Release Notes

Junos OS Release 22.2R2

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 22.2R2. 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 22.2R2 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

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

Known Limitations

IN THIS SECTION

- General Routing | **2**

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

IN THIS SECTION

- General Routing | **3**

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

- 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 ACX 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

- 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

- Interop for 1G interfaces between EX4100 SKUs and acx5448/acx5448-M/D or MX480 will not workPR1657766

- 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

- 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

Resolved Issues

IN THIS SECTION

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 ACX5448 and ACX710 platforms, it is observed that VLAN(Virtual LAN) priority may change at the egress end of the circuit.PR1630255

- On all Junos OS platforms, EVPN-MPLS/EVPN-E-Tree broadcast unknown-unicast and multicast (BUM) traffic received on non-designated forwarder (Non-DF) will be forwarded back to customer edge device (CE) via designated forwarder (DF) when CE-DF link flap.PR1643598

- On ACX5448 platform, if a firewall has a log action and it's applied on physical interface or lo0, the LDP neighbor cannot go up. PR1648968

- Periodic streaming is not available for BGP Sensor "/bgp-rib/" in Junos OS Release 22.2R1. It is advised to use on-change telemetry for such high-volume data sensors.PR1649529

- HTTP(S) file download hangs over EVPN-ETREE configuration. This issue occurs whenever the EVPN AC role is configured as leaf on the EVPN ETREE side that the (HTTPS) client resides, while it is configured as root on the server side.PR1653531

- It is a negative use case and happens when a wrong config is committed and box is booted.PR1658327

- On ACX5448 platform, when FPC (Flexible PIC Concentrator) lost communication with RE (Routing Engine), FPC remained online and it's physical ports stayed up as well. But the traffic through this interface will be black-holed.PR1659949

- On ACX710/ACX5448 platforms in the layer2 circuit scenario, if the primary path is down due to any reason, the backup circuit takes the mastership and ideally, once the primary path is up, mastership is to be reverted. But, in rare cases, the mastership gets reverted but the label might get lost from PFE and results in traffic loss for the l2circuit connection. However, deactivating and activating the affected l2circuit configuration could help in restoring the services.PR1661802

- On ACX5448 platform after add some EVPN-ETREE services/interfaces the riofeb (pfe) process may crash and 'dnx_rt_vpls_rebake_flood_route' and 'dnx_nh_composite_handle_flood_nh_change' logs will be seen. "show vmhost crash" will show riofeb coredumps.PR1662686

- On all Junos and Junos Evolved platforms, upstream interface of multicast routes points to old active RPF (Reverse Path Forwarding) instead of new active RPF even though old active interface is not available when PIM (Protocol Independent Multicast)/ multicast neighbor is removed/flapped. This issue impacts forwarding plane and causes a traffic loss as multicast route in the rpd (Routing Protocol Daemon) and PFE (Packet Forwarding Engine) goes out of sync. This issue is observed because multicast route is not updated due to MBB (Make Before Break).PR1663271

- On ACX5448/ACX710, transit traffic drop is observed for BGP-LU prefix when ECMP is enabled. It is acting as a transit router between two routers and BGP-LU prefix route towards any of them has ECMP path. This issue may impact a forwarding plane and cause a traffic impact.PR1663563

- On ACX5448 and ACX710 platforms, when an empty interface (interface which has no optics inserted) is added as a child member link to an AE (Aggregated Ethernet) bundle which has 'lacp accept-data' configured, traffic is sent over the empty interface resulting in traffic drop.PR1663651

- FXPC core file might be seen when deactivating a child memeber link from aggregated Ethernet bundle. PR1665511

- On all Junos platforms, incorrect sensor base telemetry data are collected when multiple SR-TE tunnels are configured with at least one uncolored, sharing the same single hop segment list.PR1665943

- On ACX5448, if the VRRP is configured for the aggregated Ethernet interface, the VRRP group is shown as up from Routing Engine side but the VRRP VIP does not function. PR1666853

- On ACX710 and ACX5448 its variants, when the inline Bidirectional Forwarding Detection (BFD) session is configured, Packet Forwarding Engine (PFE) might crash and impact the service.PR1667129

- On junos ACX platform, shutting the CE interface and bringing back up causes traffic (going towards the core) to drop.PR1667724

- On all Junos platforms, Link Layer Discovery Protocol (LLDP) neighborship fails if the chassis-id format of the LLDP packet is xx:xx:xx:XX:XX:xx' PR1669677

- When health monitoring is enabled on the Routing Engine disks, alarms are raised if the appropriate conditions are met. But, if there are two disks and both the disks generate the alarm condition only one will be shown. PR1669968

- Log related to resources reported after EVPN RI are deactivated or activated multiple times : "ACX_BD_ERR: dnx_bd_alloc_l2_svlan: System reached L3 IFL and BD limit(12286)"PR1670683

- The firmware count incrementing for each firmware update information being sent from lcmd (Linux Chassis Management Daemon) after every configuration commit. Therefore, the counter to increment out of bounds of the array cause memory overwriting resulting in memory corruption in chassisd. PR1672039

- In ACX5448 platform while issuing the command to check temperature-thresholds. we would see the PFE wrongly spelled as QUMARN instead of Qumran. This is identified as cosmetic issue in CLI display and the same has been corrected.PR1682819

Network Management and Monitoring

- On all Junos and EVO platforms configured with filter-duplicates, the snmpd core might be observed if the SNMP query is made simultaneously from NMS (Network Management System) 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 platforms and all Junos Evolved platforms, Routing Process Daemon (rpd) crashes and restarts when BGP (Border Gateway Protocol) 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

- Upgrade and Downgrade Support Policy for Junos OS Releases and Extended End-Of-Life Releases | 8

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 22.2R2 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 22.2R2 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 22.2R2 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 22.2R2 for cSRX.

Junos OS Release Notes for EX Series

IN THIS SECTION

These release notes accompany Junos OS Release 22.2R2 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

There are no changes in behavior and syntax in this release for EX Series switches.

Known Limitations

IN THIS SECTION

● General Routing | **11**

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 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 unified ISSU to work. PR1634695

- VLAN xlate table will have more entries if the same VLAN is shared with access and trunk port. Users shall expect more xlate HW table entries with this config combination.PR1655101

- On EX4100 devices, input pps, bps and byte counters are shown as 0 for some ports while traffic running without issues, interface stats cleared for 0-23 and not cleared for 24-47 after interface flap. Cosmetic issue with respect to display, no traffic drops and no functional impact.PR1657995

Open Issues

IN THIS SECTION

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

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

General Routing

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

- The runt, fragment and jabber counters are not incrementing on EX4300-MPsPR1492605

- 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

- EVPN VxLAN::DHCP-Snooping - vtep interface is seen in the **dhcp-security binding** table even for the directly connected clients. PR1657597

- With SFP+-10G-CU3M DAC, link stays up when the peer end device MX10008 is admin down. There is no Rx signal loss received from the peer end for EX4100 link to go down. Same scenario works with other platforms.PR1640799

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

- EX4100 MACsec interface statistics of encrypted/decrypted bytes won't be updating properly after a certain value.PR1658584

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

- Some of interfaces getting zero statistics in `monitor interface traffic` command. Sending traffic across all interfaces and applied speed of 100m on all 1g copper ports. Clearing statistics for interfaces, the issue is seen.PR1661617

- On EX92XX Series platforms with the EVPN-VXLAN (Ethernet VPN-Virtual Extensible LAN) scenario, the DHCP (Dynamic Host Configuration Protocol) packets from the client get dropped while tunneling to the EVPN-VXLAN. When this happens, the packets will not reach the DHCP server and the host could not get the IP address.PR1662524

