Release Notes

Published
2023-11-16

Junos OS Release 22.3R3®

JUNIPER NETWORKS | Engineering Simplicity

Table of Contents

Introduction

Junos OS runs on the following Juniper Networks® hardware: ACX Series, cRPD, cSRX, EX Series, JRR Series, Juniper Secure Connect, Junos Fusion Enterprise, Junos Fusion Provider Edge, MX Series, NFX Series, PTX Series, QFX Series, SRX Series, vMX, vRR, and vSRX. These release notes accompany Junos OS Release 22.3R3. They describe new and changed features, limitations, and known and resolved problems in the hardware and software.

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

Junos OS Release Notes for ACX Series

IN THIS SECTION

These release notes accompany Junos OS Release 22.3R3 for the ACX Series. They describe new and changed features, limitations, and known and resolved problems in the hardware and software.

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

What's New

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

What's Changed

IN THIS SECTION

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

General Routing

- Verified the qualification of codeph ordered-by-user codeph in the hierarchies (ACX Series, EX Series, MX Series, QFX Series, SRX Series, vMX, and vSRX)-The requested hierarchies are reviewed and checked to confirm if they qualify for the `ordered-by-user` list type. If they do not, the `flag autosort` is included in the DDL definition for the list, making it `ordered-by-system` . The hierarchies are now indexed. The benefits from this arrangement are we get accurate data modeling and optimized configuration load in the user interface infrastructure.
- In the past inet6flow.0 was not allowed to be a primary rib in a rib-group. Starting with Release 22.3 this is now allowed.
- **Label-switched interface (LSI) delay during reboot (ACX Series)** — Rebooting ACX Series routers running Junos OS Evolved with a class-of-service routing-instance configuration might encounter errors due to a delay with the label-switched interface (LSI). LSI state information has been added to the output of the `show route instance` command to assist in the analysis of such errors.

  See show route instance

Junos XML API and Scripting

- **Ability to commit `extension-service file` configuration when application file is unavailable**— When you set the `optional` option at the `edit system extension extension-service application file` *`file-name`* hierarchy level, the operating system can commit the configuration even if the file is not available at the **/var/db/scripts/jet** file path.

[See file (JET).]

- **The `xmlns:junos` attribute includes the complete software version string (ACX Series, EX Series, MX Series, PTX Series, QFX Series, SRX Series, vMX, and vSRX)**—The `xmlns:junos` namespace string in XML RPC replies includes the complete software version release number, which is identical to the version emitted by the `show version` command. In earlier releases, the `xmlns:junos` string includes only partial software version information.

Network Management and Monitoring

- **`operator` login class is restricted from viewing NETCONF trace files that are `no-world-readable` (ACX Series, EX Series, MX Series, PTX Series, QFX Series, SRX Series, vMX, and vSRX)**—When you configure NETCONF tracing options at the `[edit system services netconf traceoptions]` hierarchy level and you restrict file access to the file owner by setting or omitting the `no-world-readable` statement (the default), users assigned to the `operator` login class do not have permissions to view the trace file.

Known Limitations

IN THIS SECTION

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

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

General Routing

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

Infrastructure

- When upgrading from releases before Junos OS Release 21.2 to Release 21.2 and onward, validation and upgrade might fail. The upgrading requires using of 'no-validate' configuration statement. https://kb.juniper.net/TSB18251PR1568757

Open Issues

IN THIS SECTION

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

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

General Routing

- VXLAN VNI (multicast learning) scaling on QFX5110 traffic issue is seen from VXLAN tunnel to Layer 2 interface. PR1462548
- Due to BRCM KBP issue route lookup might fail. Need to upgrade KBP to address this issue. PR1533513
- Service MIC does not work on ACX500 running Junos 20.4 or higher. PR1569103
- On all ACX Platforms, the hosts will not receive multicast traffic when snooping is configured in a Ethernet Virtual Private Network - Multiprotocol Label Switching (EVPN-MPLS) enabled broadcast domain. PR1613462
- For ACX5448, MX204, and MX2008 "VM Host-based" platforms, starting with Junos 21.4R1 or later, ssh and root login is required for copying line card image (chspmb.elf for MX2008) from Junos VM to Linux host during installation. The ssh and root login are required during installation. Use "deny-

password" instead of "deny" as default root-login option under ssh configuration to allow internal trusted communication. Ref https://kb.juniper.net/TSB18224 PR1629943

- On Junos ACX platforms (ACX1100, ACX2100 and ACX2200) the FEB (Forwarding Engine Board) crash might occur. This might only occur when the system has encountered a dual parity error on MPLS entry memory in the hardware. There might be an impact on services when the FEB crashes, however, it returns to normal functionality after the crash. PR1632043
- A vulnerability in class-of-service (CoS) queue management in Juniper Networks Junos OS on the ACX2K Series devices allows an unauthenticated network-based attacker to cause a Denial of Service (DoS). Refer to https://kb.juniper.net/JSA70187 for more information.PR1637615
- EX4100-24mp,48mp,24p/t,48p/t,F-24p/t,F-48-p/t: In an interop scenario, when using 1G SFP Optic on PIC-2, auto-negotiation should be disabled on the peerPR1657766
- In VPLS MH cases, the standby UNI ifl in backup router will be programmed in disable state, by adding the UNI interface to invalid vpn id in HW. During switch over the UNI ifl will be deleted and will be added under the VPLS instance VPN id. In issue case, UNI interface added under invalid VPN id in backup router is tried to deleted by passing the VPLS instance vpn id, causing the issue. This issue is applicable only for ACX5000 series.PR1665178
- When there are more than 1 dhcp server connected to the device and zeroize in initiated then multiple route are added and the file server is not reachable after the zeroize if it is not reachable through the default route. PR1675011
- dc-pfe: HEAP malloc(0) detected! when a VPLS instance is deactivated in ACX5048. This are informational messages and the fix of this PR hides the messages from console output. PR1692400
- Convergance Time can be more than 60ms for OSPF TILFA Node protection testing.PR1695292
- FIPS mode is not supported in this release for SRXSME devices.PR1697999

Infrastructure

- Earlier implementation of kvmclock with vDSO (virtual Dynamic Shared Object) which helps avoid the system call overhead for user space applications had problem of time drift, the latest set of changes takes care of initializing the clock after all auxiliary processors are launched so that the clock initialization is accurate. PR1691036

Resolved Issues

IN THIS SECTION

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

General Routing

- Delegated BFD sessions configured on routing-instance may fail to come up. PR1633395
- SSH non-default port configuration causes FPC offline after an upgrade to 21.4. PR1660446
- New BFD sessions will not come up on ACX5448/ACX710 due to continuous flaps. PR1670684
- EX/QFX SNMP: jnxOperatingDescr.1.1.0.0 returns blank, but jnxOperatingState.1.1.0.0 returns value. PR1683753
- Traffic blackhole during l2circuit pseudowire redundancy neighbor switchover. PR1686260
- jdchpd core seen with dhcp-snooping persistent configuration. PR1688644
- Integration of RCP binary into the LTS19 code for Vmhost Platforms. PR1689100
- On ACX5448, an interface with SFP-T optic set to 100m and auto-negotiation disabled will remain down after reboot or on chassis-control restart. PR1702239
- Leaf to leaf traffic flow is observed on Junos ACX5448 platform with EVPN E-Tree configuration. PR1702615
- CoS rewrite rules will not work in L3VPN scenario. PR1703840
- DHCP_RELAY- ACX7100-48L :: Getting commit error for the dhcp config commit and then it is coring with the bt jtimer_start_oneshot. PR1707690
- The packet is not getting tagged in the VLAN-based EVPN scenario on Junos ACX platforms. PR1710668

- Transit traffic drop is observed for the BGP-LU route prefixes with ECMP forwarding path on Junos ACX5448/ACX710 platforms. PR1712564
- The member interface will not be added to the AE bundle if the link-speed of the AE interface doesn't match that of the member. PR1713699
- The traffic through the AE member link will be dropped. PR1714111
- SFP-T cannot be recognized after detecting an I2C error on ACX5448. PR1715924
- SNMP MIB OID output showing wrong temperature value if device running under negative temperature. PR1717105
- The multicast packets could hit the CPU/RE on ACX5448 and ACX710 platforms. PR1722277
- Intermittent MAC move is observed in VPLS environment when ACX5448 or ACX710 is acting as a PE device. PR1722919
- Traffic is getting discarded in PFE when forwarding-table is changed. PR1723624

Interfaces and Chassis

- Incompatible/unsupported configuration is not getting validated correctly during ISSU/normal upgrade causing the traffic loss. PR1692404
- On Junos platforms the dcd will flap the IFLs which are part of EVPN routing-instance. PR1712800

Routing Protocols

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

Migration, Upgrade, and Downgrade Instructions

IN THIS SECTION

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

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

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

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

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

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

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

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

Table 1: EOL and EEOL Releases

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

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

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

Junos OS Release Notes for cSRX

IN THIS SECTION

These release notes accompany Junos OS Release 22.3R3 for the cSRX Container Firewall, a containerized version of the SRX Series Services Gateway. They describe new and changed features, limitations, and known and resolved problems in the hardware and software.

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

What's New

There are no new features or enhancements to existing features in Junos OS Release 22.3R3 for cSRX.

What's Changed

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

Known Limitations

There are no known limitations in hardware and software in Junos OS 22.3R3 for cSRX.

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

Open Issues

There are no known issues in hardware and software in Junos OS Release 22.3R3 for cSRX.

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

Resolved Issues

There are no resolved issues in Junos OS Release 22.3R3 for cSRX.

Junos OS Release Notes for EX Series

IN THIS SECTION

These release notes accompany Junos OS Release 22.3R3 for the EX Series. They describe new and changed features, limitations, and known and resolved problems in the hardware and software.

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

What's New

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

What's Changed

IN THIS SECTION

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

General Routing

- **Verified the qualification of `ordered-by-user` in the hierarchies (ACX Series, EX Series, MX Series, QFX Series, SRX Series, vMX, and vSRX)**—The requested hierarchies are reviewed and checked to confirm if they qualify for the `ordered-by-user` list type. If they do not, the `flag autosort` is included in the DDL definition for the list, making it `ordered-by-system`. The hierarchies are now indexed. The benefits from this arrangement are we get accurate data modeling and optimized configuration load in the user interface infrastructure.
- In the past inet6flow.0 was not allowed to be a primary rib in a rib-group. Starting with Release 22.3 this is now allowed.

Junos XML API and Scripting

- **The `xmlns:junos` attribute includes the complete software version string (ACX Series, EX Series, MX Series, PTX Series, QFX Series, SRX Series, vMX, and vSRX)**—The `xmlns:junos` namespace string in XML RPC replies includes the complete software version release number, which is identical to the version emitted by the `show version` command. In earlier releases, the `xmlns:junos` string includes only partial software version information.

Network Management and Monitoring

- **`operator` login class is restricted from viewing NETCONF trace files that are `no-world-readable` (ACX Series, EX Series, MX Series, PTX Series, QFX Series, SRX Series, vMX, and vSRX)**—When you configure NETCONF tracing options at the `[edit system services netconf traceoptions]` hierarchy level and you restrict file access to the file owner by setting or omitting the `no-world-readable` statement (the default), users assigned to the `operator` login class do not have permissions to view the trace file.

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

- 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
- On EX4100 48P/T devices, on changing interface speed change, the interface stats are retained on ports 24-to-47 but cleared on ports 0-23. PR1657995
- On EX4100 and EX4100-F devices, the SKU PIC0 ports (except EX4100-24MP first 8 ports [mge 0-7]), Jabber frames are dropped as oversized frames. PR1663992
- On EX4100 and EX4100-F devices, VC (PIC1) 4x1G ports in network-mode will need auto-neg off on the peer-device. PR1665640
- MVRP on PVLAN promiscuous port is not supported. If MVRP is configured on promiscuous port, then hosts connected to secondary VLAN ports will not be able to reach external world through promiscuous port carrying primary VLAN tags. PR1693345
- The `request system reboot all-member at now` command might work for all members of a VC. "Reboot AT now" is not recommended to be used. Recommendation is to use reboot command for each member. PR1725406

Virtual Chassis

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

Open Issues

IN THIS SECTION

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

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

Network Management and Monitoring

- Device schema leaf may not populate the appropriate values through jvision/telemetry. PR1726505

Platform and Infrastructure

- On EX4400-48MP devices, VM cores and VC split might occur with multicast scale scenario. PR1614145
- On EX4300 devices, if you configure `encapsulation ethernet-bridge`, the interface is getting programmed as trunk instead of access in VLAN membership. This leads to untagged traffic drop. PR1665785

- On EX4300-24T, EX4300-48P, EX4300-VC, EX430024P, EX430032F and EX430048T platforms, when a VSTP (VLAN Spanning Tree Protocol) BPDU (Bridge Protocol Data Unit) arrives with a VLAN ID that is not configured in the switch, but that matches with an HW Token of any other configured VLAN, the VLAN ID of the BPDU will be changed to the VLAN ID corresponding to the matched HW Token and flooded. This disrupts STP convergence on the configured VLAN because some ports can incorrectly go into blocking state. PR1673000
- 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 devices. PR1492605
- On EX4300-48MP devices, if POE is enabled, a primary Routing Engine might reconnect that might impact traffic. PR1499771
- On EX2300, EX3400, EX4300-48MP, and EX4300 , pause frames counters does not get incremented when pause frames are sent. PR1580560
- On EX4400 devices, sometimes login prompt is not shown after the login session ends. PR1582754
- On EX4100-24mp, EX4100-48mp, EX4100-24p/t, EX4100-48p/t, EX4100-F-24p/t, and EX4100-F-48-p/t devices, in an interop scenario, when you use the 1G SFP Optic on PIC-2, auto-negotiation should be disabled on the peer. PR1657766
- On EX4600 devices, the Virtual Chassis is in unstable state for 3 to7 minutes causing traffic loss. PR1661349
- On EX4100 and EX4100-F devices, PIC 1 ports with 1G optic will display AN enabled but it is not enabled in the hardware. Example: user@device# run show interfaces ge-0/1/1 media .. .. Source filtering: Disabled, Flow control: Enabled, Auto-negotiation: Enabled, Remote fault: Online, Media type: Fiber. PR1666227
- On the EX4600 device with SFP-LX10/SFP-SX, after a power cycle/software reboot, all ports are initialized and links are up with auto-negotiation enabled. Few ports are up and traffic flows whereas few ports are up but no traffic flow through them.PR1672583
- If MVRP is enabled on an MSTP enabled interface, the interface will be made part of all the existing instances on the switch, So, if there are two interfaces between R1 and R2 as below: R1(et-0/0/1 and et-0/0/2)======(et-0/0/1 and et-0/0/2)R2 And one interface is MVRP enabled (say et-0/0/1), and et-0/0/2 is not MVRP enabled. By configuration et-0/0/1 is part of MSTI-1 and et-0/0/2 is part of MSTI-2. MSTI-1 is running on vlan-100 and MSTI-2 is running on Vlan-200. R2 in this case, is advertising only vlan-100. The MVRP enabled interface will become part of all the MSTIs(MSTI-1 and MSTI-2 both) configured on the device and it will take part in the FSM of all the MSTIs. Although et-0/0/1 is not member interface of vlan-200(correspnding to MSTI-2). This potentially can cause a problem where et-0/0/1 although not a vlan-200 member, will go into FWD state and et-0/0/2,

genuine member of vlan-200 goes into BLK state for MSTI-2. So, when traffic is received in vlan-200 it will be sent out of et-0/0/1, an it will be dropped.PR1686596

- When port beacon LED for port is enabled, show chassis led cli output shows incorrect port LED status for interfaces as lit up instead of off. PR1697678
- The EX4600 devices with Redundant Trunk Group (RTG) configured, after VCP port between members of EX4600 disconnect and connect again. Mac address entry created in RTG cannot ageout. PR1707878
- [DOT1X with GBP]:dot1x EAP authentication might not authenticate successfully. PR1728538
- When packets of size bigger than 1518 Bytes are received/transmitted, pps counter value does not show correct value. PR1700309
- In a rare scenario, due to timing issues, the Packet Forwarding Engine (PFE) crash is observed on Junos EX4300 platforms. This causes traffic loss until the PFE comes up. PR1720219
- On Junos EX series platforms, VRRP (Virtual Router Redundancy Protocol) sync will be delayed impacting the VRRP traffic if the device receives a VRRP packet when setting up the 'mac-move-limit' configuration. PR1725042
- After BIOS upgrade of EX4400-VC, device mode will be changed to HiGig mode if they are operating in HGoE mode earlier. PR1725683
- In a heaviliy loaded system in a specific scenario (Dot1x in multiple supplicant mode and dynamic vlan from radius server and non vxlan access port) following log message may be captured in the syslog - {brcm_as_dot1x_vxlan_set_mac_learning_mode:1168 dot1x bd_get failed for bd index 0}. This log is not impacting any funtionality. PR1733365

Routing Protocols

- When the shortest-path-first (SPF) algorithm for IS-IS gets triggered frequently, CPU usage might increase and impact the device performance and traffic. PR1667575

Virtual Chassis

- On Junos EX4600 Virtual Chassis (VC), the primary Routing Engine reboot and all-members reboot lead to the Packet Forwarding Engine Manager hogging logs when SFP-T pluggable gets installed. The Packet Forwarding Engine Manager hogging logs has no functionality impact.PR1685067

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

Resolved Issues

IN THIS SECTION

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

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

General Routing

- fxpc daemon core file is generated on Junos OS EX4400 platforms in a virtual chassis setup with HGoE mode. PR1682960

Forwarding and Sampling

- The device uses the MAC address of the IRB interface even after configuring static MAC for a default gateway. PR1700073

Interfaces and Chassis

- The Unicast traffic is dropped on EX4600 Virtual Chassis. PR1695663
- Traffic loss would be observed when VRRP VIP is removed and added back as a local IP in the same IFL in a single commit. PR1687826

Layer 2 Ethernet Services

- DHCP packets might not be sent to the clients when you configure `forward-only` under the routing instance. PR1689005
- Phone-home and SZTP might fail if phone-home daemon restarts. PR1693124

