Release Notes

Junos OS Release 22.2R3

Introduction

Junos OS runs on the following Juniper Networks® hardware: ACX Series, 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 22.2R3. 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.

JUNIPEr
NETWORKS

Engineering
Simplicity

Table of Contents

Junos OS Release Notes for ACX Series

These release notes accompany Junos OS Release 22.2R3 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

Learn about what changed in this release for ACX Series.

Network Management and Monitoring

- **Support for the `junos:cli-feature` YANG extension (ACX Series, EX Series, MX Series, PTX Series, QFX Series, SRX Series, vMX, and vSRX)**—The `cli-feature` YANG extension identifies certain CLI properties associated with some command options and configuration statements. The Junos YANG modules that define the configuration or RPCs include the `cli-feature` extension statement, where appropriate, in schemas emitted with extensions. This extension is beneficial when a client consumes YANG data models, but for certain workflows, the client needs to generate CLI-based tools.

  [See Understanding the Junos DDL Extensions YANG Module.]

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).]

User Interface and Configuration

- **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 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

- On dynamic addition of logical interfaces to iflset, non-CIR logical interfaces might get starved. PR1656876

Open Issues

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

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

General Routing

- In ACX5000, some next-hop routes not getting installed properly, reporting message "Failed to h/w update ip uc route entry" In LPM mode, for default route if route changes from ecmp to non-ecmp HOLD nexthop, PFE gets into a corrupted ecmp nexthop. We fix the NH index issue and fixed some issues related to handling ipv4 vs ipv6 default routes for LPM. PR1365034

- On ACX5448, MAC learning or aging might stop in Layer 2 domain after excessive MAC movements or continuous interface flaps. There may be unexpected flooding traffic when this issue occurs. PR1480235

- Due to BRCM KBP issue route lookup might fail. PR1533513

- On ACX Series platforms, traffic issue might occur with downstream devices when you configure Precision Time Protocol (PTP) (G.8275.1 PTP profile) along with PHY timestamping and MPLS terminated on 10G interface. The transit PTP IPv4 packets are updated with incorrect Correction Factor(CF). Disabling PHY stamping might restore the issue impacting the PTP performance. PR1612429

- On all ACX Series platforms, the hosts will not receive multicast traffic when snooping is configured in a 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 configuration to allow internal trusted communication. Refer to TSB18224. PR1629943

- On Junos OS ACX Series platforms (ACX1100, ACX2100 and ACX2200) the Forwarding Engine Board (FEB) crash might occur. This might occur only 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

- On ACX5048 and ACX5096 platforms interface speed 10m is not supported on 1G interface. PR1633226

- On ACX5448 and ACX710 platforms, all types of delegated BFD sessions configured on routing-instance other than the default routing-instance might not come up.PR1633395

- 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 JSA70187 for more information. PR1637615

- On ACX5448 and ACX710 devices, when an application is trying to send the packet out to an egress port of a device on IPv6 Link Local address. The L3 packet does not egress out of the router and gets dropped. PR1638642

- Interoperability for 1G interfaces between EX4100 SKUs and ACX5448 and ACX5448-M/D or MX480 will not work. PR1657766

- SNMP MIB walk on jnxVpnInfo `show snmp mib walk jnxVpnInfo` for EVPN or EVPN-VPWS routing instance: In case of routing instance type EVPN or EVPN-VPWS, system auto creates one default routing instance apart from EVPN and/or EVPN-VPWS routing instance. So, in show output of `show snmp mib walk jnxVpnInfo` the number of configured routing instances are always one more than number of EVPN and/or EVPN-VPWS instances configured in the system. For example, we have configured a single EVPN routing instance in the box.

  user@host# show routing-instances evpn { instance-type evpn; protocols { evpn { interface ge-0/0/0.0 { vpws-service-id { local 1501; remote 11501; } } } } interface ge-0/0/0.0; route-distinguisher 65501:1501; vrf-target target:65501:1501; }

  user@host# run show snmp mib walk jnxVpnInfo jnxVpnConfiguredVpns.0 = 2 jnxVpnActiveVpns.0 = 1 jnxVpnNextIfIndex.0 = 0 jnxVpnNextPwIndex.0 = 0 jnxVpnNextRTIndex.0 = 0.

  In the above output "jnxVpnConfiguredVpns.0 = 2 " which is one more than the configured routing instance. PR1659466

- In RTAG7 or enhanced hashing mode a specific traffic stream will be forwarded over a single member link over an aggregated Ethernet bundle. It will not be equally shared over all the member links in the bundle. PR1659845

- IFD based CFM sessions are not supported in RIO and ODIN. PR1660086

- Some interfaces with zero statistics in `monitor interface traffic` command, sends traffic across all interfaces with applied speed of 100m on all 1g copper ports. On clearing statistics for interfaces, the issue is seen. The issue change is related to ifinfo for Junos OS Release 22.2R1. PR1661617

- In VPLS MH cases, the standby UNI ifl in backup router will be programmed in disable state, by adding the UNI interface to invalid vpn id in HW. During switch over the UNI ifl will be deleted and will be added under the VPLS instance VPN id. In issue case, UNI interface added under invalid VPN id in backup router is tried to deleted by passing the VPLS instance vpn id, causing the issue. This issue is applicable only for ACX5k series. PR1665178

- On ACX710, when locally generated VLAN-based IP packets (e.g. ping packet) are sourced from IRB interface, the Priority and DEI bits might be changed in Packet Forwarding Engine. PR1683770

- When a VPLS instance is deactivated in ACX5048, "dc-pfe: HEAP malloc(0) detected!" informational message is shown as the output. PR1692400

Resolved Issues

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

EVPN

- RPD core file is generated upon receipt of a specific EVPN route by a BGP route reflector in an EVPN environment (CVE-2022-22219). PR1675054

General Routing

- On booting the device ACX7100-48L, jdhcpd core file is seen. PR1658327

- SSH non-default port configuration causes FPC offline after upgrading 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 aggregated Ethernet interface. PR1666853

- Chassis alarms for smart errors not set or cleared. PR1669968

- New BFD sessions will not come up on ACX5448 and ACX710 due to continuous flaps. PR1670684

- The LLDP packets will not be transmitted over Layer 2 circuit on the ACX Series platform. PR1678752

- Memory leak is seen on ACX710 and ACX5448 when the core link flaps. PR1681980

- The traffic drop might be observed with inter-vlan configuration when deactivating and activating the EVPN routing instance. PR1683321

- On Junos OS ACX Series platforms the IP packets with VLAN tags do not get a response when sent out on the IRB interface in a certain condition. PR1683770

- ACX5448: ACX710 L2 circuit traffic drop with control-word enabled or control-word configuration. change. PR1683900

- Auto-mdix is not working in ACX710. PR1685431

- subscriber-management-helper is thrashing, not restarted, messages seen on ACX5448. PR1688107

- The LACP might get stuck in a continuous update loop in the MC-LAG scenario. PR1688958

- EVPN packets might go to incorrect queues due to incorrect classification and might lead to packets drop during congestion. PR1689604

- Packet forwarding fails on specific ACX Series 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 Network platforms. PR1692063

Network Management and Monitoring

- On all Junos OS and Junos OS Evolved platforms configured with filter-duplicates, the snmpd core might be observed if the SNMP query is made simultaneously from Network Management System (NMS) as well from the CLI. PR1669510

Routing Protocols

- When inline add event for IPv6 inline BFD session comes without resolving neighbor for nexthop, inline event addition will fail. PR1650677

- On all Junos OS platforms and all Junos OS Evolved platforms, routing process daemon (rpd) crashes and restarts when BGP is configured and a specific timing condition is hit for secondary route. This issue might cause a traffic impact. PR1659441

- In an SR to LDP interworking scenario, with SRMS, when a specific low privileged command is issued on an ABR rpd will crash (CVE-2022-22233). PR1662559

- MCSNOOPD restarts and will again learn the states after generating the core file. PR1672488

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

Table 1: EOL and EEOL Releases

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

These release notes accompany Junos OS Release 22.2R3 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 this release for cSRX.

What's Changed

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

Known Limitations

There are no known limitations in hardware and software in Junos OS 22.2R3 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 22.2R3 for cSRX.

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

Resolved Issues

There are no resolved issues in Junos OS Release 22.2R3 for cSRX.

Junos OS Release Notes for EX Series

These release notes accompany Junos OS Release 22.2R3 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

Learn about what changed in this release for EX Series.

General Routing

- In order to monitor vmhost storage usage: ? A new minor alarm, VMHost RE 0 Disk 1 inode usage breached threshold is introduced ? The existing minor alarm, VMHost RE 0 Disk 1 Usage is above threshold is changed to VMHost RE 0 Disk 1 Size usage breached threshold.

Network Management and Monitoring

- **Support for the `junos:cli-feature` YANG extension (ACX Series, EX Series, MX Series, PTX Series, QFX Series, SRX Series, vMX, and vSRX)**—The `cli-feature` YANG extension identifies certain CLI properties associated with some command options and configuration statements. The Junos YANG modules that define the configuration or RPCs include the `cli-feature` extension statement, where appropriate, in schemas emitted with extensions. This extension is beneficial when a client consumes YANG data models, but for certain workflows, the client needs to generate CLI-based tools.

  [See Understanding the Junos DDL Extensions YANG Module.]

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).]

User Interface and Configuration

- **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

IN THIS SECTION

- General Routing | **13**

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

- Once VXLAN is configured on an IFD, its always treated as VXLAN port even though Layer 2 VLAN exists.PR1570689

- On EX4300-MP platforms, when the command `request system software rollback` is performed device is going down and dcpfe cores are dumping.PR1631640

- 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 unified 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 statistics are retained on ports 24-to-47 but cleared on ports 0-23. PR1657995

- Zeroize chooses a fast reboot that minimizes steps/actions and it is considered sufficient if device is in consistent state on completion of zeroize. PR1713678

Open Issues

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

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

General Routing

- When VLAN is added as an action for changing the VLAN in both ingress and egress filters, the filter is not installed. PR1362609

- On EX4600 platforms, if a change related to TPID is made in the Device Control Daemon, traffic might be dropped in Packet Forwarding Engine due to failure on Layer 2 learning or interfaces flapping. PR1477156

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

- During Routing Engine switchover interface flap might be seen along with Scheduler slippage. PR1541772

- 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

- EX4100-24mp,48mp,24p/t,48p/t,F-24p/t,F-48-p/t: In an interop scenario, when using 1G SFP Optic on PIC-2, auto-negotiation should be disabled on the peer. PR1657766

- EX4100 MACsec interface statistics of encrypted or decrypted bytes do not increment further after reaching a 40-bit limit (1099511627775). PR1658584

- High CPU utilization is seen on EX4100-48P with POE and LLDP protocol configurations. PR1660557

- EX4600 devices VC (Virtual-chassis) is in unstable state for 3-7 minutes causing traffic loss. PR1661349

- Packet count might occasionally be 0 for some interfaces in **monitor interface traffic**.PR1661617

- On EX4300-48MP, NSSU abort is seen with **error: rebooting VC**. VC instability and dc-pfe core is observed after reboot. PR1668414

- 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

- EX4100 and EX4100-F Virtual chassis: Non-existing PIC ports (e.g. PIC0:PORT100, PIC2:PORT102) while running the jvision query. PR1681673

- On all Junos OS 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

- On all Junos OS platforms, configuring Link Layer Discovery Protocol (LLDP) with `system services netconf notification` enabled will trigger the l2cpd crash. This crash causes the CPU to spike. PR1695057

- On EX Series platforms, traffic loss will be observed for deleting all Layer 2 related configurations when both Layer 2 and Layer 3 configurations are present. PR1695847

- On all Junos OS platforms, the dcd (device control daemon) process crash is observed when more than 256 VLANs as name tags are added on the same interface. PR1696428

- When a sfp is unplugged or plugged in, it might not be recognized. PR1696444

- Port status LED remains "ON" for a few seconds after removing the link connection. PR1696596

