Release Notes

Published
2023-08-09

Junos® OS Release 22.1R3

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 22.1R3 for the ACX Series, cSRX Container Firewall (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, virtual MX Series router (vMX), Virtual Route Reflector (vRR), and vSRX Virtual Firewall (vSRX). They describe new and changed features, limitations, and known and resolved problems in the hardware and software.

JUNIPER NETWORKS | Engineering Simplicity

Table of Contents

Junos OS Release Notes for ACX Series

IN THIS SECTION

These release notes accompany Junos OS Release 22.1R3 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 routers.

Known Limitations

IN THIS SECTION

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

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

Infrastructure

- When upgrading from Junos OS Release 21.2 to later releases, validation and upgrade might fail. The upgrading requires using of the `no-validate` configuration statement. PR1568757

Open Issues

IN THIS SECTION

Learn about open issues in Junos OS Release 22.1R3 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

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

- On ACX platforms, traffic issue might be observed with downstream devices when Precision Time Protocol(PTP) is configured (G.8275.1 PTP profile) along with PHY timestamping and Multiprotocol Label Switching (MPLS) terminated on 10G interface. The transit PTP ipv4 packets are updated with wrong Correction Factor(CF). This issue could be restored by disabling PHY stamping. However, disabling might impact the PTP performance. PR1612429
- On ACX5448 devices with VM Host-based platforms, starting with Junos 21.4R1 or later, you need the SSH and root login for copying line card image 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 the SSh configuration to allow internal trusted communication. PR1629943
- On ACX5448 devices, Junos OS does not support Hierarchical-scheduler (HQOS) on MPLS (Core facing) interface. Enabling HQOS on MPLS Core facing interface causes unexpected traffic forwrading behavior. PR1630086
- On ACX5048 and ACX5096 devices, Junos OS does not support interface speed 10m on 1G interface. PR1633226
- On ACX5448 and ACX710 devices, all types of delegated BFD sessions configured on routing-instance other than the default routing-instance might not come up.PR1633395
- On ACX710 devices, the rpd process might generate core files. . The rpd process keeps running and there is no functional impact. PR1663050
- On ACX5000 devices, 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. PR1665178
- Due to race condition at the time of streaming and simultaneous disconnection of clients, the na-grpcd process might generate core files at rare ocassions. This issue causes temporary outage of streaming telemetry services. The service will self recover upon restart of the process. PR1665516
- When there are more than 1 DHCP server connected to the device and zeroize in initiated then multiple route are added and the file server is not reachable after the zeroize if it is not reachable through the default route. PR1675011

Resolved Issues

IN THIS SECTION

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

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

EVPN

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

General Routing

- On ACX710 and ACX5448 devices working as a PE device stops forwarding Layer 3 VPN traffic after core-facing link flaps. PR1635801
- If a firewall has a log action and applied on physical interface or lo0, the LDP are not able to go up. PR1648968
- HTTP(S) file download becomes nonresponsive over EVPN-ETREE. PR1653531
- On ACX5448 devices, physical interfaces of FPC remain up even though it lost communication with the Routing Engine. PR1659949
- The Layer 2 circuit backup might not get reverted to primary in rare condition. PR1661802
- On ACX5448 devices, Packet Forwarding Engine might crash after activating EVPN-ETREE service. PR1662686

- Multicast upstream interface does not change to back up link when you remove or flap the PIM neighbor, and causes traffic. PR1663271
- Adding an empty interface to an aggregated Ethernet interface bundle causes traffic drop. PR1663651
- FXPC process might generate core files when deactivating a child memeber link from the aggregated Ethernet interface bundle. PR1665511
- In the SRTE scenario, sensors gets incorrectly populated for colored tunnel BSID routes when you enable uncolored tunnels. PR1665943
- Traffic loss occurs when you configure the VRRP over the aggregated Ethernet interface. PR1666853
- On ACX710 and ACX5448 devices, the variants Packet Forwarding Engine might crash due to the configuration of BFD. PR1667129
- Shutting the CE interface and bringing back up causes traffic (going towards the core) drops. PR1667724
- LLDP neighborship might fail if the chassis-id format of the LLDP packet is xx:xx:xx:XX:XX:xx. PR1669677
- On ACX710 devices, log related to resources gets reported after you activateor deactivate EVPN RI multiple times: `ACX_BD_ERR: dnx_bd_alloc_l2_svlan: System reached L3 IFL and BD limit(12286).` PR1670683
- The chassisd memory gets corrupted and the chassisd crashes. PR1672039
- MX-SPC3 PIC process generates core file when you modify a CPCD service. PR1675990
- The LLDP packets does not get transmitted over the Layer 2 circuit. PR1678752
- On ACX5448 devices, the RIO DNX Packet Forwarding Engine incorectly spelled as `QUMARN` instead of `Qumran`. PR1682819
- On ACX710 devices, the IEEE 802.1p priority and DEI values in the locally generated VLAN-based IP packets might be changed when sourced from the IRB interface. PR1683770
- On ACX5448 and ACX710 devices, the Layer 2 circuit traffic drops with control-word enabled or control-word configuration change. PR1683900
- EVPN Traffic is classfied in the wrong queue. PR1689604

Network Management and Monitoring

- The snmpd process might generate core file with filter-duplicates configuration. PR1669510

Routing Protocols

- IPv6 Inline BFD sessions goes down when neighbor does not get resolved. PR1650677
- Routing Process Daemon (rpd) crashes and restarts when a specific timing condition is hit with BGP configuration. PR1659441
- MCSNOOPD will be restarted and will again learn the states after core. PR1672488

Migration, Upgrade, and Downgrade Instructions

IN THIS SECTION

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

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

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

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

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

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

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

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

For EEOL releases only, you have an additional option - you can upgrade directly from one EEOL release to the next two subsequent EEOL releases, even if the target release is beyond the next three releases. Likewise, you can downgrade directly from one EEOL release to the previous two EEOL releases, even if the target release is beyond the previous three releases. For example, 20.4 is an EEOL release. Hence, you can upgrade from 20.4 to the next two EEOL releases – 21.2 and 21.4 or downgrade to the previous two EEOL releases – 20.2 and 19.4.

Table 1: EOL and EEOL Releases

Release Type	End of Engineering (EOE)	End of Support (EOS)	Upgrade/ Downgrade to subsequent 3 releases	Upgrade/ Downgrade to subsequent 2 EEOL releases
Standard End of Life (EOL)	24 months	End of Engineering + 6 months	Yes	No
Extended End of Life (EEOL)	36 months	End of Engineering + 6 months	Yes	Yes

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

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

Junos OS Release Notes for cSRX

IN THIS SECTION

These release notes accompany Junos OS Release 22.1R3 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 or software in this release for cSRX.

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

Open Issues

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

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

Resolved Issues

There are no resolved issues in this release for cSRX.

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

Junos OS Release Notes for EX Series

IN THIS SECTION

These release notes accompany Junos OS Release 22.1R3 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

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.

Platform and Infrastructure

- Once vxlan is configured on an IFD, its always treated as vlxan port even though L2 vlan exists.PR1570689
- On EX4600 and QFX5xx0 platforms, we should configure only one static arp with multicast-mac entry per IRB interface. If we configure more than one static arp with multicast Mac entry per IRB interface, then the packets with different destination IP having static multicast mac will always go out with any one of the multicast mac configured in the system. PR1621901
- On EX4300-MP platforms, when the command `request system software rollback` is performed device is going down and dcpfe generates core files.PR1631640
- 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

Open Issues

IN THIS SECTION

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

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

Class of Service (CoS)

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

Infrastructure

- Auxiliary serial port (type USB-C on the front panel) does not show any output. PR1616315
- There is a possibility of kernel crash when the system will be in the process of coming up after reboot (and observed only with multiple iterations of continuous reboot ccyles). This is observed only during init sequence of mgmt driver and impact is limited to increased system boot time. PR1642287

Platform and Infrastructure

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

- Runt, fragment and jabber counters are not incrementing on EX4300-MPs. PR1492605
- When running the command: `show pfe filter hw filter-name filter name`, the command fails to retrieve the PFE programming details of the filter. PR1495712
- A delay of 35 seconds is added in reboot time in Junos OS Release 20.2R1 compared to Junos OS Release 19.4R2. PR1514364
- During Routing Engine switchover interface flap might be seen along with Scheduler slippage. PR1541772
- On EX2300, EX3400,:EX4300-48MP and EX4300, pause frames counters do 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
- Due to an Improper Initialization vulnerability in Juniper Networks Junos OS on EX4650 devices, packets received on the management interface (em0) but not destined to the device, might be improperly forwarded to an egress interface, instead of being discarded. Refer to https://kb.juniper.net/JSA69494 for more information. PR1628754
- FXPC core file is seen while loading Junos OS 21.3R3.1 MR build with `abort,junos_abort,panic, dcbcm_discover,pic_discover ,cmqfx_pic_sw_init,cmqfx_all_pic_sw_init ,cmqfx_module_init ()`. PR1660130
- EX4600 and QFX5100-24Q devices VC (Virtual chassis) is in unstable state for 3-7 minutes, causing traffic loss.PR1661349
- On certain units, with `set system ports console log-out-on-disconnect`, when you log in to the device through a console, the user will be ejected out to the login prompt and be asked to log in again. PR1680408
- On EX4300-48MP, NSSU abort is seen with `error: rebooting VC". VC instability and dc-pfe core` is observed after reboot.PR1668414
- When the DHCP relay mode is configured as no-snoop, we are observing the offer gets dropped due to incorrect asic programming. This issue only affects while running DHCP relay on EVPN/VXLAN environment. PR1530160
- EX4400-48MP - VM cores and VC split might be observed with multicast scale scenario. PR1614145
- 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 might incorrectly go into blocking state. PR1673000

Resolved Issues

IN THIS SECTION

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

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

Forwarding and Sampling

- Traffic drop seen and filter not hitting as expected for match condition traffic class with FLT option. PR1573350

Network Management and Monitoring

- Observed memory leak in eventd leak during GRES. PR1602536
- The "snmpd" process might crash if SNMP timeout happens. PR1666548

Platform and Infrastructure

- DHCP traffic might be dropped when DHCP-security and RTG are enabled. PR1647209
- 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
- The show chassis led output does not match the LED behaviour. PR1656611
- LEDs on ports 0-35 are always lit on EX4400-48MP platforms. PR1662288
- In the EVPN-VXLAN scenario, the DHCP packets will get dropped when the DHCP relay agent is configured. PR1662524
- 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 with 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
- 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 members interface is removed from LAG. PR1676772
- AE interface will receive unknown unicast traffic on FPC3 reboot of a VC. PR1678430
- DHCP binding will fail for the clients (Clients connected on an AE interface with 2 or more VLANs) on a VLAN where DHCP security is not configured. PR1679094
- Licenses on the device might become invalid when the device is upgraded from a legacy licensing-based release to an Agile licensing-based release. PR1684842
- MAC address learning might not happen on specific EX/QFX platforms. PR1685938
- EX9000 and MX platforms do not relay a DHCP offer with a broadcast flag under EVPN-VXLAN scenario. PR1670923
- The fxpc process crash might be observed on EX4300 and EX4300-VC platforms. PR1675977

Virtual Chassis

- On Junos (EX4600, EX4650, QFX5000 VC) platforms, line card might be disconnected from VC post master Routing Engine reboot. PR1669241

Documentation Updates

There are no corrections or changes in Junos OS Release documentation for the EX Series documentation.

Migration, Upgrade, and Downgrade Instructions

IN THIS SECTION

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

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

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

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

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

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

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

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

For EEOL releases only, you have an additional option - you can upgrade directly from one EEOL release to the next two subsequent EEOL releases, even if the target release is beyond the next three releases. Likewise, you can downgrade directly from one EEOL release to the previous two EEOL releases, even if the target release is beyond the previous three releases. For example, 20.4 is an EEOL release. Hence, you can upgrade from 20.4 to the next two EEOL releases – 21.2 and 21.4 or downgrade to the previous two EEOL releases – 20.2 and 19.4.

Table 2: EOL and EEOL Releases

Release Type	End of Engineering (EOE)	End of Support (EOS)	Upgrade/ Downgrade to subsequent 3 releases	Upgrade/ Downgrade to subsequent 2 EEOL releases
Standard End of Life (EOL)	24 months	End of Engineering + 6 months	Yes	No
Extended End of Life (EEOL)	36 months	End of Engineering + 6 months	Yes	Yes

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

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

Junos OS Release Notes for JRR Series

IN THIS SECTION

These release notes accompany Junos OS Release 22.1R3 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 and software in this release for JRR Series Route Reflectors.

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

Resolved Issues

IN THIS SECTION

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

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

- All Junos OS platforms face the issue of 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
- A 802.1Q tagged Ethernet traffic with an expected VLAN ID and with a non-zero 802.1P value ingressing a JRR200 VLAN enabled interface is dropped. The issue is vissible in JRR200 system running Junos OS release 21.1 and later.PR1691694

Migration, Upgrade, and Downgrade Instructions

IN THIS SECTION

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

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

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

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

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

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

For EEOL releases only, you have an additional option - you can upgrade directly from one EEOL release to the next two subsequent EEOL releases, even if the target release is beyond the next three releases. Likewise, you can downgrade directly from one EEOL release to the previous two EEOL releases, even if the target release is beyond the previous three releases. For example, 20.4 is an EEOL release. Hence, you can upgrade from 20.4 to the next two EEOL releases – 21.2 and 21.4 or downgrade to the previous two EEOL releases – 20.2 and 19.4.

Table 3: EOL and EEOL Releases

Release Type	End of Engineering (EOE)	End of Support (EOS)	Upgrade/ Downgrade to subsequent 3 releases	Upgrade/ Downgrade to subsequent 2 EEOL releases
Standard End of Life (EOL)	24 months	End of Engineering + 6 months	Yes	No
Extended End of Life (EEOL)	36 months	End of Engineering + 6 months	Yes	Yes

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

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

Junos OS Release Notes for Juniper Secure Connect

IN THIS SECTION

These release notes accompany Junos OS Release 22.1R3 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 or software in this release for Juniper Secure Connect.

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

Open Issues

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

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

Resolved Issues

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

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

Junos OS Release Notes for Junos Fusion for Enterprise

IN THIS SECTION

These release notes accompany Junos OS Release 22.1R3 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 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 open issues in hardware and 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 Enterprise.

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

Migration, Upgrade, and Downgrade Instructions

IN THIS SECTION

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

Basic Procedure for Upgrading Junos OS on an Aggregation Device

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

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

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

The installation process rebuilds the file system and completely reinstalls Junos OS. Configuration information from the previous software installation is retained, but the contents of log files might be erased. Stored files on the routing platform, such as configuration templates and shell scripts (the only exceptions are the `juniper.conf` and `ssh` files), might be removed. To

preserve the stored files, copy them to another system before upgrading or downgrading the routing platform. See the Junos OS Administration Library.

To download and install Junos OS:

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

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

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

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

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

5. Select the **Software** tab.

6. Select the software package for the release.

7. Review and accept the End User License Agreement.

8. Download the software to a local host.

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

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

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

    Customers in the United States and Canada, use the following commands, where *n* is the spin number.

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

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

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

Replace *source* with one of the following values:

- */pathname*—For a software package that is installed from a local directory on the router.
- For software packages that are downloaded and installed from a remote location:
  - **ftp://** ***hostname/pathname***
  - **http://** ***hostname/pathname***
  - **scp://** ***hostname/pathname*** (available only for Canada and U.S. version)

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

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

Rebooting occurs only if the upgrade is successful.

Upgrading an Aggregation Device with Redundant Routing Engines

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

1. Disable graceful Routing Engine switchover (GRES) on the master Routing Engine and save the configuration change to both Routing Engines.
2. Install the new Junos OS release on the backup Routing Engine while keeping the currently running software version on the master Routing Engine.
3. After making sure that the new software version is running correctly on the backup Routing Engine, switch over to the backup Routing Engine to activate the new software.
4. Install the new software on the original master Routing Engine that is now active as the backup Routing Engine.

