get included in the output/Tx octets field that gets exported from the sensor. set protocols isis source-packet-routing sensor-based-stats per-interface-

per-member-link egress set protocols isis source-packet-routing sensor-based-stats per-sid egress This is a day-1 behavior on all Trio ASIC based FPCs on the MX platform.PR1646799

- With overlapping NAT pool configured with different NAT rules under different service sets, when service outside interface is moved between different routing instances (EX: from vr1 to default, and from default to vr1), NAT routes corresponding to the service-set in default routing instance are getting deleted, resulting in reverse path traffic failure for NAT sessions. PR1646822
- In the IPv6 segment routing deployment, packets are sent out with the wrong ethernet type. PR1647622
- Core file is generated intermittently where random grpc stack crashes. The license service will auto restart and recover. PR1656975
- ZTP: DHCPACK is not received at ztp-server after zeroizing the client device. PR1658287
- On Junos OS platforms, in the VPLS environment configuring the CLI `routing-options resolution preserve-nexthop-hierarchy` results in the packet drop at the egress PE device for multiple MPLS stack labels.PR1658406
- The OpenSSL project has published security advisories for multiple vulnerabilities resolved in OpenSSL. Please Refer to JSA70186 for more information. PR1661450
- The version details for certain daemons will appear in the command output after the device has been rebooted after the completion of the USB installation of Junos OS.PR1662691
- Not all MAC addresses are learnt for some VPLS instances after `clear vpls mac-table` command is executed. PR1664694
- Egress PE device rpd core file at ctx_module_config (ctx=0x2dbb914 < task_args>, errmsg=0xffffc764 "Module 0x2d753e0 Name BGP Failed in Config Pass 2, LSYS=default", elen=2048) at ../../../../../../../src/layer3/usr.sbin/rpd/lib/ctx/app_ctx_module.c:115.PR1667320
- On MX Series platforms with MIC-MACsec-20GE, Forwarding Engine Board (FEB) might go down while activating and deactivating GRES configuration.PR1668983
- License-check core file is generated upon reloading the system after applying specific set of configurations. No issues will be seen when the system comes up. PR1671419
- In the case of an active-active lease query stale-timer configuration is mandatory. This is required to optimize the synchronization time, as both peers get the solicit packets at the same time. As a workaround, the `set forwarding-options dhcp-relay stale-timer 20` configuration statement can be used. PR1671589
- Sometimes core file is generated on the backup Routing Engine during init after a reboot. When the backup Rounting Engine initializes and the system is busy, some commands executed in context of spmbpfe takes more time to complete due to the initial heavy lifting by the kernel. In this stage, if in

case the commands from spmbpfe process do not complete in 2.5 seconds, then there are chances of generating spmbpfe core files. This is a temporary issue seen on the backup Routing Engine during init time. This might not impact because if in case spmbpfe process crashes due to this, it might restart by itself and continue to init and run once the initial high CPU condition has passed. It should not cause any functionality or performance impact; especially since it is reported only on the backup Routing Engine. PR1675268

- On SyncE over LAG interfaces, if the end points have different ESMC QL configured, on one of configured syncE interface, ESMC QL is toggling between PRC and DNU and sync-E does not lock and moves to holdover state. PR1677131
- The physical interface remaining statistics flag is not set properly in chassid in today's code. It should be set to TRUE only if HCOS is configured on an interface. Else, it should not be SET. Not setting this rightly, results in statistics not being displayed OR the command output not being displayed at all. The impacted command is `run show interfaces extensive intf-name` and the impact is seen in GNF environment with no explicit CoS configuration on the interfaces. Not using "extensive" will ensure there is no issue as well. This is specific to MPC11 with sub LC (GNF) setup.PR1678071
- 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
- Observing FPC MQSS WAN reorder timeout errors after the device reboots. PR1681763
- If MVRP is enabled on an MSTP enabled interface, the interface will be made part of all the existing instances on the switch. PR1686596
- On Junos OS platforms, error messages are seen with traffic drops on the labelled route present in mpls.0 resolving over an IPv6 prefix. PR1698516
- On MX Series platforms, traffic egressing on the integrated routing and bridging (IRB) interface with the underlying Layer 2 access port that has VLAN tags imposed incorrectly.PR1700321
- Identify and report fabric link errors caused due to connector related issues.PR1700983
- When subscribing to sensor paths "/junos/system/linecard/packet/usage/", "/junos/services/label-switched-path/usage/" or other line card (PFE) sensor paths in gNMI subscription mode, packet drops may be seen in the CLI command "show network-agent statistics gnmi detail" output. The collector output may also contain missing sequence numbers. For example, the sequence number output may be 0, 3, 6, 9, 12, etc. instead of 0, 1, 2, 3, 4, etc. PR1703418
- In Chassisd, Jvision thread takes more time in streaming of jvision packets because of volume of data and number of sensors involved with this daemon. Jvision thread engaged for more time to process streaming events caused Chassisd master thread to lose receive/send keepalive messages to/from other RE, which eventually was causing automatic RE switchover in most of the cases. To avoid this, fix done for exporting small payload jvision packets (formation of which takes less time) and deferring jvision thread more in an interval, to allow chassisd master thread to process high-priority hello/

keep-alive messages. This means now, more number of packets is sent in one reporting interval and with larger spread (earlier same amount of data was sent with 2 or 3 packets of higher payload size, and 100ms of deferring time for jvision thread. This behaviour is increasing KPI-2 but lowering KPI-1 (payload size). It is not possible to back out changes done to solve keep-alive message loss issue. Hence we will have to keep Chassisd as an exception, when we measure/report KPI-2 values. Jvision in Chassisd has to give more priority/time to process keep-alive messages than sending of jvision packets. Hence delay between jvision packets are more.PR1706300

- When "routing-service" is enabled for a PPPoE Subscriber over AE, the subscriber will not have network access due to traffic drops.PR1706446
- In a Virtual-chassis (VC) scenario on Junos MX platforms installed with MPC7E Flexible PIC Concentrators (FPC), if the inline-jflow Sampling is enabled, the Inline Flow Monitoring is not working as data is not getting exported to the collector.PR1708485
- When you upgrade to new Junos OS release and apply the configuration, the rpd might create parallel MBBs due to this number of nexthops might increase and on-chip memory exhaustion might happen at FPC. This can lead to FPC crash. Issue should not be seen once system settles down. PR1710362
- When subscribing to sensor paths "/junos/system/linecard/packet/usage/" in gNMI subscription mode, packet drops ((gNMI translator lookup failures)) may be seen in the CLI command "show network-agent statistics gnmi detail" output for empty dummy packets (packets which do not have a prefix or key-value data). The collector output may also contain missing sequence numbers. For example, the sequence number output may be 0, 3, 6, 9, 12, etc. instead of 0, 1, 2, 3, 4, etc.PR1711779
- The packets are being dropped when they come from the VC (Virtual Chassis) link into member in the MX Virtual Chassis with MPC10 line card.PR1712790

High Availability (HA) and Resiliency

- After GRES with disabled em0 (or fxp0), the subnet assigned to em0 (or fxp0) remains down on the new backup, even after the interface is re-enabled. PR1372087

Interfaces and Chassis

- Logical interface packet counters are not implemented for AMS interface. It is a new change. Changes are planned for next release 22.4R2PR1673337

- When the MPC10 and MPC11 FPCs restart, error logs related to invalid anchor next hops are seen with distributed aggregated Ethernet IRB VRRP sessions. The aggregated Ethernet interfaces must span multiple FPCs. PR1674069
- With IXIA connection, we do not receive an ARP response in the DUT port to store the destination MAC address. Unable to determine the ARP response if the issue is with the MX Series port or medium or IXIA port. PR1677624
- On MX Series platforms, in a rare scenario, Flexible PIC Concentrator or Sub Line Card (FPC/SLC) might get stuck in the ready state after restarting. You will observe a syslog error message 'Device busy'. PR1682271
- This issue is specific to MX Series Virtual Chassis and the issue is not seen during manual execution of the test case. Issue is seen only with the test script that too rarely and hence the exact trigger of the issue. is not clear.PR1686425
- On all Junos platforms, while performing an upgrade from prior to Junos OS Release 20.4 and later with an incorrect configuration may fail. This issue may lead to traffic loss or network outages.PR1692404
- On Junos OS MX Series Virtual Chassis, Chassis Control Link (CCL), and Cyclic Redundancy Check (CRC) errors can be seen after Flexible PIC Concentrator (FPC) detach during the sequential operating system upgrade of MX-VC system. The CCL and CRC errors are expected after the FPC detaches and eventually, the FPC is marked offline by the MX-VC and there is an unexpected chassisd process restart. The chassisd restarted because of the connection failure between Linecard Chassis Control (LCC) chassisd and Switch Chassis Control (SCC) chassisd which is triggered by the sequence of messages exchanged between the LCC and SCC after the FPC detach event. There will be a traffic impact as the FPC will be offline, and the system recovers to a working state by itself. PR1706268
- MPC7E firmware upgrade in MX Series Virtual Chassis cannot be completed.PR1713502

Junos XML API and Scripting

- L2TP LAC functionality do not work in this release. PR1642991

Layer 2 Features

- In case of the access-side interfaces used as SP-style interfaces, when a new logical interface is added and if there is already a logical interface on the physical interface, there is 20-50 ms traffic drop on the existing logical interface. PR1367488

MPLS

- In MVPN case, if the nexthop index of a group is not same between master and backup after a nsr switchover, we might see a packet loss of 250 to 400 ms. PR1561287
- Ingress will retry after LSP stay down for extended period of time or customer can clear LSP to speed up the retry. PR1631774
- On all Junos OS and Junos OS Evolved platforms, if Circuit Cross-Connect (CCC) is configured to use a label-switched path such as IGP routed, that is, no-cspf and no strict explicit route object (ERO) configuration, then restarting egress CCC node or restarting FPC on the egress CCC node containing remote-interface-switch configuration multiple times might cause CCC to remain stuck in remote-if-down state, resulting in loss of traffic. The statement `remote-interface-switch` is configured on the egress LER of the Resource Reservation Protocol-Traffic Engineering label-switched path (RSVP-TE LSP) which binds the LSP terminating on the node to a local interface. PR1694777
- When an LSR acts as a Point of Local Repair (PLR) as well as a Merge Point (MP) for an LSP during a double failure scenario, the LSR incorrectly originates one or two PathErr messages with RoutingProblem (code=24/2) instead of originating PathErr with NotifyError (code/subcode=25/3). This will not cause any service impact if the ingress LER would not react adversely to RoutingProblem error (code=24/2).PR1713392

Network Management and Monitoring

- When `maximum-password-length` is configured and user tries to configure password whose length exceeds configured maximum-password-length, error is thrown, along with error 'ok' tag is also emitted. The configuration do not get committed. PR1585855

Platform and Infrastructure

- On all Junos OS and Junos OS Evolved platforms, while using source-address NTP configuration parameter and issue the command `set ntp date` from the CLI, packets will be sent with the source address of the outgoing interface rather than the manually configured IP address. Typically, the manually configured IP address will be a loopback address. The problem does not apply to automatically generate the NTP poll packets. PR1545022
- When the `deactivate services rpm` and `deactivate routing-options rpm-tracking` configuration statement are applied together and then committed, some of the rpm tracked added routes are not deleted from the routing table. Issue cannot be seen using the following steps.