Platform and Infrastructure

- Traffic drop seen and filter not hitting as expected for match condition traffic class with FLT option configured. PR1573350
- The interface on the device will go down when one or more interfaces are connected to the Advantech3260 device at another end. PR1678506
- The DHCP offer packet failed to send back to the client leaf from the server leaf. PR1698833
- On EX4300-48MP I/O devices, accesses disk fails. PR1720335
- On EX4100 devices, the MACsec interface statistics of encrypted/decrypted bytes do not increment further after reaching a 40-bit limit. PR1658584
- On EX4100 and EX4100-F Virtual chassis, the non-existing PIC ports are seen in jvision queries. PR1681673
- fxpc daemon core is observed on Junos EX4400 platforms in a Virtual chassis setup with HGoE mode. PR1682960
- EX/QFX SNMP: jnxOperatingDescr.1.1.0.0 returns blank, but jnxOperatingState.1.1.0.0 returns value. PR1683753
- The EX4100 and EX4100-F devices, on configuring console "logout-on-disconnect", password configuration via console does not work. PR1686364

- Traffic loss is observed in IP fabric when there is a change in the underlay network. PR1688323
- The FPC crash would be observed when the same CoS configuration is applied with wildcard for all the physical interfaces and aggregated Ethernet interface. PR1688455
- jdchpd core seen with dhcp-snooping persistent configuration. PR1688644
- A self-ping blackhole is seen along with fmpc process crash in a rare scenario causing traffic loss. PR1692365
- Few uplink ports of EX2300-48MP devices does not come up. PR1692579
- DHCP binding fails after dot1x authentication in EVPN-VXLAN network. PR1693967
- The l2cpd telemetry crash would be observed when the LLDP Netconf notification from external controllers along with Netconf services configuration is present on the device. PR1695057
- Traffic loss is seen when a MAC moves from dot1x port to non-dot1x port. PR1695771
- Traffic forwarding fails when deleting all L2 related configurations. PR1695847
- Adding more than 256 VLANs as name tags on the same interface results in dcd crash. PR1696428
- Transceiver not detected after it's unplugged and plugged in again. PR1696444
- Network port status LED will go off in Duplex mode. PR1696940
- Dot1x authentication failure for EVPN VXLAN enabled port. PR1697995
- Adaptive sampling will not work if the system clock is turned backward. PR1699585
- TCAM space might be exhausted when learning DHCP snooping entries on a trusted port. PR1699777
- The BFD session will remain in init/down state in the Virtual Chassis scenario. PR1701546
- The PXE BIOS recovery fails on EX9204, EX92049208, and EX92049214 Virtual Chassis setup. PR1704457
- Traffic drops observed with hierarchal overlay ECMP configuration. PR1704470
- Traffic gets silently discarded in the event of a link failure (Rx LOS) for 1GE-SX/LX optics. PR1705461
- EAP authentication might not be successful with 802.1X server-fail configuration. PR1705490
- Alarms were not generated as expected when the Management Interface Link was down. PR1706116
- Layer 3 forwarding issues for IRB. PR1706845

- The PoE firmware upgrade fails on EX4400 devices. PR1706952
- In a Virtual Chassis scenario, sometimes the alarms raised on the line-card or backup Routing Engine might not show on the primary Routing Engine. PR1707798
- QSFPs are displayed as UKNOWN after the upgrade. PR1708123
- License expire error will be observed after upgrade. PR1708794
- The link does not come up after PIC offline and online operation. PR1710793
- When a 100G transceiver is used as a VC port, the VC port will either not come up or come up as 40G. PR1711407
- A dot1xd crash is seen on EX2300 devices. PR1711422
- MACsec dynamic CAK not working due to interoperability issue. PR1711561
- On EX4650 devices, jnxOperatingDescr.1.1.0.0 is populated with blank. PR1714056
- On EX4400 devices, the Link/Activity LED is not lit when it transits to the factory default configuration by pressing the Factory Reset/Mode button. PR1714116
- Traffic loss occurs on the RTG bound interface. PR1715518
- The interface phy of PIC 0 comes up causing traffic loss while the device boots/reboots. PR1715680
- The EX4100MP (PSE) device does not allocate a power value requested in LLDP by Mist AP devices like AP12, AP32, AP33 and AP43 (PD). PR1716261
- MMAS flag does not reset after interface recovers due to l2-learning restart. PR1716270
- The link remains down on connecting the transceiver 10GBASE-T with the serial number starting with "2P1". PR1716703
- The `set forwarding-options evpn-vxlan shared-tunnels` command are not available for EX92XX devices. PR1716881
- On EX4400-2400 devices, the DHCP Security ARP statistics are not as expected after DHCP binds. PR1718286
- Factory default configuration does not have rstp enabled for uplink ports. PR1719509
- DHCP OFFER not received at the client for DHCP packets that have extra padding. PR1675316
- EX4300-48MP: :Interface operational states shows up even when interface as made down administratively. PR1701444
- PoE does not work as expected. PR1705212

- BFD flaps will be seen on EX4400 platforms. PR1707762
- Commit convergence gets delayed with a scaled VLAN setup on EX platforms. PR1710219
- Certain EX platforms with option-18 configured may hinder the DHCPv6 process. PR1710360
- On EX4400 and EX4400-24X platforms, BIOS upgrade is not getting successful via CLI. PR1715258
- The fxpc daemon crash is observed on Junos EX4400 platforms in a Virtual chassis setup with HGoE mode. PR1718316
- [EX4400]Alarm PEM is not supported/powered might be seen. PR1718825
- EX4400: Flow control shows as disabled at pfe, even after enabling it. PR1724188
- Traffic loss will be observed with vlan tagging and/or vlan normalisation in a specific design (using a looped cable). PR1724675
- On certain Junos EX and QFX platforms the static ARP entries for DHCP-security are not present. PR1724933
- EX4400: FPC temperature value is exported incorrectly as 0 in Telemtery server. PR1726532
- Programming of native-vlan-id on the interface fails and MAC is not learned. PR1727112
- EX4400 VC: During upgrade/reboot , fxpc core may be seen in a very rare race condition. PR1728725
- EX4400: Some log messages may get flooded in heavily loaded system. PR1731345
- The traffic drop will be observed after changing the VSTP VLAN configuration. PR1731522
- The fxpc process crashes when the next hop information is not properly maintained in the PFE table. PR1731548
- 25G DAC in 4x25G plugged in PIC2 does not come up when used as VC ports. PR1738535

Routing Protocols

- A crash might occur for the mcsnoopd process when the VLAN name for igmp-snooping has certain characters. PR1711153
- The mcscnoopd process will be stuck in resync state after snooping configuration is deleted and added again immediately. PR1699784

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 22.3R3 for the JRR Series. They describe new and changed features, limitations, and known and resolved problems in the hardware and software.

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

What's New

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

What's Changed

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

Known Limitations

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

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

Open Issues

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

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

Resolved Issues

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

Migration, Upgrade, and Downgrade Instructions

IN THIS SECTION

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

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

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

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

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

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

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

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

Table 3: EOL and EEOL Releases

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

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

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

Junos OS Release Notes for Juniper Secure Connect

IN THIS SECTION

These release notes accompany Junos OS Release 22.3R3 for Juniper Secure Connect. They describe new and changed features, limitations, and known and resolved problems in the hardware and software.

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

What's New

There are no new features or enhancements to existing features in Junos OS Release 22.3R3 for Juniper Secure Connect.

What's Changed

There are no changes in behavior and syntax in Junos OS Release 22.3R3 for Juniper Secure Connect.

Known Limitations

There are no known limitations in hardware and software in Junos OS 22.3R3 for Juniper Secure Connect.

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

Open Issues

There are no known issues in hardware and software in Junos OS Release 22.3R3 for Juniper Secure Connect.

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

Resolved Issues

There are no resolved issues in Junos OS Release 22.3R3 for Juniper Secure Connect.

Junos OS Release Notes for Junos Fusion for Enterprise

IN THIS SECTION

These release notes accompany Junos OS Release 22.3R3 for the Junos Fusion for enterprise. They describe new and changed features, limitations, and known and resolved problems in the hardware and software.

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

What's New

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

What's Changed

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

Known Limitations

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

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

Open Issues

There are no known issues in hardware or software in this release for Junos Fusion for enterprise.

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

Resolved Issues

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

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

Migration, Upgrade, and Downgrade Instructions

IN THIS SECTION

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

Basic Procedure for Upgrading Junos OS on an Aggregation Device

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

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

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

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

To download and install Junos OS:

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

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

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

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

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

5. Select the **Software** tab.

6. Select the software package for the release.

7. Review and accept the End User License Agreement.
8. Download the software to a local host.
9. Copy the software to the routing platform or to your internal software distribution site.
10. Install the new `junos-install` package on the aggregation device.

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

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

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

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

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

Replace *source* with one of the following values:

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

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

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

Rebooting occurs only if the upgrade is successful.

Upgrading an Aggregation Device with Redundant Routing Engines

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

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

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

Preparing the Switch for Satellite Device Conversion

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

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

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

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

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

- The switch running Junos OS can be converted only to SNOS 3.1 and later.

- Either the switch must be set to factory-default configuration by using the `request system zeroize` command, or the following command must be included in the configuration: `set chassis auto-satellite-conversion`.

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

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

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

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

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

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

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

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

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

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

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

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

Converting a Satellite Device to a Standalone Switch

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

Upgrade and Downgrade Support Policy for Junos OS Releases

We have two types of releases, EOL and EEOL:

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

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

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

Table 4: EOL and EEOL Releases

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

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

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

Downgrading Junos OS

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

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

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

Junos OS Release Notes for Junos Fusion for Provider Edge

IN THIS SECTION

These release notes accompany Junos OS Release 22.3R3 for Junos Fusion for provider edge. They describe new and changed features, limitations, and known and resolved problems in the hardware and software.

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

What's New

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

What's Changed

There are no changes in behavior and syntax in Junos OS Release 22.3R3 for Junos Fusion for Provider Edge.

Known Limitations

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

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

Open Issues

There are no known issues in hardware or software in this release for Junos Fusion for provider edge.

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

Resolved Issues

There are no resolved issues in Junos OS Release 22.3R3 for Junos Fusion for provider edge.

Migration, Upgrade, and Downgrade Instructions

IN THIS SECTION

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

Basic Procedure for Upgrading an Aggregation Device

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

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

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

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

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

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

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

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

5. Select the **Software** tab.

6. Select the software package for the release.
7. Review and accept the End User License Agreement.
8. Download the software to a local host.
9. Copy the software to the routing platform or to your internal software distribution site.
10. Install the new `jinstall` package on the aggregation device.

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

Customers in the United States and Canada, use the following commands.

- For 64-bit software:

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

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

- For 32-bit software:

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

All other customers, use the following commands.

- For 64-bit software:

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

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

- For 32-bit software:

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

Replace *source* with one of the following values:

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

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

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

Rebooting occurs only if the upgrade is successful.

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

Upgrading an Aggregation Device with Redundant Routing Engines

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

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

2. Install the new Junos OS release on the backup Routing Engine while keeping the currently running software version on the master Routing Engine.
3. After making sure that the new software version is running correctly on the backup Routing Engine, switch over to the backup Routing Engine to activate the new software.
4. Install the new software on the original master Routing Engine that is now active as the backup Routing Engine.

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

Preparing the Switch for Satellite Device Conversion

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

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

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

Customers with EX4300 switches, use the following command:

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

Customers with QFX5100 switches, use the following command:

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

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

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

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

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

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

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

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

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

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

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

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

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

Converting a Satellite Device to a Standalone Device

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

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

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

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

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

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

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

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

5. Review and accept the End User License Agreement.

6. Download the software to a local host.

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

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

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

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

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

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

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

9. Commit the configuration.

   To commit the configuration to both Routing Engines:

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

   Otherwise, commit the configuration to a single Routing Engine:

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

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

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

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

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

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

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

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

11. Wait for the reboot that accompanies the software installation to complete.
12. When you are prompted to log back into your device, uncable the device from the Junos fusion topology. See Removing a Transceiver from a QFX Series Device or Remove a Transceiver, as needed. Your device has been removed from Junos fusion.

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

Upgrading an Aggregation Device

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

Upgrade and Downgrade Support Policy for Junos OS Releases

We have two types of releases, EOL and EEOL:

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

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

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

Table 5: EOL and EEOL Releases

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

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

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

Downgrading from Junos OS Release 22.3

To downgrade from Release 22.3 to another supported release, follow the procedure for upgrading, but replace the 21.1 `jinstall` package with one that corresponds to the appropriate release.

NOTE: You cannot downgrade more than three releases.

For more information, see the Installation and Upgrade Guide.

Junos OS Release Notes for MX Series

IN THIS SECTION

These release notes accompany Junos OS Release 22.3R3 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.

General Routing

- **Verified the qualification of `ordered-by-user` in the hierarchies (ACX Series, EX Series, MX Series, QFX Series, SRX Series, vMX, and vSRX)**—The requested hierarchies are reviewed and checked to confirm if they qualify for the `ordered-by-user` list type. If they do not, the `flag autosort` is included in the DDL definition for the list, making it `ordered-by-system`. The hierarchies are now indexed. The benefits from this arrangement are we get accurate data modeling and optimized configuration load in the user interface infrastructure.

- In the past inet6flow.0 was not allowed to be a primary rib in a rib-group. Starting with Junos OS Release 22.3 this is now allowed.

- Two new alarms are added and can be seen with MPC11E when 400G-ZR optics are used. High Power Optics Too Warm: warning of the increase in chassis ambient temperature with no functional action taken on the optics Temperature too high for optics power on: New inserted optics when the chassis ambient temperature is elevated beyond the threshold will not be powered on and would need to be reinserted when the ambient temperature is within the acceptable range

Junos XML API and Scripting

- **Ability to commit `extension-service file` configuration when application file is unavailable**—When you set the `optional` option at the **edit system extension extension-service application file *file-name*** hierarchy level, the operating system can commit the configuration even if the file is not available at the **/var/db/scripts/jet** file path.

  [See file (JET).]

- **Ability to restart restart daemonized applications**—Use the `request extension-service restart-daemonize-app` *`application-name`* command to restart a daemonized application running on a Junos device. Restarting the application can assist you with debugging and troubleshooting.

  [See request extension-service restart-daemonize-app.]

- **The `xmlns:junos` attribute includes the complete software version string (ACX Series, EX Series, MX Series, PTX Series, QFX Series, SRX Series, vMX, and vSRX)**—The `xmlns:junos` namespace string in XML RPC replies includes the complete software version release number, which is identical to the version emitted by the `show version` command. In earlier releases, the `xmlns:junos` string includes only partial software version information.

Network Management and Monitoring

- **`operator` login class is restricted from viewing NETCONF trace files that are `no-world-readable` (ACX Series, EX Series, MX Series, PTX Series, QFX Series, SRX Series, vMX, and vSRX)**—When you configure NETCONF tracing options at the `[edit system services netconf traceoptions]` hierarchy level and you restrict file access to the file owner by setting or omitting the `no-world-readable` statement (the default), users assigned to the `operator` login class do not have permissions to view the trace file.

Known Limitations

IN THIS SECTION

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

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

General Routing

- In a scaled setup with LDP over RSVP configuration and maximum-ecmp as 32 or 64, line card CPU usage can remain high for extended duration on link flap operation. In this duration, LACP might take 5+ minutes to converge and the AE bundle to be active. PR1624219
- If proper gap is given between channelisation and dechannelisation the issue is not seen. Proper gap means allowing the system to complete the previous config before we load the new config.

Recommendation is to if we give channelisation config commit wait for the links to come up or atleast the ifd's get created on both evo and RE side and then only revert the config to dechannlisation and vice versa.PR1665625

- For GNMI subscriptions, PFE doesn't support filtering in Subscription paths. So data is streamed from PFE ignoring filteringPR1668911
- RE-S-X6-128G-K does not support enabling encryption with GRES. You must enable encryption on each Routing Engine.PR1676928
- On all Junos and Junos OS Evolved platforms, if OSPF (Open Shortest Path First) has segment routing with TI-LFA (Topology-Independent Loop-Free Alternate) protection enabled for gr-interfaes (Generic Routing Encapsulation tunnels), it is possible that we do not compute TI-LFA backup path when the primary or backup paths are over gr-interfaces. Not having TI-LFA backup paths effects convergence times during failures.PR1685064
- MVRP on PVLAN promiscuous port is not supported. If MVRP is configured on promiscuous port, then hosts connected to secondary VLAN ports will not be able to reach external world through promiscuous port carrying primary VLAN tags. PR1693345

Infrastructure

- When you upgrade from earlier release to Junos OS Release 21.2 and later, validation and upgrade might fail. As a workaround, use `no-validate` configuration statement before you upgrade. https://kb.juniper.net/TSB18251. PR1568757
- Below IPC timeouts logs can be seen for statistics query to kernel (queried from CLI or daemons querying internally) when there is configuration churn, or large number of IPCs getting exchanged between kernel and pfe in the system. if_pfe_msg_handler: pfe_peer_msg_handler error: error for msg type type, msg subtype subtype, opcode op and peer index index Default IPC timeout value in kernel for IPC statistics request is 10s. This can be incremented to larger value by setting below hidden configuration to avoid IPC timeout errors. `set system stats-timeout-lifetime 15` and `commit`. PR1629930

MPLS

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

Platform and Infrastructure

- In some scenarios with MPC, major alarm and following messages are generated. This major error is triggered due to parity error, and the impacted queue might drop packets. This might impact the forwarding, to recover MPC card need to be rebooted. PR1303489
- On MX Series and EX9200 Series platforms, under Ethernet VPN (EVPN) environment, packets routed using IRB interface could not be fragmented due to media maximum transmission unit (MTU) problem. PR1522896
- After a switchover event, when ppmd calls sendmsg system call to transmit the protocol packets, it gets blocked long enough that a few sendmsg calls cumulatively take up around 7 to 8 seconds. This indirectly impacts the BFD session because the BFD session has a Routing Engine-based detect time of 7.5 seconds to expire. PR1600684

Routing Protocols

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

Services Applications

- In Junos OS Release 17.4 and forward, subscriber sessions on the LNS that send an ICRQ that includes RFC5515 AVPs might fail to establish a session. The client will receive a CDN error "receive-icrq-avp-missing-random-vector" in response. PR1493289

