Release Notes

Published
2023-09-01

Junos OS Release 23.2R1®

Introduction

Junos OS runs on the following Juniper Network's ® products: ACX Series, cRPD, cSRX, EX Series, JRR Series, Juniper Secure Connect, MX Series, NFX Series, QFX Series, SRX Series, vMX, vRR, and vSRX. These release notes accompany Junos OS Release 23.2R1. They describe new and updated features, limitations, open and resolved problems in the hardware and software.

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

Table of Contents

Junos OS Release Notes for ACX Series

IN THIS SECTION

What's New

IN THIS SECTION

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

To view features supported on the ACX platforms, view the Feature Explorer using the following links. To see which features were added in Junos OS Release 23.2R1, click the Group by Release link. You can collapse and expand the list as needed.

- ACX710
- ACX5448-D
- ACX5448-M
- ACX5448

MPLS

- **Support for bound metrics and bandwidth for PCC Initiated/Delegated type LSPs (RSVP-TE and SR-TE) per RFC5440 (ACX5448, ACX5448-M, ACX5448-D, ACX710, MX204, MX240, MX304, MX150, MX480, MX960, MX10003, MX10004, MX10008, MX10016, MX2008, MX2010, MX2020, and vMX)**—Starting in Junos OS Release 23.2R1, we support metric object and bandwidth object for bounded constraints in a Path Computation Element Protocol (PCEP) connection for Segment Routing label-switched paths (SR-LSPs). Both metric object and bandwidth object are optional objects in PCEP, and can be present in PCInit, PCUpd, and PCRpt PCEP messages.

  To configure bounded metric values for an LSP controller, you can enter `igp-metric-bound <val> | te-metric-bound <val> | delay-metric-bound <val>` at the `[edit protocols mpls label-switched-path <lsp-name> lsp-external-controller` *`controller-name`*`]` hierarchy level.

  To configure bounded metric values for compute profiles, you can enter `bound-metric igp <val> | bound-metric te <val> | bound-metric delay <val>` at the `[edit protocols source-packet-routing compute-profile` *`compute-profile-name`*`]` hierarchy level.

  To use the maximum SR-MPLS segment identifier (SID) depth, use the `set protocols pcep maximum-srmpls-segment-list-depth <val>` configuration.

  To propogate the list, use the `set protocols pcep propagate-lsp-max-segment-list-depth` configuration.

  [See lsp-external-controller, compute-profile, and pcep.]

- **Support to report bandwidth and reservation priority for delegated and PCE-initiated segment routing–traffic engineering (SR-TE) LSPs in Path Computation Element Protocol (ACX5448, ACX5448-M, ACX5448-D, ACX710, MX150, MX204, MX240, MX304, , MX480, MX960, MX2008, MX2010, MX2020, MX10003, MX10004, MX10008, MX10016, and vMX)**—Starting in Junos OS Release 23.2R1, we support the reporting of bandwidth and reservation priority for delegated segment routing–traffic engineering (SR-TE) label-switched paths (LSPs). For Path Computation Client (PCE)-initiated SR-TE LSPs, once the bandwidth, setup priority, and reservation priority request is received from the controller, the Path Computation Client (PCC) reports the same information to the controller.

  > **NOTE**: You can configure bandwidth and reservation priority in PCC only for delegated SR-TE LSPs and not for undelegated and PCE-initiated SR-TE LSPs.

  To configure the `bandwidth-requested` and `bandwidth-reservation-priority` for delegated SR-TE LSPs, include the `bandwidth-requested | bandwidth-reservation-priority` configuration statement at the `[edit protocols source-packet-routing compute-profile` *`compute-profile-name`*`]` hierarchy level.

  [See Reporting Path Optimization Metrics in PCEP.]

Routing Protocols

- **Support to activate BFD strict mode for BGP peer sessions (ACX5448, ACX710, cRPD, MX10003, MX10004, VRR, QFX5110, and QFX5200)**—Starting in Junos OS Release 23.2R1, we support the activation of BFD strict mode for BGP peer sessions that disallows BGP to establish a session until BFD session is successfully established and has stabilized. With the BFD strict mode feature, you can prevent routing churn and minimize network interruption.

  To activate BFD strict mode for BGP peer sessions, include the `strict-mode [bfd-wait-timeout <10-255 seconds>` CLI statement under `bfd-liveness-detection` at the `[edit protocols bgp group` *`group-name`* `neighbor` *`address`*`]` hierarchy level.

  For example, use the following command to activate BFD strict mode for BGP peer sessions:

  `set protocol bgp group` *`group-name`* `neighbor` *`address`* `bfd-liveness-detection [strict-mode [bfd-wait-timeout` *`10-255 seconds`*`]]`

  [See Understanding BFD for BGP, bfd-liveness-detection (BGP).]

Additional Features

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

- **Ephemeral database support for configuring MSTP, RSTP, and VSTP** (ACX Series, EX Series, and QFX Series). You can configure the following protocols in the ephemeral configuration database:
  - Multiple Spanning Tree Protocol (MSTP)
  - Rapid Spanning Tree Protocol (RSTP)
  - VLAN Spanning Tree Protocol (VSTP)

  [See Unsupported Configuration Statements in the Ephemeral Configuration Database.]

What's Changed

IN THIS SECTION

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

General Routing

- **Label-switched interface (LSI) delay during reboot (ACX Series)**—Rebooting ACX Series routers running Junos OS Evolved with a class-of-service routing-instance configuration might encounter errors due to a delay with the label-switched interface (LSI). LSI state information has been added to the output of the <cli>show route instance</cli> command to assist in the analysis of such errors.

  [See show route instance.]

Network Management and Monitoring

- **Changes to the `show system yang package` (`get-system-yang-packages` RPC) XML output (ACX Series, EX Series, MX Series, QFX Series, SRX Series, vMX, and vSRX)**—The `show system yang package` command and `<get-system-yang-packages>` RPC include the following changes to the XML output:

  - The root element is `yang-package-information` instead of `yang-pkgs-info`.
  - A `yang-package` element encloses each set of package files.
  - The `yang-pkg-id` tag is renamed to `package-id`.
  - If the package does not contain translation scripts, the Translation Script(s) (`trans-scripts`) value is `none`.

- **NETCONF server's `<rpc-error>` response changed when `<load-configuration>` uses `operation="delete"` to delete a nonexistent configuration object (ACX Series, EX Series, MX Series, QFX Series, SRX Series, vMX, and vSRX)**—In an earlier release, we changed the NETCONF server's `<rpc-error>` response for when an `<edit-config>` or `<load-configuration>` operation uses `operation="delete"` to delete a configuration element that is absent in the target configuration. We've reverted the changes to the `<load-configuration>` response.

- **Changes to the RPC response for `<validate>` operations in RFC-compliant NETCONF sessions (ACX Series, EX Series, MX Series, QFX Series, SRX Series, vMX, and vSRX)**—When you configure the `rfc-compliant` statement at the `[edit system services netconf]` hierarchy level, the NETCONF server emits only an `<ok/>` or `<rpc-error>` element in response to `<validate>` operations. In earlier releases, the RPC reply also includes the `<commit-results>` element.

Known Limitations

IN THIS SECTION

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

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

Infrastructure

- When upgrading from releases before Junos OS Release 21.2 to Release 21.2 and onward, validation and upgrade might fail. The upgrade requires using the 'no-validate' option to complete successfully. https://kb.juniper.net/TSB18251. PR1568757

Open Issues

IN THIS SECTION

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

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

General Routing

- VXLAN VNI (multicast learning) scaling on QFX5110 traffic issue is seen from VXLAN tunnel to Layer 2 interface. PR1462548
- When there are more than 1 dhcp server connected to the device and zeroize in initiated then multiple route are added and the file server is not reachable after the zeroize if it is not reachable through the default route.PR1675011
- Reserved buffers may be shown as 0. But internally reserved buffers do get used to queue and transmit traffic on the queue. This seems to be a day one issue and will be fixed in future releasesPR1689183
- The AE stats may show 0 bps for Output traffic. It is a CLI output display issue. It will be fixed in the future releases. It does not impact the traffic output.PR1689185
- FIPS mode is not supported in this release for SRXSME devices.PR1697999

Infrastructure

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

Resolved Issues

IN THIS SECTION

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

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

General Routing

- EX/QFX SNMP: jnxOperatingDescr.1.1.0.0 returns blank, but jnxOperatingState.1.1.0.0 returns value. PR1683753
- ACX-5448: pps values seen on interface even when it is in disabled state. . PR1685344
- Traffic blackhole during l2circuit pseudowire redundancy neighbor switchover. PR1686260
- Traffic loss is more than expected with OSPF TI-LFA enabled and the primary path is down. PR1695292
- On ACX5448, an interface with SFP-T optic set to 100m and auto-negotiation disabled will remain down after reboot or on chassis-control restart. PR1702239
- CoS rewrite rules will not work in L3VPN scenario. PR1703840
- Transit traffic drop is observed for the BGP-LU route prefixes with ECMP forwarding path on Junos ACX5448/ACX710 platforms. PR1712564
- The member interface will not be added to the AE bundle if the link-speed of the AE interface doesn't match that of the member. PR1713699
- The traffic through the AE member link will be dropped. PR1714111
- SFP-T cannot be recognized after detecting an I2C error on ACX5448. PR1715924
- SNMP MIB OID output showing wrong temperature value if device running under negative temperature. PR1717105
- The multicast packets could hit the CPU/RE on ACX5448 and ACX710 platforms. PR1722277
- Intermittent MAC move is observed in VPLS environment when ACX5448 or ACX710 is acting as a PE. device PR1722919
- Traffic is getting discarded in PFE when forwarding-table is changed. PR1723624

Infrastructure

- Unable to take recovery snapshots after USB upgrade is performed on ACX710. PR1717710

Interfaces and Chassis

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

User Interface and Configuration

- The system won't come up in a working state post reboot for upgrade validation fails to detect invalid host-name. PR1703745

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.

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 sixty months after the first general availability date and customer support for an additional six more months.

> **NOTE:** The sixty months of support for EEOL releases is introduced in Junos OS 23.2 release and is available for all later releases. For releases prior to 23.2, the support for EEOL releases continues to be thirty six 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 21.2 to the next three releases – 21.3, 21.4 and 22.1 or downgrade to the previous three releases – 21.1, 20.4 and 20.3.

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, 21.2 is an EEOL release. Hence, you can upgrade from 21.2 to the next two EEOL releases – 21.4 and 22.2 or downgrade to the previous two EEOL releases – 20.4 and 20.2.

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)	60 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 cRPD

IN THIS SECTION

What's New

IN THIS SECTION

Learn about new features introduced in this release for cRPD.

Routing Protocols

- **Support to activate BFD strict mode for BGP peer sessions (ACX5448, ACX710, cRPD, MX10003, MX10004, VRR, QFX5110, and QFX5200)**—Starting in Junos OS Release 23.2R1, we support the activation of BFD strict mode for BGP peer sessions that disallows BGP to establish a session until BFD session is successfully established and has stabilized. With the BFD strict mode feature, you can prevent routing churn and minimize network interruption.

  To activate BFD strict mode for BGP peer sessions, include the `strict-mode [bfd-wait-timeout <10-255 seconds>` CLI statement under `bfd-liveness-detection` at the `[edit protocols bgp group` *`group-name`* `neighbor` *`address`*`]` hierarchy level.

  For example, use the following command to activate BFD strict mode for BGP peer sessions:

`set protocol bgp group group-name neighbor address bfd-liveness-detection [strict-mode [bfd-wait-timeout 10-255 seconds]]`

[See Understanding BFD for BGP, bfd-liveness-detection (BGP).]

- **Support for AIGP for INET, INET6, L3VPN, and L3VPN6 (cRPD, and MX10008)**—Starting in Junos OS 23.2R1, we support AIGP for INET unicast, INET6 unicast, L3VPN, and L3VPN6 address family. Use the existing show route command to see the output with multiple paths.

  [See aigp.]

Additional Features

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

- **Interoperability of segment routing with LDP** (cRPD). You can use OSPF or IS-IS to enable segment routing devices to operate with the LDP devices that are not segment routing capability.

  [See Mapping Server for Segement Routing and mapping-server-entry.]

- **BMP support for local (RIB) policy** (cRPD). We've enhanced the BGP Monitoring Protocol (BMP) to monitor the local routing information base (RIB) `loc-rib` policy. We've added the `loc-rib` policy to the RIB types under the `bmp route-monitoring` statement.

  [See BGP Monitoring Tool, BMP Routing Options, and route-monitoring.]

What's Changed

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

Known Limitations

There are no known limitations in hardware or software in this release 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 or software in this release 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

Learn about the issues fixed in this release for cRPD.

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

Infrastructure

- The rpd process generates core files while deleting protocols MPLS in krt_fc_table_destroy on cRPD. PR1703415
- JCNR can commit routing-options forwarding-table channel vrouter export pplb command although pplb policy is not defined generating core. PR1715316
- The gRPC port modification fails other than fixed port 50051. PR1722826

Routing Protocols

- Traffic null routes are observed when it takes a long time to remove the BGP routes from RIB. PR1695062
- Need changes in script /usr/sbin/rpd-helper for sysctl returns an error while starting up the rpd-helper. PR1707633

Junos OS Release Notes for cSRX

IN THIS SECTION

What's New

IN THIS SECTION

Learn about new features introduced in this release for cSRX.

Authentication and Access Control

- **SSL proxy support (cSRX)**—Starting in Junos OS Release 23.2R1, we support SSL proxy. SSL proxy is a transparent proxy that performs SSL encryption and decryption between the client and the server.

  [See SSL Proxy and show services ssl proxy statistics.]

Device Security

- **Support for security feeds (AAMW, DNS, ETI, and SecIntel) (cSRX)**—Starting in Junos OS Release 23.2R1, cSRX can receive threat feeds and intelligence such as advanced anti-malware (AAMW),

Domain Name System (DNS), Encrypted Traffic Insights (ETI), and Security Intelligence (SecIntel) from the policy enforcer.

To enable profile inspection, you assign an AAMW profile and a SecIntel profile group to security policies . After the feeds are generated, you can use the feeds as dynamic address entries against which you match designated traffic and perform policy actions.

[See **Juniper Advanced Threat Prevention Cloud (ATP Cloud)** and **Security Policies User Guide for Security Devices**.]

- **Explicit proxy support (cSRX)**—Starting in Junos OS Release 23.2R1, cSRX supports explicit proxy for remote users and mobile users. Explicit proxy acts as a secure web gateway between the client and actual destination server. Additionally, explicit proxy manages the session between a client to cSRX and from cSRX to the actual server. You must use an explicit proxy if you use proxy auto-configuration (PAC) on your end users' endpoints.

  Explicit web-proxy on cSRX does not listen to Junos events related to the physical interface (IFD), logical interface (IFL), interface family (IFF), or interface address (IFA). Therefore, cSRX cannot determine whether the interface is up or down.

  [See Understanding Explicit Proxy and Downloading the Junos OS IDP Signature Package through an Explicit Proxy Server Overview.]

- **Policy support for explicit proxy (cSRX)**—Starting in Junos OS Release 23.2R1, cSRX supports security policy configuration for explicit proxy.

  [See Understanding Explicit Proxy and Downloading the Junos OS IDP Signature Package through an Explicit Proxy Server Overview.]

