Release Notes

Published

2023-08-09

Junos® OS Release 22.1R1

SUPPORTED PLATFORMS

ACX Series, cPCE, cRPD, cSRX, EX Series, JRR Series, Juniper Secure Connect, Junos Fusion, MX Series, NFX Series, PTX Series, QFX Series, SRX Series, vMX, vRR, and vSRX

KEY FEATURES

- See Key Features in Junos OS Release 22.1 to quickly learn about the most important Junos OS features and how you can deploy them in your network.

SOFTWARE HIGHLIGHTS

- Custom mode (NFX150 devices)
- NDP and DAD proxy support on multiple interfaces (SRX Series, vSRX, and vSRX 3.0)
- Router advertisement proxy support (NFX Series, SRX Series, vSRX, and vSRX 3.0)

Engineering
Simplicity

Table of Contents

Junos OS Release Notes for JRR Series

Junos OS Release Notes for Juniper Secure Connect

Junos OS Release Notes for Junos Fusion for Enterprise

Junos OS Release Notes for Junos Fusion for Provider Edge

Junos OS Release Notes for MX Series

Junos OS Release Notes for NFX Series

Junos OS Release Notes for SRX Series

Introduction

Junos OS runs on the following Juniper Networks® hardware: ACX Series, cPCE, 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 22.1R1 for the ACX Series, Containerized Path Computation Engine (cPCE), Containerized Routing Protocol Process (cRPD), cSRX Container Firewall (cSRX), EX Series, JRR Series, Juniper Secure Connect, Junos Fusion Enterprise, Junos Fusion Provider Edge, MX Series, NFX Series, PTX Series, QFX Series, SRX Series, virtual MX Series router (vMX), Virtual Route Reflector (vRR), and vSRX Virtual Firewall (vSRX). They describe new and changed features, limitations, and known and resolved problems in the hardware and software.

Key Features in Junos OS Release 22.1

Start here to learn about the key features in Junos OS Release 22.1. For more information about a feature, click the link in the feature description.

- **Perpetual PoE (EX4400-24MP, EX4400-24P, EX4400-48MP, and EX4400-48P)**—Starting in Junos OS Release 22.1R1, you can configure perpetual PoE on EX4400 switches that support Power over Ethernet (PoE). Perpetual PoE provides uninterrupted power to connected powered devices even when the power-sourcing equipment switch is rebooting.

  [See Configuring Perpetual PoE and Fast PoE.]

- **Support for GeoIP filtering, global allowlist, and global blocklist with Juniper ATP Cloud (MX240, MX480, and MX960)**—Starting in Junos OS Release 22.1R1, you can configure the Security Intelligence process (IPFD) on MX Series routers to fetch the GeoIP feeds from Juniper ATP Cloud. You can then use the feeds to prevent devices from communicating with IP addresses belonging to specific countries.

  You can define:

  - A profile to dynamically fetch GeoIP feeds. Include the `geo-ip rule match country` *`country-name`* statement at the `[edit services web-filter profile` *`profile-name`* `security-intelligence-policy]` hierarchy level.

  - A template to dynamically fetch GeoIP feeds. Include the `geo-ip rule match group` *`group-name`* statement at the `[edit services web-filter profile` *`profile-name`* `url-filter-template` *`template-name`* `security-intelligence-policy]` hierarchy level.

You can configure a global allowlist by configuring the `white-list (IP-address-list | *file-name*)` statement at the `edit services web-filter profile *profile-name* security-intelligence-policy` hierarchy level. You can configure a global blocklist by configuring the `black-list (IP-address-list | *file-name*)` statement at the `edit services web-filter profile *profile-name* security-intelligence-policy` hierarchy level. Here, *`IP-address-list`* refers to the name of the list specified at the `[edit services web-filter]` hierarchy level. The *`file-name`* option refers to the name of the file where the list of the IP addresses to be allowed or blocked is specified. The file must be in the **/var/db/url-filterd** directory and must have the same name as in the configuration.

[See Integration of Juniper ATP Cloud and Web filtering on MX Routers .]

- **Avoid microloops in OSPFv2 segment routing networks (ACX5448, ACX6360, MX Series, PTX Series, and QFX10002)** —Starting in Junos OS Release 22.1R1, you can enable post-convergence path calculation on a device to avoid microloops if a link or metric changes in an OSPFv2 segment routing network. Note that microloop avoidance is not a replacement for local repair mechanisms such as topology-independent loop-free alternate (TI-LFA), which detects local failure very fast and activates a precomputed loop-free alternative path.

  To configure microloop avoidance in an OSPFv2 segment routing network, include the `maximum-labels` and `delay *milliseconds*` statements at the `[edit protocols ospf spf-options microloop avoidance post-convergence-path]` hierarchy level.

  [See How to Configure Microloop Avoidance for OSPFv2 SR Networks.]

Junos OS Release Notes for ACX Series

IN THIS SECTION

These release notes accompany Junos OS Release 22.1R1 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

IN THIS SECTION

Learn about new features introduced in this release for ACX Series routers.

What's New in 22.1R1

IN THIS SECTION

Learn about new features or enhancements to existing features in this release for the ACX Series.

Junos Telemetry Interface

- **Collect telemetry statistics for routes programmed through JET API (ACX710, ACX5448, MX150, MX204, MX480, MX960, MX2008, MX2010, MX2020, MX10003, MX10008, MX10016, PTX1000, and PTX10002)**—Starting in Junos OS Release 22.1R1, you can collect telemetry statistics for forwarded routing packets programmed by means of Juniper Extension Toolkit (JET) APIs and JTI. GRE tunneling and packet translation between IPv6 and IPv4, introduced in Junos OS Release 21.2R1, supports the routing statistics collected by this feature.

  [See JET APIs on Juniper EngNet and Telemetry Sensor Explorer .]

Additional Features

We've extended support for the following features to these platforms.

- **OpenConfig LACP and LLDP configuration support** (ACX5448 router, EX4650, and EX4650-48Y-VC switches, MX480, MX960, MX10003, and PTX10008 routers, , QFX10002-60C, QFX5110, QFX5110-VC, QFX5110-VCF, QFX5120-32C, QFX5120-48T, QFX5120-48T-VC, QFX5120-48Y, QFX5120-48Y-VC, QFX5120-48YM, QFX5200, QFX5210, , QFX10002, QFX10003, QFX10008, and QFX10016 switches). OpenConfig configuration support based on the OpenConfig data models openconfig-lacp.yang and openconfig-lldp.yang.

  [See Mapping OpenConfig LLDP Commands to Junos Configuration and OpenConfig User Guide.]

- **System OpenConfig configuration support and gNMI mixed-mode support** (ACX5448, MX240, MX480, MX960, MX10003, MX10008, MX10016, MX2008, MX2010, MX2020, and PTX10002)

  [See OpenConfig User Guide].

- **VLAN-level MACsec on logical interfaces** (EX9253 and QFX5120-48YM)

  [See Media Access Control Security (MACsec) over WAN.]

What's Changed

IN THIS SECTION

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

What's Changed in Release 22.1R1

IN THIS SECTION

Junos OS API and Scripting

- **The `<request-system-zeroize>` RPC response indicates when the device successfully initiates the requested operation (ACX Series, EX Series, MX Series, PTX Series, QFX Series, SRX Series, vMX, and vSRX)**—When the `<request-system-zeroize>` RPC successfully initiates the zeroize operation, the device emits the `<system-zeroize-status>zeroizing re0</system-zeroize-status>` response tag to indicate that the process has started. If the device fails to initiate the zeroize operation, the device does not emit the `<system-zeroize-status>` response tag.

Network Management and Monitoring

- **Junos XML protocol Perl modules deprecated (ACX Series, EX Series, MX Series, PTX Series, QFX Series, SRX Series, vMX, and vSRX)**—We no longer provide the Junos XML protocol Perl client for download. To use Perl to manage Junos devices, use the NETCONF Perl library instead.

  [See Understanding the NETCONF Perl Client and Sample Scripts.]

- **Changes when deactivating or deleting instances of the ephemeral configuration database (ACX Series, EX Series, MX Series, PTX Series, QFX Series, SRX Series, vMX, and vSRX)**—The following changes apply when you deactivate or delete ephemeral database instances in the static configuration database:

  - When you deactivate the entire `[edit system configuration-database ephemeral]` hierarchy level, the device deletes the files and corresponding configuration data for all user-defined ephemeral instances. In earlier releases, the files and configuration data are preserved; however, the configuration data is not merged with the static configuration database.

  - When you delete an ephemeral instance in the static configuration database, the instance's configuration files are also deleted. In earlier releases, the configuration files are preserved.

  - You can delete the files and corresponding configuration data for the default ephemeral database instance by configuring the `delete-ephemeral-default` statement in conjunction with the `ignore-ephemeral-default` statement at the `[edit system configuration-database ephemeral]` hierarchy level.

  [See Enable and Configure Instances of the Ephemeral Configuration Database.]

Routing Protocols

- To achieve consistency among resource paths, the resource path **/mpls/signalling-protocols/segment-routing/aggregate-sid-counters/aggregate-sid-counter *ip-addr='address'*/state/counters*name='name'*/out-pkts/ is changed to /mpls/signaling-protocols/segment-routing/aggregate-sid-counters/aggregate-sid-counter*ip-addr='address'*/state/counters*name='name'*/**. The leaf `out-pkts` is removed from the end of the path, and `signalling` is changed to `signaling` (with one "l").

User Interface and Configuration

- **Load JSON configuration data with unordered list entries (ACX Series, EX Series, MX Series, PTX Series, QFX Series, SRX Series, vMX, and vSRX)**—The Junos schema requires that list keys precede any other siblings within a list entry and appear in the order specified by the schema. Junos devices provide two options to load JSON configuration data that contains unordered list entries:

  - Use the `request system convert-json-configuration` operational mode command to produce JSON configuration data with ordered list entries before loading the data on the device.

  - Configure the `reorder-list-keys` statement at the `[edit system configuration input format json]` hierarchy level. After you configure the statement, you can load JSON configuration data with unordered list entries, and the device reorders the list keys as required by the Junos schema during the load operation.

  When you configure the `reorder-list-keys` statement, the load operation can take significantly longer to parse the configuration, depending on the size of the configuration and number of lists. Therefore, for large configurations or configurations with many lists, we recommend using the `request system convert-json-configuration` command instead of the `reorder-list-keys` statement.

  [See json and request system convert-json-configuration.]

Known Limitations

IN THIS SECTION

Learn about known limitations in Junos OS Release 22.1R1 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

- Delay protect fails along with primary to fallback conversion. PR1634584

Infrastructure

- When upgrading from Junos OS Release 21.2 and earlier to Junos OS Release 21.2 and later, validation and upgrade fails. Upgrading requires the use of the `no-validate` command. PR1568757

Open Issues

Learn about open issues in Junos OS Release 22.1R1 for ACX Series routers.

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

General Routing

- Due to BRCM KBP issue, the route lookup might fail. PR1533513
- On ACX5448 routers with VM host-based platforms, starting with Junos OS Release 21.4R1 or later, you need the ssh and root login for copying line card image (chspmb.elf for MX2008) from Junos VM to Linux host during installation. You need the ssh and root login during installation. Use `deny-password`

instead of deny as default root-login option under ssh configuration to allow internal trusted communication. PR1629943

- Junos OS does not support Hierarchical-scheduler (HQOS) on MPLS (core facing) interface on ACX5448 routers before Junos OS Release 22.2. Enabling HQOS on MPLS core facing interface causes unexpected traffic forwarding behavior. PR1630086

- Late drops are not at par with PN configured. PR1630724

- On ACX5048 and ACX5096 routers, Junos OS does not support interface speed 10m on 1G interface. PR1633226

- When you configure multihop BFD, delegated BFD sessions do not come up. PR1633395

- When ACX710 and ACX5448 routers work as the PE device nodes in the Layer 3 VPN environment, the router might stop forwarding the Layer 3 VPN traffic after core-facing link flaps. This occurs due to a race condition that happens during the Layer 3 VPN next-hop programming in the Packet Forwarding Engine. PR1635801

- On ACX platforms, traffic issue might be observed with downstream devices when you configure the Precision Time Protocol(PTP) (G.8275.1 PTP profile) along with PHY timestamping and Multiprotocol Label Switching (MPLS) terminated on 10G interface. The transit PTP ipv4 packets gets updated with incorrect Correction Factor(CF). This issue could be restored by disabling PHY stamping. However, disabling might impact the PTP performance. PR1612429

Resolved Issues

IN THIS SECTION

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

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

Resolved Issues: 22.1R1

IN THIS SECTION

General Routing

- On ACX5448 routers, the BFD session status goes in to the `Init` state after system reboot. This issue occurs when you have both the CFM and BFD configured on the system. PR1552235

- The MPC7E, MPC10E, MX-SPC3, and LC2103 line cards might become offline when the device runs on the FIPS mode. PR1576577

- On ACX5448 routers, CFM does not go in to the `OK` state after the router reboots. PR1602489

- On ACX5448 routers, RED-dropped packets might be observed if you configure hierarchical-scheduler. PR1603622

- On ACX5096 routers, the output pps traffic appears on the deactivated interfaces. PR1608827

- ACX710 routers running Junos OS 21.2R1 and later might experience kernel crash. PR1608852

- On ACX5448 and ACX710 routers, traffic might be dropped. PR1612026

- The routing protocol engine CPU becomes nonresponsive at 100 percent. PR1612387

- Interface state resets after a Packet Forwarding Engine restarts. PR1613314

- On ACX5448 routers, unknown SMART attributes for StorFly VSFBM6CC100G-JUN1 SSD might occur. PR1614068

- Packet fragmentation might occur when you configure MTU for the logical interface. PR1614449

- On ACX5448 routers at rates above 4GB, there might be mismatches in statistics between the physical and logical interfaces. PR1614550

- When configuring vlan-id-range/list for the aggregated Ethernet interface of l2ckt, traffic forwarding occurs for the first VLAN. PR1616147

- Traffic might not be forwarded after failover in the L2circuit hot standby mode. PR1616892

- On ACX710 and ACX5448 routers, the Packet Forwarding Engine daemon crashes if you disable the standby interface in the Layer-2 Circuit Pseudowire redundancy scenario. PR1617287

- Host-outbound-traffic might be placed in the incorrect queue. PR1619174

- Traffic might get equally load-balanced irrespective of the scheduler configuration. PR1620137

- Six to eight seconds of delay occurs when the receiver switches in between the groups. PR1620685

- Traffic forwarding to one of the the Single homed PE or ACX does not occur after you change the vlan-id under the routing instance. PR1621036

- On ACX5448 and ACX710 routers with the Layer 3 VPN scenarios, after multiple core links or protocol flaps, the error messages might be generated. PR1621425

- SNMP interface reports temperature instead of the RX alarms. PR1621894

- On ACX5448 routers, the smartd configurations do not get applied. PR1623359

- On ACX5448 routers, EXP rewrite does not work in the Layer 3 VPN scenario when you configure the mf filter. PR1623922

- On ACX5000 routers, the Local fault and Remote fault signaling does not get logged on **/var/log/messages**. PR1624761

- Unicast packet loss might be observed due to control-word configuration. PR1626058

- VPLS traffic loss might be observed post route flap. PR1626267

- The Packet Forwarding Engine might crash after the device reboots or Packet Forwarding Engine restarts. PR1626503

- On ACX2000 routers, the output packet statistics do are not increment on the unit even after configuringthe statistics. PR1627040

- On ACX5048 routers, filters reporting TCAM errors are not installed in the hardware after the upgrade from Junos OS Release 17.4R2-S8 to Junos OS Release 20.4R3. PR1630280

- On ACX710 routers running G.8275.2, the router becomes nonresponsive at the `PTP Acquiring` state if the connection gets through some timing unaware nodes. PR1632761

- The storm-control rate-limit might not work with VPLS policer under IFL. PR1633427

- DHCP clients might not come online for the IRB+VLAN/EVPN scenario. PR1633778

- IS-IS last transition time never increments. PR1634747

- On ACX5448 and ACX710 outers, the IPv6 BFD session over the aggregated Ethernet interface might stay down. PR1635020

- On ACX5448 routers, the PEM overload alarm threshold gets displayed incorrectly. PR1636222
- On ACX5448 routers with ESI configured, locally switched traffic might be dropped . PR1638386
- On ACX5448 and ACX710 routers, the Layer 3 interface creation might fail. PR1638581
- IGMP snooping configuration drops layer 2 VPN multicast traffic. PR1628600
- The LACP might delay with an `aggregate wait time` message for more than 1 second. PR1635763
- The KRT queue might get stuck with the `ENOMEM -- Cannot allocate memory` error message. PR1642172

Platform and Infrastructure

- The vmxt_lnx process generates a core file at `topo_get_link jnh_features_get_jnh jnh_stream_attach` . PR1638166

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 cPCE

IN THIS SECTION

These release notes accompany Junos OS Release 22.1R1 for cPCE. They describe new and changed features, limitations, and known and resolved problems in the hardware and software.

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

What's New

IN THIS SECTION

Learn about new features introduced in this release for cPCE.

What's New in 22.1R1

IN THIS SECTION

Learn about new features or enhancements to existing features in this release for cPCE.

Additional Features

We've extended support for the following features to these platforms.

- **VLAN-level MACsec on logical interfaces** (EX9253 and QFX5120-48YM)

  [See Media Access Control Security (MACsec) over WAN.]

What's Changed

IN THIS SECTION

Learn about what changed in the Junos OS main and maintenance releases for cPCE.

What's Changed in Release 22.1R1

There are no changes in behavior and syntax in Junos OS Release 22.1R1 for cPCE.

Known Limitations

IN THIS SECTION

Learn about known limitations in Junos OS 22.1R1 release for cPCE.

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

cPCE

- Compute offload is not supported for static-label-switched-path lsp (static LSPs), transit, egress, container, RSVP dynamic tunnel LSPs.
- For compute offload, LSPs needs to originate from master routing instance. Compute offload from non-master routing instance is not supported.
- MPLS LSP destination IP address needs to be primary loopback of egress. Externally controlled LSP will not come up when egress secondary loopback is used as destination IP address.
- Configuring explicit EXPLICIT-ROUTE object (EROs) for compute offload is not supported.
- For externally controlled LSPs, any configuration change is not applied after the LSP is already delegated.
- Primary and secondary paths for protection are not supported. The LSP can be configured on PCC using just one primary path.

Open Issues

There are no known issues in hardware and software in Junos OS Release 22.1R1 for cPCE.

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 which issues were resolved in the Junos OS main and maintenance releases for cPCE.

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

Resolved Issues: 22.1R1

There are no resolved issues in Junos OS Release 22.1R1 for cPCE.

Junos OS Release Notes for cRPD

IN THIS SECTION

These release notes accompany Junos OS Release 22.1R1 for the containerized routing protocol process (cRPD) container. They describe new and changed features, limitations, and known and resolved problems in the hardware and software.

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

What's New

IN THIS SECTION

Learn about new features introduced in this release for cRPD.

What's New in 22.1R1

IN THIS SECTION

Learn about new features or enhancements to existing features in this release for cRPD.

MPLS

- **Conditional RSVP LSP metrics (cRPD, MX960, PTX1000, and QFX10002)**—Starting in Junos OS Release 22.1R1, you can configure conditional metrics for local statically configured label-switched paths (LSPs). The conditional metrics are based on the dynamically changing IGP metric. Junos OS changes the LSP metric to the configured conditional metric that corresponds to the highest threshold reached by the IGP metric. You can configure up to four conditional metrics for an LSP.

  By default, the IGP metric of routes configured with the `install` statement is the IGP metric value of the LSP destination route. If you configure the `track-igp-metric <install-v4-prefixes> <install-v6-prefixes>` statement at the `[edit protocols mpls]` or `[edit protocols mpls label-switched-path` *`lsp-name`*`]` hierarchy level, routes installed by IGP use the IGP metric of the prefix instead.

  Use the `conditional igp-metric-threshold` *`threshold-metric-value static-metric-condition-value`* statement at the `[edit protocols mpls label-switched-path` *`lsp-name`* `metric]` hierarchy level to configure this feature. To check whether the conditional metric is configured, use the `show mpls lsp extensive` command.

  [See Configuring LSP Metrics, metric (Protocols MPLS), track-igp-metric (LSP), conditional-metric, and show mpls lsp extensive.]

Routing Protocols

- **Support for adaptive RSVP update threshold (cRPD, MX240, MX480, MX960, PTX1000, PTX10008, QFX10002-60C, and QFX10008)**—Starting in Junos OS Release 22.1R1, you can configure the RSVP update threshold percentage and threshold value to adaptively pace IGP updates. You can configure a lower frequency when the adaptive bandwidth is higher and configure a higher frequency when the bandwidth is lower.

  You can enable the threshold percentage by using the `update-threshold adaptive limit` *`limit`* `threshold-percent` *`percentage`* configuration, and threshold value by using the `update-threshold adaptive limit` *`limit`* `threshold-value` *`value`* `configuration` at the `edit protocols rsvp interface` hierarchy level.

NOTE: You cannot configure both `threshold-percent` and `threshold-value` simultaneously on the same interface.

[See update-threshold.]

What's Changed

IN THIS SECTION

Learn about what changed in the Junos OS main and maintenance releases for cRPD.

What’s Changed in Release 22.1R1

There are no changes in behavior and syntax in Junos OS Release 22.1R1 for cRPD.

Known Limitations

There are no known limitations in hardware and software in Junos OS Release 22.1R1 for cRPD.

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 22.1R1 for cRPD.

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 which issues were resolved in the Junos OS main and maintenance releases for cRPD.

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

Resolved Issues: 22.1R1

IN THIS SECTION

MPLS

- LDPv6 routes preference is not updated after modifying LDP route preference. PR1618785

Routing Protocols

- The BGP ECMP might not work and multipath route wont be created. PR1630220

Junos OS Release Notes for cSRX

IN THIS SECTION

These release notes accompany Junos OS Release 22.1R1 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

IN THIS SECTION

Learn about new features introduced in this release for cSRX.

What's New in 22.1R1

IN THIS SECTION

Learn about new features or enhancements to existing features in this release for cSRX.

Network Management and Monitoring

- **Enhancement to <get-syslog-events> RPC with additional filtering options (cSRX, MX Series routers and vMX, SRX300, SRX320, SRX340, SRX345, SRX380, SRX550HM, SRX4100, SRX4200, SRX4600, SRX5400, SRX5600, SRX5800, vSRX, and vSRX 3.0)**—In Junos OS Release 22.1R1, we've introduced the following new tags in the `<get-syslog-events>` RPC. These tags provide additional options for filtering system log messages.

  ```
  <start-count></start-count>
  <end-count></end-count>
  <total-events/>
  <pretty/>
  <print-json/>
  ```

  [See Overview of Junos OS System Log Messages and syslog (System).]

What's Changed

IN THIS SECTION

Learn about what changed in the Junos OS main and maintenance releases for cSRX.

What's Changed in Release 22.1R1

There are no changes in behavior and syntax in Junos OS Release 22.1R1 for cSRX.

Known Limitations

There are no known limitations in hardware and software in Junos OS 22.1R1 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 22.1R1 for cSRX.

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

Resolved Issues

IN THIS SECTION

Learn which issues were resolved in the Junos OS main and maintenance releases 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: 22.1R1

There are no resolved issues in Junos OS Release 22.1R1 for cSRX.

Junos OS Release Notes for EX Series

IN THIS SECTION

These release notes accompany Junos OS Release 22.1R1 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

IN THIS SECTION

Learn about new features introduced in this release for EX Series switches.

What's New in 22.1R1

IN THIS SECTION

Learn about new features or enhancements to existing features in this release for EX Series Switches.

Additional Features

We've extended support for the following features to these platforms.

- **Support for IEEE 802.1ag CFM on service provider (SP) interfaces and Q-in-Q (point-to-point) interfaces** (EX2300, EX4300-MP, EX4400-48F, EX4400-48MP, and EX4400-48P)

  [See Introduction to OAM Connectivity Fault Management (CFM).]

- **Support for 40GbE QSFPP optics** (EX4400-24MP, EX4400-24P, EX4400-24T, EX4400-48F, EX4400-48MP, EX4400-48P, and EX4400-48T). You can use QSFPP optics to channelize 40-Gbps speed on EX4400 switches.

  [See Hardware Compatibility Tool.]

- **Supported transceivers, optical interfaces, and DAC cables** (EX Series, MX Series, and QFX Series). Select your product in the Hardware Compatibility Tool to view supported transceivers, optical interfaces, and DAC cables for your platform or interface module. We update the HCT and provide the first supported release information when the optic becomes available.

- **VLAN-level MACsec on logical interfaces** (EX9253 and QFX5120-48YM)

  [See Media Access Control Security (MACsec) over WAN.]

Class of Service

- **Support for configuring multiple queues as strict-high priority (EX4400-24MP, EX4400-24P, EX4400-24T, EX4400-48F, EX4400-48MP, EX4400-48P, EX4400-48T, EX4650, EX4650-48Y-VC, QFX5120-32C, QFX5120-48T, QFX5120-48T-VC, QFX5120-48Y, QFX5120-48Y-VC, and QFX5120-48YM)**—Starting in Junos OS Release 22.1R1, you can configure multiple strict-high priority queues in which the queue with the highest priority value gets precedence.

  [See Traffic Management User Guide.]

Dynamic Host Configuration Protocol

- **Support for prefix delegation visibility with DHCPv6 snooping (EX2300)**—Starting in Junos OS Release 22.1R1, the DHCPv6 snoop table displays delegated prefix details. The `show dhcp-security ipv6 binding` command will display IA_PD details, whenever present, as a separate snoop entry with a type field against it. The type field identifies kind of snoop entry. You can use this information to infer the per-routing-instance and per-address-family counts.

  > **NOTE**: Prefix delegation is relevant only for the IPv6 address family.

  [See show dhcp-security ipv6 binding.]

Ethernet Switching and Bridging

- **Support for alternate LLDP destination addresses (EX2300, EX2300-C, EX3400, EX4400-24MP, EX4400-24P, EX4400-24T, EX4400-48MP, EX4400-48P, EX4400-48T, EX4600, EX4650, and EX9200)**—Starting in Junos OS Release 22.1R1, we support alternate LLDP destination MAC addresses as specified in the IEEE 802.1AB-2016 standard. Our new CLI statements ensure that LLDP packets arrive at the correct destination MAC address. If you don't specify a configuration, then the the device sends the packets to the nearest-bridge MAC address, which is 01:80:c2:00:00:0e. The new CLI statements are:

  - `set protocols lldp dest-mac-type <mac-type>`—For packets sent out of all interfaces.

  - `set protocols lldp interface <intf-name> dest-mac-type <mac-type>`—For packets sent out of a specific interface.

  [See Configuring LLDP.]

EVPN

- **DHCP security on Layer 3 VXLAN gateways in an EVPN-VXLAN edge-routed overlay (EX4300-MP, EX4300-MP VC, EX4400, EX4400 VC)**—Starting in Junos OS Release 22.1R1, you can configure DHCP security features on devices that function as Layer 3 VXLAN gateways in an EVPN-VXLAN edge-routed overlay. DHCP security is supported on customer edge (CE)-facing interfaces, and DHCP relay handles Layer 3 routing. The listed devices support the following features:

  - DHCPv4 and DHCPv6 snooping. [See Enabling DHCP Snooping.]

  - Dynamic ARP inspection. [See Enabling Dynamic ARP Inspection.]

  - Neighbor discovery inspection. [See Enabling ND Inspection.]

  - IPv4 and IPv6 source guard. [See Configuring IP Source Guard.]

- **Loop detection for EVPN-VXLAN fabrics (EX4650)**—Starting in Junos OS Release 22.1R1, you can configure loop detection on the server-facing Layer 2 interfaces on EX4300-48MP leaf devices in an EVPN-VXLAN fabric. This feature can detect the following types of Ethernet loops:

  - A loop between two interfaces with different Ethernet segment identifiers (ESIs), usually caused if you miswire fabric components.

  - A loop between two interfaces with the same ESI, usually caused if you miswire a third-party switch to the fabric.

  After you enable loop detection, the interfaces periodically send multicast loop-detection protocol data units (PDUs). If a loop detection-enabled interface receives a PDU, the device detects a loop, which triggers the configured action to break the loop. For example, if you configure the `interface-down` action, the device brings down the interface. After the `revert-interval` timer expires, the device reverts the action and brings the interface back up again.

  [See loop-detect (EVPN).]

Interfaces

- **Perpetual PoE (EX4400-24MP, EX4400-24P, EX4400-48MP, and EX4400-48P)**—Starting in Junos OS Release 22.1R1, you can configure perpetual PoE on EX4400 switches that support Power over Ethernet (PoE). Perpetual PoE provides uninterrupted power to connected powered devices even when the power-sourcing equipment switch is rebooting.

  [See Configuring Perpetual PoE and Fast PoE.]

- **Support for 100M optics on 1GbE ports (EX4400-48F)**—Starting in Junos OS Release 22.1R1, we support 1-Gbps speed on the first 36 ports of PIC 0.

  Use the following 100M optics on these 1GbE ports of EX4400-48F switches:

  - EX-SFP-1FE-FX

  - EX-SFP-1FE-LX

  - EX-SFP-FE20KT13R15

  - EX-SFP-FE20KT15R13

  [See Port Speed for EX4400-48F.]

Junos Telemetry Interface

- **Packet Forwarding Engine DDoS sensor support with JTI (EX4650, QFX5110, QFX5120-32C, QFX5120-48T, QFX5120-48Y, QFX5120-48YM, QFX5210 and QFX5200)**—Starting in Junos OS Release 22.1R1, JTI supports distributed denial-of-service (DDoS) telemetry sensors. To stream

DDoS statistics from a device to a collector, include the resource path **/junos/system/linecard/ddos/**) in a subscription. You can stream statistics using UDP (native) or Juniper proprietary gRPC and gNMI. This feature supports the Openconfig data model **junos/ui/openconfig/yang/junos-ddos.yang**.

Currently, there are 45 packet types for DDoS. To maintain a reasonably sized data stream, data is exported for all protocols that have traffic using the zero-suppression model.

[See sensor (Junos Telemetry Interface) and Guidelines for gRPC and gNMI Sensors (Junos Telemetry Interface).]

Software Installation and Upgrade

What's Changed

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

What’s Changed in Release 22.1R1

Junos OS API and Scripting

- **The `<request-system-zeroize>` RPC response indicates when the device successfully initiates the requested operation (ACX Series, EX Series, MX Series, PTX Series, QFX Series, SRX Series, vMX, and vSRX)**—When the `<request-system-zeroize>` RPC successfully initiates the zeroize operation, the device emits the `<system-zeroize-status>zeroizing re0</system-zeroize-status>` response tag to indicate that the process has started. If the device fails to initiate the zeroize operation, the device does not emit the `<system-zeroize-status>` response tag.

Network Management and Monitoring

- **Junos XML protocol Perl modules deprecated (ACX Series, EX Series, MX Series, PTX Series, QFX Series, SRX Series, vMX, and vSRX)**—We no longer provide the Junos XML protocol Perl client for download. To use Perl to manage Junos devices, use the NETCONF Perl library instead.

  [See Understanding the NETCONF Perl Client and Sample Scripts.]

- **Changes when deactivating or deleting instances of the ephemeral configuration database (ACX Series, EX Series, MX Series, PTX Series, QFX Series, SRX Series, vMX, and vSRX)**—The following changes apply when you deactivate or delete ephemeral database instances in the static configuration database:

  - When you deactivate the entire `[edit system configuration-database ephemeral]` hierarchy level, the device deletes the files and corresponding configuration data for all user-defined ephemeral instances. In earlier releases, the files and configuration data are preserved; however, the configuration data is not merged with the static configuration database.

  - When you delete an ephemeral instance in the static configuration database, the instance's configuration files are also deleted. In earlier releases, the configuration files are preserved.

  - You can delete the files and corresponding configuration data for the default ephemeral database instance by configuring the `delete-ephemeral-default` statement in conjunction with the `ignore-ephemeral-default` statement at the `[edit system configuration-database ephemeral]` hierarchy level.

  [See Enable and Configure Instances of the Ephemeral Configuration Database.]

- **Support for automatically synchronizing an ephemeral instance configuration upon committing the instance (EX Series, MX Series, MX Series Virtual Chassis, PTX Series, QFX Series, and vMX)**—You can configure an ephemeral database instance to synchronize its configuration to the other Routing Engine every time you commit the ephemeral instance on a dual Routing Engine device or an MX Series Virtual Chassis. To automatically synchronize the instance when you commit it, include the `synchronize` statement at the `[edit system commit]` hierarchy level in the ephemeral instance's configuration.

  [See Commit and Synchronize Ephemeral Configuration Data Using the NETCONF or Junos XML Protocol.]

User Interface and Configuration

- **Load JSON configuration data with unordered list entries (ACX Series, EX Series, MX Series, PTX Series, QFX Series, SRX Series, vMX, and vSRX)**—The Junos schema requires that list keys precede any other siblings within a list entry and appear in the order specified by the schema. Junos devices provide two options to load JSON configuration data that contains unordered list entries:

  - Use the `request system convert-json-configuration` operational mode command to produce JSON configuration data with ordered list entries before loading the data on the device.