User Interface and Configuration

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

Open Issues

IN THIS SECTION

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

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

EVPN

- 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 because MAC is not learned on the remote PE device, but learned on the A/A local PE device. The non-designated forwarder sends the IM-labeled encapsulated packet to the PE-CE interface after MAC lookup instead of dropping the packet. This creates duplicate packets on the CE side. PR1245316

- On all Junos OS platforms, Address Resolution Protocol (re-ARP) on multihoming (MH) device fails in the EVPN-MPLS multihoming scenario resulting in traffic drop. This triggers the MAC-IP route deletion and addition. PR1691132

Forwarding and Sampling

- On all EX9200 and MX Series platforms having MPC10, MPC11 and LC9600 cards, traffic is leaking through a scale filter configuration change. PR1715504

General Routing

- Compact Forwarding Engine Board (AFEB) crashes with Precision Time Protocol (PTP) thread hog on the device. As a workaround, enable PTP to process the PTP packet when PTP configuration is active. If PTP configuration does not exist, ignore the PTP packet processing even if the field-programmable gate array (FPGA) shows the available PTP packet. This 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 corrupts, the system boots with the alternate disk that helps the user to 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
- When you install the MIC-3D-8OC3-2OC12-ATM and configure ATM interface, FPC might crash on MX240 and MX2020 routers. Packet Forwarding Engine might also crash on MX104 routers for the same. PR1453893
- Error messages "TALUS(number) PCIe(number) DMA RX interrupt received. Queue stuck status 0xeeeeee0" are triggered in system logs due to queue-back pressure or FPGA drop. PR1465888
- When hardware link errors occur on all 32 links on an FPC11, all FPCs reports destination errors towards FPC11 and FPC11 are taken offline with reason "offlined due to unreachable destinations". PR1483529
- When secondary Routing Engine stops, CB1 goes offline and comes back online. This reboots the secondary Routing Engine because of the "0x1:power cycle/failure". There is no other functional impact. PR1497592

- AMS bundle state toggles mometorily from up, down, or up after configuration commit for scaled scenario. PR1521929
- In MAC-OS platforms when Juniper Secure Connect client connects successfully, the client is not getting minimized to tray icon and needs to be minimized manually.PR1525889
- 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 primary and secondary Routing Engine will help recover and get router back into stable state. PR1539305
- With IPsec PMI or fat-core enabled, `show services sessions utilization` CLI do not display right CPU utilization. PR1557751
- The Sync-E to PTP transient simulated by Calnex Paragon Test equipment is not real network scenario. In real network deployment model typically there will be two Sync-E sources (primary and secondary) and switchover occurs from one source to another source. MPCE7 passes real network SyncE switchover and associated transient mask. PR1557999
- VE and CE mesh groups are default mesh groups created for a given routing instance. On adding VLAN or bridge domain, 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 might not be a major issue. PR1560588
- To avoid the additional interface flap, interface hold time needs to be configured . PR1562857
- This issue is caused by /8 pool with block size as 1, when the configuration is committed the block creation utilizes more memory causing NAT pool memory shortage that is currently being notified to customer with syslog tagged RT_NAT_POOL_MEMORY_SHORTAGE. PR1579627
- On MX Series routers the Juniper Device Manager (JDM) server is not created in in-chassis mode of Junos node slicing, which results in mgd process crash and affects guest network function (GNF) provisioning. PR1583324
- When the active secondary interface deactivates, the PTP lock status is set to 'INITIALIZING' state in `show ptp lock-status` output for few seconds before BMCA chooses the next best slave interface. This is the day-1 behavior and there is no functional impact. PR1585529
- On all devices running Junos OS Release 19.1R3-S5-J3, the subscriber logical interface might get stuck after the Extensible Subscriber Services Manager (ESSM) deletion. PR1591603
- PIM VxLAN is not working on TD3 chipsets enabling VxLAN flexflow after Junos OS Release 21.3R1. Customers Pim VxLAN or data plane VxLAN can use the Junos OS Release 21.3R1. PR1597276
- MX2010, MX2020: MPC11E: ISSU is not supported for software upgrades from 21.2 to 21.3 and 21.4 releases due to a flag day change PR1597728

- During Routing Engine switchover, if there is a burst of ICMP, BFD, SSH, FTP, TELNET, and RSVP packets (~18K pps), a new secondary Routing Engine might restart. PR1604299
- On MX Series Virtual Chassis platforms with MS-MPC or SPC3 service cards and aggregated multi-service (AMS), traffic on the line card in the seconday chassis may not be load-balanced properly due to timing conditions. This works well on the line card in the master chassis. There might be a traffic loss when interfaces are not properly balanced. PR1605284
- On all MX Series routers, in a subscriber management environment, new subscribers might not connect if class of service (CoS) classifier rewrite (CR) features are used by the variable based flow (VBF) service. The reference count mismatching between Routing Engine and VBF is caused by VBF flow VAR CHANGE failure. PR1607056
- When user tries to disable AMS physical interface using configuration statement, the IPsec tunnels are not deleted. Deactivating the services will provide the desired result. PR1613432
- Percentage physical-interface policer is not working on aggregated Ethernet, after switching between baseline configuration to policer configuration. PR1621998
- On all Junos OS platforms the MAC address of the 17th aggregated Ethernet interface might be changed after the upgrading from Junos OS Release 18.4 to Junos OS Release 20.4 and later. It will lead to MAC based service interruption. PR1629050
- For a topology with VSTP and VRRP configured and IPv6 traffic, if VSTP bridge priority is changed a couple of times (to trigger toggling of root bridge), it is possible that V6 traffic drop is seen on some of the streams. PR1629345
- For ACX5448, MX204 and MX2008 "VM Host-based" platforms, starting with Junos 21.4R1 or later, ssh and root login is required for copying line card image (chspmb.elf for MX2008) from Junos VM to Linux host during installation. The ssh and root login are required during installation. Use "deny-password" instead of "deny" as default root-login option under ssh configuration to allow internal trusted communication. For more information refer to TSB18224. PR1629943
- On MX Series routers with enhanced subscriber management enabled, when `host-prefix-only` is configured on the underlying-interface for subscribers, it might not work in FPC. PR1631646
- The fabric statistics counters are not displayed in the output of `show snmp mib walk ascii jnxFabricMib`. PR1634372
- On all devices running Junos OS or Junos OS Evolved, where this is a high BGP scale with flapping route and the BGP Monitoring Protocol (BMP) collector or station is slow, the rpd process might crash due to memory pressure. PR1635143
- Source MAC must not be configured on the underlying static interface on the UP for PPPoE login to work correctly. PR1641495

- WIth precision time protocol (PTP) over IPv6 on MPC2E 3D EQ, secondary PTP stays in the acquiring state. PR1642890
- When CFP2-DCO is used, operator need to configure `otn-option` which is the only supported mode. PR1643815
- On MX10004, MX10008, and MX10016 routers, oamd process is not started and GRE keepalives adjacency is down. PR1644480
- Committing configuration changes during the Packet Forwarding Engine reset pause window (when Packet Forwarding Engine is disabled, yet the `pfe reset proper` has not started) has the potential of causing errors and traffic loss. In particular, the configuration changes that result in re-allocating policers (which are HMC-based) might lead to traffic being entirely policed out (I.e. not flowing). Once the PFE reset procedure has started configuration changes ought to be avoided until the procedure is complete. PR1644661
- bb device has to be manually enabled in configuration for DHCP and PPP access models for BNG CUPS. The configuration to enable bb device is `set system subscriber-management mode force-broadband-device`. PR1645075
- In the IPv6 segment routing deployment, packets are sent out with incorrect ethernet type. PR1647622
- PTP Playback Engine reset error is reported sporadically with PTP FPGA firmware version A4 7 with no functionality impact. PR1652275
- The core file is generated intermittently where random grpc stack crash is observed. The license service will auto restart and recover. PR1656975
- 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` configuration results in the packet dropped at egress PE for multiple MPLS stack labels. PR1658406
- The OpenSSL project has published security advisories for multiple vulnerabilities resolved in OpenSSL. For more information efer to JSA70186. PR1661450
- The version details for certain daemons will appear in the command output after the device has been rebooted after the completion of the USB installation of Junos OS.PR1662691
- user should not modify the locator attributes, instead locator, SIDs should be deleted and configured back. Otherwise it will lead to coredump.PR1667320
- For GNMI subscriptions, Packet Forwarding Engine doesn't support filtering in subscription paths. So data is streamed from Packet Forwarding Engine ignoring filtering. PR1668911

- On MX platforms with MIC-MACSEC-20GE, FEB(Forwarding Engine Board) may go down while activating/deactivating GRES(G?raceful Routing Engine Switchover) configuration.PR1668983
- License-check core is being dumped upon reloading the system after applying specific set of configs. Once the system comes up, everything runs fine and no issue is seen.PR1671419
- In the case of an Active-Active lease query stale-timer config is mandatory. This is required to optimize the sync time, as both peers get the solicit packets at the same time. Knob: set forwarding-options dhcp-relay stale-timer 20 The above knob is required to resolve this issue and it needs documentation. PR1671589
- On SyncE over LAG interfaces, if the end points have different ESMC QL configured, on one of configured syncE interface, ESMC QL is toggling between PRC and DNU and sync-E does not lock and moves to holdover state. PRC packets are received with MAC address of the upstream master. These packets are not dropped based on the link-local MAC address. Based on PLM recommendation inspired by the customer requirements and MEF 6.1.1 EPL Option 2 service (an excerpt below, taken from here https://www.mef.net/wp-content/uploads/2012/01/MEF-6-1-1.pdf) So, by default we are Option #2 compliant, if someone needs Option #1 behavior, a filter can be configured to match and discard. PR1677131
- On LC480 MX line-card with 1G interface 1PPS time error does not meet class B requirement (maximum absolute time error is 70 ns).PR1677471
- The IFD remaining stats flag is not set properly in chassid in today's code. It should be set to TRUE only if HCOS is configured on an interface. Else, it should not be SET. Not setting this rightly, results in statistics not being displayed OR the command output not being displayed at all. The impacted command is "run show interfaces extensive intf-name" and the impact is seen in GNF environment with no explicit COS configuration on the interfaces. Not using "extensive" will ensure there is no issue as well. This is specific to MPC11 with sub LC (GNF) setup.PR1678071
- There will be drop of syslog packets seen for RT_FLOW: RT_FLOW_SESSION_CREATE_USF logs until this is fixed. This will not impact the functionality.PR1678453
- The issue here is that we see ?MQSS(0): DRD: Error: WAN reorder ID timeout error? once per PFE during bootup of FPC. This happens because during the FPC bootup some control packet from vmhost comes before the PFE init is fully complete. Because of this the EA Asic is not able to process the packet and throwing the error. The fix involves complex changes in the bootup sequence of ASICS and will result in other major issues. The original issue has no functionality impact. It is just one error per PFE seen during the FPC reload case only. At that time the traffic is not started yet and once the system is up no other impact is seen due to the Error. Hence the issue will not be fixed. Any "WAN reorder ID timeout error" during the bootup of FPC can be safely ignored.PR1681763
- PR1683656
- 100GE interface on JNP-MIC1 TIC module may keep flapping for 1 ~ 45 minutes after a specific 3rd party peer device (NRU02 from Arista/Pluribus) is booting up. PR1686012

- On Junos MX platforms with MPC1-9E line cards, when PFE (Packet Forwarding Engine) is disabled, scenarios like multicast receiver join/leave that result in allocation and de-allocation of memory in PFE can cause a memory leak issue. This is because memory is allocated on the disabled PFE, but not freed.PR1686068

- If MVRP is enabled on an MSTP enabled interface, the interface will be made part of all the existing instances on the switch, So, if there are two interfaces between R1 and R2 as below: R1(et-0/0/1 and et-0/0/2)======(et-0/0/1 and et-0/0/2)R2 And one interface is MVRP enabled (say et-0/0/1), and et-0/0/2 is not MVRP enabled. By configuration et-0/0/1 is part of MSTI-1 and et-0/0/2 is part of MSTI-2. MSTI-1 is running on vlan-100 and MSTI-2 is running on Vlan-200. R2 in this case, is advertising only vlan-100. The MVRP enabled interface will become part of all the MSTIs(MSTI-1 and MSTI-2 both) configured on the device and it will take part in the FSM of all the MSTIs. Although et-0/0/1 is not member interface of vlan-200(correspnding to MSTI-2). This potentially can cause a problem where et-0/0/1 although not a vlan-200 member, will go into FWD state and et-0/0/2, genuine member of vlan-200 goes into BLK state for MSTI-2. So, when traffic is received in vlan-200 it will be sent out of et-0/0/1, an it will be dropped.PR1686596

- For leaves of data type ieeefloat32, the value will be encoded in bytes while being streamed to collector. The value contained in such leaves may not be completely accurate.PR1690598

- RPD process crash might be seen when the gRPC stack expects a 8 byte aligned memory but gets a 4 byte aligned memory instead. PR1692738

- The BUM (Broadcast, Unknown Unicast, and Multicast) packets are getting dropped at egress processing on all MX platforms due to an interoperability issue of MPC1/MPC2/MPC3/MPC4/MPC5/MPC6/MPC7/MPC8/MPC9 with MPC10/MPC11/LC9600 line card. It is observed when equal-cost multipath (ECMP) is enabled for the load-sharing data for an incoming traffic destined to the neighbours. It can be seen with any ECMP traffic distribution configuration.PR1695438

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

- On Junos OS Evolved Platforms, any UI (user interface) set (configuration, script, license) changes done post software addition were being lost after the subsequent reboot.PR1699699

- When packets of size bigger than 1518 Bytes are received/transmitted, pps counter value does not show correct value. PR1700309

- On MX Series platforms, traffic egressing on the IRB (Integrated Routing and Bridging) interface with the underlying L2 (layer2) access port has VLAN tags imposed incorrectly.PR1700321

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

- When subscribing to sensor paths "/junos/system/linecard/packet/usage/", "/junos/services/label-switched-path/usage/" or other line card (PFE) sensor paths in gNMI subscription mode, packet

drops may be seen in the CLI command "show network-agent statistics gnmi detail" output. The collector output may also contain missing sequence numbers. For example, the sequence number output may be 0, 3, 6, 9, 12, etc. instead of 0, 1, 2, 3, 4, etc. PR1703418

- In chassisd, Junos Telemetry interface thread takes more time in streaming of Junos Telemetry interface packets because of volume of data and number of sensors involved with this daemon. Jvision thread engaged for more time to process streaming events caused Chassisd master thread to lose receive/send keepalive messages to/from other RE, which eventually was causing automatic RE switchover in most of the cases. To avoid this, fix done for exporting small payload jvision packets (formation of which takes less time) and deferring jvision thread more in an interval, to allow chassisd master thread to process high-priority hello/keep-alive messages. This means now, more number of packets is sent in one reporting interval and with larger spread (earlier same amount of data was sent with 2 or 3 packets of higher payload size, and 100ms of deferring time for jvision thread. This behaviour is increasing KPI-2 but lowering KPI-1 (payload size). It is not possible to back out changes done to solve keep-alive message loss issue. Hence we will have to keep Chassisd as an exception, when we measure/report KPI-2 values. Jvision in Chassisd has to give more priority/time to process keep-alive messages than sending of jvision packets. Hence delay between jvision packets are more.PR1706300

- On the MX104 platform, the Wrong threshold-temperature is displayed.PR1713788

- On all Junos and Junos OS Evolved platforms, due to a bug in route resolution over specific types of next hops, the route can resolve over itself and the nexthop chain keeps expanding. Due to this issue, the depth of recursion gets higher than supported and the KRT (Kernel Routing table) queue returns errors for nexthops. As a result, there will be incorrect route resolution, traffic loss and occasionally, the rpd (routing protocol deamon) crashes. The necessary configurations and conditions that will result in this issue are below 1. BGP (Border Gateway Protocol) Prefix-Independent Convergence (PIC) ("protect core") is configured and BGP receives same prefix from EBGP and IBGP neighbors 2. BGP LU (Labeled Unicast) with "protection" to create backup path to protect the active and BGP receives same prefix from EBGP and IBGP neighbors 3. Mutually recursive Route resolvability situations like Resolving using Default-route (not having proper resolution config)PR1716436

- When NAT (Network Address Translation) is configured on interfaces along with sampling, the J-flow record will contain NAT'ed IP as opposed to the original IP.PR1716707

- The `fast-lookup-filter` is not working on the router's loopback interface with MX10008 line cards in the routers. PR1718893

- After deactivating an -lt interface with units that have CoS the interface cannot be reactivated. PR1722327

- Once the device is loaded with the new image, PIC tries to boot up. mspmand is one of the processes inside PIC, crashes sometimes.PR1727487

- Service disruptions are seen due to a consistent increase in l2ald (Layer 2 Address Learning Daemon) memory usage.PR1727954
- MX304 Major Alarm " Host 0 detected AER correctable error" after RE switchover.PR1731237

High Availability (HA) and Resiliency

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

Infrastructure

- Earlier implementation of kvmclock with virtual dynamic shared object (vDSO) helps avoid the system call overhead for user space applications had problem of time drift. The latest set of changes takes care of initializing the clock after all auxiliary processors launched. Thus, resulting in accurate clock initialization. PR1691036

Interfaces and Chassis

- Logical interface packet counters are not implemented for AMS interface. It is a new change. Changes are planned for the Junos OS Release 22.4R2 and later. PR1673337
- Error logs related to invalid anchor next hops are seen when the MPC10 and MPC11 FPCs are restarted with distributed aggregated Ethernet IRB VRRP sessions. The aggregated Ethernet must span multiple FPCs. PR1674069
- Interface_check_up verification is not as expected on primary member of MX-VC setup. PR1686425
- On all Junos OS platforms, while performing the Junos upgrade from the release before 20.4 to a higher version having an incorrect configuration may fail. This issue may lead to traffic loss or network outages.PR1692404
- On Junos OS platforms with MPC line cards, negotiated interfaces will try to come up with the speed already negotiated instead of using the original interfaces speed even if re-negotiation happens like reinserting cable.PR1714267