Platform and Infrastructure

- **Support for increased vCPUs and memory (cSRX)**—Starting in Junos OS Release 23.2R1, Container Firewall (cSRX) supports more virtual CPUs (vCPUs) and memory. With more vCPUs and memory, you can increase throughput, improve the performance and scale up your operations. You can now deploy cSRX in the cloud-native environment.

  [See cSRX Deployment Guide for Bare-Metal Linux Server | cSRX | Juniper Networks].

Unified Threat Management (UTM)

- **Support for content filtering based on file content (cSRX)**—Starting in Junos OS Release 23.2R1, Content Security performs content filtering to determine the file type, based on the file content. Content security analyzes the file to accurately determine the file type.

  This feature replaces the legacy content filtering based on MIME type, content type, and protocol commands.

You can define the content filtering rule-set and rules from the `[edit security utm utm-policy <utm-policy-name> content-filtering]` hierarchy and use these rules from the `[edit security utm default-configuration content-filtering]` hierarchy for controlling the traffic direction.

The existing `show security utm content-filtering statistics` command is enhanced to display the content filtering system statistics and errors.

[See Content Filtering, content-filtering (Security UTM Policy), utm, and utm default-configurationshow security utm content-filtering statistics.]

- **Support for cache Preload for EWF (cSRX, SRX1500, SRX4100, SRX4200, SRX4600, SRX5400, SRX5600, SRX5800, and vSRX3.0)**—Starting in Junos OS Release 23.2R1, we support preloading of cache with the top-rated, frequently visited URL list along with the classification information at the system startup stage. This feature is useful if your Internet connect is slow and you experience high latency while accessing the Web due to the remote categorization service.

  Because the Web-filter policy decision is based on the URL category information that is preloaded in the cache, you do not experience a lag even when you make the first request.

  See [Enhanced Web Filtering]

- **Support for intelligent Web filtering profile selection (cSRX, SRX1500, SRX4100, SRX4200, SRX4600, SRX5400, SRX5600, SRX5800, and vSRX3.0)**—Starting in Junos OS Release 23.2R1, dynamic app information from Juniper Networks Deep Packet Inspection (JDPI) is used to retrieve policy information before the final policy match occurs. The Web filter profile is updated again after the final policy selection, based on the final application match.

  The Content Security profile that is retrieved based on the dynamic app information is more accurate than applying the default profile, which was the earlier approach.

  [See See Web Filtering]

VPNs

- **PKI support (cSRX)**—Starting in Junos OS Release 23.2R1, cSRX supports Public Key Infrastructure (PKI) to manage certificates.

  Use the `request security pki encryption-password set plain-text-password` and `show security pki encryption-key-status` commands to verify the PKI encryption status.

  [See Public Key Infrastructure (PKI) and cSRX Deployment Guide for Bare-Metal Linux Server.]

What's Changed

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

Known Limitations

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

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

Open Issues

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

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

Resolved Issues

There are no resolved issues in this release for cSRX.

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

Junos OS Release Notes for EX Series

IN THIS SECTION

What's New

IN THIS SECTION

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

To view features supported on the EX platforms, view the Feature Explorer using the following links. To see which features were added in Junos OS Release 23.2R1, click the Group by Release link. You can collapse and expand the list as needed.

- EX2300
- EX2300-VC
- EX2300 Multigigabit
- EX3400
- EX3400-VC
- EX4100
- EX4100-F
- EX4300 Multigigabit
- EX4400
- EX4400 Multigigabit
- EX4400-24X
- EX4650-48Y
- EX9200

EVPN

- **VXLAN Group-Based Policy (EX9204, EX9208, and EX9214 switches with the EX9200-15C line card).** —Starting in Junos OS Release 23.2R1, you can secure data and assets through microsegmentation. You use the existing Layer 3 (L3) VXLAN network identifiers (VNIs) and the firewall filter policies to provide microsegmentation at the device or tag level, independent of the underlying network topology. You can use VXLAN group-based policy (VXLAN-GBP), for example, to secure IoT-generated network traffic. IoT devices typically access only specific applications on the network. GBP keeps this IoT-driven traffic isolated by automatically applying security policies without the need for Layer 2 (L2) or L3 lookups, or access control lists (ACLs).

  [See Example: Micro and Macro Segmentation using Group Based Policy in a VXLAN.]

- **New VXLAN-GBP profiles and additional L4 matches for GBP policy filters (EX4100, EX4400, EX4650, and QFX5120 switches)**—Starting in Junos OS Release 23.2R1, we've added these enhancements to the group-based policy (GBP) microsegmentation feature:

  - The EX4400, EX4650, and QFX5120 switches support new VXLAN-GBP profiles:

    - `vxlan-gbp-l2-profile`

      This profile increases the capacity for MAC addresses.

    - `vxlan-gbp-l3-profile`

      This profile increases the capacity for IP addresses.

  - The EX4400, EX4100, EX4650, and QFX5120 switches support additional Layer 4 matches for a GBP policy filter for IPv4 or IPv6. You can use protocol, source ports, destination ports, TCP flags, and other matches for MAC and IP-based GBP tagged packets.

  - You can use the `set forwarding-options evpn-vxlan gbp tag-only-policy` command to allow only GBP source and destination tags as matches in the GBP policy on the EX4650 series, QFX5120-32C, and QFX5120-48Y switches.

  [See Example: Micro and Macro Segmentation using Group Based Policy in a VXLAN.]

- **Support for detecting local and global loops in EVPN fabrics (EX4400 and QFX5120)**—Starting in Junos OS Release 23.2R1, we've enhanced the duplicate MAC address detection feature to take a configured action when a duplicate MAC address is detected. Loops can occur when provider edge (PE) devices continuously forward frames back and forth to one another in the same broadcast domain.

  To detect and resolve these loops, use the following statements at the `[edit routing-instances` *`name`* `protocols evpn duplicate-mac-detection]` hierarchy level on your peer devices:

  - `action <block | shutdown>`

The `block` option blocks any packet that has the source MAC address or destination MAC address of the duplicate MAC address. The `shutdown` option shuts down the duplicate MAC address's local interface.

- `include-local-moves`. This statement tracks duplicate MAC address movements that occur on local interfaces.

To manually clear the duplicate MAC addresses, issue the `clear evpn duplicate-mac-suppression <instance name | l2-domain-id | mac-address>` command.

To manually recover the interface that was shut down, issue the `clear ethernet-switching recovery-timeout` command.

- **Symmetric Type 2 EVPN-VXLAN to EVPN-VXLAN DCI stitching (EX4650, QFX5120-32C, QFX5120-48T, QFX5120-48Y, QFX5120-48YM, and QFX10002)**—Starting in Junos OS Release 23.2R1, we support Ethernet VPN–Virtual Extensible LAN (EVPN-VXLAN) to EVPN-VXLAN symmetric Type 2 route stitching between data center networks using Data Center Interconnect (DCI). Your network can more efficiently interoperate with data center networks that include devices from other vendors who support symmetric Type 2 route stitching. Symmetric Type 2 route stitching means that the VXLAN tunnel endpoint (VTEP) interfaces perform routing and bridging on both the ingress and egress sides of the VXLAN tunnel.

  [See Symmetric Integrated Routing and Bridging with EVPN Type 2 Routes in EVPN-VXLAN Fabrics.]

- **GBP tag propagation with EVPN-VXLAN to EVPN-VXLAN stitching (EX4650, QFX5120-32C, QFX5120-48T, QFX5120-48Y, QFX5120-48YM, and QFX10002)**—Starting in Junos OS Release 23.2R1, we support group-based policy (GBP) tag propagation for EVPN Type 2 and Type 5 routes in a stitched EVPN-VXLAN data center environment. GBP uses existing Layer 3 VXLAN network identifiers (VNIs) in conjunction with firewall filter policies to provide microsegmentation at the device or tag level, independent of the underlying network topology.

  [See Example: Micro and Macro Segmentation using Group Based Policy in a VXLAN.]

- **Hard interface shutdown when a device detects EVPN core isolation conditions (EX4100-24MP, EX4400-24MP, MX304, MX10003, QFX5120-32C, QFX5120-48T, QFX5120-48Y, and QFX5120-48YM)**—Starting in Junos OS Release 23.2R1, you can configure a device to bring associated interfaces down (hard shutdown) when the device detects an EVPN core isolation event. In the CLI:

  1. Define a service tracking profile for detecting core isolation conditions.
  2. Set the `link-down` service tracking action in the profile.
  3. Assign the profile to the interfaces you want the device to bring down after it detects a core isolation condition.

  We support core isolation service tracking on:

- Links to single-homed customer edge (CE) devices.
- Ethernet segment identifier (ESI) LAG member interfaces to multihomed CE devices.

[See network-isolation and network-isolation-profile.]

- **Simplified configuration for ESI LAGs with EVPN dual-homing (EX4100-48MP, EX4100-24MP, EX4100-48P, EX4100-48T, EX4100-24P, EX4100-24T, EX4100-F-48P, EX4100-F-24P, EX4100-F-48T, EX4100-F-24T, EX4100-F-12P, EX4100-F-12T, EX4300-MP, EX4400-24MP, EX4400-24P, EX4400-24T, EX4400-24X, 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 23.2R1, we support a new CLI statement hierarchy level, `[edit services evpn]`. Using statements at this hierarchy level, you can specify the device attributes and other parameters to configure an Ethernet segment in an EVPN fabric. This new configuration simplifies setting up EVPN fabrics with Ethernet segment identifier (ESI) link aggregation groups (LAGs) for dual-homing peer provider edge (PE) devices.

  When you commit a configuration at this hierarchy level, the device automatically invokes commit scripts to create a corresponding configuration on the device. You must specify some mandatory elements. You can also include optional elements. For optional elements that you don't specify, the automatic configuration scripts derive the optional elements (or the scripts use default parameters).

  The resulting automatic configuration includes the applicable configuration stanzas corresponding to the different elements you specify at the `[edit services evpn]` hierarchy level.

  The new hierarchy includes options to override some default parameters, and you can override the automatically configured settings by manually configuring the related statements.

J-Web

- **Support for EX4400-EM-1C uplink module (EX Series)**—Starting in Junos OS Release 23.2R1, J-Web supports EX4400-EM-1C uplink module (100GbE QSFP28 extension module) for EX4400 and EX4400-24X switches. This module supports Media Access Control Security (MACsec) with AES-256 bit encryption.

  [See Dashboard for EX Series Switches, Connecting and Configuring an EX Series Switch (J-Web Procedure), and Configuring a Virtual Chassis on an EX Series Switch (J-Web Procedure).]

Additional Features

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

- **Ephemeral database support for configuring MSTP, RSTP, and VSTP** (ACX Series, EX Series, and QFX Series). You can configure the following protocols in the ephemeral configuration database:
  - Multiple Spanning Tree Protocol (MSTP)

  - Rapid Spanning Tree Protocol (RSTP)
  - VLAN Spanning Tree Protocol (VSTP)

  [See Unsupported Configuration Statements in the Ephemeral Configuration Database.]

- **View supported transceivers, optical interfaces, and DAC cables**—Select your product in the Hardware Compatibility Tool (HCT) to view the supported transceivers, optical interfaces, and direct attach copper (DAC) cables for your platform or interface module. We update HCT and provide the first supported release information when the optic becomes available.

- **Support for port-based LAN broadcast traffic forwarding** (EX4100-24P, EX4300-MP, EX4400-24MP, EX4400-24P, EX4400-24T, EX4400-48F, EX4400-48MP, EX4400-48P, and EX4400-48T).

  [See Configuring Port-based LAN Broadcast Packet Forwarding.]

- **Support for firewall filter lists - input-list and output-list** (EX Series).

  [See input-list and output-list.]

- **Resilient hashing support for LAGs and ECMP groups** (EX4400-24X and EX4400-48F).

  [See Resilient Hashing on LAGs and ECMP Groups.]

- **Support for DHCP smart relay in an Ethernet VPN–Virtual Extensible LAN (EVPN-VXLAN) deployment** (EX4400-24X).

  [See DHCP Smart Relay in EVPN-VXLAN.]

- **View supported transceivers, optical interfaces, and DAC cables**(EX4400-24X). Select your product in the Hardware Compatibility Tool to view the supported transceivers, optical interfaces, and direct attach copper (DAC) cables for your platform or interface module. We update the tool and provide the first supported release information when the optic becomes available.

- **Firewall filter flexible match conditions** (EX4100-24P, EX4100-24T, EX4100-24MP, EX4100-48P, EX4100-48T, EX4400-24T, EX4400-24X, and EX4400-48F). You can construct firewall filters that start the match at Layer 2 or Layer 3 packet offsets.

  [See Firewall Filter Flexible Match Conditions.]

- **Remote port mirroring with VXLAN encapsulation** (EX4400-24T, EX4400-24X, and EX4400-48F).

  [See Port Mirroring and Analyzers (EVPN User Guide).]

- **Remote port mirroring to an IPv6 address (GRE)** (EX4100-24P, EX4100-24T, EX4100-24MP, EX4100-48P, EX4100-48T, EX4100-48MP, EX4400-24P, EX4400-24T, EX4400-24X, EX4400-24MP, EX4400-48P, EX4400-48T, EX4400-48F, and EX4400-48MP).

  [See Port Mirroring and Analyzers (Network Management and Monitoring Guide).]

- **Dynamic load balancing on ECMP and LAG** (EX4400-24T, EX4400-24X, and EX-4400-48F).

  [See Dynamic Load Balancing.]

- **Filter-based GRE decapsulation** (EX4100-24P, EX4100-24T, EX4100-24MP, EX4100-48P, EX4100-48T, EX4100-48MP, EX4400-24P, EX4400-24T, EX4400-24X, EX4400-24MP, EX4400-48P, EX4400-48F, and EX4400-48MP).

  [See Configuring a Firewall Filter to De-Encapsulate GRE Traffic.]

What's Changed

IN THIS SECTION

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

General Routing

- The connectivity fault management process (cfmd) runs only when the ethernet connectivity-fault-management protocol is configured.
- Prior to this change the output of a `show task replication | display xml validate` command returned an error of the form `ERROR: Duplicate data element <task-protocol-replication-name>`. With this change the XML output is properly structured with no validation errors.
- **Label for the hours unit of time displayed in output**—When there are zero minutes in the output for the `show system uptime` command, the label for the hours unit of time is displayed.

  [See show system uptime.]

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

- **Changes to Aggregate Level Policer at FPC (EX9208)**—The summation of newly added sub-policers HELLO and UNCLS for DDOS protocols OSPF, OSPFv3, and RSVP result in the correct reporting of counters at the FPC level, for e.g. packet drops. Earlier, you could configure the OSPF, OSPFv3, and RSVP aggregate policer at the FPC level directly.

  You can use the following CLI statements to configure the burst and bandwidth values for OSPF, OSPFv3, and RSVP:

  - `set system ddos-protection protocols ospf ospf-hello burst size bandwidth packets-per-second`
  - set system ddos-protection protocols ospf ospf-uncls burst 10000 bandwidth 10000
  - set system ddos-protection protocols ospfv3v6 ospfv3v6-hello burst 10000 bandwidth 10000
  - set system ddos-protection protocols ospfv3v6 ospfv3v6-uncls burst 10000 bandwidth 10000
  - set system ddos-protection protocols rsvp rsvp-hello burst 10000 bandwidth 10000
  - set system ddos-protection protocols rsvp rsvp-uncls burst 10000 bandwidth 10000

  [See Protocols (DDOS).]