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

Preparing the Switch for Satellite Device Conversion

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

Converting a Satellite Device to a Standalone Switch

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

Upgrade and Downgrade Support Policy for Junos OS Releases

Support for upgrades and downgrades that span more than three Junos OS releases at a time is not provided, except for releases that are designated as Extended End-of-Life (EEOL) releases. EEOL releases provide direct upgrade and downgrade paths—you can upgrade directly from one EEOL release to the next EEOL release even though EEOL releases generally occur in increments beyond three releases.

You can upgrade or downgrade to the EEOL release that occurs directly before or after the currently installed EEOL release, or to two EEOL releases before or after. For example, Junos OS Releases 19.3,

19.4, and 20.1 are EEOL releases. You can upgrade from Junos OS Release 19.3 to Release 19.4 or from Junos OS Release 19.3 to Release 20.1.

You cannot upgrade directly from a non-EEOL release to a release that is more than three releases ahead or behind. To upgrade or downgrade from a non-EEOL release to a release more than three releases before or after, first upgrade to the next EEOL release and then upgrade or downgrade from that EEOL release to your target release.

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

Downgrading Junos OS

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

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

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

Junos OS Release Notes for Junos Fusion Provider Edge

IN THIS SECTION

These release notes accompany Junos OS Release 22.1R3 for Junos Fusion 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 Provider Edge.

What's Changed

There are no changes in behavior and syntax in this release for Junos Fusion Provider Edge.

Known Limitations

There are no known limitations in hardware or software in this release for Junos Fusion 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 and software in this release for Junos Fusion 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

Learn about the issues fixed in this release for Junos Fusion Provider Edge.

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 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 22.1R3 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/jinstall64-22.1R3.SPIN-domestic-signed.tgz
```

- For 32-bit software:

```
user@host> request system software add validate reboot source/jinstall-22.1R3.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/jinstall64-22.1R3.SPIN-export-signed.tgz
```

- For 32-bit software:

```
user@host> request system software add validate reboot source/jinstall-22.1R3.SPIN-export-signed.tgz
```

Replace *source* with one of the following values:

- */pathname*—For a software package that is installed from a local directory on the router.
- For software packages that are downloaded and installed from a remote location:
  - **ftp://** ***hostname/pathname***
  - **http://** ***hostname/pathname***
  - **scp://** ***hostname/pathname*** (available only for the Canada and U.S. version)

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

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

Rebooting occurs only if the upgrade is successful.

NOTE: After you install a Junos OS Release 22.1R3 `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 22.1R3, you must also upgrade your satellite device to Satellite Device Software version 3.1R1.

Upgrade and Downgrade Support Policy for Junos OS Releases

Support for upgrades and downgrades that span more than three Junos OS releases at a time is not provided, except for releases that are designated as Extended End-of-Life (EEOL) releases. EEOL releases provide direct upgrade and downgrade paths—you can upgrade directly from one EEOL release to the next EEOL release even though EEOL releases generally occur in increments beyond three releases.

You can upgrade or downgrade to the EEOL release that occurs directly before or after the currently installed EEOL release, or to two EEOL releases before or after. For example, Junos OS Releases 19.3, 19.4, and 20.1 are EEOL releases. You can upgrade from Junos OS Release 19.3 to Release 19.4 or from Junos OS Release 19.3 to Release 20.1.

You cannot upgrade directly from a non-EEOL release to a release that is more than three releases ahead or behind. To upgrade or downgrade from a non-EEOL release to a release more than three releases before or after, first upgrade to the next EEOL release and then upgrade or downgrade from that EEOL release to your target release.

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

Downgrading from Junos OS Release 22.1

To downgrade from Release 22.1 to another supported release, follow the procedure for upgrading, but replace the 22.1R3`jinstall` package with one that corresponds to the appropriate release.

NOTE: You cannot downgrade more than three releases.

For more information, see the Installation and Upgrade Guide.

Junos OS Release Notes for MX Series

IN THIS SECTION

These release notes accompany Junos OS Release 22.1R3 for the MX Series. They describe new and changed features, limitations, and known and resolved problems in the hardware and software.

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

What's New

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

What's Changed

IN THIS SECTION

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

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

IN THIS SECTION

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

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

General Routing

- Currently, IP options are not supported for egress firewall attach points, relevant supporting doc attached https://www.juniper.net/documentation/us/en/software/junos/routing-policy/t opics/concept/firewall-filter-match-conditions-for-ipv4-traffic.html. The issue might occur IP-options router alert traffic not hitting the egress firewall filter. PR1490967
- BUM (Broadcast, Unknown Unicast, and Multicast) traffic replication over VTEP is sending out more packets than expected and there seems to be a loop. PR1570689
- On all MX Series platforms, changing configuration AMS 1:1 warm-standby to load-balance or deterministic NAT might result in vmcore and cause traffic loss. PR1597386
- When a packet, which triggers ARP resolution, hits services interface style filter on the output will have session create and close log with incorrect ingress interface. This typically occurs with the first session hitting such a filter. PR1597864
- We should configure only one static ARP with multicast-mac entry per IRB interface. If we configure more than one static ARP with multicast MAC entry per IRB interface, then the packets with different destination IP having static multicast MAC will always go out with any one of the multicast MAC configured in the system. PR1621901
- This is a product limitation for MX-SPC3 with new junos-ike architecture. The issue is seen when we have any-any TS configured and any-any TS negotiated (both in IPv4 and IPv6). As a workaround, do not configure any-any TS when it is sure that negotiated traffic selector for the IPsec tunnel will also be any-any. When there is no TS configured, the scenario might be treated as proxy-id case and bypasses the issue without having any impact on the described scenario. PR1624381
- Changing the root-authentication password in cpce does not bring down the existing session. The password change will be in effect for all new connections. PR1630218
- The available space check in case of: 1. Upgrade is 5 GB 2. Fresh Install is 120 GB. The scenario Upgrade/Fresh-Install is decided from within RPM spec that is if RPM finds any older version is already installed. Since RPM-DB is destroyed during LTS-19 (vm-host) upgrade, rpm install scripts deduce the upgrade as fresh-install and look for 120GB free space. The warning can be ignored, as it has no functional impact. PR1639020
- On MX operating as a SAEGW-U/UPF at high mobile session scale (around 1 Million sessions), `show services mobile-edge sessions extensive` will not work. Mobiled process will take exception and generates core files. PR1639595

Infrastructure

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

Network Management and Monitoring

- Configuring the `set system no-hidden-commands` blocks NETCONF sessions. As a workaround, customer can disable the `no-hidden-commands`. PR1590350
- When an ephemeral instance is being edited, if `show ephemeral-configuration merge` command is run from another terminal, then the uncommitted changes in the ephemeral instance being edited will also appear in the output of `show ephemeral-configuration merge` command. PR1629013

Platform and Infrastructure

- Deactivating services rpm/rpm-tracking does not remove the tracked route from the routing or forwarding tables. 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 seconds to 8 seconds. This indirectly impacts the BFD session because the BFD session has a Routing Engine-based detect time of 7.5 seconds to expire. PR1600684

Routing Protocols

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

VPNs

- In some scenario (for example, configuring firewall filter), routers might show obsolete IPsec SA and NHTB entry even when the peer tear down the tunnel. PR1432925

Open Issues

IN THIS SECTION

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

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

Class of Service (CoS)

- Platform dependency-state error is seen on cosd. PR1649388
- Show Class-of-service Interface might not show the Classifier bind info on an IFL with only Inet/Inet6 (without family mpls or not with any rewrite rules). Show issue, Classifier will be still present and functional. There is no impact to the traffic. PR1652342

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

EVPN

- A few duplicate packets might be seen in an A/A EVPN scenario when the remote PE device sends a packet with an IM label due to MAC not learned on the remote PE device, but learned on the A/A local PE device. The nondesignated forwarder sends the IM-labeled encapsulated packet to the PE-CE interface after MAC lookup instead of dropping the packet, which causes duplicate packets to be seen on the CE side. PR1245316
- In Provider Backbone Bridging - Ethernet VPN (PBB-EVPN) environment, ARP suppression feature which is not supported by PBB might be enabled unexpectedly. This could cause MAC addresses of remote CEs not to be learned and hence traffic loss. PR1529940
- EVPN-MPLS multi-homing control MACs are missing after vlan-id removal and adding back on a trunk IFL of one of the multi-homing PEs. This is not a recommended way to modify vlan-id configuration. Both MH PEs need to be in symmetric always . PR1596698
- 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 workaround, perform the following steps:
  - Clear auto-evpn ce-interface interface-name.
  - Configure editactivate interface-name family inet inet6.

  PR1630627

Flow-based and Packet-based Processing

- Use an antireplay window size of 512 for IPv4 or IPv6 in fat-tunnel. The ESP sequence check might otherwise report out-of-order packets if the fat-tunnel parallel encryption is within 384 packets (12 cores * 32 packets in one batch). Hence, there are no out-of-order packets with 512 antireplay window size. PR1470637

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

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

- The following IPC timeouts logs might be seen for statistics query to kernel (queried from CLI or daemons querying internally) when there is configuration churn, or large number of IPCs getting exchanged between kernel and 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

- The memory usage of the rpd process on the backup routing engine might increase indefinitely due to leak in krt_as_path_t. PR1614763
- On EVO platforms during lacpd process restart, child IFD indexes from the port options IFD based data, which gets stored in kernel by lacpd, might not get reused due to old indexes not being freed. When this occurs, new indexes might be generated repeatedly, which might cause the port numbers exhaustion problem in Aggregated Ethernet (ae) interface bundle.PR1647145
- The transportd.core core file is seen with fabric configuration. PR1649019
- Due to the issue, there is an error log printed and DCD is restarted. But there is no functionality impact for BFD sessions. There may be a slight delay in the new configuration to take effect as DCD is restarted.

  PR1658016

Juniper Extension Toolkit (JET)

- In Junos OS Evolved, there are two different gRPC Python files for each JAPI file. The names of the files are *pb2_grpc.py and *pb2.py. The stub creation functions are present in *pb2_grpc.py. PR1580789
- Until Junos OS Release 21.3 release mgd is 32-bit binary on EVO. libsi can only be linked with 64-bit binaries. To access data/WAN ports in EVO we need libsi to be linked with the binary. By default the shell on the EVO device includes libsi, but it's not available to CLI commands as CLI will make mgd invoke cscript to run a Python script via CLI. PR1603437

MPLS

- BFD session flaps during unified ISSU only in mpc7e card (BFD sessions from other cards of DUT to peer routers did not flap during ISSU). The issue is not seen frequently. PR1453705
- Single hop BFD sessions might sometimes flap after GRES in highly scaled setups which have RSVP link or link-node-protection bypass enabled. This happens because sometimes RSVP neighbor goes down after GRES if RSVP hellos are not received after GRES before neighbor timeout happens. As a result of RSVP neighbor going down, RSVP installs a /32 route pointing to bypass tunnel which is required to signal backup LSPs. This route is removed when all LSPs stop using bypass after link comes back up. The presence of this /32 route causes BFD to flap. PR1541814
- 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
- The `use-for-shortcut` statement is meant to be used only in SR-TE tunnels which use SSPF (Strict SPF Algo 1) prefix SIDs. If `set protocols isis traffic-engineering family inet-mpls shortcuts` and `set protocols isis traffic-engineering tunnel-source-protocol spring-te` are configured on a device, and if any SR-TE tunnel using Algo 0 prefix SIDs is configured with `use-for-shortcut` statement, it could lead to routing loops or rpd core files. PR1578994
- When there is scaled RSVP sessions [~21K] and have enabled RSVP for all the interfaces, RPD process walks through all the interfaces, which results in high CPU usage for some time, which also results in LSP flap. PR1595853
- With the `chained-composite` statement enabled, the following statement does not have any effect if ingress and egress ports are on the same Packet Forwarding Engine instance on the line card (FPC). For example, the outer label TTL would not be set as 255. Instead, it would be set as (ip TTL-1). PS: This issue is not seen if ingress and egress ports are on different FPC slots or on difference Packet Forwarding Engine instances of the same FPC. `set protocols mpls label-switched-path <lsp-name> no-`

decrement-ttl, chained-compositestatement, and set routing-options forwarding-table chained-composite-next-hop ingress l3vpn PR1621943

- 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 maximum-password-length is configured and user tries to configure password whose length exceeds configured maximum-password-length error is thrown, along with error '<ok/>' tag is also emitted. (Ideally '<ok/>' tag should not be emitted in an error scenario.) The configuration does not get committed.PR1585855
- A minor memory leak is seen in the event-daemon process when multiple GRES switchovers are performed. PR1602536
- mgd might crash when an invalid value is configured for identityref type leafs/leaf-lists while configuring Openconfig or any other third-party YANG, problem happens with json and xml loads. PR1615773
- On all Junos and EVO platforms, the "snmpd" process might crash, if there is no response for the SNMP requests, and a timeout happens.PR1666548

Platform and Infrastructure

- AFEB crashing with PTP thread hog on the device. Through this fix PTP packet processing is done when PTP is enable That is, when PTP configuration is active. If the PTP configuration is not there we will ignore PTP packet processing even if FPGA is showing PTP packet is available. The issue is a rare issue. PR1068306
- If a vmhost snapshot is taken on an alternate disk and there is no further vmhost software image upgrade, the expectation is that if the current vmhost image gets corrupted, the system boots with the alternate disk so the user can recover the primary disk to restore the state. However, the host root file system and the node boots with the previous vmhost software instead of the alternate disk. PR1281554
- When VLAN is added as an action for changing the VLAN in both ingress and egress filters, the filter is not installed. PR1362609

- 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 crashes sometimes along with mspmand crash might happen if large-scale traffic flows (that is, million flows) are processed by it. PR1482400
- When there are hardware link errors occurred on all 32 links on an FPC 11. Because of these link errors, all FPCs reported destination errors towards FPC 11 and FPC 11 was taken offline with reason `offlined due to unreachable destinations`. PR1483529
- When running the command `show pfe filter hw filter-name <filter name>`, the command fails to retrieve the Packet Forwarding Engine programming details of the filter. PR1495712
- 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
- A delay of 35 seconds is added in reboot time in Junos OS Release 20.2R1 compared to Junos OS Release 19.4R2. PR1514364
- When an AMS ifd is configured for the first time or any member of the AMS bundle is removed or added, the PICs on which the members of AMS bundle are present go for a reboot. There is a timer running in the AMS kernel which is used as a delay for the PIC reboot to complete and once that timer expires AMS assumes that the PICs might have been rebooted and it moves into next step of AMS fsm. In scaled scenarios, this rebooting of the PIC is delayed due to DCD. This is because when a PIC goes down, DCD is supposed to delete the IFDs on that PIC and then the PIC reboot happens. But DCD is busy processing the scaled configuration and the IFD deletion is delayed. This delay is much greater than the timer running in AMS kernel. When the above timer expires, the FSM in AMS kernel incorrectly assumes the PIC reboot would be completed by then, but the reboot is still pending. By the time DCD deletes this IFD the AMS bundles are already UP. Because of this, there is a momentary flap of the bundles. PR1521929
- In MAC OS platforms when Juniper Secure Connect client connects successfully, the client is not getting minimized to tray icon and needs to be minimized manually.PR1525889
- Due to BRCM KBP issue route lookup might fail. Need to upgrade KBP to address this issue. PR1533513
- The Flexible PIC Concentrator (FPC) might generate a core file (or dump 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
- During Routing Engine switchover interface flap might be seen along with Scheduler slippage. PR1541772
- Unsupported configuration is being attempted by the script that then hits the maximum threshold for the given platform. PR1555159
- 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
- With IPsec PMI/fat core file enabled, "show services sessions utilization" CLI not displaying right CPU utilization. PR1557751
- The SyncE to PTP transient response is a stringent mask to be met with two way time error. The SyncE to PTP transient response mask might not be met for MPC7E-1G and MPC7E-10G line cards. PR1557999
- VE and CE mesh groups are default mesh groups created for a given routing instance. On adding VLAN or bridge-domain add, flood tokens and routes are created for both VE and CE mesh-group and flood-group. Ideally, VE mesh-group does not require a CE router where IGMP is enabled on CE interfaces. MX Series based CE boxes have unlimited capacity of tokens. So, this would not be a major issue. PR1560588
- Support switchover on routing-crash configuration statement during abnormal termination of rpd. PR1561059
- The session status becomes nonresponsive in the invalid state after the core-facing link fails in the primary PE devices. PR1562387
- Configure an interface hold time to avoid the additional interface flap. PR1562857
- On MX480 routers, traffic loss is observed with a scale of 4000 tunnels 800 VRF test. The problem is with Layer 1 node not reflecting correct bandwidth configured for tunnel services. When baseline has 1G configuration on some FPC or PIC in groups global chassis and if we override with local chassis tunnel service in 10G bandwidth scaled scenario. Out of 10 Gbps bandwidth configured only 1 Gbps is allowed per 1G speed configured in baseline configuration.PR1568414

- 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

- The following messages might be seen in the logs from MPC11E line-card: `router-re0-fpc8 aftd-trio[18040]: [Warn] AM : IPC handling - No handler found for type:27 subtype:9.` There is no functional impact, these logs can be ignored. PR1573972

- When you commit the configuration /8 pool with block size as 1, the block creation utilizes more memeory causing NAT pool memory shortage. This results in syslog `RT_NAT_POOL_MEMORY_SHORTAGE`. PR1579627

- Firewall programming fails due to scaled prefix configuration with more than 64800 entries. PR1581767

- When you configure interim logging for PBA, syslog messages are generated in regular intervals. Change in information of PBA interim syslog message, the message string change from "allocates port block" to "interim port block". PR1582394

- When the active secondary interface is deactivated, the PTP lock status is set to 'INITIALIZING' state in `show ptp lock-status` output for few seconds before BMCA chooses the next best secondary interface. There is no functional impact. PR1585529

- On all devices running Junos OS Release 19.1R3-S5-J3, when you delete Extensible Subscriber Services Manager (ESSM) the subscriber logical interface might get stuck. PR1591603

- Currently, SyncE configurations are allowed during unified ISSU but trigger a warning since SyncE state might not be maintained during unified ISSU. PTP configurations, however, need to be deactivated, else the unified ISSU will be aborted. PR1592234

- Pim VxLAN do not work on TD3 chipsets enabling VxLAN flexflow after Junos OS Release 21.3R1. PR1597276

- On MX2010 and MX2020 devices, Junos OS does not support unified ISSU for software upgrades from Junos OS 21.2 release to Junos OS 21.3 and 21.4 releases due to a flag day change. PR1597728

- Rebooting JDM from inside JDM shell changes JDM's main PID as a result systemd's knowledge of JDM PID becomes stale. Due to this reason systemd fails to stop or start JDM. PR1605060

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

- If RPD Agent sends INH deletion/additions out of order(Rarely occurs) to backup RPD, RPD might generate core files. RPD then restarts and works fine. PR1607553

- IS-IS adjacency remains down in backup Routing Engine during link flap test. PR1608591

- Dfwd generates core files when accessing ephemeral db files which is deleted through script. PR1609201
- When user tries to disable AMS ifd using configuration, the ipsec tunnels are not deleted. Deactivating the services will provide the desired result. PR1613432
- Changing aggregated AE mode (aggregated-ether-options link-protection) with subscribers logged in on that AE will cause undesirable subscriber management behavior. You will need to confirm there are no subscribers on the AE before changing the AE protection mode. PR1614117
- In some NAPT44 and NAT64 scenarios, Duplicate SESSION_CLOSE Syslog will be seen. PR1614358
- MAX AE interfaces software index was 128. Hence, a failure is seen when you configure with 218 interfaces. Therefore, we increase the max indexes to 255. PR1618337
- Memory Zone is not reflecting properly while doing Memory Tests through Vty command `test usp service-sets memory-testing start`. PR1619499
- Percentage physical-interface policer is not working on aggregated Ethernet, after switching between baseline configuration to policer configuration. PR1621998
- Minor packet drops due to bb-drops seen while creating approximately 45000 TCP session creates with NAT EIM mapping configured. PR1623276
- On all MX Series platforms with MPC10+, configuring syslog as a filter action might cause the FPC to restart. PR1627986
- For a topology with VSTP and VRRP configured and IPv6 traffic, if you change VSTP bridge priority a couple of times (to trigger toggling of root bridge), V6 traffic drop might be seen on some of the streams. PR1629345
- For 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
- On MX Series platform with enhanced subscriber management enabled, when you configure `host-prefix-only` on the underlying-interface for subscribers, it might not work in FPC. PR1631646
- The fabric statistics counters are not displayed in the output of `show snmp mib walk ascii jnxFabricMib`. PR1634372
- Ports speed is stuck and never changes for any port profile changes, if PIC bounce is done fast not letting the previous configuration complete. PR1637954

- The USB device on MX304 can be accessed from host linux instead of junos (as is usually done on most other platofrms) MX304 is similar to PTX1000 in this respect. Regular procedure to access usb in junos on most platforms: https://kb.juniper.net/InfoCenter/index?page=content=KB12880 Procedure to access usb in host linux (ptx1000, mx304): https://www.juniper.net/documentation/us/en/software/junos/junos-install-up grade/topics/topic-map/storage-media-and-routing-engines.html#id-accessing- usb-storage-on-ptx1000-routers. PR1639071

- On all Junos and Junos Evolved platforms, there may be a high Control Processing Unit (CPU) utilization for the routing processor daemon (rpd) during commit. This might only be seen in a scaled static route setup with VRF (Virtual Routing and Forwarding) and Bi-Directional Forwarding and Detection (BFD). The reason for the CPU spike is that kernel routing table (krt) might get stuck and keeps running for a long time. The high CPU might hamper the rpd functionality in rare cases, however, the system recovers by itself when you encounter this issue.PR1639252

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

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

- On MPC10E cards upon many very quick link down and up events in msec range might not always able to drain all traffic in the queue. This causes lost of traffic going through the interface. Traffic volume and class-of-service configuration does influence the exposure. See also PR1638410.PR1642584

- An improper input validation vulnerability in the Packet Forwarding Engine of Juniper Networks Junos OS Evolved allows an adjacent attacker to cause a Packet Forwarding Engine crash and thereby a Denial of Service (DoS). An FPC will crash and reboot after receiving a specific transit IPv6 packet over MPLS. Continued receipt of this packet will create a sustained Denial of Service (DoS) condition. Refer to https://kb.juniper.net/JSA69718 for more information. PR1642721

- When we use `request vmhost zeroize` command it doesn't show entry for `no-forwarding` option under possible completions. PR1642820

- With PTPoIPv6 on MPC2E 3D EQ, PTP slave stays in acquiring state.PR1642890

- Committing configuration changes during the Packet Forwarding Engine reset pause window (when PFE is disabled, yet the Packet Forwarding Engine reset proper has not started yet) has the potential of causing errors and traffic loss. In particular, configuration changes that result in re-allocating policers (which are HMC-based) might lead to traffic being entirely policed out (that is, not flowing). Once the Packet Forwarding Engine 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-devic`. PR1645075
- On Junos OS 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
- On all MX Series and PTX Series platforms, EDAC errors are triggered but alarms are not observed until the FPC gets rebooted due to the data corruption in hardware. PR1646339
- When per-interface egress and per-sid egress SR sensor stats are configured using the CLI commands below, the (pushed) MPLS label length does not get included in the output/Tx octets field that gets exported from the sensor. set protocols isis source-packet-routing sensor-based-stats per-interface-per-member-link egress set protocols isis source-packet-routing sensor-based-stats per-sid egress This is a day-1 behavior on all Trio ASIC based FPCs on the MX platform. PR1646799