  - Configure the `reorder-list-keys` statement at the `[edit system configuration input format json]` hierarchy level. After you configure the statement, you can load JSON configuration data with unordered list entries, and the device reorders the list keys as required by the Junos schema during the load operation.

  When you configure the `reorder-list-keys` statement, the load operation can take significantly longer to parse the configuration, depending on the size of the configuration and number of lists. Therefore, for large configurations or configurations with many lists, we recommend using the `request system convert-json-configuration` command instead of the `reorder-list-keys` statement.

  [See json and request system convert-json-configuration.]

Known Limitations

IN THIS SECTION

Learn about known limitations in Junos OS Release 22.1R1 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

- On QFX5000, in an EVPN_VXLAN deployment, BUM traffic replication over VTEP might send out more packets than expected. PR1570689

- On EX4600 and QFX5xx0 platforms, you should configure only one static arp with multicast-mac entry per IRB interface. If you configure more than one static ARP with multicast MAC entry per IRB interface, then the packets with different destination IP with static multicast MAC will always go out with any one of the multicast mac configured in the system. PR1621901
- Unified ISSU on QFX5120-48Y and EX4650 switches will not be supported if there is a change in the Cancun versions of the chipset SDKs between the releases. This is a product limitation as change in the Cancun firmware leads to the chip reset and hence impacts ISSU. The Cancun versions in the chipset SDKs should be the same between two Junos OS releases for ISSU to work. PR1634695

Open Issues

IN THIS SECTION

Learn about open issues in Junos OS Release 22.1R1 for EX Series switches.

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

Forwarding and Sampling

- The `fast-lookup-filter` with match not supported in fast lookup filter hardware might cause traffic drop. PR1573350

Infrastructure

- There is a possibility of kernel crash when the system is in the process of coming up after reboot (and observed only with multiple iterations of continuous reboot cycles). This is observed only during init sequence of mgmt driver and impact is limited to increased system boot time. PR1642287

Network Management and Monitoring

- You might observe memory leak in event-daemon process during GRES. PR1602536

Platform and Infrastructure

- When you add VLAN an action for changing the VLAN in both the ingress and egress filters, the filter does not get installed. PR1362609

- When you run the `show pfe filter hw filter-name` *`filter name`* command, the command fails to retrieve the Packet Forwarding Engine programming details of the filter. PR1495712

- A delay of 35 seconds gets added in reboot time in Junos OS Release 20.2R1 compared to Junos OS Release 19.4R2. PR1514364

- Pause frames counters are not getting incremented when pause frames are sent. PR1580560

- On EX4400 family of devices, sometimes login prompt is not displayed after the login session ends. PR1582754

- During Routing Engine switchover, interface might flap along with the scheduler slippage. PR1541772

- When the DHCP relay mode is configured as no-snoop, we are observing the offer gets dropped due to incorrect asic programming. This issue only affects while running DHCP relay on EVPN/VXLAN environment. PR1530160

Routing Protocols

- EX4400-48MP - VM core files and Virtual Chassis split might be observed with multicast scale scenario. PR1614145

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.

Resolved Issues: 22.1R1

IN THIS SECTION

Class of Service (CoS)

- The dcpfe core files might be seen in the auto-channelization scenario or when SFP is plugged out. PR1616847

Infrastructure

- For EX4400 product family, net installation (PXE) does not work. PR1577562
- FreeBSD12: On Panic 0-size vmcore file gets generated. PR1607299
- DHCP packets originated from QinQ/SP vlans will have vlan-id of C-vlan in DHCP options82 circuit-id field. Whereas when configured to use vlan description, then S vlan name will be used in circuit-id. PR1616613
- Primary FPC might crash when you log into the device post powercyle of a three member EX2300-MP Virtual Chassis. PR1625987

Interfaces and Chassis

- `SNMP_TRAP_LINK_UP` and `SNMP_TRAP_LINK_DOWN` trap might be generated while activating and deactivating firewall filters. PR1609838
- The vrrpd core files might be observed after the interface state changes. PR1646480

Juniper Extension Toolkit (JET)

- JET SDK cannot produce bsd6/legacy Junos compatible package. PR1636189

Junos XML API and Scripting

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

Layer 2 Ethernet Services

- The jdhcpd process starts spiking and DHCP becomes unresponsive if you modify the configuration to add `override always-write-giaddr` and remove `forward-only`. PR1618306
- Option 82 might not be attached on the DHCP request packets. PR1625604

MPLS

- MPLS VPN packet drop occurs due to missing ARP entry on the provider edge. PR1607169

Platform and Infrastructure

- During flooding, MAC is learnt only on the normal access port but not on the aggregated Ethernet interface trunk port. PR1506403

- Junos 'et-' interface gets stuck and remains down between two particular ports. PR1535078
- ARP resolution failure might occur in the EVPN-VXLAN scenario. PR1561934
- IS-IS adjacency might fail to be formed if the MTU size of an IRB interface gets configured with a value greater than 1496 bytes. PR1595823
- Error message `error: syntax error: request-package-validate` gets generated on device CLI output during Non Stop Software Upgrade. PR1596955
- The interface on SFP-T or SFP-SX might stop forwarding traffic on EX4600 devices. PR1598805
- During day1 stage of EX4400 device management from MIST, the cloud LED remains in green state even if device loses connectivity with cloud. PR1598948
- The l2ald process might crash due to memory leak when all active interfaces in a VLAN are unstable. PR1599094
- On EX4300 platform, MAC addresses aging issue occurs. PR1600029
- The SFP-T port might stop forwarding traffic on EX4600 platforms. PR1600291
- Traffic loss might be observed if you configure dot1X with `supplicant multiple` and authenticated user from radius is in the single supplicant mode. PR1610746
- Inter-vlan connectivity might be lost in an EVPN-VXLAN with CRB topology. PR1611488
- Traffic stops when traffic switches from one LAG member to another member in case MACsec is configured. PR1611772
- Change in the commit error message appears while configuring the same vlan-id with different vlan name through openconfig CLI. PR1612566
- EX2300, EX3400, EX4300-MP, and EX4400 devices causes MAC movement when the IGMP query receives packet on the backup FPC port. PR1612596
- FPC might crash after the device restarts in the EVPN-VXLAN scenario. PR1613702
- On EX9204 device, entAliasMappingIdentifier does not reflect the correct SNMP entity to ifindex mapping for 100G and 40G ports. PR1614081
- After performing zeroize factory default configuration does not display appropriate interface in the device. PR1614098
- Removing the optical module `JNP-SFPP-10GE-T` from a port might cause certain ports to go down. PR1614139
- Packet Forwarding Engine might crash due to deletion of storm control configuration for IFL in CLI, which might lead to traffic loss. PR1616646

- Core files might be seen on EX and QFX devices after the configuration changes. PR1618352

- The dcpfe process might crash after changing and deleting the VXLAN VNI configuration on QFX5000 and EX series platforms. PR1619445

- On EX2300 Series, EX2300-MP Series, and EX3400 Series, a slow memory leak occurs due to processing of specific IPv6 packets. PR1619970

- OAM CFM session does not come up if the configured ERPS and CFM control traffic uses the same VLAN as ERPS control traffic. PR1620536

- EVPN Type5 routes might not be installed. PR1620808

- NSSU (nonstop-upgrade) CLI is not present in the Junos OS Release 21.2R1. PR1621611

- Traffic loss might be observed after configuring VXLAN over IRB interface. PR1625285

- The filter required for routing the Layer 3 traffic of targeted broadcast and static ARP entry with multicast-mac address might fail to install. PR1626620

- When clients connect to the isolated Virtual Local Area Network (VLAN) through trunk port can't communicate to the network. PR1626710

- DHCP clients might not go to `BOUND` state when you enable the AE bundle between the DHCP server and snooping device. PR1627611

- The line card might crash and reload if the EVPN MAC entry is not deleted correctly. PR1627617

- Packet drop might be observed when you configure L2PT on a transit device. PR1627857

- The error message `BCM_PVLAN_UTILS:ERR:pfe_bcm_pvlan_utils_get_sec_bd(),789: Failed to get Secondary-bd` gets logged DHCP server receives packet on a private VLAN. PR1630553

- Unicast ARP packets with the first four bytes of its destination MAC matching to system MACs of a transit system gets trapped by the system. PR1632643

- Traffic loss occurs for 20 seconds on Virtual Chassis with aggregated Ethernet link-protection when rebooting backup FPC. PR1633115

- The VCPs connected with the AOC cable might not come up after upgrading to Junos OS Release or later. PR1633998

- On EX4300-48MP, LED state remains OFF in the output of the `show chassis led` command for 40G port on PIC 2. PR1635106

- IRB traffic drop might be observed when `mac-persistence-timer` expires. PR1636422

- Configuring L2PT on a transit switch in a Q-in-Q environment breaks L2PT for other S-VLANs. PR1637249

- MAC address might not be learned on the new interface after MAC move. PR1637784
- Delay might be observed for the interfaces to come up after reboot or transceiver replacement. PR1638045
- MAC-move might be observed when you configure dhcp-security. PR1639926
- The error message dot1xd : `devrt_rtsock Don't know how to handle message type 2` gets logged even if you do not set dot1x. PR1641304
- Some interfaces might be down after a power outage or power cycle. PR1580829
- Route leak from the primary routing-instance to custom routing-instance fails for local interface. PR1623429
- The ARP resolution might get failed on the VRRP enabled interface. PR1630616
- Application of firewall filters might break connectivity towards the hosts on EX4300 device. PR1630935
- The Packet Forwarding Engine might get crash when the Virtual Chassis member flaps on EX platforms. PR1634781

Routing Protocols

- The rpd core files might be observed due to memory corruption. PR1599751
- The rpd might crash and restart when you enable NSR. PR1620463

Subscriber Access Management

- Adding the new radius access configuration might fail. PR1629395

Virtual Chassis

- During NSSU, errors related to link might be observed while IFDs are attached or detached. PR1622283
- Delay might be observed while establishing the virtual-chassis post upgrading or rebooting device. PR1624850

Documentation Updates

IN THIS SECTION

Learn about corrections and changes in Junos OS Release 22.1R1 documentation for EX Series switches.

J-Web Application Package and Platform Package for EX Series Online Help

Starting in Junos OS Release 22.1R1, EX4300 and EX4600 switches are not supported. Ignore the erroneously included information about EX4300 and EX4600 switches in the J-Web Application Package and Platform Package for EX Series Online Help.

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 22.1R1 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 Junos OS Release 22.1R1 for JRR Series Route Reflectors.

What's Changed

There are no changes in behavior and syntax in Junos OS Release 22.1R1 for JRR Series Route Reflectors.

Known Limitations

There are no known behaviors, system maximums, and limitations in hardware and software in Junos OS Release 22.1R1 for JRR Series Route Reflectors.

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

Open Issues

There are no known issues in hardware and software in Junos OS Release 22.1R1 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

There are no resolved issues in Junos OS Release 22.1R1 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.

Migration, Upgrade, and Downgrade Instructions

IN THIS SECTION

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

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

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

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

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

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

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

Table 3: EOL and EEOL Releases

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

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

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

Junos OS Release Notes for Juniper Secure Connect

IN THIS SECTION

These release notes accompany Junos OS Release 22.1R1 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

IN THIS SECTION

Learn about new features introduced in this release for Juniper Secure Connect.

What's New in 22.1R1

IN THIS SECTION

Learn about new features or enhancements to existing features in this release for Juniper Secure Connect.

VPNs

- **Support for search domain name (Juniper Secure Connect Application, SRX Series and vSRX next-generation firewalls)**—As a system administrator, you can configure the set of search domain name that the Juniper Secure Connect application will use to handle DNS lookups. This is applicable for both full tunnel and split tunnel configurations. You can provide more than one search domain names by executing the `set security remote-access client-config name domain-name domain-name` multiple times. When you enter more than one domain name, it automatically adds a separator (comma) to that value. The number of domain names are limited to the total number of characters and must not exceed 1023 characters. For example, the two domain names `juniper.net,lab.juniper.net` consumes 27 characters while `juniper.net` consumes 11 characters.

  [See client-config (Juniper Secure Connect) and Juniper Secure Connect Application Overview.]

Additional Features

We've extended support for the following features to these platforms.

- **Juniper Secure Connect application supports IPv6 addresses** (SRX5000 line of devices, and vSRX 3.0 running the iked process). While connecting to the Juniper Secure Connect application, you can provide an IPv6 address or IPv4 address as the gateway address and assign an IPv6 address or IPv4 address to a remote-access user.

  Earlier Junos OS releases support only IPv4 addresses.

  Note that IPv6 address-assignment is only supported when using certificate or EAP-based authentication

  This feature is supported on the unified iked process using `junos-ike` package. The SRX5K-SPC3 card with RE3 comes with `junos-ike` package installed by default. You must run the command `request system software add optional://junos-ike.tgz` to load the`junos-ike` package explicitly on SRX5K-SPC3 with RE2 and vSRX Virtual Firewall.

- **VLAN-level MACsec on logical interfaces** (EX9253 and QFX5120-48YM)

  [See Media Access Control Security (MACsec) over WAN.]

What's Changed

IN THIS SECTION

Learn about what changed in Junos OS main and maintenance releases for Juniper Secure Connect.

What’s Changed in Release 22.1R1

IN THIS SECTION

Platform and Infrastructure

- **Include IPv6 address in a self-signed certificate (SRX Series devices and vSRX3.0)**— We support manual generation of a self-signed certificate for the given distinguished name using IPv6 address in addition to the IPv4 address that was supported earlier. Use the `request security pki local-certificate generate-self-signed` command with `ipv6-address` option to include ipv6 address in a self-signed certificate.

VPNs

- **Save User Credentials on Juniper Secure Connect Application (SRX Series and vSRX)**—As a system administrator, you can now allow a user to save username or username and password for easy access:
  - using `set client-config` *`name`* `credentials username`option at the `edit security remote-access` hierarchy level to save the username.
  - using `set client-config` *`name`* `credentials password`option at the `edit security remote-access` hierarchy level to save both the username and password.

Note that you cannot configure both `username` and `password` options at the same time. If you have not configured any of the credentials configuration options, then the application does not remember the user credentials.

[See client-config (Juniper Secure Connect) and Juniper Secure Connect Application Overview.]

Known Limitations

There are no known limitations in hardware and software in Junos OS 22.1R1 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 22.1R1 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

IN THIS SECTION

Learn which issues were resolved in the Junos OS main and maintenance releases 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: 22.1R1

There are no resolved issues in Junos OS Release 22.1R1 for Juniper Secure Connect.

Junos OS Release Notes for Junos Fusion for Enterprise

IN THIS SECTION

These release notes accompany Junos OS Release 22.1R1 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

IN THIS SECTION

Learn about new features introduced in this release for Junos fusion for enterprise.

What's New in 22.1R1

Learn about new features or enhancements to existing features in this release for Junos fusion for enterprise.

What's Changed

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

Known Limitations

There are no known behaviors, system maximums, and limitations in hardware and software in Junos OS Release 22.1R1 for Junos fusion for enterprise.

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

Open Issues

There are no open issues in hardware and software in this release for Junos Fusion for enterprise.

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

Resolved Issues

IN THIS SECTION

Learn about the issues fixed 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: 22.1R1

- There might be a memory leak observed in Junos Fusion satellite device for the cpd process. PR1577977
- In rare cases, the anchor logical interface is not created in time which causes a core file to generate during the satellite device provisioning state. PR1555597

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 22.1R1 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 22.1R1 for Junos Fusion for Provider Edge.

What's Changed

There are no changes in behavior and syntax in Junos OS Release 22.1R1 for Junos Fusion for provider edge.

Known Limitations

There are no known behaviors, system maximums, and limitations in hardware and software in Junos OS Release 22.1R1 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 and software in Junos OS Release 22.1R1 for Junos Fusion for provider edge.

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

Resolved Issues

IN THIS SECTION

Learn about the issues fixed 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: 22.1R1

IN THIS SECTION

Junos Fusion Provider Edge

- SIP traffic drops after the `port-mirroring firewal filter` is configured on the bridge-domain. PR1607750

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 22.1R1 is different from that for earlier Junos OS releases.

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

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

2. Log in to the Juniper Networks authentication system by using the username (generally your e-mail address) and password supplied by Juniper Networks representatives.
3. Select **By Technology** > **Junos Platform** > **Junos fusion** to find the software that you want to download.
4. Select the release number (the number of the software version that you want to download) from the Version drop-down list to the right of the page.
5. Select the **Software** tab.
6. Select the software package for the release.
7. Review and accept the End User License Agreement.
8. Download the software to a local host.
9. Copy the software to the routing platform or to your internal software distribution site.

10. Install the new `jinstall` package on the aggregation device.

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

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

    - For 64-bit software:

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

      ```
      user@host> request system software add validate reboot source/jinstall64-22.1R1.SPIN-domestic-signed.tgz
      ```

    - For 32-bit software:

      ```
      user@host> request system software add validate reboot source/jinstall-22.1R1.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/jinstall64-22.1R1.SPIN-export-signed.tgz
      ```

    - For 32-bit software:

      ```
      user@host> request system software add validate reboot source/jinstall-22.1R1.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 22.1R1 `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 22.1R1, 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 21.1

To downgrade from Release 21.1 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 22.1R1 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

IN THIS SECTION

Learn about new features introduced in this release for MX Series routers.

What's New in 22.1R1

IN THIS SECTION

Learn about new features or enhancements to existing features in this release for the MX Series routers.

EVPN

- **Graceful restart support for unicast and Type 5 routing on EVPN-VXLAN (MX240, MX480, MX960, MX2010, and MX2020)**—Starting in Junos OS Release 22.1R1, the listed MX Series routers support graceful restart protocol extension for high availability (HA) handling of unicast routes on EVPN-VXLAN. The routers also support EVPN Type 5 routing . Graceful restart enables a device to recover from a routing process restart or Routing Engine switchover without nonstop active routing (NSR) enabled. Type 5 routing on MPC10E line cards (IP prefix routing) provides all necessary forwarding information required for sending VXLAN packets in the data plane to the data center's egress network virtual endpoint.

  See:

  - Availability in EVPN
  - EVPN Type 5 Route with MPLS encapsulation for EVPN-MPLS

- **Multicast feature support for EVPN-MPLS and EVPN-VXLAN implementations on MPC10E and MPC11E line cards (MX240, MX480, MX960, MX2010, and MX2020)** —In Junos OS Release 22.1, we've added support for multicast routing features on the listed MX Series routers.

  [See Multicast Support in EVPN-VXLAN Overlay Networks.]

High Availability

- **Support for automatic deactivation and activation of incompatible configurations during unified ISSU (MX960, MX2010, MX2020, MX10003, MX10008, and MX10016)**—Starting in Junos OS Release 22.1R1, you can automatically deactivate incompatible configurations on MX Series routers during a unified in-service software upgrade (ISSU). You can then reactivate them after the upgrade is completed or canceled. Currently, this feature is applicable only to clock synchronization configurations for Precision Time Protocol (PTP) and Synchronous Ethernet.

  [See request system software in-service-upgrade].

Interfaces

- **Support for admin down in PS interfaces (MX Series)**—Starting in Junos OS Release 22.1R1, we support the admin down process for PS interfaces. *Admin down* is a process you use to disable a physical interface or logical interface , marking it as down, without removing the interface configuration from the system. You can use the existing `disable` statement under the `[edit interfaces *interface-name*]` or `[edit interfaces *interface-name* unit *logical-unit-number*]` hierarchy level to disable a PS physical interface or PS logical interface, respectively.

  If you disable a PS physical interface, then the interface will be *admin down* and logical interfaces will be *link down*. If you disable a PS logical interface, then the logical interface will be admin down and link up.

  [See disable (Interface).]

Juniper Extension Toolkit (JET)

- **Support for route count for programmed routes over JET/CLI/NETCONF (MX960, MX10003, PTX1000, PTX10008, and vMX)**—Starting in Junos OS Release 22.1R1, the `show programmable-rpd clients` command shows the summary of the number of routes installed and the per-route-table breakup of the route count. You can use this information to infer the per-routing-instance and per-address-family counts.

  [See show programmable-rpd clients.]

Network Address Translation (NAT)

- **Carrier-grade NAT J-Flow version 9 and IPFIX format (MX240, MX480, and MX960 with SPC3 card)**—Starting in Junos OS Release 22.1R1, we've added new information elements in the NAT44/NAT64 session template record using J-Flow version 9 and IPFIX format. The new elements are:

IANA IPFIX ID	Field Name	Size (bytes)	Description
136	flowEndReason	1	Session termination Reason.
231	initiatorOctets	8	Number of Packet Bytes in the forward flow direction
232	responderOctests	8	Number of packets Bytes in the reverse flow direction

  [See Understanding NAT Event Logging in Flow Monitoring Format on an MX Series Router or NFX250 .]

-

Network Management and Monitoring

- **Enhancement to <get-syslog-events> RPC with additional filtering options (cSRX, MX Series routers and vMX, SRX300, SRX320, SRX340, SRX345, SRX380, SRX550HM, SRX4100, SRX4200, SRX4600, SRX5400, SRX5600, SRX5800, vSRX, and vSRX 3.0)**—In Junos OS Release 22.1R1, we've introduced the following new tags in the `<get-syslog-events>` RPC. These tags provide additional options for filtering system log messages.

```
<start-count></start-count>
<end-count></end-count>
<total-events/>
<pretty/>
<print-json/>
```

  [See Overview of Junos OS System Log Messages and syslog (System).]

Platform and Infrastructure

- **Support for ISSU on MX10K-LC480 (MX10008 and MX10016)**—Starting in Junos OS Release 22.1R1, we support ISSU on the MX10K-LC480 line card.

  [See Protocols and Applications Supported by MX10K-LC480 for MX Series Routers.]

Routing Policy and Firewall Filters

- **Programmed RPD route statistics (MX960, MX2020, PTX1000, PTX10008, and PTX10016)**—Starting in Junos OS 22.1R1 release, you can capture the routes statistics `Statistics ID Group` and `Statistics` of routes. To capture the route statistics, you must configure the `enable_stats` through the `japi` in programmable RPD (PRPD) API.

  The route statistics are displayed only for ingress traffic on label-switched path (LSP).

  [See show route extensive and show route detail.]

Routing Protocols

- **Support for DDoS IS-IS classification (MX Series with MPCs MPC1 through MPC9, PTX1000, PTX5000, PTX10002, PTX10008, QFX10002, QFX10002-60C, QFX10008, and QFX10016)**—Starting in Junos OS Release 22.1R1, Junos OS classifies IS-IS hello packets and IS-IS data packets separately. You can apply different policers to different types of IS-IS packets to improve the performance of IS-IS during congestion so that IS-IS doesn't go down when a large number of packets are entering the device.

  Configure DDoS protection settings for IS-IS hello packets and IS-IS data packets separately using the `isis-hello` or `isis-data` statement at the `[edit system ddos-protection protocols isis]` hierarchy level. Use the `show ddos-protection protocols isis parameters brief` command to view the aggregate number of IS-IS packets as well as the number of IS-IS hello packets and IS-IS data packets.

  [See protocols (DDoS) (ACX Series, PTX Series, and QFX Series) and show ddos-protection protocols isis.]

- **Support for adaptive RSVP update threshold (cRPD, MX240, MX480, MX960, PTX1000, PTX10008, QFX10002-60C, and QFX10008)**—Starting in Junos OS Release 22.1R1, you can configure the RSVP update threshold percentage and threshold value to adaptively pace IGP updates. You can configure a lower frequency when the adaptive bandwidth is higher and configure a higher frequency when the bandwidth is lower.

  You can enable the threshold percentage by using the `update-threshold adaptive limit` *`limit`* `threshold-percent` *`percentage`* configuration, and threshold value by using the `update-threshold adaptive limit` *`limit`* `threshold-value` *`value`* `configuration` at the `edit protocols rsvp interface` hierarchy level.

> **NOTE**: You cannot configure both threshold-percent and threshold-value simultaneously on the same interface.

[See update-threshold.]

- **Support for CBF fallback inside service group (MX10008)**—Starting in Junos OS Release 22.1R1, you can create a te-group-id *id* group for uncolored tunnels. This helps to enable class-based forwarding (CBF) and fallback inside a service group at the same time for uncolored static segment routing–traffic engineering (SR-TE) label-switched paths (LSPs) with the first hop as a label or as an IP address.

  > **NOTE**: Colored SR-TE LSPs do not support this feature.

  [See source-routing-path.]

Source Packet Routing in Networking (SPRING) or Segment Routing

- **Avoid microloops in OSPFv2 segment routing networks (ACX5448, ACX6360, MX Series, PTX Series, and QFX10002)** —Starting in Junos OS Release 22.1R1, you can enable post-convergence path calculation on a device to avoid microloops if a link or metric changes in an OSPFv2 segment routing network. Note that microloop avoidance is not a replacement for local repair mechanisms such as topology-independent loop-free alternate (TI-LFA), which detects local failure very fast and activates a precomputed loop-free alternative path.

  To configure microloop avoidance in an OSPFv2 segment routing network, include the maximum-labels and delay *milliseconds* statements at the [edit protocols ospf spf-options microloop avoidance post-convergence-path] hierarchy level.

  [See How to Configure Microloop Avoidance for OSPFv2 SR Networks.]

Services Applications

- **Support for GeoIP filtering, global allowlist, and global blocklist with Juniper ATP Cloud (MX240, MX480, and MX960)**—Starting in Junos OS Release 22.1R1, you can configure the Security Intelligence process (IPFD) on MX Series routers to fetch the GeoIP feeds from Juniper ATP Cloud. You can then use the feeds to prevent devices from communicating with IP addresses belonging to specific countries.

  You can define:

  - A profile to dynamically fetch GeoIP feeds. Include the `geo-ip rule match country` *`country-name`* statement at the `[edit services web-filter profile` *`profile-name`* `security-intelligence-policy]` hierarchy level.

  - A template to dynamically fetch GeoIP feeds. Include the `geo-ip rule match group` *`group-name`* statement at the `[edit services web-filter profile` *`profile-name`* `url-filter-template` *`template-name`* `security-intelligence-policy]` hierarchy level.

  You can configure a global allowlist by configuring the `white-list (IP-address-list |` *`file-name`*`)` statement at the `edit services web-filter profile` *`profile-name`* `security-intelligence-policy` hierarchy level. You can configure a global blocklist by configuring the `black-list (IP-address-list |` *`file-name`*`)` statement at the `edit services web-filter profile` *`profile-name`* `security-intelligence-policy` hierarchy level. Here, *`IP-address-list`* refers to the name of the list specified at the `[edit services web-filter]` hierarchy level. The *`file-name`* option refers to the name of the file where the list of the IP addresses to be allowed or blocked is specified. The file must be in the **/var/db/url-filterd** directory and must have the same name as in the configuration.

  [See Integration of Juniper ATP Cloud and Web filtering on MX Routers .]

Subscriber Management and Services

- **IPv6 SLAAC and dual stack (ipv4 and ipv6) support for User Endpoint address allocation in 4G and 5G (MX240, MX480, and MX960)**—Starting in Junos OS Release 22.1R1, we support IPv6 SLAAC and dual stack (ipv4 and ipv6) for UE address allocation in 4G and 5G. We also introduce support for IPv6 UE Parameter configuration via stateless DHCPv6.

- **5G compliance for lawful intercept (LI) for wireless CUPS (MX240, MX480, and MX960)**—Starting in Junos OS Release 22.1R1, we support 5G compliance for lawful intercept (LI) for wireless CUPS. 5GC lawful intercept have these characteristics :

  - Creates HTTP client or server at Routing Engine using LIGHTTPD.

  - Supports TLS encryption over HTTP for LI_T3 interface.

  - Supports XML encoding for LI_T3 signaling.

  - Supports LI task events from SMF at UPAD for target subscribers.

  - Supports generation of xCC at CC-POI in the UPF over LI_X3 over UDP transport.

  - Supports ping responses over LI_T3.

  - Existing support for 4GC lawful intercept is maintained.

  - APFE redundancy and GRES.

System Management

- **Support for Network Time Protocol (NTP) version 4.2.8p15 (ACX Series, MX Series, PTX Series, and QFX Series)**—Starting in Junos OS Release 22.1, we support the latest NTP version 4.2.8p15. The latest version provides improved device security.

  [See NTP Overview.]

Additional Features

We've extended support for the following features to these platforms.

- **OpenConfig LACP and LLDP configuration support** (ACX5448 router, EX4650, and EX4650-48Y-VC switches, MX480, MX960, MX10003, and PTX10008 routers, , QFX10002-60C, QFX5110, QFX5110-VC, QFX5110-VCF, QFX5120-32C, QFX5120-48T, QFX5120-48T-VC, QFX5120-48Y, QFX5120-48Y-VC, QFX5120-48YM, QFX5200, QFX5210, , QFX10002, QFX10003, QFX10008, and QFX10016 switches). OpenConfig configuration support based on the OpenConfig data models openconfig-lacp.yang and openconfig-lldp.yang.

  [See Mapping OpenConfig LLDP Commands to Junos Configuration and OpenConfig User Guide.]

- **PFE Restart Support** (MX240, MX480, and MX960 with MPC7, MPC8, and MPC9 and MX10008, MX10016 with LC2101)

- **PFE Reset Support** (MX10008, MX10016 with LC2101) using command `set chassis error severity threshold count action reset-pfe`, for errors including ASIC errors. [See No Link Title and No Link Title.]

- **Support for inline 6rd, Mapping of Address and Port with Encapsulation (MAP-E), NAT44, and NPTv6** (MX10008 with MX10K-LC2101 line card). The line card supports:

  - Inline 6rd

  - Mapping of Address and Port with Encapsulation (MAP-E)

  - Network Address Translator IPv4/IPv4 (NAT44)

  - Stateless Source Network Prefix Translation for IPv6 (NPTv6)

  [See Configuring Inline 6rd, Stateless Source Network Prefix Translation for IPv6 Configuring Mapping of Address and Port with Encapsulation (MAP-E).]

- **Support for inline services** (MX10008). MX10K-LC9600 line card supports inline services. The line card supports 4 inline services interfaces per PIC.

  [See bandwidth (Inline Services) .]

- **Supported transceivers, optical interfaces, and DAC cables** (EX Series, MX Series, and QFX Series). Select your product in the Hardware Compatibility Tool to view supported transceivers, optical interfaces, and DAC cables for your platform or interface module. We update the HCT and provide the first supported release information when the optic becomes available.

- **Support for Synchronous Ethernet** (MX10008 with MX10K-LC9600)

  [See Synchronous Ethernet Overview.]

- **Support for Synchronous Ethernet over a link aggregation group (LAG) with ESMC** (MX10008 with MX10K-LC9600)

  [See Synchronous Ethernet, and Ethernet Synchronization Message Channel (ESMC).]

- **Support for the Juniper Resiliency Interface** (MX10008 with MX10K-LC9600)

  [See Inline Monitoring Services Configuration.]

- **Support for monitoring link degradation** (MX10008 and MX10016 with MX10K-LC2101)

  [See Link Degrade Monitoring Overview.]

- **System OpenConfig configuration support and gNMI mixed-mode support** (ACX5448, MX240, MX480, MX960, MX10003, MX10008, MX10016, MX2008, MX2010, MX2020, and PTX10002)

  [See OpenConfig User Guide].

- **Virtual gateway address and virtual gateway MAC address support in EVPN-MPLS CRB overlay fabrics** (MX960, MX10008, and MX2020)

  [See Anycast Gateways, Understanding the MAC Addresses for a Default Virtual Gateway in an EVPN-VXLAN or EVPN-MPLS Overlay Network, virtual-gateway-address, virtual-gateway-v4-mac, and virtual-gateway-v6-mac.]

- **VLAN-level MACsec on logical interfaces** (EX9253 and QFX5120-48YM)

  [See Media Access Control Security (MACsec) over WAN.]

What's Changed

IN THIS SECTION

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

What’s Changed in Release 22.1R1

IN THIS SECTION

General Routing

- **No support for PKI operational mode commands on the Junos Limited version (MX Series routers, PTX Series routers, and SRX Series devices)**—We do not support `request` , `show` , and `clear` PKI-related operational commands on the limited encryption Junos image ("Junos Limited"). If you try to execute PKI operational commands on a limited encryption Junos image, then an appropriate error message is displayed. The `pkid` process does not run on Junos Limited version image. Hence, the limited version does not support any PKI-related operation.
-

Junos OS API and Scripting

- **The `<request-system-zeroize>` RPC response indicates when the device successfully initiates the requested operation (ACX Series, EX Series, MX Series, PTX Series, QFX Series, SRX Series, vMX, and vSRX)**—When the `<request-system-zeroize>` RPC successfully initiates the zeroize operation, the device emits the `<system-zeroize-status>zeroizing re0</system-zeroize-status>` response tag to indicate that the process has started. If the device fails to initiate the zeroize operation, the device does not emit the `<system-zeroize-status>` response tag.

Interfaces and Chassis

- Display the donor details of the IPv6 borrower interface? The output for the show interfaces command now displays the donor details of the IPv6 borrower interface.

  [See show interfaces .]