- **The active-user-count is defined as a numeric integer value in ODL request output**—The output for the get-system-uptime-information ODL request contains information for the active-user-count. The active-user-count is now defined as a numeric integer value and avoids an invalid value type error.

  [See show system uptime.]

- The packet rate and byte rate fields for LSP sensors on AFT (with the legacy path) have been renamed as jnx-packet-rate and jnx-byte-rate and is in parity with the UKERN behavior. Previously, these rate fields were named as packetRate and byteRate.

Junos XML API and Scripting

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

  [See file (JET).]

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

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

Network Management and Monitoring

- **Changes to the `show system yang package` (`get-system-yang-packages` RPC) XML output (ACX Series, EX Series, MX Series, QFX Series, SRX Series, vMX, and vSRX)**—The `show system yang package` command and `<get-system-yang-packages>` RPC include the following changes to the XML output:
  - The root element is `yang-package-information` instead of `yang-pkgs-info`.
  - A `yang-package` element encloses each set of package files.
  - The `yang-pkg-id` tag is renamed to `package-id`.
  - If the package does not contain translation scripts, the Translation Script(s) (`trans-scripts`) value is `none`.
- **NETCONF server's `<rpc-error>` response changed when `<load-configuration>` uses `operation="delete"` to delete a nonexistent configuration object (ACX Series, EX Series, MX Series, QFX Series, SRX Series, vMX, and vSRX)**—In an earlier release, we changed the NETCONF server's `<rpc-error>` response for when an `<edit-config>` or `<load-configuration>` operation uses `operation="delete"` to delete a configuration element that is absent in the target configuration. We've reverted the changes to the `<load-configuration>` response.
- **Changes to the RPC response for `<validate>` operations in RFC-compliant NETCONF sessions (ACX Series, EX Series, MX Series, QFX Series, SRX Series, vMX, and vSRX)**—When you configure the `rfc-compliant` statement at the `[edit system services netconf]` hierarchy level, the NETCONF server emits only an `<ok/>` or `<rpc-error>` element in response to `<validate>` operations. In earlier releases, the RPC reply also includes the `<commit-results>` element.

Known Limitations

IN THIS SECTION

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

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

Virtual Chassis

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

Open Issues

IN THIS SECTION

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

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

Network Management and Monitoring

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

Platform and Infrastructure

- In a rare scenario, due to timing issues, the Packet Forwarding Engine (PFE) crash is observed on Junos EX4300 platforms. This causes traffic loss until the PFE comes up. PR1720219

- On Junos EX4300-24T/24P when the native CVLAN (Customer Virtual Local Area Network) ID is configured for Q-in-Q setup, the traffic for that particular VLAN gets dropped even if the knob "input-native-vlan-push" is configured. This issue is encountered when the when inner-tag matches 'native-vlan-id' irrespective of the outer tag. PR1722284
- runt, fragment and jabber counters are not incrementing on EX4300-MPs. PR1492605
- On EX2300, EX3400,:EX4300-48MP and EX4300 devices, the pause frames counters does not get incremented when pause frames are sent. PR1580560
- When the remote end server/system reboots, QFX5100 platform ports with SFP-T 1G inserted may go into a hung state and remain in that state even after the reboot is complete. This may affect traffic after the remote end system comes online and resumes traffic transmission. PR1665800
- On the EX4600 device with SFP-LX10/SFP-SX, after a power cycle/software reboot, all ports are initialized and links are up with auto-negotiation enabled. Few ports are up and traffic flows whereas few ports are up but no traffic flow through them. PR1672583
- When the beacon LED for a port is configured as OFF, output of 'shot chassis led' incorrectly shows it as GREEN instead of OFF. When the beacon LED for a port is configured as ON, output of 'shot chassis led' incorrectly shows it as GREEN instead of 'GREEN Blinking'. Physical LED behavior reflects correctly as per beacon configuration. PR1697678
- EX4600 with Redundant Trunk Group (RTG) configured, after VCP port between members of EX4600 disconnect and connect again. Mac address entry created in RTG cannot ageout. PR1707878
- When high number of MACsec sessions present (more than 200) and traffic is passed over these interface, some of the MACsec session flap and there is traffic drop. PR1709431

Virtual Chassis

- On Junos EX4600 Virtual Chassis (VC), the primary Routing Engine reboot and all-members reboot lead to the PFE Manager hogging logs when SFP-T pluggable is installed in. The PFE Manager hogging logs has no functionality impact. PR1685067
- On EX4600-VC, when the `request system reboot all members` command gets executed, post-reboot one of the VC member/Flexible PIC Concentrator(FPC) might disconnect and join the VC back due to Packet Forwarding Engine (PFE) restart. Traffic loss is seen when FPC is disconnected. PR1700133

Resolved Issues

IN THIS SECTION

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

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

Forwarding and Sampling

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

Infrastructure

- Routing Engine fails to boot when booted directly from Junos volume. PR1701451

Layer 2 Ethernet Services

- DHCP packets might not be sent to the clients when 'forward-only' is reconfigured under the routing instance. PR1689005

Platform and Infrastructure

- The interface on the device will go down when one or more interfaces are connected to the Advantech3260 device at another end. PR1678506
- The DHCP offer packet failed to send back to the client leaf from the server leaf. PR1698833
- On EX4300-48MP I/O accesses to disk fails. PR1720335
- EX4100 MACsec interface statistics of encrypted/decrypted bytes do not increment further after reaching a 40-bit limit. PR1658584
- EX4100 and EX4100-F Virtual chassis: Non-existing PIC ports are seen in jvision queries. PR1681673
- fxpc daemon core is observed on Junos EX4400 platforms in a Virtual chassis setup with HGoE mode. PR1682960
- The mib walk with jnxOperatingDescr.1.1.0.0 returns blank, but jnxOperatingState.1.1.0.0 returns value. PR1683753
- EX4100 and EX4100-F series: On configuring console "logout-on-disconnect", password configuration via console does not work. PR1686364
- Traffic loss is observed in IP fabric when there is a change in the underlay network. PR1688323
- DHCP binding fails after dot1x authentication in EVPN-VXLAN network. PR1693967
- The l2cpd telemetry crash would be observed when the LLDP Netconf notification from external controllers along with Netconf services configuration is present on the device. PR1695057
- Traffic loss is seen when a MAC moves from dot1x port to non-dot1x port. PR1695771
- Traffic forwarding fails when deleting all L2 related configurations. PR1695847
- Adding more than 256 VLANs as name tags on the same interface results in dcd crash. PR1696428
- Transceiver not detected after it's unplugged and plugged in again. PR1696444
- Traffic loss can be seen while switching between primary and fallback sessions in MACsec setup. PR1698687
- Traffic impact is observed when OSPF adjacency formation is taking longer time. PR1699216
- Adaptive sampling will not work if the system clock is turned backward. PR1699585
- DHCP offer requests are dropped while routed towards different VRFs of transit router. PR1700203

- EX4400: pps counter does not show correct values for jubmo frames. PR1700309
- EX4400-24X ::In 4x25G uplink module, LED is ON when 1G link status is down. PR1700483
- EX4300-48MP: :Interface operational states shows up even when interface as made down administratively. PR1701444
- The BFD session will remain in init/down state in the Virtual Chassis scenario. PR1701546
- The PXE BIOS recovery fails on EX9204/9208/9214 VC setup. PR1704457
- PoE does not work as expected. PR1705212
- Traffic blackhole in the event of a link failure (Rx LOS) for 1GE-SX/LX optics. PR1705461
- EAP authentication might not be successful with 802.1X server-fail configuration. PR1705490
- Alarms were not generated as expected when the Management Interface Link was down. PR1706116
- Layer 3 forwarding issues for IRB. PR1706845
- The PoE firmware upgrade fails on EX4400 platforms. PR1706952
- In a VC scenario, sometimes the alarms raised on the line-card or backup-Routing Engine might not show on the primary Rouitng Engine. PR1707798
- QSFPs are displayed as UKNOWN after the upgrade. PR1708123
- License expire error will be observed after upgrade. PR1708794
- Certain EX platforms with option-18 configured may hinder the DHCPv6 process. PR1710360
- The link does not come up after PIC offline and online operation. PR1710793
- When a 100G transceiver is used as a VC port or network port, the VC port or network port will either not come up or come up as 40G. PR1711407
- A dot1xd crash is seen on Junos EX2300 platforms. PR1711422
- MACsec dynamic CAK not working due to interoperability issue. PR1711561
- The multiple supplicant scenario for dot1x does not work with MAC based tagging in case of Group Based Policies. PR1713982
- On EX4650, jnxOperatingDescr.1.1.0.0 is populated with blank. PR1714056
- EX4400 Link/Activity LED is not lit when it transits to the factory default configuration by pressing the Factory Reset/Mode button. PR1714116

- On EX4400 and EX4400-24X platforms, BIOS upgrade is not getting successful via CLI. PR1715258
- Traffic loss is seen on RTG bound interface. PR1715518
- The interface phy of PIC 0 comes up causing traffic loss while the device boots/reboots. PR1715680
- EX4100MP (PSE) does not allocate a power value requested in LLDP by the PD. PR1716261
- mac-move-limit : MMAS flag not getting reset after interface recovers due to l2-learning restart. PR1716270
- The link remains down on connecting the transceiver 10GBASE-T with the serial number starting with "2P1". PR1716703
- DHCP services are impacted as DHCP binding will not work as expected. PR1718286
- The fxpc daemon core is observed on Junos EX4400 platforms in a Virtual chassis setup with HGoE mode. PR1718316
- [EX4400]Alarm PEM is not supported/powered might be seen. PR1718825
- There is a missing default config of RSTP which is missing when zeroriez is done. PR1719509
- EX4400: Flow control shows as disabled at pfe, even after enabling it. PR1724188
- On certain Junos EX and QFX platforms the static ARP entries for DHCP-security are not present. PR1724933
- EAP dot1x authentication stuck in connecting state. PR1728538
- EX4400 VC: During upgrade/reboot , fxpc core may be seen in a very rare race condition. PR1728725
- EX4400: Some log messages may get flooded in heavily loaded system. PR1731345
- The traffic drop will be observed after changing the VSTP VLAN configuration. PR1731522
- The fxpc process crashes when the next hop information is not properly maintained in the PFE table. PR1731548
- On EX4400 device, syslog 'dot1xbd_get failed' are captured during MAC-Move in a heavily loaded device. PR1733365
- 25G DAC VCP ports don't come up in HGOE mode with 22.3R2-S1.7 Image. PR1738535

Routing Protocols

- A crash can be observed for 'mcsnoopd' process when the VLAN name for igmp-snooping has certain characters. PR1711153

Subscriber Access Management

- Intermittent authd crash will be seen on Junos platforms in a DHCP subscriber scenario. PR1697447

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.

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 sixty months after the first general availability date and customer support for an additional six more months.

> **NOTE**: The sixty months of support for EEOL releases is introduced in Junos OS 23.2 release and is available for all later releases. For releases prior to 23.2, the support for EEOL releases continues to be thirty six 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 21.2 to the next three releases – 21.3, 21.4 and 22.1 or downgrade to the previous three releases – 21.1, 20.4 and 20.3.

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, 21.2 is an EEOL release. Hence, you can upgrade from 21.2 to the next two EEOL releases – 21.4 and 22.2 or downgrade to the previous two EEOL releases – 20.4 and 20.2.

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)	60 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

What's New

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

What's Changed

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

Known Limitations

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

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

Open Issues

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

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

Resolved Issues

There are no resolved issues in this release for JRR Series Route Reflectors.

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

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 sixty months after the first general availability date and customer support for an additional six more months.

> **NOTE**: The sixty months of support for EEOL releases is introduced in Junos OS 23.2 release and is available for all later releases. For releases prior to 23.2, the support for EEOL releases continues to be thirty six 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 21.2 to the next three releases – 21.3, 21.4 and 22.1 or downgrade to the previous three releases – 21.1, 20.4 and 20.3.

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, 21.2 is an EEOL release. Hence, you can upgrade from 21.2 to the next two EEOL releases – 21.4 and 22.2 or downgrade to the previous two EEOL releases – 20.4 and 20.2.

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)	60 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

What's New

There are no new features or enhancements to existing features in this release for Juniper Secure Connect.

What's Changed

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

Known Limitations

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

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

Open Issues

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

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

Resolved Issues

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

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

Junos OS Release Notes for MX Series

IN THIS SECTION

What's New

IN THIS SECTION

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

To view features supported on the MX platforms, view the Feature Explorer using the following links. To see which features were added in Junos OS Release 23.2R1, click the Group by Release link. You can collapse and expand the list as needed.

- MX150
- MX204
- MX240
- MX304
- MX480
- MX960
- MX2008
- MX2010
- MX2020
- MX10003
- MX10008
- MX10016
- vMX

EVPN

- **EVPN-VXLAN to EVPN-VXLAN seamless stitching for EVPN Type 5 routes (MX480)**—Starting in Junos OS Release 23.2R1, you can configure Ethernet VPN–Virtual Extensible LAN (EVPN-VXLAN) to EVPN-VXLAN seamless stitching for EVPN Type 5 routes between two interconnected data centers or between two points of delivery (pods) in a data center.

- **Hard interface shutdown when a device detects EVPN core isolation conditions (EX4100-24MP, EX4400-24MP, MX304, MX10003, QFX5120-32C, QFX5120-48T, QFX5120-48Y, and QFX5120-48YM)**—Starting in Junos OS Release 23.2R1, you can configure a device to bring associated interfaces down (hard shutdown) when the device detects an EVPN core isolation event. In the CLI:

  1. Define a service tracking profile for detecting core isolation conditions.
  2. Set the `link-down` service tracking action in the profile.
  3. Assign the profile to the interfaces you want the device to bring down after it detects a core isolation condition.

  We support core isolation service tracking on:

  - Links to single-homed customer edge (CE) devices.
  - Ethernet segment identifier (ESI) LAG member interfaces to multihomed CE devices.

  [See network-isolation and network-isolation-profile.]

Interfaces

- **Layer 2 dynamic overhead adjustment for accounting (MX Series)**—Starting in Junos OS Release 23.2R1, you can improve network monitoring and analysis with Layer 2 dynamic overhead accounting for YT and ZT-based cards. This enhancement addresses the previous default behavior of not accounting for Layer 2 overhead in input and output statistics of physical and logical interfaces. You can now configure subscriber statistics to include the Layer 2 overhead size, which includes header and trailer bytes for both ingress and egress interfaces. This improvement ensures accurate tracking of Layer 2 overhead in input and output statistics.

  [See account-layer2-overhead (PIC Level)]

Junos Telemetry Interface

- **Health monitor sensors and counters (ACX710, ACX5448, MX240, MX480, MX960, MX2008, MX2010, MX2020, MX10004, MX10008, and MX10016)**—Starting in Junos OS Release 23.2R1, we support additional health monitor sensors for the following health parameters:

  - Memory

- License
- Clock
- System state
- SSH server
- Telnet server
- Logging
- Network Time Protocol (NTP)
- DNS
- Authentication, authorization, and accounting (AAA)

[See Junos YANG Data Model Explorer.]

- **IS-IS configuration using OpenConfig (MX204, MX240, MX304, MX150, MX480, MX960, MX10003, MX10004, MX10008, MX10016, MX2008, MX2010, MX2020, and vMX)**—Junos OS Release 23.2R1 introduces support for new configuration paths based on OpenConfig data model **openconfig-isis.yang** version 1.0.0.

  See Mapping OpenConfig ISIS Commands to Junos Configuration.