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

- On the 48 Port SKU, tagged packet greater than MTU size 1518 gets dropped due to BCM EGR_MTU set to 1518 on ports 0-24. Mitigation is to set interface MTU to 1518.PR1677902

- If 1G optic is inserted on uplink ports of EX4100-24mp/24mp/48p/48t/24p/24t SKUs, then the activity LED is lit irrespective of link present/up status.PR1682633

Forwarding and Sampling

- When the `fast-lookup-filter` statement is configured with a match that is not supported in the FLT hardware, traffic might be lost. PR1573350

Layer 2 Features

- On 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

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 EX4300-24T, 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

Resolved Issues

IN THIS SECTION

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

General Routing

- The EX2300 device might unexpectedly drop VOIP VLAN traffic after reboot. PR1633883

- Buffer-size exact will not work. PR1644355

- DHCP traffic might be dropped when DHCP-security and RTG are enabled. PR1647209

- On EX4100 devices, Junos Telemetry interface FAN and power supply names does not match with CLI. PR1648739

- On EX4100 devuces, wrong trap generated after removal of fan0 in FPC4. PR1652388

- L2PT might not work for aggregated Ethernet interfaces in Q-in-Q environment. PR1653260

- EVPN-VXLAN: EX4100 :PDT:: Partial traffic drop seen on the emerald VC , after Routing Engine switchover from primary to back up with NSR or NSB. PR1655052

- The egress traffic is not tagged properly in a L2PT scenario. PR1655511

- Filter-Based Forwarding filter might not work as expected. PR1656117

- The interface might not come up on EX platforms. PR1656540

- An incorrect PEM alarm will be raised on EX4400 devices. PR1658049

- The port/mac gbp tags might not be carried forward to the spine. PR1659384

- LEDs on ports 0-35 are always lit on EX4400-48MP platforms. PR1662288

- The fxpc crash might be observed with the RPF check enabled. PR1662508

- SSH traffic might be affected when filter log action is used. PR1663126

- MAC address learning failure and traffic loss might be observed on VXLAN enabled ports having native-VLAN configured. PR1663172

- MAC addresses learned on the RTG interface are not aging out. PR1664955

- MAC-IP bindings for IPv4 (ARP) and IPv6 (ND) might not be processed for IRB interfaces in an EVPN scenario. PR1665828

- High numbers of PDs connected might result in high CPU utilization. PR1667564

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

- [Dot1x][EX3400]:MAC radius authentication without restrict option was updating authenticated VLAN information before client authentication.PR1668144

- The chassisd memory was corrupted and the chassisd crashed. PR1672039

- Traffic flow will be affected as interfaces will be removed from VLAN. PR1675861

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

- DHCP binding will fail for the clients (Clients connected on an aggregated Ethernet interface with 2 or more VLANs) on a VLAN where DHCP security is not configured. PR1679094

- On EX4100 devices, traffic loss noticed with **igmp-snooping** running on Layer 2 switches. PR1681478

Infrastructure

- On ARM64 platforms such as EX4100, if a live vmcore is attempted to be created, the DUT might get stuck and reboot. PR1656625

Network Management and Monitoring

- Observed memory leak in event leak during GRES. PR1602536

- The **snmpd** process might crash if SNMP timeout happens. PR1666548

Platform and Infrastructure<

- GARP reply does not update ARP entry though gratuitous-arp-reply option is configured. PR1644616

- IRACL filters more than 64 might not work on IRB units. PR1653216

- The dc-pfe might crash due to the VCCP flap. PR1655530

- Junos upgrade might fail due to a storage issue in the /var/tmp directory. PR1659460

- On EX4300 platform, high CPU is seen with generation of log message **/kernel: %KERN-3: i802_3_slow_recv_input:oam/esmc PDU dropped**. PR1661332

- The fxpc process crash might be observed on EX4300 and EX4300-VC platforms. PR1675977

Virtual Chassis

- On Junos (EX4600 and EX4650) platforms, line card might be disconnected from VC post primary Routing Engine reboot. PR1669241

Migration, Upgrade, and Downgrade Instructions

IN THIS SECTION

- Upgrade and Downgrade Support Policy for Junos OS Releases and Extended End-Of-Life Releases | **17**

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 22.2R2 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 | **20**

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

General Routing

- All Junos platforms face the issue of Intermediate System-to-Intermediate System (IS-IS) packet drop where the packet headers are Generic routing encapsulation (GRE) over Flexible Tunnel Interface-Virtual Extensible LAN (FTI-VXLAN). Such packets are dropped at sender side kernel in the egress direction due to incorrect handling. PR1676912

Migration, Upgrade, and Downgrade Instructions

IN THIS SECTION

- Upgrade and Downgrade Support Policy for Junos OS Releases and Extended End-Of-Life Releases | **20**

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 22.2R2 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 22.2R2 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 22.2R2 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 22.2R2 for Juniper Secure Connect.

Junos OS Release Notes for Junos Fusion for Enterprise

IN THIS SECTION

These release notes accompany Junos OS Release 22.2R2 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

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

Basic Procedure for Upgrading Junos OS on an Aggregation Device

When upgrading or downgrading Junos OS for an aggregation device, always use the `junos-install` package. Use other packages (such as the `jbundle` package) only when so instructed by a Juniper Networks support representative. For information about the contents of the `junos-install` package and details of the installation process, see the Installation and Upgrade Guide.

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

To download and install Junos OS:

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

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

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

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

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

5. Select the **Software** tab.

6. Select the software package for the release.

7. Review and accept the End User License Agreement.

8. Download the software to a local host.

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

10. Install the new `junos-install` package on the aggregation device.

> (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.

> (i) **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 22.2R2 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

There are no resolved issues in this release for Junos Fusion for provider edge.

Migration, Upgrade, and Downgrade Instructions

IN THIS SECTION

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

Basic Procedure for Upgrading an Aggregation Device

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

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

The download and installation process for Junos OS Release 22.2R2 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/jinstall64-22.2R2.SPIN-
  domestic-signed.tgz
  ```

- For 32-bit software:

  ```
  user@host> request system software add validate reboot source/jinstall-22.2R2.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/jinstall64-22.2R2.SPIN-
  export-signed.tgz
  ```

- For 32-bit software:

```
user@host> request system software add validate reboot source/jinstall-22.2R2.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 22.2R2 `jinstall` package, you cannot return to the previously installed software by issuing the `request system software rollback` command. Instead, you must issue the `request system software add validate` command and specify the `jinstall` package that corresponds to the previously installed software.

Upgrading an Aggregation Device with Redundant Routing Engines

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

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

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

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

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

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

Preparing the Switch for Satellite Device Conversion

Satellite devices in a Junos fusion topology use a satellite software package that is different from the standard Junos OS software package. Before you can install the satellite software package on a satellite device, you first need to upgrade the target satellite device to an interim Junos OS software version that can be converted to satellite software. For satellite device hardware and software requirements, see Understanding Junos fusion Software and Hardware Requirements

> **NOTE**: The following conditions must be met before a standalone switch that is running Junos OS Release 14.1X53-D43 can be converted to a satellite device when the action is initiated from the aggregation device:
>
> - The switch can be converted to only SNOS 3.1 and later.
>
> - Either the switch must be set to factory-default configuration by using the `request system zeroize` command, or the following command must be included in the configuration: `set chassis auto-satellite-conversion`.