- With overlapping NAT pool configured with different NAT rules under different service sets, when service outside interface is moved between different routing instances (EX: from vr1 to default, and from default to vr1), NAT routes corresponding to the service-set in default routing instance are getting deleted, resulting in reverse path traffic failure for NAT sessions. PR1646822
- On all MX Series platforms with the subscriber management scenario, when unified ISSU happens from pre Junos OS Release 18.4 to post Release 18.4, subscribers that re-logged in pre 18.4 are called preNG subscribers. For any of the preNG subscribers, if the IPv4/IPv6 family interface goes up/down, the issue is triggered. PR1646846
- Observed unexpected traffic steering during the verification of path computation client. PR1647073
- The `mobiled.core-tarball.0.tgz` core file is seen while testing `hcm_dpi_pcef_usf_3.robot`". PR1648886
- The firewall filter might be incorrectly updated in the MPC10E Packet Forwarding Engine when a change (for example, add, delete, deactivate, or activate) of firewall filter terms occurs in some scenarios, such as large-scale term changes or changes happening during MPC reboot. The incorrect firewall filter might cause the traffic to silently drop or discard and even lead to an MPC crash. It is a timing issue. PR1649499
- Extra frr_inh is seeing in `show route 174.174.174.174/32 table vpn1.inet.0 protocol bgp extensive fib-expanded-nh exact` output. PR1651103
- On MX Series devices, the low priority stream might be marked as a destination error and as a result, the low priority stream is stuck and all traffic might get dropped. PR1657378
- TOS(DSCP+ECN) bits are not getting copied from the Inner Layer 3 header to Outer VXLAN header at the Ingress VTEP. Because of this in the core, ECN marking and DSCP classification are not working. PR1658142

- DHCPACK is not received at ztp-server after zeroize of the device (client). PR1658287
- On Junos OS platforms, in the VPLS environment when having "routing-options resolution preserve-nexthop-hierarchy" configured results in the packet dropped at egress PE for multiple MPLS stack labels. PR1658406
- During startup of a cBNG container or when JSD is restarted from the CLI in a cBNG container, JSD might crash creating a core file. JSD should recover from the crash and automatically restart. JSD should function normally after recovering from the crash. PR1659175
- MPC checks periodic service time. When heavy interrupts occur during periodic service, the periodic service time might exceed 200 microseconds. If it happens, `Oinker: Function` message will occur, but it doesn't have function impact. This is applicable to Junos OS 16.1R4 to 16.1R7 releases. PR1242915
- On vMX, the blockpointer in the ktree is getting corrupted leading to core-file generation. There is no function impact such as fpc restart or system down and the issue is not seen in hardware setups. PR1525594
- When the DHCP relay mode is configured as no-snoop, we are observing the offer gets dropped due to incorrect asic programming. This issue only affects while running DHCP relay on EVPN/VXLAN environment. PR1530160
- If you use the 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
- In rare occurrence Routing Engine kernel might crash while handling TCP sessions if GRES/NSR are enabled. PR1546615
- 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 might generate core files, and you might observe Virtual Chassis split with multicast scale scenario. PR1614145
- Using static labeled switched path (LSP) configuration, the child node is not removed from the flood composite when the core interface goes down. PR1631217
- With given multi dimensional scale, if a configuration is removed and restored continuously for more than 24 times, MX Trio based FPC might crash and restart. During the reboot, there can be traffic impact if backup paths are not configured. PR1636758
- Observing traffic loss after Routing Engine switchover while changing the BGP hold-down timers. PR1650940

- 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
- MX10008 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
- Micro BFD sessions which are running in distributed mode might flap if ppm thread does not get scheduled on time. This issue is applicable to MPC9 and below trio based line cards. PR1668818
- On MX Series platforms with MIC-MACSEC-20GE, Forwarding Engine Board (FEB) might go down while activating/deactivating 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 MX Series platforms with MPC10E-10C line card, with line rate traffic, continuous traffic drop can be seen when fabric mode is changed from increased bandwidth to redundant.PR1676777
- The physical interface remaining stats flag is not set properly in chassid in today's code. It should be set to TRUE only if HCOS is configured on an interface. Else, it should not be SET. Not setting this rightly, results in statistics not being displayed OR the command output not being displayed at all. The impacted command is "run show interfaces extensive "intf-name"" and the impact is seen in GNF environment with no explicit COS configuration on the interfaces. Not using "extensive" will ensure there is no issue as well. This is specific to MPC11 with sub LC (GNF) setup. PR1678071
- There will be drop of syslog packets seen for RT_FLOW: RT_FLOW_SESSION_CREATE_USF logs until this is fixed. This will not impact the functionality.PR1678453
- On MPC10E card, the port 4 can operation in either 100G or 400G speed. In certain scenario a stale QSFP56 identifier is left in PFE. It can cause the "show interfaces diagnostics optics "interfaces"" shows all 0 even if 100G QSFP-28 is inserted and the port is up. PR1678716
- In case when you first configure the SRTE LSP without delegation and get it locally computed and then delegate, then till the time controller sends an update with valid ERO the SRTE LSP will not become externally routed. In this case the SRTE LSP will not go down if the controller sends EMPTY ERO. Only when controller updates the LSP with a valid ERO the SRTE LSP route status will change to externally routed and only then the controller can send EMPTY ERO to make it DOWN. In the other case where u configure the SRTE LSP with delegation at the time of creation itself then from the very beginning the SRTE LSP route status becomes externally control. In this case the SRTE LSP will be DOWN until the controller has sent an Update with valid ERO list. So the conclusion is that when the SRTE LSP is locally routed it will continue to reply on locally computed ERO unless Controller sends a valid ERO and takes the route control of the LSP. There are different customers wanting different behaviors. so we have kept option for both.. If someone wants to get it externally

routed from beginning we can do so by delegating it from the time of the LSP creation.. if someone wants to have a local computation till controller has a valid path we can do so by choosing the first option (configure and then delegate later)PR1686317

- VPLS mesh group add is failing because L2ALD is keep trying to add mesh group for a deleted routing instance.PR1686523
- In subscriber management environment, "failed to get template var id" error messages are generated by FPC when BFD liveness detection is negotiated by DHCP subscriber which has lawful intercept enabled.PR1689621

Routing Protocols

- Certain BGP traceoption flags (for example, "open", "update", and "keepalive") might result in (trace) logging of debugging messages that do not fall within the specified traceoption category, which results in some unwanted BGP debug messages being logged to the BGP traceoption file. PR1252294
- LDP OSPF are in synchronization state because the IGP interface is down with ldp-synchronization enabled for OSPF. user@host> show ospf interface ae100.0 extensive Interface State Area DR ID BDR ID Nbrs ae100.0 PtToPt 0.0.0.0 0.0.0.0 0.0.0.0 1 Type: P2P, Address: 10.0.60.93, Mask: 255.255.255.252, MTU: 9100, Cost: 1050 Adj count: 1 Hello: 10, Dead: 40, ReXmit: 2, Not Stub Auth type: MD5, Active key ID: 1, Start time: 1970 Jan 1 00:00:00 UTC Protection type: None Topology default (ID 0) -> Cost: 1050 LDP sync state: in sync, for: 00:04:03, reason: IGP interface down config holdtime: infinity. As per the current analysis, the IGP interface goes down because although LDP notified OSPF that LDP synchronization was achieved, OSPF is not able to take note of the LDP synchronization notification, because the OSPF neighbor is not up yet. PR1256434
- On MX Series platforms, unexpected log message will appear if the CLI command 'show version detail' or 'request support information' is executed: test@test> show version detail *** messages *** Oct 12 12:11:48.406 re0 mcsnoopd: INFO: krt mode is 1 Oct 12 12:11:48.406 re0 mcsnoopd: JUNOS SYNC private vectors set PR1315429
- On all platforms, the issue is when the first time when ESIS is coming up sometimes the ESIS route might not get installed. PR1559005
- On MX Series platforms, initial multicast register packets might get dropped, this may affect multicast services. PR1621358
- Protocols (IS-IS, LDP, BFD) flapped during graceful switchover while testing ldp oam. PR1638882

- 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
- show security keychain detail cli displays algorithm as hmac instead of AO. PR1651195
- When Junos device receives BGP inetflow route with multiple nexthops, RPD will crash and generate a core file. PR1670630
- On all Junos and Junos Evolved platforms, the rpd can 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 ECMP (Equal Cost Multi-Path) happens. There will be service impact because of the rpd crash but the system self-recovers until the next crash.PR1676154

Services Applications

- L2TP LAC functionality is not working in this release. PR1642991

User Interface and Configuration

- On all Junos with persist-groups disabled (on Junos persist-groups feature is enabled by default Junos OS Release 19.4 onwards) and on EVO platforms where persist groups can be disabled (Junos OS Release 21.4R1 onwards persist-groups cannot be disabled on EVO) this issue can be seen. This issue occurs when grafting happens during configuration expansion (when `persist-groups` is disabled) and a configuration such as a customer configuration is applied (for example, a configuration in which MTU is inherited from a groups configuration). PR1636085
- Due to the existing design for rib-groups, a rib-group configured with "import-policy" configuration statement is considered changed after NSR switchover. This makes IS-IS to refresh (delete and re-add) its routes in RIB, if such a rib-group is being used for ISIS protocol. The ISIS route refresh in-turn causes SBFD sessions to flap. This issue is only applicable with rib-group configured with "import-policy". Without "import-policy" this issue would not be seen.PR1654072

VPNs

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

- Change here is basically reverting to old enum value used for ATM VPN, and using a new value for BGP multicast address family, and although these is no visible behavior change due to this, there may be impact on 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

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

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

Application Layer Gateways (ALGs)

- On Junos OS MX Series, the flowd daemon will crash if the SIP ALG is enabled and specific SIP messages are processed (CVE-2022-22175). PR1604123
- On Junos OS, flowd core observed if the SIP ALG is enabled and a specific Session Initiation Protocol (SIP) packet is received (CVE-2022-22178). PR1615438

Class of Service (CoS)

- The fabric queues priority might not get changed after activate or deactivate CoS configuration. PR1613541

EVPN

- Baseline EVPN-VXLAN transition from IPv4 to IPv6 or vice verse does not work in certain sequence. PR1552498
- Bridge MAC-table learning entries might not be as expected for the EVPN-MPLS routing instance. PR1600310
- A few ARP, ND, and MAC entries for VLANs are missing with MAC-VRF configuration. PR1609322
- Missing MAC address entries in EVPN MAC-table despite the presence of the corresponding Type 2 route. PR1611618
- Traffic loss for profile TI2-Inter-VN-Traffic_Stream-SH-MH when testing EVPN with VXLAN. PR1628586
- The l2ald crash might be seen after performing restart routing on EVPN PE. PR1629426
- Removing configuration statement `es-label-oldstyle` does not take effect if it is the only configuration statement configured under the protocol EVPN. PR1629953

- In a scenario where multiple VXLAN type-5 tunnels with the same decap prefix (Vnid+ SrcIP + DestIP) are created within a VRF, and they are not handled on MPC10 and MPC11, it might lead to traffic drop. PR1630163
- The rpd might crash when moving an interface from VPLS to EVPN-VPWS instance. PR1632364
- The traffic loss might be seen when the link goes down for the local ESI. PR1632723
- When `no-arp-suppression` is configured in EVPN-MPLS, traffic forwarding is impacted. PR1646010

Flow-based and Packet-based Processing

- Unable to execute /usr/sbin/picinfo: Bad file descriptor during `clear services inline-monitoring statistics` command is issued. PR1624094

Forwarding and Sampling

- Delay in getting the response for `clear interfaces statistics all` command with scale configuration. PR1605544
- You can commit even if you do not appliy the firewall filter to the FPC. PR1618231
- The FPC might crash when interface participating in **next-interface** filter action flaps. PR1622585
- Packet loss might be reported after hitting the firewall filter on Junos OS platform. PR1625309

General Routing

- Error message **sensord: Error updating RRD file: /var/run/sensord.rrd** might be seen on WRL9 based line card. PR1420927
- During flooding, MAC is learnt only on normal access port but not on the aggregated Ethernet interface trunk port. PR1506403

  Junos 'et-' interface gets stuck and remains down between two particular ports. http://prsearch.juniper.net/PR1535078
- Junos 'et-' interface stuck and remains down between two particular ports. PR1535078

- On MX480, issuing the `help apropos` command in configuration mode is going to cause an mgd core. The mgd process will come up and as long as the command is not issued again, the core will not occur. PR1552191
- Egress IP MTU exception and fragmentation are not supported. PR1558327
- ARP resolution failure might occur in EVPN-VxLAN scenario. PR1561934
- The na-grpcd process might generate core files during the longevity tests. PR1565255
- When using log templates with unified policies, logs were not generated in a predictable manner. A new construct has been added that allows you to define a default log profile `set security log profile default-profile` can be used to improve this behavior when multiple log profiles are defined. PR1570105
- Interfaces might fail to come up on MX240, MX480 and MX960 platforms. PR1571274
- PKID core might occur during cert signature validation. This core is not very frequent and occurs due to memory corruption. PR1573892
- The chassisd process might crash on all Junos platforms that support Virtual Chassis or Junos fusion. PR1574669
- When Hwdre application failed on primary Routing Engine, GRES switchover will not happen. PR1575246
- MPC7E, MPC10E, MX-SPC3 and LC2103 line cards might go offline when the device is running on FIPS mode. PR1576577
- Unexpected close-timeout gets refreshed for TCP session of CGNAT on MX platforms with MS-MPC line card. PR1576675
- The subscribers over PS interface are not cleared after FPC offline. PR1580812
- The line cards might fail after hitting the I2C error on MX FPC. PR1583060
- The multicast traffic is not traversing across PS interface when it is anchored on RLT interface. PR1584041
- The `show route detail` might not show Next-hop type IPoIP Chained comp nh in the output (Display only - no operation impact). PR1584322
- The `show security idp counters` does not have `tenant` statement in the syntax. PR1586220
- A high rate of small packets could cause CPU hogging and the firmware crash in MPC5E and MPC6E line cards. PR1587551
- On MX10003 routers, PEM capacity shows incorrectly. PR1587694

- NAT EIM mapping is getting created even for out to in FTP ALG child sessions. PR1587849
- Some logical interfaces might go down under logical tunnel due to the limited number of MAC addresses in a pool. PR1591853
- The DCI InterVNI and IntraVNI traffic might get silently dropped and discarded in gateway node due to the tagged underlay interfaces. PR1596462
- Inconsistency in the platform name used in multiple places, version, snmp mibs, and so on. PR1597999
- The mspmand daemon memory leak might be observed after the HA primary goes down. PR1598356
- On MX10008 and MX10016 routers with JNP10K-RE1, unknown SMART attributes for StorFly VSFBM8CC200G SSD occurs. PR1598566
- EVPN-VXLAN, RE1 went to DB prompt when tried to load profile configurations over LRM configurations. PR1598814
- During day1 stage of device management from MIST, the cloud LED will remain in green state even if device loses connectivity with cloud. PR1598948
- The l2ald process might crash due to memory leak when all active interfaces in a VLAN are unstable. PR1599094
- Traffic might get dropped silently upon link flap after a topology change. PR1599215
- The SFP-T port might stop forwarding traffic. PR1600291
- The gNMI Telemetry might stop working after Routing Engine switchover. PR1600412
- Silent drop of traffic might be seen when multicast is configured on the device and there is a interface flap or FPC restarts. PR1600642
- Observed dcpfe core-dump while testing unified ISSU from 21.1R1.11 to 21.2R1.7. PR1600807
- Layer 2 host injected packets might not go out of IRB interface. PR1602131
- Under certain scaling scenarios with EVPN-VXLAN configurations, the l2ald process might be aborted and then recovered. PR1602244
- The Ipv6 link local BFD session might not come up if we do not have child link of an aggregated Ethernet mapped to Packet Forwarding Engine inst 0. PR1602493
- The `show system errors fru detail` command is not displaying `reset-pfe` as the cmerror configured action. PR1602726

- 21.3TOT:TCP_TLS_SYSLOG:core-usf-qnc-a-fpc3.pic1-flowd_spc3.elf.0.tgz is seeing while verifying TCP based logging functionality with GRES with AMS-Nexthop style. PR1603466
- The show commands `show services web-filter secintel-policy-status profile p1` and `show services web-filter secintel-policy-db ip-prefix-information` need to populate IP address count, term count related to blacklist, whitelist of global database and geo-ip database. PR1603517
- VRRP and BFD might flap on IRB interface on MPC10 and MPC11 line cards. PR1604150
- The adapted sample rate might get reset to the configured sample rate without changing the sampling rate information in sFlow datagrams. PR1604283
- NPC logs seen when vrf localisation is enabled. PR1604304
- Remote aggregated Ethernet member failures (via disable/laser-off) might cause the high tail drop to result in high traffic loss. PR1604823
- GRE tunnel might flap when hierarchical-scheduling is configured. PR1605189
- Traffic is not load balanced across member interfaces while configuring AMS bundle with 8 members interfaces. PR1605284
- Harmless error message might be seen when downgrading from 21.2/21.3/21.4 to 21.1 or older image on VMHost platform. PR1605915
- VM host platforms might boot exactly 30 minutes after executing `request vmhost halt` command. PR1605971
- 5G-CUPS:bbe-cups-5G-setup:wf-eabu-dev.tadcaster:re1 {version} vmcore.0.gz PR1606146
- Fabric error might be seen when MPC10E to MPC2, MPC3, MPC4, MPC5, MPC6 based FPC fabric traffic is congested. PR1606296
- Observing continuous SNMP trap for "Over Temperature!" for all the MX10016 line cards (FPC: JNP10K-LC480). PR1606555
- Random IP assignment might be done on MX Series platforms configured with PCP and DS-Lite. PR1606687
- The **WO-0: OGE0 dequeue watermark hit** might seen with Layer 2 related configuration and receiving jumbo-frame packets. PR1606967
- IPv6 link-local BFD session might not come up on MX Series platforms. PR1607077
- The speed auto-negotiated SFP-T transceiver might not be joined to the aggregated Ethernet after performing dcd restart or Routing Engine switchover on MX104. PR1607734
- Address error case in open message to comply to RFC 8664 in PCCD and PCE_Server. PR1608511

- BFD over GRE tunnel interfaces gets stuck in **init** state with GRES enabled. PR1609630
- DHCP subscribers over PWHT might be dropped upon GRES after the system reboot. PR1609818
- On MX204, interface flaps might be observed on certain ports. PR1609988
- Traffic loss might be observed if dot1X is configured with **supplicant multiple** and authenticated user from radius is in single supplicant mode. PR1610746
- MACsec session might be dropped due to one way congestion. PR1611091
- Erratic behaviour might be seen on platforms using MPC line cards after unified ISSU is performed. PR1611165
- Inter-vlan connectivity might be lost in an EVPN-VXLAN with CRB topology. PR1611488
- The routing protocol engine CPU is getting stuck at 100%. PR1612387
- The B4 client traffic will be dropped on MX-SPC3 based AFTR in DS-Lite with EIM activated CGNAT scenario. PR1612555
- Some of the fabric links might go into faulty state after swapping FPC LC1201 with LC1202. PR1612624
- The PFE/SIB/SCBE/FPCs might reboot due to the unexpected fabric errors shown up on MX240, MX480 and MX960 platforms. PR1612957
- Traffic loss might be observed due to the shaping rate be adjusted incorrectly in a subscriber environment on MX Series platforms. PR1613126
- Enhanced-hash-key might not take effect when configured with forwarding-options. PR1613142
- For PS Service logical interface configured in MPC2-NG/MPC3-NG interface statistics do not show correct (shaped) value when shaping is applied. PR1613395
- Enabling security-metadata-streaming DNS policy might cause a dataplane memory leak. PR1613489
- Unknown SMART attributes for StorFly VSFBM6CC100G-JUN1 SSD might be seen.PR1614068
- FPCs might be stuck in **onlining** state after the software release upgrade. PR1614489
- Any irrelevant configuration changes might trigger NAT routes flap on MX Series routers in USF mode. PR1614688
- MPC6E 3D did not comes back up after MIC offline online test. PR1614816
- Modifying the input service-filter via COA might fail in subscriber management environment. PR1614903

- Export memory and temperature metrics for all existing components when it subscribes to telemetry sensor. PR1615045
- The l2ald process might crash in EVPN scenario. PR1615269
- Traffic drop might occur when huge number of EIM mappings are created or deleted continuously. PR1615332
- The CDA-BT process generates a core file when you turn the FPC offline. PR1615343
- Request to provide an API which gives list of potential policy given a session ID. PR1615355
- The counter might show double value when chassis enhanced-policer is configured. PR1615373
- The rasdaemon processes memory leak -- triggered by hardware memory errors on VMHost platforms. PR1615488
- On MX10008, TPI88812 on change /components/component[name='FPC7'/state/type after event does not have the correct jvalue. PR1616049
- Slow memory leak (32 bytes each time) of rpd might be seen. PR1616065
- No filter found error might be seen while deactivating filter attached to interface after MPC reboot. PR1616067
- VPLS BUM (Broadcast, unknown unicast, and multicast) traffic does not get forwarded to remote PEs over the MPLS core files. PR1616236
- The `show subscribers accounting-statistics` and `show services l2tp session interface asi0.xx statistics` might not work on LNS with asi- interfaces. PR1616454
- Observed traffic error on 100G FPC for DPT deep loopback test on ports et-0/0/6 and et-0/0/7. PR1616525
- The dual Routing Engine system might not be GRES ready after backup Routing Engine reboot in a subscriber management environment. PR1616611
- The Strict-Priority-Scheduler (SPS) might not work accurately across port queues. PR1616772
- The aftermand process generates core files at `RtIfaHandler::notifyCommand,EalIfaHandler::registryClientCommand ,EalIfaHandler::OnAdd (this=0x7f2ffe40e9a0 < EalIfaHandler::instance()::handler>, ifah=...) at ../../src/EalIfaHandler.cpp:222.` PR1616909
- Layer 2 cpd memory leak might lead to l2cpd process crash. PR1617151
- In MX Series Virtual Chassis spcd running on SPC3 crashes. PR1617280
- MPC8E in 1.6T bandwidth mode might not work correctly. PR1617469

- The l2cpd core file is seen with FIP snooping configuration on any interface. PR1617632
- Unexpected Routing Engine switchover might be observed. PR1617720
- Traceroute packets might get dropped in SFW service-set when other service-sets with asymmetric traffic processing are also enabled on the same MS-MIC/MS-MPC. PR1617830
- Match on v6-prefix for prefix lengths less than or equal to 64 bits does not work.PR1618211
- GMC clock class is seen transmitted for an additional 16 seconds after the PTP source switches from one line card to another. PR1618344
- Traffic loss might be observed if the router is configured with ECMP over IRB and the traffic go through the MPC10E and MPC11E line cards. PR1618354
- The traffic loss might be seen after cleaning the large-scaled NAT sessions in MS-SPC3 based next generation services inter-chassis stateful high availability scenario. PR1618360
- The clksyncd might crash and PTP/SyncE might not work. PR1618929
- Support whole (atomic) updates at CNHG level. PR1619011
- InputIntf is reported incorrectly for MPLS-IPv4 and MPLS-IPv6 ingress sampling in the case of Layer 3 VPN. PR1619052
- The hardware process might crash when an FPC is pulled out or some power failure or fault occurs for the FPC. PR1619102