Layer 2 Ethernet Services

- **New output fields for subscriber management statistics (MX Series)**—If you enable the enhanced subscriber management, the non-DHCPv4 bootstrap protocol (BOOTP) requests might not get processed even if you configure the DHCP relay or server with the `overrides bootp-support` statement at the `edit forwarding-options dhcp-relay` hierarchy level. To monitor the DHCP transmit and receive packet counters, we've introduced the following output fields for `show system subscriber-management statistics dhcp extensive` operational command. - BOOTP boot request packets received - BOOTP boot reply packets received - BOOTP boot request packets transmitted - BOOTP boot reply packets transmitted

  [See show system subscriber-management statistics.]

Network Address Translation (NAT)

- **NAT rule configuration command (SRX Series and MX Series)**—Starting in Junos OS Release 22.1R1, on Source NAT, Destination NAT, and Static NAT, the rule-set command configuration fails if you use the IP address with incorrect prefix. To commit the configuration, use the valid IP address prefix.

  [See rule-set (Security Source NAT), rule-set (Security Destination NAT), and rule-set (Security Static NAT).]

Network Management and Monitoring

- **Junos XML protocol Perl modules deprecated (ACX Series, EX Series, MX Series, PTX Series, QFX Series, SRX Series, vMX, and vSRX)**—We no longer provide the Junos XML protocol Perl client for download. To use Perl to manage Junos devices, use the NETCONF Perl library instead.

  [See Understanding the NETCONF Perl Client and Sample Scripts.]

- **Changes when deactivating or deleting instances of the ephemeral configuration database (ACX Series, EX Series, MX Series, PTX Series, QFX Series, SRX Series, vMX, and vSRX)**—The following changes apply when you deactivate or delete ephemeral database instances in the static configuration database:

  - When you deactivate the entire `[edit system configuration-database ephemeral]` hierarchy level, the device deletes the files and corresponding configuration data for all user-defined ephemeral instances. In earlier releases, the files and configuration data are preserved; however, the configuration data is not merged with the static configuration database.

- When you delete an ephemeral instance in the static configuration database, the instance's configuration files are also deleted. In earlier releases, the configuration files are preserved.

- You can delete the files and corresponding configuration data for the default ephemeral database instance by configuring the `delete-ephemeral-default` statement in conjunction with the `ignore-ephemeral-default` statement at the `[edit system configuration-database ephemeral]` hierarchy level.

[See Enable and Configure Instances of the Ephemeral Configuration Database.]

- **Support for automatically synchronizing an ephemeral instance configuration upon committing the instance (EX Series, MX Series, MX Series Virtual Chassis, PTX Series, QFX Series, and vMX)**—You can configure an ephemeral database instance to synchronize its configuration to the other Routing Engine every time you commit the ephemeral instance on a dual Routing Engine device or an MX Series Virtual Chassis. To automatically synchronize the instance when you commit it, include the `synchronize` statement at the `[edit system commit]` hierarchy level in the ephemeral instance's configuration.

  [See Commit and Synchronize Ephemeral Configuration Data Using the NETCONF or Junos XML Protocol.]

Routing Protocols

- To achieve consistency among resource paths, the resource path /mpls/signalling-protocols/segment-routing/aggregate-sid-counters/aggregate-sid-counter **ip-addr='address'**/state/counters **name='name'**/out-pkts/ is changed to /mpls/signaling-protocols/segment-routing/aggregate-sid-counters/aggregate-sid-counter **ip-addr='address'**/state/counters **name='name'**/. The leaf "out-pkts" is removed from the end of the path, and "signalling" is changed to "signaling" (with one "l").

User Interface and Configuration

- **Load JSON configuration data with unordered list entries (ACX Series, EX Series, MX Series, PTX Series, QFX Series, SRX Series, vMX, and vSRX)**—The Junos schema requires that list keys precede any other siblings within a list entry and appear in the order specified by the schema. Junos devices provide two options to load JSON configuration data that contains unordered list entries:

  - Use the `request system convert-json-configuration` operational mode command to produce JSON configuration data with ordered list entries before loading the data on the device.

  - Configure the `reorder-list-keys` statement at the `[edit system configuration input format json]` hierarchy level. After you configure the statement, you can load JSON configuration data with unordered list entries, and the device reorders the list keys as required by the Junos schema during the load operation.

When you configure the `reorder-list-keys` statement, the load operation can take significantly longer to parse the configuration, depending on the size of the configuration and number of lists. Therefore, for large configurations or configurations with many lists, we recommend using the `request system convert-json-configuration` command instead of the `reorder-list-keys` statement.

[See json and request system convert-json-configuration.]

Known Limitations

IN THIS SECTION

Learn about known limitations in Junos OS 22.1R1 for MX Series routers.

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

General Routing

- Currently, IP options are not supported for egress firewall attach points, relevant supporting doc attached: https://www.juniper.net/documentation/us/en/software/junos/routing-policy/t opics/concept/firewall-filter-match-conditions-for-ipv4-traffic.html. The issue might occur IP-options router alert traffic not hitting the egress firewall filter. PR1490967
- Broadcast, Unknown Unicast, and Multicast (BUM) traffic replication over VTEP is sending out more packets than expected and there seems to be a loop. PR1570689
- On all MX Series platforms, changing configuration AMS 1:1 warm-standby to load-balance or deterministic NAT might result in vmcore and cause traffic loss. PR1597386

- When a packet, which triggers ARP resolution, hits services interface style filter on the output will have session create and close log with incorrect ingress interface. This typically occurs with the first session hitting such a filter. PR1597864

- We should configure only one static ARP with multicast-mac entry per IRB interface. If we configure more than one static ARP with multicast MAC entry per IRB interface, then the packets with different destination IP having static multicast MAC will always go out with any one of the multicast MAC configured in the system. PR1621901

- This is a product limitation for MX-SPC3 with new junos-ike architecture. The issue is seen when we have any-any TS configured and any-any TS negotiated (both in IPv4 and IPv6). As a workaround, do not configure any-any TS when it is sure that negotiated traffic selector for the IPsec tunnel will also be any-any. When there is no TS configured, the scenario might be treated as proxy-id case and bypasses the issue without having any impact on the described scenario.PR1624381

- Changing the root-authentication password in cpce does not bring down the existing session. The password change will be in effect for all new connections. PR1630218

- The available space check in case of: 1. Upgrade is 5 GB 2. Fresh Install is 120 GB. The scenario Upgrade/Fresh-Install is decided from within RPM spec that is if RPM finds any older version is already installed. Since RPM-DB is destroyed during LTS-19 (vm-host) upgrade, rpm install scripts deduce the upgrade as fresh-install and look for 120GB free space. The warning can be ignored, as it has no functional impact. PR1639020

- On MX Series operating as a SAEGW-U/UPF at high mobile session scale (around 1 Million sessions), `show services mobile-edge sessions extensive` will not work. Mobiled process will take exception and generates core files. PR1639595

Infrastructure

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

Network Management and Monitoring

- Configuring the set `system no-hidden-commands` blocks NETCONF sessions. As a workaround, customer can disable the `no-hidden-commands`.PR1590350

- When an ephemeral instance is being edited, if `show ephemeral-configuration merge` command is run from another terminal, then the uncommitted changes in the ephemeral instance being edited will also appear in the output of `show ephemeral-configuration merge` command. PR1629013

Platform and Infrastructure

- Deactivating services rpm/rpm-tracking does not remove the tracked route from the routing or forwarding tables. PR1597190
- After a switchover event, when ppmd calls sendmsg system call to transmit the protocol packets, it gets blocked long enough that a few sendmsg calls cumulatively take up around 7 seconds to 8 seconds. This indirectly impacts the BFD session because the BFD session has a Routing Engine-based detect time of 7.5 seconds to expire. PR1600684

Routing Protocols

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

VPNs

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

Open Issues

IN THIS SECTION

Learn about open issues in Junos OS Release 22.1R1 for MX Series routers.

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

Class of Service (CoS)

- When rate-limit-burst knob is deleted, burst size will fall back to the previously calculated burst size with the tx rate. In the above mentioned trigger, as the rate-limit-burst configs was present when the system is coming up, the burst size from the tx rate is not at all computed and when the user try to delete the knob, it is fall back to this un-computed burst size(default to 0). This is the reason for very small burst size configured to the rate limit queues. To fix this issue, we allow the burst size to be calculated even when global ratelimit knob is present and store it and use the burst size calculated from the global rate limit knob. PR1650089
- On MX Series platforms with MPC5E and MPC6E, the hierarchical class of service (HCOS) does not work for LT interfaces configured on PIC2 and PIC3. PR1651182

EVPN

- EVPN-MPLS multihoming control MACs are missing after VLAN ID removal and adding it back to a trunk logical interface of one of the multihoming PE devices. This is not a recommended way to modify VLAN ID configuration. Always both multihoming PE devices needs be in symmetric. PR1596698

- MAC IP moves across L2-DCI is not updated in MAC-IP table of the gateway nodes. This problem happens only with the translation VNI when the MAC is moved from DC1 to DC2. VM moves across DC where there is no translate VNI configuration in the interconnect works as designed. PR1610432

- EVPN Local ESI MAC limit configuration might not get effective immediately when it has already learned remote MH MACs. Clear the MAC table from all MH PEs and configure the MAC limit over local ESI interfaces. PR1619299

- This is a case where interface is disabled and comes up as CE after a timeout. A manual intervention of clear CE interface command should restore this. This can be a workaround: 1) clear auto-evpn ce-interface <interface-name> 2) configure edit activate <interface-name> family inet inet6 We can fix this in phase 2 by keeping some persistent state on a interface being a core facing interface in some incarnation. PR1630627

- On all Junos OS and Junos OS Evolved platforms, when EVPN-VXLAN or EVPN-MPLS multihoming single-active mode through Ethernet Segment Identifier (ESI) is configured and the configurations `no-core-isolation` is enabled, then the Circuit Cross-Connect (CCC) might be Up/Forwarding for both Designated Forwarder (DF) and Backup Designated Forwarder (BDF).PR1647734

Flow-based and Packet-based Processing

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

Forwarding and Sampling

- The configuration statement `fast-lookup-filter` with match condition is not supported in FLT hardware and might cause a traffic drop. PR1573350

General Routing

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

- PTP primary and secondary port configuration only accepts PTP packets with multicast MAC address according to the port settings. If forwardable multicast is configured, only PTP packets with forwardable MAC address is accepted, non-forwardable is dropped. Link-local multicast is configured, only PTP packets with non-forwardable MAC address is accepted, forwardable is dropped. PR1442055

- The vmcore process crashes sometimes along with the mspmand process on MS-MPC or MS-MIC if large-scale traffic flows are processed. PR1482400

- When running the command, `show pfe filter hw filter-name <filter name>`, the command fails to retrieve the Packet Forwarding Engine programming details of the filter. PR1495712

- A 35-second delay is added to reboot time in Junos OS Release 22.1R1 compared to Junos OS Release 19.4R2. PR1514364

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

- When an image with the third party SDK upgrade (6.5.x) is installed, the CPU utilization might go up by around 5 percent. PR1534234

- Flap might be observed on channelized ports during ZTP when one of the ports is disabled on the supporting device. PR1534614

- FPC might core if flap-trap-monitor feature under `set protocols oam ethernet cfm performance-monitoring sla-iterator-profiles` is used and performance monitoring flap occurs. PR1536417

- On a scaled MX2020 router with VRF localization enabled, 4 million next hop scale, and 800,000 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 might not come online. Rebooting primary and backup Routing Engine will help recovering and get the router back into a stable state. PR1539305

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

- 5M DAC connected between QFX10002-60C and MX2010 doesn't link up. But with 1M and 3M DAC, this interoperation works as expected. Also it is to be noted on QFX10002-60C and ACX Series devices or traffic generator, the same 5M DAC works seamlessly. There is a 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

- The SyncE to PTP transient response is a stringent mask to be met with two way time error. The SyncE to PTP transient response mask might not be met for MPC7E-1G and MPC7E-10G line cards. PR1557999

- VE and CE mesh groups are default mesh groups created for a given routing instance. On adding VLAN or bridge domain, flood tokens and routes are created for both VE and CE mesh-group and flood-group. Ideally, VE mesh-group does not require a CE router where IGMP is enabled on CE interfaces. MX Series based CE boxes have unlimited capacity of tokens. So, this would not be a major issue. PR1560588

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

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

- Duplicate traffic might be observed for some Layer 3 multicast traffic streams. PR1568152

- The problem is with Layer 1 node not reflecting correct bandwidth configured for tunnel services. When baseline has 1G configuration on some FPC or PIC in groups global chassis and if we override with local chassis tunnel service in 10G bandwidth scaled scenario. Out of 10 Gbps bandwidth configured only 1 Gbps is allowed per 1G speed configured in baseline configuration. PR1568414

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

- The following messages might be seen in the logs from MPC11E line-card: **Feb 9 11:35:27.357 router-re0-fpc8 aftd-trio[18040]: [Warn] AM : IPC handling - No handler found for type:27 subtype:9**. There is no functional impact, these logs can be ignored. PR1573972

- **CHASSISD_FRU_IPC_WRITE_ERROR: fru_send_msg: FRU GNF 2, errno 40, Message too long** might appear periodically in the chassisd logs. PR1576173

- This issue is caused by /8 pool with block size as 1, when the configuration is committed the block creation utilizes more memory causing NAT pool memory shortage, which is currently being notified to customer with syslog tagged RT_NAT_POOL_MEMORY_SHORTAGE. PR1579627

- In a fully loaded devices at times, firewall programming fails due to scaled prefix configuration with more than 64800 entries. This issue is not observed during development setup. PR1581767

- When interim logging is configured for PBA, it generates syslog messages at regular intervals. Change in the information of PBA interim syslog message, message string change from **allocates port block** to **interim port block**. PR1582394

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

- PIM VXLAN does not work on the TD3 chipsets that enables the VXLAN flexflow. PR1597276

- On MX2010 and MX2020 Series platforms: MPC11E: Unified ISSU is not supported for software upgrades from 21.2 to 21.3 and 21.4 releases due to a flag day change. PR1597728

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

- NPU sensor path for subscription is: /junos/system/linecard/npu/memory/ Its output would contain info as follows: system_id:wf-mt-ranier component_id:4 path:sensor_1004_1_1:/junos/system/linecard/npu/memory/:/junos/system/linec ard/npu/memory/:aftd-trio sequence_number:1 timestamp:1639179017148 . . kv { key:property[name='mem-util-firewall-fw-bytes-allocated']/state/value int_value:9064 } kv { key:property[name='mem-util-firewall-fw-allocation-count']/state/value int_value:94 } kv { key:property[name='mem-util-firewall-fw-free-count']/state/value int_value:0 } kv { key:property[name='mem-util-firewall-inline-jflow-sample-rr-(dfw)-bytes-all ocated']/state/value int_value:131160 } kv { key:property[name='mem-util-firewall-inline-jflow-sample-rr-(dfw)-allocatio n-count']/state/value int_value:6 } kv { key:property[name='mem-util-firewall-inline-jflow-sample-rr-(dfw)-free-coun t']/state/value int_value:0 } kv { key:property[name='mem-util-firewall-inline-jflow-sample-nh-(dfw)-bytes-all ocated']/state/value int_value:16 } kv { key:property[name='mem-util-firewall-inline-jflow-sample-nh-(dfw)-allocatio n-count']/state/value int_value:1 } kv { key:property[name='mem-util-firewall-inline-jflow-sample-nh-(dfw)-free-coun t']/state/value int_value:0 } kv { key:property[name='mem-util-firewall-fw-strided-bytes-allocated']/state/val ue int_value:9064 } kv { key:property[name='mem-util-firewall-fw-strided-allocation-count']/state/va lue int_value:94 } kv { key:property[name='mem-util-firewall-fw-strided-free-count']/state/value int_value:0 } kv { key:property[name='mem-util-counters-fw-counter-bytes-allocated']/state/val ue int_value:16416 } kv { key:property[name='mem-util-counters-fw-counter-allocation-count']/state/va lue int_value:3 } . . The (VTY) CLI output is: root@wf-mt-ranier-fpc4:pfe> show npu memory info | match firewall mem-util-firewall-ro-edmem-size 20971520 mem-util-firewall-ro-edmem-allocated 294912 mem-util-firewall-ro-edmem-utilization 1 mem-util-firewall-ro-edmem-size 20971520 mem-util-firewall-ro-edmem-allocated 294912 mem-util-firewall-ro-edmem-utilization 1 mem-util-firewall-ro-edmem-size 20971520 mem-util-firewall-ro-edmem-allocated 294912 mem-util-firewall-ro-edmem-utilization 1. PR1606791

- If rpd agent sends indirect next hop deletions or additions in out of order to backup rpd, the rpd generates core file. This is a backup rpd crash issue and does not impact any functionality. PR1607553

- Dfwd cored when accessing ephemeral database files which is deleted through script. PR1609201

- The CLI `show ldp traffic-statistics interface p2mp` does not display traffic stats. This issue is applicable to AFT based trio line cards on MX routers. PR1611498

- IPsec tunnels are not deleted on disabling the AMS physical interface. PR1613432

- Changing aggregated Ethernet mode (aggregated-ether-options link-protection) with subscribers logged in on that aggregated Ethernet will cause undesirable subscriber management behavior. Users will need to confirm there are no subscribers on the aggregated Ethernet before changing the aggregated Ethernet protection mode. PR1614117

- In some NAPT44 and NAT64 scenarios, duplicate SESSION_CLOSE syslog error will be seen. PR1614358

- ICMP error packet does not have relevant header when configured with DS-Lite and with appropriate ICMP ALG name and one UDP application name. PR1616633

- The errors are displayed with following next-hop hierarchy INH->COMPNH->UCAST->AE_IFL. During AE-IFL flaps control detects and initiate MBB. It is possible by that Packet Forwarding Engine can see an compNH->ucast with ae-ifl down resulting into these error messages but this is only transient. There is no functional impact. PR1617388

- Maximum aggregate Ethernet interfaces software index was 128. Hence, a failure is seen when you configure with 218 interfaces. Since, we increase the maximum indexes to 255. PR1618337

- On platforms with SPC3 services card, due to flowd daemon crash, it might trigger flowd re-start due to which FPGA (field programmable gate array) DMA module might be stuck.PR1618913

- The flowd core observed with TLB configuration only with combination of MPC10 line cards. PR1624572

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

- On DUT with scaled MPLSVPN configuration and Junos Telemetry Interface sensors configured, stream of error messages **agentd_telemetry_uninstall_sensor: Deleting subscription from daemon aftsysinfo failed after mgmt_sock_retries 601, ret -1** is seen on stopping jtimon. Sensor packet drops might be seen when the error message scrolls on DUT. PR1627752

- All MX Series platforms with MPC10+, configuring syslog as a filter action might cause the FPC to restart. PR1627986

- For 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 the `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

-

- If the interface is in link up transition with Hold Up timer enable (Link down, Admin Up/ Enabled), and Packet Forwarding Engine reset occurs, the interface will come UP post Packet Forwarding Engine reset after Hold timer expiry. PR1630793

- On MX Series routers with Precision Time Protocol (PTP) hybrid mode enabled, if PTP client is configured in more than one interface and if those are in different FPC slots, disabling/deactivating/ flapping of PTP configured interface or change in master clock interface parameters might result in clksync crash. Once this happens, PTP might get stuck at holdover state and thus affects clock functionality. However, deactivating and activating PTP configuration could restore the issue. The issue could be rare.PR1631261

- On all MX devices with MX-MPC2E-3D-P and MPC2E-3D LC linecards, traffic might be flapping between ACQUIRING and HOLDOVER states while PTP with telemetry NPU is enabled.PR1631274

- On MX platform with enhanced subscriber management enabled, when `host-prefix-only` is configured on the underlying-interface for subscribers, it might not work in FPC. PR1631646

- As per FIPS compliance, in case of FIPS error on a FRU, entire system should shut down to avoid entering degraded mode.PR1632273

- Fix the CLI `show system firmware` command. PR1633187

- On all Junos OS MX devices configured with Dynamic Host Configuration Protocol (DHCP) subscribers over the Aggregated Ethernet (AE) interface and static subscribers, traffic loss might be seen for the static subscribers when the AE interface member link is removed. The static subscribers might be logged-out and logged-in automatically without any intervention.PR1634371

- Upon repeatedly querying `show network-agent statistics` command on CLI, it might not list the components at times. But, more number of queries will show the output. There is no operational impact on telemetry infra. Only this CLI command is affected. PR1634716

- On all MX150 devices, when an aggregate Ethernet (AE) interface is configured with LACP and adding a sub-interface configuration under the AE interface causes the LACP down leads to traffic loss.PR1634908

- FPC JNP10K-LC1201 frequently generates **zephyr_clock_get_tod_ext_sync_sample(xxx): READ BT-X tod_sec: xxxxxxxxxx, tod_ns: xxxxxxxxx** message. PR1635771

- From MX devices showing huge correction-field (CF) values on downstream devices in Precision Time Protocol (PTP) packets due to PTP failure on ports.PR1635877

- On MIC-MACSEC-20G on MX platforms, SFP-1FE-FX from the EOPTOLINK INC vendor does not work and the interface is down. PR1636322

- Ports speed is stuck and never changes for any port profile changes, if PIC bounce is done fast not letting the previous configuration complete. PR1637954

- NPU utilization and backpressure sensors are included to indicate the FLT utilization for the ZX and BT based PTX devices. The CLI used is `show npu utilization stats filter pfe`. PR1638487

- When Packet Forwarding Engine 0 and 1 are powered off, the new pfh interface(pfh-0/1/0) is not getting created with pfeId 2. Still, the old pfh-0/0/0 is created. Debug is still in progress. PR1639679

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

- This is a rare scenario. In a dual Routing Engine setup, assume the backup RPD has just started and re-syncing all states from FIB (Kernel). The backup RPD is not yet ready for switchover. If we do Routing Engine switchover manually through CLI or if any primary Routing Engine HW crash occurs. We end up in not installing some of the FIB entries. The work around is to restart the RPD in new primary Routing Engine. PR1641297

- Incoming packets might be sent to RX queues of core0 or core14 mistakenly, might result in the queue buffer full and the packets getting dropped.PR1641793

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

- WIth PTPoIPv6 on MPC2E 3D EQ, PTP backup stays in acquiring state.PR1642890

- Options to configure vxlan will not be available under `set interfaces fti unit tunnel encapsulation`. PR1643078

- On all Junos OS and Junos OS Evolved platforms, clearing the MAC from an interface on which persistent-learning is enabled might result in traffic impact. Please restart l2ald process to resolve the issue. PR1643258

- The 4x25/4x10G configurations can see CRC errors on links on ports 2,3,4,5,10,11,12,13 . These ports have dual vendor phys to ASIC (YT) and the SI values are not fine tuned between the vendor<-->vendor links leading to link down or CRC errors related issues. The issue is applicable for 22.1 release, we will try to fix this in next release. Issue is mostly seen with 4x25G , 4x10G the issue is not seen as per experiments done, but if seen then below can be tried. We can use port numbers 0,1,6,7,8,9,14 and 15 in 4x25 and 4x10G , these have single vendor towards ASIC (YT) and issue is not seen on these ports. PR1643433

- On DHCP subscribers stacked over AutoConf (dynamic) Vlans shows subscriber summary different count that actual DHCP bindings. PR1643863

- On all platforms, the field corresponding to the identifier of the static route if expressed in IPv6 format through NETCONF encoding or translation could generate some issues. Hence the configuration will not get translated to Junos CLI.PR1644319

- Stateful sync failing between active and backup MX chassis because active chassis might not detect TCP connection down.PR1644579

- Committing configuration changes during the PFE (Packet Forwarding Engine) reset pause window (when PFE is disabled, yet the PFE reset proper has not started yet) has the potential of causing errors and traffic loss. In particular, configuration changes that result in re-allocating policers (which are HMC-based) might lead to traffic being entirely policed out (i.e. not flowing). Once the PFE reset procedure has started config changes ought to be avoided until the procedure is completely done.PR1644661

- On all Junos OS and Junos OS Evolved platforms configured with EBGP multipath and bgp-protect-core under the routing instance, if the number of external paths along with the BGP Prefix-Independent Convergence (PIC) backup paths reaches the maximum ECMP limit, then all the traffic towards the destination is dropped on Packet Forwarding Engine with the exception of **sw error**.PR1645296

- Issue is specific to YT cards wherein during mlp delete messages the IFL ktree lookup is resulting in wrong dword for the IIF registry. Because of this, counter address is wrongly read resulting in ppe traps. Issue is not seen in ZT cards. PR1645483

- Issue is seen while bringing up dual stack DHCP subscribers. Not able to bring DHCP subscribers, as subscribers are getting logged out automatically. facing difficulties in RC analysis, as events are received from different daemons. PR1645574

- On all MX devices with the subscriber management scenario, when unified ISSU happens from pre 18.4 to post 18.4, subscribers that re-logged in pre 18.4 are called preNG subscribers. For any of the preNG subscribers, if the ipv4 or ipv6 family interface goes up or down, the issue is triggered. PR1646846

- On MPC10E or MPC11E, with type-5 tunnels configured with same Destination IP /Source IP combinations in various VRFs(with different VNIDs), if the VNIDs configured are swapped in a single commit, due to software bug there is a possibility that traffic over those two tunnel might completely stop. PR1647516

- The upstream RPF session state will be stuck in init state. This issue is seen only when HRS with min-rate feature is configured. This is applicable only to MX based platforms. PR1647746

- The `set vmhost management-if add-policer` configuration does not take effect.PR1647750

- Packet Forwarding Engine crash might be seen during installation of auto LSP filter in scale scenario. PR1648750

- Commit window is closed and will fix it in next release. PR1648886

- The firewall filter might be incorrectly updated in the MPC10E Packet Forwarding Engine when a change (for example, add, delete, deactivate, or activate) of firewall filter terms occurs in some scenarios, such as large-scale term changes or changes happening during MPC reboot. The incorrect firewall filter might cause the traffic to be silently dropped or discarded and even lead to an MPC crash. It is a timing issue. PR1649499

- BFD liveness detection on IP-demux V6 over static VLAN interface is failing. BFD liveness test for other stacking like BFD liveness on IP-demux over dynamic VLAN interface and BFD liveness on dynamic VLAN etc., are passing. PR1651695
- Subscribers cannot bind on a BNG-UP after the access interface has been disabled and re-enabled.PR1652203
- On all Junos OS and Junos OS Evolved platforms, rpd crash might be seen when BGP monitoring protocol (BMP) rib-out monitoring is configured for the flow-spec route. Since there is no next-hop for flow-spec route core might be seen while generating rib-out feed. Traffic loss might be seen due to this crash.PR1653130
- On MX series devuces when chained-composite-next-hop ingress L3VPN configuration statement is used along with internal and external BGP paths used and if IGP or BGP sessions flap BGP multi-path might not select appropriate next-hop (BGP multipath may select old stale session-id) that result into traffic drop.PR1653562
- On all Junos OS and Junos OS Evolved platforms, when two or more collectors have subscribed to gAFT sensors on the device, fibtd daemon(forwarding information base processing daemon) observes a core and initial sync with the collectors are lost. This causes the device to stop streaming telemetry data.PR1653942
- The upstream RPF session state will be stuck in the init state. This issue is seen only when hot root standby (HRS) with min-rate feature is configured. PR1647746
- On all MX devices, jdhcpd core dumps might be observed when using legacy DHCP feature with pseudowire interface after the Junos OS upgrade. PR1649638

Infrastructure

- Near-end port is not within RFC or IANA standards as ephemeral or dynamic port range has been modified. PR1602717

Interfaces and Chassis

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

- When Broadcast, Unknown Unicast, and Multicast (BUM) traffic is sent on MCLAG, MAC entries are learnt on ICL interface as DLR when ICL flaps as MAC learning. This might cause the traffic loss with certain traffic flow. PR1639713

- Dual primaries are seen in VRRP when the devices are running two different Junos OS versions.PR1650873

Juniper Extension Toolkit (JET)

- The stub creation functions will not be available. PR1580789

- GRPC on WAN port is not working. The libsi can only be linked with 64-bit binaries. To access data or WAN ports, you need to link libsi with the binary. By default, the shell on the device includes libsi, but it is not available to the CLI commands as the CLI will make mgd invoke cscript to run a Python script through CLI. PR1603437

Layer 2 Ethernet Services

- On all Junos OS MX devices, jdhcpd crash might be seen due to Transmission Control Protocol (TCP) connection restart between a pair of Dynamic Host Configuration Protocol (DHCP) Active Lease Query (ALQ) peers. TCP connection restart might happen if there are route flaps, remote DHCP daemon restart, configuration update, etc. When this crash happens, jdhcpd daemon will restart, impacting DHCP subscriber services. PR1644919

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 milliseconds to 50 milliseconds traffic drop on the existing logical interface. PR1367488

MPLS

- BFD session flaps during unified ISSU only in MPC7E line card. The issue is not seen frequently.PR1453705

- The single hop BFD sessions might flap sometimes after GRES in a highly scaled setup which have RSVP link or link-node-protection bypass enabled. This happens because the RSVP neighbor goes down sometimes after GRES if RSVP signals are not received before neighbor is timed out. As a result of the RSVP neighbor going down, RSVP installs a /32 route pointing to bypass tunnel which is required to signal backup LSPs. This route is removed when all LSPs stop using bypass after the link comes back. The presence of this /32 route causes BFD to flap. PR1541814

- In MVPN case, if the nexthop index of a group is not same between primary and backup after a NSR switchover, you might see a packet loss of 250 milliseconds to 400 milliseconds. PR1561287

- The `use-for-shortcut` statement is meant to be used only in SR-TE tunnels which use strict SPF Algo 1 (SSPF) prefix SIDs. If `[set protocols isis traffic-engineering family inet-mpls shortcuts]` and `[set protocols isis traffic-engineering tunnel-source-protocol spring-te]` is configured on a device, and if any SR-TE tunnel using Algo 0 prefix SIDs is configured with the `use-for-shortcut` statement, it could lead to routing loops or rpd process core files. PR1578994

- On the MX10016 routers, when there is scaled RSVP sessions (for example, 21,000) and the RSVP is enabled for all the interfaces, then the rpd process goes through all the interfaces which results in a high CPU utilization for some time. This also results in LSP flap.PR1595853

- With the `chained-composite` statement is enabled, the following statement does not have any effect if ingress and egress ports are on the same Packet Forwarding Engine instance on the line card (FPC). For example, the outer label TTL would not be set as 255. Instead, it would be set as (ip TTL-1). PS: This issue is not seen if ingress and egress ports are on different FPC slots or on difference Packet Forwarding Engine instances of the same FPC. The `set protocols mpls label-switched-path lsp-name no-decrement-ttl` `chained-composite` statement: `set routing-options forwarding-table chained-composite-next-hop ingress l3vpn`. PR1621943

- The ingress retries after LSP stay down for extended period of time or customer clears LSP to speed up the retry. PR1631774

- When P2MP egress interface deletes, the rpd process generates a core file while LDP p2mp MBB is in progress. PR1644952

- On all Junos OS platforms, if `routing-option resolution preserve-nexthop-hierarchy` is configured globally, routing engine (RE) kernel crash might be observed in the one-hop-LSP Multiprotocol Label Switching (MPLS) scenario with RE outbound traffic.PR1654798

Network Management and Monitoring

- The mgd might crash and generate a core file when an invalid value is configured for identityref type leafs/leaf-lists while configuring `Openconfig` or any other third-party YANG, problem occurs with JSON and XML loads. PR1615773

Platform and Infrastructure

- MPC checks periodic service time. When heavy interruptions occur during periodic service, the periodic service time might exceed 200 microseconds. If it happens, **Oinker: Function** message will occur, but it doesn't have functional impact. PR1242915

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

- When the DHCP relay mode is configured as `no-snoop`, we observe the offer drops due to incorrect ASIC programming. This issue only affects while running DHCP relay on EVPN or VXLAN environment. PR1530160

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

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

- Routing Engine-based BFD sessions might flap during switchover when there are large number of BFD, IS-IS, OSPF and LDP packets to be sent out. PR1600684

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

- Using static labeled switched path (LSP) configuration, the child node is not removed from the flood composite when the core interface goes down.PR1631217

- MACs are not getting learned initially on a specific bridge domain. However, the MACs are learned in that specific BD after some duration. This delay in MAC learning will be fixed in the upcoming releases. PR1632411

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

- On MX platforms input-vlan-map (pop) might not work on Pseudowire Subscriber (PS) interfaces if the native VLAN is configured on the uplink interface under the pseudowire headend termination (PWHT) scenario.PR1640254

Routing Policy and Firewall Filters

- Already configured routing-policies are incorrectly changed and all the configured **from** matching criterias are removed from them, when global default route-filter walkup option is changed, that is when add or delete of `set policy-options default route-filter walkup` configuration is done. This issue affects only those routing policies which do not have `from route-filter` configured in any of the terms. PR1646603

Routing Protocols

- On MX Series routers, initial multicast register packets might get dropped, this might affect multicast services. PR1621358
- When filter is configured through open configuration and bound to a routing table instance, the filter bind object is not getting published due to the absence of routing table object. Hence the filter does not work as expected since the traffic does not hit the filter. PR1644421
- When a BGP neighbor is configured in passive mode inside a non-forwarding routing instance, the BGP peer is unable to complete the TCP three-way handshake due to incoming BGP OPEN message received into the default primary instance.PR1645010
- When inline add event for IPv6 inline BFD session comes without resolving neighbor for nexthop, inline event addition will fail. PR1650677
- BGP PIC protection is not working in virtual router.PR1653356
- Route protocol process (RPD) core files might be generated if logical interface access request is sent to MPLS-LSP-interface when IS-IS multi-topology functionality and IS-IS forwarding-adjacency label switched path (FA-LSP) feature is enabled. PR1654162
- VM core files and VC split might be observed with multicast scale scenario. PR1614145