  1. deactivate routing-options rpm-tracking
  2. commit the configuration then all the rpm tracked routes will be deleted. If the RPM service needs to be deactivated,
  3. deactivate services rpm
  4. commit

  PR1597190
- With given multi dimensional scale, if configuration is removed and restored continuously for more than 24 times, MX Series FPC might crash and restart. During the reboot, there can be traffic impact if backup paths are not configured. PR1636758

Routing Protocols

- On all platforms, the issue is when the first time when ESIS is coming up sometimes the ESIS route might not get installed. PR1559005
- When l2cpd (in the context of xSTP) clears the entries that it has programmed on ppmd, that is, when you delete xSTP configurations from the box, there is a possibility of generating a ppmd core file. If ppmd is in distributed mode then there will be no service impact, else there can be a service impact as packet transmission for various protocols will happen via if ppmd is in centralized mode.PR1660299
- On all Junos OS and Junos OS Evolved platforms, whenever there is high percentage of background CPU usage that causes the rpd to run at average CPU load. BGP convergence will be slow, which results in traffic loss. PR1663883

- Any platforms with micro BFD configured on member links of the LAG and aggregated Ethernet interface, BFD Session state in Routing Engine remains as UP always even though PEER device has ceased. PR1675921

- On all Junos OS and Junos OS Evolved platforms, the rpd crashes when protocol independent multicast (PIM), multicast only fast reroute (MoFRR) configuration is present and some network churn event such as continuous interface cost changes, resulting in a change of active and backup paths for ECMP occurs. There will be service impact because of the rpd crash but the system self-recovers until the next crash. PR1676154

- Junos OS Release 22.3 and later, IS-IS yang is uplifted to 1.0.0 version which has major change in existing OC path that was supported earlier. Since OC path has change, same need to be reflected in translation script which is not done. As part of D27 release for cloud, translation script will be modified with newer OC path. Until then, older OC configuration is broken. eventually D27 code will come back to DCB and things will work fine after that.PR1686751

- On all Junos OS and Junos OS Evolved platforms BGP Labeled-Unicast (BGP-LU) advertisements fail with the message "BGP label allocation failure: Need a gateway" based on timing conditions involving route resolution and installation.PR1689904

- On Junos OS platforms, if a BGP peer is going down and stays down and the system might take an extremely long time to complete removing the BGP routes. The issue observed when a BGP peer sends many routes, only a small amount of routes are selected as the active routes in the RIB (Routing Information Base), and if the BGP delete job gets only a small part of the CPU time as the CPU shards with other work in the routing process.PR1695062

- This issue is seen with only evo and not seen Junos. Its seen in a combination of Rsvp and ISIS. Stats is getting incremented PR1700063

- On all Junos OS and Junos OS Evolved platforms, when an IPv4 prefix advertisement received by an IS-IS/OSPF router in the Extended IP reachability TLV and SR mapping server (SRMS) advertisement for the same prefix received through the segment identifier (SID) label Binding TLV, then SRMS advertised label preferred over IS-IS/OSPF SID label advertised via opaque-AS extended-prefix. Traffic will be sent via wrong path due to this issue.PR1702456

- On all Junos OS and Junos OS Evolved platforms, the mcsnoopd process crashes. This issue is seen when the devices support the VLAN (Virtual Local Area Network) style of internet group messaging protocol (IGMP) `igmp-snooping` configuration `set protocols igmp-snooping vlan` *`vlan_name`* and the VLAN name begins with the word all and has certain other characters. The workaround is not to enable the snooping for such VLANs.PR1711153

- When routing information base (RIB) 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

Services Applications

- When a configured tunnel interface is changed to another one, flow-tap-lite functionality stops working that is, packets do not get mirrored to content destination. But, this problem isn't consistently seen. PR1660588

VPNs

- Tunnel debugging configuration is not synchronized to the backup node. It needs to be configured again after RG0 failover. PR1450393
- Change here is basically reverting to old enum value used for ATM VPN, and using a new value for BGP multicast address family, and although these is no visible behavior change due to this, there may be impact on ISSU for ATMVPN and BGP multicast address family if enabled.PR1590331
- When using group VPN, in certain cases, the PUSH ACK message from the group member to the group key server may be lost. The group member can still send rekey requests for the TEK SAs before the hard lifetime expiry. Only if the key server sends any new PUSH messages to the group members, those updates would not be received by the group member since the key server would have removed the member from registered members list.PR1608290

Resolved Issues

IN THIS SECTION

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

Class of Service (CoS)

- QoS may not work as expected on aggregated Ehernet interfaces with explicit-null label. PR1675781
- The congestion details will be lost as ECN bits in DSCP are cleared after VXLAN decapsulation. PR1683438
- The oid tree jnxCosQstatEntry returns nothing for some interfaces after restarting class-of-service. PR1693977
- The aggregated Ethernet interface link flaps on MX Series platforms with MPC10, MPC11, and LC9600 when high or medium priorities are configured on the queue. PR1699714

EVPN

- The kernel crash would be observed in an EVPN multi-homed scenario. PR1649234
- In EVPN-MPLS Mutihoming scenario DF election will get stuck in the Preference based state. PR1662954
- CRB EVPN MPLS is not working with control-word enabled. PR1665130
- Traffic drop might be observed in the EVPN-VPWS scenario. PR1672749
- The ARP/ND entries are not relearnt as expected on the spine with EVPN-VxLAN. PR1677521
- EVPN Proxy ARP does not work for the static VTEP interface. PR1679115

- EVPN MPLS traffic drop can be observed in a multi-vendor PE CE setup with single-active LAG. PR1680421
- Routing Protocol Daemon (RPD) core file is observed due to remote BGP routes being flashed as active routes. PR1692249
- IPv4/IPv6 ping from PE (IRB interface) to CE works only when extended-vlan-list is configured for the specific Vlan PR1702016

Flow-based and Packet-based Processing

- In SD-WAN the association between VRF instance and VRF group fails for ISSU from Junos OS Release 19.2~21.1 to Junos OS Release 22.2R1. PR1661935
- The rpd crash will be observed when any commit is performed. PR1701146

Forwarding and Sampling

- Traffic loss may be observed when changing firewall configuration. PR1670622
- The FPC crashes when "show filter memory" command is used during a firewall filter configuration change. PR1680849

General Routing

- FPC might generate a core file if CFM flap trap monitor feature in use. PR1536417
- Error message seen in clksyncd logs with SyncEor PTP configurations "ESYNC-Error:ferrari_zl30362_reg_write: Error, EEC(0) not yet initialized". PR1583496
- On MX2008 routers, Junos OS vmcore process fail and generates core files with less partition. PR1604755
- On backup Routing Engine during GRES, you may see "RPD_KRT_KERNEL_BAD_ROUTE: krt unsolic client.128.0.0.5+62000: lost ifl 0 for route" warning messages. PR1612487
- The L3 packets with the destination as IPv6 Link Local address will not work. PR1638642
- PTP does not lock in certain scenario. PR1645562

- System does not get to shell prompt and hangs before rebooting after pressing N during PXE installation. PR1647534
- The aggregated Ethernet interface speed is not reflected correctly in certain scenarios on Junos OS platforms. PR1649958
- MX960:: Syslog errors HALP-trinity_vbf_flow_unbind_handler:1107: vbf flow 624626: ifl 526 not found,fpc5 vbf_var_get_ifs:754: ifl not found,PFE_ERROR_NOT_FOUND seen frequently on MPC7E in 5.5K DCIP/10kPPPoE FTTB Stress Test. PR1650598
- SyncE clock goes to holdover when interface flaps in sequence. PR1654008
- The 1G port always stays down while changing of 10G interface lane speed to 1G. PR1655089
- UEFI BIOS key synchronization tool - efitools.service failed after optics diagnostics test. PR1655537
- Telemetry is reporting In-Errors when `ignore-l3-incompletes` statement is configured. PR1655651
- On Junos OS MX Series with SPC3, when an inconsistent NAT configuration exists and a specific CLI command is issued, the SPC will reboot (CVE-2023-22409). PR1656798
- DHCP packets might get looped in a VXLAN setup. PR1657597
- Speed change from 10G to 1G on MX Series routers causes all other lanes to flap. PR1659087
- JSD crash is seen during cBNG container startup. PR1659175
- Some of ports on MX Series platforms with MPC7E-10G do not come up with 1G speed. PR1660154
- MX204 - SSH non-default port configuration causes FPC offline after upgrading to Junos OS Release 21.4. PR1660446
- The port LEDs do not light up when 40G physical interfaces are up. PR1660532
- No streaming data received for /telemetry-system/subscriptions/dynamic-subscriptions/ PR1661106
- Traffic loss might be seen in certain IPsec VPN and Group-VPN scenario. PR1661815
- In the EVPN-VXLAN scenario, the DHCP packets will get dropped when the DHCP relay agent is configured. PR1662524
- The rpd core file may be seen when there is a synchronization issue. PR1663050
- The command `show chassis fpc` shows inaccurate information about heap memory. PR1664448
- SPC3: Receive [Rx] queue of direct memory access might be stuck which might cause issues in packet processing. PR1664517

- RE1 alarms persistent even after removed from slot. PR1664544
- Switch fabric board information for supporting PTP on MX10k8 with MX10K-LC2101 LC(s). PR1664569
- Traffic loss is observed when you configure VRRP over the aggregated Ethernet interface. PR1666853
- H-VPLS traffic silently drops when you disable the mesh group local-switching. PR1667310
- The FPC might fail to initialize on Junos OS platforms. PR1667674
- The RSVP interfaces are not streamed when removing the interface configuration. PR1667844
- GRPC Server not decoding leaf-list correctly. PR1668319
- Type-5 routes might not get programmed in Packet Forwarding Engine when the number of active interfaces and VLAN configured is high. PR1668352
- Kernel logs on cRPD containers running on the same host are incomplete. PR1668794
- The rpd process restarts after generating a core file. PR1669346
- jsd memory leak and may lead jsd restart. PR1669426
- The error will be observed if eTree is used with EVPN-MPLS and the routing-instance is changed. PR1669609
- Interoperability issue between legacy line cards and MPC10E and MPC11E causes L2 packet drop. PR1669765
- USB installation package loads with 32-bit smartd binary version. PR1669892
- Multibit ECC error causes the whole MX Series platform chassis to go down. PR1670137
- EVPN multicast traffic may get impacted because of routes getting stuck in the kernel routing table (krt) queue. PR1670435
- PTP server state stuck in acquiring state when configured on a port enabled with Ingress Queueing Feature. PR1671262
- Traffic loss seen due to SPC3's packets getting stuck. PR1671649
- Reporting-interval in "show jvision sensor info" is stuck at 65000 when configured reporting rate is changed from 65000 to 68000. PR1673476
- SNMP traps "Power Supply failed" and "Power Supply OK" are not generated. PR1674322
- The 'kmd' process may crash due to SA re-negotiation failure during IKE phase-1. PR1674585