- ACI VLAN session setup might get failed. PR1619122
- The nsd might crash while validating NAT translation on MX Series platforms with SPC3. PR1619216
- Traffic might be dropped when the RSVP is configured with the `mtu-signaling`. PR1619510
- Additional commit warnings and errors were introduced to improve security log profile usability. PR1619694
- The /interfaces/interface/subinterfaces/subinterface/state/counters not exported during initial synchronization for on-change. PR1620160
- The bbe subscriber access services might be stuck while rebooting the one redundancy line-card of RLT interface. PR1620227
- On MX480 routers, output packet drop is observed while verifying services PCEF subscribers. PR1620421
- OAM CFM session does not come Up if ERPS configured and CFM control traffic uses the same VLAN as ERPS control traffic. PR1620536

- High wired memory utilization might be observed if GRES is enabled. PR1620599
- The EVPN type 5 routes might not be installed. PR1620808
- Static subscribers session might get stuck in initializing state after ungraceful routing engine switchover. PR1620827
- Incorrect sensor modeling or mapping when using /junos/system/linecard/interface/ native telemetry streaming. PR1621037
- SNMP get for MIB value for jnxRedundancyConfig does not work as expected. PR1621101
- SNMP get for MID ID for jnxRedundancySwitchoverReason does not work as expected. PR1621103
- IFLSet COS hierarchy might be missed in the backup leg after rebooting FPC. PR1621164
- Flapping of all ports in the same Packet Forwarding Engine might cause Packet Forwarding Engine to be disabled. PR1621286
- NSSU option is not available from Junos OS Release 21.2R1. This option is missing from the time UI component publish has been separated out. PR1621611
- PIC gets stuck in offlining state when offline command is issued right after transceiver plugin. PR1621694
- Traffic loss can be seen on the new primary Routing Engine post GRES. PR1621696
- Telemetry/jvision, system_id formate of AFT-MPC(MPC10E) is not aligned with non-AFT MPCs. PR1622073
- Chassis alarm **VMHost RE 0 Secure BIOS Version Mismatch**, firmware upgrade did not solve the issue. PR1622087
- When the PHY-Sync state of a line card moves to False, it internally disables the PHY-timestamping of PTP packets. PR1622108
- AFT firewall telemetry (ZT), suppressed **state**'container and modified field numbers in the render proto. This is to sync with uKernel proto. PR1622313
- Invocation of `netconf get` command will fail if there are no Layer 2 interfaces in the system. PR1622496
- Constant increase of PCS errors might be seen on channelized port. PR1622741
- The port speed shows as 100G even though chassis configuration is set for 40G. This is just a cosmetic display issue. PR1623237
- The ethtraceroute core file is generated. PR1623443

- Packet loss might be seen when enabling output sampling on the source interface of tunnel. PR1624057
- The `show pfe route ip` is getting timed out when route table size is large. PR1624629
- The aggregated Ethernet member link might not be correctly populated on the Packet Forwarding Engine after FPC restart on MX Series platforms. PR1624772
- Traffic drop is seen with egress features enabled on interface hosted on MPC10 and MPC11 line cards. PR1624804
- The process hwdfpc might crash. PR1624841
- On single IPSec tunnel with PMI when sending internet traffic packet processing might get delayed due to session management issue. PR1624974
- On Junos OS, specific packets over VXLAN cause FPC reset (CVE-2022-22171). PR1625292
- JNP10008-SF3, SIB-JNP10004 and JNP10016-SF3 memory errors handling improvement. PR1625305
- The flowd process lost heartbeat for 45 consecutive seconds without alarm raised. PR1625579
- The bbe-statsd crash might be seen in the LTS subscriber scenario. PR1625648
- The gNMI set RPC might fail when multiple values within a single gNMI SetRequest are used for the Junos telemetry interface. PR1625806
- Packet loops in the PIC even after stopping the traffic on MX Series platform with SPC3 line card. PR1625888
- The bbe-smgd might crash on backup Routing Engine after unified ISSU or GRES. PR1626091
- Traffic drop might be seen in node slicing scenario. PR1626115
- Some Interfaces might not come online after line card reboot. PR1626130
- Implement `show task scheduler-slip-history` to display number of scheduler slips and last 64 slip details. PR1626148
- After configuring 4000 bridge domains, messages log file floods with kernal messages. PR1626381
- The chassisd might crash on MX104. PR1626486
- The autoconf might not work if the DHCPv4 discover message has option 80 (rapid commit) ahead of option 82. PR1626558
- Broadcast traffic might not be forwarded to LT interface in VPLS routing instance after LT interface is deleted and then added back. PR1626714

- VPLS MAC age time-out might not be applied on some MAC addresses. PR1627416
- S-PTX10K-144C license SKUs do not load, 400G SKUs do load. PR1627459
- IP not-ECN-capable traffic is not RED-dropped in an ECN-enabled congested queue. PR1627496
- DHCP clients might not go to BOUND state when the aggregated Ethernet bundle is enabled between DHCP server and snooping device. PR1627611
- The shell upgrade script fails for releases earlier than Junos Os Release 21.4. PR1627618
- Tunnel interface statistics displays incorrect values when JFlow sampling is enabled. PR1627713
- Layer 3 traffic failure might be observed with scaled MC-LAG configuration. PR1627846
- Invalid IP length packets encapsulated within MPLS might trigger PPE traps. PR1628091
- Memory leak might occur on PFED process when the flat-file-profile is configured with configuration `use-fc-ingress-stats`. PR1628139
- The EAPol packets over l2circuit might get dropped at the tunnel start. PR1628196
- EVPN flood filter might not work for MPC10 and MPC11 line cards. PR1628270
- The traffic might be dropped on xSTP ports that were earlier in FWD/DESG state after unified ISSU. PR1628358
- Tunnel-service bandwidth should not be changed when there are active subscribers. PR1628628
- The `show system subscriber-management route summary` does not report route summary as expected. PR1629450
- The l2ald might be stuck in **issu state** when unified ISSU is aborted. PR1629678
- MPC10E crashes in enhanced-cfm-mode when it receives CFM packets from ONT. PR1629685
- The egress traffic on non-targeted iflset of subscribers might not be forwarded correctly over targeted aggregated Ethernet interface. PR1629910
- Multiple link flaps and traffic might be lost on the links. PR1630006
- The kmd daemon might crash with core files every few minutes on MX Series platforms. PR1630070
- LACP timeout might be observed during high CPU utilization. PR1630201
- Indirect next-hop (INH) Version ID higher than 255 might cause INH NH FRR Session moved down state and dropping transit traffic. PR1630215
- With SCBE3+SPC3, fabric drops are seen around 10M PPS/60G TCP traffic with ~750byte packet size with IPv6 SFW on a single PIC. PR1630223

- LLDP packets might be sent with incorrect source MAC for RETH or LAG child members. PR1630886
- PCIe bus error associate to PTP FPGA device during chassis reboot. PR1631300
- The kmd might crash since the pkid requested memory leak happens on M/MX Series platforms. PR1631443
- The ipv6 host route prefix match disappear from **forwarding-table** after a ping test, ping continues to work, forwarding table entry is not shown. No impact in traffic. PR1631607
- Adverse effect on subscriber management observed after deactivating chassis pseudowire-service with active subscribers. PR1631787
- DHCP ALQ Syslog error bbesmgd[26939]: LIBSDB_RSMON_PS_TABLE_PTR_FAILURE: sdb_get_ps_interface_table_record:2076 failed to get the ps_table_header ptr. PR1631858
- The rpd process generates core file with the warm-standby configurations due to reference counting issues. PR1631871
- The transit CCM sessions comes up but transit loopback(LB) ping or LinkTrace(LT) PDUs does not go through. PR1632255
- High-speed key is not reported for MPC11 in AF interface sensor. PR1632289
- When deleting the VNI and there is another vlan-id-list with a different VNI, it might cause traffic loss. PR1632444
- Firewall sensors information of MPC10E, MPC11E, MPC12E, and VMX ZT MPC line-card are not getting streamed to telemetry. PR1632477
- Summit MX chassis communication does not work after Virtual Chassis member-id set/delete. PR1632645
- The bbe-smgd process might crash after removing and adding a child link from aggregated Ethernet interface. PR1633392
- Slow chassis memory leak might occur when chassisd related configuration change is committed. PR1634164
- PTP clock class might incorrectly be downgraded to 248 when PTP is enabled on Linecard/MIC which does not support phy-timestamping. PR1634569
- When all configured anchor Packet Forwarding Engines are offline on the SAEGW-u, there might be a peer association mis-match between the SAEGW-u and SAEGW-c. PR1634966
- CFM CCM PDU is not forwarded transparently on core MX if the IFD is configured under protocols OAM. PR1635293

- BCM SDK publish build failed with error message in description is fixed. PR1635318
- Data might not be exchanged through EVPN-VxLAN domain. PR1635347
- Incorrect interface statistics might be reported on MX204. PR1636654
- Delay might be observed for the interfaces to come up after reboot or transceiver replacement. PR1638045
- BNG CUPS: ERA & OIU - Core in oiuModShMemEntry during OIU modify when restarting smg-service while bouncing subscribers. PR1638217
- Locally switched traffic might be dropped with ESI configured. PR1638386
- Packet Forwarding Engine might get stuck after 100G or 400G interface flaps. PR1638410
-
- JUNOS: JDI_FT_REGRESSION:SUBSCRIBER_SERVICES:MX480: Time difference is not as expected when DUT exports interface-queue-stats to ipfix-collector tool after changing reporting-interval. PR1639378
- The `show network-agent statistics gnmi detail` CLI command is reporting packet drops for some gnmi target-defined mode sensors. PR1641483
- The KRT queue might get stuck with the error- **ENOMEM -- Cannot allocate memory**. PR1642172
- CFM traceoptions writes on every other line. PR1642948
- On MX480 platforms, PFED CPU increased post unified ISSU and remains around 65-75% for 32000 L2VPN sBNG services. PR1643077
- PCEP SRv6 code points changed as per IANA. PR1644332
- Multicast traffic drop might be observed after performing Routing Engine switchover or rpd restart. PR1593810
- The rpd agent might get crash during NSR switchover. PR1612725
- DHCP relay no-snoop might not work with DHCP local server in the same routing-instance. PR1613738
- DHCP subscribers might not be synchronized to backup BNG when DHCP ALQ is configured without topology-discover. PR1620544
- PDT: restart ppmd triggers **EAL NH NULL for child NH** and **EalNhHandler Modify: Nh with index: 383675 does not exist**. PR1628049

High Availability (HA) and Resiliency

- Memory leaking might occur on backup Routing Engine when ksyncd is in inconsistent state and had encountered an initialization error. PR1601960
- When MTU is configured on an interface a rare ifstate timing issue could occur at a later point, resulting in ksyncd process crash on backup Routing Engine. PR1606779

Infrastructure

- A false error related to insufficient space might appear while installing a Junos OS image that is corrupted. PR1570148
- Net installation (PXE) is not working. PR1577562
- Egress TCP RST might not have correctly populated DSCP field. PR1612208

Interfaces and Chassis

- Traffic loss is seen after restarting the SIB. PR1560111
- Commit check failure might happen if similar interfaces are configured under VRRP group. PR1617020
- Delay in application of CLI configuration by DCD when aggregated Ethernet interface members are configured through JET API. PR1621482
- CFM enhanced SLA iterators monitoring might stop after restarting chassis-control daemon in vMX. PR1622081
- The subscribers might be deleted when `host-prefix-only` configuration statement is configured on the underlying-interface in GRES scenario. PR1630229
- The syslog messages and the dcd crash might be seen in Junos OS. PR1633339
- CFM sessions are not up after evo-pfemand restart or crash. PR1634721
- VRRP route tracking for routes in VRF might not work if **chained-composite-next-hop ingress l3vpn** is used. PR1635351
- Some daemons might get stuck when snmpd is at 100% CPU utilization. PR1636093

- FPC might crash if the continuity-check interval under CFM is modified. PR1636226
- The `show vrrp extensive` doesn't show the next IFL **Interface VRRP PDU statistics**. PR1637735
- On Junos 20.3 and later release, the tracking routes of VRRP might become unknown after upgradation. PR1639242
- The aggregated Ethernet interface with 400GE gets flapped on adding or removing a 400GE member link. PR1641585
- The vrrpd core file might be observed after interface state change. PR1646480

Junos XML API and Scripting

- File download using `request system download` might fail. PR1604622

Layer 2 Ethernet Services

- Making configuration changes with apply-group add/delete associated with DHCP might result in client connection failure. PR1550628
- DHCP leasequery is failing to restore binding when the reply is received over IRB interface. PR1611111
- BFD hold-down timer does not work properly when LAG is configured. PR1616764
- Enabling DHCP on Junos OS platform might cause the router's file system storage to get filled up with log files. PR1617695
- The Junos OS, the jdhcpd crashes upon receiving a specific DHCP packet (CVE-2022-22179). PR1618977
- Circuit-id handled incorrectly with backup node for ALQ with topology discover configured. PR1620461
- The jdhcpd process crashes in DHCP and DHCPv6 environment. PR1625011
- The process jdhcpd might get stuck at 100% post clients login or logout. PR1625112
- Option 82 might not be attached on DHCP request packets. PR1625604
- The rpd scheduler might continuously slip after GRES when there are 7000 DHCP clients in a subscriber management environment. PR1625617

- IPv6 IA_NA or IA_PD routes might get deleted from the DHCPv6 client. PR1629171
- Non-DHCPv4 BOOTP protocol packets might not be processed if enhanced subscriber management is enabled. PR1629172
- The aggregated Ethernet interface remains UP instead of down on deleting loopback and aggregated Ethernet interface IP on neighbor while verifying BFD sessions on router. PR1640240

MPLS

- The node SID might be seen in an unresolved state. PR1564169
- IPv4 prefixes might be associated into both IPv4 and IPv6 LDP database after Routing Engine switchover. PR1611338
- Configuring protocols MPLS lsp-external-controller also throws commit error if in-place-lsp-bandwidth-update is configured under any LSP. PR1612269
- The rpd process might generate core files for a few value configurations of signaling bandwidth on container LSP. PR1614248
- The RPD crash might happen due to refcount leak in routing table metrics. PR1615001
- Standby secondary LSP might be stuck on the same path as primary LSP upon reoptimization. PR1615326
- Protected LSP goes down with strict hops and link protection configured. PR1616841
- LDP protections paths might not be established when `auto-targeted-session` configuration is deactivated and activated. PR1620262
- Underlay Colored SRTE LSP is being wrongly shown as RSVP LSP in express-segments detail. PR1623643
- Unexpected traffic loss on LSP headend might be observed when downstream IGP metric changes. PR1625438
- VCCV BFD session keeps flapping between MX and peer device if ultimate-hop popping is enabled. PR1634632
- [mpls] [LDP-Tunneling] : mx2020 :: rpd core@ldp_destroy_lib is observed in mx2020 after post Gress. PR1635863
- The rpd memory leak might be observed in a subscriber management environment with RSVP. PR1637645

- LSP over broadcast segment stays down when RSVP setup protection is enabled. PR1638145
- Dynamic bypass LSP might flap at every re-optimization interval. PR1639292

Network Management and Monitoring

- Ephemeral instance configuration is not removed even after deleting the ephemeral instance from set system configuration-database. PR1553469
- Rtsdbd core file might be seen when IPsec configuration is activated and deactivated. PR1610594

Platform and Infrastructure

- The ppmd process might crash after an upgrade. PR1335526
- The subscribers might not come online after interface flaps on MX Series platforms. PR1591905
- Traffic through one SPU might stop with potential packet drop issue with alarm as FPC Major Errors raised due to the PIC_CMERROR_TALUS_PKT_LOSS error. PR1600216
- On MX Series platforms vmcore on both the Routing Engines might be reported due to mbuf corruption. PR1602442
- The FPC might crash if `flow-table-size` is configured on MX Series platforms. PR1606731
- CFM neighbor adjacency will be failed on the aggregated Ethernet member interface of MPC10 and MPC11 line cards. PR1611816
- Filter related service will not work when the filter is deleted/re-added frequently for aggregated Ethernet interface. PR1614480
- Degraded traffic processing performance might be observed in case of processing very high PPS rate traffic. PR1619111
- CoS custom classifier might not work on logical interface. PR1619630
- Accounting and auditd process might not work on secondary node. PR1620564
- Trio-based line cards might crash when Packet Forwarding Engine memory is hot-banking. PR1626041
- Configuration commit might fail while configuring the configuration statement `authentication-key-chains` under groups. PR1626400

- Unrealistic service accounting statistics might be reported due to firewall counter corruption. PR1627908
- Error message **gencfg_cfg_msg_gen_handler drop** might be seen after running commit. command PR1629647
- The packet drop might be seen on FPC on Trio based platforms. PR1631313
- When route preferred-metric is different for different RPM policies, the same metric is not reflected in routing records. PR1634129
- Continuous Fabric Link Sanity Check interrupts in intervals of weeks might cause at some point fabric input block traffic blackholing. PR1636060
- During unified ISSU certain EA based line cards such as LC2103 might crash, causing them to cold boot. PR1637618
- AUTO-CORE-PR : JDI-RCT vRCT : vmxt_lnx core found @ topo_get_link jnh_features_get_jnh jnh_stream_attach. PR1638166
- SCB reset with Error : zfchip_scan line = 844 name = failed due to PIO errors. PR1648850

Routing Policy and Firewall Filters

- Evaluation of inet-vpn route-filters might not work with /32 exact statements for BGP flowspec routes. PR1618726
- Services might not work after committing firewall filter counter configuration with similar name of two terms. PR1625168
- Existing routing policies might change when global default route-filter walkup is changed. PR1646603

Routing Protocols

- When igmp-snooping is removed from the device, the device might encounter inconsistent MCSNOOPD. PR1569436
- New version of OpenSSL (1.1.1) is not supported for NTF-agent of Junos Telemetry Interface. PR1597714

- After first parallel unified ISSU aborts, subsequent unified ISSU attempts on failed node aborts with **Aborting Daemon Prepare**. PR1598786
- Observing commit error while configuring **routing-options rib inet6.0 static** on all Junos OS platforms. PR1599273
- The rpd core might be observed due to memory corruption. PR1599751
- Kernel crash might be observed on platforms that have BGP configured with family Layer 2 VPN. PR1600599
- The BGP replication might be stuck in **InProgress** state. PR1606420
- The commit should fail when microloop-avoidance post-convergence-path is configured without source-packet-routing. PR1608992
- The rpd might crash after a commit if there are more than one address in the same address ranges configured under **bgp allow**. PR1611070
- The interface might receive multicast traffic from a multicast group which it is not interested in. PR1612279
- Undesired protection path might get selected for some destination prefixes. PR1614683
- The memory leak on rpd might be observed after running `show route` CLI command. PR1615162
- BFD sessions flapping might occur after performing GRES. PR1615503
- The incorrect BGP path might get selected even when a better/preferred route is available. PR1616595
- Traffic drop will be seen when VPN labels are incorrectly allocated due to change in nexthop. PR1617691
- Verification of BGP peer count fails after deleting BGP neighbors. PR1618103
- On Junos OS, OpenSSL Security Advisory. PR1618985
- The rpd might crash and restart when NSR is enabled. PR1620463
- The aggregated Ethernet interface might send/receive traffic through child link though BFD status is **client in hold-down state**. PR1624085
- Time delay to export prefixes to BGP neighbors might occur post applying peer-specific BGP export policies. PR1626367
- The rpd core file might be seen while processing the BGP updates. PR1626717
- Multipath route with List-NH which has Indirect-NH as members fails into BGP-LU. PR1626756

- eBGP Multipath route stuck in KRT queue. PR1626966
- For prefixes leaked from BGP to IS-IS, the P flag will be set for Prefix-SID advertised from IS-IS. PR1627322
- The contributing routes might not be advertised properly if **from aggregate-contributor** is used. PR1629437
- The multicast forwarding cache might not get updated after deactivating the scope-policy configuration. PR1630144
- The BGP ECMP might not work and multipath route won't be created. PR1630220
- The rpd might crash when BGP labeled-unicast family routes are present and BGP multipath is turned on. PR1630987
- The rpd might crash after clearing IS-IS database. PR1631738
- The rpd might get into an infinite loop while clearing IS-IS database. PR1632122
- The BGP session might flap after rpd crash with **switchover-on-routing-crash** and NSR enabled in a highly scaled environment. PR1632132
- IS-IS database might not be synchronized in some multiple areas scenario. PR1633858
- OSPF adjacency might take longer time to converge when the neighbour restarts non-gracefully. PR1634162
- Multipath route gets formed for a VPN prefix due to incorrect BGP route selection logic. PR1635009
- The BGP peer might stay down in shards after doing a rollback. PR1643246

Services Applications

- L2TP tunnels might go down and not be able to re-establish after restarting the bbe-smgd process. PR1629104
- Tunneled subscribers might be stuck in terminating state in L2TP subscriber scenario. PR1630150
- DTCP radius-flow-tap fails to program Packet Forwarding Engine when trigger X-NAS-Port-Id exceeds 48 character length. PR1647179

Subscriber Access Management

- Install discard routes is not supported on APM managed BNGs running Junos OS Release 21.3R1. PR1604967
- Class attribute is corrupted for radius accounting messages since unified ISSU to 19.1 or higher release on MX Series platforms. PR1624066
- Radius CoA (Change of Authorization) NAK might not be sent with the configured Source Address in a virtual-router environment. PR1625858
- ESSM sessions might get terminated in radius as class attribute has got corrupted after performing unified ISSU. PR1626718
- When connectivity between BNG and APM is lost, the BNG does not regenerate pool drained alarms to APM. PR1627974
- Event-timestamp in radius Acct-Stop might show future time. PR1643316

User Interface and Configuration

- Mgd might generate core files while running any RPC after running copy-config rpc with unreachable host in the URL on the same NETCONF session. PR1590625
- Interface configuration might get stuck and might not update after several ephemeral commits. PR1598123
- Unable to delete Linux core files by using `file delete /var/core/*/vmcore*` CLI command. PR1624562
- Junos OS upgrade might fail with error **configuration database size limit exceeded**. PR1626721
- The process mgd might crash with errors if `system scripts synchronize` is configured. PR1628046

VPNs

- The multicast route is not getting installed after exporting of secondary routes from one instance to another. PR1562056
- The rpd process might crash during unified ISSU if the `auto-sensing` configuration statement is enabled for l2circuit. PR1626219

- Type 7 routes might be lost in MVPN+PIM SSM scenario. PR1640487

Migration, Upgrade, and Downgrade Instructions

IN THIS SECTION

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

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

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

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

Basic Procedure for Upgrading to Release 22.1R3

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

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

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

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

Procedure to Upgrade to FreeBSD 12.x-Based Junos OS

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

To download and install FreeBSD 12.x-based Junos OS:

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

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

2. Select the name of the Junos OS platform for the software that you want to download.
3. Select the release number (the number of the software version that you want to download) from the Release drop-down list to the right of the Download Software page.
4. Select the Software tab.
5. In the Install Package section of the Software tab, select the software package for the release.
6. Log in to the Juniper Networks authentication system using the username (generally your e-mail address) and password supplied by a Juniper Networks representative.
7. Review and accept the End User License Agreement.

8. Download the software to a local host.
9. Copy the software to the routing platform or to your internal software distribution site.
10. Install the new jinstall package on the routing platform.

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

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

- For 32-bit Routing Engine version:

```
user@host> request system software add no-validate reboot source/junos-install-mx-x86-32-22.1R3.9-signed.tgz
```

- For 64-bit Routing Engine version:

```
user@host> request system software add no-validate reboot source/junos-install-mx-x86-64-22.1R3.9-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-x86-32-22.1R3.x-limited.tgz
```

- For 64-bit Routing Engine version:

```
user@host> request system software add no-validate reboot source/junos-install-mx-x86-64-22.1R3.9-limited.tgz
```

Replace source with one of the following values:

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

- **ftp://** ***hostname/ pathname***
- **http://** ***hostname/ pathname***
- **scp://** ***hostname/ pathname***

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

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

Rebooting occurs only if the upgrade is successful.

NOTE:

- You need to install the Junos OS software package and host software package on the routers with the RE-MX-X6 and RE-MX-X8 Routing Engines. For upgrading the host OS on these routers with VM Host support, use the junos-vmhost-install-x.tgz image and specify the name of the regular package in the `request vmhost software add` command. For more information, see the VM Host Installation topic in the Installation and Upgrade Guide.
- Starting in Junos OS Release 22.1R3, in order to install a VM host image based on Wind River Linux 9, you must upgrade the i40e NVM firmware on the following MX Series routers:
  - MX240, MX480, MX960, MX2010, MX2020, MX2008, MX10016, and MX10008

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

NOTE: After you install a Junos OS Release 22.1R3 jinstall package, you cannot return to the previously installed Junos OS (FreeBSD 6.x) software by issuing the `request system software rollback` command. Instead, you must issue the `request system software add no-validate` command and specify the jinstall package that corresponds to the previously installed software.

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

Upgrade and Downgrade Support Policy for Junos OS Releases

Support for upgrades and downgrades that span more than three Junos OS releases at a time is not provided, except for releases that are designated as Extended End-of-Life (EEOL) releases. EEOL releases provide direct upgrade and downgrade paths—you can upgrade directly from one EEOL release to the next EEOL release even though EEOL releases generally occur in increments beyond three releases.

You can upgrade or downgrade to the EEOL release that occurs directly before or after the currently installed EEOL release, or to two EEOL releases before or after. For example, Junos OS Releases 19.3, 19.4, and 20.1 are EEOL releases. You can upgrade from Junos OS Release 19.3 to Release 19.4 or from Junos OS Release 19.3 to Release 20.1.

You cannot upgrade directly from a non-EEOL release to a release that is more than three releases ahead or behind. To upgrade or downgrade from a non-EEOL release to a release more than three releases before or after, first upgrade to the next EEOL release and then upgrade or downgrade from that EEOL release to your target release.

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

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 22.1R3

To downgrade from Release 22.1R3 to another supported release, follow the procedure for upgrading, but replace the 22.1R1 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 22.1R3 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

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

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

High Availability

- On an NFX350 chassis cluster, when FPC0 (when node0 is primary) or FPC7 (when node1 is primary) is restarted by either using the `request chassis fpc slot slot restart node local` command or due to

dcpfe core files on the primary, it restarts FPC1 or FPC8. This might break the preexisting TCP sessions and fail to restart the TCP sessions. The TCP sessions might require a manual restart. PR1557607

Interfaces

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

  Workaround—Deactivate and then activate the aggregated Ethernet interface. PR1583054

Resolved Issues

There are no resolved 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.

Migration, Upgrade, and Downgrade Instructions

IN THIS SECTION

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

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

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

Upgrade and Downgrade Support Policy for Junos OS Releases

Support for upgrades and downgrades that span more than three Junos OS releases at a time is not provided, except for releases that are designated as Extended End-of-Life (EEOL) releases. EEOL releases provide direct upgrade and downgrade paths—you can upgrade directly from one EEOL release to the next EEOL release even though EEOL releases generally occur in increments beyond three releases.

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

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

Basic Procedure for Upgrading to Release 22.1

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

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

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

To download and install Junos OS Release 22.1R3:

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 22.1R3 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 PTX Series routers.

What's Changed

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

Known Limitations

IN THIS SECTION

Learn about known limitations in this release for PTX 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

- When a number of routes resolve over an ECMP path, the inline BFD sessions might flap during "clear isis adjacency" command or RPD restart trigger. PR1612802

Infrastructure

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

Open Issues

IN THIS SECTION

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

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

General Routing

- On the PTX platform with FPC-PTX-P1-A or FPC2-PTX-P1A, you might encounter a single event upset (SEU) event that might cause a linked-list corruption of the TQCHIP. The following syslog message gets reported: Jan 9 08:16:47.295 router fpc0 TQCHIP1: Fatal error pqt_min_free_cnt is zero Jan 9 08:16:47.295 router fpc0 CMSNG: Fatal ASIC error, chip TQ Jan 9 08:16:47.295 router

fpc0 TQ Chip::FATAL ERROR!! from PQT free count is zero Jan 9 08:16:47.380 router alarmd[2427]: Alarm set: FPC color=RED, class=CHASSIS, reason=FPC 0 Fatal Errors - TQ Chip Error code: 0x50002 Jan 9 08:16:47.380 router craftd[2051]: Fatal alarm set, FPC 0 Fatal Errors - TQ Chip Error code: 0x50002 The Junos OS Chassis Management error handling detects such a condition, raises an alarm, and disables the affected Packet Forwarding Engine entity. To recover this Packet Forwarding Engine entity, restart the FPC. Contact your Juniper support representative if the issue persists even after the FPC restarts. PR1254415

- Flapping might be observed on channelized ports of PTX Series routers during ZTP when one of the ports is disabled on the supporting device. PR1534614
- Unsupported configuration is being attempted by the script that then hits the maximum threshold for the given platform PTX5000. PR1555159
- On PTX platforms, when Inline Jflow is configured and high sampling rate (more than 4000 per second) is set, high CPU utilization might be observed and this might result in relevant impacts on traffic analysis and billing. PR1569229
- 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
- While loading baseline configurations in Gladiator box, continuous FPC core seen at pci_user_pio_read_func and posix_interface_abort along with scheduler hog messages. PR1644576
- On all PTX platforms, EDAC errors are triggered but alarms are not observed until the FPC gets rebooted due to the data corruption in hardware. PR1646339
- V6 default route will not get added after successful dhcpv6 client binding on PTX1000 router during ztp. PR1649576
- A limitless resource allocation vulnerability in FPC resources of Juniper Networks Junos OS Evolved on PTX Series allows an unprivileged attacker to cause Denial of Service (DoS). Please refer to https://kb.juniper.net/JSA69916 for more information. PR1657659
- ZTP: DHCPACK not received at ztp-server after zeroize of the device (client)PR1658287
- When an FPC (Flexible PIC Concentrator) on PTX5000 platforms is shut down by issuing a request command (request chassis offline slot <slot-number>) or by FPC power off configuration (set chassis fpc x power off), it gets stuck in the 'Announce Offline' state since the associated timer (fru_graceful_offline_timer) doesn't increment and expire as it is supposed to. PR1683562
- Sflow ingress or egress sampling does not work when ECMP nexthops are involved.PR1685407

Interfaces and Chassis

- The memory usage of the "rpd" process on the backup routing engine may increase indefinitely due to leak in krt_as_path_t. PR1614763

MPLS

- On PTX3000 routers, if RPD thrashes during a GRES switchover, there might be traffic loss on MPLS LSPs. PR1590681
- After an interface is disabled, `show mpls lsp bypass statistics` shows BackupActive Timeout failure bypass. PR1597733

Platform and Infrastructure

- In rare occurrence Routing Engine kernel might crash while handling TCP sessions if GRES/NSR are enabled. PR1546615

Routing Protocols

- Any platforms with Micro BFD configured on member links of the LAG or aggregated Ethernet 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 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

- IS-IS adjacency is not coming up through TCC l2circuit. PR1590387
- On Junos OS PTX platforms traffic blackholing can occur after interface flaps. PR1645488
- IRP memory parity issue might result in traffic loss on PTX Junos OS platforms. PR1650217
- PCS Errored blocks count will increment after Junos OS software upgrade to 20.2R1 or above releases. PR1651526
- IS-IS adjacency is not coming up through the Layer 2 domain. PR1663134
- PCS errored blocks count increments on PTX3000 and PTX5000 after Junos OS software upgrade. PR1669267
- Reporting-interval in `show jvision sensor info` is stuck at 65000 when configured reporting rate is changed from 65000 to 68000. PR1673476
- Issue with eth-lldp-stop.sh after Junos OS upgrade performed in PTX5000(i40e-NVM). PR1675177
- The Packet Forwarding Engine process crashes from 21.4R1 version onwards on VMhost platforms. PR1681532
- The rpd crash would be observed when two separate next-hops in rpd map to the same next-hop-index in the kernel PR1686211

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
- CPU utilization of rpd process might reach 100% while reporting LSP states to pccd if the IS-IS update churn is high. PR1673348
- 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
- In the RSVP-TE scenario, with Entropy label capability is enabled during MBB issues handling Resv Messages. PR1681403

Multicast

- Traffic silently dropped and discarded might be seen due to next-hop install failure on Junos OS PTX platforms. PR1653920

Migration, Upgrade, and Downgrade Instructions

IN THIS SECTION

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

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

Basic Procedure for Upgrading to Release 22.1

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

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

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

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

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

To download and install Junos OS Release 22.1R2:

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

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

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

3. Select the release number (the number of the software version that you want to download) from the Release drop-down list to the right of the Download Software page.
4. Select the `Software` tab.
5. In the Install Package section of the Software tab, select the software package for the release.
6. Log in to the Juniper Networks authentication system by using the username (generally your e-mail address) and password supplied by Juniper Networks representatives.
7. Review and accept the End User License Agreement.
8. Download the software to a local host.
9. Copy the software to the routing platform or to your internal software distribution site.
10. Install the new jinstall package on the router.

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

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