User Interface and Configuration

- On all Junos OS and Junos OS Evolved devices, when copy-configuration, get-configuration, and discard-change RPCs run in two parallel NETCONF sessions and the database is also accessed in parallel by two NETCONF sessions, it leads to database corruption and mgd-related services might crash. PR1641025

- When a top-level (first level) dop exists only in any of the databases (static/one ephemeral database), then instead of creating a merge_dop operation, we proceed with the walk with the dop corresponding to that database.PR1652605
- Per the current design for rib-groups, a rib-group configured with `import-policy` configuration statement will change after NSR switchover. This makes IS-IS to refresh (delete and re-add) its routes in RIB, if such a rib-group is being used for IS-IS protocol. The IS-IS route refresh in-turn causes SBFD sessions to flap. This issue is only applicable with rib-group configured with "import-policy". Without "import-policy" the issue is not seen. PR1654072

VPNs

- On MX Series devices, during unified ISSU, the IPsec tunnels flap, causing a disruption of traffic. The IPsec tunnels recover automatically after the unified ISSU process is completed. PR1416334
- When using Group VPN, in certain cases, the PUSH ACK message from the group member to the group key server might be lost. The group member can still send rekey requests for the TEK SAs before the hard lifetime expiry. Only if the key server sends any new PUSH messages to the group members, those updates would not be received by the group member since the key server would have removed the member from registered members list.PR1608290

Resolved Issues

IN THIS SECTION

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

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

Resolved Issues: 22.1R1

IN THIS SECTION

Application Layer Gateways (ALGs)

- On Junos OS MX Series, the flowd daemon will crash if the SIP ALG is enabled and specific SIP messages are processed (CVE-2022-22175). PR1604123

- On Junos OS, flowd core observed if the SIP ALG is enabled and a specific Session Initiation Protocol (SIP) packet is received (CVE-2022-22178). PR1615438

Class of Service (CoS)

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

EVPN

- Baseline EVPN-VXLAN transition from IPv4 to IPv6 or vice verse does not work in certain sequence. PR1552498
- Bridge MAC-table learning entries might not be as expected for the EVPN-MPLS routing instance. PR1600310
- A few ARP/ND/MAC entries for VLANs are missing with MAC-VRF configuration. PR1609322
- Missing MAC address entries in EVPN MAC-table despite the presence of the corresponding Type 2 route. PR1611618
- Duplicate packets might be observed in EVPN-VXLAN scenario. PR1621574
- Some local ARP/ND entries might be lost on all Junos OS and Junos OS Evolved platforms. PR1625475
- Traffic loss for profile Tl2-Inter-VN-Traffic_Stream-SH-MH when testing EVPN with VXLAN. PR1628586
- The l2ald crash might be seen after performing restart routing on EVPN PE. PR1629426
- Removing configuration statement `es-label-oldstyle` does not take effect if it is the only configuration statement configured under the protocol EVPN. PR1629953
- In a scenario where multiple VXLAN type-5 tunnels with the same decap prefix(Vnid+ SrcIP + DestIP) are created within a VRF, and they are not handled on MPC10 and MPC11, it might lead to traffic drop. PR1630163
- The rpd might crash when moving an interface from VPLS to EVPN-VPWS instance. PR1632364
- The traffic loss might be seen when the link goes down for the local ESI. PR1632723
- When `no-arp-suppression` is configured in EVPN-MPLS, traffic forwarding is impacted. PR1646010

Flow-based and Packet-based Processing

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

Forwarding and Sampling

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

General Routing

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

  Junos 'et-' interface gets stuck and remains down between two particular ports. http://prsearch.juniper.net/PR1535078
- Junos 'et-' interface stuck and remains down between two particular ports. PR1535078
- On MX480, issuing the `help apropos` command in configuration mode is going to cause an mgd core. The mgd process will come up and as long as the command is not issued again, the core will not occur. PR1552191
-
- Egress IP MTU exception and fragmentation are not supported. PR1558327
- ARP resolution failure might occur in EVPN-VxLAN scenario. PR1561934
- The na-grpcd process might generate core files during the longevity tests. PR1565255
- When using log templates with unified policies, logs were not generated in a predictable manner. A new construct has been added that allows you to define a default log profile `set security log profile default-profile` can be used to improve this behavior when multiple log profiles are defined. PR1570105
- Interfaces might fail to come up on MX240, MX480 and MX960 platforms. PR1571274
- PKID core might occur during cert signature validation. This core is not very frequent and occurs due to memory corruption. PR1573892

- The chassisd process might crash on all Junos platforms that support Virtual Chassis or Junos fusion. PR1574669
- When Hwdre application failed on primary Routing Engine, GRES switchover will not happen. PR1575246
- MPC7E, MPC10E, MX-SPC3 and LC2103 line cards might go offline when the device is running on FIPS mode. PR1576577
- Unexpected close-timeout gets refreshed for TCP session of CGNAT on MX platforms with MS-MPC line card. PR1576675
- The subscribers over PS interface are not cleared after FPC offline. PR1580812
- The line cards might fail after hitting the I2C error on MX FPC. PR1583060
- The multicast traffic is not traversing across PS interface when it is anchored on RLT interface. PR1584041
- The `show route detail` might not show Next-hop type IPoIP Chained comp nh in the output (Display only - no operation impact). PR1584322
- The `show security idp counters` does not have `tenant` statement in the syntax. PR1586220
- A high rate of small packets could cause CPU hogging and the firmware crash in MPC5E and MPC6E line cards. PR1587551
- On MX10003 routers, PEM capacity shows incorrectly. PR1587694
- NAT EIM mapping is getting created even for out to in FTP ALG child sessions. PR1587849
-
- Some logical interfaces might go down under logical tunnel due to the limited number of MAC addresses in a pool. PR1591853
- The DCI InterVNI and IntraVNI traffic might get silently dropped and discarded in gateway node due to the tagged underlay interfaces. PR1596462
- Inconsistency in the platform name used in multiple places, version, snmp mibs, and so on. PR1597999
- The mspmand daemon memory leak might be observed after the HA primary goes down. PR1598356
- On MX10008 and MX10016 routers with JNP10K-RE1, unknown SMART attributes for StorFly VSFBM8CC200G SSD occurs. PR1598566

- EVPN-VXLAN, RE1 went to DB prompt when tried to load profile configurations over LRM configurations. PR1598814

- During day1 stage of device management from MIST, the cloud LED will remain in green state even if device loses connectivity with cloud. PR1598948

- The l2ald process might crash due to memory leak when all active interfaces in a VLAN are unstable. PR1599094

- Traffic might get dropped silently upon link flap after a topology change. PR1599215

- The SFP-T port might stop forwarding traffic. PR1600291

- The gNMI Telemetry might stop working after Routing Engine switchover. PR1600412

- Silent drop of traffic might be seen when multicast is configured on the device and there is a interface flap or FPC restarts. PR1600642

- Observed dcpfe core-dump while testing unified ISSU from 21.1R1.11 to 21.2R1.7. PR1600807

- Layer 2 host injected packets might not go out of IRB interface. PR1602131

- Under certain scaling scenarios with EVPN-VXLAN configurations, the l2ald process might be aborted and then recovered. PR1602244

- The Ipv6 link local BFD session might not come up if we do not have child link of an aggregated Ethernet mapped to Packet Forwarding Engine inst 0. PR1602493

- The `show system errors fru detail` command is not displaying `reset-pfe` as the cmerror configured action. PR1602726

- 21.3TOT:TCP_TLS_SYSLOG:core-usf-qnc-a-fpc3.pic1-flowd_spc3.elf.0.tgz is seeing while verifying TCP based logging functionality with GRES with AMS-Nexthop style. PR1603466

- The show commands `show services web-filter secintel-policy-status profile p1` and `show services web-filter secintel-policy-db ip-prefix-information` need to populate IP address count, term count related to blacklist, whitelist of global database and geo-ip database. PR1603517

- VRRP and BFD might flap on IRB interface on MPC10 and MPC11 line cards. PR1604150

- The adapted sample rate might get reset to the configured sample rate without changing the sampling rate information in sFlow datagrams. PR1604283

- NPC logs seen when vrf localisation is enabled. PR1604304

- Remote aggregated Ethernet member failures (via disable/laser-off) might cause the high tail drop to result in high traffic loss. PR1604823

- GRE tunnel might flap when hierarchical-scheduling is configured. PR1605189

- Traffic is not load balanced across member interfaces while configuring AMS bundle with 8 members interfaces. PR1605284
- Harmless error message might be seen when downgrading from 21.2/21.3/21.4 to 21.1 or older image on VMHost platform. PR1605915
- VM host platforms might boot exactly 30 minutes after executing `request vmhost halt` command. PR1605971
- 5G-CUPS:bbe-cups-5G-setup:wf-eabu-dev.tadcaster:re1 {version} vmcore.0.gz PR1606146
- Fabric error might be seen when MPC10E to MPC2, MPC3, MPC4, MPC5, MPC6 based FPC fabric traffic is congested. PR1606296
- Observing continuous SNMP trap for "Over Temperature!" for all the MX10016 line cards (FPC: JNP10K-LC480). PR1606555
- Random IP assignment might be done on MX Series platforms configured with PCP and DS-Lite. PR1606687
- The **WO-0: OGE0 dequeue watermark hit** might seen with Layer 2 related configuration and receiving jumbo-frame packets. PR1606967
- IPv6 link-local BFD session might not come up on MX Series platforms. PR1607077
- The speed auto-negotiated SFP-T transceiver might not be joined to the aggregated Ethernet after performing dcd restart or Routing Engine switchover on MX104. PR1607734
- Address error case in open message to comply to RFC 8664 in PCCD and PCE_Server. PR1608511
- Interface configuration might not take effect in race condition. PR1609365
- BFD over GRE tunnel interfaces gets stuck in **init** state with GRES enabled. PR1609630
- DHCP subscribers over PWHT might be dropped upon GRES after the system reboot. PR1609818
- On MX204, interface flaps might be observed on certain ports. PR1609988
- AMZN-QFX5200 mib OID ifOutDiscards misbehaving and returning value 0 which is not expected. PR1610540
- Traffic loss might be observed if dot1X is configured with **supplicant multiple** and authenticated user from radius is in single supplicant mode. PR1610746
- Traffic might not be processed when mams-members are replaced in the AMS bundle. PR1610977
- MACsec session might be dropped due to one way congestion. PR1611091

- Erratic behaviour might be seen on platforms using MPC line cards after unified ISSU is performed. PR1611165
- Inter-vlan connectivity might be lost in an EVPN-VXLAN with CRB topology. PR1611488
- The routing protocol engine CPU is getting stuck at 100%. PR1612387
- The B4 client traffic will be dropped on MX-SPC3 based AFTR in DS-Lite with EIM activated CGNAT scenario. PR1612555
- Some of the fabric links might go into faulty state after swapping FPC LC1201 with LC1202. PR1612624
- The PFE/SIB/SCBE/FPCs might reboot due to the unexpected fabric errors shown up on MX240, MX480 and MX960 platforms. PR1612957
- Traffic loss might be observed due to the shaping rate be adjusted incorrectly in a subscriber environment on MX Series platforms. PR1613126
- Enhanced-hash-key might not take effect when configured with forwarding-options. PR1613142
- For PS Service IFL configured in MPC2-NG/MPC3-NG interface stats do not show correct (shaped) value when shaping is applied. PR1613395
- Enabling security-metadata-streaming DNS policy might cause a dataplane memory leak. PR1613489
- Unknown SMART attributes for StorFly VSFBM6CC100G-JUN1 SSD might be seen.PR1614068
- FPCs might be stuck in **onlining** state after the software release upgrade. PR1614489
- Any irrelevant configuration changes might trigger NAT routes flap on MX in USF mode. PR1614688
- MPC6E 3D did not comes back up after MIC offline online test. PR1614816
- Modifying the input service-filter via COA might fail in subscriber management environment. PR1614903
- Export memory and temperature metrics for all existing components when it subscribes to telemetry sensor. PR1615045
- The l2ald process might crash in EVPN scenario. PR1615269
- Traffic drop might occur when huge number of EIM mappings are created or deleted continuously. PR1615332
- The CDA-BT process generates a core file when you turn the FPC offline. PR1615343
- Request to provide an API which gives list of potential policy given a session ID. PR1615355

- The counter might show double value when chassis enhanced-policer is configured. PR1615373
- The rasdaemon processes memory leak -- triggered by hardware memory errors on VMHost platforms. PR1615488
- On MX10008, TPI88812 Onchnage: /components/component[name='FPC7']/state/type after event does not have the correct jvalue. PR1616049
- Slow memory leak (32 bytes each time) of rpd might be seen. PR1616065
- No filter found error might be seen while deactivating filter attached to interface after MPC reboot. PR1616067
- VPLS BUM (Broadcast, Unknown Unicast, and Multicast) traffic does not get forwarded to remote PEs over the MPLS core. PR1616236
- The `show subscribers accounting-statistics` and `show services l2tp session interface asi0.xx statistics` might not work on LNS with asi- interfaces. PR1616454
- Observed traffic error on 100G FPC for DPT deep loopback test on ports et-0/0/6 and et-0/0/7. PR1616525
- The dual Routing Engine system might not be GRES ready after backup Routing Engine reboot in a subscriber management environment. PR1616611
- The Strict-Priority-Scheduler (SPS) might not work accurately across port queues. PR1616772
- The aftermand process generates core files at `RtIfaHandler::notifyCommand,EalIfaHandler::registryClientCommand ,EalIfaHandler::OnAdd (this=0x7f2ffe40e9a0 < EalIfaHandler::instance()::handler>, ifah=...) at ../../src/EalIfaHandler.cpp:222.` PR1616909
- Layer 2 cpd memory leak might lead to l2cpd process crash. PR1617151
- In MX Series Virtual Chassis spcd running on SPC3 crashes. PR1617280
- MPC8E in 1.6T bandwidth mode might not work correctly. PR1617469
- The l2cpd core file is seen with FIP snooping configuration on any interface. PR1617632
- Unexpected Routing Engine switchover might be observed. PR1617720
- Traceroute packets might get dropped in SFW service-set when other service-sets with asymmetric traffic processing are also enabled on the same MS-MIC/MS-MPC. PR1617830
- Match on v6-prefix for prefix lengths less than or equal to 64 bits does not work.PR1618211
- GMC clock class is seen transmitted for an additional 16 seconds after the PTP source switches from one line card to another. PR1618344

- Traffic loss might be observed if the router is configured with ECMP over IRB and the traffic go through the MPC10E and MPC11E line cards. PR1618354

- The traffic loss might be seen after cleaning the large-scaled NAT sessions in MS-SPC3 based Next Gen Services Inter-Chassis Stateful High Availability scenario. PR1618360

- The clksyncd might crash and PTP/SyncE might not work. PR1618929

- Support whole (atomic) updates at CNHG level. PR1619011

- InputIntf is reported incorrectly for MPLS-ipv4 and MPLS-ipv6 ingress sampling in the case of Layer 3 VPN. PR1619052

- The hardware process might crash when an FPC is pulled out or some power failure or fault occurs for the FPC. PR1619102

- ACI VLAN session setup might get failed. PR1619122

- The nsd might crash while validating NAT translation on MX Series platforms with SPC3. PR1619216

- Traffic might be dropped when the RSVP is configured with the `mtu-signaling`. PR1619510

- Additional commit warnings and errors were introduced to improve security log profile usability. PR1619694

- The /interfaces/interface/subinterfaces/subinterface/state/counters not exported during initial sync for on-change. PR1620160

- The bbe subscriber access services might be stuck while rebooting the one redundancy line-card of RLT interface. PR1620227

- On MX480 routers, output packet drop is observed while verifying services PCEF subscribers. PR1620421

- OAM CFM session does not come Up if ERPS configured and CFM control traffic uses the same VLAN as ERPS control traffic. PR1620536

- High wired memory utilization might be observed if GRES is enabled. PR1620599

- The EVPN type 5 routes might not be installed. PR1620808

- Static subscribers session might get stuck in initializing state after ungraceful routing engine switchover. PR1620827

- Incorrect sensor modeling or mapping when using /junos/system/linecard/interface/ native telemetry streaming. PR1621037

- SNMP get for MIB value for jnxRedundancyConfig does not work as expected. PR1621101

- SNMP get for MID ID for jnxRedundancySwitchoverReason does not work as expected. PR1621103
- IFLSet COS hierarchy might be missed in the backup leg after rebooting FPC. PR1621164
- Flapping of all ports in the same Packet Forwarding Engine might cause Packet Forwarding Engine to be disabled. PR1621286
- NSSU option is not available from Junos OS Release 21.2R1. This option is missing from the time UI component publish has been separated out. PR1621611
- PIC gets stuck in offlining state when offline command is issued right after transceiver plugin. PR1621694
- Traffic loss can be seen on the new primary Routing Engine post GRES. PR1621696
- Telemetry/jvision, system_id formate of AFT-MPC(MPC10E) is not aligned with non-AFT MPCs. PR1622073
- Chassis alarm **VMHost RE 0 Secure BIOS Version Mismatch**, firmware upgrade did not solve the issue. PR1622087
- When the PHY-Sync state of a line card moves to False, it internally disables the PHY-timestamping of PTP packets. PR1622108
- AFT firewall telemetry (ZT), suppressed **state**'container and modified field numbers in the render proto. This is to sync with uKernel proto. PR1622313
- Invocation of `netconf get` command will fail if there are no Layer 2 interfaces in the system. PR1622496
- Constant increase of PCS errors might be seen on channelized port. PR1622741
- The device will be unavailable while performing FIPS 140-2/FIPS 140-3 level 2 internal test on FreeBSD 12 based Junos OS platforms. PR1623128
- The port speed shows as 100G even though chassis configuration is set for 40G. This is just a cosmetic display issue. PR1623237
- The ethtraceroute core file is generated. PR1623443
- Packet loss might be seen when enabling output sampling on the source interface of tunnel. PR1624057
- The mcontrol might frequently miss keepalives from backup Routing Engine. PR1624623
- The `show pfe route ip` is getting timed out when route table size is large. PR1624629
- The aggregated Ethernet member link might not be correctly populated on the Packet Forwarding Engine after FPC restart on MX Series platforms. PR1624772

- Traffic drop is seen with egress features enabled on interface hosted on MPC10 and MPC11 line cards. PR1624804
- The process hwdfpc might crash. PR1624841
- On single IPSec tunnel with PMI when sending internet traffic packet processing might get delayed due to session management issue. PR1624974
- On Junos OS, specific packets over VXLAN cause FPC reset (CVE-2022-22171). PR1625292
- JNP10008-SF3, SIB-JNP10004 and JNP10016-SF3 memory errors handling improvement. PR1625305
- The flowd process lost heartbeat for 45 consecutive seconds without alarm raised. PR1625579
- The bbe-statsd crash might be seen in the LTS subscriber scenario. PR1625648
- The gNMI set RPC might fail when multiple values within a single gNMI SetRequest are used for the Junos telemetry interface. PR1625806
- Packet loops in the PIC even after stopping the traffic on MX Series platform with SPC3 line card. PR1625888
- Service set gets into INIT_PEND state after performing GRES on Junos OS platforms with SPC3 card. PR1626027
- The bbe-smgd might crash on backup Routing Engine after unified ISSU or GRES. PR1626091
- Traffic drop might be seen in node slicing scenario. PR1626115
- Some Interfaces might not come online after line card reboot. PR1626130
- Implement `show task scheduler-slip-history` to display number of scheduler slips and last 64 slip details. PR1626148
- After configuring 4000 bridge domains, messages log file floods with kernal messages. PR1626381
- The chassisd might crash on MX104. PR1626486
- The autoconf might not work if the DHCPv4 discover message has option 80 (rapid commit) ahead of option 82. PR1626558
- Broadcast traffic might not be forwarded to LT interface in VPLS routing instance after LT interface is deleted and then added back. PR1626714
- VPLS MAC age time-out might not be applied on some MAC addresses. PR1627416
- S-PTX10K-144C license SKUs do not load, 400G SKUs do load. PR1627459

- IP not-ECN-capable traffic is not RED-dropped in an ECN-enabled congested queue. PR1627496
- DHCP clients might not go to BOUND state when the aggregated Ethernet bundle is enabled between DHCP server and snooping device. PR1627611
- The shell upgrade script fails for releases earlier than Junos Os Release 21.4. PR1627618
- Tunnel interface statistics displays incorrect values when JFlow sampling is enabled. PR1627713
- Layer 3 traffic failure might be observed with scaled MC-LAG configuration. PR1627846
- Invalid IP length packets encapsulated within MPLS might trigger PPE traps. PR1628091
- Memory leak might occur on PFED process when the flat-file-profile is configured with configuration `use-fc-ingress-stats`. PR1628139
- The EAPol packets over l2circuit might get dropped at the tunnel start. PR1628196
- EVPN flood filter might not work for MPC10 and MPC11 line cards. PR1628270
- The traffic might be dropped on xSTP ports that were earlier in FWD/DESG state after unified ISSU. PR1628358
- Tunnel-service bandwidth should not be changed when there are active subscribers. PR1628628
- The **monitor traffic interface** might not work for em2.PR1629242
- The `show system subscriber-management route summary` does not report route summary as expected. PR1629450
- The l2ald might be stuck in **issu state** when unified ISSU is aborted. PR1629678
- MPC10E crashes in enhanced-cfm-mode when it receives CFM packets from ONT. PR1629685
- The egress traffic on non-targeted iflset of subscribers might not be forwarded correctly over targeted aggregated Ethernet interface. PR1629910
- Multiple link flaps and traffic might be lost on the links. PR1630006
- The kmd daemon might crash with core files every few minutes on MX Series platforms. PR1630070
- LACP timeout might be observed during high CPU utilization. PR1630201
- Indirect next-hop (INH) Version ID higher than 255 might cause INH NH FRR Session moved down state and dropping transit traffic. PR1630215
- With SCBE3+SPC3, fabric drops are seen around 10M PPS/60G TCP traffic with ~750byte packet size with IPv6 SFW on a single PIC. PR1630223

- Index of the link might get missed in the distribution table of Packet Forwarding Engines after the flap. PR1630408
- LLDP packets might be sent with incorrect source MAC for RETH or LAG child members. PR1630886
- The FPC might crash after enabling MACsec. PR1631010
- PCIe bus error associate to PTP FPGA device during chassis reboot. PR1631300
- The kmd might crash since the pkid requested memory leak happens on M/MX Series platforms. PR1631443
- The ipv6 host route prefix match disappear from **forwarding-table** after a ping test, ping continues to work, forwarding table entry is not shown. No impact in traffic. PR1631607
- Adverse effect on subscriber management observed after deactivating chassis pseudowire-service with active subscribers. PR1631787
- DHCP ALQ Syslog error bbesmgd[26939]: LIBSDB_RSMON_PS_TABLE_PTR_FAILURE: sdb_get_ps_interface_table_record:2076 failed to get the ps_table_header ptr. PR1631858
- The rpd process generates core file with the warm-standby configurations due to reference counting issues. PR1631871
- The transit CCM sessions comes up but transit loopback(LB) ping or LinkTrace(LT) PDUs does not go through. PR1632255
- High-speed key is not reported for MPC11 in AF interface sensor. PR1632289
- When deleting the VNI and there is another vlan-id-list with a different VNI, it might cause traffic loss. PR1632444
- Firewall sensors information of MPC10E, MPC11E, MPC12E, and VMX ZT MPC line-card are not getting streamed to telemetry. PR1632477
- Summit MX chassis communication does not work after Virtual Chassis member-id set/delete. PR1632645
- The bbe-smgd process might crash after removing and adding a child link from aggregated Ethernet interface. PR1633392
- The linecard crash might be observed in a subscriber scenario. PR1633825
- Slow chassis memory leak might occur when chassisd related configuration change is committed. PR1634164

- PTP clock class might incorrectly be downgraded to 248 when PTP is enabled on Linecard/MIC which does not support phy-timestamping. PR1634569
- The fpc might crash on enabling port-mirroring. PR1634570
- When all configured anchor Packet Forwarding Engines are offline on the SAEGW-u, there might be a peer association mis-match between the SAEGW-u and SAEGW-c. PR1634966
- CFM CCM PDU is not forwarded transparently on core MX if the IFD is configured under protocols OAM. PR1635293
- BCM SDK publish build failed with error message in description is fixed. PR1635318
- Data might not be exchanged through EVPN-VxLAN domain. PR1635347
- The LACP delay might be observed with an **aggregate wait time** of more than 1 second. PR1635763
- FPCs might get restarted due to either faulty PEM module. PR1636118
- DHCP offer not getting processed in the routing instance when using LT interfaces. PR1636579
- Incorrect interface statistics might be reported on MX204. PR1636654
- Delay might be observed for the interfaces to come up after reboot or transceiver replacement. PR1638045
- BNG CUPS: ERA & OIU - Core in oiuModShMemEntry during OIU modify when restarting smg-service while bouncing subscribers. PR1638217
- Locally switched traffic might be dropped with ESI configured. PR1638386
- Packet Forwarding Engine might get stuck after 100G or 400G interface flaps. PR1638410
-
- JUNOS: JDI_FT_REGRESSION:SUBSCRIBER_SERVICES:MX480: Time difference is not as expected when DUT exports interface-queue-stats to ipfix-collector tool after changing reporting-interval. PR1639378
- The `show network-agent statistics gnmi detail` CLI command is reporting packet drops for some gnmi target-defined mode sensors. PR1641483
- Traffic drop due to incorrect memory allocation for the default route on MPC10E and MPC11E line cards. PR1642851
- The KRT queue might get stuck with the error- **ENOMEM -- Cannot allocate memory**. PR1642172
- CFM traceoptions writes on every other line. PR1642948

- On MX480 platforms, PFED CPU increased post unified ISSU and remains around 65-75% for 32000 L2VPN sBNG services. PR1643077

- Traffic over conditional metric enabled LSP might get blackholed. PR1643587

-

- PCEP SRv6 code points changed as per IANA. PR1644332

- The video console for vRR might not work after an upgrade to Junos OS with upgraded FreeBSD. PR1644806

- Multicast traffic drop might be observed after performing Routing Engine switchover or rpd restart. PR1593810

- [ecmp] [ecmp] acx7509 : :: Unable to configure 256 ecmp paths. PR1609063

- The rpd agent might get crash during NSR switchover. PR1612725

- DHCP relay no-snoop might not work with DHCP local server in the same routing-instance. PR1613738

- DHCP subscribers might not be synchronized to backup BNG when DHCP ALQ is configured without topology-discover. PR1620544

- PDT: restart ppmd triggers **EAL NH NULL for child NH** and **EalNhHandler Modify: Nh with index: 383675 does not exist**. PR1628049

- DHCP ALQ needs a new configuration parameter to adjust failover times. PR1631770

High Availability (HA) and Resiliency

- Memory leaking might occur on backup Routing Engine when ksyncd is in inconsistent state and had encountered an initialization error. PR1601960

- When MTU is configured on an interface a rare ifstate timing issue could occur at a later point, resulting in ksyncd process crash on backup Routing Engine. PR1606779

Infrastructure

- A false error related to insufficient space might appear while installing a Junos OS image that is corrupted. PR1570148

- Net installation (PXE) is not working. PR1577562

- FreeBSD12: On Panic 0-size vmcore file get generated. PR1607299

- Egress TCP RST might not have correctly populated DSCP field. PR1612208
- Primary FPC might crash when user logs into the device post powercyle of a 3 member EX2300-MP VC. PR1625987

Interfaces and Chassis

- Traffic loss is seen after restarting the SIB. PR1560111
- Commit check failure might happen if similar interfaces are configured under VRRP group. PR1617020
- Delay in application of CLI configuration by DCD when aggregated Ethernet interface members are configured through JET API. PR1621482
- CFM enhanced SLA iterators monitoring might stop after restarting chassis-control daemon in vMX. PR1622081
- The subscribers might be deleted when `host-prefix-only` configuration statement is configured on the underlying-interface in GRES scenario. PR1630229
- The syslog messages and the dcd crash might be seen in Junos OS. PR1633339
- CFM sessions are not up after evo-pfemand restart or crash. PR1634721
- VRRP route tracking for routes in VRF might not work if **chained-composite-next-hop ingress l3vpn** is used. PR1635351
- Some daemons might get stuck when snmpd is at 100% CPU utilization. PR1636093
- FPC might crash if the continuity-check interval under CFM is modified. PR1636226
- [VALE] [USB-Upgrade] JDI_REG_TPTX_REGRESSIONS::The FPCs are not online with USB upgrade from 21.3R1.9 to 21.4R1.11. PR1637636
- The `show vrrp extensive` doesn't show the next IFL **Interface VRRP PDU statistics**. PR1637735
- On Junos 20.3 and later release, the tracking routes of VRRP might become unknown after upgradation. PR1639242
- The aggregated Ethernet interface with 400GE gets flapped on adding or removing a 400GE member link. PR1641585
- Traffic might be impacted due to the RCP session number reaching the maximum limit. PR1643855
- The vrrpd core file might be observed after interface state change. PR1646480

Junos Fusion Provider Edge

- Configuring port mirroring firewall filter in a bridge domain with IRB might cause traffic loss over IRB. PR1607750

Junos XML API and Scripting

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

Layer 2 Ethernet Services

- Making configuration changes with apply-group add/delete associated with DHCP might result in client connection failure. PR1550628
- DHCP leasequery is failing to restore binding when the reply is received over IRB interface. PR1611111
- BFD hold-down timer does not work properly when LAG is configured. PR1616764
- Enabling DHCP on Junos OS platform might cause the router's file system storage to get filled up with log files. PR1617695
- The Junos OS, the jdhcpd crashes upon receiving a specific DHCP packet (CVE-2022-22179). PR1618977
- Circuit-id handled incorrectly with backup node for ALQ with topology discover configured. PR1620461
- The jdhcpd process crashes in DHCP and DHCPv6 environment. PR1625011
- The process jdhcpd might get stuck at 100% post clients login or logout. PR1625112
- Option 82 might not be attached on DHCP request packets. PR1625604
- The rpd scheduler might continuously slip after GRES when there are 7000 DHCP clients in a subscriber management environment. PR1625617
- IPv6 IA_NA or IA_PD routes might get deleted from the DHCPv6 client. PR1629171
- Non-DHCPv4 BOOTP protocol packets might not be processed if enhanced subscriber management is enabled. PR1629172
- The aggregated Ethernet interface remains UP instead of down on deleting loopback and aggregated Ethernet interface IP on neighbor while verifying BFD sessions on router. PR1640240

MPLS

- The node SID might be seen in an unresolved state. PR1564169
- IS-IS BFD sessions might take a long time to recover when the interface flaps. PR1593959
- IPv4 prefixes might be associated into both IPv4 and IPv6 LDP database after Routing Engine switchover. PR1611338
- Configuring protocols MPLS lsp-external-controller also throws commit error if in-place-lsp-bandwidth-update is configured under any LSP. PR1612269
- The rpd process might generate core files for a few value configurations of signaling bandwidth on container LSP. PR1614248
- The RPD crash might happen due to refcount leak in routing table metrics. PR1615001
- Standby secondary LSP might be stuck on the same path as primary LSP upon reoptimization. PR1615326
- Protected LSP goes down with strict hops and link protection configured. PR1616841
- LDP protections paths might not be established when `auto-targeted-session` configuration is deactivated and activated. PR1620262
- Underlay Colored SRTE LSP is being wrongly shown as RSVP LSP in express-segments detail. PR1623643
- Unexpected traffic loss on LSP headend might be observed when downstream IGP metric changes. PR1625438
- VCCV BFD session keeps flapping between MX and peer device if ultimate-hop popping is enabled. PR1634632
- [mpls] [LDP-Tunneling] : mx2020 :: rpd core@ldp_destroy_lib is observed in mx2020 after post Gress. PR1635863
- The rpd memory leak might be observed in a subscriber management environment with RSVP. PR1637645
- LSP over broadcast segment stays down when RSVP setup protection is enabled. PR1638145
- Dynamic bypass LSP might flap at every re-optimization interval. PR1639292
- When the primary path goes down MPLS LSP does not use the most preferred path after the primary path restoration. PR1640918