- In a rare case, 'pccd' will crash when the PCEP connection is down. PR1675816
- Packet Forwarding Engine core file is seen when the CPCD service is modified. PR1675985
- MX-SPC3 PIC core file is seen when a CPCD service is modified. PR1675990
- MPC stuck in present state with log " graceful offline in progress, returning false" flooding. PR1676008
- While processing SNMP GetNext requests 'trasportd' may reach 100 percent of CPU utilization. PR1676593
- The traffic does not re-route quickly causing traffic blackholing. PR1676740
- Traffic drop can be seen on MX Series platforms with MPC10E-10C line card. PR1676777
- After upgrading to Junos OS Release 22.2R1, "show system license" will display some protocol as "invalid" state if no flex license. PR1677869
- Traffic drop can be seen for MPC7, MPC8, and MPC9 during unified ISSU in a specific scenario. PR1678130
- Packet Forwarding Engine memory usage gets impacted after GRES. PR1678217
- `show interfaces diagnostics optics interface` shows all 0 on 100/400G port on MPC10E card. PR1678716
- The rpd process crashes when a delegated LSP with IPv6 install prefix is configured. PR1678874
- The pccd process might crash during MBB for an externally controlled LSP. PR1678970
- The l2ald is treating MAC as a duplicate causing traffic loss. PR1680242
- The bbe-smgd process on the router might stop processing new PPPoE subscribers session. PR1680453
- The dynamic tunnel route is removed when a new tunnel is brought up for the same selector. PR1680775
- Traffic might drop only when the backup link is up on link-protection LAG interface. PR1680889
- The Packet Forwarding Engine process crashes from Junos OS Release 21.4R1 and later on VMhost platforms. PR1681532
- Fabric plane check or error alarm might be seen due to the burst traffic in MS-MPC line cards. PR1681624
- Auto-negotiation reflects on the MPC7E-10GE line card. PR1682962

- Traffic loss is seen with port-mirroring is enabled on aggregated Ethernet interface in multicast downstream. PR1683192
- 'clear interfaces statistics all' taking more than 9 min due to invalid PIC configuration inside GNF. PR1683312
- The traffic drop would be observed with inter-vlan configuration when deactivating and activating the EVPN routing instance. PR1683321
- Commit check error message is not thrown when DetNAT is configured with AMS load-balancing-options. PR1683772
- [MAP-E] PPE errors are seen when you deactivate and then activate the partial reassembly - ZTCHIP_MQSS_CMERROR_DRD_RORD_ENG_INT_REG_CMD_FSM_STATE_ERR (0x227fa5) PR1683845
- More than one label stack is not suppoting, gives as "Maximum number of sids supported is 0" error in srv6 ping in Alfa-Romeo[lc9600] PR1683883
- rpd crash when SRv6 service routes resolve over SRv6 SRTE policies using older resolution scheme PR1683993
- Traffic would hit wrong queue post ISSU PR1684019
- The l2cpd process crash may be observed when disabling RSTP on an interface. PR1684072
- MFT: rpd cores @spring_te_stats_info_lookup_transit_stats_info_from_ingress_stats_info at Backup RE with multiple times deactivate/activate of source-packet routing PR1684111
- An interface configured as 1G may flap on a port with the mixed speeds of 1G and 10G after a PIC restart. PR1684728
- Insufficient space for vmcores for Junos VM. PR1684968
- TI-LFA backup path is not computed which effects slow convergence in case of failures. PR1685064
- Multiple bbe-smgd cores might be observed resulting in subscribers being lost or failing to login in the Enhanced subscriber scenario PR1685070
- when uncorrectable FEC/CRC errors above the threshold are injected the plane is not going to check state PR1685230
- license-check might generate a core file on MX Series routers. PR1685433
- PICs on the GNF failed to come online after the chassisd restart. PR1685453

- bbe-smd-cpd core file is generated (patricia_delete; - bbe_cos_drop_profile_remove_all .../ bbe_cos_drop_profile.c:837) during commit after adding very large class-of-service stanza to CP configuration. PR1685482
- On MX Series or PTX Series platforms, when you configure BMP RIB-IN and BMP RIB-OUT, large number of BGP routes remain in Holddown state after route churn. PR1685510
- The l2ald core file seen after zeroize. PR1686097
- The rpd crash would be observed when two separate next-hops in rpd map to the same next-hop-index in the kernel PR1686211
- VPLS traffic loss might be seen when deleting and adding a routing-instance. PR1686523
- Traffic via the ICL link to MC-AE peer box gets looped back to the VTEP tunnel on MX240 and MX480 platforms. PR1687024
- The PIMv6 is not getting enabled for L2TP subscribers. PR1687138
- The rpd process crash is seen when the BGP SR-TE tunnel is marked for deletion PR1687287
- The FPC crash is observed with a "flexible-match-mask" condition. PR1687862
- On Junos OS and Junos OS Evolved platforms delegated LSP control will not be returned to the PCC in a specific scenario. PR1687885
- The LLDP output packets are not transmitting on the em0 interface of Junos OS and Junos OS Evolved platforms. PR1688023
- A kernel crash can be seen with MIC-3D-8DS3-E3 installed. PR1688315
- The LACP might get stuck in a continuous update loop in the MC-LAG scenario. PR1688958
- Packet Forwarding Engine wedge will be seen due to fast link flaps. PR1688972
- The logical interface policer is not working as expected when applied to filter input-list/output-list PR1689199
- "failed to get template var id" error messages are generated by FPC when BFD liveness detection is negotiated by DHCP subscriber which has lawful intercept enabled PR1689621
- A 1G port on a QSFPP-4x10G transceiver will be down sometimes after the FPC restart. PR1689644
- Traffic drop on the system when traffic sent to remote IPv6. PR1690679
- Use latest os-package when upgrading. PR1691209
- The rpd process crashes on deleting the Segment Routing Traffic Engineering (SR-TE) tunnel. PR1691459

- PCS errors and framing errors on 100GE interfaces on certain Junos OS platforms. PR1692063
- The firewall bridge filter policers (attached to ae interface) are not working on all Junos OS MX Series platform with MPC10 card upon deactivate-activate a term intended to limit overall traffic. PR1692070
- ALG child session will not be transported through the DS-Lite tunnel which might lead to traffic failures in absence of a direct route to the host. PR1692525
- MacSec session will not be up on the new fallback key during the primary key transition. PR1693301
- Traffic loss is observed when the ECMP path is IRB over the aggregated Ethernet interface (IPv4->MPLS). PR1693424
- Traffic loss will be seen when MACSEC is configured. PR1693730
- NDP cannot resolve neighbor after clearing IPv6 neighbor. PR1694009
- license-check warning reported on backup Routing Engine by commit or commit check. PR1694935
- The l2cpd telemetry crashes when the LLDP Netconf notification from external controllers along with Netconf services configuration is present on the device. PR1695057
- BMP EOR is sent with wrong peer address causing BMP failure. PR1695320
- MPC11E goes offline on configuring `fpc-slice`. PR1695510
- The dot1x authentication will not be enabled on interfaces with specific configuration combination. PR1696906
- FPC crashes when firewall filter is unconfigured and reconfigured with same index. PR1697404
- Junos OS and Junos OS Evolved: A BGP session will flap upon receipt of a specific, optional transitive attribute in Junos OS Release 22.3R1 (CVE-2022-22184). PR1698446
- Transit tunnels fails and remains down on all Junos OS based MX Series and SRX Series platforms with IKE-NAT-ALG enabled. PR1699115
- The rpd crashes when rib-sharding is configured. PR1699557
- FPC restart and core file is generated in MPLS scaled scenario with always-mark-connection-protection-tlv configured. PR1701147
- Traffic loss is seen due to interface flap when changing speed from 10G and 1G. PR1701183
- On Junos OS platforms with MS-MPC cards the IKE ALG inactivity timeout value stays fixed. PR1701305

High Availability (HA) and Resiliency

- The rpd memory leak might be observed when flapping BGP sessions relates to rt_ modules. PR1681394
- Traffic will be impacted if GR-ISSU fails. PR1694669
- The rpd crashes when any commit is performed. PR1701146

Interfaces and Chassis

- em0 interface ppeed is reflecting as 10G instead of 1G. PR1636668
- The Packet Forwarding Engine input/output chip setup failed for some interfaces and causes those interfaces missing in Packet Forwarding Engine after backup chassis upgraded via sequential upgrade. PR1670345
- VRRP master-master condition might occur when there are more than two devices in the VRRP group. PR1680178
- If VRRP authentication key is more than 16 characters it is ignoring remaining characters. PR1683871
- Traffic is getting impacted as interface hold-time is not working with wan-phy framing. PR1684142
- VRRP master session on aggregated Ethernet interface, logical interface having child links on satellite device stops transmission post GRES. PR1697394
- The backup MX Series Virtual Chassis router could become master after the system reboot. PR1697630

Junos Fusion Satellite Software

- The Junos Fusion Satellite device will be stuck in the SyncWait state. PR1682680

Layer 2 Ethernet Services

- MX240: Verify VRRP statistics fails after deactivating the access interface. PR1666943

- DHCP packets sent to the client have the Option-82 suboption length set to 0. PR1684521
- IPv4 ALQ does not work with authentication. PR1688272
- DHCP packets might not be sent to the clients when 'forward-only' is reconfigured under the routing instance PR1689005
- A dcd process crashes continuously when the dhcp-service restarts. PR1698798

MPLS

- The error severity of syslog message "ted_client reset" generated during commit is incorrect. PR1649565
- RSVP refcount leak and the rpd crash observed post LSP churn. PR1621771
- The rpd core is seen due to IGP database and BGP LS database out of sync. PR1655031
- Memory utilization keeps incrementing due to the path error message. PR1657872
- LDP session stuck in non-existent state when router has multiple addresses configured on loopback interface. PR1666506
- Traffic loss will be seen in an LDP->BGP-LU stitching scenario. PR1670334
- LDP traffic might drop or get discarded when the L-ISIS/L-OSPF route changes due to interface level configuration. PR1671187
- CPU utilization of rpd process may reach 100 percent while reporting LSP states to pccd if the IS-IS update churn is high. PR1673348
- LDP egress-policy for default route (0.0.0.0/0) with 'exact' option will make output label for the unrelated routes. PR1676551
- In an LDP -> BGP LU stitching scenario, Multiple LSPs will not be installed in the forwarding table, even if BGP Multipath and ECMP are enabled. PR1680574
- In the RSVP-TE scenario, with Entropy label capability is enabled during MBB issues handling Resv Messages. PR1681403
- The Routing Engine crashes when MPLS next-hop is created and deleted frequently. PR1681892
- RSVP path tear is not encapsulated by the MPLS header when bypass is configured. PR1685182
- On a controller based MPLS setup with container LSPs, rpd daemon crashes after LSP deletion occurs. PR1690458

- The rpd crash will be observed during the MPLS label block allocation. PR1694648
- [MX]L2VPN ping is failing when UHP rsvp LSP is used. PR1697982
- The rpd core and traffic loss is observed on Junos OS and Junos OS Evolved platforms. PR1701420
- Memory leak issue in TED. PR1701800
- LDP flaps will be observed having LT interface with VLAN and LDP running between the logical-system instance and global instance. PR1702220