Customers with EX4300 switches, use the following command:

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

Customers with QFX5100 switches, use the following command:

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

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

1. Log in to the device by using the console port.

2. Clear the device:

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

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

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

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

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

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

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

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

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

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

Converting a Satellite Device to a Standalone Device

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

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

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

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

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

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

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

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

5. Review and accept the End User License Agreement.

6. Download the software to a local host.

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

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

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

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

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

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

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

9. Commit the configuration.

   To commit the configuration to both Routing Engines:

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

   Otherwise, commit the configuration to a single Routing Engine:

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

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

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

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

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

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

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

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

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

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

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

Upgrading an Aggregation Device

When you upgrade an aggregation device to Junos OS Release 22.2R2, 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 22.2R2 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 introducedThe existing minor alarm, VMHost RE 0 Disk 1 Usage is above threshold is changed to VMHost RE 0 Disk 1 Size usage breached threshold.

MPLS

- **CSPF LSP resignaling uses new instance ID (MX480)**—A Constrained Shortest Path First (CSPF) LSP uses a new instance ID when attempting to resignal an LSP that is down. In earlier releases, the CSPF LSPs that went down were stuck in CSPF path computation stage. You had to manually clear the affected LSPs and recompute the paths for the LSPs to be up again.

  [See LSP Computation.]

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 might be seen, but these are harmless and does not have functional impact: `timestamp device kernel: i2c i2c-100: (11/1:0x41) i2c transaction error (0x00000002) timestamp device kernel: i2c i2c-64: (7/1:0x41) i2c transaction error (0x00000002)`. PR1457655

- Currently, we do not support IP options for egress firewall attach points. Relevant supporting document attached: https://www.juniper.net/documentation/us/en/software/junos/routing-policy/topics/concept/firewall-filter-match-conditions-for-ipv4-traffic.html. The issue might cause IP-options router alert traffic not hitting the egress firewall filter. PR1490967

- Once you configure VXLAN on an IFD, its always treated as vxlan port even though Layer 2 vlan exists. PR1570689

- During reboot, `warning: requires 'idp-sig' license` spams screen. PR1594014

- 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

- The CPU might overrun while performing sanity check due to incompatibility issues between ukern scheduler and Linux driver, which might lead to traffic loss. PR1641517

- 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

Infrastructure

- You can see the following IPC timeouts logs for statistics query to kernel (queried from CLI or daemons querying internally) when there is configuration churn, or large number of IPCs get 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. PR1629930

Interfaces and Chassis

- MX240: Device prompt is not responding after issuing the `commit` command. PR1662883

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 do not work if defined under group. PR1637730

Platform and Infrastructure

- In some scenarios with MPC, you might observe major alarm and error messages. This major error is triggered due to parity error, and the impacted queue might drop packets. This might impact the forwarding, and to recover, reboot the 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 you apply `deactivate services rpm` and `deactivate routing-options rpm-tracking` and then commit, some of the rpm tracked added routes are not deleted from the routing table. As a workaround, perform the following steps:

  1. Deactivate `routing-options rpm-tracking`.

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

  3. Deactivate `services rpm`.

  4. 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 you configure a hierarchy specified in apply-path in an ephemeral instance, then rpd may not be able to update the prefix-list for the configuration in ephemeral instance. PR1636390

Routing Protocols

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

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 logical interfaces in a single commit leads to race-conditions. PR1666010

EVPN

- In Provider Backbone Bridging - Ethernet VPN (PBB-EVPN) environment, ARP suppression feature, which is not supported by PBB might be enabled unexpectedly. This might cause MAC addresses of remote CEs not to be learned and hence cause 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, perform the following steps:

  1. Clear auto-evpn ce-interface interface-name.

  2. Configure editactivate interface-name family inet inet6.

  We can fix this by keeping some persistent state on a interface being a core facing interface in some incarnation. PR1630627

- On all platforms that support Ethernet Virtual Private Networks -Multiprotocol Label Switching (EVPN-MPLS) services, during switchover or l2-learning restart, some EVPN next hops are not correctly associated with routing-instance in Routing Engine (RE), impacting the traffic forwarding. PR1633344

- When Assisted Replication (AR) feature as Replicator role is used in an Ethernet VPN (EVPN) multi-homed scenario, out-of-bound memory access issue might be observed, which could result in the kernel crash, leading to the service impact. PR1649234

- On all Junos and Junos Evolved platforms that support Type-2 (T-2) Integrated Routing and Bridging (IRB) symmetric routing, Virtual Extensible LAN (EVPN VXLAN) symmetric type-2 route needs to be imported in Layer 2 mac-vrf instance for IP host route to be added in Layer 3 (L3) vrf. Layer 3 inter-subnet routing will fail if there is no reachability for the remote IP-host route. PR1669585

- On all Junos platforms running Ethernet Virtual Private Network (EVPN) Multi-Protocol Labeled Switching (MPLS) and a single active Link Aggregation (LAG), the traffic can get forwarded to the Non-Designed Forwarder (NDF) router, which can lead to a traffic drop. This issue is seen in multi-vendor Provider Edge (PE) Customer Edge (CE) setup when there is a DF switchover, that is, Designated Forwarder (DF) role changes and the backup router starts advertising the EVPN type 2 route, now there is another switchover and the old DF again becomes the DF and advertises EVPN type 1 route but the NDF does not withdraw its route consequently the traffic gets forwarded to the NDF. PR1680421

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. Restart the dfwd daemon to recover the issue. PR1397171

- When you configure the "fast-lookup-filter" statement with a match that is not supported in the FLT hardware, traffic might be lost. PR1573350

General Routing

- 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: `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 you take a vmhost snapshot 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 you add VLAN as an action for changing the VLAN in both ingress and egress filters, the filter is not installed. PR1362609

- On MX Series routers with MPC7E, MPC8E, or MPC9E installed, if optics QSFPP-4X10GE-LR from Innolight vendor (subset of modules with part number 740-054050) is used, the link might flap. PR1436275

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

- The issue occurs when there are hardware link errors on all 32 links on an FPC 11. Because of these link errors, all FPCs reported destination errors towards FPC 11 and FPC 11 get taken offline with the 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 Routing Engine 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

- The AMS bundle state toggles momentarily as up, down, and up after configuring commit for a scaled scenario. 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 by 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, and the riot might crash. It is a rare issue. PR1534145

- The Flexible PIC Concentrator (FPC) might generate a core file if the flap-trap-monitor feature under `set protocols oam ethernet cfm performance-monitoring sla-iterator-profiles` is used and performance monitoring flap occurs. PR1536417

- 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 Routing Engine 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 correct 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

- Support switchover on routing-crash knob during abnormal termination of RPD. PR1561059

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

- To avoid the additional interface flap , interface hold time needs to be configured. PR1562857

- 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

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

- On all devices running Junos 19.1R3-S5-J3, the subscriber IFL(logical interface) 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 21.3R1 version. PR1597276

- MX2010, MX2020: MPC11E: Unified ISSU is not supported for software upgrades from Junos OS Release 21.2 to 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 Virtual Chassis (MX-VC) 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 on a rare occasion to backup RPD, RPD generates core files. PR1607553

- 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

- Memory Zone is not reflecting properly while doing Memory Tests through Vty command `test usp service-sets memory-testing start`. PR1619499

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

- 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), V6 traffic drop might be 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

- Script fails while verifying Access Internal Routes after daemon restart during advanced DHCP test. PR1640567

- 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 (i.e. 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.PR1646799