- **On-box aggregation support (MX150, MX204, MX240, MX304, MX480, MX960, MX2008, MX2010, MX2020, MX10003, MX10004, MX10008, MX10016, and vMX)**—Starting in Junos OS Release 23.2R1, we support onbox aggregation of interface, CoS, MPLS, and aggregated Ethernet counters. Off-box aggregation has limited insight into systemic events, such as line card resets or LAG membership changes. On-box aggregation support aggregates the counters at the source and generates a telemetry stream of aggregated PFE statistics and telemetry data. With this data you can reduce production errors at the collector.

  We support these sensors with on-box aggregation:

  - **/junos/system/linecard/interface/traffic/**
  - **/junos/system/linecard/interface/queue/**
  - **/junos/system/linecard/interface/logical/usage/**
  - **/junos/system/linecard/cos/interface/interface-set/output/queue/**
  - **/junos/services/label-switched-path/usage/**
  - **/qos/interfaces/interface/output/queues/queue/state/**
  - **/interfaces/interface/state/counters/**

- **/interfaces/interface/subinterfaces/subinterface/state/counters/**
- **/interfaces/interface/subinterfaces/subinterface/ipv4/state/counters/**
- **/interfaces/interface/subinterfaces/subinterface/ipv6/state/counters/**
- **/network-instances/network-instance/mpls/lsps/constrained-path/tunnels/tunnel/state/counters/**
- **/junos/system/linecard/interface/queue/**
- **/junos/system/linecard/qmon-sw/**
- **/qos/interfaces/interface/output/queues/queue/state/**
- **/qos/interfaces/interface/input/virtual-output-queues/voq-interface/queues/queue/state/**

See Junos YANG Data Model Explorer for OpenConfig sensors and Guidelines for gRPC and gNMI Sensors (Junos Telemetry Interface) for native sensors.

- **Support for OpenConfig multicast data model (ACX5448, ACX710, EX2300, EX2300-MP, EX2300-C, EX2300-VC, EX3400, EX3400-VC, EX4100, EX4100-MP, EX4300-MP, EX4300-VC, EX4400-MP, EX4400, EX4650, EX4650-VC, EX9214, MX204, MX240, MX304, MX150, MX480, MX960, MX2008, MX2010, MX2020, MX10003, MX10004, MX10008, MX10016, vMX, QFX10002-60C, QFX5110, QFX5110-VC, QFX5110-VCF, QFX5120, QFX5120-VC, QFX5200, QFX5210, QFX5500, QFX10002, QFX10008, and QFX10016)**—Junos OS Release 23.2R1 introduces support for OpenConfig multicast data models **openconfig-pim.yang** (version 0.4.2) and **openconfig-igmp.yang** (version 0.3.0). This feature includes telemetry streaming of operational state data and configuration using OpenConfig.

  See Junos YANG Data Model Explorer for state sensors and Mapping OpenConfig Multicast Commands to Junos Configuration for configuration.

- **QoS telemetry on virtual interfaces (MX204, MX480, MX960, MX10004, MX10008, MX10016, MX2010, and MX2020)**—Junos OS Release 23.2R1 extends support for streaming statistics for quality-of-service (QoS) queues to the following virtual interface types: pseudowire, GRE, LT, inline service, and link services intelligent queuing interface (LSQ). You can stream QoS queue statistics using OpenConfig or native Junos operational state sensors.

  [For OpenConfig sensors, see Junos YANG Data Model Explorer. For native Junos sensors, see Guidelines for gRPC and gNMI Sensors (Junos Telemetry Interface).]

- **Support for configuring the routing-instance and source address for each gRPC tunnel session (MX204, MX240, MX480, MX960, MX10003, MX10004, MX10008, MX10016, MX2008, MX2010, MX2020, VMX, and QFX5110)**—Starting with Junos OS Release 23.2R1, you can configure the routing instance and the source address for each gRPC remote procedure call (gRPC) tunnel session to dial out a connection to the tunnel server.

To configure the routing instance, add the `routing-instance <routing-instance>` option and to configure the source address, add the `source-address <ip-address>` option in the `grpc-tunnel` configuration statement.

If you do not configure a routing instance, the gRPC tunnel uses the default routing instance. If you do not configure the source address, the kernel picks the source address that can reach the tunnel server.

[See gRPC Tunnels Overview and grpc-tunnel].

- **Support for FEC monitoring sensors and counters (MX204, MX240, MX480, MX960, MX2010, MX10008, and MX2020)**—Starting in Junos OS Release 23.2R1, we support forward error correction (FEC) monitoring sensors and counters on Ethernet interfaces. You can stream Ethernet FEC mode and see other FEC counters: codeword size, codeword rate, bit errors, corrected words, and uncorrected words.

  [See Junos YANG Data Model Explorer.]

- **Routing Engine and chassis statistics sensors in GNFs (MX240, MX480, MX960, MX2008, MX2010, and MX2020)**—Starting in Junos OS Release 23.2R1, Junos telemetry interface (JTI) expands the sensor support for guest network functions (GNFs) to collect Routing Engine and chassis statistics. JTI already supports CPU sensors and line-card sensors (with some limitations) in GNFs. When the sensors cannot export statistics from a GNF, they export them from the base system (BSYS).

  When node sliced, the MX Series router functions as the BSYS. Node slicing creates additional VMs that function as GNFs. The BSYS owns all the hardware components such as chassis, linecards, and switch fabric. GNFs own and implement logical functions and maintain related states.

  Because of this distribution of ownership of hardware components and functions between BSYS and GNFs, the GNFs do not have access to all the information that is available to a standalone router or the BSYS on a node-sliced router. JTI can export complete statistical information from a node-sliced router only if you subscribe to the BSYS and the GNF with the required sensor path.GNFs do not have access to all information that is available to a standalone router or BSYS on a node-sliced router. In order to export complete statistical information from a node-sliced router using JTI, one has to subscribe to both the BSYS and the GNF with the required sensor path.

  [See Junos YANG Data Model Explorer.]

- **Telemetry streaming for IS-IS protocol based on OpenConfig data model (MX204, MX240, MX304, MX150, MX480, MX960, MX10003, MX10004, MX10008, MX10016, MX2008, MX2010, MX2020, and vMX)**—Starting in Junos OS Release 23.2R1, the data model for IS-IS is compliant with OpenConfig. The node type for **/network-instances/network-instance/protocols/protocol/** is defined as a list which contains user-configurable keys for the protocol name and identifier.

  [See Junos YANG Data Model Explorer.]

- **Telemetry streaming for static and local aggregate routes based on OpenConfig (MX10008)**—Starting in Junos OS Release 23.2R1, the data model for static and local aggregate routes is compliant with OpenConfig. The node type for **/network-instances/network-instance/protocols/protocol/** is defined as a list which contains user-configurable keys for the protocol name and identifier.

  [See Junos YANG Data Model Explorer.]

- **Upgrade of OpenConfig BGP models (MX480 and vRR)**—Junos OS Release 23.2R1 supports an upgrade for the following OpenConfig BGP models to version 9.1.0:

  - **openconfig-bgp-global.yang**
  - **openconfig-bgp-neighbor.yang**
  - **openconfig-bgp-peer-group.yang**

  The upgraded models introduce new leaves for operational state sensors and configuration.

  See Junos YANG Data Model Explorer for state sensors and Mapping OpenConfig BGP Commands to Junos Configuration for configuration.

- **Upgrade of OpenConfig BGP RIB models (ACX5448, ACX710, MX204, MX240, MX150, MX480, MX960, MX10003, MX10004, MX10008, MX10016, MX2008, MX2010, MX2020, vRR)**—Junos OS Release 23.2R1 supports operational state sensors based on the latest OpenConfig BGP RIB data models:

  - **openconfig-rib-bgp-attributes.yang (version 0.8.1)**
  - **openconfig-rib-bgp-ext.yang (version 0.6.0)**
  - **openconfig-rib-bgp-shared-attributes.yang (version 0.8.1)**
  - **openconfig-rib-bgp-table-attributes.yang (version 0.8.1)**
  - **openconfig-rib-bgp-tables.yang (version 0.8.1)**
  - **openconfig-rib-bgp-types.yang (version 0.5.0)**
  - **openconfig-rib-bgp.yang (version 0.8.1)**

  The following model versions are no longer supported:

  - **openconfig-rib-bgp-ext.yang (version 0.2.0)**
  - **openconfig-rib-bgp-types.yang (version 0.2.0)**
  - **openconfig-rib-bgp.yang (version 0.2.0)**

  See Junos YANG Data Model Explorer.

Network Address Translation (NAT)

- **Aggregated multiservices support for load balancing (MX Series)**—Starting in Junos OS Release 23.2R1, in Deterministic NAT (DetNat), we support load balancing using the new CLI option `modulo-key` in the `set interfaces ams0 unit 1 load-balancing-options` command.

  The `modulo-key` option now supports only with DetNat.

  [See Configuring Load Balancing on AMS Infrastructure.]

Network Management and Monitoring

- **Support for ephemeral database cyclic versioning and resizing (MX240, MX480, MX960, MX2010, MX2020, MX10004, MX10008, MX10016, and vMX)**—Starting in Junos OS Release 23.2R1, Junos devices implement cyclic versioning and database resizing to more effectively manage the space used by the ephemeral configuration database. The cyclic version value defines the number of versions of an ephemeral database for which the system stores deleted configuration objects. During a commit operation, the system reclaims the space occupied by objects deleted in the previous database version relative to the current database version as determined by the cyclic version value. You can also configure the device to resize the database when its size exceeds certain thresholds. With effective space management, you can prevent the database from hitting the maximum database size and improve performance by reducing database fragmentation.

  [See Managing Ephemeral Configuration Database Space.]

Precision Time Protocol (PTP)

- **Support for PTP G.8275.1 profile Building Integrated Timing Supply (BITS) as a frequency source in hybrid mode (MX10004 and MX10008 for MX10K-LC480 and SFB or SFB2)** – You can configure Building Integrated Timing Supply (BITS) as a frequency source with the G.8275.1 profile in PTP hybrid mode. G.8275.1 also supports PTPoE over LAG with BITS as a frequency source on MX10004 and MX10008 with the MX10000-LC9600 line card. Based on the clock selection, the device chooses BITS as the frequency source in the hybrid mode.The BITS frequency input support includes 2048KHz (E1 unframed), E1, and T1 frequencies, in compliance with T-BC performance standards for Class B on MX10K-LC480 line card.

- **Support for PTP Transparent clock on MPC7E and MPC10E line cards on SCBE3 routing control board**—Starting in Junos OS Release 23.2R1, you can enable or disable the PTP transport clock support on MPC7E and MPC10E line cards with Enhanced Switch Control Board (SCBE3) control board on MX240, MX480 and MX960 chassis.

  See https://www.juniper.net/documentation/us/en/software/junos/time-mgmt/topics/topic-map/clock-synchronization.html

Routing Policy and Firewall Filters

- **Improved DDoS protection protocol prioritization (MX104, MX204, MX240, MX304, MX480, MX960, MX2008, MX2010, MX2020, MX10003, MX10004, MX10008, and MX10016)**—In releases before Junos OS Release 23.2R1, the type of line card in the device drives the distributed denial of service (DDoS) priority of incoming protocols. Starting in Junos OS Release 23.2R1, the device determines the DDoS priority of a protocol based on the DDoS parameters table. This enhancement enables the device to treat all packets of a particular protocol the same by default, regardless of the device's line card. You can modify the DDoS parameters table using CLI. This feature improves consistency in the way devices in the network prioritize protocols to protect against DDoS attacks.

  [See Control Plane Distributed Denial-of-Service (DDoS) Protection Overview and protocols (DDoS).]

- **Improved DDoS protocol classification for ARP request and reply traffic (MX Series)**—Starting in Junos OS Release 23.2R1, you can configure separate DDoS protocol packet-types, `bcast` and `ucast`, at the [`edit system ddos-protection protocols arp`] hierarchy level for ARP request and reply traffic. The separate DDoS policers provide an improved packet rate limiting and priority handling for the ARP traffic. Prior to this release, the ARP request and reply traffic had a single DDoS protocol.

  [See protocols (DDoS) and show ddos-protection protocols.]

Routing Protocols

- **Enhancements to show ospf spring and ospf database commands (MX240, MX480, MX960, MX2010, MX2020, and vMX)**— Starting in Junos OS Release 23.2R1, we have enhanced the `show ospf spring` and `show ospf database` commands to display the following additional segment-routing information:

  - `show ospf spring sid-database`—Displays the segment identifier (SID) database with prefix and index of native segment routing nodes.
  - `show ospf spring prefix-sid-map`—Displays segment routing mapping server (SRMS) advertisements
  - `show ospf database opaque-area ext-link link-addr` *`link-address`*—Displays the specific extended-link link-state advertisements (LSAs) based on the link-address.
  - `show ospf database opaque-area ext-prefix prefix` *`prefix/len`*—Displays the specific extended-prefix link-state advertisement based on the prefix

  [See show ospf database, show-ospf-spring-sid-database], show-ospf-spring-prefix-sid-map.

- **Support to activate BFD strict mode for BGP peer sessions (ACX5448, ACX710, cRPD, MX10003, MX10004, VRR, QFX5110, and QFX5200)**—Starting in Junos OS Release 23.2R1, we support the activation of BFD strict mode for BGP peer sessions that disallows BGP to establish a session until BFD session is successfully established and has stabilized. With the BFD strict mode feature, you can prevent routing churn and minimize network interruption.

To activate BFD strict mode for BGP peer sessions, include the `strict-mode [bfd-wait-timeout <10-255 seconds>` CLI statement under `bfd-liveness-detection` at the `[edit protocols bgp group` *`group-name`* `neighbor` *`address`*] hierarchy level.

For example, use the following command to activate BFD strict mode for BGP peer sessions:

`set protocol bgp group` *`group-name`* `neighbor` *`address`* `bfd-liveness-detection [strict-mode [bfd-wait-timeout` *`10-255 seconds`*`]]`

[See Understanding BFD for BGP, bfd-liveness-detection (BGP).]

- **Support for RFC8814 (Signaling MSD using BGP-LS) (MX Series)**—Starting in Junos OS Evolved Release 23.2R1, we partially support RFC 8814, *Signaling Maximum SID Depth (MSD) Using the Border Gateway Protocol - Link State*. Currently, we support signalling Maximum SID Depth (MSD) using IS-IS for both SR-MPLS and SRv6. For non-SR networks, this will reflect the maximum label depth.

  A controller in a segment routing network learns the MSD of the participating router and computes the SR path. The controller ensures that the label stack is not greater than what the routers can support.

  See [Link-State Distribution Using BGP.]

- **Support for AIGP for INET, INET6, L3VPN, and L3VPN6 (cRPD, and MX10008)**—Starting in Junos OS 23.2R1, we support AIGP for INET unicast, INET6 unicast, L3VPN, and L3VPN6 address family. Use the existing show route command to see the output with multiple paths.

  [See aigp.]

Software Defined Networking (SDN)

- **Support for podman-based JDM deployment**—Starting in Junos OS Release 23.2R1, the external server-based Junos node slicing supports deployment of Juniper Device Manager (JDM) using the Pod Manager tool (podman). This change is applicable to servers running Red Hat® Enterprise Linux® (RHEL) 9. In Junos releases prior to 23.2R1, Junos node slicing supported RHEL 7.3, which provided libvirt lxc driver (libvirt-lxc) to deploy JDMs.