Network Management and Monitoring

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

Platform and Infrastructure

- The ppmd process might crash after an upgrade. PR1335526
- Packet Forwarding Engine NH free error messages are seen on all FPCs. PR1543684
- The subscribers might not come online after interface flaps on MX Series platforms. PR1591905
- Traffic through one SPU might stop with potential packet drop issue with alarm as FPC Major Errors raised due to the PIC_CMERROR_TALUS_PKT_LOSS error. PR1600216
- On MX Series platforms vmcore on both the Routing Engines might be reported due to mbuf corruption. PR1602442
- The FPC might crash if `flow-table-size` is configured on MX Series platforms. PR1606731
- CFM neighbor adjacency will be failed on the aggregated Ethernet member interface of MPC10 and MPC11 line cards. PR1611816
- Filter related service will not work when the filter is deleted/re-added frequently for aggregated Ethernet interface. PR1614480
- Degraded traffic processing performance might be observed in case of processing very high PPS rate traffic. PR1619111
- CoS custom classifier might not work on logical interface. PR1619630
- Accounting and auditd process might not work on secondary node. PR1620564
- Trio-based line cards might crash when Packet Forwarding Engine memory is hot-banking. PR1626041
- Configuration commit might fail while configuring the configuration statement `authentication-key-chains` under groups. PR1626400
- Unrealistic service accounting statistics might be reported due to firewall counter corruption. PR1627908
- Error message **gencfg_cfg_msg_gen_handler drop** might be seen after running commit. command PR1629647

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

Routing Policy and Firewall Filters

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

Routing Protocols

- When igmp-snooping is removed from the device, the device might encounter inconsistent MCSNOOPD. PR1569436
- New version of OpenSSL (1.1.1) is not supported for NTF-agent of Junos Telemetry Interface. PR1597714
- After first parallel unified ISSU aborts, subsequent unified ISSU attempts on failed node aborts with **Aborting Daemon Prepare**. PR1598786
- Observing commit error while configuring **routing-options rib inet6.0 static** on all Junos OS platforms. PR1599273
- The rpd core might be observed due to memory corruption. PR1599751
- Kernel crash might be observed on platforms that have BGP configured with family Layer 2 VPN. PR1600599
- The BGP replication might be stuck in **InProgress** state. PR1606420

- The commit should fail when microloop-avoidance post-convergence-path is configured without source-packet-routing. PR1608992
- The rpd might crash after a commit if there are more than one address in the same address ranges configured under **bgp allow**. PR1611070
- The interface might receive multicast traffic from a multicast group which it is not interested in. PR1612279
- Undesired protection path might get selected for some destination prefixes. PR1614683
- The memory leak on rpd might be observed after running `show route` CLI command. PR1615162
- BFD sessions flapping might occur after performing GRES. PR1615503
- The incorrect BGP path might get selected even when a better/preferred route is available. PR1616595
- Traffic drop will be seen when VPN labels are incorrectly allocated due to change in nexthop. PR1617691
- Verification of BGP peer count fails after deleting BGP neighbors. PR1618103
- On Junos OS, OpenSSL Security Advisory. PR1618985
- The rpd might crash and restart when NSR is enabled. PR1620463
- The aggregated Ethernet interface might send/receive traffic through child link though BFD status is **client in hold-down state**. PR1624085
- Time delay to export prefixes to BGP neighbors might occur post applying peer-specific BGP export policies. PR1626367
- The rpd core file might be seen while processing the BGP updates. PR1626717
- Multipath route with List-NH which has Indirect-NH as members fails into BGP-LU. PR1626756
- eBGP Multipath route stuck in KRT queue. PR1626966
- For prefixes leaked from BGP to IS-IS, the P flag will be set for Prefix-SID advertised from IS-IS. PR1627322
- The contributing routes might not be advertised properly if **from aggregate-contributor** is used. PR1629437
- The multicast forwarding cache might not get updated after deactivating the scope-policy configuration. PR1630144
- The BGP ECMP might not work and multipath route won't be created. PR1630220

- The rpd might crash when BGP labeled-unicast family routes are present and BGP multipath is turned on. PR1630987
- The rpd might crash after clearing IS-IS database. PR1631738
- The rpd might get into an infinite loop while clearing IS-IS database. PR1632122
- The BGP session might flap after rpd crash with **switchover-on-routing-crash** and NSR enabled in a highly scaled environment. PR1632132
- IS-IS database might not be synchronized in some multiple areas scenario. PR1633858
- OSPF adjacency might take longer time to converge when the neighbour restarts non-gracefully. PR1634162
- Multipath route gets formed for a VPN prefix due to incorrect BGP route selection logic. PR1635009
- The multicast traffic might get dropped in the Packet Forwarding Engine. PR1638141
- The BGP peer might stay down in shards after doing a rollback. PR1643246
- The BGP route might still be present in the multi-path route after increased IGP cost. PR1643665
- Traffic impact might be seen due to failure of IS-IS shortcuts. PR1645414

Services Applications

- L2TP tunnels might go down and not be able to re-establish after restarting the bbe-smgd process. PR1629104
- Tunneled subscribers might be stuck in terminating state in L2TP subscriber scenario. PR1630150
- The kmd crash might be observed in IPsec scenario. PR1637906
- DTCP radius-flow-tap fails to program Packet Forwarding Engine when trigger X-NAS-Port-Id exceeds 48 character length. PR1647179

Subscriber Access Management

- Install discard routes is not supported on APM managed BNGs running Junos OS Release 21.3R1. PR1604967
- Class attribute is corrupted for radius accounting messages since unified ISSU to 19.1 or higher release on MX Series platforms. PR1624066
- Radius CoA (Change of Authorization) NAK might not be sent with the configured Source Address in a virtual-router environment. PR1625858

- ESSM sessions might get terminated in radius as class attribute has got corrupted after performing unified ISSU. PR1626718

- When connectivity between BNG and APM is lost, the BNG does not regenerate pool drained alarms to APM. PR1627974

- Event-timestamp in radius Acct-Stop might show future time. PR1643316

User Interface and Configuration

- Mgd might generate core files while running any RPC after running copy-config rpc with unreachable host in the URL on the same NETCONF session. PR1590625

- Interface configuration might get stuck and might not update after several ephemeral commits. PR1598123

- Unable to delete Linux core files by using `file delete /var/core/*/vmcore*` CLI command. PR1624562

- Junos OS upgrade might fail with error **configuration database size limit exceeded**. PR1626721

- The process mgd might crash with errors if `system scripts synchronize` is configured. PR1628046

VPNs

- The multicast route is not getting installed after exporting of secondary routes from one instance to another. PR1562056

- The rpd process might crash during unified ISSU if the `auto-sensing` configuration statement is enabled for l2circuit. PR1626219

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

- The Multicast Tunnel interface is not selected as per the configuration for the Draft-Rosen. PR1642182

- The device enabled with FIPS mode and rebooted the system fails to boot. PR1655355

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 22.1R1

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-
      x86-32-22.1R1.9-signed.tgz
      ```

    - For 64-bit Routing Engine version:

      ```
      user@host> request system software add no-validate reboot source/junos-install-mx-
      x86-64-22.1R1.9-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-
      x86-32-22.1R1.x-limited.tgz
      ```

    - For 64-bit Routing Engine version:

      ```
      user@host> request system software add no-validate reboot source/junos-install-mx-
      x86-64-22.1R1.9-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 22.1R1, 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 22.1R1 jinstall package, you cannot return to the previously installed Junos OS (FreeBSD 6.x) software by issuing the `request system software rollback` command. Instead, you must issue the `request system software add no-validate` command and specify the jinstall package that corresponds to the previously installed software.

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

Upgrade and Downgrade Support Policy for Junos OS Releases

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

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

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

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

Upgrading a Router with Redundant Routing Engines

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

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

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

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

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

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

Downgrading from Release 22.1R1

To downgrade from Release 22.1R1 to another supported release, follow the procedure for upgrading, but replace the 22.1R1 jinstall package with one that corresponds to the appropriate release.

> **NOTE**: You cannot downgrade more than three releases.

For more information, see the Installation and Upgrade Guide.

Junos OS Release Notes for NFX Series

IN THIS SECTION

These release notes accompany Junos OS Release 22.1R1 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

IN THIS SECTION

Learn about new features introduced in this release for the NFX Series devices.

What's New in 22.1R1

IN THIS SECTION

Learn about new features or enhancements to existing features in this release for the NFX Series.

Architecture

- **Custom mode (NFX150 devices)**—Starting in Junos OS Release 22.1R1, you can define and specify a custom-mode template for NFX150 devices. Custom mode provides an option to allocate resources to the Layer 2 data plane, Layer 3 data plane, and Network Functions Virtualization (NFV) backplane. The custom mode supports only basic firewall features.

  [See NFX150 Overview.]

- **Enhancements to custom-mode configuration (NFX250 NextGen and NFX350 devices)**—Starting in Junos OS Release 22.1R1, we've enhanced the custom-mode configuration to support optimal use of CPU and memory resources. You can limit the CPU utilization of the Layer 3 data plane by configuring the `cpu colocation quota` parameter. This configuration allows for sharing of CPUs in deployments where the Layer 3 data plane does not require a dedicated CPU. You can configure the CPU utilization rate in custom mode by using the `set vmhost mode custom` *`name`* `layer-3-infrastructure cpu colocation quota` *`quota-value`* command.

We've also introduced support to pin the emulator to specific physical CPUs.

[See NFX350 Overview and NFX250 NextGen Overview.]

IPv6

- **Router advertisement proxy support (NFX Series, SRX Series, vSRX, and vSRX 3.0)**—Starting in Junos OS Release 22.1R1, we support router advertisement proxy on the listed devices. With this functionality, the device can proxy the router advertisement packets from a service provider router to the clients (host).

  [See Router Advertisement Proxy, downstream, downstream-mode, upstream-mode, and show ipv6 router-advertisement.]

Juniper Advanced Threat Prevention Cloud (ATP Cloud)

- **IoT device discovery and classification (NFX150, NFX350, SRX340, SRX345, SRX4100, SRX4200, SRX5400, SRX5600, SRX5800 line of devices, and vSRX)**—In Junos OS Release 22.1R1, we introduce the Internet of Things (IoT) device discovery and classification feature on the listed devices.

  In a typical workflow:

  1. A security device identifies IoT devices based on the traffic flow.

  2. The device streams relevant packet metadata to Juniper Advanced Threat Prevention (ATP) Cloud.

  3. Juniper ATP Cloud discovers and classifies IoT devices based on brand, device model, type, and so on.

  You can view the list of identified IoT devices on the Juniper ATP Cloud portal. You can also create threat feeds to enforce security policies across IoT traffic in the network.

  With the knowledge of IoT devices in a network, network administrators can better manage their network security and reduce the IoT attack surface.

  [See IoT Security Overview.]

Network Management and Monitoring

- **Support for libvirt MIB traps (NFX150, NFX250 NextGen, and NFX350)**—Starting in Junos OS Release 22.1R1, you can enable libvirt MIB traps for NFX Series devices. The livbirt MIB traps monitor the virtual network functions (VNFs) and send notifications to the network management server when an event (for example, a VNF crash) occurs. The host OS generates the traps and sends them to the network management server through the snmptrapd daemon on vjunos0. You can use either SNMPv2c or SNMPv3 to configure the traps.

[See Configuring SNMP on NFX150, NFX250 NextGen, and NFX350 Devices.]

What's Changed

IN THIS SECTION

There are no changes in behavior and syntax in Junos OS Release 22.1R1 for NFX Series devices.

What's Changed in Release 22.1R1

Known Limitations

IN THIS SECTION

Learn about known limitations in Junos OS Release 22.1R1 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.

Interfaces

- When you issue a show interface command on NFX150 devices to check the interface details, the system does not check whether the interface name provided is valid or invalid. The system does not generate an error message if the interface name is invalid. PR1306191

Open Issues

IN THIS SECTION

Learn about open issues in Junos OS Release 22.1R1 for NFX Series devices.

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

General Routing

- On the NFX350, if you change the device operational mode to custom mode, ovs-vswitchd cores might be seen on the device. PR1634245

Platform and Infrastructure

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

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

  PR1664814

Resolved Issues

IN THIS SECTION

Learn about the issues fixed 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.

Resolved Issues: 22.1R1

IN THIS SECTION

General Routing

- On NFX150 devices, the destination service lookup does not work with UDP and TCP if a port range is not configured. PR1636174
- On NFX250 device, core files are dumped into the device when you delete vmhost VLANs. PR1637649

Interfaces

- The data displayed by the CLI command `show system visibility jcp` in the JCP Interfaces, JCP Interfaces Statistics, and JCP Disk Information sections is shifted to the right by one column.PR1600414

Routing Protocols

- FIPS mode enabling fails with self-test failure and kernel crash.

PR1623128

Migration, Upgrade, and Downgrade Instructions

IN THIS SECTION

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

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

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

Upgrade and Downgrade Support Policy for Junos OS Releases

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

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

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

Basic Procedure for Upgrading to Release 22.1

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

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

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

To download and install Junos OS Release 22.1R1:

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 22.1R1 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

IN THIS SECTION

Learn about new features introduced in this release for PTX Series routers.

What's New in 22.1R1

IN THIS SECTION

Learn about new features or enhancements to existing features in this release for PTX Series routers.

Forwarding Options

- **Support to exclude MAC addresses for load balancing** (PTX1000, PTX5000, PTX10002, and QFX10002-60C). You can use the `no-destination-mac` option to exclude the destination MAC address in the hash key for load balancing. Use the `source-mac` option to include source MAC addresses in the hash key.

  [See enhanced hash key.]

Hardware

Routing Policy and Firewall Filters

- **Programmed RPD route statistics (MX960, MX2020, PTX1000, PTX10008, and PTX10016)**—Starting in Junos OS 22.1R1 release, you can capture the routes statistics `Statistics ID Group` and `Statistics` of routes. To capture the route statistics, you must configure the `enable_stats` through the `japi` in programmable RPD (PRPD) API.

  The route statistics are displayed only for ingress traffic on label-switched path (LSP).

  [See show route extensive and show route detail.]

Routing Protocols

- **Support for DDoS IS-IS classification (MX Series with MPCs MPC1 through MPC9, PTX1000, PTX5000, PTX10002, PTX10008, QFX10002, QFX10002-60C, QFX10008, and QFX10016)**—Starting in Junos OS Release 22.1R1, Junos OS classifies IS-IS hello packets and IS-IS data packets separately. You can apply different policers to different types of IS-IS packets to improve the performance of IS-IS during congestion so that IS-IS doesn't go down when a large number of packets are entering the device.

  Configure DDoS protection settings for IS-IS hello packets and IS-IS data packets separately using the `isis-hello` or `isis-data` statement at the `[edit system ddos-protection protocols isis]` hierarchy level. Use the `show ddos-protection protocols isis parameters brief` command to view the aggregate number of IS-IS packets as well as the number of IS-IS hello packets and IS-IS data packets.

  [See protocols (DDoS) (ACX Series, PTX Series, and QFX Series) and show ddos-protection protocols isis.]

- **Support for adaptive RSVP update threshold (cRPD, MX240, MX480, MX960, PTX1000, PTX10008, QFX10002-60C, and QFX10008)**—Starting in Junos OS Release 22.1R1, you can configure the RSVP update threshold percentage and threshold value to adaptively pace IGP updates. You can configure a lower frequency when the adaptive bandwidth is higher and configure a higher frequency when the bandwidth is lower.

  You can enable the threshold percentage by using the `update-threshold adaptive limit` *`limit`* `threshold-percent` *`percentage`* configuration, and threshold value by using the `update-threshold adaptive limit` *`limit`* `threshold-value` *`value`* `configuration` at the `edit protocols rsvp interface` hierarchy level.

  NOTE: You cannot configure both `threshold-percent` and `threshold-value` simultaneously on the same interface.

  [See update-threshold.]

Source Packet Routing in Networking (SPRING) or Segment Routing

- **Avoid microloops in OSPFv2 segment routing networks (ACX5448, ACX6360, MX Series, PTX Series, and QFX10002)** —Starting in Junos OS Release 22.1R1, you can enable post-convergence path calculation on a device to avoid microloops if a link or metric changes in an OSPFv2 segment routing network. Note that microloop avoidance is not a replacement for local repair mechanisms such as topology-independent loop-free alternate (TI-LFA), which detects local failure very fast and activates a precomputed loop-free alternative path.

To configure microloop avoidance in an OSPFv2 segment routing network, include the `maximum-labels` and `delay` *`milliseconds`* statements at the `[edit protocols ospf spf-options microloop avoidance post-convergence-path]` hierarchy level.

[See How to Configure Microloop Avoidance for OSPFv2 SR Networks.]

System Management

- **Support for Network Time Protocol (NTP) version 4.2.8p15 (ACX Series, MX Series, PTX Series, and QFX Series)**—Starting in Junos OS Release 22.1, we support the latest NTP version 4.2.8p15. The latest version provides improved device security.

  [See NTP Overview.]

Additional Features

We've extended support for the following features to these platforms.

- **OpenConfig LACP and LLDP configuration support** (ACX5448 router, EX4650, and EX4650-48Y-VC switches, MX480, MX960, MX10003, and PTX10008 routers, , QFX10002-60C, QFX5110, QFX5110-VC, QFX5110-VCF, QFX5120-32C, QFX5120-48T, QFX5120-48T-VC, QFX5120-48Y, QFX5120-48Y-VC, QFX5120-48YM, QFX5200, QFX5210, , QFX10002, QFX10003, QFX10008, and QFX10016 switches). OpenConfig configuration support based on the OpenConfig data models openconfig-lacp.yang and openconfig-lldp.yang.

  [See Mapping OpenConfig LLDP Commands to Junos Configuration and OpenConfig User Guide.]

- **Support for endpoint de-encapsulation and specific IP table lookup (PTX Series)** In enhanced mode, we support the endpoint de-encapsulation of outer IPV6 header and lookup of the inner IPV4 or IPv6 packets in specific route table defined by the end dt46 SID route's nexthop. This enables configuration of BGP-based Layer 3 services over the SRv6 core network with BGP as the control pane and SRv6 as the dataplane,

  [See Understanding SRv6 Network Programming and Layer 3 Services over SRv6 in BGP]

- **System OpenConfig configuration support and gNMI mixed-mode support** (ACX5448, MX240, MX480, MX960, MX10003, MX10008, MX10016, MX2008, MX2010, MX2020, and PTX10002)

  [See OpenConfig User Guide].

- **VLAN-level MACsec on logical interfaces** (EX9253 and QFX5120-48YM)

  [See Media Access Control Security (MACsec) over WAN.]

What's Changed

IN THIS SECTION

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

What’s Changed in Release 22.1R1

IN THIS SECTION

Junos OS API and Scripting

- **The `<request-system-zeroize>` RPC response indicates when the device successfully initiates the requested operation (ACX Series, EX Series, MX Series, PTX Series, QFX Series, SRX Series, vMX, and vSRX)**—When the `<request-system-zeroize>` RPC successfully initiates the zeroize operation, the device emits the `<system-zeroize-status>zeroizing re0</system-zeroize-status>` response tag to indicate that the process has started. If the device fails to initiate the zeroize operation, the device does not emit the `<system-zeroize-status>` response tag.

Network Management and Monitoring

- **Junos XML protocol Perl modules deprecated (ACX Series, EX Series, MX Series, PTX Series, QFX Series, SRX Series, vMX, and vSRX)**—We no longer provide the Junos XML protocol Perl client for download. To use Perl to manage Junos devices, use the NETCONF Perl library instead.

  [See Understanding the NETCONF Perl Client and Sample Scripts.]

- **Changes when deactivating or deleting instances of the ephemeral configuration database (ACX Series, EX Series, MX Series, PTX Series, QFX Series, SRX Series, vMX, and vSRX)**—The following changes apply when you deactivate or delete ephemeral database instances in the static configuration database:

  - When you deactivate the entire `[edit system configuration-database ephemeral]` hierarchy level, the device deletes the files and corresponding configuration data for all user-defined ephemeral instances. In earlier releases, the files and configuration data are preserved; however, the configuration data is not merged with the static configuration database.

  - When you delete an ephemeral instance in the static configuration database, the instance's configuration files are also deleted. In earlier releases, the configuration files are preserved.

  - You can delete the files and corresponding configuration data for the default ephemeral database instance by configuring the `delete-ephemeral-default` statement in conjunction with the `ignore-ephemeral-default` statement at the `[edit system configuration-database ephemeral]` hierarchy level.

  [See Enable and Configure Instances of the Ephemeral Configuration Database.]

- **Support for automatically synchronizing an ephemeral instance configuration upon committing the instance (EX Series, MX Series, MX Series Virtual Chassis, PTX Series, QFX Series, and vMX)**—You can configure an ephemeral database instance to synchronize its configuration to the other Routing Engine every time you commit the ephemeral instance on a dual Routing Engine device or an MX Series Virtual Chassis. To automatically synchronize the instance when you commit it, include the `synchronize` statement at the `[edit system commit]` hierarchy level in the ephemeral instance's configuration.

  [See Commit and Synchronize Ephemeral Configuration Data Using the NETCONF or Junos XML Protocol.]

User Interface and Configuration

- **Load JSON configuration data with unordered list entries (ACX Series, EX Series, MX Series, PTX Series, QFX Series, SRX Series, vMX, and vSRX)**—The Junos schema requires that list keys precede any other siblings within a list entry and appear in the order specified by the schema. Junos devices provide two options to load JSON configuration data that contains unordered list entries:

  - Use the `request system convert-json-configuration` operational mode command to produce JSON configuration data with ordered list entries before loading the data on the device.

  - Configure the `reorder-list-keys` statement at the `[edit system configuration input format json]` hierarchy level. After you configure the statement, you can load JSON configuration data with unordered list entries, and the device reorders the list keys as required by the Junos schema during the load operation.

  When you configure the `reorder-list-keys` statement, the load operation can take significantly longer to parse the configuration, depending on the size of the configuration and number of lists. Therefore, for large configurations or configurations with many lists, we recommend using the `request system convert-json-configuration` command instead of the `reorder-list-keys` statement.

[See json and request system convert-json-configuration.]

Known Limitations

IN THIS SECTION

Learn about known limitations in Junos OS Release 22.1R1 for PTX Series routers.

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

General Routing

- When number of routes resolves over ECMP path, inline BFD sessions might flap during clear IS-IS adjacency or RPD restart trigger. PR1612802

Infrastructure

- When upgrading from Junos OS Release 21.2 and earlier to Junos OS Release 21.2 and later, validation and upgrade fails. Use the `no-validate` command to upgrade. PR1568757

Open Issues

IN THIS SECTION

Learn about open issues in Junos OS Release 22.1R1 for PTX Series routers.

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

General Routing

- PTX Series platforms with the FPC-PTX-P1-A or FPC2-PTX-P1A line card might encounter a single event upset (SEU) event that causes a linked-list corruption of the TQCHIP. The following syslog message gets reported: `Jan 9 08:16:47.295 router fpc0 TQCHIP1: Fatal error pqt_min_free_cnt is zero Jan 9 08:16:47.295 router fpc0 CMSNG: Fatal ASIC error, chip TQ Jan 9 08:16:47.295 router fpc0 TQ Chip::FATAL ERROR!! from PQT free count is zero jan 9 08:16:47.380 router alarmd[2427]: Alarm set: FPC color=RED, class=CHASSIS, reason=FPC 0 Fatal Errors - TQ Chip Error code: 0x50002 Jan 9 08:16:47.380 router craftd[2051]: Fatal alarm set, FPC 0 Fatal Errors - TQ Chip Error code: 0x50002` The Junos OS chassis management error handling does detect such a condition, raises an alarm, and performs the disable-pfe action for the affected Packet Forwarding Engine entity. To recover this Packet Forwarding Engine entity, restart the FPC as needed. Soft errors are transient or non-recurring. FPCs experiencing such SEU events do not have any permanent damage. Contact your Juniper Networks support representative if the issue occurs after an FPC restart.PR1254415

- Flapping might occur on the channelized ports of PTX Series routers during ZTP, when one of the port gets disabled on the supporting device. PR1534614

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

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

- The `output-mac-control-frames` and `output-mac-pause-frames` counters do not increase. PR1610745

- On PTX Series devices using QSFP and optic toolkit, QSFP in slot et-0/0/0 might not come up after plug-in. When this happens, one or a few ports might start showing i2c errors and eventually not come up. When this happens, the link does not come up in that particular port.PR1620527

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

- This is a rare scenario. In a dual Routing Engine setup, Assume the backup RPD has just started and re-syncing all states from FIB(Kernel). The backup RPD is not yet ready for switchover. If we do Routing Engine switchover manually through CLI or if any primary Routing Engine HW crash occurs, We end up in not installing some of the FIB entries. The work around is to restart the RPD in new primary Routing Engine. PR1641297

- While loading baseline configurations in Gladiator box, continuous FPC core seen at pci_user_pio_read_func and posix_interface_abort along with scheduler hog messages. PR1644576

- In current Junos OS implementation, MAC-vrf doesn't support MAC limit configuration. As a result of this, MAC-vrf instance extensive command won't show customer configured value correctly. In the following output, MAC limit count is set 262144 which is unexpected. user@router# show routing-instances TEST | display set set routing-instances TEST protocols evpn mac-table-size 100 set routing-instances TEST protocols evpn interface-mac-limit 10 user@router> show mac-vrf forwarding instance TEST extensive Information for routing instance and VLAN: Routing instance : TEST RTB index: 51 MAC limit: 262144 MACs learned: 0 Local Macs learned: 0PR1647327

- When there is a telemetry subscription to /components/component/ subscription path, data for chassis will not get exported. PR1647745

- V6 default route will not get added after successful DHCPv6 client binding on PTX1000 router during zero-touch provisioning. PR1649576

Interfaces and Chassis

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

MPLS

- On PTX3000 routers, if RPD thrashes during a GRES switchover, there might be traffic loss on MPLS LSPs. PR1590681

Platform and Infrastructure

- In rare occurrence, Routing Engine kernel might crash while handling TCP sessions if you enable GRES/NSR. PR1546615

User Interface and Configuration

- On all Junos OS and Junos OS Evolved devices, when copy-configuration, get-configuration, and discard-change RPCs run in two parallel NETCONF sessions and the database is also accessed in parallel by two NETCONF sessions, it leads to database corruption and mgd-related services might crash. PR1641025

Resolved Issues

IN THIS SECTION

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

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

Resolved Issues: 22.1R1

IN THIS SECTION

General Routing

- IS-IS over Layer 2 circuit does not come up if the encapsulation is translation cross-connect. PR1590387

- On PTX10001-36MR platforms, inconsistency occurs in the platform name used in multiple places, version, and snmp mibs. PR1597999

- FPC does not become fully offline after the FPC BAD_VOLTAGE fault gets reported. PR1602556

- MACsec session might be dropped due to one way congestion. PR1611091

- The **FPC 0 Major Errors** alarm might be generated on PTX10002-60C device due to a rare timing issue. PR1613229

- VCCV for LDP signaled pseudowire goes down periodically on PTX10008 and PTX10004 devices with Junos OS. PR1615419

- The rasdaemon processes memory leak gets triggered by hardware memory errors on the VMHost platforms. PR1615488

- On PTX10008 and PTX10016 devices, 90 percent traffic gets dropped when the number of Switch Interface Board (SIB) plane gets reduced from 4 to 3. PR1615942

- Slow memory leak (32 bytes each time) of rpd might occur. PR1616065

- Memory leak might be seen when you configure LLDP. PR1617151

- Unexpected Routing Engine switchover might be observed. PR1617720

- Performance of Jflow service might be impacted on PTX platforms. PR1617932

- Traffic loss might be observed with some MPLS labels in the multipath BGP scenarios. PR1618507

- The /interfaces/interface/subinterfaces/subinterface/state/counters not exported during initial sync for on-change. PR1620160

- ZTP does not work properly on PTX platforms if an EX device is used as a DHCP server. PR1621987

- The mcontrol might frequently miss keepalives from backup routing engine. PR1624623

- Tunnel interface statistics displays incorrect values when jflow sampling is enabled. PR1627713

- EAPol packets over l2circuit might get dropped at the tunnel start. PR1628196

- On PTX platforms, the ddos-protection protocols group ARP counters does not show correct values. PR1629097

- [interface] [snmp-trap] ptx10002-60c : :: SNMP Trap message for fpc restart, shows as FRU removal instead of Fru Offline/Fru Power off. PR1629738

- Multiple link flaps and traffic might be lost on the links. PR1630006

- The rpd process might generate core files with warm-standby configurations due to reference counting issues. PR1631871

- SPMB might crash immediately after a switchover. PR1637950

- Traffic over conditional metric enabled LSP might get blackholed. PR1643587

Interfaces and Chassis

- [VALE] [USB-Upgrade] JDI_REG_TPTX_REGRESSIONS::The FPCs are not online with USB upgrade from 21.3R1.9 to 21.4R1.11. PR1637636

Layer 2 Ethernet Services

- BFD hold-down timer does not work properly when you configure LAG. PR1616764

- The aggregated Ethernet interface remains in the **Up** state instead of **Down** state on deleting the loopback and aggregated Ethernet interface IP on neighbor while verifying BFD sessions on router. PR1640240

MPLS

- IPv4 prefixes might be associated into both IPv4 and IPv6 LDP database after Routing Engine switchovers. PR1611338
- The RPD might crash due to reference count leak in routing table metrics. PR1615001
- Unexpected traffic loss on LSP headend might be observed when downstream IGP metric changes. PR1625438

Routing Policy and Firewall Filters

- Filters in openconfig acl execute terms in the order of their definition and not based on sequence-ids. PR1621620

Routing Protocols

- Delay occurs in adding or removing static routes from the router. PR1612173
- Undesired protection path might get selected for some destination prefixes. PR1614683
- The rpd might crash and restart when you enable NSR. PR1620463
- Aggregated Ethernet interface might send or receive traffic through child link even though the BFD status is client in the **hold down** state. PR1624085
- The rpd dump file might be seen while processing the BGP updates. PR1626717
- The rpd might crash after clearing IS-IS database. PR1631738
- The BGP route might still be present in the multi-path route after increased IGP cost. PR1643665

User Interface and Configuration

- Not able to delete Linux core using CLI `file delete /var/core/*/vmcore*`. PR1624562

Migration, Upgrade, and Downgrade Instructions

IN THIS SECTION

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

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

Basic Procedure for Upgrading to Release 22.1

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

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

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

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

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

To download and install Junos OS Release 22.1R1:

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-
x86-64-22.1R1.9.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-
x86-64-22.1R1.9-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 22.1 jinstall package, you cannot return to the previously installed software by issuing the `request system software rollback` command. Instead, you must issue the `request system software add validate` command and specify the jinstall package that corresponds to the previously installed software.

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

Upgrade and Downgrade Support Policy for Junos OS Releases

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 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 22.1R1 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

IN THIS SECTION

Learn about new features introduced in the Junos OS main and maintenance releases for QFX Series switches.

Class of Service

- **Support for configuring multiple queues as strict-high priority (EX4400-24MP, EX4400-24P, EX4400-24T, EX4400-48F, EX4400-48MP, EX4400-48P, EX4400-48T, EX4650, EX4650-48Y-VC, QFX5120-32C, QFX5120-48T, QFX5120-48T-VC, QFX5120-48Y, QFX5120-48Y-VC, and QFX5120-48YM)**—Starting in Junos OS Release 22.1R1, you can configure multiple strict-high priority queues in which the queue with the highest priority value gets precedence.

  [See Traffic Management User Guide.]

- **Forwarding classes and loss priority enhancement (QFX10002, QFX10008, and QFX10016)**—Starting in Junos OS Release 22.1R1, we've increased the number of supported forwarding classes from 8 to 16 and the number of supported loss priorities from 3 to 4. This enhancement enables you to classify all available 64 Differentiated Services code point (DSCP) values.

  You can also configure the loss priority as `medium-low` at the following hierarchy levels:

  - `[edit class-of-service classifiers` *`cls-type classifier-name`* `forwarding-class` *`class-name`* `loss-priority]`
  - `[edit class-of-service rewrite-rules` *`rw-type rewrite-name`* `forwarding-class` *`class-name`* `loss-priority]`

  [See loss-priority (Classifiers) and loss-priority (Rewrite Rules).]

EVPN

- **Preference-based DF election for EVPN (QFX5110, QFX5120-32C, QFX5120-48T, QFX5120-48Y, QFX5200, QFX5210, QFX10002, QFX10002-60C, QFX10008, and QFX10016)**—Starting in Junos OS Release 22.1R1, you can enable QFX Series switches to select a designated forwarder (DF) based on the preference value. Provider edge (PE) devices send the preference value to the other multihomed PE devices using the extended community attribute in the EVPN Type 4 route advertisement.

  To enable preference-based DF election, include the `df-election-type` statement at the `[edit interfaces` *`interface-name`* `esi]` hierarchy level. You can also enable DF election based on the lowest preference value. To do this, include the `designated-forwarder-preference-least` statement at the `[edit routing-instance` *`routing-instance-name`* `protocols evpn]` hierarchy level.

  [See **Designated Forwarder Election**.]

- **Support for EVPN/VXLAN filtering and policing capability over a pure IPv6 underlay (QFX10002-60C, QFX10002, QFX10008 and QFX10016)**—Starting in Junos OS Release 22.1, Juniper supports filter-based forwarding for both IPV4 and IPV6 on an EVPN/VXLAN topology with added firewall policing of IPV6 packets once the forwarding tunnel terminates.

[See Routing IPv6 Data Traffic through an EVPN-VXLAN Network with an IPv4 Underlay.]