- With overlapping NAT pool configured with different NAT rules under different service sets, when service outside interface is moved between different routing instances (EX: from vr1 to default, and from default to vr1), NAT routes corresponding to the service-set in default routing instance are getting deleted, resulting in reverse path traffic failure for NAT sessions. PR1646822

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

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

- 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. PR1655712

- On MX304 in few cases if mce-inject is invoked, logs reporting MCE errors might not get registered .PR1656004

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

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

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

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

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

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

- 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

- MX10k8 with MX10K-LC2101 Linecard(s) supports *PTP* only with JNP10008-SF Switch Fabric Board(s), *PTP* currently doesn't work with JNP10008-SF2 Switch Fabric Board(s). PR1664569

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

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

- On MX platforms with MIC-MACSEC-20GE, Forwarding Engine Board (FEB) 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

- On the 48 Port SKU, tagged packet greater than MTU size 1518 gets dropped due to BCM EGR_MTU set to 1518 on ports 0-24. Mitigation is to set interface MTU to 1518. PR1677902

- 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

- Invalid PIC configuration inside GNF might add delay to `clear interface statistic all` command. This issue does not impact any functionality. chassis fpc SLOT pic IS. PR1683312

High Availability (HA) and Resiliency

- When you perform GRES 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

- You can the following IPC timeouts logs for statistics query to kernel (queried from CLI or daemons querying internally) when there is configuration churn, or large number of IPCs getting exchanged between kernel and 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. PR1629930

Layer 2 Features

- In case of the access-side interfaces used as SP-style interfaces, when you add a new logical interface 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

Network Management and Monitoring

- When you configure `maximum-password-length` and user tries to configure password whose length exceeds configured maximum-password-length, the system displays error, 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

- The mgd might crash when you configure an invalid value for identityref type leafs/leaf-lists while configuring Openconfig or any other third-party YANG, problem happens with json and xml loads. PR1615773

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

- 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 generates core files and VC might split with multicast scale scenario. PR1614145

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

- 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 core file will be created. Because of the core ssh, access is denied. PR1672581

Routing Protocols

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

- 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 (for example, IPv6) than the NLRI address family (for example, 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, that is, when you delete xSTP configurations from the box, there can be a possibility of ppmd core file. 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

- On all Junos and Junos Evolved platforms, by default, inactive routes from inet.3 are advertised in BGP. When add-path is configured, inactive routes from inet.3 are no longer advertised, this behavior is unexpected. PR1665610

- On all Junos and Junos Evolved platforms, when BGP update-threading is enabled and executed a certain sequence of flap events like flapping IS-IS adjacencies, LDP, iBGP peers, clearing ARP table, interface flap for an hour by turning OFF and ON laser which triggers the rpd crash. It is a rare case. PR1669615

- The routing protocol daemon (rpd) crash happens when a non Border Gateway Protocol (non-BGP) route is exported through Label Distribution Protocol (LDP) 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 routing protocol daemon (rpd) might crash when Protocol Independent Multicast (PIM), Multicast only Fast Reroute (MoFRR) configuration is present and some network churn event such as continuous interface cost changes, resulting in a change of active and backup paths for Equal Cost Multi-Path (ECMP) 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

User Interface and Configuration

- Root cause- In test configuration flow we are calling mustd as **/usr/sbin/mustd -q /var/run/db/file.data /var/run/db/file.data+ -F -m** where we just copy the existing cog.db (generated out of committed config) as cdg.db+ , use it for testing the configuration passed, and remove it once the testing is done. This is creating the issue because the configuration is tested against the existing cdg.db. Fix would be to create the cdg.db fresh from the configuration to be tested and test the configuration against that. This new cdg.db should not replace the existing one in **/var/run/db**. PR1671112

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 unified 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 might be lost. The group member can still send rekey requests for the TEK SAs before the hard lifetime expiry. Only if the key server sends any new PUSH messages to the group members, those updates would not be received by the group member since the key server would have removed the member from registered members list. PR1608290

Resolved Issues

IN THIS SECTION

- VPNs | **70**

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

Class of Service (CoS)

- QoS might not work as expected on AE interfaces with explicit-null label. PR1675781

EVPN

- The rpd process crash might occur due to memory allocation failure. PR1636690

- EVPN Proxy ARP doesn't work for the restricted feature on the IRB interface. PR1650665

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

- CRB EVPN MPLS is not working with control-word enabled. PR1665130

- Traffic drop might occur in the EVPN-VPWS scenario. PR1672749

- RPD core files upon receipt of a specific EVPN route by a BGP route reflector in an EVPN environment. PR1675054

- EVPN Proxy ARP doesn't work for the static VTEP interface. PR1679115

Forwarding and Sampling

- mib2d core file hitting `@mib2d_fwstats_async_handler_cb rtslib_async_process_msg` during GRES testing with page pooling enabled. PR1647669

- The MPC/FPC crash is seen on specific LC's running BGP Flowspec. PR1662955

- Traffic loss occurs in the VPLS scenario after the upgrade. PR1663717

- Traffic loss might be observed when changing firewall configuration. PR1670622

- The FPC crashes when you use `show filter memory` command during a firewall filter configuration change. PR1680849

General Routing

- LTS19: MX2008: junos vmcore file failed. Partition too small. PR1604755

- M/Mx: IS-IS adjacency remains down in backup Routing Engine during link flap test. PR1608591

- Pkid crash occurs due to null pointer dereferencing during local certificate verification in some cases. PR1624844

- Fabric request timeouts and fabric healing occur. PR1625820

- DSLite might not work on MX platforms installed with MPC7E line card and SPC3 service PIC. PR1632278

- Junos OS 21.4R1.2 - RESET PFE - Single hop BFD session over AE stuck at INIT after "reset PFE". PR1632585

- The `show chassis firmware` does not show the revision for PIC FPGA. PR1633187

- The error message will be seen during FPC boot up on MX10003. PR1637756

- USB device not visible in Junos. PR1639071

- The dynamic tunnel might flap every 15 minutes with a non-forwarding route. PR1639134

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

- Buffer-size exact will not work. PR1644355

- The rpd crash might be seen in backup Routing Engine. PR1645457

- DHCP dual-stack subscriber scale-up failed in the access model DHCP relay. PR1645574

- DHCP Subscriber traffic might get dropped due to the rpf-check filter. PR1647214

- MX960: During bbe-smgd daemon restart there is a small window during which requests for subscriber statistics results in bbe-statsd daemon core file. PR1648565

- BGP sensor **/bgp-rib/afi-safis/afi-safi/ipv4-unicast/loc-rib/** is not available as a 'periodic' sensor. PR1649529

- MX10008: Auto detection of affected YT from ZF parity error. PR1649858

- Traffic loss will be observed with virtual-router. PR1650335

- VMcore is triggered when control packets go over IRB and GRE. PR1651273

- PCS errored blocks count will increment after Junos software upgrade to Junos OS Release 20.2R1 or above releases. PR1651526

- Transit traffic might get dropped and protocols might be down when you modify the firewall filters. PR1651546

- The L2BSA subscribers might not be able to browse due to incorrect entries in the VPLS mac-table. PR1652337

- The syslog errors and PPE traps might be observed. PR1652901

- The bbe-smgd core file is observed on MX platforms. PR1653546

- SyncE clock goes to holdover when interface flaps in sequence. PR1654008

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

- The 1G port always stays down while changing of 10G interface lane speed to 1G. PR1655089

- [gRIBI]IP-IP tunnel remains in the Packet Forwarding Engine even after clearing all programmed route entries. PR1655531