- On EX2300, EX3400, EX4400, EX4100 and EX4300-MP platforms, when primary FPC with mac-persistence-timer configured on a virtual chassis switch is halted, it leads to Layer 3 (l3) forwarding issues for the integrated routing and bridging (IRB). PR1706845

Platform and Infrastructure

- EX4400-48MP - VM cores and VC split might be observed with multicast scale scenario. PR1614145

- On EX4300 platform, this issue occurs only when chassisd got restarted after filter configuration. This results in MAC-address change and sometimes MAC-address collision as well. PR1615548

- On EX4300 platform, if `encapsulation ethernet-bridge` is configured, the interface is getting 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 platforms, 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 blocking state. PR1673000

Virtual Chassis

- On Junos OS EX4600 Virtual Chassis (VC), the priamry Routing Engine reboot and all-members reboot lead to the Packet Forwarding Engine (PFE) manager hogging logs when SFP-T pluggable is installed in. The PFE manager hogging logs has no functionality impact (PR 1641556).PR1685067

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

Resolved Issues

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

General Routing

- DHCP packets getting looped in EVPN-VXLAN setup. PR1657597

- In the EVPN-VXLAN scenario, the DHCP packets will get dropped when the DHCP relay agent is configured. PR1662524

- 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

- 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

- EX SNMP: jnxOperatingDescr.1.1.0.0 returns blank, but jnxOperatingState.1.1.0.0 returns value. PR1683753

- 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

- EX4300-48MP, Factory Reset/Mode button cannot toggle status mode LED (SPD, DX, EN, and PoE). PR1687407

- EX4400 SNMP: FRU removal/insertion trap might 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

- Packet Forwarding Engine 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

- Dot1x memory is spiking up even after clearing the dot1x sessions. PR1702388

- The PXE boot recovery fails on EX9204/9208/9214 VC setup. PR1704457

- Traffic drops observed with hierarchal overlay ECMP configuration. PR1704470

- On EX3400-24P platforms, the fxpc process crashes after upgrading from 21.4R1.12 to any 22.xRx version except 22.4. PR1705387

- The PoE firmware upgrade fails on EX4400 platforms. PR1706952

Interfaces and Chassis

- 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

- The unicast traffic is dropped on EX4600-VC platforms. PR1695663

Layer 2 Ethernet Services

- The phone-home and SZTP might fail if phone-home daemon restarts. PR1693124

Platform and Infrastructure

- EX9000 platforms do not relay a DHCP offer with a broadcast flag under EVPN-VXLAN scenario. PR1670923

- The interface on the device will go down when one or more interfaces are connected to the Advantech3260 device at another end. PR1678506

Virtual Chassis

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

Migration, Upgrade, and Downgrade Instructions

IN THIS SECTION

- Upgrade and Downgrade Support Policy for Junos OS Releases and Extended End-Of-Life Releases | 19

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

Likewise, you can downgrade directly from one EEOL release to the previous two EEOL releases, even if the target release is beyond the previous three releases.

Table 2: EOL and EEOL Releases

Release Type	End of Engineering (EOE)	End of Support (EOS)	Upgrade/ Downgrade to subsequent 3 releases	Upgrade/ Downgrade to subsequent 2 EEOL releases
Standard End of Life (EOL)	24 months	End of Engineering + 6 months	Yes	No
Extended End of Life (EEOL)	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 22.2R3 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 Series Route Reflectors.

Known Limitations

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

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

Open Issues

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

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

Resolved Issues

IN THIS SECTION

- General Routing | **22**

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

General Routing

- With BMP RIB-IN and BMP RIB-OUT configured on MX or PTX Platforms, large number of BGP routes remain in Holddown state after route churn. PR1685510

- 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

- Upgrade and Downgrade Support Policy for Junos OS Releases and Extended End-Of-Life Releases | 22

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.

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

Table 3: EOL and EEOL Releases

Release Type	End of Engineering (EOE)	End of Support (EOS)	Upgrade/ Downgrade to subsequent 3 releases	Upgrade/ Downgrade to subsequent 2 EEOL releases
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 Juniper Secure Connect

IN THIS SECTION

These release notes accompany Junos OS Release 22.2R3 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 this release for Juniper Secure Connect.

What's Changed

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

Known Limitations

There are no known limitations in hardware and software in Junos OS 22.2R3 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 22.2R3 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 22.2R3 for Juniper Secure Connect.

Junos OS Release Notes for Junos Fusion for Enterprise

IN THIS SECTION

These release notes accompany Junos OS Release 22.2R3 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 this release for Junos fusion for enterprise.

What's Changed

There are no changes in behavior and syntax in in this release 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

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.

> (i) **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
```

> **(i)** **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
```

> **(i)** **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 and Extended End-Of-Life 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 EEOL releases only, you have an additional option - you can upgrade directly from one EEOL release to the next two subsequent EEOL releases, even if the target release is beyond the next three releases. Likewise, you can downgrade directly from one EEOL release to the previous two EEOL releases, even if the target release is beyond the previous three releases.

Table 4: EOL and EEOL Releases

Release Type	End of Engineering (EOE)	End of Support (EOS)	Upgrade/ Downgrade to subsequent 3 releases	Upgrade/ Downgrade to subsequent 2 EEOL releases
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

These release notes accompany Junos OS Release 22.2R3 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 this release for Junos Fusion for provider edge.

What's Changed

There are no changes in behavior and syntax in in this release 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

IN THIS SECTION

- Junos Fusion Satellite Software | 34

Learn about the issues fixed in this release for Junos Fusion for provider edge.

Junos Fusion Satellite Software

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

Migration, Upgrade, and Downgrade Instructions

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 22.2R3 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/jinstall64-22.2R3.SPIN-
domestic-signed.tgz
```

- For 32-bit software:

```
user@host> request system software add validate reboot source/jinstall-22.2R3.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/jinstall64-22.2R3.SPIN-
export-signed.tgz
```

- For 32-bit software:

```
user@host> request system software add validate reboot source/jinstall-22.2R3.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.

> (i) **NOTE**: After you install a Junos OS Release 22.2R3 `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.

> (i) 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 22.2R3, you must also upgrade your satellite device to Satellite Device Software version 3.1R1.

Upgrade and Downgrade Support Policy for Junos OS Releases and Extended End-Of-Life 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 EEOL releases only, you have an additional option - you can upgrade directly from one EEOL release to the next two subsequent EEOL releases, even if the target release is beyond the next three releases. Likewise, you can downgrade directly from one EEOL release to the previous two EEOL releases, even if the target release is beyond the previous three releases.

Table 5: EOL and EEOL Releases

Release Type	End of Engineering (EOE)	End of Support (EOS)	Upgrade/ Downgrade to subsequent 3 releases	Upgrade/ Downgrade to subsequent 2 EEOL releases
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 22.2

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

These release notes accompany Junos OS Release 22.2R3 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 the MX Series routers.

What's Changed

Learn about what changed in this release for MX Series.

General Routing

- In order to monitor vmhost storage usage:

  A new minor alarm, VMHost RE 0 Disk 1 inode usage breached threshold is introduced. The existing minor alarm, VMHost RE 0 Disk 1 Usage is above threshold is changed to VMHost RE 0 Disk 1 Size usage breached threshold.

- PTP configuration might not function correctly on an MX10008 Router with JNP10K-LC2101 Line card: - when Hypermode is enabled. Hypermode can be enabled by default when MX10008 Router has Switch Fabric Board 2 (SFB2), or by using the command set forwarding-options hyper mode. Hence, such PTP interfaces (slave, master, stateful) are unsupported. - if an aggregated Ethernet (AE) interface is configured and either the primary or secondary links on the AE do not support PTP with Hypermode, then the whole AE is marked as unsupported.

- An optics configuration mismatch alarm may be triggered when there is a discrepancy between the configured speed of an interface and the supported speed of the optic. This alarm indicates that the optic installed in the specified FPC is incompatible with the speed configured on the interface.

- **Change the output of the show arp command to display IP addresses and hostnames (MX Series routers)**—You can force the show arp command output to display the IP address next to the hostname of each device. To do this, enable the force-show-arp-resolve statement at the [`edit system services subscriber-management overrides`] hierarchy level. This makes it easier to manage subscriber access if your subscriber configuration relies on the IP addresses of the devices.

  [See overrides (Enhanced Subscriber Management) and Configuring Junos OS Enhanced Subscriber Management..]

Network Management and Monitoring

- **Support for the `junos:cli-feature` YANG extension (ACX Series, EX Series, MX Series, PTX Series, QFX Series, SRX Series, vMX, and vSRX)**—The `cli-feature` YANG extension identifies certain CLI properties associated with some command options and configuration statements. The Junos YANG modules that define the configuration or RPCs include the `cli-feature` extension statement, where appropriate, in schemas emitted with extensions. This extension is beneficial when a client consumes YANG data models, but for certain workflows, the client needs to generate CLI-based tools.

  [See Understanding the Junos DDL Extensions YANG Module.]

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).]

User Interface and Configuration

- **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 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

- Upon MPC11 boot up, errors such as following could be seen, but these are harmless and do not have functional impact. PR1457655

- Currently, IP options are not supported for egress firewall attach points, relevant supporting doc attached: Firewall Filter Match Conditions for IPv4 Traffic. The issue might occur IP-options router alert traffic not hitting the egress firewall filter. PR1490967

- On all MX/SRX platforms, changing configuration AMS 1:1 warm-standby to load-balance or deterministic NAT might result in vmcore and cause traffic loss. PR1597386

- When CFM Linktrace is initiated from AFT based MX line cards and platforms and no class of service classifiers and rewrite rules are configured for that interface, then the linktrace frames will not have the priority set as per the linktrace command. Example: `traceroute ethernet maintenance-domain md6 maintenance-association ma6 mep 601 priority 7` In above case, the linktrace frame is expected to be sent out with priority 7 set in the PDU. If no class of service classifiers and rewrite rules are configured, the priority set in the PDU will not be same as priority configured in CLI.PR1630096

- On bootup, a harmless error log is seen which does not have any functionality impact and is coming only during bootup due to the static arp configuration of the internal interfaces which in this case seems to be bme0. The static arp configuration are setup for IRI1 and during bootup both the REs tries to assign the IP addresses to their internal interfaces during which this log messages would have been displayed. But this eventually is resolved and internal IP addresses are assigned to the IRI1 interfaces, so you can ignore this error messages for the internal interfaces. The 128.0.0.63 is mostly unused in case of Bugatti but present more due to legacy reasons. PR1642399

- Configuring MPC11 in 4x100G and keeping peer in 400G mode, Link comes up on peer while staying down on local end. This issue is also specific to 400G-ZR optics as it has single media lane. The issue is not seen on other 400G optics supporting 4x100G mode.PR1653946

- There will be no explicit `PMB IDEEPROM Failure` alarm generated in case there is a failure with the PMB IDEEPROM. PR1660089

- The alarm string under `show chassis alarms` will display a generic alarm string code`FPC X PIC firmware outdated/FPC X PIC upgrade failed/FPC X PIC boot from golden`. This alarm string does not contain any details of the PIC/LMIC slot, which has raised the alarm. PR1665581

- Normal 25G on bootup or first time configuration work. In a special sequence when we move the speed from 25G to 10G on same link and back to 25G , the link doesnt come up in 25G. Due to transitioning between 10g to back 25G , there is some sequence which leaves YT in bad state, and it keeps reporting fault.PR1697272

Infrastructure

- Below IPC timeouts logs can be seen for statistics query to kernel(queried from cli or daemons querying internally)when there is config churn, or large number of IPCs getting exchanged between kernel and pfe 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 larger value by setting below hidden config to avoid IPC timeout errors. `# set system stats-timeout-lifetime 15 # 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. As a workaround, remove local-reversion configuration. PR1576979

- The automatic sorting of configuration entries does not work if defined under group. PR1637730

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, reboot MPC card. PR1303489

- On MX and EX9200 serial platforms, under Ethernet VPN (EVPN) environment, packets routed using IRB interface could not be fragmented due to media maximum transmission unit (MTU) problem. PR1522896

- When the `deactivate services rpm` and `deactivate routing-options rpm-tracking` CLIs are applied together and then committed, some of the rpm tracked added routes are not deleted from the routing table. The issue cannot be seen using the following steps.