Junos XML API and Scripting

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

Layer 2 Features

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

MPLS

- In MVPN Case, if the nexthop index of a group is not same between primary and secondary after a nsr switchover, we may see a packet loss of 250 to 400 ms. PR1561287
- ingress will retry after lsp stay down for extended period of time or customer can clear lsp to speed up the retry PR1631774
- On all Junos OS and Junos OS Evolved platforms, if Circuit Cross-Connect (CCC) is configured to use a label-switched-path such as IGP routed, i.e., no-cspf and no strict explicit route object (ERO) configuration, then restarting egress CCC node or restarting FPC on the egress CCC node containing remote-interface-switch configuration multiple times might cause CCC to remain stuck in remote-if-down state, resulting in loss of traffic. (The configuration statement `remote-interface-switch` is configured on the egress LER of the Resource Reservation Protocol-Traffic Engineering label-switched-path (RSVP-TE LSP) which binds the LSP terminating on the node to a local interface.)PR1694777

Network Management and Monitoring

- When you configure `maximum-password-length` and you try to configure password whose length exceeds the configured maximum-password-length, error is thrown, along with error 'ok' tag. (Ideally 'ok' tag should not be emitted in an error scenario.) The configuration will not get committed.PR1585855
- In some NAPT44 and NAT64 scenarios, duplicate SESSION_CLOSE syslog is seen. PR1614358

Platform and Infrastructure

- On all Junos OS and Junos OS Evolved platforms, while using source-address NTP configuration parameter and issue the command `set ntp date` from the CLI, packets will be sent with the source address of the outgoing interface rather than the manually configured IP address. Typically, the manually configured IP address would be a loopback address. The problem does not apply to automatically generated NTP poll packets. PR1545022
- When the `deactivate services rpm` and `deactivate routing-options rpm-tracking` CLIs are applied together and then committed, some of the rpm tracked added routes are not deleted from the routing table. PR1597190
- On all Junos OS platforms, if the interface configuration is altered to switch from one routing instance to another, it might result in closing of BGP session on the secondary Routing Engine.PR1700438
- On Junos OS MX Series platforms, when Virtual Router Redundancy Protocol (VRRP) packets come from the LAG interface with delegate-processing enabled, it should be processed on anchor PFE. If it comes from non-anchor PFE - it goes to anchor PFE through the fabric. In that case, TTL is decremented. If a FW filter on the loopback interface is applied for VRRP with a ttl=255 condition, the VRRP won't work - there will be a service impact.PR1701874
- On Junos OS MX Series and EX9200 devices with specific line cards, VLAN rewrites will not happen for traffic egressing from integrated routing and bridging (IRB) interface over an L2 aggregated Ethernet logical interface, if the L2 aggregated Ethernet is configured to perform VLAN rewrites on the frames. This happens when the IRB is configured as a routing-interface on Ethernet Virtual Private LAN (EVPN) or Virtual Extensible LAN (VXLAN) routing instances and the traffic has to egress on IRB over an L2 aggregated Ethernet logical interface. As a result, the frames are forwarded with incorrect VLAN tag information.PR1720772
- Irrespective of ingress forwarding class configured and marked, all the TWAMP reflected packets are sent over the Q3(Network control). PR1722232
- On all MX Series platforms, qualified-bum-pruning-mode completely blackholes VPLS (Virtual Private LAN Service) traffic with network-services configured in enhanced-ip mode.PR1731564
- Heap memory leak on access MPCs used for subscriber termination may be observed in a subscriber-management environment.PR1732690

Routing Policy and Firewall Filters

- Delete single prefix from prefix-list will cause all the prefixes to be deleted.PR1691218

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 routers, unexpected log message appears if the CLI command `show version detail` or `request support information` is executed. user@host> show version detail *** messages *** Oct 12 12:11:48.406 re0 mcsnoopd: INFO: krt mode is 1 Oct 12 12:11:48.406 re0 mcsnoopd: JUNOS SYNC private vectors set. PR1315429

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

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

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

- Any platform with micro BFD configured on member links of the LAG or aggregated Ethernet interface, BFD session state in the Routing Engine remain UP always even if the PEER device is ceased. PR1675921

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

- Junos OS Release 22.3 onwards, IS-IS yang is uplifted to 1.0.0 version which has major change in existing OC path that was supported earlier. The OC path change need to be reflected in translation script which is not done. As part of D27 release for cloud, translation script will be modified with newer OC path. Till then supported older OC configuration is broken. eventually D27 code will come back to DCB and things will work fine after that. PR1686751
- OSPF route type extended community cannot be configured as 'rte-type'. PR1687273
- Secondary path is not found in ASBR6 MPLS table while verifying BGP multipath protection functionality. PR1691131
- On all Junos OS and Junos OS Evolved platforms, you might see the BGP scheduler slip while deleting a large set of prefixes. PR1696870
- On all Junos OS and Junos Evolved platforms, when IPv4 prefix advertisement received by an IS-IS/OSPF router in the Extended IP reachability TLV and SR mapping server (SRMS) advertisement for the same prefix received through the segment identifier (SID) label Binding TLV, then SRMS advertised label preferred over IS-IS/OSPF SID label advertised via opaque-AS Extended-Prefix. Traffic will be sent via wrong path due to this issue.PR1702456
- Show route advertising-protocol bgp reporting next hop self rather than IP in the configured policy-statement for next-hop. Behavior change observed after upgrading Junos OS Release 18.4 to Junos OS Release 20.4. PR1712527
- On all Junos OS and Junos OS Evolved platforms with TI-LFA (Topology-Independent Loop-Free Alternate) feature enabled, when IP address is removed from one interface and is assigned to another interface in the same commit, the rpd process crashes affecting routing control plane. PR1723172
- On all Junos OS and Junos OS Evolved platforms, if the proxy BGP (Border Gateway Protocol) route reflector is connected to the only peer present in the BGP group then it stops advertising the routes coming from the remote cluster and that leads to proxy route-target routes not getting added which causes traffic disruption.PR1728604

Services Applications

- When a configured tunnel interface is changed to another one, flow-tap-lite functionality stops working i.e, packets don't get mirrored to content destination. PR1660588

VPNs

- Tunnel debugging configuration is not synchronized to the backup node. It needs to be configured again after RG0 failover. PR1450393
- Change here is basically reverting to old enum value used for ATM VPN, and using a new value for BGP multicast address family, and although there is no visible behavior change due to this, there may be impact on ISSU for ATMVPN and BGP multicast address family if enabled.PR1590331
- When using group VPN, in certain cases, the PUSH ACK message from the group member to the group key server may be lost. The group member can still send rekey requests for the TEK SAs before the hard lifetime expiry. Only if the key server sends any new PUSH messages to the group members, those updates are not be received by the group member since the key server might have removed the member from registered members list. PR1608290
- The rpd crashes when multicast virtual private network (MVPN) is configured with separate route-targets scenario. PR1700345
- The pseudowire interfaces are not showing up after performing Routing Engine switchover on all Junos OS and Junos OS Evolved platforms. PR1708572

Resolved Issues

IN THIS SECTION

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

General Routing

- Continuous deactivate or activate of security config can lead to process restart. PR1566044
- On backup RE during GRES, you may see "RPD_KRT_KERNEL_BAD_ROUTE: krt unsolic client.128.0.0.5+62000: lost ifl 0 for route" warning messages. PR1612487
- Delegated BFD sessions configured on routing-instance may fail to come up. PR1633395
- SR-stats : Per-Interface egress and per-sid Egress sensor stats do not take MPLS label length into account in the output octet calculations. PR1646799
- NAT session reverse traffic fails due to NAT routes getting deleted from routing instance. PR1646822
- The user-defined speed does not take effect on the AE interface in certain scenarios on Junos OS platforms. PR1649958
- Images older than 22.2R1S2 can be installed on RE-S-X6-128G-K. This will result in system booting to Linux prompt. PR1655935
- Change in few fields of IKE_VPN_UP_ALARM_USER and IKE_VPN_DOWN_ALARM_USER syslogs of IKED PR1657704
- EX4100 MACsec interface statistics of encrypted/decrypted bytes do not increment further after reaching a 40-bit limit (1099511627775). PR1658584

- SSH non-default port configuration causes FPC offline after an upgrade to 21.4. PR1660446
- family bridge disappeared on commit check when Network-services lan has been configured. PR1661057
- GNF : No streaming data received for /telemetry-system/subscriptions/dynamic-subscriptions/. PR1661106
- MPC11E temperature alarms with 400G-ZR optics. PR1663175
- The RSVP interfaces are not streamed when removing the interface configuration. PR1667844
- New BFD sessions will not come up on ACX5448/ACX710 due to continuous flaps PR1670684
- MX304:: Observed spmbpfe core on RE1 when installed image on both the Routing Engines. PR1675268
- 40G-QSFP+ flapping on MX204. PR1676005
- PTP state moves from PA ---> ACQ state. PR1676269
- Bgp peers status is not as expected. PR1677624
- Traffic loss is seen with port-mirroring is enabled on AE interface in multicast downstream. PR1683192
- EX/QFX SNMP: jnxOperatingDescr.1.1.0.0 returns blank, but jnxOperatingState.1.1.0.0 returns value. PR1683753
- [MAP-E] PPE errors seen during deactivate/activate of partial reassembly - ZTCHIP_MQSS_CMERROR_DRD_RORD_ENG_INT_REG_CMD_FSM_STATE_ERR (0x227fa5). PR1683845
- license-check might generate core file on MX Series routers. PR1685433
- New CLI commands addition to support Routing Engine and Chassis power-cycle. PR1686577
- Subscribers are not able to connect to the device after the device reboot. PR1686654
- The pre-installed optional packages and JSUs will be lost after a VMHost rollback. PR1686825
- The FPC crash would be observed when the same CoS configuration is applied with wildcard for all the physical interfaces and aggregated Ethernet. PR1688455
- Packet Forwarding Engine wedge will be seen due to fast link flaps. PR1688972
- Integration of RCP binary into the LTS19 code for Vmhost platforms. PR1689100

- The firewall bridge filter policers (attached to aggregated Ethernet interface) are not working on all Junos OS MX Series platform with MPC10 card upon deactivate-activate a term intended to limit overall traffic PR1692070
- A self-ping silently drops and discards the packet when fmpc process crashes in a rare scenario causing traffic loss. PR1692365
- The fxpc core file is generated and an FPC restart results in traffic impact. PR1692993
- PDT: ONDATRA: context deadline exceeded observed on while adding NH, IPv4. PR1693567
- The fabspoked-pfe process crashes when a FATAL ERROR occurs in the PFE. PR1693697
- dot1xd.core-tarball.0.tgz is observed in 22.1R3 at #0x009113f0 in __mem_assert(). PR1694129
- The l2cpd telemetry crashes when the LLDP netconf notification from external controllers along with Netconf services configuration is present on the device. PR1695057
- Traffic loss is seen when a MAC moves from dot1x port to non-dot1x port. PR1695771
- Adding more than 256 VLANs as name tags on the same interface results in dcd crash. PR1696428
- Transceiver not detected after it's unplugged and plugged in again. PR1696444
- After a chassis power cycle the backup Routing Engine is in present state and the "Loss of communication with backup Routing Engine" alarm is seen. PR1696816
- In the rare scenario, huge PTP time errors are introduced and propagated to the downstream devices after the chassis reboot. PR1696957
- Time error observed on JNP10K-LC2101. PR1697167
- The agentd process crash might crash in a telemetry scenario. PR1697986
- Dot1x authentication failure for EVPN VXLAN enabled port. PR1697995
- Junos OS and Junos OS Evolved: A BGP session will flap upon receipt of a specific, optional transitive attribute in version 22.3R1 (CVE-2022-22184). PR1698446
- The mpls routing table resolving over IPv6 prefix causes traffic drop. PR1698516
- The kernel crash can be seen in the VPLS scenario. PR1698781
- Transit tunnels fails and remains down on all Junos OS based MX Series and SRX Series platform with IKE-NAT-ALG enabled. PR1699115
- Output of "show chassis ethernet-switch statistics" includes 32 bit values which may overflow PR1699136

- The rpd crash is observed when rib-sharding configured. PR1699557
- Traffic loss is seen due to interface flap when changing speed from 10G and 1G. PR1701183
- On Junos platforms with MS-MPC cards the IKE ALG inactivity timeout value stays fixed. PR1701305
- Some PPPoE subscriber connection lost during Routing Engine switchover. PR1701739
- Leaf to leaf traffic flow is observed on Junos ACX5448 platform with EVPN E-Tree configuration. PR1702615
- License will be deleted due to multiple FPC reboot or switchover on QFX Series or MX Series VC scenario. PR1703200
- The l2ld process will crash when an logical interface is changed to trunk mode and a new VLAN is added. PR1703226
- The line card abruptly reboots when ISSU is performed. PR1703910
- Routing Engine will crash when static route duplicates with an interface IP address. PR1703940
- The next-hop is shown as unicast instead of reject even when the IPv6 neighbor is unreachable. PR1704114
- A transit PTP packet is modified when passing through an MPC5E and MPC6G line card 100G ports part of PTP boundary/ordinary clock configuration PR1704606
- Traffic silently drops and get discarded in the event of a link failure (Rx LOS) for 1GE-SX/LX optics. PR1705461
- EAP authentication might not be successful with 802.1X server-fail configuration. PR1705490
- No network reachability when enabling the routing-service knob for PPPoE subscribers over AE. PR1706446
- VMX :: JUNOS-REG: VMX: PFE syslog tags are missing for the command help syslog "^PFE_?". PR1707504
- QSFPs are displayed as UKNOWN after the upgrade. PR1708123
- The inline flow monitoring is not working on Junos MX-VC platforms. PR1708485
- Polling of jnxSubscriberPicCountTable and jnxSubscriberSlotCountTable MIBs is broken if any subscribers are terminated over ps interface. PR1709029
- The telemetry sensor will not be created for PCE initiated SRTE. PR1709557
- Ports with QSA adapter are down PR1709817

- AIGP not distinguished with BGP-LU when rib-sharding is enabled. PR1710829
- The FPC will be offline after upgrading the system. PR1710855
- gNMI line card (PFE) sensor /junos/system/linecard/packet/usage/ may have packet drops (gNMI translator lookup failures). PR1711779
- The interface does not come up or keeps flapping. PR1712007
- FPC memory leak will cause FPC crash. PR1712076
- PCT : Show Ephemeral-Configuration Instance Junos-Analytics is not giving expected output while verifying the commit operation with new configuration hierarchy openconfig-telemetry:telemetry-system. PR1712409
- [MPC10E] If both Macsec IFL and Macsec IFD coexist on the channelized interface, enabling macsec on the Channelized IFD impacts the Macsec Traffic on other channelized IFL interface with in the same port and vice versa. PR1712554
- The traffic is dropped while passing through VCP link on MX Series Virtual Chassis with MPC10 line card. PR1712790
- The rpd process will crash when BMP is configured. PR1713444
- The member interface will not be added to the AE bundle if the link-speed of the AE interface doesn't match that of the member. PR1713699
- Unexpected load balancing of packets having GRE header. PR1713958
- Traffic loss is seen on telemetry streaming in BGP sharding environment. PR1714087
- PPPoE and DHCP subscriber connection on dynamic VLAN can fail on Junos OS MX Series platforms. PR1714778
- JDI-REG: [MX480][MX2010]: IPSEC:: IPSEC Tunnels are not coming up after configuring IPSEC under Service-sets. PR1715071
- The bbe-smgd process is seen to crash if a large scale PWHT configuration is present. PR1715410
- Known multicast traffic is not forwarded when MLD snooping is enabled. PR1715429
- Traffic loss is seen on RTG bound interface. PR1715518
- The link remains down on connecting the transceiver 10GBASE-T with the serial number starting with "2P1". PR1716703
- A 10G port on a MPC2E or MPC3E 4x10G MIC can randomly flap constantly every few seconds. PR1716766

- set forwarding-options evpn-vxlan shared-tunnels command will not be available for EX9200 and MX Series platforms. PR1716881
- SNMP MIB OID output shows incorrect temperature value when the device is running under negative temperature. PR1717105
- Traffic loop is seen due to incorrect root bridge ID. PR1717267
- In a DHCP ALQ subscriber scenario delete-binding-on-renegotiation configuration statement does not work as expected due to a synchronization error between the primary and the backup routers. PR1718342
- The PPTP connection itself will not work when you try to establish PPTP connection along with DSLITE. PR1718840
- Observing Major Host 1 Chassis Manager connection down Alarm. PR1719767
- Convergence delay is seen when FPC is offlined under heavy traffic and scaled scenario. PR1719956
- The rpd process crash will be observed while creating or updating the PCEP tunnel. PR1720031
- The dcpfe process crash will be observed in the EVPN-VXLAN multihoming scenario. PR1721322
- BFD session failed when configured on the loopback sub interface. PR1721714
- PTSP subscribers are stuck in 'configured' state. PR1726136
- Enabling disk smart-check utility on the routing-engine with Innodisk SSD raises a false positive smart error. PR1726252
- Traffic drops with percent policer attached using list. PR1726733
- FPC will crash when the ASIC usage is high. PR1727427
- Traffic drops when MX Series platforms are configured with PCP and DS-lite. PR1729801

Application Layer Gateways (ALGs)

- The PPTP connection is not stable and is lost in DS-Lite+ALG scenario. PR1715315

Authentication and Access Control

- Connection fails are observed on Junos despite a valid auth entry. PR1692398

Class of Service (CoS)

- While attaching TCP which has only scheduler-map to IFL , no commit error thrown. PR1688790
- Control packets would be dropped when CoS configuration under AE wildcard IFLs gets applied to aggregated Ethernet control logical interfaces as well. PR1702836
- The cosd process crash might be seen on all Junos OS platforms. PR1719028

EVPN

- PBB-EVPN PE cannot learn remote CE MAC address due to ARP suppression enabled. PR1529940
- Layer3 inter-subnet routing will fail if there is no reachability for the remote IP-host route. PR1669585
- The rpd crash would be observed when activating or deactivating the EVPN routing-instances. PR1673157
- RPD (Routing Protocol Daemon) core is observed due to remote bgp routes being flashed as active routes. PR1692249
- Traffic loss is seen when IPv6 entries are not refreshed and age out under the EVPN-VXLAN scenario. PR1699509
- Traffic drop would be observed due to the VTEP tunnels not being established in the EVPN-VxLAN scenario. PR1700196
- A config change caused a rpd core dump for the EVPN migrated instance. PR1701632
- ARP/ND does not resolve when extended-vlan-list is configured for the specific VLAN. PR1702016
- In EVPN scenario, proxy-arp on IRB interfaces do not work as expected. PR1709007
- The Anycast Gateway stretched across 2 DCs over the seamless MPLS stitching DCI does not have Anycast Gateway MAC information coming from the remote DC when VLAN and VNI ids are different PR1712259
- A high CPU consumption of mcsnoopd process is seen under IGMP-snooping configured scenario leading to its crash. PR1713508
- Ping overlay vxlan replies Overlay-segment present even the bridge-domain has been deactivated. PR1715343
- The rpd core is seen in the long-running devices with EVPN enabled PR1723832