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

- GRE-in-GRE encapsulated traffic might be dropped when the recursion-control bit is set to non-zero, which does not comply with RFC standard. PR1656499

- jnxDomCurrentLaneRxLaserPower SNMP MIB is not providing lane 0 information if polled using ifindex without Lane number. PR1656702

- PIC of SPC3 card will reboot when you execute `show services nat source deterministic xlated-ip x.x.x.x` with non-determined IP. PR1656798

- Junos OS Release 22.2R1: MISC:: mspmand core file found `@sarena_free @mum_free @jsf_shm_free @jssl_mem_pool_free @jsf_openssl_free @CRYPTO_free @ssl_cert_free @jssl_config_dtor @msvcs_plugin_send_control_rt` . PR1657027

- The transit traffic might be impacted in the PTP scenario. PR1657132

- SR-TE LSP state might go down due to "Compute Result failure". PR1657176

- The jdhcpd process might be stuck at 99% if traceoptions is enabled in high DHCP traffic scenario. PR1658087

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

- The CPU usage SPMB might hit 100% for a short while. PR1658206

- Some Layer 3 VPN prefixes are not active because nexthop is not usable. PR1658277

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

- The rpd memory leak might be seen while processing vlan-ccc configuration. PR1659102

- JSD crash during cBNG container startup or restart from CLI from within a cBNG container. PR1659175

- The multipath route might be missing when you configure multipath. PR1659255

- Multiple stale EIM mappings observed on Junos MX platforms due to the aging timer getting stuck. PR1659284

- Traffic loss might occur when a VxLAN port is recovering from a failure. PR1659533

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

- After changing the MTU on an aggregated interface along with IRB, we might observe the kernel crash. PR1660208

- Soft assertions in RPD will fail during GRES. PR1660484

- Transit PTP over IP packet drop might occur on an AE interface. PR1660844

- The l2circuit backup might not revert to primary in rare condition. PR1661802

- Traffic loss might be seen in certain IPsec VPN and Group-VPN scenario. PR1661815

- The fxpc crash might occur with the RPF check enabled. PR1662508

- TCP MSS value might not get reflected to packets. PR1662950

- The network-instance name for streaming telemetry to be changed from default to DEFAULT to align with CONFIG stanza. PR1662999

- The offset value might be high on the downstream node while switching between line cards, which impacts 5G services. PR1663065

- The forwarding plane is not updated properly in scaled MVPN scenario after receiving PIM leave messages. PR1663568

- Subscribers will be stuck in the initializing or terminating state. PR1663689

- On MX960, line cards with VPLS and CFM configuration might crash when the indirect NH associated with LSI IFL is deleted. PR1663725

- Post switchover error message is seen during pccd initialization. PR1664165

- The `show chassis fpc` command shows inaccurate information about heap memory. PR1664448

- The routing process on the device might crash when the IP address of local interface is changed to the IP address of BGP peer. PR1664527

- Line card might crash after offline/online plane. PR1664602

- MAC addresses learned on the RTG interface are not aging out. PR1664955

- The link-degrade recovery might not work for a specific interface speed. PR1664978

- For MPC11 , we are not seeing yellow alarm when the yellow alarm threshold are breeched for MPC11 temp sensors. PR1665071

- The rpf-check feature might not be working in a Junos Subscriber management scenario. PR1665234

- In the SR-TE scenario, sensors are incorrectly populated for colored tunnel BSID routes when uncolored tunnels are enabled. PR1665943

- BGP-LU traffic might drop when you configure `CCNH ingress labeled-bgp inet`. PR1666760

- Traffic drop might occur on AF interface when PFE gets in disabled state on GNF in NodeSlice platforms. PR1666992

- The hyper-mode might be set incorrectly after power cycle on MX platforms. PR1667226

- H-VPLS traffic might drop silently when you enable mesh group local-switching. PR1667310

- High numbers of PDs connected might result in high CPU utilization. PR1667564

- The FPC might fail to initialize on Junos platforms. PR1667674

- Shutting the CE interface and bringing back up causes traffic (going towards the core) drop. PR1667724

- The RSVP interfaces are not streamed when removing the interface configuration. PR1667844

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

- Periodic event generation doesn't work after Routing Engine reboot. PR1668152

- The BGP multipath might not install some of the available next-hops. PR1668481

- Kernel logs on cRPD containers running on the same host are incomplete. PR1668794

- EVPN provide edge router might respond traceroute with unexpected source IP address to remote CE. PR1668837

- Commit configuration check-out failed while configuring syslog stream host IP in specific range. PR1668941

- Traffic loss occurs for the multicast traffic. PR1668976

- The rpd process restarts after generating core file. PR1669346

- jsd memory leak and might lead jsd restart. PR1669426

- LLDP neighborship might fail if the chassis-id format of the LLDP packet is xx:xx:xx:XX:XX:xx'. PR1669677

- Interoperability issue between legacy line cards and MPC10E/11E causes L2 packet drop. PR1669765

- USB installation package loads with 32-bit smartd binary version. PR1669892

- Fabric Destination error and Fabric plane going in check state after changing the fabric redundancy mode. PR1670507

- Routing Engine reboots when PPPoE subscribers login. PR1671135

- MX150 platform reports error for bandwidth license. PR1671347

- The chassisd memory was corrupted and the chassisd crashed. PR1672039

- ECN bits are not getting copied to vxlan tunnel header at the encapsulation node. PR1672308

- Traffic might be impacted due to an unexpected reboot of SPC3 card. PR1672819

- Backup FEB1 links down after master FEB0 restart. PR1673274

- Training failures reported on the MX2010/MX2020 Junos platforms post fabric plane offline-online. PR1673806

- During the smooth upgrade from SFB1 to SFB2, SFB2 gets detected as "Unknown Fabric Board". PR1674309

- SNMP alarms `Power Supply failed` and `Power Supply OK` are not generated. PR1674322

- The "nsd" might crash post NAT rule configuration change. PR1674381

- The 'kmd' process might crash due to SA re-negotiation failure during IKE phase-1. PR1674585

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

- In a rare case, 'pccd' will crash when the PCEP connection is down. PR1675816

- Traffic flow will be affected as interfaces will be removed from VLAN. PR1675861

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

- Minor memory leak in 'bbe-statsd' daemon might be seen when you enable `subscriber-management` on MX platforms. PR1676049

- While processing SNMP GetNext requests 'trasportd' might reach 100% of CPU utilization. PR1676593

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

- IS-IS packet drop occurs for packets with GRE over FTI-VXLAN header. PR1676912

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

- The dynamic tunnel route gets removed when a new tunnel is brought up for the same selector. PR1680775

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

- Fabric Plane check/error alarm would be seen due to the burst traffic in MS-MPC line cards. PR1681624

- Traffic would hit incorrect queue post unified ISSU. PR1684019

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

- Multiple bbe-smgd core files get generated, resulting in subscribers being lost or failing to login in the Enhanced subscriber scenario. PR1685070

Infrastructure

- Public nexthops cleanup fails for "mpls" family nexthops on MX platforms. PR1608991

Interfaces and Chassis

- VRRP flaps between MC-LAG peers. PR1579016

- VRRP failover might occur over 2 seconds. PR1652549

- reth1 interface down and DCD core files are observed on node1. PR1657021

- When moving a few child members from one AE bundle to another AE bundle, you might observe the error log `UI_CONFIGURATION_ERROR: Process: dcd, path: none, statement: none, ae12, Micro BFD local address should be configured on ae12 or lo0`. PR1658016