Network Management and Monitoring

- Aggregated Ethernet interface beyond 1099 are allotted 0 SNMP index. PR1683264

Platform and Infrastructure

- Traffic drop seen and filter not hitting as expected for match condition traffic class with FLT option configured. PR1573350
- The core interface goes down. PR1631217
- The MPC hosting an aggregated Ethernet member interface with a shared bandwidth policer configured at the aggregated Ethernet could crash upon encountering an HMC fatal error. PR1666966
- You might observe a traffic drop with layer 2 circuit local switching with PS interface. PR1669410
- You might observe a traffic drop with SP style configuration for the logical tunnel in Layer2 domain. PR1669478
- Junos OS: Receipt of crafted TCP packets destined to the device results in MBUF leak, leading to a Denial of Service (DoS) (CVE-2023-22396). PR1670303
- Layer 2 packets other than IPv4 or IPv6 (for example, CFM) will get forwarded as out of order via MPC10 and MPC11 in the egress direction. PR1670316
- DHCP bindings will fail for the client connected on an LT interface when DHCP snooping is enabled PR1677631
- BGP session flap with error BGP_IO_ERROR_CLOSE_SESSION. PR1685113

- Probes received counter is not correct when set "moving-average-size" > "history-size" under TWAMP client configuration. PR1685952
- Packet Forwarding Engine will be disabled whenever XQ_TOE CM error is being detected. PR1692256
- Packets received from type-5 tunnel are not sent out to local CE in EVPN-VxLAN scenario. PR1696106

Routing Protocols

- On enabling BGP PIC, you might observe an incorrect next-hop weight. PR1652666
- Traffic loss will be seen due to delay in BGP convergence time. PR1663883
- SSH access is possible without ssh setting. PR1664512
- Rpd crash might be observed due to multiple sequences of flap events. PR1669615
- Source and destination AS fields shows up as 0 in the flow record. PR1670673
- The routes with an independent resolution can trigger an rpd crash when the last BGP peer is down. PR1673160
- BGP or OSPF neighbors will not come up in Junos OS Evolved platforms if IPsec Security Associations are used to authenticate the peer. PR1674802
- KRT queue shows deferred operation while creating a logical interface after FPC offline and online event. PR1675212
- Label traffic will drop at the one-hop LSP stitching node if the packet has more than one label. PR1677567
- High CPU is seen on the platforms running IPv6. PR1677749
- Inter-domain forwarding connectivity will be broken between different lo0s in the option-C network causing problems for the MPLS transit-route. PR1677935
- RV task replication will be stuck in the "NotStarted" state when routing-options validation is deactivated and then activated. PR1679495
- The aggregator attribute will not be set correctly when the independent-domain is configured. PR1679646
- BGP auto-discovery sessions does not work any more after an interface flaps. PR1679950

- Inbound convergence pending flag is set after Routing Engine switchover. PR1680360
- The rpd process will crash and generate core file post graceful restart. PR1682778
- On single Packet Forwarding Engine with fusion satellite, LACP is not sending PDUs. PR1687395
- BMP will not send EOR message. PR1690213
- The rpd might crash on a system running with IGP shortcuts. PR1690231
- The rpd crash is seen when using a BGP neighbor telemetry subscription in a sharding environment. PR1692255
- Commit error when trying to configure rib-group under BGP in no-forward (default) RI. PR1696576
- An incorrect SR-TE secondary path weight makes the secondary path active in the forwarding table. PR1696598
- OSPF stuck in InitStrictBFD state for the neighbor which doesn't send LLS header. PR1700966
- OSPF routes are not getting installed after the interface is flapped. PR1705975

Subscriber Access Management

- Authd doesn't report CoS-Shaping-Rate VSA in accounting stop messages. PR1641416
- The authd process crashes during GRES recovery phase. PR1687998
- A few subscriber sessions will not be up post Routing Engine switchover. PR1697392

VPNs

- Traffic over IPSec tunnels might drop during unified ISSU. PR1416334
- The multicast receiver receives no traffic in an extranet scenario having an SPT tree already established. PR1675099
- Multiple deamon restart results in generating core files. PR1682573
- Two-digit numbered interfaces cannot be used as protect-interfaces. PR1695075

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.

Starting in Junos OS release 21.2R1, all Junos OS products which were previously running on FreeBSD 11.x based Junos OS are migrated to FreeBSD 12.x based Junos OS, except EX4400. Starting with Junos OS release 21.3R1, EX4400 platforms are migrated to FreeBSD 12.x based Junos OS.

The following table shows detailed information about which Junos OS can be used on which products:

Platform	FreeBSD 6.x-based Junos OS	FreeBSD 12.x-based Junos OS
MX5, MX10, MX40,MX80, MX104	YES	NO
MX240, MX480, MX960, MX2010, MX2020	NO	YES

Basic Procedure for Upgrading to Release 22.3R1

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 FreeBSD 12.x-Based Junos OS

Products impacted: MX240, MX480, MX960, MX2010, and MX2020.

To download and install FreeBSD 12.x-based 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-x86-32-22.3R1.9-signed.tgz
```

- For 64-bit Routing Engine version:

```
user@host> request system software add no-validate reboot source/junos-install-mx-x86-64-22.3R1.9-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-x86-32-22.3R1.x-limited.tgz
```

- For 64-bit Routing Engine version:

```
user@host> request system software add no-validate reboot source/junos-install-mx-x86-64-22.3R1.9-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***

Do not use the `validate` option while upgrading from Junos OS (FreeBSD 6.x, 10.x, and 11.x) to Junos OS (FreeBSD 12.x). This is because programs in the **junos-upgrade-x** package are built based on FreeBSD 12.x, and Junos OS (FreeBSD 6.x, 10.x, and 11.x) would not be able to run these programs. You must run the `no-validate` option. The `no-validate` statement disables the validation procedure and allows you to use an import policy instead.

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 22.3R2, 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: After you install a Junos OS Release 22.3R2 jinstall package, you cannot return to the previously installed Junos OS (FreeBSD 6.x) software by issuing the `request system software rollback` command. Instead, you must issue the `request system software add no-validate` command and specify the jinstall package that corresponds to the previously installed software.

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, EOL and EEOL:

- 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 thirty six months after the first general availability date and customer support for an additional six more months.

For both EOL and EEOL releases, you can upgrade to the next three subsequent releases or downgrade to the previous three releases. For example, you can upgrade from 20.4 to the next three releases – 21.1, 21.2 and 21.3 or downgrade to the previous three releases – 20.3, 20.2 and 20.1.

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. For example, 20.4 is an EEOL release. Hence, you can upgrade from 20.4 to the next two EEOL releases – 21.2 and 21.4 or downgrade to the previous two EEOL releases – 20.2 and 19.4.

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
End of Life (EOL)	24 months	End of Engineering + 6 months	Yes	No
Extended End of Life (EEOL)	36 months	End of Engineering + 6 months	Yes	Yes

For more information about 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 22.3R1

To downgrade from Release 22.3R1 to another supported release, follow the procedure for upgrading, but replace the 22.2R1 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

These release notes accompany Junos OS Release 22.3R2 for the NFX Series Network Services Platforms. They describe new and changed features, limitations, and known and resolved problems in the hardware and software.

You can also find these release notes on the Juniper Networks Junos OS Documentation webpage, located at https://www.juniper.net/documentation/product/en_US/junos-os.

What's New

There are no new features or enhancements to existing features in Junos OS Release 22.3R2 for NFX.

What's Changed

There are no changes in behavior and syntax in Junos OS Release 22.3R2 for NFX Series devices.

Known Limitations

There are no known limitations in hardware or software 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.

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.

High Availability

- On an NFX350 chassis cluster, when FPC0 (when node0 is primary) or FPC7 (when node1 is primary) is restarted by either using the request `chassis fpc slot slot restart` node local command or because of dcpfe core files on the primary, it restarts FPC1 or FPC8. This might break the preexisting TCP sessions and fail to restart the TCP sessions. The TCP sessions might require a manual restart. PR1557607

Interfaces

- If you disable the xe ports on NFX350, the ports' admin state appears down but the link state is up. PR1697877

Resolved Issues

IN THIS SECTION

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

Virtual Network Functions (VNFs)

- The NFX350 device stops responding after you configure VNF with SRIOV interfaces, and delete the VNF. Also, JDM becomes unreachable. PR1664814

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.

Starting in Junos OS release 21.2R1, all Junos OS products which were previously running on FreeBSD 11.x based Junos OS are migrated to FreeBSD 12.x based Junos OS, except EX4400. Starting with Junos OS release 21.3R1, EX4400 platforms are migrated to FreeBSD 12.x based Junos OS.

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, EOL and EEOL:

- 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 thirty six months after the first general availability date and customer support for an additional six more months.

For both EOL and EEOL releases, you can upgrade to the next three subsequent releases or downgrade to the previous three releases. For example, you can upgrade from 20.4 to the next three releases – 21.1, 21.2 and 21.3 or downgrade to the previous three releases – 20.3, 20.2 and 20.1.

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. For example, 20.4 is an EEOL release. Hence, you can upgrade from 20.4 to the next two EEOL releases – 21.2 and 21.4 or downgrade to the previous two EEOL releases – 20.2 and 19.4.

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
End of Life (EOL)	24 months	End of Engineering + 6 months	Yes	No
Extended End of Life (EEOL)	36 months	End of Engineering + 6 months	Yes	Yes

For more information about 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.

To upgrade or downgrade from a non-EEOL release to a release more than three releases before or after, first upgrade to the next EEOL release and then upgrade or downgrade from that EEOL release to your target release.

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 22.3

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 22.3R2:

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 PTX Series

IN THIS SECTION

These release notes accompany Junos OS Release 22.3R2 for the PTX Series. They describe new and changed features, limitations, and known and resolved problems in the hardware and software.

You can also find these release notes on the Juniper Networks Junos OS Documentation webpage, located at https://www.juniper.net/documentation/product/en_US/junos-os.

What's New

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

What's Changed

IN THIS SECTION

Learn about what changed in this release for the PTX Series.

General Routing

- **JNP10K-PWR-DC2 power supplies installed in PTX10008 and PTX10016 routers display as online when the power supplies are switched off**—JNP10K-PWR-DC2 power supplies installed in PTX10008 and PTX10016 routers in which Junos OS Release 21.4R1 or Junos OS Evolved Release 21.4R1 is installed display as online in the output of the command 'show chassis environment psm' when the input power feeds are connected, but the power switch on the power supplies are switched off.

Junos XML API and Scripting

- **The `file copy` command supports only text-formatted output in the CLI (ACX Series, EX Series, MX Series, PTX Series, QFX Series, SRX Series, vMX, and vSRX)**—The `file copy` command does not emit output when the operation is successful and supports only text-formatted output when an error occurs. The `file copy` command does not support using the `| display xml` filter or the `| display json` filter to display command output in XML or JSON format in any release. We've removed these options from the CLI.

Software Installation and Upgrade

- **New options for the `request system snapshot` command (ACX Series, EX Series, MX Series, PTX Series, QFX Series, and SRX Series)**—The `request system snapshot` command includes new options for non-recovery snapshots. You can include the `name` option to specify a user-defined name for the snapshot, and you can include the `configuration` or `no-configuration` option to include or exclude configuration files in the snapshot. By default, the snapshot saves the configuration files, which include the contents of the **/config** and **/var** directories and certain SSH files.

  [See request system snapshot (Junos OS with Upgraded FreeBSD).]

Known Limitations

IN THIS SECTION

Learn about known limitations in this release for the PTX Series.