Forwarding and Sampling

- Deactivating and activating the GRES causes churn in dfwd filter addition/deletion. PR1697959
- The device is using the MAC address of the IRB interface even after configuring static MAC for a default gateway. PR1700073
- Firewall filter counters are not written to accounting file when interface-specific knob is used. PR1706085

General Routing

- Observed re0:rpdagent:20852:TRACE_ERR Rtsock_ERROR_MSG Function = "rpd_rtsock_dispatch", error = 7, msg = "rttable after device reboot PR1690105

High Availability (HA) and Resiliency

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

Infrastructure

- The next-hops entries are not cleared in some error-handling scenarios PR1677512

Interfaces and Chassis

- The dcd core may be seen on the backup RE after GRES is disabled if targeted distributed configuration is used PR1650676
- Node Slicing: In a rare scenario, the FPC/SLC will get stuck in the ready state after a restart PR1682271
- Subscribers will fail to negotiate the PPP session and be unable to login post-software upgrade PR1686940

- Incompatible/unsupported configuration is not getting validated correctly during ISSU/normal upgrade causing the traffic loss PR1692404
- VRRP Master session on AE ifl having child links on Satellite Device stops transmission post GRES PR1697394
- The cstm4 interface on MIC-3D-8CHOC3-4CHOC12 cannot be partitioned to more than 10 E3 interfaces PR1701875
- FPC offline can be seen on MX-VC during the sequential upgrade PR1706268
- JDI-REG:[VIRTUAL]:[eoam] [eoamtag] MX304 :: Not getting the expected values while verifying ['linktrace_egress_mac_address', 'linktrace_flags', 'linktrace_ingress_mac_address', 'reply_ttl'] On devices. PR1707126
- On Junos platforms the dcd will flap the IFLs which are part of EVPN routing-instance PR1712800
- The firmware upgradation will fail for MPC7E line card in MX-VC scenario PR1713502
- Issue in VRRP inline adjacency whenever a master router uplink goes down on MX platforms PR1720943

Junos Fusion Provider Edge

- The SDPD crash can be seen in Junos Fusion environment PR1679794

Layer 2 Ethernet Services

- DHCP packets might not be sent to the clients when 'forward-only' is reconfigured under the routing instance PR1689005
- A dcd process crash is observed continuously when the dhcp-service is restarted PR1698798
- DHCPv6 client options missing in solicit messages if TLV's exceeds a certain length PR1702831
- A jdhcpd process crash is observed on all Junos platforms PR1713619
- The DHCPv4 relay will send two option-82 to the server and the DHCP session will not be established PR1714260

MPLS

- RSVP refcount leak and the rpd crash observed post LSP churn PR1621771
- Traffic is not load-balanced when one of the next-hop LSP is down PR1690110
- The rpd crash will be observed during the MPLS label block allocation PR1694648
- The rpd process will crash when rpd is restarted PR1698889
- The rpd core and traffic loss is observed on Junos and Junos Evolved platforms PR1701420
- Memory leak issue in TED PR1701800
- LDP flaps will be observed having LT interface with VLAN and LDP running between the logical-system instance and global instance PR1702220
- Path Tear message is not forwarded by PLR to merge point which is causing data plane blackholing PR1703424
- When LDP dual transport is enabled, LDP V4 connection id changes from dual transport v4 id to router-id when rouer-id changes. PR1706064
- PathErr with RoutingProblem error code generated unexpectedly during dual failure local repair PR1713392

Platform and Infrastructure

- Traffic drop seen and filter not hitting as expected for match condition traffic class with FLT option configured. PR1573350
- JDI-RCT:M/Mx: FPC core @ jnh_call_read_index, trinity_nh_ucast_uninstall_hw. PR1636758
- The interface on the device will go down when one or more interfaces are connected to the Advantech3260 device at another end. PR1678506
- The traffic loss duration increases during the LSP switchover. PR1681250
- BGP session flap with error BGP_IO_ERROR_CLOSE_SESSION. PR1685113
- CoS memory errors are seen when "chassis traffic-manager enhanced-priority-mode" is configured. PR1687642
- The egress rewrite-rule might not work as expected for traffic entering the aggregated Ethernet interface. PR1700860

- Traffic is blocked on a queue when enhanced priority mode is configured. PR1704129
- Severity reclassification of queuing ASIC XQSS and memory parity error auto recovery. PR1706494
- The DEI bit will not be copied in the inner VLAN tag although the incoming traffic has the DEI bit set. PR1714429
- In a rare case FPC crashes and reboots generating a core. PR1720591
- On certain Junos OS MX Series platforms queue buffer-size temporal computation is not happening correctly. PR1726698

Routing Policy and Firewall Filters

- The flowd process crash is observed with the security policy updated with changing IP address related to the FQDN. PR1713576
- Commit error will not be seen after deactivating routing-instance applied under firewall filter. PR1720389

Routing Protocols

- The ppmd daemon memory leak might happen in the scenario where BFD authentication with ISIS is configured. PR1480648
- Traffic loss will be seen due to delay in BGP convergence time. PR1663883
- BGP LU Advertisements fail with the message "BGP label allocation failure: Need a gateway". PR1689904
- Traffic blackholing is observed when removing the BGP routes take a long time to get removed from RIB. PR1695062
- Wrong SRTE Secondary path weight makes the secondary path active in forwarding table. PR1696598
- The rpd process might crash when SPF is recalculated. PR1699076
- [bfd] [bfd_ospf3] ACX7100-32C :: Not all BFD sessions are coming up in 4K scaled sessions. PR1699085

- The BGP graceful-shutdown community is not advertised on Junos/Junos Evolved platforms. PR1699633
- Anycast PIM doesn't work when the peer has an authentication key configured for MSDP. PR1703707
- The BGP sessions will flap after the Routing Engine switchover. PR1705938
- OSPF routes are not getting installed after the interface is flapped. PR1705975
- The BFD session would flap when the GRES is triggered with single-hop BFD over AE interfaces configured. PR1706018
- A crash can be observed for 'mcsnoopd' process when the VLAN name for igmp-snooping has certain characters. PR1711153
- IPv4 routes learnt over a link-local BGP session not advertised ahead to other BGP peers. PR1712406
- Multipath route is not getting compute and skip the multipath eligibility check. PR1716153
- Unexpected behavior of bandwidth based metric for IS-IS protocol. PR1718734
- The rpd process crashes when TI-LFA is enabled. PR1719033

Services Applications

- A stale nat-long-route entry is present in the device causing incoming packets to be dropped. PR1719216

Subscriber Access Management

- The interim-rate under radius-options feature is not working post implementing BBE statistics performance and scale improvements. PR1695956
- A few subscriber sessions will not be up post Routing Engine switchover. PR1697392
- The subscriber sessions will be logged out when assigned IP addresses from Radius or AAA via framed-IP. PR1709574
- High CPU utilization is seen on Junos OS MX Series platforms. PR1710145

- IPv4 and IPv6 address allocation will be impacted due to changes in address pool configuration. PR1715490

User Interface and Configuration

- gNMI GET request fails when OpenConfig is present. PR1697869

VPNs

- Routes flapping when configuration changes are applied to custom routing instance. PR1654516
- 22.4R1:SRX_RIAD:srx5600:MN_HA:ike cookies didn't change in rekey lifetime expire cases after manual failover. PR1690921
- Two-digit numbered interfaces cannot be used as protect-interfaces. PR1695075
- IPsec VPNs will disconnect after ISSU. PR1696102
- VMX :: JDI-REG:Virtual:MVPN tunnel is not synced to back up router. MPVN tunnel interface is missed in show multicast route inet instance BLACK group 225.1.1.1 source-prefix 1.1.1.1 output PR1710323
- The iked process will crash when VPN tunnels parameters are not matching. PR1716092

Migration, Upgrade, and Downgrade Instructions

IN THIS SECTION

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

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

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

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

Basic Procedure for Upgrading to Release 22.3R1

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

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

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

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

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

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

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

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

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

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

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

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

- For 32-bit Routing Engine version:

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

- For 64-bit Routing Engine version:

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

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

- For 32-bit Routing Engine version:

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

- For 64-bit Routing Engine version:

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

Replace source with one of the following values:

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

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

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

Rebooting occurs only if the upgrade is successful.

NOTE:

- You need to install the Junos OS software package and host software package on the routers with the RE-MX-X6 and RE-MX-X8 Routing Engines. For upgrading the host OS on these routers with VM Host support, use the junos-vmhost-install-x.tgz image and specify the name of the regular package in the `request vmhost software add` command. For more information, see the VM Host Installation topic in the Installation and Upgrade Guide.
- Starting in Junos OS Release 22.3R2, in order to install a VM host image based on Wind River Linux 9, you must upgrade the i40e NVM firmware on the following MX Series routers:
  - MX240, MX480, MX960, MX2010, MX2020, MX2008, MX10016, and MX10008

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

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

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

Upgrade and Downgrade Support Policy for Junos OS Releases

We have two types of releases, EOL and EEOL:

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

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

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

Table 6: EOL and EEOL Releases

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

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

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

Upgrading a Router with Redundant Routing Engines

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

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

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

Downgrading from Release 22.3R1

To downgrade from Release 22.3R1 to another supported release, follow the procedure for upgrading, but replace the 22.2R1 jinstall package with one that corresponds to the appropriate release.

NOTE: You cannot downgrade more than three releases.

For more information, see the Installation and Upgrade Guide.

Junos OS Release Notes for NFX Series

IN THIS SECTION

These release notes accompany Junos OS Release 22.3R3 for the NFX Series Network Services Platforms. They describe new and changed features, limitations, and known and resolved problems in the hardware and software.

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

What's New

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

What's Changed

There are no changes in behavior and syntax in Junos OS Release 22.3R3 for NFX Series devices.

Known Limitations

There are no known limitations in hardware or software in this release for NFX Series devices.

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

Open Issues

IN THIS SECTION

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

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

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

Virtual Network Functions (VNFs)

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

Resolved Issues

IN THIS SECTION

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

Interfaces

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

Flow-Based and Packet-Based Processing

- High latency and packet drops will be observed with the "transmit-rate exact" knob enabled for one or more schedulers of an IFL/IFD.PR1692559

Migration, Upgrade, and Downgrade Instructions

IN THIS SECTION

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

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

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

Upgrade and Downgrade Support Policy for Junos OS Releases

We have two types of releases, EOL and EEOL:

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

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

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

you can upgrade from 20.4 to the next two EEOL releases – 21.2 and 21.4 or downgrade to the previous two EEOL releases – 20.2 and 19.4.

Table 7: EOL and EEOL Releases

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

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

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

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

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

Basic Procedure for Upgrading to Release 22.3

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

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

stored files, copy them to another system before upgrading or downgrading the device. For more information, see the Software Installation and Upgrade Guide.

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

To download and install Junos OS Release 22.3R2:

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

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

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

Junos OS Release Notes for PTX Series

IN THIS SECTION

These release notes accompany Junos OS Release 22.3R3 for the PTX Series. They describe new and changed features, limitations, and known and resolved problems in the hardware and software.

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

What's New

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

What's Changed

IN THIS SECTION

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

Junos XML API and Scripting

- **Ability to commit `extension-service file` configuration when application file is unavailable**— When you set the `optional` option at the `edit system extension extension-service application file` *`file-name`* hierarchy

level, the operating system can commit the configuration even if the file is not available at the **/var/db/scripts/jet** file path.

[See file (JET).]

- **The `xmlns:junos` attribute includes the complete software version string (ACX Series, EX Series, MX Series, PTX Series, QFX Series, SRX Series, vMX, and vSRX)**—The `xmlns:junos` namespace string in XML RPC replies includes the complete software version release number, which is identical to the version emitted by the `show version` command. In earlier releases, the `xmlns:junos` string includes only partial software version information.

Network Management and Monitoring

- **`operator` login class is restricted from viewing NETCONF trace files that are `no-world-readable` (ACX Series, EX Series, MX Series, PTX Series, QFX Series, SRX Series, vMX, and vSRX)**—When you configure NETCONF tracing options at the `[edit system services netconf traceoptions]` hierarchy level and you restrict file access to the file owner by setting or omitting the no-world-readable statement (the default), users assigned to the `operator` login class do not have permissions to view the trace file.

Known Limitations

IN THIS SECTION

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

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

General Routing

- Whenever the underlay interface flaps for 1K legacy GR-tunnels, BGP establishment over these tunnels may take ~8 to 10 minutes.PR1614179

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. https://kb.juniper.net/TSB18251. PR1568757

Routing Protocols

- When "routing-options transport-class fallback none" is not configured - do not configure more than 10 transport-classes. Or advertise more than 10 distinct colors in SRTE or FlexAlgo. This limitation will be fixed by PR-1695020. PR1648490

User Interface and Configuration

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

Open Issues

IN THIS SECTION

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

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

General Routing

- On routers and switches running Junos OS, with Link Aggregation Control Protocol (LACP) enabled, deactivating a remote Aggregate Ethernet (AE) member link makes the local member link move to LACP detached state and cause traffic drops on that member link. The same scenario applied when a new member link is added where the other end of that link is not yet configured with LACP. PR1423707
- Unsupported config 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 may be observed and this might result in relevant impacts on traffic analysis and billing. PR1569229
- On PTX10002-60C/QFX10002-60C, after the system is rebooted, the "FPC 0 Major Errors" alarm might be seen due to a rare timing issue. The issue could cause the host path traffic to get dropped. It is a rare issue and does not always happen during reboot. Please try to perform "request vmhost reboot" for recovery. PR1613229
- On dual-RE platforms, if certain PTX3000/5000 Linux based FPCs (FPC3-SFF-PTX-1X,FPC3-SFF-PTX-2X,FPC-P1,FPC-P2) are installed, when TNP (Trivial Network Protocol) neighbor towards backup RE continuously flaps, FPC might reboot after GRES due to the TNP neighbor issue.PR1630393
- V6 default route will not get added after successful dhcpv6 client binding on PTX1000 router during ztp. PR1649576
- Presence of consistent hash/resiliency feature in the running configuration causes the system to take much longer to converge in case of a churn. PR1652750
- ZTP: DHCPACK not received at ztp-server after zeroize of the device (client). PR1658287
- When subscribing to sensor paths "/junos/system/linecard/packet/usage/", "/junos/services/label-switched-path/usage/" or other line card (PFE) sensor paths in gNMI subscription mode, packet drops may be seen in the CLI command "show network-agent statistics gnmi detail" output. The collector output may also contain missing sequence numbers. For example, the sequence number output may be 0, 3, 6, 9, 12, etc. instead of 0, 1, 2, 3, 4, etc. PR1703418

- In Chassisd, Jvision thread takes more time in streaming of jvision packets because of volume of data and number of sensors involved with this daemon. Jvision thread engaged for more time to process streaming events caused Chassisd master thread to lose receive/send keepalive messages to/from other RE, which eventually was causing automatic RE switchover in most of the cases. To avoid this, fix done for exporting small payload jvision packets (formation of which takes less time) and deferring jvision thread more in an interval, to allow chassisd master thread to process high-priority hello/keep-alive messages. This means now, more number of packets is sent in one reporting interval and with larger spread (earlier same amount of data was sent with 2 or 3 packets of higher payload size, and 100ms of deferring time for jvision thread. This behaviour is increasing KPI-2 but lowering KPI-1 (payload size).It is not possible to back out changes done to solve keep-alive message loss issue. Hence we will have to keep Chassisd as an exception, when we measure/report KPI-2 values. Jvision in Chassisd has to give more priority/time to process keep-alive messages than sending of jvision packets. Hence delay between jvision packets are more.PR1706300

Routing Protocols

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

Resolved Issues

IN THIS SECTION

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

General Routing

- The user-defined speed does not take effect on the AE interface in certain scenarios on Junos platforms. PR1649958

- EX/QFX SNMP: jnxOperatingDescr.1.1.0.0 returns blank, but jnxOperatingState.1.1.0.0 returns value. PR1683753
- [Paradise] Currently no alarm is raised when onchip memory exhausts on paradise based FPCs. PR1690289
- EVO jkey path changed under protocol/isis. "isis/levels" is missing. PR1698192
- Ports with QSA adapter are down. PR1709817
- gNMI line card (PFE) sensor /junos/system/linecard/packet/usage/ may have packet drops (gNMI translator lookup failures). PR1711779
- The interface does not come up or keeps flapping. PR1712007
- FPC memory leak will cause FPC crash. PR1712076
- Next-hop programming issue at PFE on Junos PTX and QFX10k platforms when the member of unilist is in hold state. PR1713279
- Traffic loop is seen due to incorrect root bridge ID. PR1717267
- Convergence delay is seen when FPC is offlined under heavy traffic and scaled scenario. PR1719956

Routing Protocols

- The rpd process might crash when SPF is recalculated. PR1699076
- Unexpected behavior of bandwidth based metric for IS-IS protocol. PR1718734

Migration, Upgrade, and Downgrade Instructions

IN THIS SECTION

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

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

Basic Procedure for Upgrading to Release 22.3

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

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

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

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

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

To download and install Junos OS Release 22.3R2:

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

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

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

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

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

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

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

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

Replace the source with one of the following values:

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

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

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

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

Rebooting occurs only if the upgrade is successful.

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

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

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

Upgrade and Downgrade Support Policy for Junos OS Releases

We have two types of releases, EOL and EEOL:

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

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

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

Table 8: EOL and EEOL Releases

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

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

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

Upgrading a Router with Redundant Routing Engines

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

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

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

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

Junos OS Release Notes for QFX Series

IN THIS SECTION

These release notes accompany Junos OS Release 22.3R3 for the QFX Series. They describe new and changed features, limitations, and known and resolved problems in the hardware and software.