- **Zero traffic loss when you add new member interfaces ECMP underlay next hop (QFX10002-60C, QFX10002, QFX10008, and QFX10016)**—Starting in Junos OS Release 22.1R1, on VXLAN tunnels configured over ECMP underlays, there is no traffic loss when you add new members to the underlay ECMP next hop. Previously on single-FPC devices, when you added a member to the unilist (a pointer to a list of unicast next hops), the new member was installed at the beginning of the list for the egress pipeline. In the ingress pipeline, however, the unilist still pointed the old member but used the new member's index number. The traffic would then exit the device using the old member but with the index number of the new member. Because the MAC address didn't match the device from which it was sent, the next-hop device would drop the traffic. To solve this problem, you now add new members to the end of the list so that the existing indexes aren't affected.

  Previously on multiple-FPC devices, each FPC updated its ingress and egress pipelines independently and would be out of sync with each other. For example, if you had two members in the unilist, and then added a third member, the third member had its port on FPC2. The fix for single-FPC devices doesn't help in this situation. Instead, you can configure a delay timer, which enables you to defer populating the ingress pipeline for a predetermined amount of time while programming the egress pipeline. When the timer expires, you can then program the ingress pipeline.

  [See EVPN Overview.]

Forwarding Options

- **Support to exclude MAC addresses for load balancing** (PTX1000, PTX5000, PTX10002, and QFX10002-60C). You can use the `no-destination-mac` option to exclude the destination MAC address in the hash key for load balancing. Use the `source-mac` option to include source MAC addresses in the hash key.

  [See enhanced hash key.]

Junos Telemetry Interface

- **Packet Forwarding Engine DDoS sensor support with JTI (EX4650, QFX5110, QFX5120-32C, QFX5120-48T, QFX5120-48Y, QFX5120-48YM, QFX5210 and QFX5200)**—Starting in Junos OS Release 22.1R1, JTI supports distributed denial-of-service (DDoS) telemetry sensors. To stream DDoS statistics from a device to a collector, include the resource path **/junos/system/linecard/ddos/**) in a subscription. You can stream statistics using UDP (native) or Juniper proprietary gRPC and gNMI. This feature supports the Openconfig data model **junos/ui/openconfig/yang/junos-ddos.yang**.

  Currently, there are 45 packet types for DDoS. To maintain a reasonably sized data stream, data is exported for all protocols that have traffic using the zero-suppression model.

  [See sensor (Junos Telemetry Interface) and Guidelines for gRPC and gNMI Sensors (Junos Telemetry Interface).]

MPLS

- **Conditional RSVP LSP metrics (cRPD, MX960, PTX1000, and QFX10002)**—Starting in Junos OS Release 22.1R1, you can configure conditional metrics for local statically configured label-switched paths (LSPs). The conditional metrics are based on the dynamically changing IGP metric. Junos OS changes the LSP metric to the configured conditional metric that corresponds to the highest threshold reached by the IGP metric. You can configure up to four conditional metrics for an LSP.

  By default, the IGP metric of routes configured with the `install` statement is the IGP metric value of the LSP destination route. If you configure the `track-igp-metric <install-v4-prefixes> <install-v6-prefixes>` statement at the `[edit protocols mpls]` or `[edit protocols mpls label-switched-path` *`lsp-name`*`]` hierarchy level, routes installed by IGP use the IGP metric of the prefix instead.

  Use the `conditional igp-metric-threshold` *`threshold-metric-value static-metric-condition-value`* statement at the `[edit protocols mpls label-switched-path` *`lsp-name`* `metric]` hierarchy level to configure this feature. To check whether the conditional metric is configured, use the `show mpls lsp extensive` command.

  [See Configuring LSP Metrics, metric (Protocols MPLS), track-igp-metric (LSP), conditional-metric, and show mpls lsp extensive.]

- **MPLS TTL propagation flexibility for LDP-signaled LSPs (MX80, MX104, MX150, MX204, MX240, MX480, MX960, MX2008, MX2010, MX2020, MX10003, MX10008, MX10016, PTX1000, PTX5000, PTX10001, PTX10008, PTX10016, and QFX10002)**—Starting in Junos OS Release 22.1R1, we support disabling time-to-live (TTL) propagation at a more granular level. You can disable TTL propagation specifically for LDP-signaled label-switched paths (LSPs). When a route is very long, disable TTL propagation to ensure that the TTL doesn't expire while the packet is traversing the path. This feature also gives you more flexibility in hiding your network topology.

  To disable TTL propagation for LDP-signaled LSPs, use the `no-propagate-ttl` statement at the `[edit protocol ldp]` hierarchy level.

  > **NOTE**: If the TTL value of the top label is less than the TTL value of the bottom label at an egress node, Junos OS copies the TTL value from the top label to the bottom label. In this case, the TTL value can still propagate down even when `no-propagate-ttl` is configured.

  [See no-propagate-ttl.]

Routing Protocols

- **Support for DDoS IS-IS classification (MX Series with MPCs MPC1 through MPC9, PTX1000, PTX5000, PTX10002, PTX10008, QFX10002, QFX10002-60C, QFX10008, and QFX10016)**—Starting in Junos OS Release 22.1R1, Junos OS classifies IS-IS hello packets and IS-IS data packets separately. You can apply different policers to different types of IS-IS packets to improve the performance of IS-IS during congestion so that IS-IS doesn't go down when a large number of packets are entering the device.

Configure DDoS protection settings for IS-IS hello packets and IS-IS data packets separately using the `isis-hello` or `isis-data` statement at the `[edit system ddos-protection protocols isis]` hierarchy level. Use the `show ddos-protection protocols isis parameters brief` command to view the aggregate number of IS-IS packets as well as the number of IS-IS hello packets and IS-IS data packets.

[See protocols (DDoS) (ACX Series, PTX Series, and QFX Series) and show ddos-protection protocols isis.]

- **Support for adaptive RSVP update threshold (cRPD, MX240, MX480, MX960, PTX1000, PTX10008, QFX10002-60C, and QFX10008)**—Starting in Junos OS Release 22.1R1, you can configure the RSVP update threshold percentage and threshold value to adaptively pace IGP updates. You can configure a lower frequency when the adaptive bandwidth is higher and configure a higher frequency when the bandwidth is lower.

  You can enable the threshold percentage by using the `update-threshold adaptive limit` *`limit`* `threshold-percent` *`percentage`* configuration, and threshold value by using the `update-threshold adaptive limit` *`limit`* `threshold-value` *`value`* `configuration` at the `edit protocols rsvp interface` hierarchy level.

  NOTE: You cannot configure both `threshold-percent` and `threshold-value` simultaneously on the same interface.

  [See update-threshold.]

Additional Features

We've extended support for the following features to these platforms.

- **Supported transceivers, optical interfaces, and DAC cables** (EX Series, MX Series, and QFX Series). Select your product in the Hardware Compatibility Tool to view supported transceivers, optical interfaces, and DAC cables for your platform or interface module. We update the HCT and provide the first supported release information when the optic becomes available.

- **Support for PTP boundary clock over IRB for media and enterprise profiles** (QFX5120-48YM)

  [See PTP Media Profile, PTP Enterprise Profile, and PTP over IRB for Broadcast Profiles.]

- **VLAN-level MACsec on logical interfaces** (EX9253 and QFX5120-48YM)

  [See Media Access Control Security (MACsec) over WAN.]

What's Changed

IN THIS SECTION

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

What’s Changed in Release 22.1R1

IN THIS SECTION

Junos OS API and Scripting

- **The `<request-system-zeroize>` RPC response indicates when the device successfully initiates the requested operation (ACX Series, EX Series, MX Series, PTX Series, QFX Series, SRX Series, vMX, and vSRX)**—When the `<request-system-zeroize>` RPC successfully initiates the zeroize operation, the device emits the `<system-zeroize-status>zeroizing re0</system-zeroize-status>` response tag to indicate that the process has started. If the device fails to initiate the zeroize operation, the device does not emit the `<system-zeroize-status>` response tag.

Network Management and Monitoring

- **Junos XML protocol Perl modules deprecated (ACX Series, EX Series, MX Series, PTX Series, QFX Series, SRX Series, vMX, and vSRX)**—We no longer provide the Junos XML protocol Perl client for download. To use Perl to manage Junos devices, use the NETCONF Perl library instead.

  [See Understanding the NETCONF Perl Client and Sample Scripts.]

- **Changes when deactivating or deleting instances of the ephemeral configuration database (ACX Series, EX Series, MX Series, PTX Series, QFX Series, SRX Series, vMX, and vSRX)**—The following changes apply when you deactivate or delete ephemeral database instances in the static configuration database:

- When you deactivate the entire `[edit system configuration-database ephemeral]` hierarchy level, the device deletes the files and corresponding configuration data for all user-defined ephemeral instances. In earlier releases, the files and configuration data are preserved; however, the configuration data is not merged with the static configuration database.

- When you delete an ephemeral instance in the static configuration database, the instance's configuration files are also deleted. In earlier releases, the configuration files are preserved.

- You can delete the files and corresponding configuration data for the default ephemeral database instance by configuring the `delete-ephemeral-default` statement in conjunction with the `ignore-ephemeral-default` statement at the `[edit system configuration-database ephemeral]` hierarchy level.

[See Enable and Configure Instances of the Ephemeral Configuration Database.]

- **Support for automatically synchronizing an ephemeral instance configuration upon committing the instance (EX Series, MX Series, MX Series Virtual Chassis, PTX Series, QFX Series, and vMX)**—You can configure an ephemeral database instance to synchronize its configuration to the other Routing Engine every time you commit the ephemeral instance on a dual Routing Engine device or an MX Series Virtual Chassis. To automatically synchronize the instance when you commit it, include the `synchronize` statement at the `[edit system commit]` hierarchy level in the ephemeral instance's configuration.

  [See Commit and Synchronize Ephemeral Configuration Data Using the NETCONF or Junos XML Protocol.]

User Interface and Configuration

- **Load JSON configuration data with unordered list entries (ACX Series, EX Series, MX Series, PTX Series, QFX Series, SRX Series, vMX, and vSRX)**—The Junos schema requires that list keys precede any other siblings within a list entry and appear in the order specified by the schema. Junos devices provide two options to load JSON configuration data that contains unordered list entries:

  - Use the `request system convert-json-configuration` operational mode command to produce JSON configuration data with ordered list entries before loading the data on the device.

  - Configure the `reorder-list-keys` statement at the `[edit system configuration input format json]` hierarchy level. After you configure the statement, you can load JSON configuration data with unordered list entries, and the device reorders the list keys as required by the Junos schema during the load operation.

  When you configure the `reorder-list-keys` statement, the load operation can take significantly longer to parse the configuration, depending on the size of the configuration and number of lists. Therefore, for large configurations or configurations with many lists, we recommend using the `request system convert-json-configuration` command instead of the `reorder-list-keys` statement.

[See json and request system convert-json-configuration.]

Known Limitations

IN THIS SECTION

Learn about known limitations in Junos OS Release 22.1R1 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 you upgrade from Junos OS Release 21.2 and earlier version to the later version, validation and upgrade fails. You must use the `no-validate` command to upgrade. PR1568757

Platform and Infrastructure

- On QFX5100 switches, NSSU from the previous verion of Junos OS Releases with the Broadcom SDK 6.3.x to the new Junos OS Releases with the Broadcom SDK 6.5.x might not work. As a workaround, perform normal upgrade from the previous release to the new release. PR1496765
- On QFX5000 switches in the EVPN_VXLAN deployment, the BUM traffic replication over VTEP might send out more packets than expected. PR1570689
- On QFX5000 switches, the IRACL filters cannot match on the VXLAN tunnel terminated packets. PR1594319

- On QFX5000 switches, you must configure only one static arp with multicast-mac entry per the IRB interface. If you configure more than one static arp with multicast MAC entry per the IRB interface, the packets with different destination IP with static multicast MAC goes out with any one of the multicast MAC configured in the system. PR1621901

- On QFX5120-48Y switches, Junos OS does not support the unified ISSU if there is a change in the chipset SDKs between the releases. This limitation is due to the change in the firmware that leads to the chip reset causing ISSU impact. The versions in the chipset SDKs must be the same between the two Junos OS releases for ISSU to work. PR1634695

Open Issues

IN THIS SECTION

Learn about open issues in Junos OS Release 22.1R1 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

- Modifying the I-ESI value causes traffic effecting event. To modify the value, you must deactivate interconnect stanza for the routing-instance in question, modify the I-ESI value, and then activate the interconnect stanza. PR1600600

- VM move across DC where there is no translate VNI configuration in the interconnect. This issue occurs when you move MAC from DC1 to DC2 with translation VNI. PR1610432

PR1610432

- There are 10 seconds of traffic loss when a MH leaf in the scaled environment is brought down. The loss is both in the Layer 2 and Layer 3 traffic. When the MH peer is brought up, there are no traffic loss. PR1611565

- EVPN Local ESI MAC limit configuration might not get effective immediately when it has already learned the remote MH MACs. You must clear the MAC table from all the MH PE devices and configure the MAC limit over the local ESI interfaces. PR1619299

Interfaces and Chassis

- When BUM traffic is sent on MCLAG, MAC entries are learnt on ICL interface as DLR when ICL gets flapped as MAC learning. This might cause traffic loss with certain traffic flow. PR1639713

Layer 2 Features

- In case of an access-side interfaces used as the SP-style interfaces, when you add a new logical interface and if already a logical interface on the physical interface is present, there are 20 to 50 minutes of traffic drop on the existing logical interface. PR1367488

Platform and Infrastructure

- When you add VLAN as an action for changing the VLAN in both the ingress and egress filters, the filter does not get installed. PR1362609

- VXLAN VNI (multicast learning) scaling occurs on QFX5110 switches, and causes traffic issue from the VXLAN tunnel to the Layer 2 interface. PR1462548

- When you run the `show pfe filter hw filter-name filter name` command, the command fails to retrieve the Packet Forwarding Engine programming details of the filter. PR1495712

- On QFX5100 switches not running the QFX 5E codes (non-TVP architecture), when you install an image with the Broadcom SDK upgrade (6.5.x), the CPU utilization might increase by around 5 percent. PR1534234

- 5M DAC connected between QFX10002-60C and MX2010 does not link up. But with 1M and 3M DAC this interop works as expected. Also, it is to be noted that the QFX10002-60C and ACX devices, or the traffic generator of the same 5M DAC works seamlessly. There seems to be certain SI or link level configuration on both the QFX10002-60C and MX2010 devices. PR1555955

- To avoid the additional interface flap, interface hold time needs to be configured. PR1562857
- On QFX51000 Virtual Chassis fan setup, duplicate traffic might be observed for some Layer 3 multicast traffic streams. PR1568152
- Partial traffic loss occurs after disabling the protected link on R2 due to which convergence delays for link-protection for the PE1_P link. PR1579931
- In a fully loaded devices at times, the firewall programming fails due to scaled prefix configuration with more than 64800 entries. PR1581767
- Pim VXLAN does not work on the TD3 chipsets enabling the VXLAN flexflow after Junos OS Release 21.3R1. PR1597276
- On QFX5100 switches, optical power appears after detaching and attaching QSFP on the disable interface. PR1606003
- On QFX10002-60C switches, the `output-mac-control-frames` and `output-mac-pause-frames` MAC statistics does not increment. PR1610745
- On QFX5000 switches with 5E image, chassis status LED does not work properly. You might observe unexpected state of SYS or MST LED on the primary or backup FPC. PR1630380
- Junos OS does not support the bounded delay configuration feature for IFL. Core file gets generated only when you enable the configuration on the device. PR1634941
- On the QFX10008 and QFX10016 switches, the following logs gets generated every 5 seconds in the output of the `show log chassisd` command: `Jun 14 18:09:38 CHASSISD_UTIL_RW_ERR: Cannot read hw.chassis.startup_time value: m Jun 14 18:09:43 CHASSISD_UTIL_RW_ERR: Cannot read hw.chassis.startup_time value: m Jun 14 18:09:48 CHASSISD_UTIL_RW_ERR: Cannot read hw.chassis.startup_time value: m Jun 14 18:09:53 CHASSISD_UTIL_RW_ERR: Cannot read hw.chassis.startup_time value: m Jun 14 18:09:58 CHASSISD_UTIL_RW_ERR: Cannot read hw.chassis.startup_time value: m Jun 14 18:10:03 CHASSISD_UTIL_RW_ERR: Cannot read hw.chassis.startup_time value: m Jun 14 18:10:08 CHASSISD_UTIL_RW_ERR: Cannot read hw.chassis.startup_time value: m Jun 14 18:10:13 CHASSISD_UTIL_RW_ERR: Cannot read hw.chassis.startup_time value: m Jun 14 18:10:18 CHASSISD_UTIL_RW_ERR: Cannot read hw.chassis.startup_time value: m Jun 14 18:10:23 CHASSISD_UTIL_RW_ERR: Cannot read hw.chassis.startup_time value: m Jun 14 18:10:28 CHASSISD_UTIL_RW_ERR: Cannot read hw.chassis.startup_time value: m` PR1603588
- The dfwd process generates file when accessing ephemeral db files, which gets deleted through script. PR1609201

Platform and Infrastructure

- When you configure the DHCP relay mode as no-snoop, the offer gets dropped due to incorrect ASIC programming. This issue occurs while running the DHCP relay on EVPN-VXLAN environment. PR1530160

Routing Protocols

- When the `accept-remote-source` configuration statement under PIM is removed, the PIM SG entries might not be updated with the correct RPF. Clearing of the states would take care of the issue. This is day-1 behavior. PR1593283
- The mcsnoopd process generates a core file sometimes due to nexthop index being quickly reused by the kernel. As a result, when the application still holds the old nexthop reference, which waits for the deletion response from kernel, the same nexthop index can be received from the other applications like RPD for EVPN core-NH updates as in current case. This leads to the mcsnoopd process incorrectly manipulating the nexthop reference counting, leading to the usage of a freed Nexthop memory when this nexthop-index gets freed. PR1605393

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.

Resolved Issues: 22.1R1

IN THIS SECTION

Class of Service (CoS)

- The dcpfe process might generate core file in the auto-channelization scenario or when you plug out SFP. PR1616847
- The uplink interface remains down for a longer duration due to VXLAN scaled configuration. PR1631448

EVPN

- A few ARP/ND/MAC entries for VLANs are missed with the MAC-VRF configuration. PR1609322
- mac-table aging timeout fails in some scenarios. PR1612866
- IRB proxy-arp unrestricted might not work if EVPN/l2alm proxy is enabled. PR1613201
- Multiple memory leaks might be seen, leading to process rpd crash. PR1626416
- The MAC address might not be visible in the EVPN-VXLAN environment. PR1645591

High Availability (HA) and Resiliency

- Memory might leak on the backup Routing Engine when the ksyncd process is in the `Inconsistent` state and had encountered an initialization error. PR1601960

Infrastructure

- A false error related to insufficient space might appear while installing a corrupted Junos OS image. PR1570148

Layer 2 Ethernet Services

- Enabling DHCP on Junos OS might cause the file system storage of the router to get filled up with log files. PR1617695

MPLS

- MPLS VPN packets drop due to missing ARP entry on the PE devices. PR1607169
- On QFX5000 switches, traffic loss occurs after the STP topology changes. PR1616878
- On QFX5000 switches, traffic towards MPLS-Core does not get rerouted to alternate port. PR1627002

Platform and Infrastructure

- The unexpected next-hop might appear after the route gets deleted. PR1477603
- Multiple entries to vlan-id-list might not work in the EVPN-VXLAN scenario. PR1564403
- The grpcd process might crash if the route or interface flaps. PR1565255
- On QFX10K2-60C switches, disk missing alarms does not appear. PR1573139
- When you commit the soft loopback port and analyzer configurations together, mirror ingress to local port does not work. PR1581542
- On QFX5000 switches, the output of the `show route detail` command might not display `next-hop type IPoIP chained component next hop`. PR1584322
- IPv6 link-local traffic getting classified to firewall might affect communication on the IPv6 link-local addresses. PR1600085
- Packet might drop on FPC on the Trio-based platforms.

- On QFX5000 switches, the dcpfe process might crash. PR1588704
- IS-IS adjacency might fail to be formed if you configure the MTU size of an IRB interface with a value greater than 1496 bytes. PR1595823
- The DCI InterVNI and IntraVNI traffic might be silently discarded in the gateway node due to the tagged underlay interfaces. PR1596462
- On QFX5110 switches during FRR, when more than one multi-home interface goes in to the `Down` state, traffic might loop. PR1596589
- The following error message gets generated on the device during continuous software upgrade:

  ```
  error: syntax error: request-package-validate
  ```

  PR1596955
- On QFX10000 switches, the dcpfe or fpc process might crash in a rare case. PR1597479
- On QFX10008 switches, the Routing Engine1 goes to the DB prompt when you try to load the profile configurations over the LRM configurations. PR1598814
- The VCP might not form adjacency after rebooting the primary FPC in the Virtual Chassis scenario. PR1600398
- Removing and adding Virtual Chassis ports might cause the FPC to reboot. PR1601557
- InterDC traffic loss might occur in the MAC-VRF EVI with the `dlu.ucode.discard` trap status. PR1601961
- In a very rare case, the l2ald process generates a core file when EVPN(mac-vrf) uses the IPv4 underlay. PR1602244
- On QFX5120 switches, even after deactivating the analyzer configuration, traffic gets mirrored. PR1603192
- Unicast DHCP packets might get flooded when you configure the DHCP relay in the non-default routing-instance. PR1603444
- Virtual Chassis ports might remain in the `Down` state after the addition and removal of the ports. PR1606705
- The sFlow samples might not get generated for the transit MPLS traffic carrying the IPv6 packets. PR1607497
- FPC might crash post firewall filter configuration changes. PR1608610

- On QFX10016 switches, an additional VLAN tag might be added for Point-to-Point Protocol over Ethernet (PPPoE) packets. PR1610012

- On QFX10000 switches, continuous Layer 3 traffic drop might occur with MC-LAG configuration. PR1610173

- Inter-VLAN connectivity might be lost in an EVPN-VXLAN with CRB topology. PR1611488

- On QFX10002-60C switches, continuous FPC crash and dcpfe process might generate core file. PR1612871

- ARP resolution for data traffic received over Type5 might fail. PR1612905

- On QFX10002-60C switches, the `FPC 0 Major Errors` alarm might get generated due to a rare timing issue. PR1613229

- FPC might crash after the device restarts in the EVPN-VXLAN scenario. PR1613702

- Removing the optical module `JNP-SFPP-10GE-T` from a port might cause certain ports to go down. PR1614139

- On QFX5000 switches, the VLAN firewall filter does not get deleted in the Packet Forwarding Engine after configuration change. PR1614767

- The l2ald process might crash in the EVPN scenario. PR1615269

- Slow memory leakage (32 bytes each time) of rpd process might occur. PR1616065

- On QFX5120-48YM switches, the BFD session might flap. PR1616692

- The l2cpd process generates core file with FIP snooping configuration on any interface. PR1617632

- The BFD session might become nonresponsive in the `Init` state after l2-learning restart due to incomplete ARP resolutions. PR1618280

- Core file might be generated after the configuration changes. PR1618352

- Traffic might be dropped when you configure IRB and remove from VLAN. PR1618425

- The `sample` and `accept` firewall action drops inbound packets destined to cpu-host. PR1646740

- On QFX5000 switches, the dcpfe process might crash after performing VXLAN VNI configuration change and deleting the configuration. PR1619445

- Disabled VCP (Virtual chassis port) goes in to the `Up` state after the optic on it is reseated. PR1619997

- High wired memory utilization might be observed if you enable GRES. PR1620599

- Routes learned through the EVPN Type-5 route are not resolved. PR1620627
- On QFX10000 switches, the EVPN-VXLAN Type5 traffic might get fail on the Spine device. PR1620924
- NSSU (nonstop-upgrade) CLI gets missed from Junos OS Release 21.2R1. PR1621611
- On QFX5120 switches, the following error message gets generated while loading the build:

  ```
  tvp_is_qsfp_has_single_led ioctl call failed ret:-1
  ```

  PR1621630
- LED indicator might display the status as `ON` once you remove QSFP. PR1622580
- Host generated IPv4 traffic sent over IPv6 next-hop with IRB interface might get dropped. PR1623262
- On QFX52000 switches, interface does not come up after swapping from 100G to 40G. PR1623283
- MACsec session might flap if multiple logical interfaces gets created on the single physical interface. PR1624524
- In rare circumstances, PKID might crash and generate a core file when there was limited memory available on the routing-engine. PR1624613
- On QFX5000 switches, the following log messages do not process packet further:

  ```
  fpc0 SRIRAM Tx VxLAN Ucast: ifd_out = vtep dst_gport
  ```

  PR1624925
- Traffic loss might be observed after configuring the VXLAN over IRB interface. PR1625285
- On QFX10002 and QFX10008 switches, the `no-incoming-port` command does not get applied after reboot. PR1625988
- The `show task scheduler-slip-history` command displays the number of scheduler slips and last 64 slip details. PR1626148
- Routing Engine generating traffic might not be forwarded when next-hop is indirect unilist of the EVPN Type 5 tunnel. PR1627363
- The QFX10002-60C switches might not respond back to ICMP packets received with TTL or hop limit value of 1. PR1627566

- On QFX10002, QFX10008, and QFX10016 switches, the Layer 3 traffic failure might occur with the scaled MC-LAG configuration. PR1627846

- The 802.1p BA classification might not work on the mixed Virtual Chassis when the interface has a DSCP and 802.1p classifier. PR1628447

- When you use DHCP smart relay, DHCP inform acknowledge might be sent with the broadcast address. PR1628837

- The vmhost process might crash in a rare condition when you add and change the route. PR1629200

- On QFX5110-32Q Virtual Chassis, some ports (port 20 and above) might not come up after a device restarts or the Packet Forwarding Engine reboots. PR1629231

- Traffic might get dropped when you configure `family ethernet-switching` on the interface in the Q-in-Q scenario. PR1629680

- On QFX5000 switches, the Chassis Status LED does not work. PR1630380

- The interface might remain in the `UP/UP` state even if the admin disables the interface. PR1632440

- On QFX5000 switches, the FBF filtered VLAN traffic does not get passed properly to the forwarding routing instances over the aggregated Ethernet interfaces. PR1633452

- Traffic loss after the MAC ages. PR1633879

- The VCPs connected with the AOC cable might not come up after upgrading to Junos OS Release 17.3 or later. PR1633998

- Data might not be exchanged through the EVPN-VxLAN domain. PR1635347

- On QFX10008 switches, chassisd crashes after configuring the chassis disk-partition. PR1635812

- Traffic might be silently discarded when you configure STP in the VXLAN environment. PR1636950

- Configuring L2PT on a transit switch in a Q-in-Q environment breaks L2PT for other S-VLANs. PR1637249

- There might be delay for the interfaces to come up after reboot or transceiver replacement. PR1638045

- On QFX5000 switches, the targeted broadcast or WOL feature might not work. PR1638619

- MAC-move might be observed when you configure dhcp-security. PR1639926

- Packets drop in ingress QFX5000 switches with EVPN-LAG multihoming due to VP-LAG programming issue. PR1644152

- On QFX5200 switches, the dcpfe process generates core file while testing ISSU from Junos OS Release 21.1R1.11 to Junos OS Release 21.2R1.7. PR1600807

- Junos OS does not support the Dot1x based firewall policers. PR1619405

- The third 802.1Q tag might not be pushed onto the stack in the Q-in-Q tunneling. PR1626011

- The `show interface extensive` command might not display the Local/Remote fault. PR1629735

- LACP timeout might be observed during high CPU utilization. PR1630201

- Inner VLAN might be stripped off when input-native-vlan-push gets disabled. PR1631771

- The KRT queue might get stuck with the `ENOMEM -- Cannot allocate memory` error message. PR1642172

Routing Policy and Firewall Filters

- The rpd process might become nonresponsive at 100 percent when you enable the EVPN vrf-target and after changing any configuration. PR1616167

Routing Protocols

- When you remove igmp-snooping from the device, the device might encounter inconsistent MCSNOOPD. PR1569436

- The interface might receive multicast traffic from a multicast group. PR1612279

- The incorrect BGP path might get selected when a preferred route becomes available. PR1616595

- Traffic drops when the VPN labels gets incorrectly allocated due to change in nexthop. PR1617691

- Verification of the BGP peer count fails after deleting the BGP neighbors. PR1618103

- Time delay to export prefixes to the BGP neighbors might occur post applying the peer-specific BGP export policies. PR1626367

- OSPF adjacency might take longer time to converge when the neighbour restarts non-gracefully. PR1634162

User Interface and Configuration

- On QFX5700 switches, you cannot use the `file delete /var/core/*/vmcore*` command to delete the Linux core file. PR1624562

Migration, Upgrade, and Downgrade Instructions

IN THIS SECTION

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

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

Upgrading Software on QFX Series Switches

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

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

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

   The Junos Platforms Download Software page appears.

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

3. Select **22.1** in the Release pull-down list to the right of the Software tab on the Download Software page.

4. In the Install Package section of the Software tab, select the QFX Series Install Package for the 22.1 release.

   An Alert box appears.

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

   A login screen appears.

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

7. Download the software to a local host.

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

9. Install the new jinstall package on the device.

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

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

   ```
   user@host> request system software add source/jinstall-host-qfx-5-x86-64-22.1R1.n-secure-signed.tgz reboot
   ```

   Replace *source* with one of the following values:

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

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

Rebooting occurs only if the upgrade is successful.

NOTE: After you install a Junos OS Release 22.1 `jinstall` package, you can issue the `request system software rollback` command to return to the previously installed software.

Installing the Software on QFX10002-60C Switches

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

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

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

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

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

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

For example:

```
user@switch> request vmhost software add /var/tmp/junos-vmhost-install-qfx-x86-64-22.1R1.9.tgz
```

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

For example:

```
user@switch> request vmhost software add ftp://ftpserver/directory/junos-vmhost-install-qfx-
x86-64-22.1R1.9.tgz
```

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

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

Installing the Software on QFX10002 Switches

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

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

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

For example:

```
user@switch> request system software add /var/tmp/jinstall-host-qfx-10-f-x86-64-22.1R1.n-secure-
signed.tgz reboot
```

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

For example:

```
user@switch> request system software add ftp://ftpserver/directory/jinstall-host-qfx-10-f-
x86-64-22.1R1.n-secure-signed.tgz reboot
```

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

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

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

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

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

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

To install the software on re0:

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

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

For example:

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

To install the software on re1:

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

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

For example:

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

Reboot both Routing Engines.

For example:

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

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

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

Installing the Software on QFX10008 and QFX10016 Switches

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

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

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

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

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

2. From the command line, enter configuration mode:

   ```
   user@switch> configure
   ```

3. Disable Routing Engine redundancy:

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

4. Disable nonstop-bridging:

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

5. Save the configuration change on both Routing Engines:

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

6. Exit the CLI configuration mode:

   ```
   user@switch# exit
   ```

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

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

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

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

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

   ```
   user@switch> request system software add validate /var/tmp/jinstall-host-qfx-10-f-
   x86-64-22.1R1.n-secure-signed.tgz
   ```

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

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

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

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

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

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

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

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

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

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

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

12. Transfer routing control to the backup Routing Engine:

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

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

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

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

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

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

    ```
    user@switch> request system software add validate /var/tmp/jinstall-host-qfx-10-f-
    x86-64-22.1R1.n-secure-signed.tgz
    ```

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

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

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

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

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

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

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

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

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

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

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

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

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

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

Performing a Unified ISSU

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

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

Perform the following tasks:

- "Preparing the Switch for Software Installation" on page 179
- "Upgrading the Software Using Unified ISSU" on page 180

Preparing the Switch for Software Installation

Before you begin software installation using unified ISSU:

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

  To verify that nonstop active routing is enabled:

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

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

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

- Enable nonstop bridging (NSB). See Configuring Nonstop Bridging on EX Series Switches for information on how to enable it.

- (Optional) Back up the system software—Junos OS, the active configuration, and log files—on the switch to an external storage device with the `request system snapshot` command.

Upgrading the Software Using Unified ISSU

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

To upgrade the switch using unified ISSU:

1. Download the software package by following the procedure in the Downloading Software Files with a Browser section in Installing Software Packages on QFX Series Devices.

2. Copy the software package or packages to the switch. We recommend that you copy the file to the `/var/tmp` directory.

3. Log in to the console connection. Using a console connection allows you to monitor the progress of the upgrade.

4. Start the ISSU:

   - On the switch, enter:

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

   where *package-name*.tgz is, for example, `jinstall-host-qfx-10-f-x86-64-22.1-R1.n-secure-signed.tgz`.

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

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

   ```
   warning: Do NOT use /user during ISSU. Changes to /user during ISSU may get lost!
   ISSU: Validating Image
   ISSU: Preparing Backup RE
   Prepare for ISSU
   ISSU: Backup RE Prepare Done
   Extracting jinstall-host-qfx-5-f-x86-64-18.3R1.n-secure-signed.tgz ...
   Install jinstall-host-qfx-5-f-x86-64-19.2R1.n-secure-signed.tgz completed
   Spawning the backup RE
   Spawn backup RE, index 0 successful
   GRES in progress
   GRES done in 0 seconds
   Waiting for backup RE switchover ready
   GRES operational
   ```

```
Copying home directories
Copying home directories successful
Initiating Chassis In-Service-Upgrade
Chassis ISSU Started
ISSU: Preparing Daemons
ISSU: Daemons Ready for ISSU
ISSU: Starting Upgrade for FRUs
ISSU: FPC Warm Booting
ISSU: FPC Warm Booted
ISSU: Preparing for Switchover
ISSU: Ready for Switchover
Checking In-Service-Upgrade status
  Item           Status                  Reason
  FPC 0          Online (ISSU)
Send ISSU done to chassisd on backup RE
Chassis ISSU Completed
ISSU: IDLE
Initiate em0 device handoff
```

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

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

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

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

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

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

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

Upgrade and Downgrade Support Policy for Junos OS Releases

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.