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

General Routing

- PDT:10002-60C:BGP neighbor is not going to estalished state for a long time over GRE tunnel when the tunnel interface is disabled and enabled. PR1614179

Infrastructure

- The image validation is not supported during upgrading from pre Junos oS Release 21.2 to 21.2 and onward. PR1568757

Interfaces and Chassis

- Device prompt is not responding after issuing `commit` command. PR1662883

Routing Protocols

- Rpd generates core files if 100 transport-classes configured. PR1648490

User Interface and Configuration

- The mustd process crash might be observed with persist-group-inheritance. PR1638847

Open Issues

IN THIS SECTION

Learn about open issues in this release for the PTX Series.

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

General Routing

- Traffic drops after the FPC reboots with the aggregated Ethernet member links deactivated by the remote device. PR1423707
- High CPU utilization observed for RPD after applying test configuration on PTX5000. PR1555159
- High CPU usage might be observed when Inline Jflow and sampling are both configured. PR1569229
- The "FPC 0 Major Errors" alarm might be seen on PTX10002-60C/QFX10002-60C due to a rare timing issue. PR1613229
- PTX1000: V6 default route is not added after successful dhcpv6 binding on PTX1000 router. PR1649576

- PTX1002-60C : krt queue stuck in "CHANGE FROM gf 6 inst id 0" on disable/enable bgp. PR1652750
- ZTP: DHCPACK not received at ztp-server after zeroize of the device (client). PR1658287

Routing Protocols

- Micro BFD session state in Routing Engine remain UP even peer side session is down. PR1675921

Resolved Issues

IN THIS SECTION

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

General Routing

- IS-IS adjacency is not coming up through TCC l2circuit. PR1590387
- On Junos ACX/PTX/QFX platforms traffic blackholing might occur after interface flaps. PR1645488
- The AE interface speed is not reflected correctly in certain scenarios on Junos platforms. PR1649958
- IS-IS adjacency is not coming up through the Layer 2 domain. PR1663134
- PCS errored blocks count increments on PTX3000/PTX5000 after Junos software upgrade. PR1669267
- jsd memory leak and might lead jsd restart. PR1669426

- Reporting-interval in `show jvision sensor info` is stuck at 65000 when configured reporting rate is changed from 65000 to 68000. PR1673476
- The PFE process crashes from Junos OS Release 21.4R1 version onwards on VMhost platforms. PR1681532
- On PTX5000 platforms when a command is issued to power off an FPC, it gets stuck in the 'Announce Offline' state. PR1683562
- jnxOperatingDescr.1.1.0.0 returns blank, but jnxOperatingState.1.1.0.0 returns value. PR1683753
- The rpd crash would be observed when two separate next-hops in rpd map to the same next-hop-index in the kernel. PR1686211
- On all Junos PTX3000 and PTX5000, upgrading from older Junos to 20.2R1 or later release might trigger intermittent link flapping. PR1693367
- jkey path changed under protocol/isis. "levels" is missing. PR1698192

MPLS

- The error severity of syslog message `ted_client reset` generated during commit is incorrect. PR1649565
- CPU utilization of rpd process might reach 100% while reporting LSP states to pccd if the IS-IS update churn is high. PR1673348
- In an LDP -> BGP LU stitching scenario, multiple LSPs will not be installed in the forwarding table, even if BGP Multipath and ECMP are enabled. PR1680574
- In the RSVP-TE scenario, with Entropy label capability enabled during MBB issues handling Resv messages. PR1681403

Routing Protocols

- The rpd crash would be seen on a system running with IGP shortcuts. PR1690231

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 PTX Series. Upgrading or downgrading Junos OS might take several hours, depending on the size and configuration of the network.

Starting in Junos OS release 21.2R1, all Junos OS products which were previously running on FreeBSD 11.x based Junos OS are migrated to FreeBSD 12.x based Junos OS, except EX4400. Starting with Junos OS release 21.3R1, EX4400 platforms are migrated to FreeBSD 12.x based Junos OS.

Basic Procedure for Upgrading to Release 22.3

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: Back up the file system and the currently active Junos OS configuration before upgrading Junos OS. This allows you to recover to a known, stable environment if the upgrade is unsuccessful. Issue the following command:

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

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 router, 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.

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 22.3R2:

1. Using a Web browser, navigate to the All Junos Platforms software download URL on the Juniper Networks webpage:

   https://support.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 by 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 routing platform or to your internal software distribution site.
10. Install the new jinstall package on the router.

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:

```
user@host> request system software add validate reboot source/junos-install-ptx-
x86-64-22.3R2.9.tgz
```

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

```
user@host> request system software add validate reboot source/junos-install-ptx-
x86-64-22.3R2.9-limited.tgz
```

Replace the 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*

The validate option validates the software package against the current configuration as a prerequisite to adding the software package to ensure that the router reboots successfully. This is the default behavior when the software package being added is a different release.

Adding the `reboot` command reboots 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-PTX-X8 Routing Engine. For upgrading the host OS on this router 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.

NOTE: After you install a Junos OS Release 22.3 jinstall package, you cannot return to the previously installed software by issuing the `request system software rollback` command. Instead, you must issue the `request system software add validate` command and specify the jinstall package that corresponds to the previously installed software.

NOTE: Most of the existing `request system` commands are not supported on routers with RE-PTX-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, EOL and EEOL:

- 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 thirty six months after the first general availability date and customer support for an additional six more months.

For both EOL and EEOL releases, you can upgrade to the next three subsequent releases or downgrade to the previous three releases. For example, you can upgrade from 20.4 to the next three releases – 21.1, 21.2 and 21.3 or downgrade to the previous three releases – 20.3, 20.2 and 20.1.

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. For example, 20.4 is an EEOL release. Hence, you can upgrade from 20.4 to the next two EEOL releases – 21.2 and 21.4 or downgrade to the previous two EEOL releases – 20.2 and 19.4.

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
End of Life (EOL)	24 months	End of Engineering + 6 months	Yes	No
Extended End of Life (EEOL)	36 months	End of Engineering + 6 months	Yes	Yes

For more information about 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 a Junos OS installation on each Routing Engine separately to avoid disrupting network operation as follows:

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.

Junos OS Release Notes for QFX Series

IN THIS SECTION

These release notes accompany Junos OS Release 22.3R2 for the QFX Series. They describe new and changed features, limitations, and known and resolved problems in the hardware and software.

You can also find these release notes on the Juniper Networks Junos OS Documentation webpage, located at https://www.juniper.net/documentation/product/en_US/junos-os.

What's New

There are no new features or enhancements to existing features in this release for QFX Series switches.

What's Changed

IN THIS SECTION

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

Junos XML API and Scripting

- **The `file copy` command supports only text-formatted output in the CLI (ACX Series, EX Series, MX Series, PTX Series, QFX Series, SRX Series, vMX, and vSRX)**—The `file copy` command does not emit output when the operation is successful and supports only text-formatted output when an error occurs. The `file copy` command does not support using the `| display xml` filter or the `| display json` filter to display command output in XML or JSON format in any release. We've removed these options from the CLI.

Software Installation and Upgrade

- **New options for the `request system snapshot` command (ACX Series, EX Series, MX Series, PTX Series, QFX Series, and SRX Series)**—The `request system snapshot` command includes new options for non-recovery snapshots. You can include the `name` option to specify a user-defined name for the snapshot, and you can include the `configuration` or `no-configuration` option to include or exclude configuration files in the snapshot. By default, the snapshot saves the configuration files, which include the contents of the **/config** and **/var** directories and certain SSH files.

  [See request system snapshot (Junos OS with Upgraded FreeBSD).]

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.

General Routing

- Unified ISSU on EX4650 devices will not be supported if there is a change in the chipset SDKs between the releases. This is a product limitation leading to the chip reset and hence unified ISSU is impacted. PR1634695
- On QFX10000 switches, wWhen EVPN-VXLAN tunnel gets established over IPv6 underlay, the encapsulated packets emitted out of leaf node might have UDP checksum zero. This is the default behavior of all IPv6 tunneled UDP packets and it is allowed as per RFC6936. PR1656363
- On QFX10008 devices, statistics for multicast packets is not as expected as the packets has Layer 2 header stripped during replication in Packet Forwarding Engine because of which it is not forwarded to the next hop. PR1678723

Infrastructure

- When upgrading from Junos OS Release 21.2 and prior to Junos OS Release 21.2 and later, validation and upgrade might fail. The upgrading requires the use of the `no-validate` configuration statement. 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.

Class of Service (CoS)

- On QFX5100 platforms, traffic might not get classified based on a fixed classifier in MPLS as well as the VXLAN scenario. PR1650051
- On all Junos platforms, in a scaled scenario when some of the ge/xe/et interfaces are members of Aggregated Ethernet (AE) and the Class of Service (CoS) forwarding-class-set configuration is applied with a wildcard for all the physical interfaces and AE, it would trigger a Flexible PIC Concentrators (FPC) crash which leads to traffic loss. PR1688455

General Routing

- When you add VLAN as an action for changing the VLAN in both ingress and egress filters, the filter is not installed. PR1362609
- On the QFX5100 line of switches, inserting or removing optics on a port might cause a Packet Forwarding Engine Manager CPU spike and an eventual microcode failure. PR1372041
- VXLAN VNI (multicast learning) scaling on QFX5110 traffic issue is seen from VXLAN tunnel to Layer 2 interface. PR1462548
- 5M DAC connected between QFX10002-60C switches does not link up. But with 1M and 3M DAC this interop works as expected. Also it is to be noted QFX10002-60C and ACX or Traffic generator the same 5M DAC works seamlessly. There seems to be certain SI or link level configuration on both QFX10002-60C and MX2010 which needs to be debugged with the help from HW and SI teams and resolved. PR1555955
- To avoid the additional interface flap, interface hold time needs to be configured. PR1562857
- On QFX5100 devices, media type for SFP+-10G-CU1M and SFP-T cables are shown as Fiber. This is only a display issue and no functionality impact is observed. PR1570555
- On QFX5110 VC, FPC might gets disconnected with 24,000 DHCPv6 relay scaling, after the traffic is stopped. "pfe_listener_disconnect" error messages may be seen. PR1594748
- Pim VXLAN does not work on TD3 chipsets enabling VXLAN flexflow after Junos OS Release 21.3R1. Customers Pim VXLAN or data plane VXLAN can use the version prior to Junos OS Release 21.3R1. PR1597276