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

What's New

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

What's Changed

IN THIS SECTION

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

General Routing

- **Verified the qualification of `ordered-by-user` in the hierarchies (ACX Series, EX Series, MX Series, QFX Series, SRX Series, vMX, and vSRX)**—The requested hierarchies are reviewed and checked to confirm if they qualify for the `ordered-by-user` list type. If they do not, the `flag autosort` is included in the DDL definition for the list, making it `ordered-by-system`. The hierarchies are now indexed. The benefits from this arrangement are we get accurate data modeling and optimized configuration load in the user interface infrastructure.
- In the past inet6flow.0 was not allowed to be a primary rib in a rib-group. Starting with Release 22.3 this is now allowed.

Junos XML API and Scripting

- **The `xmlns:junos` attribute includes the complete software version string (ACX Series, EX Series, MX Series, PTX Series, QFX Series, SRX Series, vMX, and vSRX)**—The `xmlns:junos` namespace string in XML RPC replies includes the complete software version release number, which is identical to the version emitted by the `show version` command. In earlier releases, the `xmlns:junos` string includes only partial software version information.

Network Management and Monitoring

- **`operator` login class is restricted from viewing NETCONF trace files that are `no-world-readable` (ACX Series, EX Series, MX Series, PTX Series, QFX Series, SRX Series, vMX, and vSRX)**—When you configure NETCONF tracing options at the `[edit system services netconf traceoptions]` hierarchy level and you restrict file access to the file owner by setting or omitting the `no-world-readable` statement (the default), users assigned to the `operator` login class do not have permissions to view the trace file.

Known Limitations

IN THIS SECTION

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

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

Infrastructure

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

Platform and Infrastructure

- 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

- When EVPN-VxLAN tunnel is established over V6 underlay, the encapsulated pkts emitted out of leaf node (QFX10K) may have UDP checksum zero. This is the default behavior of all V6 tunneled UDP pkts and it is allowed as per RFC6936. PR1656363
- On QFX10008 devices, statistics for multicast packets is not as expected as the packets has Layer 2 header stripped during replication in PFE because of which it is not forwarded to the next hop. PR1678723

Open Issues

IN THIS SECTION

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

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

Infrastructure

- Earlier implementation of kvmclock with vDSO (virtual Dynamic Shared Object) which helps avoid the system call overhead for user space applications had problem of time drift, the latest set of changes takes care of initializing the clock after all auxiliary processors are launched so that the clock initialization is accurate. PR1691036

Interfaces and Chassis

- Following two Failure messages seen brcm_rt_ip_mc_ipmc_install:2455 Failed (Invalid parameter:-4) This message is due to IPMC Group being used is not created, when RE tried to add this check indicates there is a parameter mis-match. brcm_rt_ip_mc_ipmc_install:2455 Failed (Internal error:-1) This message is due to Failure to read IPMC Table or any memory/register. PR1461339

Layer 2 Features

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

Layer 2 Ethernet Services

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

MPLS

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

Platform and Infrastructure

- 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

- On the QFX5100 line of switches, inserting or removing optics on a port might cause a Packet Forwarding Engine Manager CPU spike and an eventual microcode failure. PR1372041
- VXLAN VNI (multicast learning) scaling on QFX5110 traffic issue is seen from VXLAN tunnel to Layer 2 interface. PR1462548
- 5M DAC connected between QFX10002-60C and MX2010 doesn't link up. But with 1M and 3M DAC this interop works as expected. Also it is to be noted QFX10002-60C and ACX or Traffic generator the same 5M DAC works seamlessly. There seems to be certain SI or link level configuration on both QFX10002-60C and MX2010 which needs to be debugged with the help from HW and SI teams and resolved. PR1555955
- To avoid the additional interface flap , interface hold time needs to be configured. PR1562857
- On QFX5100 devices, the media type for SFP+-10G-CU1M and SFP-T cables are shown as fiber. This is only a display issue and no functionality impact is observed. PR1570555
- On QFX5110 VC, FPC may gets disconnected with 24K DHCPv6 relay scaling, after the traffic is stopped. The `pfe_listener_disconnect` error messages gets generated. PR1594748
- Pim Vxlan not working on TD3 chipsets enabling VxLAN flexflow after release 21.3R1. Customers Pim Vxlan or data plane VxLAN can use the version 21.3R1. PR1597276
- On QFX5100, optical power is seen after detached and attached QSFP on disable interface. PR1606003
- On QFX5120-48Y, when scaled config and baseline configs are loaded multiple times one after other without much wait time in between then traffic or protocols on pure L3 interfaces may behave in undefined/unexpected manner. PR1612973
- On PTX10002-60C/QFX10002-60C, after the system is rebooted, the "FPC 0 Major Errors" alarm might be seen due to a rare timing issue. The issue could cause the host path traffic to get dropped. It is a rare issue and does not always happen during reboot. Please try to perform "request vmhost reboot" for recovery. PR1613229
- In QFX5110-32Q, a part of the traffic is lost after renumbering master in VC. Issue was seen in all the releases before 22.4 and not seen from 22.4 release when sdk is upgraded to 6.5.26. The workaround provided here is to either flap the Higig port or flap the ingress interface. PR1632565
- Backup FPC lose their connection to the master when new members are added to the VCF (Virtual Chassis Fabric). PR1634533
- On all devices running Junos OS or Junos OS Evolved, where this is a high BGP scale with flapping route and the BGP Monitoring Protocol (BMP) collector/station is very slow, the rpd process might crash due to memory pressure. PR1635143

- When MACSEC and VRRP are enabled on QFX5120 VC, MACSEC sessions are flapping at random times. Without VRRP this issue is not seen. PR1640031
- On 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 QFX5100 platforms, traffic may not get classified based on a fixed classifier in MPLS as well as the VXLAN scenario. PR1650051
- On QFX devices, IPv6 ifl status gets derived from the underlying ifd stats unlike on PTX where they are hardware assisted. Hence, they are not very reliable and are at best, guesstimate. PR1653671
- On QFX5100-24Q devices, Virtual-chassis is in unstable state for 3 to 7 minutes causing traffic loss. PR1661349
- On all QFX platforms, Ethernet VPN (EVPN) Type-5 traffic drops are observed when the device is configured only with Type-5 Virtual Routing and Forwarding (VRF) and without an Integrated Routing and Bridging (IRB) interface. PR1663804
- When the remote end server/system reboots, QFX5100 platform ports with SFP-T 1G inserted may go into a hung state and remain in that state even after the reboot is complete. This may affect traffic after the remote end system comes online and resumes traffic transmission. PR1665800
- On the EX4600 device with SFP-LX10/SFP-SX, after a power cycle/software reboot, all ports are initialized and links are up with auto-negotiation enabled. Few ports are up and traffic flows whereas few ports are up but no traffic flow through them. PR1672583
- On QFX5200 devices after NSSU upgrade for a 4 member VC , FPC might toggle resulting in interfaces going offline. PR1673116
- Each locally learned ARP/ND Nexthop requires unique fabric token from Kernel. This unique token maps to physical address in HW and this address points to EDF memory for the ARP/ND nexthops. Token pool in kernel is also used by different features like flood nexthops, arp/ndp nexthops. Token usage has increased as tokens are now used by IRB interfaces and default mesh groups also. 96k ARP/ND scale might not be achievable always. It is recommended to scale upto 95K ARP/ND. PR1673626
- On QFX10008 devices, statistics for multicast packets is not as expected as the packets has Layer 2 header stripped during replication in PFE because of which it is not forwarded to the next hop. PR1678723
- On QFX5100 platforms (both stand-alone and VC scenario) running Junos, occasionally during the normal operation of the device, Packet Forwarding Engine might crash resulting in total loss of traffic. The Packet Forwarding Engine reboots itself following the crash. PR1679919

- On QFX5100 Virtual Chassis (VC) and Virtual Chassis Fabric (VCF) platforms on upgrading Virtual Chassis Fabric (VCF) and toggling the interface, when FPC (Flexible PIC Concentrators) is disabled and rebooted, the member fails to join the virtual chassis and the interface remains disabled even after been enabled. PR1689499
- The `show chassis hardware` command indicates duplicate entries for PSU and FAN tray after USB clean install or zeroize. PR1704106
- as list_get_head function is called in multiple places in pfe we needed previous 3 functions on the stack which had called list_get_head so we could debug why 'list_get_head list has bad magic ' this error has occured. PR1705853
- On all EX and QFX platforms, BFD (Bidirectional Forwarding Detection) sessions are flapped with VLAN configuration change on LAG interface. PR1709664
- Service disruptions are seen due to a consistent increase in l2ald (Layer 2 Address Learning Daemon) memory usage. PR1727954
- On all Junos EX46xx/QFX5k (except QFX5100) platforms, child links that are in LACP (Link Aggregation Control Protocol) detached state are up and accepting incoming traffic, expecting it to drop. PR1730076
- QFX5120 will reboot without causing a dcpfe crash upon the deletion of EP style(trunk) interface with multiple IFLs and native vlan configured. PR1733022

Routing Protocols

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

Virtual Chassis

- On QFX5100 devices running QFX-5e images in Virtual Chassis setup, when Virtual Chassis Port (VCP) links are connected between PHY and PHYLESS ports, CRC alignment errors will be seen. As a result, there can be traffic loss on these links. PR1692102

Resolved Issues

IN THIS SECTION

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

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

EVPN

- The rpd crash would be observed when activating or deactivating the EVPN routing-instances. PR1673157
- Traffic drop would be observed due to the VTEP tunnels not being established in the EVPN-VXLAN. scenario PR1700196
- In EVPN scenario, proxy-arp on IRB interfaces do not work as expected. PR1709007
- The generation of the VXLAN table appears to be lost after loading configuration. PR1712805
- L2ALD core at l2ald_vxlan_ifl_create_msg_build. PR1718534
- The rpd core is seen in the long-running devices with EVPN enabled. PR1723832
- Traffic loss is seen as Type 2 routes are not pushed even after withdrawing Type 5 routes. PR1723968

Forwarding and Sampling

- The device is using the MAC address of the IRB interface even after configuring static MAC for a default gateway. PR1700073

Infrastructure

- The next-hops entries are not cleared in some error-handling scenarios. PR1677512

Interfaces and Chassis

- The Unicast traffic is dropped on QFX51000 Virtual Chassis platforms. PR1695663

Platform and Infrastructure

- On QFX10008 devices, while verifying em0 statistics interface speed is displaying in Gbps instead of mbps. PR1589942
- Virtual Chassis members are reloading randomly.PR1671293
- The protocol MTU for the IRB interface is not rolled back when the MTU of the IRB or IFD interfaces is modified or deleted. PR1685406
- DHCPv6 packets are not forwarded if it contains the trailer or extra bytes out of the IP stack. PR1688316
- Traffic loss is observed in IP fabric when there is a change in the underlay network. PR1688323
- The FPC crash would be observed when the same CoS configuration is applied with wildcard for all the physical interfaces and aggregated Ethernet interface. PR1688455
- dot1xd.core-tarball.0.tgz is observed in 22.1R3 at #0x009113f0 in __mem_assert(). PR1694129
- All members of the VCF will not reboot on QFX5000 platforms. PR1694996
- The l2cpd telemetry crash would be observed when the LLDP Netconf notification from external controllers along with Netconf services configuration is present on the device. PR1695057
- Intra VLAN communication breaks in SP style config using VXLAN. PR1695058

- On QFX5110-VC-VCF platforms, traffic impact is seen when the firewall filter with DSCP action is enabled. PR1695820
- Traffic forwarding fails when deleting all Layer 2 related configurations. PR1695847
- Traffic drop is observed for the VCP ports when there is traffic congestion in the egress queues. PR1696119
- Adding more than 256 VLANs as name tags on the same interface results in dcd crash. PR1696428
- VSTP will not work in the EVPN-VxLAN network. PR1696979
- Assigning VNI to VLAN will cause a small number of packets lost on other VLANs on the same interface. PR1697244
- Local multicast traffic forwarding issue can be seen on QFX5K in EVPN-VXLAN OISM setup. PR1697614
- PE device changes an outer tag-id in a local return environment. PR1697835
- Dot1x authentication failure for EVPN VXLAN enabled port. PR1697995
- On QFX5000 switch, VGA is not working when SP style config is mixed with EP style configuration. PR1698491
- Adaptive sampling will not work if the system clock is turned backward. PR1699585
- The BFD session remains in init/down state in the Virtual Chassis scenario. PR1701546
- License will be deleted due to multiple FPC reboot or switchover on QFX/MX VC scenario. PR1703200
- The dcpfe process crashes which leads to FPC restart. PR1706515
- The FPC crash can be seen on QFX5k platforms during simultaneous soft and hard OIR of SFP. PR1707094
- The spine does not reply to RS messages coming through the VXLAN tunnel in the CRB scenario. PR1707679
- License expire error will be observed after upgrade. PR1708794
- Traffic drop is observed with the `vxlan encapsulate-inner-vlan` command on QFX10000 devices. PR1709605
- Ports with QSA adapter are down. PR1709817
- The Virtual Chassis members splits when you remove and insert the em0 cable. PR1709938

- FPC is down on QFX5000 after committing an IPv6 filter. PR1710704
- The `fpc0 list_get_head, list has bad magic (0x0)` message might be an output after the commit operation is complete. PR1710776
- The FPC will be offline after upgrading the system. PR1710855
- On the QFX5110 devices, chassis alarm does not get generated when inserted PSU module which has a different airflow. PR1710952
- When a 100G transceiver is used as a VC port, the VC port will either not come up or come up as 40G. PR1711407
- Traffic drops in the EVPN-VXLAN scenario with Type-2 ESI Tunnel. PR1711889
- VXLAN traffic gets dropped after new Layer 3 VLANs are created. PR1712405
- On QFX5120-32C devices, the dcpfe process generates core file after Restart l2-learning process. PR1713133
- Next-hop programming issue at PFE on Junos PTX and QFX10k platforms when the member of unilist is in hold state. PR1713279
- The member interface will not be added to the aggregated Ethernet interface bundle if the link-speed of the AE interface does not match that of the member. PR1713699
- Known multicast traffic is not forwarded when you enable MLD snooping. PR1715429
- Untagged packets get dropped while adding a layer 3 logical unit to an interface with native VLAN configured. PR1715477
- The dcpfe process crashes on QFX5000 devices. PR1716996
- Traffic loop is seen due to incorrect root bridge ID. PR1717267
- Traffic egressing over the EVPN-VXLAN tunnel drops which has aggregated Ethernet interface as underlay. PR1718528
- Traffic failure with error message 'Buffers are stuck on queue' after removing and attaching 100G QSFP. PR1641572
- Traffic Loss will be observed with Virtual-Router. PR1650335
- Traffic loss might be seen when l2circuit configurations are deactivated and activated on QFX5110 devices. PR1666260
- Power supplies are showing as present state. PR1701240

- Aggregated Ethernet interface member with vlan-id-list configured not forwarding traffic. PR1701636
- High CPU utilization causes a latency/slowness issue on QFX platforms. PR1704489
- The dcpfe process crash is seen on QFX5k platforms due to stale vtep entry. PR1712175
- Traffic blackhole after reboot. PR1714701
- VMcore crashes in a rare scenario. PR1714785
- Error message "%PFE-3: fpc0 Failed to get ifl for ifl index = XXX" is generated when receives DHCP packet via remote vtep. PR1721318
-
- PFE crash is seen on Junos when file-logging is disabled. PR1723465
- ECMP traffic is not being forwarded on all QFX10002 platforms after software upgrade. PR1723545
- Traffic loss will be observed with vlan tagging and/or vlan normalisation in a specific design (using a looped cable). PR1724675
- Traffic loss will be observed with vlan tagging and/or vlan normalisation in a specific design (using a looped cable). PR1724675
- The 100G interface will remain down post rebooting the device. PR1725116
- On QFX5K platforms, the status of 'ECMP Resilient Hashing' will not be displayed in output of CLI command 'show forwarding-options enhanced-hash-key'. PR1725916
- The 100G interface will remain down post rebooting the device. PR1725116
- On QFX5K platforms, the status of 'ECMP Resilient Hashing' will not be displayed in output of CLI command 'show forwarding-options enhanced-hash-key'. PR1725916
- Delete notifications for sub-interfaces missed in gRPC telemetry. PR1726205
- Traffic is impacted due to high CPU and dcpfe/fxpc crash (in some cases) in EVPN-VXLAN scenario. PR1730771
- SNMP polling Timeout due to OID 1.3.6.1.2.1.31.1.1.1.10.514 (ifInOctets.514). PR1732708

Routing Protocols

- The BGP graceful-shutdown community is not advertised. PR1699633

- IPv4 routes learnt over a link-local BGP session not advertised ahead to other BGP peers. PR1712406
- Unexpected behavior of bandwidth based metric for IS-IS protocol. PR1718734
- The mcscnoopd process will be stuck in resync state after snooping configuration is deleted and added again immediately. PR1699784

Migration, Upgrade, and Downgrade Instructions

IN THIS SECTION

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

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

Upgrading Software on QFX Series Switches

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

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

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

   The Junos Platforms Download Software page appears.

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

3. Select **22.3** in the Release pull-down list to the right of the Software tab on the Download Software page.

4. In the Install Package section of the Software tab, select the QFX Series Install Package for the 22.3 release.

   An Alert box appears.

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

   A login screen appears.

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

7. Download the software to a local host.

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

9. Install the new jinstall package on the device.

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

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

```
user@host> request system software add source/jinstall-host-qfx-5-x86-64-22.3-R3.n-secure-signed.tgz reboot
```

Replace *source* with one of the following values:

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

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

Rebooting occurs only if the upgrade is successful.

NOTE: After you install a Junos OS Release 22.3 `jinstall` package, you can issue the `request system software rollback` command to return to the previously installed software.

Installing the Software on QFX10002-60C Switches

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

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

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

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

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

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

For example:

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

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

For example:

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

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

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

Installing the Software on QFX10002 Switches

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

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

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

For example:

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

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

For example:

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

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

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

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

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

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

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

To install the software on re0:

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

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

For example:

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

To install the software on re1:

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

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

For example:

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

Reboot both Routing Engines.