  - Deactivate routing-options rpm-tracking.

  - Commit the configuration then all the rpm tracked routes will be deleted.

  - If the RPM service needs to be deactivated, deactivate services rpm.

  - Commit

    PR1597190

- 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 Policy and Firewall Filters

- When a hierarchy specified in apply-path is configured in an ephemeral instance, then rpd might not be able to update the prefix-list for the configuration in ephemeral instance. PR1636390

Routing Protocols

- When we have high scale, the Openconfig telemetry sensor /bgp-rib/ used in periodic streaming will cause high CPU usage by RPD. PR1625396

- 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

User Interface and Configuration

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

Open Issues

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.

Class of Service (CoS)

- The AE interfaces in per-unit-scheduler mode and committing CoS configuration on AE IFLs in a single commit leads to race-conditions. PR1666010

EVPN

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

- In PBB-EVPN (Provider Backbone Bridging - Ethernet VPN) 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

- This is a case where interface is disabled and comes up as CE after a timeout. A manual intervention of clear ce interface command should restore this.

  As a workaround,

  - Clear auto-evpn ce-interface interface-name

  - Configure edit activate interface-name family inet inet6

    PR1630627

Forwarding and Sampling

- When GRES is triggered by SSD hardware failure, the syslog error of `rpd[2191]: krt_flow_dfwd_open,8073: Failed connecting to DFWD, error checking reply - Operation timed out` might be seen. The issue can be recovered by restarting the dfwd daemon. PR1397171

- On all Junos dual-RE platforms, when performing activate/deactivate Graceful Routing Engine Switchover (GRES) multiple times, synchronization issues are observed between the master and backup dfwd process. PR1697959

General Routing

- AFEB crashing with PTP thread hog on the device. PR1068306

- On the PTX Platform with FPC-PTX-P1-A or FPC2-PTX-P1A, you might encounter a single event upset (SEU) event that might cause a linked-list corruption of the TQCHIP. The following syslog message gets reported: Jan 9 08:16:47.295 router fpc0 TQCHIP1: Fatal error pqt_min_free_cnt is zero Jan 9 08:16:47.295 router fpc0 CMSNG: Fatal ASIC error, chip TQ Jan 9 08:16:47.295 router fpc0 TQ Chip::FATAL ERROR!! from PQT free count is zero Jan 9 08:16:47.380 router alarmd[2427]: Alarm set: FPC color=RED, class=CHASSIS, reason=FPC 0 Fatal Errors - TQ Chip Error code: 0x50002 Jan 9 08:16:47.380 router craftd[2051]: Fatal alarm set, FPC 0 Fatal Errors - TQ Chip Error code: 0x50002 The Junos OS Chassis Management error handling detects such a condition, raises an alarm, and disables the affected Packet Forwarding Engine entity. To recover this Packet Forwarding Engine entity, restart the FPC. Contact your Juniper support representative if the issue persists even after the FPC restarts. PR1254415

- 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

- `TALUS(number) PCIe(number) DMA RX interrupt received. Queue stuck status 0xeeeeeee0` are spurious messages which are triggered in system logs due to queue-back pressure or FPGA drops. PR1465888

- With NAT/Stateful-firewall/TCP tickle (enable by default) configured on MS-MPC/MS-MIC, the vmcore crash sometimes along with mspmand crash might happen if large-scale traffic flows (e.g. million flows) are processed by it. PR1482400

- When there are hardware 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. PR1492605

- 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

- PR1463859 introduces a software defect that causes a 10GE interface to flap continuously when configuring with the WAN-PHY framing with the default `hold-down` timer (0). Once upgrading a router to an affected software release, the interface might flap continuously. This is not applicable to an interface with the default framing - LAN-PHY. PR1508794

- 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 configuration 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 incorrectly 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

- Due to BRCM KBP issue route lookup might fail. Need to upgrade KBP to address this issue. PR1533513

- If vMX product is configured to run in performance mode via configuring `chassis fpc 0 performance-mode` (Note: performance mode is enabled by default starting from Junos OS Release 15.1F6), flow cache will be used to improve the traffic forwarding performance. With performance mode enabled, if traffic cause a single flow in the flow cache to have a large number of flow actions which hit the max supported number (that is, 18) of flow actions. Typically, the addition of lots of firewall counters and policers in a single flow can make it add up. The riot might crash. It is a rare issue. PR1534145

- In scaled MX2020 router, with vrf localisation enabled, 4 million nexthop scale, 800k route scale. FPCs might go offline on GRES. Post GRES, router continues to report many fabric related CM_ALARMs. FPC might continue to reboot and not come online. Rebooting master and backup Routing Engine will help recover and get router back into stable state. PR1539305

- On MX platforms with MS-MPC/MS-MIC service card installed, the card might run out of memory due to process mspmand memory leak, which might cause traffic interruption if adding and/or deleting of telemetry sensor. This is because these operations will trigger the memory allocation for decoding configuration change messages and will not release the memory at the end of processing. PR1540538

- During RE switchover interface flap might be seen along with Scheduler slippage. PR1541772

- USF-SPC3 : With ipsec PMI/fat-core enabled, `show services sessions utilization` CLI not displaying right 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 happens from one source to another source. MPCE7 would pass real network SyncE switchover and associated transient mask. PR1557999

- 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 might display the session status as Invalid. This 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

- When Inline Jflow is configured and high sampling rate (more than 4000 per second) is set, high CPU utilization might 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

- Copying files to **/tmp/** causes a huge JTASK_SCHED_SLIP. Copy files to **/var/tmp/** instead. PR1571214

- This issue is caused by /8 pool with block size as 1, when the configuration 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

- In a fully loaded devices, at times, firewall programming was failing due to scaled prefix configuration with more than 64800 entries. However, this issue is not observed in development setup. PR1581767

- Error message seen on MX10K8 chassis with SyncE/PTP configurations, This does not affect any functionality. The error seen here because the API called is specific to ferrari platform which needs to be vecterized. PR1583496

- 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 OS Release 19.1R3-S5-J3, the subscriber logical interface (IFL) might be in a stuck state after the Extensible Subscriber Services Manager (ESSM) deletion. PR1591603

- Pim Vxlan not working on TD3 chipsets enabling VxLAN flexflow after Junos OS Release 21.3R1. Customers Pim Vxlan or data plane VxLAN can use the version 21.3R1. PR1597276

- MX2010, MX2020: MPC11E: unified ISSU is not supported for software upgrades from Junos OS Release 21.2 to release 21.3 and 21.4 releases due to a flag day change. PR1597728

- During Routing Engine 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 Series Virtual Chassis platforms with MS-MPC or SPC3 service cards and Aggregated Multi-Service (AMS), traffic on the line card in the backup chassis might 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

- Leaf difference with regards to memory-usage/heap in the output of Sensor (/junos/system/linecard/firewall) between MPC7E and MPC10E. PR1606791

- On all MX platforms, in a subscriber management environment, new subscribers might not connect if Class of service (CoS) CR-features (Classifier Rewrite) are used by the Variable Based Flow (VBF) service. The reference count mismatching between Routing Engine (RE) and VBF is caused by VBF flow VAR CHANGE failure. PR1607056

- If RPD Agent sends INH deletion/additions out of order (rarely occurs) to backup RPD, RPD generates core files. PR1607553

- NPU and IFL sensors path not programmed on AFT and EVO based LC. PR1610766

- When user tries to disable AMS ifd using configuration statement, 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

- Percentage physical-interface policer is not working on AE, after switching between baseline configuration to policer configuration. PR1621998

- Tunnel statistics displays incorrect values because it was not supposed that tunnel interfaces would cache flow. PR1627713

- On all Junos platforms the MAC address of the 17th ae interface might be changed after the upgrade from Junos OS 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 OS Release 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 configuration to allow internal trusted communication. Ref https://kb.juniper.net/TSB18224 PR1629943

- 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

- Same vlan cannot be used as data vlan and voip vlan together. PR1637195

- With SFP+-10G-CU3M DAC, peer cannot detect admin down on MX10008. PR1640799

- The mspmand daemon running on MS-MPC/MS-MIC cards might occasionally crash when the service card (fpc/pic) is turned offline and then online at regular intervals when the number of service-set configured is moderately high and when extensive hardware crypto operations are being performed. Exact issue is yet to be isolated. PR1641107

- Source MAC should not 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

- Committing configuration changes during the Packet Forwarding Engine reset pause window (when PFE is disabled, yet the PFE reset proper has not started yet) has the potential of causing errors and traffic loss. In particular, configuration changes that result in re-allocating policers (which are HMC-based) might lead to traffic being entirely policed out (that is, not flowing). Once the PFE reset procedure has started configuration 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-device`. PR1645075

- On Junos platform, PTP does not lock when port speed is not configured under PIC hierarchy or port speed for some additional random ports are configured under the PIC hierarchy or perform PIC deactivate/activate. PR1645562

- 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 (For example, 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

- It is non impacting message in journal logs, without any functional impact. Removing all .include inclusions from service files, via this PR.PR1647592

- In the IPv6 segment routing deployment, packets are sent out with the incorrect ethernet type. PR1647622

- Configuring MPC11 in 4x100G and keeping peer in 400G mode, Link comes up on peer while staying down on local end. This issue is also specific to 400G-ZR optics as it has single media lane. The issue is not seen on other 400G optics supporting 4x100G mode.PR1653946

- When interop with the following systems, flow control must be enabled when MACsec is configured on the peer system. Because on these systems, flow control is forced to be on regardless of the CLI provisioning. Other Reference (already documented) https://www.juniper.net/documentation/us/en/software/junos/security-service s/topics/ref/statement/interfaces-edit-security-macsec-mx-series.htmlPR1655712

- Currently user can install images older that the minimum supported image on RE-S-X6-128G-K. System comes up in Linux prompt in such cases.PR1655935

- Core file reported intermittently where random grpc stack crash is observed. The license service will auto restart and recover. PR1656975

- UDP Telemetry output fields might misalign on AFT-based line cards such as MPC10/11 or Junos Evolved platform. PR1658017

- ZTP: DHCPACK not received at ztp-server after zeroize of the device (client). PR1658287

- On Junos platforms, in the VPLS environment when having `routing-options resolution preserve-nexthop-hierarchy` configured results in the packet dropped at egress PE for multiple MPLS stack labels. PR1658406

- SNMP MIB walk on jnxVpnInfo `show snmp mib walk jnxVpnInfo` for EVPN or EVPN-VPWS routing instance. PR1659466

- On configuring `network-services lan` and performed commit check, the system changes the Layer 2 structures and family bridge disappeared from CLI.PR1661057

- The OpenSSL project has published security advisories for multiple vulnerabilities resolved in OpenSSL. Please Refer to https://kb.juniper.net/JSA70186 for more information.PR1661450

- When there is hard failure on the RE-RE link, the system might fail to recognise the fault and report as an alarm. PR1661635

- Traffic drop observed for few instances while it send via irbv6 routed interface.PR1662620

- 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.PR1662691

- If the physical link status of the ethernet link between the RE and FPC goes down, there are recovery attempts to bring up the link again. Log messages indicate the recovery attempts and the success/ failure status of the attempt. However an alarm is not raised when this failure occurs. PR1664592

- RE0 to RE1 interface EM4 MTU is changed to 9192 bytes through PR 1642364. If one of the REs don't have this fix, RE sync fails. Due to this reason, ISSU will not work. In such scenario, cold image upgrade should be done. PR1665690

- UDP Telemetry might not work when subscribes to **/junos/system/linecard/intf-exp/** sensor. PR1666714

- On MX platforms with MIC-MACSEC-20GE, FEB(Forwarding Engine Board) might go down while activating/deactivating Graceful Routing Engine Switchover (GRES) configuration.PR1668983

- These are expected error logs, and doesn't cause any functional impact. `jsr_iha_pri_unrepl_msg_func: Error: Invalid primary handle in msg 0x10006c600000621, error=2` These logs might be seen if the following conditions are met:

  On all Junos OS platforms

  non stop routing is enabled

  with scaled setup

  The possible triggers would be restart chassisd, ksyncd, switchover, re reboot, which causes nsr unreplication/replication. PR1675057

- The issue was recreated only with IXIA connection. Arp response is not received in the DUT port to store the destination MAC address. unable to determine if the issue is with the MX port or medium or IXIA port. PR1677624

- The IFD remaining stats 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

- On all MX platforms with MPC7E-10GE line card, auto-negotiation will not be set properly when changing the port speed from 10GE to 1G on a port with auto-negotiation configured. The port remains down until the commit is done separately for changing the port speed.PR1682962

- One time l2ald (Layer 2 Address Learning Daemon) core will be seen once the box comes up after zeroize. There will be no service impact due to this.PR1686097

- On all Junos and Junos Evolved platforms, configuring Link Layer Discovery Protocol (LLDP) with `system services netconf notification` enabled will trigger the l2cpd crash. This crash causes the CPU to spike. PR1695057

- On all Junos platforms, the dcd (device control daemon) process crash is observed when more than 256 VLANs as name tags are added on the same interface.PR1696428

- FIPS mode is not supported in this release.PR1697999

- The optic configuration mismatch alarm was always enabled, but was not reported by the RE during `show chassis alarms`. This alarm will now be correctly reported by the FPC and displayed in the RE. There is no behavior change other than the alarm being reported correctly now.PR1700606

High Availability (HA) and Resiliency

- When GRES is performed with the interface em0 (or fxp0) disabled on the primary Routing Engine, then enable the interface on the new backup Routing Engine, it isn't able to access network.PR1372087

Infrastructure

- Below IPC timeouts logs can be seen for statistics query to kernel(queried from cli or daemons querying internally)when there is config churn, or large number of IPCs getting exchanged between kernel and pfe 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 larger value by setting below hidden config to avoid IPC timeout errors. `# set system stats-timeout-lifetime 15 # commit`. PR1629930

Interfaces and Chassis

- On MX platforms with Subscriber Management configured, the subscribers will fail to negotiate the PPP (Point-to-Point Protocol) session and be unable to login when jpppd transitions from backup to Master and does not receive all the Routing Table events from Kernel post upgrade.PR1686940

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 and Junos OS Evolved platforms, if CCC (Circuit Cross-Connect) is configured to use a label-switched-path such as IGP routed, i.e., no-cspf and no strict ERO (Explicit Route Object) configuration, then restarting egress CCC node or restarting FPC on the egress CCC node containing remote-interface-switch configuration multiple times may cause CCC to remain stuck in remote-if-down state, resulting in loss of traffic. (The knob `remote-interface-switch` is configured on the egress LER of the RSVP-TE LSP (Resource Reservation Protocol-Traffic Engineering label-switched-path) which binds the LSP terminating on the node to a local interface).PR1694777

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. (Ideally 'ok/' tag should not be emitted in an error scenario.) The configuration does not get committed.PR1585855

- On Junos and Junos Evolved platforms, post ephemeral database configuration commit sync leads to a state mismatch between master and backup.PR1610713

Platform and Infrastructure

- On all Junos 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 would be a loopback address. The problem does not apply to automatically generated NTP poll packets. PR1545022

- On MX platform, when the "fast-lookup-filter" statement is configured with a match that is not supported in the FLT(fast-lookup-filter) hardware, traffic might be lost.PR1573350

- Don't use the control-type light under platforms where this feature is not supported at present. At present IPv4 and IPv6 twamp-light is supported on the platforms using TRIO and PE chipsets. PR1603128

- VM cores and Virtual Chassis split might be observed with multicast scale scenario. PR1614145

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

- On SRX5k and MX240/MX480/MX960 platforms,when device is powered on with multiple line cards, power might not be sufficient and few line cards fail to come into online state.PR1645817

- The process sshd will crash if Terminal Access Controller Access Control System (TACACS) user authentication is configured and the user is successfully authenticated by the TACACS server. The crash occurs with every successful authentication and an sshd coredump will be created. Because of the core ssh access is denied. PR1672581

- On Junos with MX platform using specific MPC7E/MPC8E/MPC9E/JNP10K-LC2101/JNP10003-LC2103/JNP10K-LC480 line cards in the event of a transient memory hardware issue, parity errors are generated which cannot be rectified by the ASIC. When the Flexible PIC Concentrators(FPC) encounters such an error, it will automatically deactivate the Packet Forwarding Engine(PFE) which leads to traffic impact. PR1706494

Routing Protocols

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

- LDP OSPFs are in the Synchronization state because the IGP interface is down with ldp-synchronization enabled for OSPF. PR1256434

- On MX platforms, unexpected log message will appear if the CLI command `show version detail` or `request support information` is executed.PR1315429

- On all platforms, the issue is when the first time when ESIS is coming up sometimes the ESIS route might not get installed. PR1559005

- On MX platforms, initial multicast register packets might get dropped, this might affect multicast services. PR1621358

- On all Junos and Junos OS Evolved platforms, when configuring the network instance for openconfig, an error might be observed while executing a commit if the configured network instance type is "default_instance" but the instance name is not default.PR1644421

- RFC 8950/RFC 5549, permits the advertisement of a BGP Nexthop of a different family (e.g. IPv6) than the NLRI address family (e.g. IPv4). The mapping of possible address families that can be used are exchanged using BGP Capabilities. The BGP Capabilities specification, RFC 5492, recommends that a single capability TLV of a given type is advertised when multiple elements within that TLV are present. That RFC also permits multiple capabilities of the same type to be advertised for multiple elements for backward compatibility. Junos BGP handling of the BGP extended nexthop capability did not handle multiple capabilities of the same code point when multiple extended nexthop capabilities were present. It incorrectly kept only the last one sent. This PR addresses that deficiency. PR1649332

- The `show security keychain detail` CLI displays algorithm as hmac-* instead of ao.PR1651195

- When l2cpd (in the context of xSTP) clears the entries that it has programmed on ppmd, ie when you delete xSTP configs from the box, there can be a possibility of ppmd core. If ppmd is in distributed mode then there will be no service impact, else there can be service impact as packet transmission for various protocols will happen via if ppmd is in centralized mode.PR1660299

- The rpd (routing protocol daemon) crash happens when a non-BGP (Border Gateway Protocol) route is exported via LDP (Label Distribution Protocol) and later on, if the same prefix advertised by BGP is received, we select that as the forwarded route rather than the already advertised route. This is due to the logic in the forwarding route to pick the BGP route for the BGP-owned routes rather than the active route. This is a rare case and the system recovers by itself until the next event.PR1671081

- Dynamic IFL add request is waiting to be processed in KRT queue during that if chassid down event occurs. To handle the chassid down event RPD Infra sends notification to protocol(producer of Dynamic IFL add request) and it is producer jobs to DELETE the dynamic ifls request which were there in the KRT queue. PIM code is not clearing those Dyanamic IFLs ADD request during chassis fpc down event. Hence getting error 'ENOENT -- Item not found' when chassis comes back up.PR1675212

- Any platforms with Micro BFD configured on member links of the LAG/ae interface, BFD Session state in RE remains as UP always even though PEER device has ceased.PR1675921

- On all Junos and Junos Evolved platforms, the rpd (routing protocol daemon) can crash when PIM (Protocol Independent Multicast), MoFRR (Multicast only Fast Reroute) 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 (Equal Cost Multi-Path) happens. There will be service impact because of the rpd crash but the system self-recovers until the next crash.PR1676154

- VRF Rouging table might not get updated immediately upon change of maximum-prefixes. PR1680277

- OSPF Route Type Extended Community cannot be configured as 'rte-type'. PR1687273

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

- On Junos and Junos Evolved platforms configured with graceful-shutdown sender under the BGP dynamic neighborship, the peer device does not receive routes with communities "graceful-shutdown", as it is not advertised by the sender causing the traffic drop for the affected routes.PR1699633

- On all Junos and Junos Evolved platforms, when 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 incorrect path due to this issue. PR1702456

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 might 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

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

- With inter area/AS segmented scenario the provider tunnel termination interface on ASBR/ABR is set to global lo0 and added to tai data structure. However if there is a change in lsi/vt interface, specifically causing deletion of interface, in change notification callback MVPN tries to delete tai data structure with lsi/vt interface and not lo0 since this is inter area/AS segmented scenario. Since lsi/vt was never added, the code asserts. PR1710255

Resolved Issues

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

Class of Service (CoS)

- 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 (AE) link flaps on MX 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

- Layer 3 inter-subnet routing will fail if there is no reachability for the remote IP-host route. PR1669585

- EVPN MPLS traffic drop can be observed in a multi-vendor PE CE setup with single-active LAG. PR1680421

- Routing Protocol Daemon (RPD) core files is observed due to remote bgp routes being flashed as active routes. PR1692249

- A configuration change caused a rpd core dump for the EVPN migrated instance. PR1701632

- 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 19.2~21.1 to 22.2R1. PR1661935

General Routing

- FPC might generate core files if CFM flap trap monitor feature in use. PR1536417

- MPC10E: Quick 100G link-flaps has still some race conditions which can cause MQSS stream drain failures and xqss_sched_flush_queue failures. PR1642584

- Bugatti: RCB: system does not got to shell prompt and hangs before rebooting after pressing N during PXE installation. PR1647534

- The MPC/FPC might crash or the traffic might be silently dropped/discarded. PR1649499

- The user-defined speed does not take effect on the AE interface in certain scenarios on Junos 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

- UEFI BIOS Key synchronization tool - efitools.service failed after optics diagnostics test. PR1655537

- Telemetry is reporting In-Errors when knob "ignore-l3-incompletes" is configured. PR1655651

- DHCP packets getting looped in EVPN-VXLAN setup. PR1657597

- On LC2101 / LC480 line cards normal discard counter increasing (no traffic running through device). PR1658268

- Speed change from 10G to 1G on MX causes all other lanes to flap. PR1659087

- JSD crash is seen during cBNG container startup. PR1659175

- Some of ports on MX platforms with MPC7E-10G do not come up with 1G speed. PR1660154

- MX204 - SSH non-default port configuration causes FPC offline after upgrade to Junos OS Release 21.4. PR1660446

- The port LEDs do not light up when 40G physical interfaces are up. PR1660532

- GNF : No streaming data received for **/telemetry-system/subscriptions/dynamic-subscriptions/**. PR1661106

- In the EVPN-VXLAN scenario, the DHCP packets will get dropped when the DHCP relay agent is configured. PR1662524

- The rpd core might be seen when there is a synchronization issue. PR1663050

- 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 the VRRP is configured over the AE interface. PR1666853

- Type-5 routes might not get programmed in PFE when the number of active interfaces and Vlan configured is high. PR1668352

- jsd memory leak and may lead jsd restart. PR1669426

- Multibit ECC error causes the whole MX platform chassis to go down. PR1670137

- EVPN multicast traffic might 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 might be 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

- Issue with eth-lldp-stop.sh after junos upgrade performed in PTX5000(i40e-NVM). PR1675177

- Observed spmbpfe core on RE1 when installed image on both the REs. PR1675268

- PFE core files is seen when the CPCD service is modified. PR1675985

- MPC stuck in present state with log " graceful offline in progress, returning false" flooding. PR1676008

- The traffic doesn't re-route quickly causing traffic getting dropped silently. PR1676740

- Traffic drop might be seen on MX platforms with MPC10E-10C line card. PR1676777

- PFE memory usage gets impacted after GRES. PR1678217

- The `show interfaces diagnostics optics interface` shows all 0 on 100/400G port on MPC10E card. PR1678716

- The LLDP packets will not be transmitted over l2circuit on the ACX platform. PR1678752

- The process bbe-smgd on the router would stop processing new PPPoE subscribers session. PR1680453

- Traffic drop would be observed only when the backup link is up on link-protection LAG interface. PR1680889

- The PFE process crashes from 21.4R1 version onwards on VMhost platforms. PR1681532

- Traffic loss is seen with port-mirroring is enabled on AE interface in multicast downstream. PR1683192