- On QFX5100, optical power is seen after detached and attached QSFP on disable interface. PR1606003
- On QFX5120-48Y devices, when scaled configuration and baseline configs are loaded multiple times one after other without much wait time in between then traffic or protocols on pure Layer 3 interfaces might behave in undefined/unexpected manner. PR1612973
- On PTX10002-60C and QFX10002-60C switches after the system is rebooted, the `FPC 0 Major Errors` alarm might be seen due to a rare timing issue. The issue could cause the host path traffic to get dropped. It is a rare issue and does not always happen during reboot. Please try to perform "request vmhost reboot" for recovery. PR1613229
- On QFX5110-32Q devices, traffic loss occurs after renumbering primary in Virtual Chassis. PR1632565
- Backup FPC lose their connection to the master when new members are added to the VCF (Virtual Chassis Fabric). PR1634533
- On all devices running Junos OS or Junos OS Evolved, where this is a high BGP scale with flapping route and the BGP Monitoring Protocol (BMP) collector/station is very slow, the rpd process might crash due to memory pressure. PR1635143
- When MACSEC and VRRP are enabled on QFX5120 VC, MACsec sessions are flapping at random times. Without VRRP this issue is not seen. PR1640031
- On all QFX5100 Virtual Chassis platforms, after the reboot, Virtual Chassis port (VCP) ports may not establish a VCP connection and Cyclic Redundancy Check (CRC) errors are also observed.PR1646561
- On QFX platform, IPv6 ifl status are being derived from the underlying ifd stats unlike on PTX where they are hardware assisted. Hence, they are not very reliable and are at best, guesstimate. PR1653671
- On QFX5100-24Q devices VC (Virtual-chassis) is in unstable state for 3-7 minutes causing traffic loss. PR1661349
- On all QFX platforms, Ethernet VPN (EVPN) Type-5 traffic drops are observed when the device is configured only with Type-5 Virtual Routing and Forwarding (VRF) and without an Integrated Routing and Bridging (IRB) interface. PR1663804
- When the remote end server/system reboots, QFX5100 platform ports with SFP-T 1G inserted may 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 QFX5200 devices after NSSU upgrade for a 4 member VC , FPC might toggle resulting in interfaces goes offline. PR1673116

- Each locally learned ARP/ND Nexthop requires unique fabric token from Kernel. This unique token maps to physical address in HW and this address points to EDF memory for the ARP/ND nexthops. Token pool in kernel is also used by different features like flood nexthops, arp/ndp nexthops. Token usage has increased as tokens are now used by IRB interfaces and default mesh groups also. 96,000 ARP/ND scale might not be achievable always. It is recommended to scale upto 95,000 ARP/ND. PR1673626

- On QFX10008 devices, statistics for multicast packets is not as expected as the packets has L2 header stripped during replication in PFE because of which it is not forwarded to the next hop.PR1678723

- On QFX5100 devices (both stand-alone and VC scenario) running Junos, occasionally during the normal operation of the device, Packet Forwarding Engine can crash resulting in total loss of traffic. The PFE reboots itself following the crash. PR1679919

Interfaces and Chassis

- On QFX5100 switches configured with Virtual Chassis(VC), if a primary member is unplugged or forced to power off, the unicast traffic is dropped due to mac-persistence-timer expiry there is a difference in mac addresses between logical aggregated parent interface and member aggregated ethernet(ae) interface. PR1695663

Layer 2 Features

- In case of the access-side interfaces used as SP-style interfaces, when a new logical interface is added and if there is already a logical interface on the physical interface, there is 20--50 ms traffic drop on the existing logical interface. PR1367488

Layer 2 Ethernet Services

- On QFX5100 and QFX5110 devices, vendor-id format maybe incorrect for network ports. This does not impact the ZTP functionality or service. The DHCP client config is coming from two places, i.e AIU script and vsdk sandbox. The DHCP client config coming from AIU script has the serial Id in vendor id where as the default config from sandbox does not have.PR1601504

Platform and Infrastructure

- On all Junos OS platforms, while using source-address NTP configuration parameter and issue the command "set ntp date" from the CLI, packets will be sent with the source address of the outgoing interface rather than the manually configured IP address. Typically, the manually configured IP address would be a loopback address. The problem does not apply to automatically generated NTP poll packets. PR1545022

Resolved Issues

IN THIS SECTION

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.

Class of Service (CoS)

- The congestion details will be lost as ECN bits in DSCP are cleared after VXLAN decapsulation. PR1683438

EVPN

- The kernel crash would be observed in an EVPN multi-homed scenario. PR1649234
- In EVPN-MPLS Mutihoming scenario DF election will get stuck in the Preference based state. PR1662954
- The ARP/ND entries are not relearnt as expected on the spine with EVPN-VXLAN. PR1677521

General Routing

- On Junos ACX/PTX/QFX platforms traffic blackholing can occur after interface flaps. PR1645488
- The port LEDs do not light up when 40G physical interfaces are up. PR1660532
- The dc-pfe process crash is observed with PTP Transparent clock on QFX platforms. PR1661602
- IS-IS adjacency is not coming up through the Layer 2 domain. PR1663134
- The DHCP offer packets will not be sent to the clients when the DHCP relay agent is configured over Type-5 EVPN. PR1664656
- PVLAN IGMP packet is forwarded between Isolated ports and also duplicated to primary vlan port (Promiscous). PR1667069
- Type-5 routes might not get programmed in Packet Forwarding Engine when the number of active interfaces and Vlan configured is high. PR1668352
- Route table and multicast add/change requests are got queued in the KRT queue post deleting EVPN enabled configuration followed by the rpd restart. PR1669161
- FPC1 is getting disconnected after ISSU and before switchover while checking ISSU status. PR1669702
- EVPN multicast traffic may get impacted because of routes getting stuck in the kernel routing table (krt) queue. PR1670435
- Packet drops are seen after flapping or changing a passive monitor interface. PR1671449
- Flow sample packet is not sent to the collector when the destination is an ECMP path. PR1672121
- The traffic doesn't re-route quickly causing traffic blackholing. PR1676740

- Interfaces with QFX-10000-30C and QFX10000-30C-M Line Cards will not work properly. PR1677325
- Firewall functions will not work as expected when egress firewall filter is configured. PR1679574
- ARP resolution will fail on QFX5120 VC. PR1679684
- BFD sessions will remain down in the EVPN-VxLAN scenario. PR1680757
- The PFE process crashes from 21.4R1 version onwards on VMhost platforms. PR1681532
- LLDP neighborship fails to come up with a Private VLAN configuration. PR1681614
- The dcpfe crash seen with PTP configuration on Junos platforms supporting boundary clock. PR1683308
- Traffic loss is seen when MAC flaps between the MC-AE interface and the ICL interface. PR1683771
- Licenses on the device might become invalid when the device is upgraded from a legacy licensing-based release to an Agile licensing-based release. PR1684842
- The protocol MTU for the IRB interface is not rolled back when the MTU of the IRB or IFD interfaces is modified or deleted. PR1685406
- Traffic statistics verification fails as receiving packet count exceeds specified limit in evpn vxlan multicast scenario. PR1685467
- Traffic via the ICL link to MC-AE peer box gets looped back to the VTEP tunnel on QFX5000 platforms. PR1687024
- QFX5120 will drop ingress traffic on an l2circuit configured interface on continuous flaps. PR1687257
- VXLAN configured on access port breaks L2 connectivity with the `vxlan encapsulate-inner-vlan` command. PR1687565
- OVSDB certificate files are not copied from the primary to the backup. PR1687847
- ARP resolution to the CE port having EP style AE with multiple VLANs would get fail in the EVPN-VXLAN scenario. PR1687861
- The LLDP output packets are not transmitting on the em0 interface of Junos and Junos OS Evolved platforms. PR1688023
- On QFX10008 and QFX10016 platforms fails to detect flaps even though the remote device connected has observed flaps. PR1688993
- On QFX10008 devices, while verifying the `show ethernet-switching global-mac-count | display xml` command, `global-mac-count` is not as expected. PR1689127

- Packet Loss seen on the EVPN-VXLAN spine router router. PR1691029
- Traffic loss is observed when the ECMP path is IRB over aggregated Ethernet interface. PR1693424
- PFE crash is seen on all Junos QFX5000 devices with L2PT configuration. PR1694076
- On QFX5120-48YM devices, dot1xd.core-tarball.0.tgz is observed in 22.1R3 at #0x009113f0 in __mem_assert (func=0x5c5b5a "free_jemalloc", file=0x58d668 "../../../../../../src/daemon-infra/lib/libjtask/mem/task_mem_cookie_jemalloc.c", line=201, expr=0x5e98f4 "!\"Cookie RedZone Validation Failed\"") at ../../../../../../src/daemon-infra/lib/libjtask/mem/task_mem_barrier.c:74. PR1694129
- Intra VLAN communication breaks in SP style config using VXLAN. PR1695058
- BMP EOR is sent with wrong peer address causing BMP failure. PR1695320
- On QFX5110-32Q Virtual Chassis, after loading "20.4R3-S5.3" dcpfe core is observed and device is unstable. PR1695943
- The BFD session might be stuck in "Init" state on certain QFX5000 switches. PR1696113
- Local multicast traffic forwarding issue can be seen on QFX5k in EVPN-VXLAN OISM setup. PR1697614
- Traffic drop is observed after deleting or deactivating the logical interface. PR1697827
- PE device changes an outer tag-id is translated on a local return environment. PR1697835

Interfaces and Chassis

- em0 interface ppeed is reflecting as 10G instead of 1G. PR1636668

MPLS

- Traffic loss will be seen in an LDP->BGP-LU stitching scenario. PR1670334

Routing Protocols

- BGP auto-discovery sessions does not work any more after an interface flap. PR1679950

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.

Starting in Junos OS release 21.2R1, all Junos OS products which were previously running on FreeBSD 11.x based Junos OS are migrated to FreeBSD 12.x based Junos OS, except EX4400. Starting with Junos OS release 21.3R1, EX4400 platforms are migrated to FreeBSD 12.x based Junos OS.

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 **22.3** 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 22.3 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-x86-64-22.3-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 22.3 `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-
x86-64-20.4R1.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-
x86-64-20.4R1.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, EOL and EEOL:

- 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 thirty six months after the first general availability date and customer support for an additional six more months.

For both EOL and EEOL releases, you can upgrade to the next three subsequent releases or downgrade to the previous three releases. For example, you can upgrade from 20.4 to the next three releases – 21.1, 21.2 and 21.3 or downgrade to the previous three releases – 20.3, 20.2 and 20.1.

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. For example, 20.4 is an EEOL release. Hence, you can upgrade from 20.4 to the next two EEOL releases – 21.2 and 21.4 or downgrade to the previous two EEOL releases – 20.2 and 19.4.

Table 9: 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
End of Life (EOL)	24 months	End of Engineering + 6 months	Yes	No
Extended End of Life (EEOL)	36 months	End of Engineering + 6 months	Yes	Yes

For more information about 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

IN THIS SECTION

These release notes accompany Junos OS Release 22.3R2 for the SRX Series Services Gateways. They describe new and changed features, limitations, and known and resolved problems in the hardware and software.

You can also find these release notes on the Juniper Networks Junos OS Documentation webpage, located at https://www.juniper.net/documentation/product/en_US/junos-os.

What's New

There are no new features or enhancements to existing features in Junos OS Release 22.3R2 for SRX Series devices.

What's Changed

IN THIS SECTION

Learn about what changed in this release for SRX Series.

Junos XML API and Scripting

- **The `file copy` command supports only text-formatted output in the CLI (ACX Series, EX Series, MX Series, PTX Series, QFX Series, SRX Series, vMX, and vSRX)**—The `file copy` command does not emit output when the operation is successful and supports only text-formatted output when an error occurs. The `file copy` command does not support using the `| display xml` filter or the `| display json` filter to display command output in XML or JSON format in any release. We've removed these options from the CLI.

Software Installation and Upgrade

- **New options for the `request system snapshot` command (ACX Series, EX Series, MX Series, PTX Series, QFX Series, and SRX Series)**—The `request system snapshot` command includes new options for non-recovery snapshots. You can include the `name` option to specify a user-defined name for the snapshot, and you can include the `configuration` or `no-configuration` option to include or exclude configuration files in the snapshot. By default, the snapshot saves the configuration files, which include the contents of the **/config** and **/var** directories and certain SSH files.