For example:

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

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

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

Installing the Software on QFX10008 and QFX10016 Switches

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

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

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

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

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

2. From the command line, enter configuration mode:

   ```
   user@switch> configure
   ```

3. Disable Routing Engine redundancy:

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

4. Disable nonstop-bridging:

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

5. Save the configuration change on both Routing Engines:

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

6. Exit the CLI configuration mode:

```
user@switch# exit
```

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

12. Transfer routing control to the backup Routing Engine:

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

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

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

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

Routing Engine status:
  Slot 1:
```

```
    Current state                   Master
    Election priority               Backup (default)
```

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

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

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

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

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

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

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

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

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

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

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

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

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

```
user@switch> show chassis routing-engine
Routing Engine status:
  Slot 0:
```

```
    Current state                   Master
    Election priority               Master (default)

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

Performing a Unified ISSU

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

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

Perform the following tasks:

- No Link Title
- No Link Title

Preparing the Switch for Software Installation

Before you begin software installation using unified ISSU:

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

  To verify that nonstop active routing is enabled:

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

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

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

- Enable nonstop bridging (NSB). See Configuring Nonstop Bridging on EX Series Switches for information on how to enable it.
- (Optional) Back up the system software—Junos OS, the active configuration, and log files—on the switch to an external storage device with the `request system snapshot` command.

Upgrading the Software Using Unified ISSU

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

To upgrade the switch using unified ISSU:

1. Download the software package by following the procedure in the Downloading Software Files with a Browser section in Installing Software Packages on QFX Series Devices.
2. Copy the software package or packages to the switch. We recommend that you copy the file to the `/var/tmp` directory.
3. Log in to the console connection. Using a console connection allows you to monitor the progress of the upgrade.
4. Start the ISSU:
   - On the switch, enter:

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

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

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

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

```
warning: Do NOT use /user during ISSU. Changes to /user during ISSU may get lost!
ISSU: Validating Image
ISSU: Preparing Backup RE
Prepare for ISSU
ISSU: Backup RE Prepare Done
Extracting jinstall-host-qfx-5-f-x86-64-18.3R1.n-secure-signed.tgz ...
Install jinstall-host-qfx-5-f-x86-64-19.2R1.n-secure-signed.tgz completed
Spawning the backup RE
Spawn backup RE, index 0 successful
GRES in progress
GRES done in 0 seconds
Waiting for backup RE switchover ready
GRES operational
Copying home directories
Copying home directories successful
Initiating Chassis In-Service-Upgrade
Chassis ISSU Started
ISSU: Preparing Daemons
ISSU: Daemons Ready for ISSU
ISSU: Starting Upgrade for FRUs
ISSU: FPC Warm Booting
ISSU: FPC Warm Booted
ISSU: Preparing for Switchover
ISSU: Ready for Switchover
Checking In-Service-Upgrade status
  Item           Status                  Reason
  FPC 0          Online (ISSU)
Send ISSU done to chassisd on backup RE
Chassis ISSU Completed
ISSU: IDLE
Initiate em0 device handoff
```

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

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

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

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

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

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

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

Upgrade and Downgrade Support Policy for Junos OS Releases

We have two types of releases, EOL and EEOL:

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

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

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

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

Table 9: EOL and EEOL Releases

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

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

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

Junos OS Release Notes for SRX Series

IN THIS SECTION

These release notes accompany Junos OS Release 22.3R3 for the SRX Series Services Gateways. They describe new and changed features, limitations, and known and resolved problems in the hardware and software.

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

What's New

There are no new features or enhancements to existing features in Junos OS Release 22.3R3 for SRX Series devices.

What's Changed

IN THIS SECTION

Learn about what changed in this release for SRX Series.

General Routing

- **Verified the qualification of `ordered-by-user` in the hierarchies (ACX Series, EX Series, MX Series, QFX Series, SRX Series, vMX, and vSRX)**—The requested hierarchies are reviewed and checked to confirm if they qualify for the `ordered-by-user` list type. If they do not, the `flag autosort` is included in the DDL definition for the list, making it `ordered-by-system`. The hierarchies are now indexed. The benefits from this arrangement are we get accurate data modeling and optimized configuration load in the user interface infrastructure.
- In the past inet6flow.0 was not allowed to be a primary rib in a rib-group. Starting with Release 22.3 this is now allowed.

Junos XML API and Scripting

- **Ability to commit `extension-service file` configuration when application file is unavailable**—When you set the `optional` option at the **edit system extension extension-service application file *file-name*** hierarchy level, the operating system can commit the configuration even if the file is not available at the **/var/db/scripts/jet** file path.

  [See file (JET).]

- **Ability to restart restart daemonized applications**—Use the `request extension-service restart-daemonize-app *application-name*` command to restart a daemonized application running on a Junos device. Restarting the application can assist you with debugging and troubleshooting.

  [See request extension-service restart-daemonize-app.]

- **The `xmlns:junos` attribute includes the complete software version string (ACX Series, EX Series, MX Series, PTX Series, QFX Series, SRX Series, vMX, and vSRX)**—The `xmlns:junos` namespace string in XML RPC replies includes the complete software version release number, which is identical to the version emitted by the `show version` command. In earlier releases, the `xmlns:junos` string includes only partial software version information.

Network Management and Monitoring

- **`operator` login class is restricted from viewing NETCONF trace files that are `no-world-readable` (ACX Series, EX Series, MX Series, PTX Series, QFX Series, SRX Series, vMX, and vSRX)**—When you configure NETCONF tracing options at the `[edit system services netconf traceoptions]` hierarchy level and you restrict file access to the file owner by setting or omitting the `no-world-readable` statement (the default), users assigned to the `operator` login class do not have permissions to view the trace file.

VPNs

- **Limited ECDSA Certificate Support with SSL Proxy (SRX Series and vSRX 3.0)**—With SSL proxy configured on SRX Series firewall and vSRX Virtual firewalls.

  - ECDSA based websites with P-384/P-521 server certificates are not accessible with any root-ca certificate as the security device has limitation to support only P-256 group.

  - When RSA based root-ca and P-384/P-521 ECDSA root-ca certificate is configured, all ECDSA websites will not be accessible as SSL-Terminator is negotiated with RSA, which is why the security device is sending only RSA ciphers and sigalgs to the destination web server while doing

the SSL handshake. To ensure both ECDSA and RSA-based websites are accessible along with the RSA root certificate, configure a 256-bits ECDSA root certificate.

- In some scenarios, even if 256-bit ECDSA root certificate is used in the SSL proxy configuration, ECDSA based websites with P-256 server certificates are not accessible if the server does not support P-256 groups.
- In other scenarios, even if 256-bit ECDSA root certificate is used in the SSL proxy configuration, ECDSA based websites with P-256 server certificates are not accessible if the server supports sigalgs other than P-256. The issue is seen in hardware offload mode with failing signature verification. As hardware offload for ECDSA certificate is introduced in Junos OS release 22.1R1, this issue will not be observed if you use Junos OS released prior to 22.1R1. Also, the issue is not seen if the SSL-proxy for ECDSA certificate is handled in software.

VPNs

- **Syslogs to capture commit warning messages related to traffic loss prevention over VPN (SRX, vSRX, NFX platforms)**—Configuration commit warnings such as `warning: Policy 'traditional' does not contain any dynamic-applications or url-categories but is placed below policies that use them. Please insert policy 'traditional' before your Unified policies` or `warning: Source address or address_set (made_up_address) not found. Please check if it is a SecProfiling Feed` caused the MGD to inform IKED or KMD process about *DAX_ITEM_DELETE_ALL* resulting in VPN flaps and outage events. These warnings messages are captured by syslogs to prevent traffic loss over VPN. We recommend you to resolve these syslog warning messages to prevent major outages.

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 primary to back-up.PR1667098
- On SRX4100 and SRX4200 devices, due to hardware limitation of Intel 82599 NIC where maximum of 128 unit case mac addresses plus mac filters are supported. For MNHA switching mode, if you define more than 127 virtual MACs on same revenue or aggregated Ethernet interface, the extra

(those beyond 127) virtual MAC filters could not be programmed to the NIC so you would see traffics toward those vMACs got silently dropped.PR1687262

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. https://kb.juniper.net/TSB18251PR1568757

User Interface and Configuration

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

VPNs

- In some scenario(e.g configuring firewall filter) sometimes SRX5000 line of devices 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.

Application Layer Gateways (ALGs)

- FTPS connection to the server will not be successful until the first attempt is aborted and a new connection to the server is made. PR1715918

Chassis Clustering

- 10G DAC cable is not supported at CTL/FAB link at SRX4100/4200 Cluster setup. Hardware Compatibility Tool (https://apps.juniper.net/hct/home/) reports 10G DAC cables are as "supported", but CTL and FAB links are out of scope. - SRX-SFP-10GE-DAC-1M - SRX-SFP-10GE-DAC-3MPR1636365
- DSCP remarking is required to classify BFD packets as high priority.PR1693457

Flow-Based and Packet-Based Processing

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

General Routing

- In mac-os platforms when Juniper Secure Connect client connects successfully, the client is not getting minimized to tray icon and needs to be minimized manually.PR1525889
- IPsec rekey fails when SRX is configured with kilobyte based lifetime in remote access solution. PR1527384
- With ssl-proxy configured along with web-proxy, the client session might not get closed on the device until session timeout, even though the proxy session ends gracefully.PR1580526
- All VPN traffic may internally drop during encryption / decryption processing in HW engine requiring Packet Forwarding Engine plane reset. PR1630981
- SRX550HM interfaces LED of ge-0/0/6-9 will auto turn off after device bootup some minutes.PR1634965
- SMTPS sessions are not getting identified when traffic is sent from IXIA (BPS) profile. PR1635929
- Device does not drop session with server certificate chain more than 6.PR1663062
- On SRX platforms using authentication-scheme (pass-through/web-auth/web-redir) and authentication sources (firewall-user/ldap/radius) do not display the complete user's group information because the display buffer for showing group names for an authentication entry is too small.PR1673125
- For logical system, tenant logical interface with unit 0 and without VLAN tagging/ VLAN id can be created from Network>Connectivity>Interfaces. Same cannot be done from Logical system or tenant workflow.PR1676235
- FIPS mode is not supported in this release for SRX devices.PR1697999
- On SRX380, the Autonegotiation status on the 1G/10G ports may be incorrectly displayed as "Incomplete". This has no impact to traffic.PR1703002
- On SRX platforms, log streaming to the security director cloud fails on TLS when DNS re-query is performed.PR1708116
- On all Junos SRX platforms, when security log profile is added without a category or stream can cause the srxpfe to crash. Due to this there will be complete traffic loss.PR1708777

Routing Policy and Firewall Filters

- On SRX platforms configured with security policies, having huge number approx. 15 thousand of addresses and performing addition/deletion of such policies in short intervals of time might result in srxpfe process crash and hence, datapath traffic gets impacted. PR1725567

VPNs

- In some scenarios, the kmd core might be seen when all VPNs are down. PR1336368
- 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

Resolved Issues

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

Application Layer Gateways (ALGs)

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

Authentication and Access Control

- Connection fails are observed on Junos despite a valid auth entry PR1692398

Chassis Clustering

- New secondary node to go into a disabled state after ISSU and failover RG0 because of fabric link failure PR1678772
- The secure tunnel interface does not work properly in SRX standalone mode PR1702763
- GTPv2 Message Filtering is not working PR1704472
- From 20.4 onwards,St0.16000 to st0.16385 will not be allowed to be configured in HA and MNHA mode PR1704670

Flow-Based and Packet-Based Processing

- The non-fragmented packets will get dropped on the SRX5K platforms with SPC3 card PR1683835
- VPN logs in monitor hierarchy on j-web not being seen. PR1691095
- Packet loss is observed for IPSec sessions when PMI is enabled PR1692885
- Application traffic drop seen on all SRX platforms due to TCP window size issue PR1699578
- Core dump will be seen when user is changing interface configuration PR1704623
- A flowd process crash is seen on SRX4100/4200/4600, vSRX, and SRX5K with SPC3 card when a route is changed frequently PR1705996
- The IPv6 source-level fragmented SCTP packets passing through an IPSec tunnel will be dropped PR1708876

General Routing

- HA AP mode on-box logging in LSYS and Tenant: Security log verification is failing as the contents of binary log file in LSYS are not as expected PR1587360
- SRX4600 - Packet drop or srxpfe coredump might be observed PR1620773
- SRX5600/5800 - SNMP mib queries may result in occasional response timeouts PR1631149
- No system or chassis alarm will be seen when device booting from backup partition PR1646943
- SRX4600HA might not failover properly due to a hardware failure PR1683213
- SRX1500 chassis cluster port ge-0/0/1 does not work in switching mode PR1690621
- IPSEC tunnel is not getting established back after the execution of 'clear security ike sa' PR1694604
- The user-id entries will not be synced with secondary node PR1701990
- TCP packet drops are seen when services-offload is enabled PR1702138
- The flowd crash and core will be observed when TLS 1.3 session ticket is received on SSL-I PR1705044
- TX would be stuck and no packet can be transferred by the SPC3 card PR1706756
- The ECDSA certificate based websites are not accessible when the SSL proxy is enabled from 22.1R1 onwards PR1709386
- SRX4600 doesn't support ae interfaces PR1711467

- The 'targeted-broadcast' feature will not work on some SRX platforms. PR1711729
- Continuous vmcores observed on the secondary node when committing set system management-instance command PR1712727
- Continuous vmcores observed on the secondary node when committing the "set system management-instance" command PR1713759
- The SSL session drops because of the wrong SNI value PR1716893
- The flowd process crash is observed when the web proxy packet reinjection fails PR1719703
- ISSU is aborted after one node upgrade and flowd process crash is observed PR1722122

Interfaces and Chassis

- SRX1500: Traffic fail seen on irb interface for network control forwarding class when verifying dscp classification based on single and multiple code-points PR1611623
- Incompatible/unsupported configuration is not getting validated correctly during ISSU/normal upgrade causing the traffic loss PR1692404

Intrusion Detection and Prevention (IDP)

- Network outage caused during change in IDP policy PR1705491

J-Web

- [Jweb] "address-book address-book name attach zone" is unexpectedly removed when address-book entry is added or removed by Jweb PR1712454

Layer 2 Ethernet Services

- DHCPv6 client options missing in solicit messages if TLV's exceeds a certain length PR1702831

Network Address Translation (NAT)

- ICMP based traceroute is not showing any hops after SRX when SRX is configured with NAT64 PR1706541
- Some sessions will not be deleted when the NAT rule is deleted from the system PR1712738

Network Management and Monitoring

- source-address on syslog at custom routing-instance not applied right after rebooting PR1689661

Platform and Infrastructure

- Fabric monitoring suspension and control link failure may cause HA cluster outage PR1698797
- vmcores can be seen on SRX5k platforms when the fxp0 interface is configured under management-instance PR1714002

Routing Policy and Firewall Filters

- Packet drops are seen for SRX destined traffic with self-traffic-policy PR1698021
- Security policies go out of sync during ISSU PR1698508
- The flowd process crash is observed with the security policy updated with changing IP address related to the FQDN PR1713576

Routing Protocols

- The traffic drops are seen for the static route after VRRP failover when VRRP VIP is set as next-hop for that static route PR1687884

VPNs

- Routes flapping when configuration changes are applied to custom routing instance PR1654516
- 22.4R1:SRX_RIAD:srx5600:MN_HA:ike cookies didn't change in rekey lifetime expire cases after manual failover PR1690921
- IPsec VPNs will disconnect after ISSU PR1696102
- Mismatch in configured and negotiated proxy-identity parameters can lead to KMD core. PR1699691
- The iked process will crash when VPN tunnels parameters are not matching PR1716092

Migration, Upgrade, and Downgrade Instructions

IN THIS SECTION

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

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

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

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

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

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

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

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

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

Table 10: EOL and EEOL Releases

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

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

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

Junos OS Release Notes for vMX

IN THIS SECTION

These release notes accompany Junos OS Release 22.3R3 for vMX. They describe new and changed features, limitations, and known and resolved problems in the hardware and software.

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

What's New

There are no new features or enhancements to existing features in Junos OS Release 22.3R3 for vMX.

What's Changed

IN THIS SECTION

Learn about what changed in this release for vMX.

General Routing

- **Verified the qualification of `ordered-by-user` in the hierarchies (ACX Series, EX Series, MX Series, QFX Series, SRX Series, vMX, and vSRX)**—The requested hierarchies are reviewed and checked to confirm if they qualify for the `ordered-by-user` list type. If they do not, the `flag autosort` is included in the DDL definition for the list, making it `ordered-by-system`. The hierarchies are now indexed. The benefits from this arrangement are we get accurate data modeling and optimized configuration load in the user interface infrastructure.
- In the past inet6flow.0 was not allowed to be a primary rib in a rib-group. Starting with Release 22.3 this is now allowed.

Junos XML API and Scripting

- **The `xmlns:junos` attribute includes the complete software version string (ACX Series, EX Series, MX Series, PTX Series, QFX Series, SRX Series, vMX, and vSRX)**—The `xmlns:junos` namespace string in XML RPC replies includes the complete software version release number, which is identical to the version

emitted by the `show version` command. In earlier releases, the `xmlns:junos` string includes only partial software version information.

Network Management and Monitoring

- **`operator` login class is restricted from viewing NETCONF trace files that are `no-world-readable` (ACX Series, EX Series, MX Series, PTX Series, QFX Series, SRX Series, vMX, and vSRX)**—When you configure NETCONF tracing options at the `[edit system services netconf traceoptions]` hierarchy level and you restrict file access to the file owner by setting or omitting the `no-world-readable` statement (the default), users assigned to the `operator` login class do not have permissions to view the trace file.

Known Limitations

There are no known limitations in hardware and software in Junos OS 22.3R3 for vMX.

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

Open Issues

There are no known issues in hardware and software in Junos OS Release 22.3R3 for vMX.

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

Resolved Issues

IN THIS SECTION

Learn about the issues fixed in this release for vMX.

General Routing

- PFE syslog tags are missing for the command help syslog "^PFE_?" PR1707504
- Virtual:MVPN tunnel is not synced to back up router. MPVN tunnel interface is missed in show multicast route inet instance BLACK group 225.1.1.1 source-prefix 1.1.1.1 output PR1710323

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 22.3R3 for vRR. They describe new and changed features, limitations, and known and resolved problems in the hardware and software.

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

What's New

There are no new features or enhancements to existing features in Junos OS Release 22.3R3 for vRR.