  [See Junos Node Slicing Upgrade]

Subscriber Management and Services

- **Support for Wireless CUPS (MX10008)**—Starting in Junos OS Release 23.2R1, we support wireless Control and User Plane Separation (CUPS) features on LC480 line cards in use on MX10008 platforms. This includes GRES and Anchor Packet Forwarding Engine redundancy support for 4G and 5G use cases.

  [See Multi-Access User Plane Overview.]

- **Support for Wireless CUPS User Plane Function (MX Series)**—Starting in Junos OS Release 23.2R1, we support User Plane Function (UPF) features on MPC10 and LC9600 line cards for MX Series devices.

  [See Multi-Access User Plane Overview.]

- **Support for DHCP groups across dynamic VLANs on a physical interface (MX960 and MX10003 routers)**—Starting in Junos OS Release 23.2R1, we introduce the `interface-tag` statement. The `interface-tag` statement supports mapping auto-configured dynamic VLAN subsets to different DHCP groups. Before this release, you could only map one DHCP group on a physical interface (IFD) that is supporting dynamic VLANs.

  For example, subscribers that connect to a broadband network gateway (BNG) have different DHCP requirements than subscribers that connect to the Access Gateway Function (AGF). By grouping BNG and AGF subscribers on different VLAN ranges, you can use the `interface-tag` statement to migrate subscribers from the BNG to the AGF.

  To use the `interface-tag` statement to map a group of dynamic VLANs to a DHCP group:

  - Configure the `interface-tag` in the dynamic profile on a VLAN demux interface.
    - `set dynamic-profiles` *`profile-name`* `interfaces demux0 unit $junos-interface-unit interface-tag` *`interface-tag-name`*
  - Configure the auto-sensed VLANs on the physical interface on the physical interface. Specify the dynamic profile and the VLAN range subset. The router determines the DHCP group from the VLAN range and dynamic profile.
  - Map the dynamic profile to the associated DHCP group by specifying the same `interface-tag` name.

    DHCP Relay

    - `set forwarding-options dhcp-relay group` *`name`* `interface-tag` *`interface-tag-name`*
    - `set forwarding-options dhcp-relay dhcpv6 group` *`name`* `interface-tag` *`interface-tag-name`*

    DHCP Local Server

    - `set system services dhcp-local-server group` *`sgroup`* `interface-tag` *`interface-tag-name`*
    - `set system services dhcp-local-server dhcpv6 group` *`sgroup`* `interface-tag` *`interface-tag-name`*

  [Seefiveqi-map Configuring Group-Specific DHCP Local Server Options, Configuring Group-Specific DHCP Relay Options, and Migrate Subscribers from BNG to AGF.]

- **Support to configure QoS parameters in the 5QI table (MX204, MX240, MX480, MX960, and MX10003 routers)**—Starting in Junos OS Release 23.2R1, you can configure the Quality of Service

(QoS) attributes for a 5G QoS identifier (5QI) value in the 5QI table. The Access and Mobility Function (AMF) sends N2 messages to the Access Gateway Function containing the 5QI value. The 5QI value corresponds to Junos CoS parameters. AGF inspects the N2 and N1 messages for 5QI and QoS Flow ID (QFI) values and matches those values to parameters in the 5QI table. AGF can then update data packets with an updated differentiated services code point (DSCP) in the payload to match the derived QoS parameters.

You can set the following QoS attributes for a 5QI value in the 5QI table:

- Differentiated Services code point (DSCP) value
- DSCP value for the N3 interface
- Forwarding class
- Loss Priority

To set the QoS attributes, use the `set services agf fiveqi-map` *`identifier`* `upstream-rewrite` statement. [See , upstream-rewrite, and CoS for Subscriber Access Overview.]

- **PCEF diameter enhancements for MX480** that include:

  • Support for PFE specific filter entries for protocols like ARP, BGP, ICMP pre-installed based on requirement.

  • Support for customization of Subscription-Id-Data in CCR, sourced from RADIUS server. External Subscription ID is activated by default.

  • Support for customization of Calling-Station-Id in RADIUS requests. To customize Calling-Station-Id in RADIUS requests, use the command `set remote-circuit-id-format (postpend | prepend)` under `[edit access profile <`*`profile-name`*`> radius options]` mode.

  • Usage monitoring through 3rd Generation Partnership Project (3GPP) attribute-value pairs (AVPs) defined as Gx for subscriber services using `dynamic-profile` configuration.

  [See No Link Title and No Link Title.]

- **Subscriber management functionality on MX304**—Starting in Junos OS Release 23.2R1, we provide the following support:

  - Basic and advanced class of service (CoS) and filters (IPv4 or dual stack) support for:
    - Dynamic Virtual Local Area Networks (DVLANs) with DHCP (Dynamic Host Configuration Protocol) subscribers
    - DVLAN with Point-to-Point Protocol (PPP) subscribers
    - DVLAN and Agent Circuit Identifier (ACI) with DHCP subscribers

    - DVLAN and ACI with PPP subscribers
    - Stacked DVLAN with DHCP subscribers
    - Stacked DVLAN with PPP subscribers
    - Pseudowire DVLAN with DHCP subscribers
    - Pseudowire DVLAN with PPP subscribers
- DVLAN with L2TP Access Concentrator (LAC) (IPv4) basic and advanced CoS and filters
- DVLAN with L2TP Network Server (LNS) (IPv4 and dual stack) basic CoS and filters
- Advanced CoS and filters (IPv4 or dual stack) support for:
    - DHCP subscribers
    - PPP subscribers
- L2TP tunnels
- Subscriber services (customer solutions test scripts) processing
- Scaling and performance for the following features:
    - DHCP subscribers with authenticated dynamic VLAN
    - DHCP subscribers with authenticated dynamic S-VLAN (Service-Virtual Local Area Network)
    - LNS subscribers
    - LAC subscribers
    - CoS service
    - Firewall service

[See Features Supported on MX304.]

Additional Features

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

- **Segment routing–traffic engineering (SR-TE) colored policy RIB5 and SR-TE colored telemetry sensor support** (MX10004, MX10008, and vMX).

  [See Schema Explorer.]

- **View supported transceivers, optical interfaces, and DAC cables**—Select your product in the Hardware Compatibility Tool (HCT) to view the supported transceivers, optical interfaces, and direct

attach copper (DAC) cables for your platform or interface module. We update HCT and provide the first supported release information when the optic becomes available.

- **v4ov6 tunnel support for gateway functionality** (MX304 with MPC10, MPC11, and LC9600 line cards).

  [See Understanding Redistribution of IPv4 Routes with IPv6 Next Hop into BGPveness Detection]

- **IP liveness detection and IP session monitoring for DHCP BBE subscribers using asynchronous single-hop (UDP Port 3784) and multi-hop (UDP Port 4784) BFD** (MX Series).

  [See DHCP Liveness Detection and show bfd session]

- **Support for PTP G.8275.1 and Timing G.8275.1 over LAG interfaces** (MX304). We support the Precision Time Protocol (PTP) G.8275.1 and Timing G.8275.1 over LAG interfaces.

  [See Understanding the Time Management Administration Guide and profile-type]

- **1G CoS support** (MX304). We support 1G class-of-service (Cos) on 1G ports.

  [See Port speed on MX304 Router Overview]

- **1G firewall support** (MX304). We support firewall for an 1G interface.

  [See Port speed on MX304 Router Overview]

- **Access Gateway Function Support** (MX10008 with MX10K-LC2101 and MX10K-LC480**)**.

  [See Access Gateway Function User Guide.]

What's Changed

IN THIS SECTION

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

General Routing

- The connectivity fault management process (cfmd) runs only when the ethernet connectivity-fault-management protocol is configured.
- Prior to this change the output of a `show task replication | display xml validate` command returned an error of the form `ERROR: Duplicate data element <task-protocol-replication-name>`. With this change the XML output is properly structured with no validation errors.
- **Label for the hours unit of time displayed in output**—When there are zero minutes in the output for the `show system uptime` command, the label for the hours unit of time is displayed.

  [See show system uptime.]
- In the past inet6flow.0 was not allowed to be a primary rib in a rib-group. Starting with Release 22.3 this is now allowed.
- **The active-user-count is defined as a numeric integer value in ODL request output**—The output for the get-system-uptime-information ODL request contains information for the active-user-count. The active-user-count is now defined as a numeric integer value and avoids an invalid value type error.

  [See show system uptime.]
- The packet rate and byte rate fields for LSP sensors on AFT (with the legacy path) have been renamed as jnx-packet-rate and jnx-byte-rate and is in parity with the UKERN behavior. Previously, these rate fields were named as packetRate and byteRate.
- **Multicast debug information added in EVPN options to request system information command (MX Series and QFX Series)**—The output from CLI command `request support information evpn-vxlan` now includes additional information to help debug EVPN multicast issues.

  [See request support information.]
- **Increased maximum limit for TTP TLVs (MX Series)**—The Junos Kernel now accommodates an increased number of TTP TLVs (TNP Tunneling Protocol: type, length, and value messages) to help avoid dropped packets.

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

Junos XML API and Scripting

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

  [See file (JET).]

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

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

Network Management and Monitoring

- **Changes to the `show system yang package` (`get-system-yang-packages` RPC) XML output (ACX Series, EX Series, MX Series, QFX Series, SRX Series, vMX, and vSRX)**—The `show system yang package` command and `<get-system-yang-packages>` RPC include the following changes to the XML output:

  - The root element is `yang-package-information` instead of `yang-pkgs-info`.
  - A `yang-package` element encloses each set of package files.
  - The `yang-pkg-id` tag is renamed to `package-id`.
  - If the package does not contain translation scripts, the Translation Script(s) (`trans-scripts`) value is `none`.

- **NETCONF server's `<rpc-error>` response changed when `<load-configuration>` uses `operation="delete"` to delete a nonexistent configuration object (ACX Series, EX Series, MX Series, QFX Series, SRX Series, vMX, and vSRX)**—In an earlier release, we changed the NETCONF server's `<rpc-error>` response for when an `<edit-config>` or `<load-configuration>` operation uses `operation="delete"` to delete a configuration element that is absent in the target configuration. We've reverted the changes to the `<load-configuration>` response.

- **Changes to the RPC response for `<validate>` operations in RFC-compliant NETCONF sessions (ACX Series, EX Series, MX Series, QFX Series, SRX Series, vMX, and vSRX)**—When you configure the `rfc-compliant` statement at the `[edit system services netconf]` hierarchy level, the NETCONF server emits only an `<ok/>` or `<rpc-error>` element in response to `<validate>` operations. In earlier releases, the RPC reply also includes the `<commit-results>` element.

Known Limitations

IN THIS SECTION

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

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

General Routing

- In Junos OS Release 23.2, Juniper BNG User Planes are not supported by Juniper BNG CUPS.
- When you configure a P or PE router with inline active flow monitoring and MPLS template with tunnel-observation IPv4 or IPv6 is used, there is a chance that some EoMPLS packets might be exported using mpls-ipv4 or mpls-ipv6 template instead of mpls template. PR1713728

Infrastructure

- When upgrading from releases before Junos OS Release 21.2 to Release 21.2 and later validation and upgrade might fail. The upgrade requires using the 'no-validate' option to complete successfully. https://kb.juniper.net/TSB18251. PR1568757

MPLS

- Traceroute in MPLS OAM may fail with unreachable in ECMP case when topology has multiple ecmp paths in each transit router. This is because destination address is not available. Destination address is computed using base address + bitmap index(available for that leg).Junos currently supports 64 bitvector size.Each transit ecmp legs consumes available bitmap indexes in the echo request packet.

When all the bitmap indexes are consumed by the previous transit routers/ecmp legs, then for other ecmp legs bitmap indexes are not available hence multipath information tlv bitmap will be zero leading to unreachable issue as no destination address is available. Even RFC 8029 section 4.1 says full coverage is not possible as below, If several transit LSRs have ECMP, the ingress may attempt to compose these to exercise all possible paths. However, full coverage may not be possible. Hence this is an expected behavior.PR1699685

Open Issues

IN THIS SECTION

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

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

Infrastructure

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

Layer 2 Features

- in a H-VPLS network with VPLS hot-standby and the `routing-options forwarding-table vpls-hotstandby-convergence` command enabled on spokes, if the active hub is rebooted, 20-25 seconds loss for inter-zone traffic stream is seen. This is due to hubs in other zones connected by full-mesh ldp, starting global repair before spokes starting local repair. PR1699645

MPLS

- Tag rnh appears to be freed somewhere in the corner case, but the relevant pat node has been missed to delete from the tag patricia tree. That makes tag rnh/(pat_node->Tnh) a dangling pointer and later on, it results in a crash while accessing invalid pointer addresses in the tag rnh/Tnh structure. PR1707053
- Traceroute in MPLS OAM on SR over IPv6 may fail in ECMP case if EVO box is in topology. This is because linux kernel in EVO puts an autoflowlabel on every IPv6 packet. This flow label is transparent to daemon process, which uses a null value for it and calculates the NH details. PFE however takes the flow label into account and calculates the NH details. This difference in calculation of NH details leads to a mismatch in the path the packet takes to the destination and can cause traceroute to fail. PR1710285
- On all Junos and Junos OS Evolved platforms (For QFX5100, only in Virtual Chassis-VC setup) with RSVP (Resource Reservation Protocol) LSP (Label-Switched Paths) configured in multi vendor deployment and Juniper routers is acting as a transit/ingress routers and RESV (Reservation Request) message is received with RESVCONF object from other vendors, rpd process crash will be observed. PR1723229

Network Management and Monitoring

- In some NAPT44 and NAT64 scenarios, duplicate SESSION_CLOSE Syslog occurs. PR1614358
- YANG: After upgradation s/w version on DUT, yang package with lower revisions are available in upgraded s/w version. PR1693646

Platform and Infrastructure

- When the "deactivate services rpm" and "deactivate routing-options rpm-tracking" clis are applied together and then committed, some of the rpm tracked added routes are not deleted from the routing table. Issue cannot be seen using the following steps. 1. deactivate routing-options rpm-tracking 2. commit the configuration then all the rpm tracked routes will be deleted. If the RPM service needs to be deactivated, 3. deactivate services rpm 4. commit. PR1597190
- If a vmhost snapshot is taken on an alternate disk and there is no further vmhost software image upgrade, the expectation is that if the current vmhost image gets corrupted, the system boots with the alternate disk so the user can recover the primary disk to restore the state. However, the host root file system and the node boots with the previous vmhost software instead of the alternate disk. PR1281554
- VXLAN VNI (multicast learning) scaling on QFX5110 traffic issue is seen from VXLAN tunnel to Layer 2 interface. PR1462548
- Runt, fragment and jabber counters are not incrementing on EX4300-MPs. PR1492605
- VE and CE mesh groups are default mesh groups created for a given Routing instance. On vlan/bridge-domain add, flood tokens and routes are created for both VE and CE mesh-group/flood-group. Ideally, VE mesh-group doesn't require on a CE router where IGMP is enabled on CE interfaces. Trinity based CE boxes have unlimited capacity of tokens, so this would not be a major issue. PR1560588
- On EX2300, EX3400,:EX4300-48MP and EX4300 , Pause frames counters does not get incremented when pause frames are sent. PR1580560
- Pim Vxlan not working on TD3 chipsets enabling VxLAN flexflow after release 21.3R1. Customers Pim Vxlan or data plane VxLAN can use the version 21.3R1. PR1597276
- output of show network agent command should be null, which shows statistic per component after GRES. PR1610325
- For a topology with VSTP and VRRP configured and IPV6 traffic, if VSTP bridge priority is changed a couple of times (to trigger toggling of root bridge), it is possible that V6 traffic drop is seen on some of the streams. PR1629345
- mspmand daemon running on MS-MPC/MS-MIC cards can occasionally crash when the service card (fpc/pic) is turned offline and then online at regular intervals when the number of service-set configured is moderately high and when extensive hardware crypto operations are being performed. Exact issue is yet to be isolated. PR1641107
- Please do not enable host-path tracing when there is high volume of packets been received in the host-path. PR1645741