  [See request system snapshot (Junos OS with Upgraded FreeBSD).]

VPNs

- **Remote-access VPN solution doesn't support hexadecimal pre-shared (SRX Series and vSRX 3.0)**—With remote-access VPN solution, for pre-shared-key based authentication method, we support ascii-text format. This means, do not use hexademical format for the pre-shared keys in your configuration for remote-access VPN solution. Therefore, configure the statement `ascii-text` with ascii text format at `[edit security ike policy policy-name pre-shared-key]` hierarchy level for use with Juniper Secure Connect.

- **Removal of power mode IPsec Intel QAT option in IPsec VPN (SRX Series)**—We have removed the option `power-mode-ipsec-qat` at `[edit security flow]` hierarchy level from Junos CLI for display. This option is now hidden as it is not recommended to be configured with multiple IPsec VPN tunnels. We continue to use AES-NI in PMI mode for better performance than QAT.

  [See Improving IPsec Performance with PowerMode IPsec.]

- **PMI Mode Passthrough ESP traffic (SRX Series)**—we support the PMI express path processing for passthrough ESP traffic.

Known Limitations

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

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

Chassis Clustering

- In Z-mode configuration, sometimes the statistics of back-up session may not be correct on fail-over from master to back-up.PR1667098
- In SRX4100 and SRX4200 devices, there is a hardware limitation of Intel 82599 NIC where maximum of 128 unit case mac addresses plus mac filters are supported. For MNHA switching mode, if you define more than 127 virtual MACs on same revenue or AE interface, the extra (those beyond 127) virtual MAC filters could not be programmed to the NIC so you would see traffics (towards those vMACs) got silently dropped.PR1687262

Infrastructure

- On SRX4600 platform, the CPU may overrun while performing sanity check due to incompatibility issues between ukern scheduler and Linux driver which might lead to traffic loss.PR1641517
- When upgrading from releases before Junos OS Release 21.2 to Release 21.2 and onward, validation and upgrade might fail. The upgrading requires using of 'no-validate' configuration statement.PR1568757

User Interface and Configuration

- On all Junos and Evolved platforms configured with persist-group-inheritance, which is enabled by default from 19.4R3 onwards, might lead to mustd process crash in highly scaled configuration.PR1638847

VPNs

- In some scenario(e.g configuring firewall filter) sometimes srx5K might show obsolete IPsec SA and NHTB entry even when the peer tear down the tunnel. PR1432925

Open Issues

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

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

Chassis Clustering

- 10G DAC cable is not supported at CTL/FAB link at SRX4100/4200 Cluster setup. Hardware Compatibility Tool (https://apps.juniper.net/hct/home/) reports 10G DAC cables are as "supported", but CTL and FAB links are out of scope. - SRX-SFP-10GE-DAC-1M - SRX-SFP-10GE-DAC-3MPR1636365

Flow-Based and Packet-Based Processing

- For accelerated flows such as Express Path, the packet or byte counters in the session close log and show session output take into account only the values that accumulated while traversing the NP. PR1546430

Interfaces and Chassis

- Traffic drop might be seen on irb interface on SRX1500 for network control forwarding class when verifying dscp classification based on single and multiple code-points. PR1611623

Platform and Infrastructure

- In Mac-OS platforms when Juniper Secure Connect client connects successfully, the client is not getting minimized to tray icon and needs to be minimized manually.PR1525889
- IPSec rekey fails when SRX is configured with kilobyte based lifetime in remote access solution. PR1527384
- With ssl-proxy configured along with web-proxy, the client session might not get closed on the device until session timeout, even though the proxy session ends gracefully.PR1580526
- On MX platforms the JDM (Juniper Device Manager) server could not be created in in-chassis mode of junos node slicing, which results in mgd process crash and affects GNF's (Guest Network Function) provisioning. PR1583324
- HA AP mode on-box logging in LSYS and Tenant, Intermittently Security log contents of binary log file in LSYS are not as expected PR1587360
- SMTPS sessions are not getting identified when traffic is sent from IXIA (BPS) profile. PR1635929

- Firewall-authentication with user-firewall based RADIUS access has syslog missing the username and rule.PR1654842
- On SRX series platform with chassis cluster enabled, the reth (Redundant Ethernet) interface might not come up due to speed mismatch when the reth interface speed is changed after RG0 (redundancy group) failover.PR1658276
- On SRX platforms using authentication-scheme (pass-through/web-auth/web-redir) and authentication sources (firewall-user/ldap/radius) do not display the complete user's group information because the display buffer for showing group names for an authentication entry is too small.PR1673125
- For logical system, tenant logical interface with unit 0 and without vlan tagging/ vlan id can be created from Network>Connectivity>Interfaces. Same cannot be done from Logical system or tenant workflow.PR1676235
- On SRX380, the Autonegotiation status on the 1G/10G ports may be incorrectly displayed as "Incomplete". This has no impact to traffic.PR1703002

VPNs

- Tunnel debugging configuration is not synchronized to the backup node. It needs to be configured again after RG0 failover. PR1450393

Resolved Issues

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

Application Layer Gateways (ALGs)

- Junos OS: SRX 5000 Series: Upon processing of a specific SIP packet an FPC can crash (CVE-2023-22408) PR1658604
- SIP 200 OK(INVITE) response packets are dropped leading to SIP Call failure PR1677554
- SIP calls are getting dropped due to NAT failure and SIP ALG is enabled PR1686613

Chassis Clustering

- Policy configured with condition route-active-on import is not working properly after RG0 failover. PR1686648

- Chassis cluster IP monitoring on the secondary node failed after the system reboot on the SRX platforms. PR1691071
- GTPv2 message filtering not working. PR1704472

Class of Service (CoS)

- "show interfaces queue interface" command output not correctly displaying bps values for throughput higher than 4.25Gbps PR1596172

Flow-Based and Packet-Based Processing

- 22.2R1:SRX5K:SD-WAN: To track RE and PFE sync issue with NAT configs and closed scan session counter issue PR1661796
- In SD-WAN the association between VRF instance and VRF group fails for ISSU from 19.2~21.1 to 22.2R1 PR1661935
- The flow sessions traversing the IOC2 card would time out early when Express Path is enabled PR1688658
- SOF was incorrectly offloading short-lived flows leading to early exhaustion of NP memory, reducing overall device performance PR1692100
- The PMI mode IPSEC tunnel on SRX4100/4200/4600, vSRX, and SRX5K with SPC3 card will core when the route is changed frequently PR1705996

J-Web

- All the security policies on Junos SRX platforms can get deleted while trying to delete any particular policy via J-Web PR1681549

Network Address Translation (NAT)

- MNHA: Incorrectly a warning is thrown at commit check for Source NAT config when the source-address or destination-address of the NAT rule is set as 0.0.0.0/0 PR1699407

Network Management and Monitoring

- High logging rate may cause 'eventd' to increase RE CPU utilization PR1661323

Platform and Infrastructure

- SMS Channel Down alarm on primary node of HA pair after upgrade PR1629972
- 21.3R2:SRX_RIAD:srx1500,srx4200:SKYATP:IMAP/IMAPS Email permitted counter is not incremented in AAMW email statistics while testing whole email block. PR1646661
- Packet loss might be seen on SRX4100 and SRX4200 devices from 20.2R2 PR1650112
- Split tunneling feature will not work PR1655202
- Archived files created by non-root users may not include some files PR1657958
- SRX4600 platforms in split brain scenario post ISSU PR1658148
- show fwauth user details is not displaying group information PR1659115
- PR : monitored IP addresses for a redundancy group are reachable despite removing the redundant Ethernet interface from a zone PR1668532
- Traffic loss seen due to SPC3's packets getting stuck PR1671649
- VPN tunnel will not be established in exclusive client scenario PR1674522
- Netbios traffic (IRB broadcast) is getting dropped post upgrade on the SRX platform PR1675853
- PKID process crashes when validating the certificate chain of a certificate PR1679067
- Dial-on-demand mode on the dialer interface is not working as expected PR1680405
- "%DAEMON-4: Set system alarm failed: Operation not supported by device" message is seen on high end SRX PR1681701
- SRX4600HA might not failover properly due to a hardware failure PR1683213
- "NSD_CLEAR_POLICY_DNS_CACHE_ENTRY_IP" log is not found on the device after keeing DNS cache entry unchanged PR1684268
- The cluster fabric link will be down post reboot of node or power cycle PR1684756
- The user authentication page is not rendering on the client browser PR1685116
- unexpected default event-rate value for event mode logging PR1687244
- The chassis cluster will not respond to DNS queries when configured with DNS proxy service PR1688481
- The system may crash when Jflow inactive timeout is configured to be less than 'previous flow-inactive-timeout + 180' seconds PR1688627

- SNMP MIB walk for jnxBoxDescr OID returns incorrect value PR1689705
- SRX cluster may fail in a rare scenario when node status changes to disabled state without going through the ineligible state PR1692611
- Fabric monitoring suspension and control link failure may cause HA cluster outage PR1698797
- The process srxpfd/ flowd will crash on SRX devices PR1694449

Routing Policy and Firewall Filters

- SRX stops refreshing the FQDNs used in the security policies and NAT PR1680749

Routing Protocols

- High CPU is seen on the platforms running IPv6 PR1677749

User Interface and Configuration

- IPSec tunnel will flap post MNHA configuration commit PR1669104

VLAN Infrastructure

- Traffic Stops when the mac address of a node changes in L2 secure-wire SOF PR1597681
- OSPF neighbor won't establish under Transparent mode when neighborship across different zone PR1599891

VPNs

- Traffic over IPSec tunnels may be dropped during ISSU PR1416334
- 19.2TH:VPN:SRX5600: While verifying "show security ipsec next-hop-tunnels" output in device the IPsec SA and NHTB entry is not getting cleared after configuring firewall filter PR1432925
- Packets traversing through a policy-based VPN get dropped when PowerMode is enabled PR1663364
- The kmd crash is seen if the external-interface is empty in the IKE gateway configuration PR1664910
- Master-encryption-password is not accessible when system is in FIPS mode PR1665506
- VPN traffic loss is seen after HA node reboot while using traffic selectors PR1667223

- High Control Plane CPU utilisation while the kmd process is stuck after the core file PR1673391
- 22.4R1:SRX_RIAD:srx5600:MN_HA:ike cookies didn't change in rekey lifetime expire cases after manual failover PR1690921

Migration, Upgrade, and Downgrade Instructions

IN THIS SECTION

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

Starting in Junos OS release 21.2R1, all Junos OS products which were previously running on FreeBSD 11.x based Junos OS are migrated to FreeBSD 12.x based Junos OS, except EX4400. Starting with Junos OS release 21.3R1, EX4400 platforms are migrated to FreeBSD 12.x based Junos OS.

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 thirty six months after the first general availability date and customer support for an additional six more 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 example, you can upgrade from 20.4 to the next three releases – 21.1, 21.2 and 21.3 or downgrade to the previous three releases – 20.3, 20.2 and 20.1.

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. For example, 20.4 is an EEOL release. Hence, you can upgrade from 20.4 to the next two EEOL releases – 21.2 and 21.4 or downgrade to the previous two EEOL releases – 20.2 and 19.4.