- The `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

- jnxOperatingDescr.1.1.0.0 returns blank, but jnxOperatingState.1.1.0.0 returns value. PR1683753

- srv6-oam: 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

- Traffic might hit incorrect queue post ISSU. PR1684019

- The l2cpd process crash might be observed when disabling RSTP on an interface. PR1684072

- An interface configured as 1G might flap on a port with the mixed speeds of 1G and 10G after a PIC restart. PR1684728

- Insufficient space for vm core files for JUNOS VM. PR1684968

- TI-LFA backup path is not computed which effects slow convergence in case of failures. PR1685064

- Multiple bbe-smgd core files might be observed resulting in subscribers being lost or failing to login in the Enhanced subscriber scenario. PR1685070

- license-check might core files on MX routers. PR1685433

- PICs on the GNF failed to come online after the chassisd restart. PR1685453

- Illinois: K8 CP: Telenor Norway CST: `bbe-smd-cpd core (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

- With BMP RIB-IN and BMP RIB-OUT configured on MX or PTX Platforms, large number of BGP routes remain in Holddown state after route churn. PR1685510

- The rpd crash might 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. 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

- CoS memory errors are seen when `chassis traffic-manager enhanced-priority-mode` is configured. PR1687642

- The FPC crash is observed with a "flexible-match-mask" condition. PR1687862

- On Junos and Junos 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 and Junos OS Evolved platforms. PR1688023

- A kernel crash can be seen with MIC-3D-8DS3-E3 installed. PR1688315

- The LACP would 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

- The "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 hits an unresolved destination PR1690679

- Use latest os-package when upgrading. PR1691209

- The process rpd crash will be observed with the SR-TE tunnel delete. PR1691459

- PCS errors and framing errors on 100GE interfaces on certain Juniper platforms. PR1692063

- The firewall bridge filter policers (attached to AE interface) are not working on all Junos MX 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

- The fxpc core files is generated and an FPC restart results in traffic impact. PR1692993

- MACSec session will not come up on the new fallback key during the primary key transition. PR1693301

- Traffic loss is observed when the ECMP path is IRB over AE (IPv4->MPLS). PR1693424

- Traffic loss will be seen when MACSEC is configured. PR1693730

- NDP cannot resolve neighbor after clearing IPv6 neighbor. PR1694009

- dot1xd.core-tarball.0.tgz is observed in Junos OS Release 22.1R3 at #0x009113f0 in __mem_assert(). PR1694129

- License-check warning reported on backup RE by commit or commit check. PR1694935

- BMP EOR is sent with incorrect peer address causing BMP failure. PR1695320

- MPC11E goes offline with "fpc-slice" configured. PR1695510

- Occassionally, after a chassis power cycle, the backup Routing Engine is in Present state and the `Loss of communication with Backup RE` alarm is seen. PR1696816

- The dot1x authentication will not be enabled on interfaces with specific configuration combination. PR1696906

- In the rare scenario, huge PTP Time errors are introduced and propagated to the downstream devices after the chassis reboot. PR1696957

- FPC crash will be observed when firewall filter is unconfigured and reconfigured with same index. PR1697404

- jkey path changed under protocol/isis. "levels" is missing. PR1698192

- On Junos platforms MPLS resolving over IPV6 route traffic drop is seen. PR1698516

- Transit tunnels fails and remains down on all Junos based MX and SRX platform with IKE-NAT-ALG enabled. PR1699115

- Output of `show chassis ethernet-switch statistics` includes 32 bit values which might overflow. PR1699136

- The rpd crash is observed when rib-sharding configured. PR1699557

- FPC restart and core files 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 platforms with MS-MPC cards the IKE ALG inactivity timeout value stays fixed. PR1701305

High Availability (HA) and Resiliency

- The rpd crash will be observed when any commit is performed. PR1701146

Interfaces and Chassis

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

- The PFE I/O 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

- Node Slicing: In a rare scenario, the FPC/SLC will get stuck in the ready state after a restart. PR1682271

- 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 AE ifl having child links on Satellite Device stops transmission post GRES. PR1697394

- MX Series Virtual Chassis: The backup Virtual Chassis router could become master after the system reboot. PR1697630

Juniper Extension Toolkit (JET)

- The connection might get closed by the collector when connecting to jsd. PR1653968

Layer 2 Ethernet Services

- MX240:Verify VRRP stats is failed after Deactivate the Access interface. PR1666943

- DHCP packets sent to the client have the Option 82 Suboption length set to 0. PR1684521

- IPv4 ALQ not working with authentication. PR1688272

- A dcd process crash is observed continuously when the dhcp-service is restarted. PR1698798

MPLS

- RSVP refcount leak and the rpd crash observed post LSP churn. PR1621771

- The error severity of syslog message `ted_client reset` generated during commit is incorrect. PR1649565

- The rpd core files is seen due to IGP database and BGP LS database out of sync. PR1655031

- The rpd crash would be observed in a RSVP scenario. PR1661526

- 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 will be blackholed when the L-ISIS/L-OSPF route changes due to interface level configuration. PR1671187

- CPU utilization of rpd process might reach 100% 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 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 and Junos 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

- AE (aggregated ethernet)interface beyond 1099 are allotted 0 snmp index. PR1683264

Platform and Infrastructure

- The core interface goes down. PR1631217

- The MPC hosting an AE member interface with a shared bandwidth policer configured at the AE could crash upon encountering an HMC fatal error. PR1666966

- Traffic drop is be observed with layer 2 circuit local switching with PS interface. PR1669410

- Traffic drop observed 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/IPv6 (e.g. 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

- The interface on the device will go down when one or more interfaces are connected to the Advantech3260 device at another end. PR1678506

- The traffic loss duration increases during the LSP switchover. PR1681250

- BGP session flap with error BGP_IO_ERROR_CLOSE_SESSION. PR1685113

- PFE 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

- The egress rewrite-rule might not work as expected for traffic entering the AE interface. PR1700860

Routing Protocols

- Junos OS and Junos OS Evolved: RPD crash upon receipt of specific OSPFv3 LSAs (CVE-2022-22230). PR1645221

- Incorrect next-hop weight might be observed with BGP PIC enabled. PR1652666

- SSH access is possible without ssh setting. PR1664512

- BGP labeled-unicast inactive routes might not be advertised when add-path is configured. PR1665610

- RPD crash might be observed due to multiple sequences of flap events. PR1669615

- Source/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

- 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

- 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 flap. PR1679950

- On single PFE with Fusion satellite, LACP is not sending PDUs. PR1687395

- BMP will not send EOR message. PR1690213

- Backup Path is Not Found in ASBR6 MPLS Table while verifying BGP Multipath Protection functionality. PR1691131

- The rpd crash is seen when using a BGP neighbor telemetry subscription in a sharding environment. PR1692255

- Silent drop of traffic is observed when removing the BGP routes take a long time to get removed from RIB. PR1695062

- Commit error when trying to configure rib-group under BGP in no-forward (default) RI. PR1696576

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

- The BGP Auto-discovered neighborship is not formed after a reboot. PR1699233

- OSPF stuck in InitStrictBFD state for the neighbor which doesn't send LLS header. PR1700966

- Anycast PIM doesn't work when the peer has an authentication key configured for MSDP. PR1703707

- 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

VPNs

- Traffic over IPSec tunnels might be dropped during unified ISSU. PR1416334

- The multicast receiver receives no traffic in an extranet scenario having an SPT tree already established. PR1675099

- Core files are observed with multiple daemons restart. 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.

Basic Procedure for Upgrading to Release 22.2R3

> ⓘ **NOTE**: Before upgrading, back up the file system and the currently active Junos OS configuration so that you can recover to a known, stable environment in case the upgrade is unsuccessful. Issue the following command:
>
> ```
> user@host> request system snapshot
> ```
>
> The installation process rebuilds the file system and completely reinstalls Junos OS. Configuration information from the previous software installation is retained, but the contents of log files might be erased. Stored files on the routing platform, such as configuration templates and shell scripts (the only exceptions are the juniper.conf and ssh files might be removed. To preserve the stored files, copy them to another system before upgrading or downgrading the routing platform. For more information, see the Installation and Upgrade Guide.

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

Procedure to Upgrade to Junos OS

To download and install Junos OS:

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

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

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

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

4. Select the Software tab.

5. In the Install Package section of the Software tab, select the software package for the release.

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

7. Review and accept the End User License Agreement.

8. Download the software to a local host.

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

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

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

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

- For 32-bit Routing Engine version:

```
user@host> request system software add no-validate reboot source/junos-install-mx-
x86-32-22.2R3.9-signed.tgz
```

- For 64-bit Routing Engine version:

```
user@host> request system software add no-validate reboot source/junos-install-mx-
x86-64-22.2R3.9-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-
x86-32-22.2R3.x-limited.tgz
```

- For 64-bit Routing Engine version:

```
user@host> request system software add no-validate reboot source/junos-install-mx-
x86-64-22.2R3.9-limited.tgz
```

Replace source with one of the following values:

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

- For software packages that are downloaded and installed from a remote location:

  - **ftp://***hostname***/***pathname*

  - **http://***hostname***/***pathname*

  - **scp://***hostname***/***pathname*

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

Rebooting occurs only if the upgrade is successful.

> ⓘ **NOTE**:
> - You need to install the Junos OS software package and host software package on the routers with the RE-MX-X6 and RE-MX-X8 Routing Engines. For upgrading the host OS on these routers with VM Host support, use the junos-vmhost-install-x.tgz image and specify the name of the regular package in the `request vmhost software add` command. For more information, see the VM Host Installation topic in the Installation and Upgrade Guide.
>
> - Starting in Junos OS Release 22.2R1, in order to install a VM host image based on Wind River Linux 9, you must upgrade the i40e NVM firmware on the following MX Series routers:
>
>   - MX240, MX480, MX960, MX2010, MX2020, MX2008, MX10016, and MX10008
>
>   [See https://kb.juniper.net/TSB17603.]

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

Upgrade and Downgrade Support Policy for Junos OS Releases and Extended End-Of-Life 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 EEOL releases only, you have an additional option - you can upgrade directly from one EEOL release to the next two subsequent EEOL releases, even if the target release is beyond the next three releases. Likewise, you can downgrade directly from one EEOL release to the previous two EEOL releases, even if the target release is beyond the previous three releases.

Table 6: EOL and EEOL Releases

Release Type	End of Engineering (EOE)	End of Support (EOS)	Upgrade/ Downgrade to subsequent 3 releases	Upgrade/ Downgrade to subsequent 2 EEOL releases
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 22.2R3

To downgrade from Release 22.2R3 to another supported release, follow the procedure for upgrading, but replace the 22.2R3 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 22.2R3 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 this release for NFX Series devices.

What's Changed

There are no changes in behavior and syntax in Junos OS Release 22.3R3 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.

General Routing

- On the NFX150 devices, after loading 22.2R1.1, the fablinks go down and the cluster status displays an FL.PR1664636

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

- On the NFX350 device, even though the ethernet cable is physically plugged in and the `show interface` `command` displays Front panel LED status as `up`, the front panel LED is not ON. PR1702799

Resolved Issues

IN THIS SECTION

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

Virtual Network Functions (VNFs)

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

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 droppedPR1691694

Migration, Upgrade, and Downgrade Instructions

IN THIS SECTION

- Upgrade and Downgrade Support Policy for Junos OS Releases and Extended End-Of-Life Releases | 84
- Basic Procedure for Upgrading to Release 22.2 | 84

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.

> (i) **NOTE**: For information about NFX product compatibility, see NFX Product Compatibility.

Upgrade and Downgrade Support Policy for Junos OS Releases and Extended End-Of-Life 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 EEOL releases only, you have an additional option - you can upgrade directly from one EEOL release to the next two subsequent EEOL releases, even if the target release is beyond the next three releases. Likewise, you can downgrade directly from one EEOL release to the previous two EEOL releases, even if the target release is beyond the previous three releases.

Table 7: EOL and EEOL Releases

Release Type	End of Engineering (EOE)	End of Support (EOS)	Upgrade/ Downgrade to subsequent 3 releases	Upgrade/ Downgrade to subsequent 2 EEOL releases
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.