- If the physical link status of the ethernet link between the RE and FPC goes down, there are recovery attempts to bring up the link again. Log messages indicate the recovery attempts and the success/failure status of the attempt. However an alarm is not raised when this failure occurs. PR1664592
- In case Port is DOWN then Tx Laser need to enable via cli-pfe> prompt.PR1673892
- There will be drop of syslog packets seen for RT_FLOW: RT_FLOW_SESSION_CREATE_USF logs until this is fixed. This will not impact the functionality. PR1678453
- On QFX5100 platforms (both stand-alone and VC scenario) running Junos, occasionally during the normal operation of the device, PFE (Packet Forwarding Engine) can crash resulting in total loss of traffic. The PFE reboots itself following the crash. PR1679919
- The issue here is that we see ?MQSS(0): DRD: Error: WAN reorder ID timeout error? once per PFE during bootup of FPC. This happens because during the FPC bootup some control packet from vmhost comes before the PFE init is fully complete. Because of this the EA Asic is not able to process the packet and throwing the error. The fix involves complex changes in the bootup sequence of ASICS and will result in other major issues. The original issue has no functionality impact. It is just one error per PFE seen during the FPC reload case only. At that time the traffic is not started yet and once the system is up no other impact is seen due to the Error. Hence the issue will not be fixed. Any "WAN reorder ID timeout error" during the bootup of FPC can be safely ignored. PR1681763
- See PR Fix Info -> Root Cause for details: VxLAN Terminal End Point (VTEP Nodes) are expected to be reachable over the Data Path. If a route to the VTEP is resolved over the management interface of the switch/router, based on the current route tables, this is usually a configuration issue and may lead to further problems. PR1688296
- For leaves of data type ieeefloat32, the value will be encoded in bytes while being streamed to collector. The value contained in such leaves may not be completely accurate. PR1690598
- FIPS mode is not supported in this release for SRXSME devices. PR1697999
- When subscribing to sensor paths "/junos/system/linecard/packet/usage/", "/junos/services/label-switched-path/usage/" or other line card (PFE) sensor paths in gNMI subscription mode, packet drops may be seen in the CLI command "show network-agent statistics gnmi detail" output. The collector output may also contain missing sequence numbers. For example, the sequence number output may be 0, 3, 6, 9, 12, etc. instead of 0, 1, 2, 3, 4, etc. PR1703418
- In Chassisd, Jvision thread takes more time in streaming of jvision packets because of volume of data and number of sensors involved with this daemon. Jvision thread engaged for more time to process streaming events caused Chassisd master thread to lose receive/send keepalive messages to/from other RE, which eventually was causing automatic RE switchover in most of the cases. To avoid this, fix done for exporting small payload jvision packets (formation of which takes less time) and deferring jvision thread more in an interval, to allow chassisd master thread to process high-priority hello/keep-alive messages. This means now, more number of packets is sent in one reporting interval and with larger spread (earlier same amount of data was sent with 2 or 3 packets of higher payload size,

and 100ms of deferring time for jvision thread. This behaviour is increasing KPI-2 but lowering KPI-1 (payload size). It is not possible to back out changes done to solve keep-alive message loss issue. Hence we will have to keep Chassisd as an exception, when we measure/report KPI-2 values. Jvision in Chassisd has to give more priority/time to process keep-alive messages than sending of jvision packets. Hence delay between jvision packets are more. PR1706300

- Current stack and display is correctly set to 128 ports that is qualified on all MX10K8 line cards. PR1706376
- On the MX104 platform, the Wrong threshold-temperature is displayed. PR1713788
- fec-codeword-rate data with render type decimal64 is rendered as string in grpc python decoder.PR1717520
- With no-reduced-srh configured, MX304 removes the last SID value from the SRH. Expectation is Last SID should be retained in SRH when "no-reduced-srh" is configured. There is no impact to the traffic. Traffic flow fine, since the "SEGMENT-LIST" and "LAST ENTRY" are encoded properly in the packet. PR1721404
- In some srv6 scenarios, with no-reduced-srh configured, next header in SRH is not set and packets may be dropped as invalid hop option. PR1721429
- On the Junos QFX5200 platform, sometimes upon restarting the device the 100G link will not come up and will remain down, impacting the traffic flowing through it. PR1725116
- On Junos MX platforms, to enable Enhanced Subscriber Management feature without 'max-db-size' configuration on router >=32GB DRAM(Dynamic Random Access Memory), router needs to be rebooted only once instead of rebooting twice. PR1732216
- There is no functional impact but the previously installed JSU will show up even though it is deleted during major upgrade. This PR will fix that issue. Workaround is to remove /packages/sets/active/junos-version file. PR1732878

Routing Protocol

- Errors might be seen on ephemeral commit during ISSU.PR1679645
- BGP LU statistics does not report correct statistics when sharding is enabled. This is not specific to BGP CT feature of this RLI. PR1684238
- This issue is seen with only evo and not seen Junos. Its seen in a combination of Rsvp and ISIS. Stats is getting incremented. PR1700063

- Show route advertising-protocol bgp reporting NextHop self rather than IP in the configured policy-statement for next-hop. Behavior change observed after JUNOS upgrade from 18.4 to 20.4. #set policy-options policy-statement set-NH-MX term to-PP-All then next-hop 20.20.20.1 show route advertising-protocol bgp 10.10.10.10 test.inet.0: 5 destinations, 5 routes (5 active, 0 holddown, 0 hidden) Prefix Nexthop MED Lclpref AS path * 10.0.0.0/31 Self 65000 I The CLI output for Nexthop reported Self rather than IP address 20.20.20.1. PR1712527
- On all Junos and Junos Evolved platforms with TI-LFA (Topology-Independent Loop-Free Alternate) feature enabled, when IP address is removed from one interface and is assigned to another interface in the same commit, the rpd process crashes affecting routing control plane. PR1723172

VPNs

- Tunnel debugging configuration is not synchronized to the backup node. It needs to be configured again after RG0 failover. PR1450393
- On all Junos and Junos Evolved platforms, when OSPF inter-area is configured with segmented provider-tunnel and master undergoes MBB(make-before-break), the multicast route entry on backup router will not have the tunnel name synced with master. PR1710323

Resolved Issues

IN THIS SECTION

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

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

Application Layer Gateways (ALGs)

- The traffic will be dropped in the DS-Lite+ALG scenario. PR1715315

Authentication and Access Control

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

Class of Service (CoS)

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

- QOS scheduler map incorrect when using wildcard interface configuration: " interface unit * " starting with Junos OS Release 21. PR1734013

EVPN

- delete control-word from the configuration. PR1698059
- Traffic loss is seen when IPv6 entries are not refreshed and age out under the EVPN-VXLAN scenario. PR1699509
- ARP/ND doesn't resolve when extended-vlan-list is configured for the specific VLAN. PR1702016
- In EVPN scenario, proxy-arp on IRB interfaces do not work as expected. PR1709007
- The Anycast Gateway stretched across 2 DCs over the seamless MPLS stitching DCI does not have Anycast Gateway MAC information coming from the remote DC when VLAN and VNI ids are different. PR1712259
- A high CPU consumption of mcsnoopd process is seen under IGMP-snooping configured scenario leading to its crash. PR1713508
- Ping overlay vxlan replies Overlay-segment present even the bridge-domain has been deactivated. PR1715343
- The rpd core is seen in the long-running devices with EVPN enabled. PR1723832
- EVPN-VXLAN interconnection DCI forwarding problem observed when one of the AGW irb interfaces deactivated. PR1732414

Forwarding and Sampling

- The device is using the MAC address of the IRB interface even after configuring static MAC for a default gateway. PR1700073
- Firewall filter counters are not written to accounting file when you use the `interface-specific` command. PR1706085
- Traffic is leaking during a filter change. PR1715504

General Routing

- Observed re0:rpdagent:20852:TRACE_ERR Rtsock_ERROR_MSG Function = "rpd_rtsock_dispatch", error = 7, msg = "rttable after device reboot. PR1690105
- RPD core is seen after the switchover. PR1694773
- Continuous Deactivate/activate of security config can lead to process restart. PR1566044
- On backup Routing Engine during GRES, you may see "RPD_KRT_KERNEL_BAD_ROUTE: krt unsolic client.128.0.0.5+62000: lost ifl 0 for route" warning messages. PR1612487
- Per-Interface egress and per-sid Egress sensor stats do not take MPLS label length into account in the output octet calculations. PR1646799
- NAT session reverse traffic fails due to NAT routes getting deleted from routing instance. PR1646822
- The system does not got to shell prompt and hangs before rebooting after pressing N during PXE installation. PR1647534
- .include directives are deprecated, and support for them will be removed in a future version> warning comes for all custom services. PR1647592
- PTP Playback Engine reset error is reported sporadically with PTP FPGA Firmware version A4 7. PR1652275
- Images older than 22.2R1S2 can be installed on RE-S-X6-128G-K. This will result in system booting to Linux prompt. PR1655935
- Change in few fields of IKE_VPN_UP_ALARM_USER and IKE_VPN_DOWN_ALARM_USER syslogs of IKED. PR1657704
- The license might get out of sync between master and backup Routing Engine. PR1658869
- Not all MAC addresses are learnt for some VPLS instances. PR1664694
- BIOS version REH_P_MTR1_00.30.07. PR1675016
- MX304:: Observed spmbpfe core on RE1 when installed image on both the Routing Engines. PR1675268
- 40G-QSFP+ flapping on mx204. PR1676005
- QFX10000 series platforms generates error messages constantly and IPv6 routing is not performed when configured rpf-check and inet6 on VXLAN enabled interface and trying to resolve arp ndp. PR1677422

- On LC480 MX line-card with 1G interface PTP performance will not be good. PR1677471
- Bgp peers status is not as expected. PR1677624
- PTP servo is stuck in ACQUIRING state with high CF when configured with LAG on MX10k8 with JNP10K-LC480 Linecards. PR1679657
- maintenance-domain (MD) configuration and maintenance-association (MA configuration) under the connectivity-fault-management stanza will be ordered by the system. PR1682939
- Auto-negotiation is not getting reflected on the MPC7E-10GE line card. PR1682962
- The mib walk with jnxOperatingDescr.1.1.0.0 returns blank, but jnxOperatingState.1.1.0.0 returns value. PR1683753
- 100GE interface on JNP-MIC1 TIC module may keep flapping for 1 to 45 minutes after a specific 3rd party peer device (NRU02 from Arista/Pluribus) is booting up. PR1686012
- New CLI commands addition to support RE and Chassis power-cycle. PR1686577
- Subscribers are not able to connect to the device after the device reboot. PR1686654
- The pre-installed optional packages and JSUs will be lost after a VMHost rollback. PR1686825
- Traffic loss is seen with latest ZR-M firmware (61.23) during optics power up. PR1687583
- PFE wedge will be seen due to fast link flaps. PR1688972
- Without GRES, backup RE does not take up mastership after Plugging out Master RE (re 0). PR1690508
- Synce to PTP and SyncE to 1PPS Transient Response not meeting G.8273.2 mask. PR1692202
- On all Junos lsys systems RPD process crashes due to JET client invoking rpc handled by RPD daemon. PR1692738
- The rpd crash will be observed when there is a temporary recursion loop and routes flaps. PR1692776
- Various component level sensor path for FAN, FABRIC, FAN, POWER_SUPPLY, STORAGE, STORAGE, BOOT_LOADER, BIOS, OPERATING_SYSTEM, LINECARD, TRANSCEIVER not working. PR1694612
- The l2cpd telemetry crash would be observed when the LLDP Netconf notification from external controllers along with Netconf services configuration is present on the device. PR1695057
- The BUM packets are getting dropped on MX platforms during egress processing due to PFE mismatch. PR1695438

- The routing protocol daemon may core dump when streaming telemetry data. PR1695523
- Traffic loss is seen when a MAC moves from dot1x port to non-dot1x port. PR1695771
- rpc error when resource name exceeding 255 character. PR1695980
- [01;31m[KFPC3:NPU0[m[K" string is missing in Npu memory after jvision exports data. PR1696021
- An rpd crash is observed while creating indirect-next-hop in the BGP sharding environment with bgp.l3vpn.0 with next-shop as a color route. PR1696035
- Dynamic Tables stuck in KRT Queue. PR1696199
- Adding more than 256 VLANs as name tags on the same interface results in dcd crash. PR1696428
- Transceiver not detected after it's unplugged and plugged in again. PR1696444
- After a chassis power cycle the backup RE is in Present state and the "Loss of communication with Backup RE (Routing Engine)" alarm gets generated. PR1696816
- In the rare scenario, huge PTP Time errors are introduced and propagated to the downstream devices after the chassis reboot. PR1696957
- Time error observed on JNP10K-LC2101. PR1697167
- There was no error message when sflow collector with wrong source-address commit got failed. PR1697796
- MPC10 and MPC11 will undergo silent reboot. PR1697812
- The agentd process crash might crash in a telemetry scenario. PR1697986
- RPC "get-bgp-group-information' execution failure with WARNING and CRITICAL ERROR. PR1698030
- XQSS_CMERROR_DSTAT_INT_REG_DROP0_QDEPTH_UNDRN alarm is seen on MX2K platforms with MPC11E line cards upon aggregate interface down/flap event. PR1698135
- The mpls routing table resolving over IPv6 prefix causes traffic drop. PR1698516
- Traffic loss can be seen while switching between primary and fallback sessions in MACsec setup. PR1698687
- The kernel crash can be seen in the VPLS scenario. PR1698781
- Transit tunnels fails and remains down on all Junos based MX platform with IKE-NAT-ALG enabled. PR1699115
- The rpd core will be seen when the route monitor stream times out. PR1699356

- DHCP offer requests are dropped while routed towards different VRFs of transit router. PR1700203
- EX4400: pps counter does not show correct values for jubmo frames. PR1700309
- BFD priority is received as Low instead of High in AFT Cards. PR1700315
- JDI-REG:MX10008 :: core-renault-bbe-fpc0-indus.elf-crashinfo.0 core seen during teardown. PR1700909
- How to identify and report fabric link errors caused due to connector related issues. PR1700983
- JNP10K-LC9600: G.8275.1: Multiple GRES operation resulting in huge time error. PR1701017
- CMIS Google CX : CMIS Google CX : Telemetry : subscription to path /components/component[name='Routing Engine0:bootloader']/state/location/ and /components/component[name='Routing Engine0:bootloader']/state/parent/ not working. PR1701239
- On Junos platforms with MS-MPC cards the IKE ALG inactivity timeout value stays fixed. PR1701305
- CB2 not properly offlined upon Power Zone Failure. PR1701539
- Aggregated Ethernet interface member with vlan-id-list configured not forwarding traffic. PR1701636
- Some PPPoE subscriber connection lost during RE switchover. PR1701739
- Guardian occasionally occurring link stuck down require reboot to recover after multiple fpc restarts. PR1701941
- The xmlproxyd process crash is observed in telemetry scenario. PR1702250
- License will be deleted due to multiple FPC reboot or switchover on the MX VC scenario. PR1703200
- The l2ld process will crash when an IFL is changed to trunk mode and a new VLAN is added. PR1703226
- Some of the interfaces are going down on rebooting the MPC11E line card. PR1703374
- Updated "show l2-learning vxlan-tunnel-end-point remote" now display svtep for multiple routing instance. PR1703412
- The line card abruptly reboots when ISSU is performed. PR1703910
- RE will crash when static route duplicates with an interface IP address. PR1703940
- The next-hop is shown as unicast instead of reject even when the IPv6 neighbor is unreachable. PR1704114