Table 10: 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)	36 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 vMX

IN THIS SECTION

These release notes accompany Junos OS Release 22.3R2 for vMX. They describe new and changed features, limitations, and known and resolved problems in the hardware and software.

You can also find these release notes on the Juniper Networks Junos OS Documentation webpage, located at https://www.juniper.net/documentation/product/en_US/junos-os.

What's New

There are no new features or enhancements to existing features in Junos OS Release 22.3R2 for vMX.

What's Changed

IN THIS SECTION

Learn about what changed in this release for vMX.

Junos XML API and Scripting

- **The `file copy` command supports only text-formatted output in the CLI (ACX Series, EX Series, MX Series, PTX Series, QFX Series, SRX Series, vMX, and vSRX)**—The `file copy` command does not emit output when the operation is successful and supports only text-formatted output when an error occurs. The `file copy` command does not support using the `| display xml` filter or the `| display json` filter to display command output in XML or JSON format in any release. We've removed these options from the CLI.

Known Limitations

There are no known limitations in hardware and software in Junos OS 22.3R2 for vMX.

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 and software in Junos OS Release 22.3R2 for vMX.

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 Junos OS Release 22.3R2 for vMX.

Upgrade Instructions

You cannot upgrade Junos OS for the vMX router from earlier releases using the `request system software add` command.

You must deploy a new vMX instance using the downloaded software package.

Remember to prepare for upgrades with new license keys and/or deploying Agile License Manager.

Starting in Junos OS release 21.2R1, all Junos OS products which were previously running on FreeBSD 11.x based Junos OS are migrated to FreeBSD 12.x based Junos OS, except EX4400. Starting with Junos OS release 21.3R1, EX4400 platforms are migrated to FreeBSD 12.x based Junos OS.

Junos OS Release Notes for vRR

IN THIS SECTION

These release notes accompany Junos OS Release 22.3R2 for vRR. They describe new and changed features, limitations, and known and resolved problems in the hardware and software.

You can also find these release notes on the Juniper Networks Junos OS Documentation webpage, located at https://www.juniper.net/documentation/product/en_US/junos-os.

What's New

There are no new features or enhancements to existing features in Junos OS Release 22.3R2 for vRR.

What's Changed

There are no changes in behavior and syntax in Junos OS Release 22.3R2 for vRR.

Known Limitations

There are no known limitations in hardware and software in Junos OS 22.3R2 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 22.3R2, see "Known Limitations" on page 44 for MX Series routers.

Open Issues

There are no known issues in hardware and software in Junos OS Release 22.3R2 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

Learn about the issues fixed in this release for vRR.

Platform and Infrastructure

- A 802.1Q tagged Ethernet traffic with an expected VLAN ID and with a non-zero 802.1P value ingressing a JRR200 VLAN enabled interface is dropped. PR1691694
- The rpd crash is observed when rib-sharding configured PR1699557

Junos OS Release Notes for vSRX

IN THIS SECTION

These release notes accompany Junos OS Release 22.3R2 for vSRX. They describe new and changed features, limitations, and known and resolved problems in the hardware and software.

You can also find these release notes on the Juniper Networks Junos OS Documentation webpage, located at https://www.juniper.net/documentation/product/en_US/junos-os.

What's New

IN THIS SECTION

Learn about new features introduced in this release for vSRX.

Platform and Infrastructure

- **Support for AMD processor (vSRX 3.0)**—Starting in Junos OS Release 22.3R2, vSRX 3.0 on Amazon Web Services (AWS) support the Advanced Micro Devices (AMD) processor for better performance. AMD processors have more cores, affordable, and provide better performance. AMD based vSRX instances in AWS allows you to interpret exact scaling and performance numbers.

  [See Requirements for vSRX on AWS.]

What's Changed

IN THIS SECTION

Learn about what changed in this release for vSRX.

Junos XML API and Scripting

- **The `file copy` command supports only text-formatted output in the CLI (ACX Series, EX Series, MX Series, PTX Series, QFX Series, SRX Series, vMX, and vSRX)**—The `file copy` command does not emit output when the operation is successful and supports only text-formatted output when an error occurs. The `file copy` command does not support using the `| display xml` filter or the `| display json` filter to display command output in XML or JSON format in any release. We've removed these options from the CLI.

Known Limitations

Learn about known limitations in this release for vSRX.

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

Chassis Clustering

- Currently max BFD detection interval tested by RLI is 16s. If the detection interval is too large, no BFD down event will be posted by BFDD daemon to jsrpd and jsrpd cannot be aware that ICL once goes down since BFD is the single source of MNHA ICL link failure detection. We don't have other (or plan to add other) ways to detect ICL link going down as it introduces extra complexity. So currently this is a product-limitation.PR1671622

Platform and Infrastructure

- VRRP is not supported on vSRX instances based on VMware hypervisors because VMware does not support virtual MAC addresses. PR1079742

Open Issues

Learn about open issues in this release for vSRX.

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

Platform and Infrastructure

- With ssl-proxy configured along with web-proxy, the client session might not get closed on the device until session timeout, even though the proxy session ends gracefully.PR1580526

VPNs

- When using Group VPN, in certain cases, the PUSH ACK message from the group member to the group key server may be lost. The group member can still send rekey requests for the TEK SAs before the hard lifetime expiry. Only if the key server sends any new PUSH messages to the group members, those updates would not be received by the group member since the key server would have removed the member from registered members list. PR1608290

Resolved Issues

Learn about the issues fixed in this release for vSRX.

Flow-Based and Packet-Based Processing

- Expected TCP sequences not found in ICMP6 dump PR1611202
- Packet loss on GRE Tunnel due to improper route look-up for tunnel destination PR1683334

Network Address Translation (NAT)

- MNHA: Incorrectly a warning is thrown at commit check for Source NAT config when the source-address or destination-address of the NAT rule is set as 0.0.0.0/0 PR1699407

Platform and Infrastructure

- Split tunneling feature will not work PR1655202
- ARP will not get learned if reth interface is configured with VLAN PR1681042
- "NSD_CLEAR_POLICY_DNS_CACHE_ENTRY_IP" log is not found on the device after keeing DNS cache entry unchanged PR1684268

Migration, Upgrade, and Downgrade Instructions

IN THIS SECTION

This section contains information about how to upgrade Junos OS for vSRX 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 22.3R2 for vSRX using J-Web (see J-Web) or the Junos Space Network Management Platform (see Junos Space).

Starting in Junos OS release 21.2R1, all Junos OS products which were previously running on FreeBSD 11.x based Junos OS are migrated to FreeBSD 12.x based Junos OS, except EX4400. Starting with Junos OS release 21.3R1, EX4400 platforms are migrated to FreeBSD 12.x based Junos OS.

Direct upgrade of vSRX 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 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 and vSRX 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 machine (VM) instead of performing a Junos OS upgrade. That also gives you the option to move from vSRX to the newer and more recommended vSRX 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 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 instance on the targeted OS version.

Upgrading Software Packages

To upgrade the software using the CLI:

1. Download the **Junos OS Release 22.3R2 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 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 Aug 25 14:15 /var/jail/tmp/alarmd.ts
       259.7K Aug 25 14:11 /var/log/hostlogs/vjunos0.log.1.gz
       494B Aug 25 14:15 /var/log/interactive-commands.0.gz
       20.4K Aug 25 14:15 /var/log/messages.0.gz
       27B Aug 25 14:15 /var/log/wtmp.0.gz
       27B Aug 25 14:14 /var/log/wtmp.1.gz
       3027B Aug 25 14:13 /var/tmp/BSD.var.dist
       0B Aug 25 14:14 /var/tmp/LOCK_FILE
       666B Aug 25 14:14 /var/tmp/appidd_trace_debug
```

```
        0B Aug 25 14:14 /var/tmp/eedebug_bin_file
        34B Aug 25 14:14 /var/tmp/gksdchk.log
        46B Aug 25 14:14 /var/tmp/kmdchk.log
        57B Aug 25 14:14 /var/tmp/krt_rpf_filter.txt
        42B Aug 25 14:13 /var/tmp/pfe_debug_commands
        0B Aug 25 14:14 /var/tmp/pkg_cleanup.log.err
        30B Aug 25 14:14 /var/tmp/policy_status
        0B Aug 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 to free up disk space.

4. Use FTP, SCP, or a similar utility to upload the Junos OS Release 22.3R2 for vSRX .tgz file to **/var/crash/corefiles/** on the local file system of your vSRX VM. For example:

```
root@vsrx> file copy ftp://username:prompt@ftp.hostname.net/pathname/
junos-vsrx-x86-64-20.4-2022-08-08.0_RELEASE_22.3_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-
x86-64-22.3-2022-08-08.0_RELEASE_22.3_THROTTLE.tgz no-copy no-validate reboot
Verified junos-vsrx-x86-64-22.3-2022-08-08.0_RELEASE_22.3_THROTTLE signed by
PackageDevelopmentEc_2017 method ECDSA256+SHA256
THIS IS A SIGNED PACKAGE
WARNING:     This package will load JUNOS 22.3 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-22.3-2022-08-08.0_RELEASE_22.3_THROTTLE.tgz
```

```
Extracting the package ...
total 975372
-rw-r--r-- 1 30426 950 710337073 Oct 19 17:31 junos-srx-mr-
vsrx-22.3-2022-08-08.0_RELEASE_22.3_THROTTLE-app.tgz
-rw-r--r-- 1 30426 950 288433266 Oct 19 17:31 junos-srx-mr-
vsrx-22.3-2022-08-08.0_RELEASE_22.3_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-22.3-2022-08-08.0_RELEASE_22.3_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-22.3-2022-08-08.0_RELEASE_22.3_THROTTLE-linux.tgz ...
upgrade_platform: Input package /var/tmp/junos-srx-mr-
vsrx-22.3-2022-08-08.0_RELEASE_22.3_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-22.3-2022-08-08.0_RELEASE_22.3_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-22.3-2022-08-08.0_RELEASE_22.3_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 22.3R2 for vSRX.

NOTE: Starting in Junos OS Release 17.4R1, upon completion of the vSRX 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 22.3-2022-08-08.0_RELEASE_22.3_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: 22.3-2022-08-08.0_RELEASE_22.3_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 .ova image and need to validate it, see Validating the vSRX .ova File for VMware.

Note that only .ova (VMware platform) vSRX images can be validated. The .qcow2 vSRX 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 thirty six months after the first general availability date and customer support for an additional six more 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 example, you can upgrade from 20.4 to the next three releases – 21.1, 21.2 and 21.3 or downgrade to the previous three releases – 20.3, 20.2 and 20.1.

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. For example, 20.4 is an EEOL release. Hence, you can upgrade from 20.4 to the next two EEOL releases – 21.2 and 21.4 or downgrade to the previous two EEOL releases – 20.2 and 19.4.

Table 11: 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)	36 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/
- Create a service request online: https://myjuniper.juniper.net/

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 https://myjuniper.juniper.net/
- 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

17 April 2024—Revision 6, Junos OS Release 22.3R2

20 July 2023—Revision 5, Junos OS Release 22.3R2

6 July 2023—Revision 4, Junos OS Release 22.3R2

2 March 2023—Revision 3, Junos OS Release 22.3R2

23 February 2023—Revision 2, Junos OS Release 22.3R2

2 February 2023—Revision 1, Junos OS Release 22.3R2