- The MAC address might be learned over the incorrect interface in the MC-AE scenario. PR1658742

- The VRRP track might go down upon GRES. PR1668280

Layer 2 Ethernet Services

- The jdhcpd crash might occur in a DHCP Relay Agent scenario. PR1668015

- The DHCP unicast acknowledge packet might be dropped. PR1676573

MPLS

- P2MP LSP flaps after the MVPN CE facing interface goes down. PR1652439

- The rpd might generate the `@task_quit::task_assert::ted_delete_link::ted_delete_halflink_inc::rtlist_walker_job::task_job_run_common::task_job_run_job_bg::task_job_bg_dispatch` core file. PR1655031

- Memory utilization keeps incrementing due to the path error message. PR1657872

- LSPs are getting stuck in a down state after deactivating/activating protocol BGP. PR1659340

- The LSP might get stuck in the CSPF path computation stage. PR1661954

- Dynamic label space usage crossed the threshold limit of 90 percent. PR1664670

- Transit LSR might stop sending RESV message if there is no RRO in the LSP's PATH message. PR1667708

- Premature RSVP Path Error BW-Unavailable originated by PLR. PR1670638

- LDP traffic will be dropped silently when the L-ISIS/L-OSPF route changes due to interface level configuration. PR1671187

- The rpd crash might occur with container LSPs. PR1672804

- The rpd crashes very rarely when constructing LDP trace message irrespective of enable/disable LDP traceoptions. PR1676503

- The traffic might drop when the Link State protocol with the least preference is set to active and fails the CSPF algorithm. PR1677930

- In an LDP -> BGP LU stitching scenario, multiple LSPs will not be installed in the forwarding table, even if BGP Multipath and ECMP are enabled. PR1680574

- The Routing Engine crashes when MPLS next-hop is created and deleted frequently. PR1681892

Network Management and Monitoring

- Memory leak might occur in eventd leak during GRES. PR1602536

- The snmpd process might crash if SNMP timeout happens. PR1666548

- The snmpd core file might be observed with filter-duplicates configuration. PR1669510

- While loading MIB file, you might see the error `DESCRIPTION" is missing for "mib-jnx-chas-defines.txt`. PR1670858

Platform and Infrastructure

- The core interface goes down. PR1631217

- CCL-DT-BNG: show interface and monitoring interface (ifd level) counters are tripled. PR1651407

- RPM probes configured with target HTTP/HTTPS URLs will fail if the URL contains '[' or ']' PR1651489

- Multicast packet drop causes pixelization. PR1655363

- The MPC might crash for the IRB interface flap part of the layer 2 domain in a multicast scenario. PR1657983

- 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

Routing Policy and Firewall Filters

- The rpd process crashes whenever it shuts down with router reboot, rpd restart, Routing Engine switchover, or software upgrade. PR1670998

Routing Protocols

- RPD crashes upon receipt of specific OSPFv3 LSAs. PR1645221

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

- Traffic loss might be seen when the new Multicast Composite Next-Hop is computed. PR1651824

- "--RT--" memory is slowly incrementing in `show task memory detail` output. PR1657321

- The memory leak and process rpd crash might be observed when the peer interface flaps continuously in the Segment Routing. PR1659366

- 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 might not work. PR1660424

- Incorrect inactive routes are being propagated to neighbors with add-path. PR1660456

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

- The damping policy will not work as expected. PR1660571

- The v4 prefixes might not be advertised over the BGPv6 sessions. PR1664168

- The BSR information might not be flooded over NG-MVPN. PR1664211

- The rpd crashes while making configurational changes. PR1669716

- BGP inactive routes might not be advertised to peers in BGP-LU scenario. PR1669930

- The rpd crashes upon receiving BGP multi-nexthops inetflow route in the 21.4 software release and onward. PR1670630

- The backup next hop computation might not be as expected for some random prefixes when there is a topology change. PR1671672

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

- The IS-IS learnt routes might be downloaded to RIB again and again if the prefix attribute flags are different. PR1673953

- Label traffic will be dropped at the one-hop LSP stitching node if the packet has more than one label. PR1677567

- Inter-domain forwarding connectivity will be broken between different lo0s in the option-C network, causing problems for the MPLS transit-route. PR1677935

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

- RV task replication will be stuck in the "NotStarted" state when routing-options validation is deactivated/activated. PR1679495

Services Applications

- L2TP session might not come up when L2TP access-line-information is not configured. PR1667861

- VMcore or Routing Engine crash might be triggered due to the memory corruption when the FPC is restarted for LNS subscribers. PR1667950

Subscriber Access Management

- New service profile provided by Radius during re-authentication triggered by DHCP Renew packet with changed actual data rate TLVs might not be applied. PR1665947

- CoA-NAK might not be sent for a coa-request-retry of the same service. PR1667002

- Errors are seen when the accounting server source address is IPv6. PR1669284

User Interface and Configuration

- Unified ISSU failure might be seen due to timer expiry. PR1634334

- The message `gethostbyname: Host name lookup failure` displays during commit. PR1673176

VPNs

- Tunnel bringing up failed from strongswan when changing the configuration IKE in VR and observed the `NO_PROPOSAL_CHOSEN notify error` message. PR1627963

- Vmcore is seen on Junos platforms when you configure data plane IPSec. PR1648249

- Traffic drop might be seen when Inter-AS option-B label spoofing is configured along with vrf-table-label. PR1661542

- Core observed with multiple daemons restart. PR1682573

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 22.2R2

> *ⓘ* **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.

> (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.

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-
x86-32-22.2R2.9-signed.tgz
```

- For 64-bit Routing Engine version:

```
user@host> request system software add no-validate reboot source/junos-install-mx-
x86-64-22.2R2.9-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-
x86-32-22.2R2.x-limited.tgz
```

- For 64-bit Routing Engine version:

```
user@host> request system software add no-validate reboot source/junos-install-mx-
x86-64-22.2R2.9-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.

> **(i) 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.]

> **(i) 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 22.2R2

To downgrade from Release 22.2R2 to another supported release, follow the procedure for upgrading, but replace the 22.2R2 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 22.2R2 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 this release 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

- General Routing | **76**
- Interfaces | **77**
- Virtual Network Functions (VNFs) | **77**

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

Interfaces

- On NFX250 devices, the LACP subsystem is not started automatically when dc-pfe process is restarted. PR1583054

Virtual Network Functions (VNFs)

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

Resolved Issues

IN THIS SECTION

- Routing Protocols | 77

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

Routing Protocols

- The BSR information might not be flooded over NG-MVPN. PR1664211

Migration, Upgrade, and Downgrade Instructions

IN THIS SECTION

- Upgrade and Downgrade Support Policy for Junos OS Releases and Extended End-Of-Life Releases | 78

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

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

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

Upgrade and Downgrade Support Policy for Junos OS Releases 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.

> **(i) 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.

> **(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.

To download and install Junos OS Release 22.2R2:

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

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

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

3. Select the **Software** tab.

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

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

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

7. Review and accept the End User License Agreement.

8. Download the software to a local host.

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

10. Install the new package on the device.

Junos OS Release Notes for PTX Series

IN THIS SECTION

These release notes accompany Junos OS Release 22.2R2 for the PTX Series. They describe new and changed features, limitations, and known and resolved problems in the hardware and software.

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

What's New

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

What's Changed

IN THIS SECTION

- General Routing | **81**
- User Interface and Configuration | **81**

Learn about what changed in this release for PTX Series.