Basic Procedure for Upgrading to Release 22.2

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 22.2R3:

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

These release notes accompany Junos OS Release 22.2R3 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

Learn about what changed in this release for PTX Series.

Network Management and Monitoring

- **Support for the `junos:cli-feature` YANG extension (ACX Series, EX Series, MX Series, PTX Series, QFX Series, SRX Series, vMX, and vSRX)**—The `cli-feature` YANG extension identifies certain CLI properties associated with some command options and configuration statements. The Junos YANG modules that define the configuration or RPCs include the `cli-feature` extension statement, where appropriate, in schemas emitted with extensions. This extension is beneficial when a client consumes YANG data models, but for certain workflows, the client needs to generate CLI-based tools.

  [See Understanding the Junos DDL Extensions YANG Module.]

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).]

User Interface and Configuration

- **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 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.

MPLS

- The automatic sorting of configuration entries do not work if defined under group. PR1637730

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 SRTE or FlexAlgo. PR1648490

User Interface and Configuration

- On all Junos OS 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

Open Issues

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

- On the PTX platform with FPC-PTX-P1-A or FPC2-PTX-P1A, you might encounter a single event upset (SEU) event that might cause a linked-list corruption of the TQCHIP. The following syslog message gets reported: Jan 9 08:16:47.295 router fpc0 TQCHIP1: Fatal error pqt_min_free_cnt is zero Jan 9 08:16:47.295 router fpc0 CMSNG: Fatal ASIC error, chip TQ Jan 9 08:16:47.295 router fpc0 TQ Chip::FATAL ERROR!! from PQT free count is zero Jan 9 08:16:47.380 router alarmd[2427]: Alarm set: FPC color=RED, class=CHASSIS, reason=FPC 0 Fatal Errors - TQ Chip Error code: 0x50002 Jan 9 08:16:47.380 router craftd[2051]: Fatal alarm set, FPC 0 Fatal Errors - TQ Chip Error code: 0x50002 The Junos OS Chassis Management error handling detects such a condition, raises an alarm, and disables the affected Packet Forwarding Engine entity. To recover this Packet Forwarding Engine entity, restart the FPC. Contact your Juniper support representative if the issue persists even after the FPC restarts. PR1254415

- On routers and switches running Junos OS platform, with Link Aggregation Control Protocol (LACP) enabled, deactivating a remote Aggregate Ethernet (AE) member link makes the local member link move to LACP detached state and cause traffic drops on that member link. The same scenario applied when a new member link is added where the other end of that link is not yet configured with LACP. PR1423707

- In Link aggregation groups (LAGs) Enhanced link aggregation group (a.k.a. Aggregated Ethernet child NH reduction/AE Simple/LAG Enhanced) scenario, if FPC hosting single child member AE bundle is rebooted, the aggregate next-hops on such AE bundles might be discarding traffic, as the IFL reroute

tables might get stuck in the down state, the packets drop might be seen on all other FPCs that the ingress traffic towards such AE bundles and the AE interfaces might not be used. PR1551736

- Unsupported configuration is being attempted by the script that then hits the maximum threshold for the given platform PTX5000. PR1555159

- On PTX platforms, when Inline Jflow is configured and high sampling rate (more than 4000 per second) is set, high CPU utilization might be observed and this might result in relevant impacts on traffic analysis and billing. PR1569229

- Copying files to /tmp/ causes a huge JTASK_SCHED_SLIP. Copy files to /var/tmp/ instead. PR1571214

- Tunnel statistics displays incorrect values because it was not supposed that tunnel interfaces would cache flow. PR1627713

- When sending BGP Labeled Unicast (BGP-LU) traffic or Layer 3 VPN traffic over IPIP tunnels, if the remote end device is a purely IP device that does not understand labels, the labeled unicast or Layer 3 VPN label cannot go on top. PR1631671

- V6 default route will not get added after successful dhcpv6 client binding on PTX1000 router during ZTP. PR1649576

- ZTP: DHCPACK not received at ztp-server after zeroize of the device (client). PR1658287

- When an FPC (Flexible PIC Concentrator) on PTX5000 platforms is shut down by issuing a request command (request chassis offline slot <slot-number>) or by FPC power off configuration (set chassis fpc x power off), it gets stuck in the **Announce Offline** state since the associated timer (fru_graceful_offline_timer) doesn't increment and expire as it is supposed to.PR1683562

Multicast

- On Junos PTX platforms there might be a traffic that is silently dropped and discarded which happens because of next-hop installation failure for multicast RSVP(Resource Reservation Protocol) P2MP(Point to Multipoint) traffic. This issue might only be encountered in a scaled RSVP P2MP environment after a network event which might cause reconvergence. PR1653920

Routing Protocols

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

Resolved Issues

IN THIS SECTION

- General Routing | **91**
- MPLS | **92**

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

General Routing

- IS-IS adjacency is not coming up through TCC l2circuit. PR1590387

- The user-defined speed does not take effect on the aggregate Ethernet interface 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 and PTX5000 after Junos OS software upgrade. PR1669267

- The 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

- Issue with eth-lldp-stop.sh after Junos OS upgrade performed in PTX5000(i40e-NVM). PR1675177

- The Packet Forwarding Engine process crashes from 21.4R1 version onwards on VMhost platforms. PR1681532

- EX SNMP: 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 OS to 20.2R1 or later release might trigger intermittent link flapping. PR1693367

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 the RSVP-TE scenario, with entropy label capability is enabled during MBB issues handling Resv Messages. PR1681403

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 22.2

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 22.2R3:

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 `22.2` tab.

5. In the Install Package section of the Software tab, select the software package for the 22.2.

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-
x86-64-22.2R1.9.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-
x86-64-22.2R1.9-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 22.2 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 and Extended End-Of-Life 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 EEOL releases only, you have an additional option - you can upgrade directly from one EEOL release to the next two subsequent EEOL releases, even if the target release is beyond the next three releases. Likewise, you can downgrade directly from one EEOL release to the previous two EEOL releases, even if the target release is beyond the previous three releases.

Table 8: EOL and EEOL Releases

Release Type	End of Engineering (EOE)	End of Support (EOS)	Upgrade/ Downgrade to subsequent 3 releases	Upgrade/ Downgrade to subsequent 2 EEOL releases
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

These release notes accompany Junos OS Release 22.2R2 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

Learn about what changed in this release for QFX Series.

General Routing

- **New ARP and NDP packet classification (QFX10002, QFX10008, and QFX10016)**—We've introduced two control plane classes for ARP and NDP packets received over VTEP interface. When your device identifies a packet as ARP or NDP, it performs an ingress port check which verifies whether the VTEP interface receives these packets. If VTEP interface receives the packet, datapath re-writes the control plane class to the newly defined values. Based on this new control plane class, the system performs the remaining packet processing and forwards the packets toward the host path. The system adds a separate DDoS policer to this ARP traffic, which ensures that the ARP traffic is not triggering underlay ARP DDoS violation.

Network Management and Monitoring

- **Support for the `junos:cli-feature` YANG extension (ACX Series, EX Series, MX Series, PTX Series, QFX Series, SRX Series, vMX, and vSRX)**—The `cli-feature` YANG extension identifies certain CLI properties associated with some command options and configuration statements. The Junos YANG modules that define the configuration or RPCs include the `cli-feature` extension statement, where appropriate, in schemas emitted with extensions. This extension is beneficial when a client consumes YANG data models, but for certain workflows, the client needs to generate CLI-based tools.

  [See Understanding the Junos DDL Extensions YANG Module.]

Routing Protocols

- **AR replicators with OISM install multicast states only on the OISM SBD (QFX5130-32CD and QFX5700)**—In an EVPN-VXLAN ERB fabric with many VLANs, QFX5130-32CD and QFX5700 switches running as assisted replication (AR) replicators with optimized intersubnet multicast (OISM) might have scaling issues when they install multicast (*,G) states (with IGMPv2) or (S,G) states (with IGMPv3). As a result, these switches only install these multicast states on the OISM supplemental

bridge domain (SBD) VLAN. they don't install these states on all OISM revenue bridge domain VLANs. On those devices, you see multicast group routes only on the SBD in show multicast snooping route command output.

[See OISM and AR Scaling with Many VLANs].

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).]

User Interface and Configuration

- **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

IN THIS SECTION

- General Routing | **100**

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

- After configuring VxLAN on a physical interface, its always treated as VxLAN port even though L2 VLAN exists. PR1570689

- Unified ISSU on QFX5120-48Y and EX4650 switches will not be supported if there is a change in the Cancun versions of the chipset SDKs between the releases. This is a product limitation as change in the Cancun firmware leads to the chip reset and hence ISSU is impacted. The Cancun versions in the chipset SDKs should be the same between two Junos OS releases for ISSU to work. PR1634695

- The incoming VLAN tag is removed at ingress. So, it is not available at egress sampling.PR1654879

- For traffic dropped at egress due to split horizon in BCM during egress path processing, statistics are shown on vtep as statistics are fetched at ingress pipeline in BCM. PR1656400

- When VNI ranges spawn across two beta blocks, the programming ranges have limitations. The forwarding pipeline places the VNI ID along with the flags in the GRE key. This is specific to implementation and discrete nature of non-overlapping ranges, we recommend the allowed VNI ranges. Therefore, it is recommended to configure VNI matches as specific number or a list of VNIs instead of a range.PR1660623

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 all Junos OS 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 aaggregated Ethernet, it might trigger a Flexible PIC Concentrators (FPC) crash which leads to traffic loss. PR1688455

EVPN

- On all Junos OS and Junos OS Evolved platforms where EVPN feature is enabled, the l2ald process might crash in a rare scenario when a loopback IP address is changed.PR1631280

- While verifying, `show mac-vrf routing database instance User_mvs1 extensive` command "mobility-seq-num" is not as expected.PR1694943

General Routing

- When VLAN is added 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 and MX2010 doesn't 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, 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 a QFX5120, when you disable a protected link. You may see a delay of 200-400 mSec for the system to react to the disable link event.PR1579931

- In a fully loaded devices, at times, firewall programming was failing due to scaled prefix configuration with more than 64800 entries. However, this issue is not observed in development setup. PR1581767

- Management interface speed is displayed as 10G instead of 1G though there is no functionality impact. PR1589942

- 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 Junos OS Release 21.3R1. Customers Pim VxLAN or data plane VxLAN can use the Junos OS Release 21.3R1. PR1597276

- On QFX5100, optical power is seen after detached and attached QSFP on disable interface. PR1606003

- On QFX5120-48Y, when scaled config and baseline configs are loaded multiple times one after other without much wait time in between then traffic or protocols on pure L3 interfaces may behave in undefined/unexpected manner. PR1612973

- On Junos QFX10k platforms with scaled number of BFD (Bidirectional Forwarding Detection) sessions configured, addition of a new BFD session might cause flapping in newly added session and other existing BFD sessions.PR1621976

- QFX5110-32Q : Traffic loss seen after renumbering master in VCPR1632565

- Backup FPC lose their connection to the master when new members are added to the VCF (Virtual Chassis Fabric).PR1634533

- The bounded delay config feature for IFL is not supported on Pyrite platform. The core is seen only when this config is enabled on the device. PR1634941

- 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 a 100G interface on a QFX5120 is converted to a VC port, the interface stays down as the port is configured as 40G internally. PR1638156

- 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 Series platform, v6 logical interfaces statistics are being derived from the underlying physical interfaces statistics unlike on PTX Series where they are hardware assisted. Therefore, they are not very reliable and are at best, guesstimate. PR1653671

- After converting access side port from SP style to EP style, MAC-IP learning fails for a host and ARP doesn't get resolved. PR1658657

- QFX5100-24Q and EX4600 devices Virtual-chassis is in unstable state for 3-7 minutes causing traffic loss. PR1661349

- On all QFX Series platforms, 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 might go into a hung state and remain in that state even after the reboot is complete. This might affect traffic after the remote end system comes online and resumes traffic transmission.PR1665800