- RPD core@bgp_rt_terminate_job->bgp_process_rt_terminate->bgp_rt_terminate_subr->bgp_rto_adv_q_free (). PR1704393
- A transit PTP packet is modified when passing through an MPC5E and MPC6G line card 100G ports part of PTP boundary/ordinary clock configuration. PR1704606
- Enhancement needed on PTP nbr-update || lcinfo_bmc || utc_arrival_time || lcinfo_msg || utc_arrival_time. PR1704644
- Syslog "[Error] COS SCHED : Token mismatch during Q stats update" seen during config change or when subscriber sessions are going down. PR1705353
- Traffic blackhole in the event of a link failure (Rx LOS) for 1GE-SX/LX optics. PR1705461
- EAP authentication might not be successful with 802.1X server-fail configuration. PR1705490
- No network reachability when enabling the routing-service knob for PPPoE subscribers over the aggregated Ethernet interface. PR1706446
- evo-aftmand-zx not responding, ping, arp not working after unsubscribing some telemetry sensors. PR1706708
- hwdfpc owned records are not exported in the EVO platform for FPC environment sensor. PR1706833
- The PFE syslog tags are missing for the command help syslog "^PFE_?". PR1707504
- Upon ISSU upgrade or system reboot or FPC restart the DAC 100G speed configured port might not come up. PR1707976
- QSFPs are displayed as UKNOWN after the upgrade. PR1708123
- Unsupported AsIndex logs reported continuously on the device for MPC10/MPC11 line cards. PR1708195
- Adaptive Load Balancing (ALB) fails to load balance the VPLS traffic properly on MX platforms with MPC10, MPC11 and LC9600. PR1708264
- Cosmetic logs may appear on MX platforms during ISSU. PR1708283
- The rpd process crash is seen with scaled multicast next-hops. PR1708299
- The Inline Flow Monitoring is not working on Junos MX-VC platforms PR1708485
- Polling of jnxSubscriberPicCountTable and jnxSubscriberSlotCountTable MIBs is broken if any subscribers are terminated over ps interface. PR1709029
- The telemetry sensor will not be created for PCE initiated SRTE. PR1709557

- RPD CPU utilization is 100 percent when configured with virtual router-advertisement for the aggregated Ethernet interface. PR1709629
- Ports with QSA adapter are down. PR1709817
- CRDC MFT: picd core observed after FPC OIR with CRDC baseline configuration. PR1709962
- ICCP connection establishment b/w JUNOS and EVO is not supported. PR1710448
- AIGP not distinguished with BGP-LU when rib-sharding is enabled. PR1710829
- The FPC will be offline after upgrading the system. PR1710855
- MX304 continuous log messages are seen for "FEC is not supported for pcs-type" and "aft-proxy: SHARED MEMORY ifd_index 178 valid = 1". PR1711258
- gNMI line card (PFE) sensor /junos/system/linecard/packet/usage/ may have packet drops (gNMI translator lookup failures). PR1711779
- Observed vmcore while executing MTS (scripr profile: ospf_db_protection_mts_001.robot_BRACKLA.... #bad_area_nosemaphore, #uio_dma_buf_ops_release, #task_work_run) . PR1711964
- The interface does not come up or flaps. PR1712007
- FPC memory leak will cause FPC crash. PR1712076
- Master and Backup RE synchronization issue will be seen if chassisd is restarted on the primary Routing Engine. PR1712352
- PCT : Show Ephemeral-Configuration Instance Junos-Analytics is not giving expected output while verifying the commit operation with new config hierarchy openconfig-telemetry:telemetry-system. PR1712409
- The MACsec on the channelized IFD impacts the MACsec traffic on other channelized IFL interfaces within the same port and vice versa. PR1712554
- VXLAN tunnels not rerouting as expected. PR1712713
- When a 4x10GE channelized interface is set to disable from config, the channel 0 also goes down. PR1712920
- The rpd process will crash when BMP is configured. PR1713444
- RA can be sent in response to an invalid RS. PR1713485
- When VPLS is enabled on the LT interface, unknown unicast traffic is forwarded rather than discarded. PR1713523

- ppe_error_interrupt and ppe_traps seen on MPC10 with MPLS ps over rlt config with ultimate-hop-popping enabled. PR1713606
- The member interface will not be added to the AE bundle if the link-speed of the AE interface doesn't match that of the member. PR1713699
- IPv6 Fragmentation is not working on MS-MPC/MS-MIC in DS-Lite scenario. PR1713725
- Unexpected load balancing of packets having GRE header. PR1713958
- Subscribers connectivity is lost due to multiple MIC restart on all Junos MX platforms with MPC5E and BBE configuration. PR1713968
- Traffic loss is seen on telemetry streaming in BGP sharding environment. PR1714087
- JUNOS-REG-REGRESSIONS: VMX :Total LSP count mismatch on path computation client after PCCD restart. PR1714158
- Illinois: CP: Incorrect multicast adjustment shown with interface-set queuing. PR1714271
- PPPoE and DHCP subscriber connection on dynamic VLAN can fail on Junos MX platforms. PR1714778
- JDI-REG: [MX480][MX2010]: IPSEC:: IPSEC Tunnels are not coming up after configuring IPSEC under Service-sets. PR1715071
- DSCP field in IPv4 header is incorrectly re-written. PR1715149
- The bbe-smgd process is seen to crash if a large scale PWHT configuration is present. PR1715410
- Known multicast traffic is not forwarded when MLD snooping is enabled. PR1715429
- Traffic loss is seen on RTG bound interface. PR1715518
- BMP station will not receive the RIBs as expected. PR1715886
- The link remains down on connecting the transceiver 10GBASE-T with the serial number starting with "2P1". PR1716703
- A 10G port on a MPC2E or MPC3E 4x10G MIC can randomly flap constantly every few seconds. PR1716766
- SNMP MIB OID output showing wrong temperature value if device running under negative temperature. PR1717105
- Traffic loop is seen due to incorrect root bridge ID. PR1717267
- Tomatin: xml output for show chassis environment psm is different across releases. PR1717630

- The RPD process generates the core files at `lr_logicalrouterid_get rpd_platform_init rpd_infra_family_inits_set`. PR1718324
- In a DHCP ALQ subscriber scenario delete-binding-on-renegotiation knob does not work as expected due to a synchronization error between the primary and the backup routers. PR1718342
- RPD cores when routing churn happens, if RE restart was missed after configuring the FMBB command. PR1718510
- mx2010::DVAITA-SUBLC: Fabric plane on few PFEs assigned to SLC shows as unused. PR1718834
- The PPTP connection itself won't work when trying to establish PPTP connection along with DSLITE. PR1718840
- On MX30 devices, major Host 1 Chassis Manager connection down alarm. PR1719767
- Convergence delay is seen when FPC is offlined under heavy traffic and scaled scenario. PR1719956
- The rpd process crash will be observed while creating/updating the PCEP tunnel. PR1720031
- On MX10004 devices, few UPF sessions remain in deleting state after logout attempt. PR1720536
- The dcpfe process crash will be observed in the EVPN-VXLAN multihoming scenario. PR1721322
- Sending GARP reply packet on a VTEP interface causes flooding in network on QFX5130 and QFX5700 platforms. PR1721704
- BFD session failed when configured on the loopback sub interface. PR1721714
- The filter will not work as configured upon changing the "physical-interface-policer" parameters. PR1722776
- Router Send RA with Router lifetime 0 when the upstream interface is shut. PR1722809
- Complete traffic blackhole from one PFE to another on fabric links after injecting/reporting CRC errors on fabric links of MX10008. PR1724007
- On certain Junos MX platforms with SCB3 SyncE fails after enabling PTP. PR1724254
- PTSP subscribers are stuck in 'configured' state. PR1726136
- Enabling disk smart-check utility on the routing-engine with Innodisk SSD raises a false positive smart error. PR1726252
- JSU installation fails when you configure MACsec. PR1726264
- Traffic drops with percent policer attached using list. PR1726733
- FPC crash observed when the ASIC usage is high. PR1727427

- On all Junos platforms, the l2ald process memory usage is seen to increase over time. PR1727954
- SNMP walk timeout for NMS . PR1728510
- Traffic drop might be observed on MX Platform configured with PCP mapping with NAT. PR1729801
- IPSEC traffic drops when two ARI routes get installed for the same tunnel. PR1734212

Infrastructure

- RE fails to boot when booted directly from Junos volume. PR1701451

Interfaces and Chassis

- The dcd core may be seen on the backup RE after GRES is disabled if targeted distributed configuration is used. PR1650676
- Incompatible/unsupported configuration is not getting validated correctly during ISSU/normal upgrade causing the traffic loss. PR1692404
- The cstm4 interface on MIC-3D-8CHOC3-4CHOC12 cannot be partitioned to more than 10 E3 interfaces. PR1701875
- FPC offline can be seen on MX-VC during the sequential upgrade. PR1706268
- JDI-REG:[VIRTUAL]:[eoam] [eoamtag] MX304 :: Not getting the expected values while verifying ['linktrace_egress_mac_address', 'linktrace_flags', 'linktrace_ingress_mac_address', 'reply_ttl'] On devices. PR1707126
- On Junos platforms the dcd will flap the IFLs which are part of EVPN routing-instance. PR1712800
- The firmware upgradation will fail for MPC7E line card in MX-VC scenario. PR1713502
- The interface speed gets set to a lower speed when the interface is enabled. Renegotiation of the interfaces happens are the negotiated speed. PR1714267
- Issue in VRRP inline adjacency whenever a master router uplink goes down on MX platforms. PR1720943

Junos Fusion Provider Edge

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

Layer 2 Features

- The rpd process crash will be observed during VPLS to EVPN migration. PR1729052

Layer 2 Ethernet Services

- DHCP packets might not be sent to the clients when 'forward-only' is reconfigured under the routing instance. PR1689005
- DHCPv6 client options missing in solicit messages if TLV's exceeds a certain length. PR1702831
- On all Junos MX Series and PTX Series routers, multiple LACP timeouts cause traffic loss due to ppman resource starvation. PR1706224
- A jdhcpd process crash is observed on all Junos platforms. PR1713619
- The DHCPv4 relay will send two option-82 to the server and the DHCP session will not be established. PR1714260

MPLS

- Traffic is not load-balanced when one of the next-hop LSP is down. PR1690110
- The rpd process crash is seen when PCCD is deactivated. PR1694957
- The rpd core generated and routing daemon gets restarted. PR1696017
- RPD(LDP) cores with configurations like BGP static routes or SR-TE routes in INET.0. PR1697498
- RPD core can be seen on the dual RE platform. PR1697988
- The rpd process will crash when rpd is restarted. PR1698889
- LDP flaps will be observed having LT interface with VLAN and LDP running between the logical-system instance and global instance. PR1702220

- Pathtear message is not forwarded by PLR to merge point which is causing data plane blackholing. PR1703424
- Member LSPs of a container LSP will be torn down unexpectedly. PR1705964
- When LDP dual transport is enabled, LDP V4 connection id changes from dual transport v4 id to router-id when rouer-id changes. PR1706064
- PathErr with RoutingProblem error code generated unexpectedly during dual failure local repair. PR1713392
- Routing engine initiated PING failed over MPLS interface. PR1723145

Network Management and Monitoring

- The ok response is getting generated along with rpc-error. PR1585855
- Consistent high CPU usage is seen on the device post reboot. PR1691986

Platform and Infrastructure

- M/Mx: FPC core @ jnh_call_read_index , trinity_nh_ucast_uninstall_hw. PR1636758
- The interface on the device will go down when one or more interfaces are connected to the Advantech3260 device at another end. PR1678506
- The traffic loss duration increases during the LSP switchover. PR1681250
- Disabling PFE triggers the memory leak which may cause FPC to crash. PR1686068
- CoS memory errors are seen when "chassis traffic-manager enhanced-priority-mode" is configured. PR1687642
- The TCP sessions for BGP are closed on the backup Routing Engine. PR1700438
- VRRP does not work when a firewall filter is configured to accept VRRP packets with a TTL value of 255. PR1701874
- Traffic is blocked on a queue when enhanced priority mode is configured. PR1704129
- Severity reclassification of queuing ASIC XQSS and memory parity error auto recovery. PR1706494

- The DEI bit will not be copied in the inner VLAN tag although the incoming traffic has the DEI bit set. PR1714429
- In a rare case FPC crashes and reboots generating a core. PR1720591
- VLAN rewrite will not work for traffic egressing on IRB over L2 AE IFL. PR1720772
- In TWAMP server/reflector, test traffic classified by ingress filter is re-classified by host-outbound-traffic statement. PR1722232
- On certain Junos MX platforms queue buffer-size temporal computation is not happening correctly. PR1726698
- Multiple CFM sessions are not coming up when CFM configured on AE interfaces. PR1727049

Routing Policy and Firewall Filters

- Issue in committing more than 23, 4-byte AS on Junos platforms. PR1706143
- The flowd process crash is observed with the security policy updated with changing IP address related to the FQDN. PR1713576
- Commit error will not be seen after deactivating routing-instance applied under firewall filter. PR1720389

Routing Protocols

- The ppmd daemon memory leak might happen in the scenario where BFD authentication with ISIS is configured. PR1480648
- Traffic loss observed due to multicast routes exceeding the scale for OISM feature. PR1671901
- More than expected traffic loss is seen with ECMP FRR enabled during link down scenario. PR1687887
- BGP LU Advertisements fail with the message "BGP label allocation failure: Need a gateway". PR1689904
- BMP will not send EOR message. PR1690213
- Deletion and addition of BGP transport-class caused the rpd crash. PR1692320

- RLI-53108: When Lsys is configured with 'family route-target', there is a certain corner case scenario where Lsys shutdown does not complete. PR1695050
- Traffic null routes are observed when it takes a long time to remove the BGP routes from RIB. PR1695062
- mcsnoopd-agent core @x00005556c3037dfa in McsnoopdAgentRtTableEvents::OnDelete. PR1696374
- Multicast traffic loss for 2 to 3 seconds. PR1698265
- The rpd process might crash when SPF is recalculated. PR1699076
- [bfd] [bfd_ospf3] ACX7100-32C :: Not all BFD sessions are coming up in 4000 scaled sessions. PR1699085
- The BGP graceful-shutdown community is not advertised on Junos platforms. PR1699633
- The mcscnoopd process will be stuck in resync state after snooping configuration is deleted and added again immediately. PR1699784
- The ppmd process crash will be seen after GRES. PR1702687
- Anycast PIM doesn't work when the peer has an authentication key configured for MSDP. PR1703707
- On all Junos and Junos OS Evolved platforms, the TI-LFA and Legacy LFA are mutually exclusive, and the commit check will fail and blocks LFA on one instance. PR1704521
- FORWARD_NULL:DEV_COMMON_BRANCH. PR1704834
- Traffic loss happens when ISIS LSP size of more than 8500 bytes. PR1704924
- Invalid integer value error need a fix across the sub hierarchy of `show bfd session` command. PR1705820
- The BGP sessions will flap after the RE switchover. PR1705938
- OSPF routes are not getting installed after the interface is flapped. PR1705975
- The BFD session would flap when the GRES is triggered with single-hop BFD over AE interfaces configured. PR1706018
- A crash can be observed for 'mcsnoopd' process when the VLAN name for igmp-snooping has certain characters. PR1711153
- On all Junos and Junos OS Evolved platforms with max-lsp-size configured some flex-algo routes are not getting leaked from IS-IS Layer 1 to Layer 2. PR1711565