Junos OS Release Notes for SRX Series

IN THIS SECTION

These release notes accompany Junos OS Release 22.1R1 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

IN THIS SECTION

Learn about new features introduced in this release for SRX Series devices.

Application Identification (AppID)

- **TLS 1.3 support for session resumption using PSK (SRX Series and vSRX)**—Starting in Junos OS Release 22.1R1, TLS 1.3 supports session resumption using a pre-shared key (PSK) in SSL proxy to reduce SSL handshake overhead. Session resumption using PSK allows resuming the session with a previously established shared secret key.

  Session resumption shortens the handshake process and accelerates SSL transactions resulting in improved performance while maintaining appropriate level of security.

  [See SSL Performance Enhancements.]

Intrusion Detection and Prevention

- **Encryption support for IDP packet capture (SRX Series, vSRX, and vSRX 3.0)**—Starting in Junos OS Release 22.1R1, you can enable a secure SSL or TLS connection to send an encrypted IDP packet capture log to the packet capture receiver. To establish the SSL or TLS connection, you must specify the SSL initiation profile that you want to use in the IDP packet log configuration.

  In earlier releases, when IDP detects an attack, it sends a decrypted IDP packet log to the packet capture receiver over UDP traffic. Sending a decrypted packet log is not a secure process, especially when packet-log is captured for encrypted traffic.

  To enable SSL or TLS connection for IDP packet log, run the `set security idp sensor-configuration packet-log ssl-profile-name` *`profile-name`* command. To view the new packet log counters, use the `show security idp counters packet-log` command.

  [See IDP Security Packet Capture, packet-log (Security IDP Sensor Configuration), and show security idp counters packet-log.]

IPv6

- **NDP and DAD proxy support on multiple interfaces (SRX Series, vSRX, and vSRX 3.0)**—Starting in Junos OS Release 22.1R1, we support Neighbor Discovery Protocol (NDP) and Duplicate Address Detection (DAD) proxy functionality on multiple interfaces (interface unrestricted mode).

  To enable NDP and DAD proxy (interface unrestricted mode), use the `set interfaces <interface> unit <number> family inet6 ndp-proxy interface-unrestricted` and `set interfaces <interface> unit <number> family inet6 dad-proxy interface-unrestricted` commands respectively.

  To view the NDP and DAD proxy (interface unrestricted mode) statistics and to monitor proxy requests and responses use the `show system statistics icmp6` command.

  [See NDP Proxy and DAD Proxy, ndp-proxy, dad-proxy, and show system statistics icmp6.]

- **Router advertisement proxy support (NFX Series, SRX Series, vSRX, and vSRX 3.0)**—Starting in Junos OS Release 22.1R1, we support router advertisement proxy on the listed devices. With this functionality, the device can proxy the router advertisement packets from a service provider router to the clients (host).

  [See Router Advertisement Proxy, downstream, downstream-mode, upstream-mode, and show ipv6 router-advertisement.]

Juniper Advanced Threat Prevention Cloud (ATP Cloud)

- **IoT device discovery and classification (NFX150, NFX350, SRX340, SRX345, SRX4100, SRX4200, SRX5400, SRX5600, SRX5800 line of devices, and vSRX)**—In Junos OS Release 22.1R1, we introduce the Internet of Things (IoT) device discovery and classification feature on the listed devices.

  In a typical workflow:

  1. A security device identifies IoT devices based on the traffic flow.

  2. The device streams relevant packet metadata to Juniper Advanced Threat Prevention (ATP) Cloud.

  3. Juniper ATP Cloud discovers and classifies IoT devices based on brand, device model, type, and so on.

  You can view the list of identified IoT devices on the Juniper ATP Cloud portal. You can also create threat feeds to enforce security policies across IoT traffic in the network.

  With the knowledge of IoT devices in a network, network administrators can better manage their network security and reduce the IoT attack surface.

  [See IoT Security Overview.]

J-Web

- **Support for IPS signatures (SRX Series)**—Starting in Junos OS Release 22.1R1, you can use the IPS Signatures page in J-Web to configure and manage intrusion prevention system (IPS) signatures. A signature specifies the types of network intrusions that the device must detect and report. Whenever a traffic pattern matches a signature, IPS triggers an alarm and blocks the traffic from reaching its destination.

  To access this page, select **Security Services** > **IPS** > **Signatures**.

[See About the IPS Signatures Page.]

Network Management and Monitoring

- **Enhancement to <get-syslog-events> RPC with additional filtering options (cSRX, MX Series routers and vMX, SRX300, SRX320, SRX340, SRX345, SRX380, SRX550HM, SRX4100, SRX4200, SRX4600,**

SRX5400, SRX5600, SRX5800, vSRX, and vSRX 3.0)—In Junos OS Release 22.1R1, we've introduced the following new tags in the `<get-syslog-events>` RPC. These tags provide additional options for filtering system log messages.

```
<start-count></start-count>
<end-count></end-count>
<total-events/>
<pretty/>
<print-json/>
```

[See Overview of Junos OS System Log Messages and syslog (System).]

VPNs

- **Support for search domain name (Juniper Secure Connect Application, SRX Series and vSRX next-generation firewalls)**—As a system administrator, you can configure the set of search domain name that the Juniper Secure Connect application will use to handle DNS lookups. This is applicable for both full tunnel and split tunnel configurations. You can provide more than one search domain names by executing the `set security remote-access client-config name domain-name domain-name` multiple times. When you enter more than one domain name, it automatically adds a separator (comma) to that value. The number of domain names are limited to the total number of characters and must not exceed 1023 characters. For example, the two domain names `juniper.net,lab.juniper.net` consumes 27 characters while `juniper.net` consumes 11 characters.

  [See client-config (Juniper Secure Connect) and Juniper Secure Connect Application Overview.]

Additional Features

We've extended support for the following features to these platforms.

- **Dynamic routing protocols** (SRX5000 line of devices, and vSRX 3.0 running the iked process). We've extended our support to the exchange of dynamic routing information through IPsec VPN tunnels on SRX Series devices running the iked process. You can now enable dynamic routing protocols, such as OSPF, BGP, BFD, PIM, and RIP, on a st0 interface of an IPsec VPN tunnel.

  This feature is supported on the unified iked process using `junos-ike` package. The SRX5K-SPC3 card with RE3 comes with `junos-ike` package installed by default. You must run the command `request system software add optional://junos-ike.tgz` to load the`junos-ike` package explicitly on SRX5K-SPC3 with RE2 and vSRX Virtual Firewall.

  [See Routing Protocols Support on IPsec VPN Tunnels.]

- **Juniper Secure Connect application supports IPv6 addresses** (SRX5000 line of devices, and vSRX 3.0 running the iked process). While connecting to the Juniper Secure Connect application, you can provide an IPv6 address or IPv4 address as the gateway address and assign an IPv6 address or IPv4 address to a remote-access user.

Earlier Junos OS releases support only IPv4 addresses.

Note that IPv6 address-assignment is only supported when using certificate or EAP-based authentication

This feature is supported on the unified iked process using `junos-ike` package. The SRX5K-SPC3 card with RE3 comes with `junos-ike` package installed by default. You must run the command `request system software add optional://junos-ike.tgz` to load the`junos-ike` package explicitly on SRX5K-SPC3 with RE2 and vSRX Virtual Firewall.

- **Support for an enhanced hash key** (SRX5400, SRX5600, and SRX5800). SRX5000 devices support an enhanced hash key. You implement a control path for the configured setting to reach the services processing cards SPC2 and SPC3. You can configure the `session-id` option under the `[edit forwarding-options enhanced-hash-key]` hierarchy.

  [See enhanced-hash-key.]

- **Traffic selector configuration changes impacts only partial tunnels** (SRX5000 line of devices, and vSRX 3.0 running the iked process). When you modify a traffic selector configuration within a VPN object, only the modified and below configured traffic selectors will go down, and any traffic selector above the modified one is unaffected. In earlier Junos OS releases, when you modify a traffic selector in a VPN object, all the traffic selectors that are part of the VPN object go down and then the tunnel renegotiation occurs.

  Only partial tunnels are impacted when you modify a traffic selector configuration as follows:

  - Add a new configuration.

  - Delete an existing configuration.

  - Update an existing parameter in the configuration.

  - Update the sequence of the configuration by moving it above or below another configuration.

  This feature is supported on the unified iked process using `junos-ike` package. The SRX5K-SPC3 card with RE3 comes with `junos-ike` package installed by default. You must run the command `request system software add optional://junos-ike.tgz` to load the`junos-ike` package explicitly on SRX5K-SPC3 with RE2 and vSRX Virtual Firewall.

  [See traffic-selector.]

- **VLAN-level MACsec on logical interfaces** (EX9253 and QFX5120-48YM)

  [See Media Access Control Security (MACsec) over WAN.]

What's Changed

IN THIS SECTION

Learn about what changed in the Junos OS main and maintenance releases for SRX Series.

What’s Changed in Release 22.1R1

IN THIS SECTION

Authentication and Access Control

- **Enhanced UAC authentication (SRX Series)**—To regulate the lifespan (default 60 seconds) of event table entries, we've added a new configuration statement set services unified-access-control event-table-lifetime time interval in seconds> . If there is a delay in authentication at the SRX Series device, use this configuration statement to enable UAC traffic after the user is authorized from the IC. See Configuring Junos OS Enforcer Failover Options (CLI Procedure)

  [See See Configuring Junos OS Enforcer Failover Options (CLI Procedure).]

General Routing

- **No support for PKI operational mode commands on the Junos Limited version (MX Series routers, PTX Series routers, and SRX Series devices)**—We do not support `request` , `show` , and `clear` PKI-related operational commands on the limited encryption Junos image ("Junos Limited"). If you try to execute PKI operational commands on a limited encryption Junos image, then an appropriate error message is displayed. The `pkid` process does not run on Junos Limited version image. Hence, the limited version does not support any PKI-related operation.

J-Web

- **Changes to the Dashboard and Monitor pages (SRX Series):**—To improve the J-Web UI loading speed: On the Dashboard page, we've removed the on-box reports related widgets. On the Monitor > Maps and Charts > Traffic Map page, we've changed the default duration from Last "1 hour" to Last "5 minutes."

- **Changes in Identity Management page (SRX Series)**—Starting in Junos OS Release 21.4R1, we've renamed Identity Management as Juniper Identity Management Services (JIMS) in the following location: In Security Services > Firewall Authentication, the Identity Management menu is renamed to JIMS. In Identity Management page (new JIMS page), all instances of Identity Management are renamed to Juniper Identity Management Services.

Junos OS API and Scripting

- **The `<request-system-zeroize>` RPC response indicates when the device successfully initiates the requested operation (ACX Series, EX Series, MX Series, PTX Series, QFX Series, SRX Series, vMX, and vSRX)**—When the `<request-system-zeroize>` RPC successfully initiates the zeroize operation, the device emits the `<system-zeroize-status>zeroizing re0</system-zeroize-status>` response tag to indicate that the process has started. If the device fails to initiate the zeroize operation, the device does not emit the `<system-zeroize-status>` response tag.

Network Management and Monitoring

- **Junos XML protocol Perl modules deprecated (ACX Series, EX Series, MX Series, PTX Series, QFX Series, SRX Series, vMX, and vSRX)**—We no longer provide the Junos XML protocol Perl client for download. To use Perl to manage Junos devices, use the NETCONF Perl library instead.

  [See Understanding the NETCONF Perl Client and Sample Scripts.]

- **Changes when deactivating or deleting instances of the ephemeral configuration database (ACX Series, EX Series, MX Series, PTX Series, QFX Series, SRX Series, vMX, and vSRX)**—The following changes apply when you deactivate or delete ephemeral database instances in the static configuration database:

- When you deactivate the entire `[edit system configuration-database ephemeral]` hierarchy level, the device deletes the files and corresponding configuration data for all user-defined ephemeral instances. In earlier releases, the files and configuration data are preserved; however, the configuration data is not merged with the static configuration database.

- When you delete an ephemeral instance in the static configuration database, the instance's configuration files are also deleted. In earlier releases, the configuration files are preserved.

- You can delete the files and corresponding configuration data for the default ephemeral database instance by configuring the `delete-ephemeral-default` statement in conjunction with the `ignore-ephemeral-default` statement at the `[edit system configuration-database ephemeral]` hierarchy level.

[See Enable and Configure Instances of the Ephemeral Configuration Database.]

Network Address Translation (NAT)

- **NAT rule configuration command (SRX Series and MX Series)**—Starting in Junos OS Release 22.1R1, on Source NAT, Destination NAT, and Static NAT, the rule-set command configuration fails if you use the IP address with incorrect prefix. To commit the configuration, use the valid IP address prefix.

  [See rule-set (Security Source NAT), rule-set (Security Destination NAT), and rule-set (Security Static NAT).]

Platform and Infrastructure

- **Include IPv6 address in a self-signed certificate (SRX Series devices and vSRX3.0)**— We support manual generation of a self-signed certificate for the given distinguished name using IPv6 address in addition to the IPv4 address that was supported earlier. Use the `request security pki local-certificate generate-self-signed` command with `ipv6-address` option to include ipv6 address in a self-signed certificate.

Unified Threat Management (UTM)

- **Content filtering CLI updates (SRX Series and vSRX)**—Starting in Junos OS Release 22.1R1, we've the following updates to the content filtering CLI:

  - Trimmed the list of file types supported for content filtering rule match criteria. Instead of uniquely representing different variants of a file type, now only one `file-type` string represents all variants. Hence, the `show security utm content-filtering statistics` output is also updated to align with the new file types available in the rule match criteria.

  - Renamed the content filtering security logging option `seclog` to `log` to match with the Junos OS configuration standard.

- Rephrased the reason string associated with content filtering security log message.

  [See content-filtering (Security UTM Policy), content-filtering (Security Feature Profile), and show security utm content-filtering statistics.]

User Interface and Configuration

- **Load JSON configuration data with unordered list entries (ACX Series, EX Series, MX Series, PTX Series, QFX Series, SRX Series, vMX, and vSRX)**—The Junos schema requires that list keys precede any other siblings within a list entry and appear in the order specified by the schema. Junos devices provide two options to load JSON configuration data that contains unordered list entries:

  - Use the `request system convert-json-configuration` operational mode command to produce JSON configuration data with ordered list entries before loading the data on the device.

  - Configure the `reorder-list-keys` statement at the `[edit system configuration input format json]` hierarchy level. After you configure the statement, you can load JSON configuration data with unordered list entries, and the device reorders the list keys as required by the Junos schema during the load operation.

  When you configure the `reorder-list-keys` statement, the load operation can take significantly longer to parse the configuration, depending on the size of the configuration and number of lists. Therefore, for large configurations or configurations with many lists, we recommend using the `request system convert-json-configuration` command instead of the `reorder-list-keys` statement.

  [See json and request system convert-json-configuration.]

VPNs

- **Deprecating IPsec Manual VPN Configuration Statement (SRX Series Devices and vSRX running kmd process)**—Starting in Junos OS Release 22.3R1, we'll be deprecating the Manual IPsec VPN (flow mode). This means that you cannot establish a manual IPsec security association (SA) using the `[edit security ipsec vpn` *`vpn-name`* `manual]` configuration hierarchy.

  As part of this change, we'll be deprecating the `[edit security ipsec vpn vpn-name manual]` hierarchy level and its configuration options.

  [See manual.]

- **Save User Credentials on Juniper Secure Connect Application (SRX Series and vSRX)**—As a system administrator, you can now allow a user to save username or username and password for easy access:

  - using `set client-config` *`name`* `credentials username` option at the `edit security remote-access` hierarchy level to save the username.

- using `set client-config name credentials password` option at the `edit security remote-access` hierarchy level to save both the username and password.

Note that you cannot configure both `username` and `password` options at the same time. If you have not configured any of the credentials configuration options, then the application does not remember the user credentials.

[See client-config (Juniper Secure Connect) and Juniper Secure Connect Application Overview.]

Known Limitations

IN THIS SECTION

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.

Infrastructure

- To upgrade to Junos OS Release 21.2R1, you need to include the no-validate option when issuing the upgrade command. Junos OS releases prior to 20.4R1 do not support the no-validate option with unified ISSU. In order to upgrade from an older release to Junos OS Release 21.2R1 with unified ISSU, you must first upgrade to a release that supports the no-validate option for unified ISSU, such as Junos OS release 20.4R1. PR1568757

VPNs

- On SRX5000 line of devices, in some scenario, the device output might display obsolete IPsec SA and NHTB entry even when the peer tear down the tunnel. PR1432925

Open Issues

IN THIS SECTION

Learn about open issues in Junos OS Release 22.1R1 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.

Flow-Based and Packet-Based Processing

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

General Routing

- HTTP sessions takes approximately 10 minutes to re-establish after a link flap between hub and spoke. PR1577021

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

- HA AP mode on-box logging in Logical Systems and Tenant Systems, Intermittently Security log contents of binary log file in Logical Systems and Tenant Systems are not as expected. PR1587360

- When you enable TCP path finder in the VPN gateway, VPN connection is established properly. After VPN connection is established, able to ping from JSC installed client to server behind gateway, but unable to ping from server behind gateway to JSC installed client.

  PR1611003

- The PKID process stops due to null pointer dereferencing during local certificate verification in some cases. PR1624844
- On SRX1500 devices, ISSU is getting aborted with ISSU is not supported for Clock Synchronization (SyncE). PR1632810
- SMTPS sessions are not getting identified when traffic is sent from IXIA (BPS) profile. PR1635929
- The remote access Juniper Networks standard license might not get freed up while disconnect or reconnect after RG0 failover. PR1642653
- AAMW ACTION LOG are not observed when setting log notifications sometimes. PR1644000
- IDP clear counters for Logical Systems and Tenant Systems not working. PR1648187

High Availability (HA) and Resiliency

- ISSU will be aborted or failed with the warning. `'warn-message "ISSU is not supported for Clock Synchronization (SyncE)";''override'In '/var/tmp/paSBfY/etc/indb//config.indb' line 162included from '/var/tmp/paSBfY/etc/indb/issu.indb' line 10 'override' syntax errorISSU not supported as current image uses explicit tags for message structures.` PR1628172

Network Address Translation (NAT)

- In AA mode with NAT configuration, on RG failover, traffic getting dropped on SRX Series devices. PR1636596

User Interface and Configuration

- Use load update instead of load override to prevent the error messages. PR1630315

- On all Junos OS and Junos OS EVO platforms, when copy-config, get-configuration, discard-change RPCs run in two parallel NETCONF sessions and the database is also accessed in parallel by two NETCONF sessions, it leads to database corruption and mgd related services might stop. PR1641025

VPNs

- On SRX5400, SRX5600, and SRX5800 devices, during in-service software upgrade (ISSU), the IPsec tunnels flap, causing a disruption of traffic. The IPsec tunnels recover automatically after the ISSU process is completed. PR1416334
- Fragment packets through policy based IPsec tunnel could be dropped in some rare case when PMI is enabled. PR1624877

Resolved Issues

IN THIS SECTION

Learn which issues were resolved in the Junos OS main and maintenance releases 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.

Resolved Issues: 22.1R1

IN THIS SECTION

Application Layer Gateways (ALGs)

- Junos OS: MX Series and SRX Series: The flowd daemon will crash if the SIP ALG is enabled and specific SIP messages are processed (CVE-2022-22175). PR1604123

Authentication and Access Control

- The authentication delay might occur upto 60 seconds if same user authenticates. PR1626667

Chassis Clustering

- SRX chassis cluster redundancy group IP monitoring might fail for redundancy group on secondary node. PR1594187
- Secondary node in a chassis cluster might go into reboot loop on SRX Series devices. PR1606724
- SPU might become offline on standby node after failover in SRX Series devices. PR1624262
- BFD over high availability ICL link might flap. PR1631938
- Post a series of actions MNHA functionality might not be available despite the configuration presence. PR1638794

Flow-Based and Packet-Based Processing

- The services offload packets processed counter not incremented in security flow statistics. PR1616875
- Security traffic log display service-name as none for some applications. PR1619321
- Cleartext fragments are not processed by flow. PR1620803
- VLAN tagged packets might be dropped at TAP mode enabled interface. PR1624041
- The flowd process might generate core files if route change or delete in PMI mode. PR1624707
- Packets might not be classified according to the CoS rewrite configuration. PR1634146
- The process nsd might crash continuously due to failure in creating/reinitializing the file /var/db/ext/monitor-flow-cfg. PR1638008

General Routing

- When using log templates with Unified Policies, logs were not generated in a predictable manner. A new construct has been added that allows you to define a default log profile using the set security log profile name default-profile command can be used to improve this behavior when multiple log profiles are defined. PR1570105
- The process pkid might generate core file is observed during local certificate enrollment. PR1573892
- The fxp0 interface of an SRX550 in cluster might become unreachable from an external network. PR1575231
- On SRX Series devices with Chassis Cluster, the error message tcp_timer_keep:Local(0x81100001:60753) Foreign(0x8f100001:33010) is seen in messages log every 80 seconds. PR1580667
- BGP adjacency might not get established in Layer 2 IRB scenario. PR1582871
- The show security idp counters command is not having tenant option in it's syntax. PR1586220
- Getting UNKNOWN instead of HTTP-PROXY for application and UNKNOWN instead of GOOGLE-GEN in RT-FLOW close messages These messages can be seen in the RT-flow close log and these are due to JDPI not engaged for the session. This might affect the app identification for the web-proxy session traffic. PR1588139
- Cross ping fails to another device with packet size above 2400 bytes and Jumbo frame is enabled. PR1593015

- When combining log profiles and unified policies RT_FLOW_SESSION_DENY logs were not being generated corrected. PR1594587

- DNS proxy functionality might not work on VRRP interfaces. PR1607867

- Interface state is reset after a Packet Forwarding Engine restarts. PR1613314

- Enabling security-metadata-streaming DNS policy might cause a data plane memory leak. PR1613489

- The new client might not be able to connect using Juniper Secure Connect if the size of INI file content exceeds the maximum INI file size buffer. PR1613993

- PFE might crash and flowd core might be observed when APPQoS is configured. PR1615797

- On SRX-Series devices running DNS Security in secure-wire mode, DGA verdicts would not be returned to the device PR1616075

- The SRX Series device Packet Forwarding Engine crash might be observed when the DNS Security feature is enabled. PR1616171

- On SRX Series devices using on-box logging, LLMD write failures might be seen under high load. The output of show security log llmd counters command can be used to view LLMD behavior. PR1620018

- Traffic might get dropped due to memory issue on some SRX Series devices. PR1620888

- The flowd process might stop on SRX or NFX in AppQoE scenarios. PR1621495

- A major chassis alarm for Intel NIC Tx port stuck issue is added on SRX4100 and SRX4200 devices. PR1624078

- Under rare circumstances, an Packet Forwarding Engine or flowd process generates core files when running AAMW. PR1624124

- In rare circumstances, the pkid process could stop and generate a core file when there was limited memory available on the Routing Engine. PR1624613

- Running DNS on all SRX Series devices, a memory leak on Packet Forwarding Engine might occur. PR1624655

- Core files might be reported on installing IDP security package. PR1625364

- The flowd process lost heartbeat for 45 consecutive seconds without alarm raised. PR1625579

- The error might be seen after configuring a unified security policy allowing some application categories PR1628202

- When viewing DNS Tunnel detections in the ATP cloud portal, the source IP and destination IP metadata is reversed. PR1629995

- Depending on the configuration of the SRX Series devices, the duplicate events might have been written to the on-box logging database. PR1630123

- LLDP packets might be sent with incorrect source MAC for RETH or LAG child members. PR1630886

- The srxpfe process might crash on SRX4600. PR1630990

- Reverse DNS lookups will no longer be stored in the DNSF cache when using DNS security. PR1631000

- Signature package update might fail and the appid process might stop on SRX Series devices. PR1632205

- Tasks of download manager might not be resumed post reboot. PR1633503

- Unable to connect to domain controller on installing Microsoft KB update. PR1637548

- The error is seen during the NON-ISSU upgrade from Junos OS 15.1 release to Junos OS 18.2 release and later releases. PR1639610

- Configuration change during AppQoS session might result in Packet Forwarding Engine pause with flowd core. PR1640768

- The KRT queue might get stuck with the error- ENOMEM -- Cannot allocate memory. PR1642172

- The pfe process might pause on SRX Series devices. PR1642914

- On-box security logs might be not storing the session-id as a 64-bit integer, resulting in incorrect session-id's being present in the on-box logs. PR1644867

Interfaces and Chassis

- Members MAC might be different from parent reth0 interface, resulting loss of traffic. PR1583702

Intrusion Detection and Prevention (IDP)

- IDP signature install taking longer time. PR1615985

- Device is paused while checking the show security idp attack attack-list policy combine-policy command. PR1616782

- On SRX Series devices, the request security idp pcap-analysis tool has had usability improvements. PR1617390

- Updating the IDP signature database might get the upgrade stuck in the state In progress:Performing Offline download. PR1623857

J-Web

- Error your session has expired. Click ok to re-login might get error when using J-Web with root user. PR1611448
- The AM or PM time format is displayed in Customize for Last field at Monitor > Logs > All Events. PR1628649
- After a HA cluster is created, you are unable to edit it in J-Web. PR1636237
- The reboot or halt from J-Web might fail on SRX series devices. PR1638370

Network Address Translation (NAT)

- DNS proxy service on SRX Series devices might stop working after commit operation is performed. PR1598065
- New persistent NAT or normal source NAT sessions might fail due to noncleared aged out sessions. PR1631815

Platform and Infrastructure

- The ppmd process might stop after an upgrade on SRX Series devices. PR1335526
- Traffic through one SPU might stop with potential packet drop issue with alarm as FPC major errors raised due to the PIC_CMERROR_TALUS_PKT_LOSS error. PR1600216
- The SNMP packet (traps or polls) will be dropped if it crosses multiple routing instances on SRX Series devices. PR1616775
- SRX accounting and auditd process might not work on secondary node. PR1620564
- Error message gencfg_cfg_msg_gen_handler drop might be seen after running commit command. PR1629647
- When route preferred metric is different for different RPM policies, the same metric is not reflected in routing records. PR1634129
- SCB reset with error: zfchip_scan line = 844 name = failed due to PIO errors. PR1648850

Routing Policy and Firewall Filters

- SSL proxy might not be performed when SSL proxy profile is referenced in the zone or global policy. PR1608029
- All feed(s) of category IP filter might be removed after committing SecIntel related configurations. PR1611073
- Redundancy might get affected in SRX Chassis Cluster scenario. PR1618025

Routing Protocols

- Observing commit error while configuring routing-options rib inet6.0 static on all Junos OS platforms. PR1599273
- The wrong BGP path might get selected even when a better or preferred route is available. PR1616595

User Interface and Configuration

- The mgd process might generate core files upon ISSU upgrade. PR1632853

VPNs

- The iked process might restart and generate core during session state activation or deactivation. PR1573102
- Certificate identifier length for PKI CMPv2 CA cert is not displayed as expected in certain cases. PR1589084
- The configuration change in SRG-1 might cause HA link encryption tunnel flap. PR1598338
- The kmd might crash with IPsec tunnel enabled on SRX or vSRX platforms. PR1599639
- The flowd process might stop and generate a corefile after upgrade. PR1603670
- Uneven IPsec tunnel distribution might be seen post tunnels re-establishment. PR1615763
- Traffic over IPsec tunnels might be dropped post control link failure. PR1627557
- Traffic loss over IPsec tunnel might be seen on SRX Series devices. PR1628007
- SRX Series devices generates core files after upgrading to any Junos OS release. PR1628947
- The kmd process might stop if the IKE negotiation fragment packets are missed during initiating an IKE SA rekey. PR1638437

- The pki process might stop during cmpv2 auto-re-enrollment. PR1642410

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 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
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 22.1R1 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

IN THIS SECTION

Learn about new features introduced in this release for vMX.

Multicast

- **Translation of MVPN Type 5 routes to MSDP SA routes (MX480, MX960, and vMX)**—Starting in Junos OS Release 22.1R1, Junos OS supports the conversion of multicast virtual private network (MVPN) Type 5 routes to Multicast Source Discovery Protocol (MSDP) source active (SA) routes, as described in the RFC draft-ietf-bess-mvpn-sa-to-msdp-00.txt. In previous releases, Junos OS supports conversion only from MSDP SA to MVPN Type 5.

  Enable MVPN-to-MSDP conversion at the `[edit routing-instance` *`routing-instance-name`* `protocols mvpn mvpn-mode spt-only convert-sa-to-msdp]` hierarchy level.

  You can verify the conversion by running the `[show msdp source-active instance` *`instance-name`*`]` command.

  [See Understanding Next-Generation MVPN Control Plane.]

Network Management and Monitoring

- **Enhancement to <get-syslog-events> RPC with additional filtering options (cSRX, MX Series routers and vMX, SRX300, SRX320, SRX340, SRX345, SRX380, SRX550HM, SRX4100, SRX4200, SRX4600, SRX5400, SRX5600, SRX5800, vSRX, and vSRX 3.0)**—In Junos OS Release 22.1R1, we've introduced the following new tags in the `<get-syslog-events>` RPC. These tags provide additional options for filtering system log messages.

  ```
  <start-count></start-count>
  <end-count></end-count>
  <total-events/>
  ```

```
<pretty/>
<print-json/>
```

[See Overview of Junos OS System Log Messages and syslog (System).]

What's Changed

IN THIS SECTION

Learn about what changed in the Junos OS main and maintenance releases for vMX.

What’s Changed in Release 22.1R1

IN THIS SECTION

Junos OS API and Scripting

- **The `<request-system-zeroize>` RPC response indicates when the device successfully initiates the requested operation (ACX Series, EX Series, MX Series, PTX Series, QFX Series, SRX Series, vMX, and vSRX)**—When the `<request-system-zeroize>` RPC successfully initiates the zeroize operation, the device emits the `<system-zeroize-status>zeroizing re0</system-zeroize-status>` response tag to indicate that the process has started. If the device fails to initiate the zeroize operation, the device does not emit the `<system-zeroize-status>` response tag.

Network Management and Monitoring

- **Junos XML protocol Perl modules deprecated (ACX Series, EX Series, MX Series, PTX Series, QFX Series, SRX Series, vMX, and vSRX)**—We no longer provide the Junos XML protocol Perl client for download. To use Perl to manage Junos devices, use the NETCONF Perl library instead.

  [See Understanding the NETCONF Perl Client and Sample Scripts.]

- **Changes when deactivating or deleting instances of the ephemeral configuration database (ACX Series, EX Series, MX Series, PTX Series, QFX Series, SRX Series, vMX, and vSRX)**—The following changes apply when you deactivate or delete ephemeral database instances in the static configuration database:

  - When you deactivate the entire `[edit system configuration-database ephemeral]` hierarchy level, the device deletes the files and corresponding configuration data for all user-defined ephemeral instances. In earlier releases, the files and configuration data are preserved; however, the configuration data is not merged with the static configuration database.

  - When you delete an ephemeral instance in the static configuration database, the instance's configuration files are also deleted. In earlier releases, the configuration files are preserved.

  - You can delete the files and corresponding configuration data for the default ephemeral database instance by configuring the `delete-ephemeral-default` statement in conjunction with the `ignore-ephemeral-default` statement at the `[edit system configuration-database ephemeral]` hierarchy level.

  [See Enable and Configure Instances of the Ephemeral Configuration Database.]

- **Support for automatically synchronizing an ephemeral instance configuration upon committing the instance (EX Series, MX Series, MX Series Virtual Chassis, PTX Series, QFX Series, and vMX)**—You can configure an ephemeral database instance to synchronize its configuration to the other Routing Engine every time you commit the ephemeral instance on a dual Routing Engine device or an MX Series Virtual Chassis. To automatically synchronize the instance when you commit it, include the `synchronize` statement at the `[edit system commit]` hierarchy level in the ephemeral instance's configuration.

  [See Commit and Synchronize Ephemeral Configuration Data Using the NETCONF or Junos XML Protocol.]

User Interface and Configuration

- **Load JSON configuration data with unordered list entries (ACX Series, EX Series, MX Series, PTX Series, QFX Series, SRX Series, vMX, and vSRX)**—The Junos schema requires that list keys precede any other siblings within a list entry and appear in the order specified by the schema. Junos devices provide two options to load JSON configuration data that contains unordered list entries:

- Use the `request system convert-json-configuration` operational mode command to produce JSON configuration data with ordered list entries before loading the data on the device.
- Configure the `reorder-list-keys` statement at the `[edit system configuration input format json]` hierarchy level. After you configure the statement, you can load JSON configuration data with unordered list entries, and the device reorders the list keys as required by the Junos schema during the load operation.

When you configure the `reorder-list-keys` statement, the load operation can take significantly longer to parse the configuration, depending on the size of the configuration and number of lists. Therefore, for large configurations or configurations with many lists, we recommend using the `request system convert-json-configuration` command instead of the `reorder-list-keys` statement.