- On QFX5110 platforms with more than one Layer 2 circuit configured, deactivating and activating the l2circuit configurations successively might cause traffic drop on one or more L2 circuits. PR1666260

- Native VLAN with VLAN rewrite on same interface not supported. PR1671372

- On QFX5200, after NSSU upgrade for a 4 member Virtual Chassis, FPC might toggle resulting in interfaces going offline. PR1673116

- On QFX5120 Virtual Chassis with Open vSwitch Database (OVSDB) VxLAN topology, Address Resolution Protocol (ARP) resolution fails if the traffic passes through Virtual Chassis port (VCP) ports. As a result, ARP packets drops. PR1679684

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

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

- On all Junos OS platforms, the device control daemon (dcd) process crash is observed when more than 256 VLANs as name tags are added on the same interface.PR1696428

- On Junos QFX5110 and QFX5120 devices, a small number of packets are lost when assigned VNI (VXLAN Network Identifier) to the VLAN. There is a packet loss on incoming packets, but no packet loss on outgoing packets. PR1697244

Layer 2 Ethernet Services

- On QFX5100 and QFX5110, vendor-id format might be incorrect for network ports. This does not impact the ZTP functionality or service. The DHCP client configuration is coming from two places, that is, AIU script and vsdk sandbox. The DHCP client configuration coming from AIU script has the serial id in vendor id where as the default configuration from sandbox doesn't have.PR1601504

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

- On QFX5100 and EX4600 platforms, if a change related to TPID is made in the Device Control Daemon, traffic might be dropped in PFE due to failure on l2 learning or interfaces flapping. PR1477156

MPLS

- In MVPN Case, if the nexthop index of a group is not same between master and backup after a nsr switchover, we may see a packet loss of 250 to 400 ms. PR1561287

Platform and Infrastructure

- On all Junos and Junos OS Evolved platforms, while using source-address NTP configuration parameter and issue the command "set date ntp" 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

Routing Protocols

- On Junos OS and Junos OS Evolved platforms configured with graceful-shutdown sender under the BGP dynamic neighborship, the peer device does not receive routes with communities "graceful-shutdown", as it is not advertised by the sender causing the traffic drop for the affected routes. PR1699633

Resolved Issues

IN THIS SECTION

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

Chassis Clustering

- GTP control packets might be incorrectly dropped/passed if there is more than one APN IMSI filter configured PR1673879

Class of Service (CoS)

- The fixed classifier may not work in MPLS and VXLAN scenario PR1650051

EVPN

- The process rpd might crash when protocol EVPN is deactivated PR1659786

- BUM traffic might be blackholed for ESI configured CE interface flap PR1669811

- The ARP/ND entries are not relearnt as expected on the spine with EVPN-VxLAN PR1677521

General Routing

- Traffic loss might be observed on EX4650-48Y and QFX5120-48Y switches when there is a link flap PR1634495

- Multicast traffic received on the INET interface might be dropped PR1636842

- On Junos ACX/PTX/QFX platforms traffic blackholing can occur after interface flaps PR1645488

- The local-minimum-links feature not working as expected on QFX5100 VC platforms PR1649637

- Traffic Loss will be observed with Virtual-Router PR1650335

- Transit traffic might get dropped and protocols might be down when firewall filters are modified PR1651546

- The MAC address from local CE may not be learned due to the VLAN programming issue PR1651827

- Port might be down after inserting specific SFP PR1653723

- The ARP might not resolve with the native-vlan configuration PR1654215

- The interface might not come up on EX platforms PR1656540

- FEC link is down after disabling/enabling interface PR1657534

- TOS(DSCP+ECN) bits not getting copied from the Inner L3 header to Outer VXLAN header. PR1658142

- BFD session session-state is showing DOWN while checking Micro BFD Sessions with Authentication in Non-Distributed Mode PR1658317

- Valid software licenses might not be in sync between members in the Virtual chassis. PR1658913

- The multipath route might be missing when multipath is configured PR1659255

- 'no-multicast' knob within storm-control profile triggers randomly PR1659434

- The slave PTP device will not lock its clock with the master PTP device PR1659453

- Traffic loss might be seen when a VxLAN port is recovering from a failure PR1659533

- On QFX10K Junos platforms configuration of IGMP group range might result in traffic loss PR1659732

- MACsec session configured over IFD might be down when an IFL configured on IFD is disabled/ deactivated PR1660070

- After changing the MTU on an aggregated interface along with IRB the kernel crash might be observed PR1660208

- QFX : OSPF Flow Check function violating RFC6864 PR1660369

- spmb0 Cell drops on sib 'x' pf 'x' errors seen in QFX10008/QFX10016 platforms without generating any alarms PR1660699

- CoS might not get applied on VC ports PR1660787

- BUM traffic might loop post adding/removing EVPN-VXLAN FRR configuration PR1662515

- IPv6 ND packets might be dropped in QFX5100 and QFX5110 platforms PR1662707

- L2 Multicast traffic loss observed on EX4400 Virtual Chassis platform. PR1663102

- IS-IS adjacency is not coming up through the Layer 2 domain PR1663134

- Verification of stats for BFD session is "UP" while checking BFD session PR1663790

- ALB stats not showing in CLI PR1663881

- The DHCP offer packets will not be sent to the clients when the DHCP relay agent is configured over Type-5 EVPN PR1664656

- On QFX5K series platforms, duplicate packets might be seen in the multihomed scenario in an EVPN-VxLAN fabric when unicast ARP packets are received PR1665306

- Static MACs are not programmed after reboot, resulting in floods of unicast traffic PR1666399

- Multihop BFD sessions might remain down in inline mode PR1667751

- Shaping-rate is not taking 20bytes of overhead into account. PR1667879

- Route/Multicast add get queued in KRT QUEUE post interface flap. PR1669161

- On specific QFX5k platforms, member links may reduce their configured speed when the other side doesn't have auto-negotiation disabled PR1669436

- FPC1 is getting disconnected after ISSU and before switchover while checking ISSU status PR1669702

- The dcpfe process might generate core-dumps and FPC might crash after line card reboot or switchover PR1670240

- 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

- QFX5120-48YM :: QFX-EVPN_VXLAN: ECN bits not getting copied to vxlan tunnel header at the encap node PR1672308

- The BFD packets will drop in an EVPN-VxLAN scenario due to incorrect layer3 offset being set in the host path PR1674116

- VLAN translation mapping gets deleted when one of the member interface removed from LAG PR1676772

- Traffic drop will be observed if an IP packet with TTL=1 is routed over VXLAN Tunnel PR1678992

- Firewall functions will not work as expected when egress firewall filter is configured PR1679574

- BFD is running in distributed mode on QFX10K8 and QFX10K16 platforms that might remain down in EVPN-VXLAN topology. PR1680757

- The PFE process crashes from 21.4R1 version onwards on VMhost platforms PR1681532

- QFX5110-48S PTP dcpfe core may be seen with PTP configuration PR1683308

Interfaces and Chassis

- VRRP flaps between MC-LAG peers PR1579016

- The MAC address may be learned over the wrong interface in the MC-AE scenario PR1658742

Layer 2 Ethernet Services

- The DHCP unicast acknowledge packet might be dropped PR1676573

Routing Protocols

- Ipv6 Inline BFD sessions are down when neighbor is not resolved PR1650677

- Routing Process Daemon (rpd) crashes and restarts when a specific timing condition is hit with BGP configuration PR1659441

- A policy with a policy action "community" configuration may not work PR1660424

- Packets getting dropped on the Server leaf in EVPN-VXLAN with OISM PR1665791

- MCSNOOPD will be restarted and will again learn the states after core PR1672488

- Traffic drops due to the generation of the FPC core, which makes the system unstable. PR1678016

User Interface and Configuration

- "gethostbyname: Host name lookup failure" is displayed during commit PR1673176

VPNs

- [mvpn] QFX10k : Auto-RP is going down after some time on QFX10k in NGMVPN scenario PR1617620

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 **22.2** 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 22.2 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-x86-64-22.2R2.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.

> ℹ️ **NOTE**: After you install a Junos OS Release 22.2 `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.

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

> ℹ️ **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-x86-64-22.2R2.9.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-x86-64-22.2R2.9.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-x86-64-22.2R1.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-x86-64-22.2R1.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-
x86-64-22.2R1.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-
x86-64-22.2R1.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-x86-64-22.2-R1.n-secure-signed.tgz`.

> ℹ **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 and Extended End-Of-Life 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 EEOL releases only, you have an additional option - you can upgrade directly from one EEOL release to the next two subsequent EEOL releases, even if the target release is beyond the next three releases. Likewise, you can downgrade directly from one EEOL release to the previous two EEOL releases, even if the target release is beyond the previous three releases.

Table 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 22.2R2 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 this release for SRX Series devices.

What's Changed

IN THIS SECTION

Learn about what changed in this release for SRX Series.

Flow-Based and Packet-Based Processing

- PMI Mode Passthrough ESP traffic: Starting in Junos OS Release 22.1R3, we support the PMI express path processing for passthrough ESP traffic on the SRX Series devices.

Network Management and Monitoring

- **Support for the `junos:cli-feature` YANG extension (ACX Series, EX Series, MX Series, PTX Series, QFX Series, SRX Series, vMX, and vSRX)**—The `cli-feature` YANG extension identifies certain CLI properties associated with some command options and configuration statements. The Junos YANG modules that define the configuration or RPCs include the `cli-feature` extension statement, where appropriate, in schemas emitted with extensions. This extension is beneficial when a client consumes YANG data models, but for certain workflows, the client needs to generate CLI-based tools.

  [See Understanding the Junos DDL Extensions YANG Module.]

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).]

User Interface and Configuration

- **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.

VPNs

- **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.]

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

- After RG0 failover, node priorities are set to zero for both nodes with relinquish monitoring failure. PR1670772

User Interface and Configuration

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

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

- In Z-mode configuration, sometimes the statistics of back-up session may not be correct on fail-over from master to back-up.PR1667098

- After RG0 failover, node priorities are set to zero for both nodes with Relinquish monitoring failure. Expected behaviour is, RG0 Failover should happen gracefully without node priority being disturbed. Issue is seen after image upgrade and perform RG0 failover to node1 and/or fallback to node0. Issue is seen on latest 22.2R1.6 and 22.2R1.7 build. Issue is seen only when HA Link encryption feature is enabled to secure communication between primary and backup node Issue is not seen during fresh bringup of L2HA cluster Issue not seen in 22.3 releases L2HA device here is combination of RE3+SCB4+SPC3+IOC4.PR1670772

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

- IPSEC SA life-time kilobytes is not supported on PMI/PME datapath, when PMI is enabled globally, the rekey cannot be triggered based on life-time kilobytes.PR1669228

General Routing

- On vSRX, SRX1500, SRX4100 and SRX4200 devices, NTP synchronization may fail after some time. PR1331444

- 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 Application-Based Multipath Routing enabled, HTTP sessions take approx 10 minutes to re-establish after a link flap between hub and spoke. PR1577021

- 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

- 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

- Trigger: On SRX platform, perform ISSU from any release prior to 22.1 to 22.1 or above releases. Symptom: ISSU will be aborted / failed with the below warning. 'warn-message "ISSU is not supported for Clock Synchronization (SyncE)";"override'In '/var/tmp/paSBfY/etc/indb//config.indb' line 162included from '/var/tmp/paSBfY/etc/indb/issu.indb' line 10 'override' syntax errorISSU not supported as current image uses explicit tags for message structures\n PR1632810

- 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

- SRX cli command to show fwauth user details like "show security firewall-authentication users identifier 1" and "show security firewall-authentication users address 10.1.1.1" does not display user's group information.PR1659115

- Device does not drop session with server certificate chain more than 6.PR1663062

- FIPS mode is not supported in this release for SRXSME devices.PR1697999

High Availability (HA) and Resiliency

- Trigger: Perform ISSU from any release prior to 22.1 to 22.1 or above releases. This issue is applicable to all the platforms. Symptom: ISSU will be aborted / failed with the below warning. 'warn-message "ISSU is not supported for Clock Synchronization (SyncE)";'override'In '/var/tmp/paSBfY/etc/indb//config.indb' line 162included from '/var/tmp/paSBfY/etc/indb/issu.indb' line 10 'override' syntax errorISSU not supported as current image uses explicit tags for message structures \n PR1628172