General Routing

- For PTX Series devices running Junos OS Evolved, software priority "medium-low" maps to hardware priority "medium" for normal scheduling mode and "low" for strict priority scheduling mode.

- sFlow configuration. sFlow configuration is allowed only on et, xe, and ge interfaces in EVO-based platforms. All other interfaces are blocked for configuring sFlow on EVO platforms. A cli error will be thrown if sFlow is configured on any other interface other than et, xe or ge interface.

User Interface and Configuration

- **Support for temperature sensor (PTX10001-36MR)**—We support the temperature sensor statement at the edit chassis cb hierarchy level. You can use the temperature sensor statement to increase the fan speed and customize the temperature threshold. We recommend certain values for ZR and ZR-M modules to work which helps the temperature to remain within the thresholds.

  See temperature-sensor.

Known Limitations

IN THIS SECTION

- MPLS | **82**

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 does not work if defined under a group. PR1637730

Open Issues

IN THIS SECTION

- General Routing | **83**
- Interfaces and Chassis | **84**
- Routing Protocols | **84**

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. PR1254415

- On routers and switches running Junos OS, 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 Aggregate Ethernet (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

- 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

- On PTX platforms, packets drop is seen because of increment in PCS and framing errors on some of the 100GE ports on PIC or its peer devices after firmware migration.PR1669267

- 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

Interfaces and Chassis

- On Junos PTX platforms, there might be a traffic silently droppped 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/AE interface, BFD Session state in Routing Engine remains as UP always even though PEER device has ceased.PR1675921

Resolved Issues

IN THIS SECTION

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

Class of Service (CoS)

- The default code-point aliases and respective CoS value Bit patterns are inconsistent with Junos.PR1667404

General Routing

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

- On Junos PTX platforms, the traffic silently dropping can occur after interface flaps. PR1645488

- BGP Sensor **/bgp-rib/afi-safis/afi-safi/ipv4-unicast/loc-rib/** not available as a 'periodic' sensor.
  PR1649529

- PCS Errored blocks count will increment after Junos software upgrade to 20.2R1 or above releases.
  PR1651526

- The Junos Telemetry interface sensors might not get reset after routing is restarted resulting in
  verification failure. PR1652372

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

- 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

Interfaces and Chassis

- 22.2TOT :SecPDT:Unified L4/L7 Use Case Sky ATP: reth1 interface down and DCD cores observed
  on node1 during test on 22.2TOT image. PR1657021

MPLS

- Premature RSVP Path Error BW-Unavailable originated by PLR. PR1670638

- The rpd crash might be observed with Container LSPs. PR1672804

- The traffic might drop when the Link State protocol with the least preference is set to active and fails
  the CSPF algorithm. PR1677930

- In an LDP -> BGP LU stitching scenario, multiple LSPs will not be installed in the forwarding table,
  even if BGP Multipath and ECMP are enabled. PR1680574

Migration, Upgrade, and Downgrade Instructions

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.

> (i) **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

> (i) **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 22.2R2:

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.

> *i* **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

Table 8: EOL and EEOL Releases *(Continued)*

Release Type	End of Engineering (EOE)	End of Support (EOS)	Upgrade/ Downgrade to subsequent 3 releases	Upgrade/ Downgrade to subsequent 2 EEOL releases
Extended End of Life (EEOL)	36 months	End of Engineering + 6 months	Yes	Yes

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

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

Upgrading a Router with Redundant Routing Engines

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

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

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

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

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

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

Junos OS Release Notes for QFX Series

IN THIS SECTION

These release notes accompany Junos OS Release 22.2R2 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

IN THIS SECTION

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.

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].

Known Limitations

IN THIS SECTION

-

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

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

General Routing

- 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 QFX10002/QFX10008/QFX10016 (only QFX10K) platforms, when Assisted Replication (AR) feature as Replicator role is used in an Ethernet VPN (EVPN) multi-homed scenario, You can see out-of-bound memory access issue that might result in the kernel crash leading to the service impact.PR1649234

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

- 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

- 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 VCP (Virtual Chassis Port) ports. As a result, ARP packets are dropped. PR1679684

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/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

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

Resolved Issues

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

- Upgrading Software on QFX Series Switches | 102

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.

> **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.

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

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

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

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

For example:

```
user@switch> request vmhost software add /var/tmp/junos-vmhost-install-qfx-x86-64-22.2R2.9.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

> (i) **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.

> (i) **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
```