[See json and request system convert-json-configuration.]

Known Limitations

There are no known limitations in hardware and software in Junos OS 22.1R1 for vMX.

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

Open Issues

IN THIS SECTION

Learn about open issues in Junos OS Release 22.1R1 release for vMX.

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

Platform and Infrastructure

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

Resolved Issues

IN THIS SECTION

Learn which issues were resolved in the Junos OS main and maintenance releases 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: 22.1R1

IN THIS SECTION

General Routing

- Firewall sensors information of MPC10E, MPC11E, MPC12E, vMX ZT MPC line cards are not getting streamed to telemetry. PR1632477

Interfaces and Chassis

- CFM enhanced SLA iterators monitoring might stop after restarting chassis control process in vMX. PR1622081

Platform and Infrastructure

- vMX might see an FPC restarts when trying to gather software features of its FPC during its start up process. PR1638166

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 22.1R1 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

Learn about new features introduced in this release for vRR.

What's Changed

IN THIS SECTION

Learn about what changed in the Junos OS main and maintenance releases for vRR.

What's Changed in Release 22.1R1

There are no changes in behavior and syntax in Junos OS Release 22.1R1 for vRR.

Known Limitations

There are no known limitations in hardware and software in Junos OS 22.1R1 for vRR.

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

To learn more about common BGP or routing known limitations in Junos OS 21.1R1, see "Known Limitations" on page 78 for MX Series routers.

Open Issues

There are no known issues in hardware and software in Junos OS Release 22.1R1 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

IN THIS SECTION

Learn which issues were resolved in the Junos OS main and maintenance releases 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: 22.1R1

IN THIS SECTION

General Routing

- Monitor traffic interface doesn't work on em2 interface. PR1629242
- vRR VM might establish its identity as Olive after a CLI software upgrade PR1635950
- Video console for vRR might not work after an upgrade. PR1644806

Junos OS Release Notes for vSRX

IN THIS SECTION

These release notes accompany Junos OS Release 22.1R1 for vSRX. They describe new and changed features, limitations, and known and resolved problems in the hardware and software.

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

What's New

IN THIS SECTION

Learn about new features introduced in this release for vSRX.

Application Identification (AppID)

- **TLS 1.3 support for session resumption using PSK (SRX Series and vSRX)**—Starting in Junos OS Release 22.1R1, TLS 1.3 supports session resumption using a pre-shared key (PSK) in SSL proxy to reduce SSL handshake overhead. Session resumption using PSK allows resuming the session with a previously established shared secret key.

  Session resumption shortens the handshake process and accelerates SSL transactions resulting in improved performance while maintaining appropriate level of security.

  [See SSL Performance Enhancements.]

Ethernet Switching and Bridging

- **Flexible VLAN tagging (vSRX and vSRX 3.0)**—Starting in Junos OS Release 22.1R1, vSRX and vSRX 3.0 instances deployed on KVM and VMware platforms support flexible VLAN tagging on revenue and reth interfaces.

  You use VLAN tagging to indicate which packet belongs to which VLAN by tagging the packet with a VLAN tag in the Ethernet frame. Flexible VLAN tagging supports transmission of 802.1Q VLAN single-tag frames on logical interfaces on the Ethernet port. With this feature support you can avoid multiple virtual functions on the network interface card (NIC) and reduce the need of additional interfaces.

  [See Configuring VLAN Tagging and flexible-vlan-tagging (Interfaces).]

Intrusion Detection and Prevention

- **Encryption support for IDP packet capture (SRX Series, vSRX, and vSRX 3.0)**—Starting in Junos OS Release 22.1R1, you can enable a secure SSL or TLS connection to send an encrypted IDP packet capture log to the packet capture receiver. To establish the SSL or TLS connection, you must specify the SSL initiation profile that you want to use in the IDP packet log configuration.

  In earlier releases, when IDP detects an attack, it sends a decrypted IDP packet log to the packet capture receiver over UDP traffic. Sending a decrypted packet log is not a secure process, especially when packet-log is captured for encrypted traffic.

  To enable SSL or TLS connection for IDP packet log, run the `set security idp sensor-configuration packet-log ssl-profile-name` *`profile-name`* command. To view the new packet log counters, use the `show security idp counters packet-log` command.

  [See IDP Security Packet Capture, packet-log (Security IDP Sensor Configuration), and show security idp counters packet-log.]

IPv6

- **NDP and DAD proxy support on multiple interfaces (SRX Series, vSRX, and vSRX 3.0)**—Starting in Junos OS Release 22.1R1, we support Neighbor Discovery Protocol (NDP) and Duplicate Address Detection (DAD) proxy functionality on multiple interfaces (interface unrestricted mode).

  To enable NDP and DAD proxy (interface unrestricted mode), use the `set interfaces <interface> unit <number> family inet6 ndp-proxy interface-unrestricted` and `set interfaces <interface> unit <number> family inet6 dad-proxy interface-unrestricted` commands respectively.

  To view the NDP and DAD proxy (interface unrestricted mode) statistics and to monitor proxy requests and responses use the `show system statistics icmp6` command.

  [See NDP Proxy and DAD Proxy, ndp-proxy, dad-proxy, and show system statistics icmp6.]

- **Router advertisement proxy support (NFX Series, SRX Series, vSRX, and vSRX 3.0)**—Starting in Junos OS Release 22.1R1, we support router advertisement proxy on the listed devices. With this functionality, the device can proxy the router advertisement packets from a service provider router to the clients (host).

  [See Router Advertisement Proxy, downstream, downstream-mode, upstream-mode, and show ipv6 router-advertisement.]

Juniper Advanced Threat Prevention Cloud (ATP Cloud)

- **IoT device discovery and classification (NFX150, NFX350, SRX340, SRX345, SRX4100, SRX4200, SRX5400, SRX5600, SRX5800 line of devices, and vSRX)**—In Junos OS Release 22.1R1, we introduce the Internet of Things (IoT) device discovery and classification feature on the listed devices.

  In a typical workflow:

  1. A security device identifies IoT devices based on the traffic flow.

  2. The device streams relevant packet metadata to Juniper Advanced Threat Prevention (ATP) Cloud.

  3. Juniper ATP Cloud discovers and classifies IoT devices based on brand, device model, type, and so on.

  You can view the list of identified IoT devices on the Juniper ATP Cloud portal. You can also create threat feeds to enforce security policies across IoT traffic in the network.

  With the knowledge of IoT devices in a network, network administrators can better manage their network security and reduce the IoT attack surface.

  [See IoT Security Overview.]

Network Management and Monitoring

- **Enhancement to <get-syslog-events> RPC with additional filtering options (cSRX, MX Series routers and vMX, SRX300, SRX320, SRX340, SRX345, SRX380, SRX550HM, SRX4100, SRX4200, SRX4600, SRX5400, SRX5600, SRX5800, vSRX, and vSRX 3.0)**—In Junos OS Release 22.1R1, we've introduced the following new tags in the `<get-syslog-events>` RPC. These tags provide additional options for filtering system log messages.

```
<start-count></start-count>
<end-count></end-count>
<total-events/>
<pretty/>
<print-json/>
```

  [See Overview of Junos OS System Log Messages and syslog (System).]

VPNs

- **Support for search domain name (Juniper Secure Connect Application, SRX Series and vSRX next-generation firewalls)**—As a system administrator, you can configure the set of search domain name that the Juniper Secure Connect application will use to handle DNS lookups. This is applicable for both full tunnel and split tunnel configurations. You can provide more than one search domain names by executing the `set security remote-access client-config name domain-name domain-name` multiple times. When you enter more than one domain name, it automatically adds a separator (comma) to that value. The number of domain names are limited to the total number of characters and must not exceed 1023 characters. For example, the two domain names `juniper.net,lab.juniper.net` consumes 27 characters while `juniper.net` consumes 11 characters.

  [See client-config (Juniper Secure Connect) and Juniper Secure Connect Application Overview.]

Additional Features

We've extended support for the following features to these platforms.

- **Dynamic routing protocols** (SRX5000 line of devices, and vSRX 3.0 running the iked process). We've extended our support to the exchange of dynamic routing information through IPsec VPN tunnels on SRX Series devices running the iked process. You can now enable dynamic routing protocols, such as OSPF, BGP, BFD, PIM, and RIP, on a st0 interface of an IPsec VPN tunnel.

  This feature is supported on the unified iked process using `junos-ike` package. The SRX5K-SPC3 card with RE3 comes with `junos-ike` package installed by default. You must run the command `request system software add optional://junos-ike.tgz` to load the`junos-ike` package explicitly on SRX5K-SPC3 with RE2 and vSRX Virtual Firewall.

  [See Routing Protocols Support on IPsec VPN Tunnels.]

- **Juniper Secure Connect application supports IPv6 addresses** (SRX5000 line of devices, and vSRX 3.0 running the iked process). While connecting to the Juniper Secure Connect application, you can provide an IPv6 address or IPv4 address as the gateway address and assign an IPv6 address or IPv4 address to a remote-access user.

  Earlier Junos OS releases support only IPv4 addresses.

  Note that IPv6 address-assignment is only supported when using certificate or EAP-based authentication

  This feature is supported on the unified iked process using `junos-ike` package. The SRX5K-SPC3 card with RE3 comes with `junos-ike` package installed by default. You must run the command `request system software add optional://junos-ike.tgz` to load the`junos-ike` package explicitly on SRX5K-SPC3 with RE2 and vSRX Virtual Firewall.

- **Traffic selector configuration changes impacts only partial tunnels** (SRX5000 line of devices, and vSRX 3.0 running the iked process). When you modify a traffic selector configuration within a VPN object, only the modified and below configured traffic selectors will go down, and any traffic selector above the modified one is unaffected. In earlier Junos OS releases, when you modify a traffic selector in a VPN object, all the traffic selectors that are part of the VPN object go down and then the tunnel renegotiation occurs.

  Only partial tunnels are impacted when you modify a traffic selector configuration as follows:

  - Add a new configuration.

  - Delete an existing configuration.

  - Update an existing parameter in the configuration.

  - Update the sequence of the configuration by moving it above or below another configuration.

  This feature is supported on the unified iked process using `junos-ike` package. The SRX5K-SPC3 card with RE3 comes with `junos-ike` package installed by default. You must run the command `request system software add optional://junos-ike.tgz` to load the`junos-ike` package explicitly on SRX5K-SPC3 with RE2 and vSRX Virtual Firewall.

  [See traffic-selector.]

- **VLAN-level MACsec on logical interfaces** (EX9253 and QFX5120-48YM)

  [See Media Access Control Security (MACsec) over WAN.]

What's Changed

IN THIS SECTION

Learn about what changed in the Junos OS main and maintenance releases for vSRX.

What’s Changed in Release 22.1R1

IN THIS SECTION

Junos OS API and Scripting

- **The `<request-system-zeroize>` RPC response indicates when the device successfully initiates the requested operation (ACX Series, EX Series, MX Series, PTX Series, QFX Series, SRX Series, vMX, and vSRX)**—When the `<request-system-zeroize>` RPC successfully initiates the zeroize operation, the device emits the `<system-zeroize-status>zeroizing re0</system-zeroize-status>` response tag to indicate that the process has started. If the device fails to initiate the zeroize operation, the device does not emit the `<system-zeroize-status>` response tag.

Network Management and Monitoring

- **Junos XML protocol Perl modules deprecated (ACX Series, EX Series, MX Series, PTX Series, QFX Series, SRX Series, vMX, and vSRX)**—We no longer provide the Junos XML protocol Perl client for download. To use Perl to manage Junos devices, use the NETCONF Perl library instead.

[See Understanding the NETCONF Perl Client and Sample Scripts.]

- **Changes when deactivating or deleting instances of the ephemeral configuration database (ACX Series, EX Series, MX Series, PTX Series, QFX Series, SRX Series, vMX, and vSRX)**—The following changes apply when you deactivate or delete ephemeral database instances in the static configuration database:

  - When you deactivate the entire `[edit system configuration-database ephemeral]` hierarchy level, the device deletes the files and corresponding configuration data for all user-defined ephemeral instances. In earlier releases, the files and configuration data are preserved; however, the configuration data is not merged with the static configuration database.

  - When you delete an ephemeral instance in the static configuration database, the instance's configuration files are also deleted. In earlier releases, the configuration files are preserved.

  - You can delete the files and corresponding configuration data for the default ephemeral database instance by configuring the `delete-ephemeral-default` statement in conjunction with the `ignore-ephemeral-default` statement at the `[edit system configuration-database ephemeral]` hierarchy level.

  [See Enable and Configure Instances of the Ephemeral Configuration Database.]

Platform and Infrastructure

- **Include IPv6 address in a self-signed certificate (SRX Series devices and vSRX3.0)**— We support manual generation of a self-signed certificate for the given distinguished name using IPv6 address in addition to the IPv4 address that was supported earlier. Use the `request security pki local-certificate generate-self-signed` command with `ipv6-address` option to include ipv6 address in a self-signed certificate.

Unified Threat Management (UTM)

- **Content filtering CLI updates (SRX Series and vSRX)**—Starting in Junos OS Release 22.1R1, we've the following updates to the content filtering CLI:

  - Trimmed the list of file types supported for content filtering rule match criteria. Instead of uniquely representing different variants of a file type, now only one `file-type` string represents all variants. Hence, the `show security utm content-filtering statistics` output is also updated to align with the new file types available in the rule match criteria.

  - Renamed the content filtering security logging option `seclog` to `log` to match with the Junos OS configuration standard.

  - Rephrased the `reason` string associated with content filtering security log message.

[See content-filtering (Security UTM Policy), content-filtering (Security Feature Profile), and show security utm content-filtering statistics.]

User Interface and Configuration

- **Load JSON configuration data with unordered list entries (ACX Series, EX Series, MX Series, PTX Series, QFX Series, SRX Series, vMX, and vSRX)**—The Junos schema requires that list keys precede any other siblings within a list entry and appear in the order specified by the schema. Junos devices provide two options to load JSON configuration data that contains unordered list entries:

  - Use the `request system convert-json-configuration` operational mode command to produce JSON configuration data with ordered list entries before loading the data on the device.

  - Configure the `reorder-list-keys` statement at the `[edit system configuration input format json]` hierarchy level. After you configure the statement, you can load JSON configuration data with unordered list entries, and the device reorders the list keys as required by the Junos schema during the load operation.

  When you configure the `reorder-list-keys` statement, the load operation can take significantly longer to parse the configuration, depending on the size of the configuration and number of lists. Therefore, for large configurations or configurations with many lists, we recommend using the `request system convert-json-configuration` command instead of the `reorder-list-keys` statement.

  [See json and request system convert-json-configuration.]

VPNs

- **Deprecating IPsec Manual VPN Configuration Statement (SRX Series Devices and vSRX running kmd process)**—Starting in Junos OS Release 22.3R1, we'll be deprecating the Manual IPsec VPN (flow mode). This means that you cannot establish a manual IPsec security association (SA) using the `[edit security ipsec vpn` *`vpn-name`* `manual]` configuration hierarchy.

  As part of this change, we'll be deprecating the `[edit security ipsec vpn vpn-name manual]` hierarchy level and its configuration options.

  [See manual.]

- **IKEv1 Tunnel establishment not allowed with HSM enabled (vSRX3.0)**—On vSRX 3.0, you can safeguard the private keys used by `pkid` and `iked` processes using Microsoft Azure Key Vault hardware security module (HSM) service. But, you cannot configure Internet Key Exchange version 1 (IKEv1) after enabling the HSM service. If you still try to configure IKEv1 when HSM is enabled, a warning message is displayed.

- **Save User Credentials on Juniper Secure Connect Application (SRX Series and vSRX)**—As a system administrator, you can now allow a user to save username or username and password for easy access:

  - using `set client-config name credentials username` option at the `edit security remote-access` hierarchy level to save the username.

  - using `set client-config name credentials password` option at the `edit security remote-access` hierarchy level to save both the username and password.

  Note that you cannot configure both `username` and `password` options at the same time. If you have not configured any of the credentials configuration options, then the application does not remember the user credentials.

  [See client-config (Juniper Secure Connect) and Juniper Secure Connect Application Overview.]

Known Limitations

There are no known limitations in hardware and software in Junos OS 22.1R1 for vSRX.

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

Open Issues

IN THIS SECTION

Learn about open issues in Junos OS Release 22.1R1 release for vSRX.

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

Flow-Based and Packet-Based Processing

- Traffic in the power mode still passthrough when the ingress logic interface is manually disabled. PR1604144
- The ICMPv6 TCP sequence information is missing in the ICMPv6 error generated. PR1611202
- Keep 1~2 minutes gap between two configuration commits if there are lots of security policies which need time to be processed. PR1625531

General Routing

- Tag RT_FLOW_SESSION_XXX is missing in stream mode. PR1565153
- With SSL proxy configured along with Web proxy, the client session might not closed on the device even though proxy session ends gracefully. PR1580526
- With manual AppID sigpack installation, micro applications group name is not showing in CLI. PR1640040
- AMR when it is enabled in non-cso v6 over v6 mode with IPsec tunnels, the first session after reboot or forward restart, will not have multipath treatment, post that the feature works fine. PR1643570

VPNs

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

Resolved Issues

IN THIS SECTION

Learn which issues were resolved in the Junos OS main and maintenance releases for vSRX.

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

Resolved Issues: 22.1R1

IN THIS SECTION

Flow-Based and Packet-Based Processing

- On SRX Series devices using Unified Policies with IPv6, when attempting to reject certain dynamic-applications a flowd core file might be generated. PR1601806
- Cleartext fragments are not processed by flow. PR1620803

General Routing

- When using log templates with Unified Policies, logs were not generated in a predictable manner. A new construct has been added that allows you to define a default log profile using the set security log profile name default-profile command can be used to improve this behavior when multiple log profiles are defined. PR1570105

- The pkid process might generate core files during auto-re-enrollment of CMPv2 certificates. PR1580442

- Getting UNKNOWN instead of HTTP-PROXY for application and UNKNOWN instead of GOOGLE-GEN in RT-FLOW close messages These messages can be seen in the RT-flow close log and these are due to JDPI not engaged for the session. This might affect the app identification for the web-proxy session traffic. PR1588139

- When combining log profiles and unified policies RT_FLOW_SESSION_DENY logs were not being generated corrected. PR1594587

- High CPU utilization might be seen when Jflow sampling is configured on vSRX HA setup. PR1604775

- For apps getting classified on first packet, the volume update syslog are not getting generated. PR1613516

- The interface speed is limited to 1G on vSRX 2.0 even the speed is set as more than 1G. PR1617397

- Assert core file might be seen when the application goes to no path selected state. PR1617506

- During SaaS probing, due to race condition between APP entry addition and session processing, this core is seen. PR1622787

- Running DNS on all SRX Series devices, a memory leak on Packet Forwarding Engine might occur. PR1624655

- The application package installation might fail with error in SRX Series devices. PR1626589

- vSRX3.0 on VMware ESXi versions 7.0u2 or 7.0u3 with i40e SR-IOV, the traffic stopped after reboot. PR1627481

- Resource errors in show interfaces extensive command output. PR1629986

- Signature package update might fail and the appid process might stop on SRX Series devices. PR1632205

- The pfe process might pause on SRX Series devices. PR1642914

Infrastructure

- The failover process might become slow in a vSRX cluster if the gstatd process stops running. PR1626423

Interfaces and Chassis

- Static route might not work on vSRX. PR1613430

Intrusion Detection and Prevention (IDP)

- Device is paused while checking the show security idp attack attack-list policy combine-policy command. PR1616782

J-Web

- J-Web might only allow certain types of interfaces to be added in a routing instance. PR1637917

Routing Policy and Firewall Filters

- After policy configuration commit with source tenant and destination services id field set as 0 due to this Incoming traffic processed by first policy. PR1617026

- Policy re-match extensive is not working for SVR traffic. PR1618717

Routing Protocols

- The rpd process might generate core file due to memory corruption. PR1599751

- Memory leak in global data shm process might lead to traffic outage. PR1626704

VPNs

- Unable to set DynamoDB in HSM module. PR1599069

- The process kmd might stop if the ike gateway is configured with two IP address. PR1626830

- Issue in certificate based VPN tunnels initiation while using GCP KMS. PR1628722

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 22.1R1 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 22.1R1 for vSRX .tgz** file from the Juniper Networks website. Note the size of the software image.

2. Verify that you have enough free disk space on the vSRX instance to upload the new software image.

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

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

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

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

4. Use FTP, SCP, or a similar utility to upload the Junos OS Release 22.1R1 for vSRX .tgz file to **/var/crash/corefiles/** on the local file system of your vSRX VM. For example:

```
root@vsrx> file copy ftp://username:prompt@ftp.hostname.net/pathname/
junos-vsrx-x86-64-22.1-2022-10-12.0_RELEASE_22.1_THROTTLE.tgz /var/crash/corefiles/
```

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

```
root@vsrx> request system software add /var/crash/corefiles/junos-vsrx-
x86-64-22.1-2022-10-12.0_RELEASE_22.1_THROTTLE.tgz no-copy no-validate reboot
Verified junos-vsrx-x86-64-22.1-2022-10-12.0_RELEASE_22.1_THROTTLE signed by
PackageDevelopmentEc_2017 method ECDSA256+SHA256
THIS IS A SIGNED PACKAGE
WARNING:     This package will load JUNOS 22.1 software.
WARNING:     It will save JUNOS configuration files, and SSH keys
WARNING:     (if configured), but erase all other files and information
WARNING:     stored on this machine.  It will attempt to preserve dumps
WARNING:     and log files, but this can not be guaranteed.  This is the
WARNING:     pre-installation stage and all the software is loaded when
WARNING:     you reboot the system.
Saving the config files ...
Pushing Junos image package to the host...
Installing /var/tmp/install-media-srx-mr-vsrx-22.1-2022-10-12.0_RELEASE_22.1_THROTTLE.tgz
Extracting the package ...
total 975372
-rw-r--r-- 1 30426 950 710337073 Oct 19 17:31 junos-srx-mr-
vsrx-22.1-2022-10-12.0_RELEASE_22.1_THROTTLE-app.tgz
-rw-r--r-- 1 30426 950 288433266 Oct 19 17:31 junos-srx-mr-
vsrx-22.1-2022-10-12.0_RELEASE_22.1_THROTTLE-linux.tgz
Setting up Junos host applications for installation ...
============================================
Host OS upgrade is FORCED
Current Host OS version: 3.0.4
New Host OS version: 3.0.4
Min host OS version required for applications: 0.2.4
============================================
Installing Host OS ...
upgrade_platform: -------------------
upgrade_platform: Parameters passed:
upgrade_platform: silent=0
upgrade_platform: package=/var/tmp/junos-srx-mr-vsrx-22.1-2022-10-12.0_RELEASE_22.1_THROTTLE-
```

```
linux.tgz
upgrade_platform: clean install=0
upgrade_platform: clean upgrade=0
upgrade_platform: Need reboot after staging=0
upgrade_platform: -------------------
upgrade_platform:
upgrade_platform: Checking input /var/tmp/junos-srx-mr-
vsrx-22.1-2022-10-12.0_RELEASE_22.1_THROTTLE-linux.tgz ...
upgrade_platform: Input package /var/tmp/junos-srx-mr-
vsrx-22.1-2022-10-12.0_RELEASE_22.1_THROTTLE-linux.tgz is valid.
upgrade_platform: Backing up boot assets..
cp: omitting directory '.'
bzImage-intel-x86-64.bin: OK
initramfs.cpio.gz: OK
version.txt: OK
initrd.cpio.gz: OK
upgrade_platform: Checksum verified and OK...
/boot
upgrade_platform: Backup completed
upgrade_platform: Staging the upgrade package - /var/tmp/junos-srx-mr-
vsrx-22.1-2022-10-12.0_RELEASE_22.1_THROTTLE-linux.tgz..
./
./bzImage-intel-x86-64.bin
./initramfs.cpio.gz
./upgrade_platform
./HOST_COMPAT_VERSION
./version.txt
./initrd.cpio.gz
./linux.checksum
./host-version
bzImage-intel-x86-64.bin: OK
initramfs.cpio.gz: OK
version.txt: OK
upgrade_platform: Checksum verified and OK...
upgrade_platform: Staging of /var/tmp/junos-srx-mr-
vsrx-22.1-2022-10-12.0_RELEASE_22.1_THROTTLE-linux.tgz completed
upgrade_platform: System need *REBOOT* to complete the upgrade
upgrade_platform: Run upgrade_platform with option -r | --rollback to rollback the upgrade
Host OS upgrade staged. Reboot the system to complete installation!
WARNING:     A REBOOT IS REQUIRED TO LOAD THIS SOFTWARE CORRECTLY. Use the
WARNING:     'request system reboot' command when software installation is
WARNING:     complete. To abort the installation, do not reboot your system,
WARNING:     instead use the 'request system software rollback'
```

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

If no errors occur, Junos OS reboots automatically to complete the upgrade process. You have successfully upgraded to Junos OS Release 22.1R1 for vSRX.

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

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

```
--- JUNOS 22.1-2022-10-12.0_RELEASE_22.1_THROTTLE Kernel 64-bit
JNPR-11.0-20171012.170745_fbsd-
At least one package installed on this device has limited support.
Run 'file show /etc/notices/unsupported.txt' for details.
root@:~ # cli
root> show version
Model: vsrx
Junos: 22.1-2022-10-12.0_RELEASE_22.1_THROTTLE
JUNOS OS Kernel 64-bit  [20171012.170745_fbsd-builder_stable_11]
JUNOS OS libs [20171012.170745_fbsd-builder_stable_11]
JUNOS OS runtime [20171012.170745_fbsd-builder_stable_11]
JUNOS OS time zone information [20171012.170745_fbsd-builder_stable_11]
JUNOS OS libs compat32 [20171012.170745_fbsd-builder_stable_11]
JUNOS OS 32-bit compatibility [20171012.170745_fbsd-builder_stable_11]
JUNOS py extensions [20171017.110007_ssd-builder_release_174_throttle]
JUNOS py base [20171017.110007_ssd-builder_release_174_throttle]
JUNOS OS vmguest [20171012.170745_fbsd-builder_stable_11]
JUNOS OS crypto [20171012.170745_fbsd-builder_stable_11]
JUNOS network stack and utilities [20171017.110007_ssd-builder_release_174_throttle]
JUNOS libs [20171017.110007_ssd-builder_release_174_throttle]
JUNOS libs compat32 [20171017.110007_ssd-builder_release_174_throttle]
JUNOS runtime [20171017.110007_ssd-builder_release_174_throttle]
JUNOS Web Management Platform Package [20171017.110007_ssd-builder_release_174_throttle]
JUNOS srx libs compat32 [20171017.110007_ssd-builder_release_174_throttle]
JUNOS srx runtime [20171017.110007_ssd-builder_release_174_throttle]
JUNOS common platform support [20171017.110007_ssd-builder_release_174_throttle]
JUNOS srx platform support [20171017.110007_ssd-builder_release_174_throttle]
JUNOS mtx network modules [20171017.110007_ssd-builder_release_174_throttle]
JUNOS modules [20171017.110007_ssd-builder_release_174_throttle]
JUNOS srxtvp modules [20171017.110007_ssd-builder_release_174_throttle]
JUNOS srxtvp libs [20171017.110007_ssd-builder_release_174_throttle]
JUNOS srx libs [20171017.110007_ssd-builder_release_174_throttle]
JUNOS srx Data Plane Crypto Support [20171017.110007_ssd-builder_release_174_throttle]
JUNOS daemons [20171017.110007_ssd-builder_release_174_throttle]
JUNOS srx daemons [20171017.110007_ssd-builder_release_174_throttle]
JUNOS Online Documentation [20171017.110007_ssd-builder_release_174_throttle]
JUNOS jail runtime [20171012.170745_fbsd-builder_stable_11]
JUNOS FIPS mode utilities [20171017.110007_ssd-builder_release_174_throttle]
```

Validating the OVA Image

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

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

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

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

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

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

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

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

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

Table 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
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.

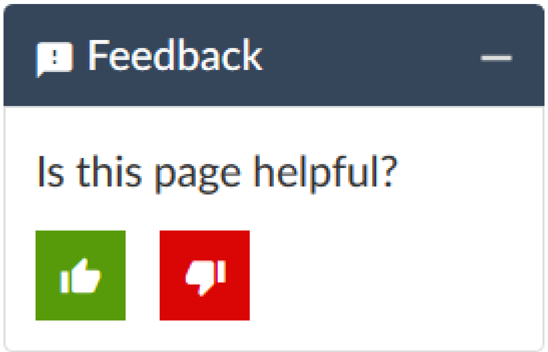
- **Juniper Networks Compliance Advisor**—Review regulatory compliance information about Common Criteria, FIPS, Homologation, RoHS2, and USGv6.

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

Documentation Feedback

We encourage you to provide feedback, comments, and suggestions so that we can improve the documentation. You can provide feedback by using either of the following methods:

- Online feedback system—Click TechLibrary Feedback, on the lower right of any page on the Juniper Networks TechLibrary site, and do one of the following:



Feedback

Is this page helpful?

- Click the thumbs-up icon if the information on the page was helpful to you.
- Click the thumbs-down icon if the information on the page was not helpful to you or if you have suggestions for improvement, and use the pop-up form to provide feedback.

- E-mail—Send your comments to techpubs-comments@juniper.net. Include the document or topic name, URL or page number, and software version (if applicable)

Requesting Technical Support

IN THIS SECTION

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

- JTAC policies—For a complete understanding of our JTAC procedures and policies, review the JTAC User Guide located at https://www.juniper.net/content/dam/www/assets/resource-guides/us/en/jtac-user-guide.pdf.
- Product warranties—For product warranty information, visit https://support.juniper.net/support/warranty/.

- JTAC hours of operation—The JTAC centers have resources available 24 hours a day, 7 days a week, 365 days a year.

Self-Help Online Tools and Resources

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

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

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

Creating a Service Request with JTAC

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

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

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

Revision History

10 August 2023—Revision 12, Junos OS Release 22.1R1– ACX Series, cSRX, EX Series, JRR Series, Juniper Secure Connect, Junos Fusion, MX Series, NFX Series, PTX Series, QFX Series, SRX Series, vMX, vRR, and vSRX.

20 July 2023—Revision 11, Junos OS Release 22.1R1– ACX Series, cSRX, EX Series, JRR Series, Juniper Secure Connect, Junos Fusion, MX Series, NFX Series, PTX Series, QFX Series, SRX Series, vMX, vRR, and vSRX.

2 June 2023—Revision 10, Junos OS Release 22.1R1– ACX Series, cSRX, EX Series, JRR Series, Juniper Secure Connect, Junos Fusion, MX Series, NFX Series, PTX Series, QFX Series, SRX Series, vMX, vRR, and vSRX.

4 May 2023—Revision 9, Junos OS Release 22.1R1– ACX Series, cSRX, EX Series, JRR Series, Juniper Secure Connect, Junos Fusion, MX Series, NFX Series, PTX Series, QFX Series, SRX Series, vMX, vRR, and vSRX.

29 March 2023—Revision 8, Junos OS Release 22.1R1– ACX Series, cSRX, EX Series, JRR Series, Juniper Secure Connect, Junos Fusion, MX Series, NFX Series, PTX Series, QFX Series, SRX Series, vMX, vRR, and vSRX.

25 November 2022—Revision 7, Junos OS Release 22.1R1– ACX Series, cSRX, EX Series, JRR Series, Juniper Secure Connect, Junos Fusion, MX Series, NFX Series, PTX Series, QFX Series, SRX Series, vMX, vRR, and vSRX.

14 September 2022—Revision 6, Junos OS Release 22.1R1– ACX Series, cSRX, EX Series, JRR Series, Juniper Secure Connect, Junos Fusion, MX Series, NFX Series, PTX Series, QFX Series, SRX Series, vMX, vRR, and vSRX.

29 July 2022—Revision 5, Junos OS Release 22.1R1– ACX Series, cSRX, EX Series, JRR Series, Juniper Secure Connect, Junos Fusion, MX Series, NFX Series, PTX Series, QFX Series, SRX Series, vMX, vRR, and vSRX.

16 June 2022—Revision 4, Junos OS Release 22.1R1– ACX Series, cRPD, cSRX, EX Series, JRR Series, Juniper Secure Connect, Junos Fusion, MX Series, NFX Series, PTX Series, QFX Series, SRX Series, vMX, vRR, and vSRX.

5 April 2022—Revision 3, Junos OS Release 22.1R1– ACX Series, cRPD, cSRX, EX Series, JRR Series, Juniper Secure Connect, Junos Fusion, MX Series, NFX Series, PTX Series, QFX Series, SRX Series, vMX, vRR, and vSRX.

24 March 2022—Revision 2, Junos OS Release 22.1R1– ACX Series, cRPD, cSRX, EX Series, JRR Series, Juniper Secure Connect, Junos Fusion, MX Series, NFX Series, PTX Series, QFX Series, SRX Series, vMX, vRR, and vSRX.

16 March 2022—Revision 1, Junos OS Release 22.1R1– ACX Series, cRPD, cSRX, EX Series, JRR Series, Juniper Secure Connect, Junos Fusion, MX Series, NFX Series, PTX Series, QFX Series, SRX Series, vMX, vRR, and vSRX.