```
user@host> request system software add validate reboot source/junos-install-ptx-
x86-64-22.1R3.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-
x86-64-22.1R3-limited.tgz
```

Replace the source with one of the following values:

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

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

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

Rebooting occurs only if the upgrade is successful.

NOTE: You need to install the Junos OS software package and host software package on the routers with the RE-PTX-X8 Routing Engine. For upgrading the host OS on this router with VM Host support, use the junos-vmhost-install-x.tgz image and specify the name of the regular package in the `request vmhost software add` command. For more information, see the VM Host Installation topic in the Installation and Upgrade Guide.

NOTE: After you install a Junos OS Release 22.1 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

Support for upgrades and downgrades that span more than three Junos OS releases at a time is not provided, except for releases that are designated as Extended End-of-Life (EEOL) releases. EEOL releases provide direct upgrade and downgrade paths—you can upgrade directly from one EEOL release to the next EEOL release even though EEOL releases generally occur in increments beyond three releases.

You can upgrade or downgrade to the EEOL release that occurs directly before or after the currently installed EEOL release, or to two EEOL releases before or after. For example, Junos OS Releases 19.3, 19.4, and 20.1 are EEOL releases. You can upgrade from Junos OS Release 19.3 to Release 19.4 or from

Junos OS Release 19.3 to Release 20.1. However, you cannot upgrade directly from a non-EEOL release that is more than three releases ahead or behind.

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

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

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 22.1R3 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

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

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

- On QFX5100 switches, NSSU from older Junos OS Release with Broadcom SDK 6.3.x to new Junos release with Broadcom SDK 6.5.x might not work. As a workaround normal upgrade from older release to new release can be done. PR1496765
- Once VLAN is configured on an IFD, its always treated as vlxan port even though Layer 2 VLAN exists.PR1570689
- On QFX5000 devices, IRACL filters will not be able to match on VxLAN tunnel terminated packets. PR1594319
- On QFX5000 devices, we should configure only one static arp with multicast-mac entry per IRB interface. If we configure more than one static arp with multicast Mac entry per IRB interface, then the packets with different destination IP having static multicast mac will always go out with any one of the multicast mac configured in the system. PR1621901
- 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

Infrastructure

- When upgrading from Junos OS Releases 21.2 and later, validation and upgrade might fail. The upgrading requires using of the `no-validate` configuration statement. PR1568757

Open Issues

IN THIS SECTION

Routing Protocols | 105

Learn about open issues in Junos OS Release 22.1R3 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 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 aggregated Ethernet interface, it would trigger a flexible PIC Concentrators (FPC) crash which leads to traffic loss. PR1688455

EVPN

- Multiple remote DCI MAC (IRB and Host) entries go missing after the I-ESI modification in the local DC GW nodes. PR1600600
- This problem happens only with translation VNI when mac moved one from DC1 to DC2. VM move across DC where there is not translate VNI configuration in the interconnect works as designed. PR1610432
- EVPN Local ESI Mac limit config mayn't not get effective immediately when it has already learned remote MH Macs. Clear the Mac table from all MH PEs and configure the Mac limit over local ESI interfaces. PR1619299

Layer 2 Features

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

Layer 2 Ethernet Services

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

Platform and Infrastructure

- When the DHCP relay mode is configured as no-snoop, we are observing the offer gets dropped due to incorrect asic programming. This issue only affects while running DHCP relay on EVPN/VXLAN environment. PR1530160
- 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
- When VLAN is added as an action for changing the VLAN in both ingress and egress filters, the filter is not installed. PR1362609
- VXLAN VNI (multicast learning) scaling on QFX5110 traffic issue is seen from VXLAN tunnel to Layer 2 interface. PR1462548
- When running the command: show pfe filter hw filter-name filter name, the command fails to retrieve the PFE programming details of the filter. PR1495712
- On QFX5100 devices not running the qfx-5e codes (non-TVP architecture), when an image with the Broadcom SDK upgrade (6.5.x) is installed, the CPU utilization may go up by around 5 percent. PR1534234
- 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
- In mixed QFX5100 device, EX4300 VCF setup, duplicate traffic might be observed for some Layer 3 multicast traffic streams. PR1568152

- 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
- 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 gets generated. PR1594748
- Pim Vxlan not working on TD3 chipsets enabling VLAN flexflow after release 21.3R1. Customers Pim Vxlan or data plane VxLAN can use the version 21.3R1. PR1597276
- On QFX5100, optical power is seen after detached and attached QSFP on disable interface. PR1606003
- Dfwd cored when accessing ephemeral db files which is deleted through script. PR1609201
- On Junos QFX1000 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
- minimal traffic loss can be expected if the number of interfaces in ae and could see slight increase if the number of interfaces in ae is increased but the drop is inconsistent and the packet drop would be expected around ~0.0001 percent. PR1629661
- On the QFX5000 devices switch which is working on the 5e image and with VC setup, the chassis status LED does not work properly. An unexpected state of SYS (System) or MST (Master) LED on master or backup FPC might be seen. This could be observed after reboot or change in FPC role. PR1630380
- On QFX5110-32Q devices, traffic loss occurs after renumbering master in VC. PR1632565
- 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
- Management interface speed is displayed as 10G instead of 1G though there is no functionality impact. PR1636668
- On QFX10002-60c, in EVPN/VxLAN scenario multicast traffic received on the INET interface (L3 interface) might be dropped. PR1636842

- On all QFX5100 Virtual Chassis platforms, after the reboot, Virtual Chassis port (VCP) ports may not establish a VCP connection and Cyclic Redundancy Check (CRC) errors are also observed. PR1646561
- On QFX platform, v6 ifl stats are being derived from the underlying ifd stats unlike on PTX where they are hardware assisted. Hence, they are not very reliable and are at best, guesstimate. PR1653671
- EX4600 and QFX5100-24Q devices VC (Virtual-chassis) is in unstable state for 3-7 minutes causing traffic loss. PR1661349
- On QFX10002-60c platform, the DHCP (Dynamic Host Configuration Protocol) offer messages from the DHCP server will be dropped when the device acts as a DHCP relay agent over a Type-5 tunnel. Due to this, the IP address will not be assigned to the requesting client from the DHCP server. PR1664656
- When the remote end server/system reboots, QFX5100 platform ports with SFP-T 1G inserted may go into a hung state and remain in that state even after the reboot is complete. This may affect traffic after the remote end system comes online and resumes traffic transmission. PR1665800
- On QFX5200, after NSSU upgrade for a 4 member VC , FPC may toggle resulting in interfaces going offline. PR1673116
- On 21.4 and 22.1 releases, when QFX5120 performs IFA init for vxlan flows, it will not update the congestion field of IFA meta-data stack which needs to be copied from ECN field of outer IP header. PR1674431
- On all VMHOST based platforms, traffic blackholing happens because the traffic does not re-route quickly as chassisd doesn't recognize an FPC failure from a BAD_VOLTAGE notification. PR1676740
- Sflow ingress/egress sampling not working when ECMP nexthops are involved. PR1685407

Routing Protocols

- When the knob accept-remote-source under PIM is removed, the PIM SG entries may not be updated with the correct RPF. Clearing of the states would take care of the issue. This is day-1 behavior. PR1593283
- MCSNOOPD core is seen sometimes due to Nexthop index being quickly reused by the Kernel. As a result when application is still holding old Nexthop reference which is waiting for deletion response from Kernel, the same Nexthop Index can be hence be received from other applications like RPD for EVPN core-NH updates as in current case. This will lead to MCSNOOPD wrongly manipulating the Nexthop ref counting, leading to using a freed Nexthop memory when this Nexthop-index is finally being freed. This will be fixed via a feature enhancement underway where the Kernel will maintain a

timer to ensure a Nexthop-index is not put to free pool immediately for reuse and hence can be reused post the new timer expiry. PR1605393

Resolved Issues

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

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

Chassis Clustering

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

EVPN

- The kernel crash would be observed in an EVPN multi-homed scenario. PR1649234
- 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

Interfaces and Chassis

- VRRP flaps between MC-LAG peers. PR1579016

Layer 2 Ethernet Services

- The DHCP unicast acknowledge packet might be dropped. PR1676573

MPLS

- Traffic loss will be seen in an LDP->BGP-LU stitching scenario. PR1670334
- The rpd crashes very rarely when constructing LDP trace message irrespective of enable/disable LDP traceoptions. PR1676503

Platform and Infrastructure

- On QFX devices, traffic gets silently discarded after interface flaps. PR1645488

- Traffic loss occurs with Virtual-Router. PR1650335
- The MAC address from the local CE might not be learned due to the VLAN programming issue. PR1651827
- The interface might not come up on EX platforms PR1656540
- FEC link goes down after disabling or enabling the interface. PR1657534
- TOS (DSCP+ECN) bits does not get copied from the inner Layer 3 header to the outer VXLAN header. PR1658142
- The BFD session session-state shows `DOWN` while checking the Micro BFD sessions with authentication in the Non-Distributed mode. PR1658317
- The multipath route might be missing when you configure multipath. PR1659255
- On QFX10000 devices, configuration of IGMP group range might result in traffic loss. PR1659732
- MACsec session configured over IFD might be down when you enable or disable an IFL configured on IFD. PR1660070
- On QFX10008 and QFX10016 devices, the `spmb0 Cell drops on sib 'x' pf 'x'` error message gets generated without generating any alarms. PR1660699
- BUM traffic might loop post when you add or remove a EVPN-VXLAN FRR configuration. PR1662515
- On QFX5100 and QFX5110 devices, IPv6 ND packets might be dropped. PR1662707
- IS-IS adjacency does not come up through the Layer 2 domain. PR1663134
- Verification of the status for BFD session is in the `Up` state while checking the BFD session. PR1663790
- Type-5 traffic drops when you configure the device without IRB in the EVPN-VxLAN scenario. PR1663804
- On QFX5000 devices, dulpicate packets might occur 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
- PVLAN IGMP packet is forwarded between Isolated ports and also duplicated to primary VLAN port (Promiscous). PR1667069
- Multihop BFD sessions might remain down in inline mode. PR1667751
- Shaping-rate does not take 20 bytes of overhead into account. PR1667879

- On specific QFX5000 devices, member links might reduce their configured speed when the other side does not have auto-negotiation disabled. PR1669436
- FPC1 gets disconnected after ISSU and before switchover while checking ISSU status. PR1669702
- The dcpfe process might generate core files and FPC might crash after line card reboot or switchover. PR1670240
- Packet drops after flapping or changing a passive monitor interface. PR1671449
- Flow sample packet does not get sent to the collector when the destination is an ECMP path. PR1672121
- The BFD packets drop in an EVPN-VXLAN scenario due to incorrect Layer 3 offset being set in the host path. PR1674116
- VLAN translation mapping gets deleted when one of the member interface removed from LAG. PR1676772
- Interfaces with QFX-10000-30C and QFX10000-30C-M line cards will not work properly. PR1677325
- Traffic drops if an IP packet with TTL=1 is routed over VXLAN Tunnel. PR1678992
- Firewall functions do not work as expected when you configure egress firewall filter. PR1679574
- On QFX5120 Virtual Chassis, ARP resolution fails. PR1679684
- In distributed mode, BFD sessions remains down in the EVPN-VXLAN scenario. PR1680757
- The PFE process crashes from 21.4R1 version onwards on VMhost platforms. PR1681532
- LLDP neighborship fails to come up with a Private VLAN configuration. PR1681614
- dcpfe core seen with PTP configuration on Junos platforms supporting boundary clock. PR1683308
- Licenses on the device might become invalid when the device is upgraded from a legacy licensing-based release to an Agile licensing-based release. PR1684842
- OVSDB certificate files are not copied from the Master to the Backup. PR1687847
- ARP resolution to the IRB interface would get fail in the EVPN-VXLAN scenario. PR1687861
- On QFX10008/QFX10016 platforms fails to detect flaps even though the remote device connected has observed flaps. PR1688993
- [Blocker:Test] ULTIMAT[QFX10008]: While verifying "show ethernet-switching global-mac-count | display xml" command "global-mac-count" is not as expected. PR1689127

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
- 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
- The peer-auto-discovery for BGP doesn't work after soft detach/attach of QSFP. PR1679950

User Interface and Configuration

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

VPNs

- On QFX10000 devices NGMVPN scenario, Auto-RP goes down after some time. PR1617620

Migration, Upgrade, and Downgrade Instructions

IN THIS SECTION

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

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

Upgrading Software on QFX Series Switches

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

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

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

   The Junos Platforms Download Software page appears.

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

3. Select **22.1** 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 22.1 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-x86-64-22.1R2.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 22.1 `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-x86-64-22.1R2.9.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-
x86-64-22.1R2.9.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 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-x86-64-22.1R2.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-x86-64-22.1R2.n-secure-signed.tgz reboot
```

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

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

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

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

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

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

To install the software on re0:

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

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

For example:

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

To install the software on re1:

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

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

For example:

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

Reboot both Routing Engines.

For example:

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

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

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

Installing the Software on QFX10008 and QFX10016 Switches

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

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

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

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

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

2. From the command line, enter configuration mode:

```
user@switch> configure
```

3. Disable Routing Engine redundancy:

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

4. Disable nonstop-bridging:

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

5. Save the configuration change on both Routing Engines:

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

6. Exit the CLI configuration mode:

```
user@switch# exit
```

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

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

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

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

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

```
user@switch> request system software add validate /var/tmp/jinstall-host-qfx-10-f-
x86-64-22.1R2.n-secure-signed.tgz
```

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

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

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

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

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

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

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

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

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

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

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

12. Transfer routing control to the backup Routing Engine:

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

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

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

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

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

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

```
user@switch> request system software add validate /var/tmp/jinstall-host-qfx-10-f-
x86-64-22.1R2.n-secure-signed.tgz
```

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

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

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

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

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

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

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

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

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

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

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

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

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

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

Performing a Unified ISSU

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

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

Perform the following tasks:

- Preparing the Switch for Software Installation
- Upgrading the Software Using Unified ISSU

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-x86-64-22.1-R2.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

Support for upgrades and downgrades that span more than three Junos OS releases at a time is not provided, except for releases that are designated as Extended End-of-Life (EEOL) releases. EEOL releases provide direct upgrade and downgrade paths—you can upgrade directly from one EEOL release to the next EEOL release even though EEOL releases generally occur in increments beyond three releases.

You can upgrade or downgrade to the EEOL release that occurs directly before or after the currently installed EEOL release, or to two EEOL releases before or after. For example, Junos OS Releases 19.3, 19.4, and 20.1 are EEOL releases. You can upgrade from Junos OS Release 19.3 to Release 19.4 or from Junos OS Release 19.3 to Release 20.1.

You cannot upgrade directly from a non-EEOL release to a release that is more than three releases ahead or behind. To upgrade or downgrade from a non-EEOL release to a release more than three releases before or after, first upgrade to the next EEOL release and then upgrade or downgrade from that EEOL release to your target release.

For more information about EEOL releases and to review a list of 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 22.1R3 for the SRX Series Services Gateways. They describe new and changed features, limitations, and known and resolved problems in the hardware and software.

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

What's New

There are no new features or enhancements to existing features in this release for SRX Series devices.

What's Changed

IN THIS SECTION

Learn about what changed in this release for SRX Series.

VPNs

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

  [See Improving IPsec Performance with PowerMode IPsec.]