> *(i)* **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
```

> (i) **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.

> (i) **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`.

    > **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

There are no changes in behavior and syntax in Junos OS Release 22.2R2 for SRX Series.

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.

Platform and Infrastructure

- During reboot, a warining message "warning: requires 'idp-sig' license" can be seen on the screen even when the device has valid license. PR1594014

- On SRX4600 platform, the CPU may overrun while performing sanity check due to incompatibility issues between ukern scheduler and Linux driver which might lead to traffic loss.PR1641517

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

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.

Application Layer Gateways (ALGs)

- On all SRX platforms, some SIP calls might get dropped when NAT is needed and the SIP ALG is enabledPR1686613

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

- 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

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

Platform and Infrastructure

- In Mac-OS platforms when Juniper Secure Connect client connects successfully, the client is not getting minimized to tray icon and needs to be minimized manually.PR1525889

- 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 closed on the device even though 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

- 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 SKYATP:IMAP/IMAPS Email permitted counter may have incorrect value under certain conditions.PR1646661

- 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

- SRX CLI command to show auth entry user detail "show services user-identification authentication-table ip-address" is failing when auth entry boundary testing with auth entry containing maximum length group-name and resource-group-name is used.PR1665691

- On SRX4600 platform, when using a cluster-id of 16 or higher post cluster node reboot, the fabric link will stay monitored down.PR1684756

- On SRX platform, when event mode logging is used without event-rate option, the logging rate was unexpectedly set to 100 although the default event rate is 1500PR1687244

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-modePR1653793

User Interface and Configuration

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

VPNs

- On SRX5400, SRX5600, and SRX5800 devices, during in-service software upgrade (ISSU), the IPsec tunnels flap, causing a disruption of traffic. The IPsec tunnels recover automatically after the ISSU process is completed. PR1416334

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

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

Resolved Issues

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

Application Layer Gateways (ALGs)

- The flowd crash might be observed on SRX5k series platforms where Central Point is present PR1658370

- SIP 200 OK(INVITE) response packets are dropped leading to SIP Call failure PR1677554

Chassis Clustering

- In the MNHA SRG scenario on the IPv6 switching mode, not using 'Virtual MAC' as the source MAC address for G-NDP PR1670309

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

Class of Service (CoS)

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

Flow-Based and Packet-Based Processing

- The hardware acceleration flag was not properly updated on RT_FLOW_SESSION_CLOSE logs. Additionally, the values for "Services-offload-sessions" for customers using SPC2's in their SRX5000-Series devices was incorrect. PR1629216

- The gre-performance-acceleration might cause VPLS traffic drop PR1661409

- In SD-WAN the association between VRF instance and VRF group fails for ISSU from 19.2~21.1 to 22.2R1 PR1661935

- vSRX not processing fragmented packets PR1668898

- On SRX5K series devices with IOC2 line-cards installed, when running JUNOS 21.2R1 or later where Automated Express Path is enabled by default, sessions traversing the IOC2 card may time out early, leading to traffic loss and unpredictable flow behaviour. This issue does not affect traffic traversing IOC3 and IOC4 cards. PR1688658

Interfaces and Chassis

- 22.2TOT :SecPDT:Unified L4/L7 Use Case Sky ATP: reth1 interface down and DCD cores observed on node1 during test on 22.2TOT image PR1657021

J-Web

- Various page errors have been corrected in JWeb PR1658330

- J-Web page not properly loaded for a user using a username including .(dot) PR1665006

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

Network Address Translation (NAT)

- The NAT ports exhaust when address-pooling pair is configured in SRX devices PR1651939

Network Management and Monitoring

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

Platform and Infrastructure

- 21.4R1:IPSEC:pkid.core-tarball found @ pkid_request_security_pki_local_cert_verify (msp=0x1abc940, csb=0xffffdb60, unparsed=0x1a7402e "certificate-id") at ../../../../../../src/junos/usr.sbin/pkid/pkid_ui.c:1076 PR1624844

- A major alarm DPDK (data plane development kit) Tx stuck issue of SRX4100/4200 PR1626562

- SMS Channel Down alarm on primary node of HA pair after upgrade PR1629972

- 22.1TOT : SnP :SRX5K_SPC3 : Observing Error "usp_ipc_client_recv_:ipc_pipe_read() " due to coredump,when checking "show security monitoring" cli command, in the latest 22.1(22.1I-20220108.0.0529) build. PR1641995

- 21.3R2:NCP Secure Connect:Licensing: remote-access-juniper-std license not getting freed up while disconnect/reconnect after RG0 failover PR1642653

- Packet loss might be seen on SRX4100 and SRX4200 devices from 20.2R2 PR1650112

- 22.1R1:AUTH:unable to get the "firewall-authentication users" details on node 1 PR1651129

- The fxp0 interface might remain 'UP' when the cable is disconnected PR1656738

- 22.2R1:: MISC:: mspmand core found @sarena_free @mum_free @jsf_shm_free @jssl_mem_pool_free @jsf_openssl_free @CRYPTO_free @ssl_cert_free @jssl_config_dtor @msvcs_plugin_send_control_rt PR1657027

- Archived file which created by non-root user may not include some files under /var/log/ directory PR1657958

- The PFE may crash when a large amount of traffic is submitted to ATP Cloud for inspection PR1661766

- Ssl-proxy: Cache miss counter increments twice instead of one PR1663678

- SRX alarming "SMS control channel down" without SMS feature configured PR1666420

- 22.1 DCB: IPv6 feature not working on 5K platform. PR1668473

- The Forwarding plane crashes during HA failover PR1672378

- Information about users groups is not displayed completely PR1673125

- A FlowD crash might occur when AAMW (Advanced-Anti-Malware) encounters a memory leak
  PR1675722

- Netbios traffic (IRB broadcast) is getting dropped post upgrade on the SRX platform PR1675853

- PKID process crashes when validating the certificate chain of a certificate PR1679067

- "NSD_CLEAR_POLICY_DNS_CACHE_ENTRY_IP" log is not found on the device after keeing DNS
  cache entry unchanged PR1684268

Routing Policy and Firewall Filters

- The utility 'monitor security packet-drop' now correctly reports policy-related drops for unified policy
  (includes the exact policy that dropped the packet) PR1576150

- Security policy state may be invalid on SRX platforms PR1669386

- The rpd process crashes whenever it is getting shut down with router reboot, rpd restart, RE
  switchover, software upgrade PR1670998

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

Routing Protocols

- The BSR information might not be flooded over NG-MVPN PR1664211

User Interface and Configuration

- IPSec tunnel will flap post MNHA configuration commit PR1669104

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

VLAN Infrastructure

- Traffic Stops when the mac address of a node changes in L2 secure-wire SOF PR1597681

- OSPF neighbor won't establish under Transparent mode when neighborship across different zone
  PR1599891

VPNs

- 21.4Th :SPC3-Config payload :Tunnel bringing up failed from strongswan when changing the
  configuration IKE in VR and observed the " NO_PROPOSAL_CHOSEN notify error" message
  PR1627963

- Severity is unknown at some IPSec syslog messages PR1629793

- Vmcore is seen on Junos platforms when data plane IPSec is configured PR1648249

- The Juniper secure connect VPN users may face login issues intermittently PR1655140

- Packets traversing through a policy-based VPN get dropped when PowerMode is enabled
  PR1663364

- IPSec tunnels may flap on SRX platforms PR1665332

- 22.2R1: Master Password for Configuration Encryption and FIPS mode should not be enabled
  together PR1665506

- High Control Plane CPU utilisation while the kmd process is stuck after the core file PR1673391

Migration, Upgrade, and Downgrade Instructions

IN THIS SECTION

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

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

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

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

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

We have two types of releases, 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

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

Known Limitations

There are no known limitations in hardware and software in Junos OS 22.2R2 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

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 is configured to run in performance mode through the chassis fpc 0 performance-mode command, 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 of flow actions the riot processmight stop. It is a rare issue. PR1534145

Resolved Issues

There are no resolved issues in Junos OS Release 22.2R2 for vMX.

Upgrade Instructions

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

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

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

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

Junos OS Release Notes for vRR

IN THIS SECTION

These release notes accompany Junos OS Release 22.2R2 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 22.2R2 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 22.2R2 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 22.2R2 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

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

Known Limitations

There are no known limitations in hardware and software in Junos OS 22.2R2 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

- We recommend 1 to 2 minutes gap between two configuration commits if there are lots of security policies which need time to be processed. PR1625531

Platform and Infrastructure

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

VPNs

- In certain cases, when using group VPN, the PUSH ACK message from the group member to the group key server might 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

- traffic in the power-mode still passthrough when the ingress logic interface is manually disabled PR1604144

- Expected TCP sequences not found in ICMP6 dump PR1611202

- vSRX not processing fragmented packets PR1668898

J-Web

- Various page errors have been corrected in JWeb PR1658330

Network Address Translation (NAT)

- Datapath daemon might crash resulting in total traffic and service failure PR1645039

Platform and Infrastructure

- AMR first session traffic is not copying over multiple paths for v6 traffic over v6 ipsec tunnel mode PR1643570

- Ssl-proxy: Cache miss counter increments twice instead of one PR1663678

- VSRX 3.0 | Eval license reappears after deletion and reboot. PR1664434

- SRX alarming "SMS control channel down" without SMS feature configured PR1666420

- "NSD_CLEAR_POLICY_DNS_CACHE_ENTRY_IP" log is not found on the device after keeing DNS cache entry unchanged PR1684268

Routing Policy and Firewall Filters

- The utility 'monitor security packet-drop' now correctly reports policy-related drops for unified policy (includes the exact policy that dropped the packet) PR1576150

VPNs

- 22.4DCB-PCT:"ipsec tunnel-events-statistics" is not coming as expected while Verifying IPv4 Auto-VPN in point-to-multipoint mode using IKEv2 with DUT as spoke with latest DCB PR1669110

Migration, Upgrade, and Downgrade Instructions

IN THIS SECTION

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

You also can upgrade to Junos OS Release 22.2R1 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 9, Junos OS Release 22.2R2.

15 August 2025—Revision 8, Junos OS Release 22.2R2.

3 April 2025—Revision 7, Junos OS Release 22.2R2.

27 March 2025—Revision 6, Junos OS Release 22.2R2.

20 July 2023—Revision 5, Junos OS Release 22.2R2.

1 June 2023—Revision 4, Junos OS Release 22.2R2.

9 March 2023—Revision 3, Junos OS Release 22.2R2.

25 November 2022—Revision 2, Junos OS Release 22.2R2.

9 November 2022—Revision 1, Junos OS Release 22.2R2.