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

J-Web

- On SRX platform series, when address-book entry is added or removed by Jweb, "address-book address-book name attach zone" might be unexpectedly removed at configuration commit.PR1712454

Network Management and Monitoring

- syslog may not be sent out via configured source address when target host exists on a custom routing-instancePR1689661

Platform and Infrastructure

- On SRX5k and MX240/MX480/MX960 platforms,when device is powered on with multiple line cards, power might not be sufficient and few line cards fail to come into online state.PR1645817

Unified Threat Management (UTM)

- If only EWF is configured, there can be a performance impact due to JDPI parsing overhead. In such case, to recover the performance, Web Filter can be configured in performance mode using the following CLI command: set security utm default-configuration web-filtering performance-mode PR1653793

User Interface and Configuration

- Please use "load update" instead of "load override" to prevent the error messages PR1630315

VPNs

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

- First time when we add this command the existing active connections are not changed, only the new connection after this command will be taken into effect. PR1608715

- Sometimes after manual failover, IKE-SA rekey does not succeed. In order to recover from this scenario, enable dead-peer-detection with always-send PR1690921

- On SRX5K platforms with SPC3 card, the IPSEC (Internet Protocol Security) tunnels do not get established after the tunnels are deleted using the command 'clear security ike sa'. PR1694604

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

- H.323 traffic failure caused by RAS packet drops when incorrect route lookup performed PR1688986

Chassis Clustering

- New secondary node to go into a disabled state after ISSU and failover RG0 because of fabric link failure PR1678772

- 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

- The secure tunnel interface does not work properly in SRX standalone mode PR1702763

- GTPv2 Message Filtering is not working PR1704472

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 non-fragmented packets will get dropped on the SRX5K platforms with SPC3 card PR1683835

- 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

- Application traffic drop seen on all SRX platforms due to TCP window size issue PR1699578

General Routing

- SRX4600 - Packet drop or srxpfe coredump might be observed PR1620773

- SRX5600/5800 - SNMP mib queries may result in occasional response timeouts PR1631149

- 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

- 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

- PR : monitored IP addresses for a redundancy group are reachable despite removing the redundant Ethernet interface from a zone PR1668532

- Traffic loss may be 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

- Dial-on-demand mode on the dialer interface is not working as expected PR1680405

- 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

- SRX1500 chassis cluster port ge-0/0/1 does not work in switching mode PR1690621

- SRX cluster may fail in a rare scenario when node status changes to disabled state without going through the ineligible state PR1692611

- The process srxpfd/ flowd will crash on SRX devices PR1694449

- The flowd crash and core will be observed when TLS 1.3 session ticket is received on SSL-I PR1705044

Platform and Infrastructure

- "%DAEMON-4: Set system alarm failed: Operation not supported by device" message is seen on high end SRX PR1681701

- Fabric monitoring suspension and control link failure may cause HA cluster outage PR1698797

Routing Protocols

- High CPU is seen on the platforms running IPv6 PR1677749

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

- 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

- Mismatch in configured and negotiated proxy-identity parameters can lead to KMD core. PR1699691

Migration, Upgrade, and Downgrade Instructions

IN THIS SECTION

● Upgrade and Downgrade Support Policy for Junos OS Releases and Extended End-Of-Life Releases | **133**

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

Table 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
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 vMX

These release notes accompany Junos OS Release 22.2R2 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 this release for vMX.

What's Changed

Learn about what changed in this release for vMX.

Network Management and Monitoring

- **Support for the `junos:cli-feature` YANG extension (ACX Series, EX Series, MX Series, PTX Series, QFX Series, SRX Series, vMX, and vSRX)**—The `cli-feature` YANG extension identifies certain CLI properties associated with some command options and configuration statements. The Junos YANG modules that define the configuration or RPCs include the `cli-feature` extension statement, where appropriate, in schemas emitted with extensions. This extension is beneficial when a client consumes YANG data models, but for certain workflows, the client needs to generate CLI-based tools.

    [See Understanding the Junos DDL Extensions YANG Module.]

User Interface and Configuration

- **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 22.2R3 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

IN THIS SECTION

- Platform and Infrastructure | **136**

Learn about open issues in this release for vMX.

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

- If vMX product is configured to run in performance mode via configuring "chassis fpc 0 performance-mode" (Note: performance mode is enabled by default starting from Junos OS Release 15.1F6), flow cache will be used to improve the traffic forwarding performance. With performance mode enabled, if traffic cause a single flow in the flow cache to have a large number of flow actions which hit the max supported number (i.e. 18) of flow actions (Typically, the addition of lots of firewall counters and policers in a single flow can make it add up), the riot might crash. It is a rare issue. PR1534145

Resolved Issues

There are no resolved issues in Junos OS Release 22.2R3 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

These release notes accompany Junos OS Release 22.2R2 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 this release for vRR.

What's Changed

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

Known Limitations

There are no known limitations in hardware and software in Junos OS 22.2R3 for vRR.

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 22.2R3 for vRR.

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

Resolved Issues

There are no resolved issues in Junos OS Release 22.2R3 for vRR.

Junos OS Release Notes for vSRX

IN THIS SECTION

These release notes accompany Junos OS Release 22.2R2 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

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

What's Changed

Learn about what changed in this release for vSRX.

Network Management and Monitoring

- **Support for the `junos:cli-feature` YANG extension (ACX Series, EX Series, MX Series, PTX Series, QFX Series, SRX Series, vMX, and vSRX)**—The `cli-feature` YANG extension identifies certain CLI properties associated with some command options and configuration statements. The Junos YANG modules that define the configuration or RPCs include the `cli-feature` extension statement, where appropriate, in schemas emitted with extensions. This extension is beneficial when a client consumes YANG data models, but for certain workflows, the client needs to generate CLI-based tools.

  [See Understanding the Junos DDL Extensions YANG Module.]

User Interface and Configuration

- **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 22.2R3 for vSRX.

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

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.

Flow-Based and Packet-Based Processing

- Due to JUNOS CLI framework's implementation, Current fix has a caveat that customer had better keep 1~2 minutes gap between two configuration commits if there are lots of security policies which need time to be processed. PR1625531

General Routing

- On vSRX, SRX1500, SRX4100 and SRX4200 devices, NTP synchronization may fail after some time. PR1331444

- 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

- Device does not drop session with server certificate chain more than 6.PR1663062

- FIPS mode is not supported in this release for SRXSME devices.PR1697999

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

- Packet loss on GRE Tunnel due to improper route look-up for tunnel destination PR1683334

- Slowness issue seen on GRE tunnel after upgrading to 21.4R3.15. PR1708646

General Routing

- Split tunneling feature will not work PR1655202

- ARP will not get learned if reth interface is configured with VLAN PR1681042

- EX/QFX SNMP: jnxOperatingDescr.1.1.0.0 returns blank, but jnxOperatingState.1.1.0.0 returns value. PR1683753

- "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

- Upgrade and Downgrade Support Policy for Junos OS Releases and Extended End-Of-Life Releases | 148

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 22.2R1 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 22.2R1 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 Sep 25 14:15 /var/jail/tmp/alarmd.ts
       259.7K Sep 25 14:11 /var/log/hostlogs/vjunos0.log.1.gz
       494B Sep 25 14:15 /var/log/interactive-commands.0.gz
       20.4K Sep 25 14:15 /var/log/messages.0.gz
       27B Sep 25 14:15 /var/log/wtmp.0.gz
       27B Sep 25 14:14 /var/log/wtmp.1.gz
       3027B Sep 25 14:13 /var/tmp/BSD.var.dist
       0B Sep 25 14:14 /var/tmp/LOCK_FILE
       666B Sep 25 14:14 /var/tmp/appidd_trace_debug
       0B Sep 25 14:14 /var/tmp/eedebug_bin_file
       34B Sep 25 14:14 /var/tmp/gksdchk.log
       46B Sep 25 14:14 /var/tmp/kmdchk.log
       57B Sep 25 14:14 /var/tmp/krt_rpf_filter.txt
       42B Sep 25 14:13 /var/tmp/pfe_debug_commands
```

```
        0B Sep 25 14:14 /var/tmp/pkg_cleanup.log.err
        30B Sep 25 14:14 /var/tmp/policy_status
        0B Sep 25 14:14 /var/tmp/rtsdb/if-rtsdb
        Delete these files ? [yes,no] (no) yes
<
output omitted>
```

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

4. Use FTP, SCP, or a similar utility to upload the Junos OS Release 22.2R1 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-x86-64-22.2-2022-10-12.0_RELEASE_22.2_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-
x86-64-22.2-2022-10-12.0_RELEASE_22.2_THROTTLE.tgz no-copy no-validate reboot
Verified junos-vsrx-x86-64-22.2-2022-10-12.0_RELEASE_22.2_THROTTLE signed by
PackageDevelopmentEc_2017 method ECDSA256+SHA256
THIS IS A SIGNED PACKAGE
WARNING:     This package will load JUNOS 22.2 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-22.2-2022-10-12.0_RELEASE_22.2_THROTTLE.tgz
Extracting the package ...
total 975372
-rw-r--r-- 1 30426 950 710337073 Oct 19 17:31 junos-srx-mr-
vsrx-22.2-2022-10-12.0_RELEASE_22.2_THROTTLE-app.tgz
-rw-r--r-- 1 30426 950 288433266 Oct 19 17:31 junos-srx-mr-
```

```
vsrx-22.2-2022-10-12.0_RELEASE_22.2_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-22.2-2022-10-12.0_RELEASE_22.2_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-22.2-2022-10-12.0_RELEASE_22.2_THROTTLE-linux.tgz ...
upgrade_platform: Input package /var/tmp/junos-srx-mr-
vsrx-22.2-2022-10-12.0_RELEASE_22.2_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-22.2-2022-10-12.0_RELEASE_22.2_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-22.2-2022-10-12.0_RELEASE_22.2_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 22.2R1 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 22.2-2022-10-12.0_RELEASE_22.2_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: 22.2-2022-10-12.0_RELEASE_22.2_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 EEOL releases only, you have an additional option - you can upgrade directly from one EEOL release to the next two subsequent EEOL releases, even if the target release is beyond the next three releases. Likewise, you can downgrade directly from one EEOL release to the previous two EEOL releases, even if the target release is beyond the previous three releases.

Table 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

  > (i) **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

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/content/dam/www/assets/resource-guides/us/en/jtac-user-guide.pdf.

- Product warranties—For product warranty information, visit https://support.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://support.juniper.net/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://supportportal.juniper.net/s/knowledge

- Download the latest versions of software and review release notes: https://support.juniper.net/support/downloads/

- Search technical bulletins for relevant hardware and software notifications: https://supportportal.juniper.net/s/knowledge

- Join and participate in the Juniper Networks Community Forum: https://www.juniper.net/company/communities/

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

Creating a Service Request with JTAC

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

- Visit Juniper Support Portal: Case Management, Product Support & More.

- Call 1-888-314-JTAC (1-888-314-5822 toll-free in the USA, Canada, and Mexico).

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

Revision History

09 January 2026—Revision 12, Junos OS Release 22.2R3.

15 August 2025—Revision 11, Junos OS Release 22.2R3.

3 April 2025—Revision 10, Junos OS Release 22.2R3.

27 March 2025—Revision 9, Junos OS Release 22.2R3.

18 April 2024—Revision 8, Junos OS Release 22.2R3.

12 December 2023—Revision 7, Junos OS Release 22.2R3.

28 September 2023—Revision 6, Junos OS Release 22.2R3.

20 July 2023—Revision 5, Junos OS Release 22.2R3.

6 July 2023—Revision 4, Junos OS Release 22.2R3.

1 June 2023—Revision 3, Junos OS Release 22.2R3.

27 March 2023—Revision 2, Junos OS Release 22.2R3.

23 February 2023—Revision 1, Junos OS Release 22.2R3.