Known Limitations

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

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

Chassis Clustering

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

Infrastructure

- When upgrading from releases before Junos OS Release 21.2 to Release 21.2 and onward, validation and upgrade might fail. The upgrading requires using of 'no-validate' configuration statement.PR1568757

- 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

VPNs

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

Open Issues

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

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

Chassis Clustering

- On SRX platform with chassis cluster enabled, chassis cluster IP monitoring on the secondary node might fail after system rebootPR1691071

Flow-Based and Packet-Based Processing

- Use an antireplay window size of 512 for IPv4 or IPv6 in fat-tunnel. The ESP sequence check might otherwise report out-of-order packets if the fat-tunnel parallel encryption is within 384 packets (12 cores * 32 packets in one batch). Hence, there are no out-of-order packets with 512 antireplay window size. PR1470637
- For accelerated flows such as Express Path, the packet or byte counters in the session close log and show session output take into account only the values that accumulated while traversing the NP. PR1546430

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
- IPSec rekey fails when SRX is configured with kilobyte based lifetime in remote access solution. PR1527384
- With Application-Based Multipath Routing enabled, HTTP sessions take approx 10 minutes to re-establish after a link flap between hub and spoke. PR1577021
- With ssl-proxy configured along with web-proxy, the client session might not get closed on the device until session timeout, even though the proxy session ends gracefully.PR1580526
- On MX platforms the JDM (Juniper Device Manager) server could not be created in in-chassis mode of junos node slicing, which results in mgd process crash and affects GNF's (Guest Network Function) provisioning. PR1583324
- HA AP mode on-box logging in LSYS and Tenant, Intermittently Security log contents of binary log file in LSYS are not as expected PR1587360
- On the SRX4100 and SRX4200 platforms, it can detect DPDK (data plane development kit) Tx stuck issue and trigger a major chassis alarm goes which might trigger RG1 failover to the healthy node. A DPDK reset will be triggered only to the stuck port and if the reset resolves the tx stuck issue, the major chassis alarm will go off.PR1626562
- A Missing Release of Memory after Effective Lifetime vulnerability in the Application Quality of Experience (appqoe) subsystem of the PFE of Juniper Networks Junos OS on SRX Series allows an unauthenticated network based attacker to cause a Denial of Service (DoS). Please refer to https://kb.juniper.net/JSA69709 for more information.PR1628090
- 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 SRX5000 line of devices 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
- File submission success counter is not changed when file is submitted to cloud. PR1651101
- Firewall-authentication with user-firewall based RADIUS access has syslog missing the username and rule.PR1654842
- File archive command under non-root account may not archive all files under /var/log.PR1657958
- On SRX series platform with chassis cluster enabled, reth interface might not go up due to speed mismatch when reth interface speed is changed afger RG0 failoverPR1658276
- SRX cli command to show fwauth user details like "show security firewall-authentication users identifier 1" and "show security firewall-authentication users address 10.1.1.1" does not display user's group information.PR1659115
- Device does not drop session with server certificate chain more than 6.PR1663062

User Interface and Configuration

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

VPNs

- In some scenario(e.g configuring firewall filter) sometimes srx5K might show obsolete IPsec SA and NHTB entry even when the peer tear down the tunnel. PR1432925
- Tunnel debugging configuration is not synchronized to the backup node. It needs to be configured again after RG0 failover. PR1450393
- First time when we add this command the existing active connections are not changed, only the new connection after this command will be taken into effect. PR1608715
- Sometimes after manual failover, IKE-SA rekey does not succeed. In order to recover from this scenario, enable dead-peer-detection with always-sendPR1690921

Resolved Issues

Learn about the issues fixed 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)

- 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
- SIP calls are getting dropped due to NAT failure and SIP ALG is enabled PR1686613

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)

- "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
- vSRX not processing fragmented packets PR1668898
- The flow sessions traversing the IOC2 card would time out early when Automated Express Path is enabled PR1688658
- On SRX5K and SRX 4600 series devices, Automated Express Path (SOF) was incorrectly offloading short-lived flows. This consumed additional resources on the Network Processor (NP) which could lead to an early exhaustion of its memory, reducing overall device performance PR1692100

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

Intrusion Detection and Prevention (IDP)

- 21.2R3:SRX345:vSRX3.0:Device is hanging while checking the cli " show security idp attack attack-list policy combine-policy" PR1616782

J-Web

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

Network Management and Monitoring

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

Platform and Infrastructure

- SMS Channel Down alarm on primary node of HA pair after upgrade PR1629972
- 5K device SSL Session-Cache Inconsistencies from other platforms wrt tls1.3 resumption sessions PR1642174
- 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
- The mspmand will crash when service-set is configured with syslog and SSL PR1657027
- 22.2TOT SecPDT: SRX4600: After ISSU upgrade completed, RG1 nodes priority remains in CS state and fab interfaces are down. PR1658148
- Ssl-proxy: Cache miss counter increments twice instead of one PR1663678
- SRX alarming "SMS control channel down" without SMS feature configured PR1666420
- NG custom app identification fails on Junos SRX platforms PR1667221
- 22.1 DCB: IPv6 feature not working on 5K platform. PR1668473
- Traffic loss seen due to SPC3's packets getting stuck PR1671649
- The Forwarding plane crashes during HA failover PR1672378
- Information about users groups is not displayed completely PR1673125
- VPN tunnel will not be established in exclusive client scenario PR1674522

- 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
- Dial-on-demand mode on DL interface not working as expected PR1680405
- The cluster fabric link will be down post reboot of node or power cycle PR1684756
- unexpected default event-rate value for event mode logging PR1687244

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
- Junos OS: SRX Series: Cache poisoning vulnerability in BIND used by DNS Proxy (CVE-2021-25220) PR1656324
- 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

Routing Protocols

- The BSR information might not be flooded over NG-MVPN PR1664211
- High CPU is seen on the platforms running IPv6 PR1677749

User Interface and Configuration

- "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

- Traffic over IPSec tunnels may be dropped during ISSU PR1416334

- Vmcore is seen on Junos platforms when data plane IPSec is configured PR1648249
- Packets traversing through a policy-based VPN get dropped when PowerMode is enabled PR1663364
- IPSec tunnels may flap on SRX platforms PR1665332
- 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, standard EOL and EEOL:

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

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

For EEOL releases only, you have an additional option - you can upgrade directly from one EEOL release to the next two subsequent EEOL releases, even if the target release is beyond the next three releases. Likewise, you can downgrade directly from one EEOL release to the previous two EEOL releases, even if the target release is beyond the previous three releases. For example, 20.4 is an EEOL release. Hence, you can upgrade from 20.4 to the next two EEOL releases – 21.2 and 21.4 or downgrade to the previous two EEOL releases – 20.2 and 19.4.

Table 4: EOL and EEOL Releases

Release Type	End of Engineering (EOE)	End of Support (EOS)	Upgrade/ Downgrade to subsequent 3 releases	Upgrade/ Downgrade to subsequent 2 EEOL releases
Standard End of Life (EOL)	24 months	End of Engineering + 6 months	Yes	No
Extended End of Life (EEOL)	36 months	End of Engineering + 6 months	Yes	Yes

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

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

Junos OS Release Notes for vMX

IN THIS SECTION

These release notes accompany Junos OS Release 22.1R3 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 or software 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.

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

- On vMX, the blockpointer in the ktree is getting corrupted leading to core-file generation. There is no function impact such as fpc restart or system down and the issue is not seen in hardware setups. PR1525594

Resolved Issues

There are no resolved 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.

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 22.1R3 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 or software in this release for vRR.

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

To learn more about common BGP or routing known limitations in Junos OS 21.1R3, see "Known Limitations" on page 40 for MX Series routers.

Open Issues

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

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

Resolved Issues

Learn about the issues fixed in this release for vRR.

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

Platform and Infrastructure

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

Junos OS Release Notes for vSRX

IN THIS SECTION

These release notes accompany Junos OS Release 22.1R3 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 or software 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.

Open Issues

Learn about open issues in this release for vSRX.

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

Flow-Based and Packet-Based Processing

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

Platform and Infrastructure

- With ssl-proxy configured along with web-proxy, the client session might not get closed on the device until session timeout, even though the proxy session ends gracefully.PR1580526
- A Missing Release of Memory after Effective Lifetime vulnerability in the Application Quality of Experience (appqoe) subsystem of the PFE of Juniper Networks Junos OS on SRX Series allows an unauthenticated network based attacker to cause a Denial of Service (DoS). Please refer to https://kb.juniper.net/JSA69709 for more information.PR1628090
- Device does not drop session with server certificate chain more than 6.PR1663062

VPNs

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

Resolved Issues

Learn about the issues fixed in this release for vSRX.

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

- Expected TCP sequences not found in ICMP6 dump PR1611202
- vSRX not processing fragmented packets PR1668898
- Packet loss on GRE Tunnel due to improper route look-up for tunnel destination PR1683334

Intrusion Detection and Prevention (IDP)

- 21.2R3:SRX345:vSRX3.0:Device is hanging while checking the cli " show security idp attack attack-list policy combine-policy" PR1616782

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
- NG custom app identification fails on Junos SRX platforms PR1667221
- ARP will not get learned if reth interface is configured with VLAN PR1681042

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

- "vpn-monitoring" will not work as expected when PMI enable 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 22.1R2 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 22.1R2 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 22.1R2 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-x86-64-22.1-2022-10-12.0_RELEASE_22.1_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-
x86-64-22.1-2022-10-12.0_RELEASE_22.1_THROTTLE.tgz no-copy no-validate reboot
Verified junos-vsrx-x86-64-22.1-2022-10-12.0_RELEASE_22.1_THROTTLE signed by
PackageDevelopmentEc_2017 method ECDSA256+SHA256
THIS IS A SIGNED PACKAGE
WARNING:     This package will load JUNOS 22.1 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-22.1-2022-10-12.0_RELEASE_22.1_THROTTLE.tgz
Extracting the package ...
total 975372
-rw-r--r-- 1 30426 950 710337073 Oct 19 17:31 junos-srx-mr-
vsrx-22.1-2022-10-12.0_RELEASE_22.1_THROTTLE-app.tgz
-rw-r--r-- 1 30426 950 288433266 Oct 19 17:31 junos-srx-mr-
vsrx-22.1-2022-10-12.0_RELEASE_22.1_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-22.1-2022-10-12.0_RELEASE_22.1_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-22.1-2022-10-12.0_RELEASE_22.1_THROTTLE-linux.tgz ...
upgrade_platform: Input package /var/tmp/junos-srx-mr-
vsrx-22.1-2022-10-12.0_RELEASE_22.1_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-22.1-2022-10-12.0_RELEASE_22.1_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-22.1-2022-10-12.0_RELEASE_22.1_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 22.1R2 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 22.1-2022-10-12.0_RELEASE_22.1_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: 22.1-2022-10-12.0_RELEASE_22.1_THROTTLE
JUNOS OS Kernel 64-bit  [20171012.170745_fbsd-builder_stable_11]
JUNOS OS libs [20171012.170745_fbsd-builder_stable_11]
JUNOS OS runtime [20171012.170745_fbsd-builder_stable_11]
JUNOS OS time zone information [20171012.170745_fbsd-builder_stable_11]
JUNOS OS libs compat32 [20171012.170745_fbsd-builder_stable_11]
JUNOS OS 32-bit compatibility [20171012.170745_fbsd-builder_stable_11]
```

```
JUNOS py extensions [20171017.110007_ssd-builder_release_174_throttle]
JUNOS py base [20171017.110007_ssd-builder_release_174_throttle]
JUNOS OS vmguest [20171012.170745_fbsd-builder_stable_11]
JUNOS OS crypto [20171012.170745_fbsd-builder_stable_11]
JUNOS network stack and utilities [20171017.110007_ssd-builder_release_174_throttle]
JUNOS libs [20171017.110007_ssd-builder_release_174_throttle]
JUNOS libs compat32 [20171017.110007_ssd-builder_release_174_throttle]
JUNOS runtime [20171017.110007_ssd-builder_release_174_throttle]
JUNOS Web Management Platform Package [20171017.110007_ssd-builder_release_174_throttle]
JUNOS srx libs compat32 [20171017.110007_ssd-builder_release_174_throttle]
JUNOS srx runtime [20171017.110007_ssd-builder_release_174_throttle]
JUNOS common platform support [20171017.110007_ssd-builder_release_174_throttle]
JUNOS srx platform support [20171017.110007_ssd-builder_release_174_throttle]
JUNOS mtx network modules [20171017.110007_ssd-builder_release_174_throttle]
JUNOS modules [20171017.110007_ssd-builder_release_174_throttle]
JUNOS srxtvp modules [20171017.110007_ssd-builder_release_174_throttle]
JUNOS srxtvp libs [20171017.110007_ssd-builder_release_174_throttle]
JUNOS srx libs [20171017.110007_ssd-builder_release_174_throttle]
JUNOS srx Data Plane Crypto Support [20171017.110007_ssd-builder_release_174_throttle]
JUNOS daemons [20171017.110007_ssd-builder_release_174_throttle]
JUNOS srx daemons [20171017.110007_ssd-builder_release_174_throttle]
JUNOS Online Documentation [20171017.110007_ssd-builder_release_174_throttle]
JUNOS jail runtime [20171012.170745_fbsd-builder_stable_11]
JUNOS FIPS mode utilities [20171017.110007_ssd-builder_release_174_throttle]
```

Validating the OVA Image

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

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

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

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

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

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

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

For EEOL releases only, you have an additional option - you can upgrade directly from one EEOL release to the next two subsequent EEOL releases, even if the target release is beyond the next three releases. Likewise, you can downgrade directly from one EEOL release to the previous two EEOL releases, even if the target release is beyond the previous three releases. For example, 20.4 is an EEOL release. Hence, you can upgrade from 20.4 to the next two EEOL releases – 21.2 and 21.4 or downgrade to the previous two EEOL releases – 20.2 and 19.4.

Table 5: EOL and EEOL Releases

Release Type	End of Engineering (EOE)	End of Support (EOS)	Upgrade/ Downgrade to subsequent 3 releases	Upgrade/ Downgrade to subsequent 2 EEOL releases
Standard End of Life (EOL)	24 months	End of Engineering + 6 months	Yes	No
Extended End of Life (EEOL)	36 months	End of Engineering + 6 months	Yes	Yes

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

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

Licensing

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

The major components of the framework are:

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

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

Finding More Information

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

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

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

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

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

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

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

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

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

Requesting Technical Support

IN THIS SECTION

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

- JTAC policies—For a complete understanding of our JTAC procedures and policies, review the JTAC User Guide located at https://www.juniper.net/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/
- Create a service request online: https://supportportal.juniper.net/

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

Creating a Service Request with JTAC

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

- Visit https://support.juniper.net/support/requesting-support/
- 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

10 August 2023—Revision 4, Junos OS Release 22.1R3– ACX Series, cRPD, cSRX, EX Series, JRR Series, Juniper Secure Connect, Junos Fusion, MX Series, NFX Series, PTX Series, QFX Series, SRX Series, vMX, vRR, and vSRX.

6 July 2023—Revision 3, Junos OS Release 22.1R3– ACX Series, cRPD, cSRX, EX Series, JRR Series, Juniper Secure Connect, Junos Fusion, MX Series, NFX Series, PTX Series, QFX Series, SRX Series, vMX, vRR, and vSRX.

2 June 2023—Revision 2, Junos OS Release 22.1R3– ACX Series, cRPD, cSRX, EX Series, JRR Series, Juniper Secure Connect, Junos Fusion, MX Series, NFX Series, PTX Series, QFX Series, SRX Series, vMX, vRR, and vSRX.

5 December 2022—Revision 1, Junos OS Release 22.1R3– ACX Series, cRPD, cSRX, EX Series, JRR Series, Juniper Secure Connect, Junos Fusion, MX Series, NFX Series, PTX Series, QFX Series, SRX Series, vMX, vRR, and vSRX.

Juniper Networks, the Juniper Networks logo, Juniper, and Junos are registered trademarks of Juniper Networks, Inc. in the United States and other countries. All other trademarks, service marks, registered marks, or registered service marks are the property of their respective owners. Juniper Networks assumes no responsibility for any inaccuracies in this document. Juniper Networks reserves the right to change, modify, transfer, or otherwise revise this publication without notice. Copyright © 2023 Juniper Networks, Inc. All rights reserved.