What's Changed

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

Known Limitations

There are no known limitations in hardware and software in Junos OS 22.3R3 for vRR.

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

To learn more about common BGP or routing known limitations in Junos OS 22.3R3, see "Known Limitations" on page 49 for MX Series routers.

Open Issues

There are no known issues in hardware and software in Junos OS Release 22.3R3 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.

General Routing

- VRR should not advertise entropy-label-capability since it is a non-forwarding device. PR1695530
- The rpd crash is observed when rib-sharding configured. PR1699557
- AIGP not distinguished with BGP-LU when rib-sharding is enabled. PR1710829

Junos OS Release Notes for vSRX

IN THIS SECTION

These release notes accompany Junos OS Release 22.3R3 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 Junos OS Release 22.3R3 for vSRX.

What's Changed

IN THIS SECTION

Learn about what changed in this release for vSRX.

General Routing

- **Verified the qualification of `ordered-by-user` in the hierarchies (ACX Series, EX Series, MX Series, QFX Series, SRX Series, vMX, and vSRX)**—The requested hierarchies are reviewed and checked to confirm if they qualify for the `ordered-by-user` list type. If they do not, the `flag autosort` is included in the DDL definition for the list, making it `ordered-by-system`. The hierarchies are now indexed. The benefits from this arrangement are we get accurate data modeling and optimized configuration load in the user interface infrastructure.

- In the past inet6flow.0 was not allowed to be a primary rib in a rib-group. Starting with Release 22.3 this is now allowed.

Junos XML API and Scripting

- **The `xmlns:junos` attribute includes the complete software version string (ACX Series, EX Series, MX Series, PTX Series, QFX Series, SRX Series, vMX, and vSRX)**—The `xmlns:junos` namespace string in XML RPC replies includes the complete software version release number, which is identical to the version emitted by the `show version` command. In earlier releases, the `xmlns:junos` string includes only partial software version information.

Network Management and Monitoring

- **`operator` login class is restricted from viewing NETCONF trace files that are `no-world-readable` (ACX Series, EX Series, MX Series, PTX Series, QFX Series, SRX Series, vMX, and vSRX)**—When you configure NETCONF tracing options at the `[edit system services netconf traceoptions]` hierarchy level and you restrict file access to the file owner by setting or omitting the `no-world-readable` statement (the default), users assigned to the `operator` login class do not have permissions to view the trace file.

VPNs

- **Limited ECDSA Certificate Support with SSL Proxy (SRX Series and vSRX 3.0)**—With SSL proxy configured on SRX Series firewall and vSRX Virtual firewalls.
  - ECDSA based websites with P-384/P-521 server certificates are not accessible with any root-ca certificate as the security device has limitation to support only P-256 group.
  - When RSA based root-ca and P-384/P-521 ECDSA root-ca certificate is configured, all ECDSA websites will not be accessible as SSL-Terminator is negotiated with RSA, which is why the security device is sending only RSA ciphers and sigalgs to the destination web server while doing the SSL handshake. To ensure both ECDSA and RSA-based websites are accessible along with the RSA root certificate, configure a 256-bits ECDSA root certificate.
  - In some scenarios, even if 256-bit ECDSA root certificate is used in the SSL proxy configuration, ECDSA based websites with P-256 server certificates are not accessible if the server does not support P-256 groups.
  - In other scenarios, even if 256-bit ECDSA root certificate is used in the SSL proxy configuration, ECDSA based websites with P-256 server certificates are not accessible if the server supports sigalgs other than P-256. The issue is seen in hardware offload mode with failing signature verification. As hardware offload for ECDSA certificate is introduced in Junos OS release 22.1R1, this issue will not be observed if you use Junos OS released prior to 22.1R1. Also, the issue is not seen if the SSL-proxy for ECDSA certificate is handled in software.

Known Limitations

Learn about known limitations in this release for vSRX.

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

Chassis Clustering

- Currently max BFD detection interval tested by RLI is 16s. If the detection interval is too large, no BFD down event will be posted by BFDD process to jsrpd process. The jsrpd cannot be aware that ICL once goes down since BFD is the single source of MNHA ICL link failure detection.PR1671622

Platform and Infrastructure

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

Open Issues

Learn about open issues in this release for vSRX.

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

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
- Device does not drop session with server certificate chain more than 6.PR1663062
- Earlier implementation of kvmclock with vDSO (virtual Dynamic Shared Object) which helps avoid the system call overhead for user space applications had problem of time drift, the latest set of changes takes care of initializing the clock after all auxiliary processors are launched so that the clock initialization is accurate.PR1691036
- FIPS mode is not supported in this release for SRX devices.PR1697999
- On SRX platforms, log streaming to the security director cloud fails on TLS when DNS re-query is performed.PR1708116

VPNs

- In some scenarios, the kmd core might be seen when all VPNs are down. PR1336368
- 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.

Application Layer Gateways (ALGs)

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

Flow-Based and Packet-Based Processing

- Expected TCP sequences not found in ICMP6 dump PR1611202
- High latency and packet drops will be observed with the "transmit-rate exact" knob enabled for one or more schedulers of an IFL/IFD PR1692559
- Packet loss is observed for IPSec sessions when PMI is enabled PR1692885
- Packets are dropped because flow sessions will not be created for the MPLS routed traffic PR1703678
- TCP session timeout seen on GRE tunnel PR1708646

General Routing

- Change in few fields of IKE_VPN_UP_ALARM_USER and IKE_VPN_DOWN_ALARM_USER syslogs of IKED PR1657704
- EX/QFX SNMP: jnxOperatingDescr.1.1.0.0 returns blank, but jnxOperatingState.1.1.0.0 returns value. PR1683753
- VLAN tagging does not work for vSRX3.0 on HyperV Windows Server 2019 Datacenter PR1711440
- RSI does not collect PFE related commands on vSRX3 in Chassis cluster PR1711733
- The flowd process crash is observed when the web proxy packet reinjection fails PR1719703

VPNs

- IPsec VPNs will disconnect after ISSU PR1696102

Migration, Upgrade, and Downgrade Instructions

IN THIS SECTION

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

You also can upgrade to Junos OS Release 22.3R2 for vSRX using J-Web (see J-Web) or the Junos Space Network Management Platform (see Junos Space).

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

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

The following limitations apply:

- Direct upgrade of vSRX from Junos OS 15.1X49 Releases to Junos OS Release 19.3 and higher is not supported. For upgrade between other combinations of Junos OS Releases in vSRX and vSRX 3.0, the general Junos OS upgrade policy applies.
- The file system mounted on /var usage must be below 14% of capacity.

  Check this using the following command:

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

  Using the `request system storage cleanup` command might help reach that percentage.
- The Junos OS upgrade image must be placed in the directory /var/host-mnt/var/tmp/. Use the `request system software add /var/host-mnt/var/tmp/<upgrade_image>`
- We recommend that you deploy a new vSRX virtual machine (VM) instead of performing a Junos OS upgrade. That also gives you the option to move from vSRX to the newer and more recommended vSRX 3.0.

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

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

Upgrading Software Packages

To upgrade the software using the CLI:

1. Download the **Junos OS Release 22.3R2 for vSRX .tgz** file from the Juniper Networks website. Note the size of the software image.
2. Verify that you have enough free disk space on the vSRX instance to upload the new software image.

```
root@vsrx> show system storage
       Filesystem              Size       Used      Avail  Capacity   Mounted on
       /dev/vtbd0s1a           694M       433M       206M       68%  /
       devfs                   1.0K       1.0K         0B      100%  /dev
       /dev/md0                1.3G       1.3G         0B      100%  /junos
       /cf                     694M       433M       206M       68%  /junos/cf
       devfs                   1.0K       1.0K         0B      100%  /junos/dev/
       procfs                  4.0K       4.0K         0B      100%  /proc
       /dev/vtbd1s1e           302M        22K       278M        0%  /config
       /dev/vtbd1s1f           2.7G        69M       2.4G        3%  /var
       /dev/vtbd3s2             91M       782K        91M        1%  /var/host
       /dev/md1                302M       1.9M       276M        1%  /mfs
       /var/jail               2.7G        69M       2.4G        3%  /jail/var
       /var/jails/rest-api       2.7G        69M       2.4G      3%  /web-api/var
       /var/log                2.7G        69M       2.4G        3%  /jail/var/log
       devfs                   1.0K       1.0K         0B      100%  /jail/dev
       192.168.1.1:/var/tmp/corefiles       4.5G       125M       4.1G    3%  /var/crash/
corefiles
       192.168.1.1:/var/volatile       1.9G       4.0K       1.9G    0%  /var/log/host
       192.168.1.1:/var/log       4.5G       125M       4.1G     3%  /var/log/hostlogs
```

```
        192.168.1.1:/var/traffic-log       4.5G       125M       4.1G    3%  /var/traffic-log
        192.168.1.1:/var/local       4.5G       125M       4.1G    3%  /var/db/host
        192.168.1.1:/var/db/aamwd       4.5G       125M       4.1G    3%  /var/db/aamwd
        192.168.1.1:/var/db/secinteld       4.5G       125M       4.1G    3%  /var/db/secinteld
```

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

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

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

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

```
root@vsrx> file copy ftp://username:prompt@ftp.hostname.net/pathname/
junos-vsrx-x86-64-20.4-2022-08-08.0_RELEASE_22.3_THROTTLE.tgz /var/crash/corefiles/
```

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

```
root@vsrx> request system software add /var/crash/corefiles/junos-vsrx-
x86-64-22.3-2022-08-08.0_RELEASE_22.3_THROTTLE.tgz no-copy no-validate reboot
Verified junos-vsrx-x86-64-22.3-2022-08-08.0_RELEASE_22.3_THROTTLE signed by
PackageDevelopmentEc_2017 method ECDSA256+SHA256
THIS IS A SIGNED PACKAGE
WARNING:     This package will load JUNOS 22.3 software.
WARNING:     It will save JUNOS configuration files, and SSH keys
WARNING:     (if configured), but erase all other files and information
WARNING:     stored on this machine.  It will attempt to preserve dumps
WARNING:     and log files, but this can not be guaranteed.  This is the
WARNING:     pre-installation stage and all the software is loaded when
WARNING:     you reboot the system.
Saving the config files ...
Pushing Junos image package to the host...
Installing /var/tmp/install-media-srx-mr-vsrx-22.3-2022-08-08.0_RELEASE_22.3_THROTTLE.tgz
Extracting the package ...
total 975372
-rw-r--r-- 1 30426 950 710337073 Oct 19 17:31 junos-srx-mr-
vsrx-22.3-2022-08-08.0_RELEASE_22.3_THROTTLE-app.tgz
-rw-r--r-- 1 30426 950 288433266 Oct 19 17:31 junos-srx-mr-
vsrx-22.3-2022-08-08.0_RELEASE_22.3_THROTTLE-linux.tgz
Setting up Junos host applications for installation ...
============================================
Host OS upgrade is FORCED
Current Host OS version: 3.0.4
New Host OS version: 3.0.4
Min host OS version required for applications: 0.2.4
============================================
Installing Host OS ...
upgrade_platform: --------------------
upgrade_platform: Parameters passed:
upgrade_platform: silent=0
upgrade_platform: package=/var/tmp/junos-srx-mr-vsrx-22.3-2022-08-08.0_RELEASE_22.3_THROTTLE-
```

```
linux.tgz
upgrade_platform: clean install=0
upgrade_platform: clean upgrade=0
upgrade_platform: Need reboot after staging=0
upgrade_platform: --------------------
upgrade_platform:
upgrade_platform: Checking input /var/tmp/junos-srx-mr-
vsrx-22.3-2022-08-08.0_RELEASE_22.3_THROTTLE-linux.tgz ...
upgrade_platform: Input package /var/tmp/junos-srx-mr-
vsrx-22.3-2022-08-08.0_RELEASE_22.3_THROTTLE-linux.tgz is valid.
upgrade_platform: Backing up boot assets..
cp: omitting directory '.'
bzImage-intel-x86-64.bin: OK
initramfs.cpio.gz: OK
version.txt: OK
initrd.cpio.gz: OK
upgrade_platform: Checksum verified and OK...
/boot
upgrade_platform: Backup completed
upgrade_platform: Staging the upgrade package - /var/tmp/junos-srx-mr-
vsrx-22.3-2022-08-08.0_RELEASE_22.3_THROTTLE-linux.tgz..
./
./bzImage-intel-x86-64.bin
./initramfs.cpio.gz
./upgrade_platform
./HOST_COMPAT_VERSION
./version.txt
./initrd.cpio.gz
./linux.checksum
./host-version
bzImage-intel-x86-64.bin: OK
initramfs.cpio.gz: OK
version.txt: OK
upgrade_platform: Checksum verified and OK...
upgrade_platform: Staging of /var/tmp/junos-srx-mr-
vsrx-22.3-2022-08-08.0_RELEASE_22.3_THROTTLE-linux.tgz completed
upgrade_platform: System need *REBOOT* to complete the upgrade
upgrade_platform: Run upgrade_platform with option -r | --rollback to rollback the upgrade
Host OS upgrade staged. Reboot the system to complete installation!
WARNING:     A REBOOT IS REQUIRED TO LOAD THIS SOFTWARE CORRECTLY. Use the
WARNING:     'request system reboot' command when software installation is
WARNING:     complete. To abort the installation, do not reboot your system,
WARNING:     instead use the 'request system software rollback'
```

```
WARNING:     command as soon as this operation completes.
NOTICE: 'pending' set will be activated at next reboot...
Rebooting. Please wait ...
shutdown: [pid 13050]
Shutdown NOW!
*** FINAL System shutdown message from root@ ***
System going down IMMEDIATELY
Shutdown NOW!
System shutdown time has arrived\x07\x07
```

If no errors occur, Junos OS reboots automatically to complete the upgrade process. You have successfully upgraded to Junos OS Release 22.3R2 for vSRX.

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

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

```
--- JUNOS 22.3-2022-08-08.0_RELEASE_22.3_THROTTLE Kernel 64-bit
JNPR-11.0-20171012.170745_fbsd-
At least one package installed on this device has limited support.
Run 'file show /etc/notices/unsupported.txt' for details.
root@:~ # cli
root> show version
Model: vsrx
Junos: 22.3-2022-08-08.0_RELEASE_22.3_THROTTLE
JUNOS OS Kernel 64-bit  [20171012.170745_fbsd-builder_stable_11]
JUNOS OS libs [20171012.170745_fbsd-builder_stable_11]
JUNOS OS runtime [20171012.170745_fbsd-builder_stable_11]
JUNOS OS time zone information [20171012.170745_fbsd-builder_stable_11]
JUNOS OS libs compat32 [20171012.170745_fbsd-builder_stable_11]
JUNOS OS 32-bit compatibility [20171012.170745_fbsd-builder_stable_11]
JUNOS py extensions [20171017.110007_ssd-builder_release_174_throttle]
JUNOS py base [20171017.110007_ssd-builder_release_174_throttle]
JUNOS OS vmguest [20171012.170745_fbsd-builder_stable_11]
JUNOS OS crypto [20171012.170745_fbsd-builder_stable_11]
JUNOS network stack and utilities [20171017.110007_ssd-builder_release_174_throttle]
JUNOS libs [20171017.110007_ssd-builder_release_174_throttle]
JUNOS libs compat32 [20171017.110007_ssd-builder_release_174_throttle]
JUNOS runtime [20171017.110007_ssd-builder_release_174_throttle]
JUNOS Web Management Platform Package [20171017.110007_ssd-builder_release_174_throttle]
```

```
JUNOS srx libs compat32 [20171017.110007_ssd-builder_release_174_throttle]
JUNOS srx runtime [20171017.110007_ssd-builder_release_174_throttle]
JUNOS common platform support [20171017.110007_ssd-builder_release_174_throttle]
JUNOS srx platform support [20171017.110007_ssd-builder_release_174_throttle]
JUNOS mtx network modules [20171017.110007_ssd-builder_release_174_throttle]
JUNOS modules [20171017.110007_ssd-builder_release_174_throttle]
JUNOS srxtvp modules [20171017.110007_ssd-builder_release_174_throttle]
JUNOS srxtvp libs [20171017.110007_ssd-builder_release_174_throttle]
JUNOS srx libs [20171017.110007_ssd-builder_release_174_throttle]
JUNOS srx Data Plane Crypto Support [20171017.110007_ssd-builder_release_174_throttle]
JUNOS daemons [20171017.110007_ssd-builder_release_174_throttle]
JUNOS srx daemons [20171017.110007_ssd-builder_release_174_throttle]
JUNOS Online Documentation [20171017.110007_ssd-builder_release_174_throttle]
JUNOS jail runtime [20171012.170745_fbsd-builder_stable_11]
JUNOS FIPS mode utilities [20171017.110007_ssd-builder_release_174_throttle]
```

Validating the OVA Image

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

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

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

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

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

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

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

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

Table 11: EOL and EEOL Releases

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

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

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

Licensing

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

The major components of the framework are:

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

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

Finding More Information

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

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

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

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

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

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

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

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

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

Requesting Technical Support

IN THIS SECTION

Technical product support is available through the Juniper Networks Technical Assistance Center (JTAC). If you are a customer with an active Juniper Care or Partner Support Services support contract, or are

covered under warranty, and need post-sales technical support, you can access our tools and resources online or open a case with JTAC.

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

Self-Help Online Tools and Resources

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

- Find CSC offerings: https://www.juniper.net/customers/support/
- Search for known bugs: https://prsearch.juniper.net/
- Find product documentation: https://www.juniper.net/documentation/
- Find solutions and answer questions using our Knowledge Base: https://kb.juniper.net/
- Download the latest versions of software and review release notes: https://www.juniper.net/customers/csc/software/
- Search technical bulletins for relevant hardware and software notifications: https://kb.juniper.net/InfoCenter/
- Join and participate in the Juniper Networks Community Forum: https://www.juniper.net/company/communities/
- Create a service request online: https://myjuniper.juniper.net/

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

Creating a Service Request with JTAC

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

- Visit https://myjuniper.juniper.net/
- Call 1-888-314-JTAC (1-888-314-5822 toll-free in the USA, Canada, and Mexico).

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

Revision History

16 November 2023—Revision 3, Junos OS Release 22.3R3

20 July 2023—Revision 2, Junos OS Release 22.3R3

16 June 2023—Revision 1, Junos OS Release 22.3R3

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.