- IPv4 routes learnt over a link-local BGP session not advertised ahead to other BGP peers. PR1712406
- Stale entries present in the lsdist table after ISO address change. PR1713008
- Multipath route is not getting compute and skip the multipath eligibility check. PR1716153
- BGP connection doesn't establish when it is configured with rfc8950-compliant under logical-systems on all Junos platforms. PR1716946
- Unexpected behavior of bandwidth based metric for IS-IS protocol. PR1718734
- The rpd process crashes when TI-LFA is enabled. PR1719033
- Slow convergence of PIM joins causes temporary traffic loss with scaled downstream interfaces. PR1720708
- Packet loss observed when Junos Evolved PTX platforms with Graceful Restart enabled have rpd restarted. PR1721008
- Multiple flaps of the interface will cause the BFD session to be down. PR1725971

Services Applications

- Impaired accuracy for delay measurements using PAA. PR1697270
- A stale nat-long-route entry is present in the device causing incoming packets to be dropped. PR1719216

Subscriber Access Management

- The interim-rate under radius-options feature is not working post implementing BBE statistics performance and scale improvements. PR1695956
- A few subscriber sessions will not be up post RE switchover. PR1697392
- Intermittent authd crash will be seen on Junos platforms in a DHCP subscriber scenario. PR1697447
- The subscriber sessions will be logged out when assigned IP addresses from Radius or AAA through framed-IP. PR1709574
- High CPU utilization is seen on Junos MX series platforms. PR1710145

- IPv4 and IPv6 address allocation will be impacted due to changes in address pool configuration. PR1715490
- Subscriber sessions will fail to login post GRES and scaled subscriber scenario. PR1723183

User Interface and Configuration

- The mustd process crash might be observed with persist-group-inheritance. PR1638847
- gNMI GET request fails when OpenConfig is present. PR1697869
- The mgd process might crash during commit synchronize. PR1699245
- The system won't come up in a working state post reboot for upgrade validation fails to detect invalid host-name. PR1703745
- MX960 :: CST:RE goes to amnesiac state, when rebooting the DUT -mgd: error: translation script failure. PR1708321

VPNs

- Routes flapping when configuration changes are applied to custom routing instance. PR1654516
- IKE cookies didn't change in rekey lifetime expire cases after manual failover. PR1690921
- Two-digit numbered interfaces cannot be used as protect-interfaces. PR1695075
- IPsec VPNs will disconnect after ISSU. PR1696102
- The rpd crash happens when Multicast VPN (Virtual Private Network) is configured with separate route-targets scenario. PR1700345
- The pseudowire interface is not showing after performing the switchover. PR1708572
- MVPN sender site not working with IR tunnels. PR1709175
- The iked process will crash when VPN tunnels parameters are not matching. PR1716092

Migration, Upgrade, and Downgrade Instructions

IN THIS SECTION

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

Starting in Junos OS 17.4R1 release, FreeBSD 11.x is the underlying OS for all Junos OS platforms which were previously running on FreeBSD 10.x based Junos OS. FreeBSD 11.x does not introduce any new Junos OS related modifications or features but is the latest version of FreeBSD.

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

Platform	FreeBSD 6.x-based Junos OS	FreeBSD 11.x-based Junos OS
MX5, MX10, MX40,MX80, MX104	YES	NO
MX240, MX480, MX960, MX2010, MX2020	NO	YES

Basic Procedure for Upgrading to Release 21.1R1

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 11.x-Based Junos OS

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

To download and install FreeBSD 11.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-x86-32-23.2R1.9-signed.tgz
```

- For 64-bit Routing Engine version:

```
user@host> request system software add no-validate reboot source/junos-install-mx-x86-64-23.2R1.9-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-x86-32-23.2R1.x-limited.tgz
```

- For 64-bit Routing Engine version:

```
user@host> request system software add no-validate reboot source/junos-install-mx-x86-64-23.2R1.9-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) to Junos OS (FreeBSD 11.x). This is because programs in the **junos-upgrade-x** package are built based on FreeBSD 11.x, and Junos OS (FreeBSD 6.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 21.1R1, 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 21.1R1 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.

Procedure to Upgrade to FreeBSD 6.x-Based Junos OS

Products impacted: MX5, MX10, MX40, MX80, MX104.

To download and install FreeBSD 6.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:

```
user@host> request system software add validate reboot source/jinstall-ppc-23.2R1.9-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 OS package):

```
user@host> request system software add validate reboot source/jinstall-ppc-23.2R1.9-limited-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*

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.

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

Upgrading 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 21.1R1

To downgrade from Release 21.1R1 to another supported release, follow the procedure for upgrading, but replace the 21.1R1 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.

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 sixty months after the first general availability date and customer support for an additional six more months.

  NOTE: The sixty months of support for EEOL releases is introduced in Junos OS 23.2 release and is available for all later releases. For releases prior to 23.2, the support for EEOL releases continues to be thirty six 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 21.2 to the next three releases – 21.3, 21.4 and 22.1 or downgrade to the previous three releases – 21.1, 20.4 and 20.3.

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, 21.2 is an EEOL release. Hence, you can upgrade from 21.2 to the next two EEOL releases – 21.4 and 22.2 or downgrade to the previous two EEOL releases – 20.4 and 20.2.

Table 4: EOL and EEOL Releases

Release Type	End of Engineering (EOE)	End of Support (EOS)	Upgrade/ Downgrade to subsequent 3 releases	Upgrade/ Downgrade to subsequent 2 EEOL releases
Standard End of Life (EOL)	24 months	End of Engineering + 6 months	Yes	No
Extended End of Life (EEOL)	60 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 NFX Series

IN THIS SECTION

What's New

IN THIS SECTION

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

To view features supported on the NFX platforms, view the Feature Explorer using the following links. To see which features were added in Junos OS Release 23.2R1, click the Group by Release link. You can collapse and expand the list as needed.

- NFX150
- NFX250
- NFX350

Platform and Infrastructure

- **Support for dynamic update of trusted CA bundle (SRX1500, SRX4100, SRX4200, SRX4600, SRX5400, SRX5600, SRX5800, vSRX 3.0 and NFX350)**—Starting in Junos OS Release 23.2R1, we support the dynamic update of default trusted CA certificates. With this feature, you have the latest list of default trusted CA certificates on Junos OS devices. You can easily download, install, and update the certificate bundle periodically.

  [See Dynamic Update of Trusted CA Certificates.]

VPNs

- **Support for dynamic update of trusted CA bundle (SRX1500, SRX4100, SRX4200, SRX4600, SRX5400, SRX5600, SRX5800, vSRX 3.0 and NFX350)**—Starting in Junos OS Release 23.2R1, we support the dynamic update of default trusted CA certificates. With this feature, you have the latest list of default trusted CA certificates on Junos OS devices. You can easily download, install, and update the certificate bundle periodically.

  [See Dynamic Update of Trusted CA Certificates.]

What's Changed

Learn about what changed in this release for NFX Series devices.

Known Limitations

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

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

Open Issues

IN THIS SECTION

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

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

Interfaces

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

  WorkaroundDeactivate and then activate the aggregated Ethernet interface. PR1583054

Resolved Issues

IN THIS SECTION

Learn about the issues fixed in this release for NFX Series

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

Interfaces

- On the NFX350 device, even though the ethernet cable is physically plugged in and the `show interface command` displays Front panel LED status as `up`, the front panel LED is not ON.PR1702799
- When issuing request support information, there was a syntax error when looking at the nfx-back-plane (was nfx-backplane, instead of nfx-back-plane)

  PR1720228
- On Junos NFX350 Platforms, if you disable any RJ-45 interface through configuration, auto-negotiation at the MAC (Media Access Control) level on the remaining ports of the group of 4 ports (either 0-3 or 4-7) is disabled, resulting in traffic disruption. The impact isconfined to the group of ports on which the port is disabled and the other group is not affected.

  PR1731242

Software Installation and Upgrade

- **Two-step Downgrade (NFX150, NFX250 NextGen, and NFX350)**—You cannot downgrade Junos OS Release 23.1R1 directly to certain releases (listed in the **Target Release** column in Table 5 on page

88). As a workaround, you can perform downgrade as a two-step activity, in which you downgrade Junos OS Release 23.1R1 first to a corresponding intermediate release (listed in Table 5 on page 88), and then to the target release.

Table 5: Release Compatibility for Downgrading Junos OS 23.1R1 on NFX Series Devices

Target Release	Intermediate Release
Any 22.4x release earlier than 22.4R2	22.4R2
Any 22.3x release earlier than 22.3R2.	22.3R2
• Any 22.2x release earlier than 22.2R3. • Any 22.1x release or earlier releases.	22.2R3

PR1694074

VPNs

- IPSec tunnel is down if IKE external-interface is configured with IPv4 and IPv6 address. As a workaround, specify the local-address inside the ike gateway object if the configured external-interface contains both IPv4 and IPv6 address hosted on it.

  PR1716697

VNFs

- On Junos NFX350 Platforms, in spite of disabling the Auto Negotiation (AN) on the interface through configuration, it stays enabled on the copper ports.This could result in mismatch of AN settings with the remote side configuration and disrupt traffic.

  PR1719973

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.

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

Basic Procedure for Upgrading to Release 23.2R1

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 23.2R1:

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.

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 sixty months after the first general availability date and customer support for an additional six more months.

> **NOTE**: The sixty months of support for EEOL releases is introduced in Junos OS 23.2 release and is available for all later releases. For releases prior to 23.2, the support for EEOL releases continues to be thirty six 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 21.2 to the next three releases – 21.3, 21.4 and 22.1 or downgrade to the previous three releases – 21.1, 20.4 and 20.3.

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, 21.2 is an EEOL release. Hence, you can upgrade from 21.2 to the next two EEOL releases – 21.4 and 22.2 or downgrade to the previous two EEOL releases – 20.4 and 20.2.

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
Standard End of Life (EOL)	24 months	End of Engineering + 6 months	Yes	No
Extended End of Life (EEOL)	60 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 QFX Series

IN THIS SECTION

What's New

IN THIS SECTION

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

To view features supported on the QFX platforms, view the Feature Explorer using the following links. To see which features were added in Junos OS Release 23.2R1, click the Group by Release link. You can collapse and expand the list as needed.

- QFX5110
- QFX5120-48Y
- QFX5120-32C
- QFX5120-48T
- QFX5120-48YM
- QFX5200
- QFX5210-64C
- QFX10002
- QFX10008
- QFX10016
- QFX10002-60C

Class of Service

- **Port shaping support (EX4650, QFX5110, QFX5120, QFX5200, and QFX5210)**—Starting in Junos OS Release 23.2R1, you can improve excess traffic management with traffic shaping at the port level. By default, an egress port transmits traffic up to the line-rate of the port. With port shaping, you can limit the rate of traffic an egress port transmits to a value less than the line rate.

  [See CoS Port Shaping.]

EVPN

- **New VXLAN-GBP profiles and additional L4 matches for GBP policy filters (EX4100, EX4400, EX4650, and QFX5120 switches)**—Starting in Junos OS Release 23.2R1, we've added these enhancements to the group-based policy (GBP) microsegmentation feature:

  - The EX4400, EX4650, and QFX5120 switches support new VXLAN-GBP profiles:

    - `vxlan-gbp-l2-profile`

      This profile increases the capacity for MAC addresses.

    - `vxlan-gbp-l3-profile`

      This profile increases the capacity for IP addresses.

  - The EX4400, EX4100, EX4650, and QFX5120 switches support additional Layer 4 matches for a GBP policy filter for IPv4 or IPv6. You can use protocol, source ports, destination ports, TCP flags, and other matches for MAC and IP-based GBP tagged packets.

  - You can use the `set forwarding-options evpn-vxlan gbp tag-only-policy` command to allow only GBP source and destination tags as matches in the GBP policy on the EX4650 series, QFX5120-32C, and QFX5120-48Y switches.

  [See Example: Micro and Macro Segmentation using Group Based Policy in a VXLAN.]

- **Support for detecting local and global loops in EVPN fabrics (EX4400 and QFX5120)**—Starting in Junos OS Release 23.2R1, we've enhanced the duplicate MAC address detection feature to take a configured action when a duplicate MAC address is detected. Loops can occur when provider edge (PE) devices continuously forward frames back and forth to one another in the same broadcast domain.

  To detect and resolve these loops, use the following statements at the `[edit routing-instances` *`name`* `protocols evpn duplicate-mac-detection]` hierarchy level on your peer devices:

  - `action <block | shutdown>`

The `block` option blocks any packet that has the source MAC address or destination MAC address of the duplicate MAC address. The `shutdown` option shuts down the duplicate MAC address's local interface.

- `include-local-moves`. This statement tracks duplicate MAC address movements that occur on local interfaces.

To manually clear the duplicate MAC addresses, issue the `clear evpn duplicate-mac-suppression <instance name | l2-domain-id | mac-address>` command.

To manually recover the interface that was shut down, issue the `clear ethernet-switching recovery-timeout` command.

- **Symmetric Type 2 EVPN-VXLAN to EVPN-VXLAN DCI stitching (EX4650, QFX5120-32C, QFX5120-48T, QFX5120-48Y, QFX5120-48YM, and QFX10002)**—Starting in Junos OS Release 23.2R1, we support Ethernet VPN–Virtual Extensible LAN (EVPN-VXLAN) to EVPN-VXLAN symmetric Type 2 route stitching between data center networks using Data Center Interconnect (DCI). Your network can more efficiently interoperate with data center networks that include devices from other vendors who support symmetric Type 2 route stitching. Symmetric Type 2 route stitching means that the VXLAN tunnel endpoint (VTEP) interfaces perform routing and bridging on both the ingress and egress sides of the VXLAN tunnel.

  [See Symmetric Integrated Routing and Bridging with EVPN Type 2 Routes in EVPN-VXLAN Fabrics.]

- **GBP tag propagation with EVPN-VXLAN to EVPN-VXLAN stitching (EX4650, QFX5120-32C, QFX5120-48T, QFX5120-48Y, QFX5120-48YM, and QFX10002)**—Starting in Junos OS Release 23.2R1, we support group-based policy (GBP) tag propagation for EVPN Type 2 and Type 5 routes in a stitched EVPN-VXLAN data center environment. GBP uses existing Layer 3 VXLAN network identifiers (VNIs) in conjunction with firewall filter policies to provide microsegmentation at the device or tag level, independent of the underlying network topology.

  [See Example: Micro and Macro Segmentation using Group Based Policy in a VXLAN.]

- **Domain path attribute for EVPN-VXLAN Type 5 stitching (QFX10002)**—Starting in Junos OS Release 23.2R1, we support domain path with EVPN Type 5 routes. Domain path is a BGP attribute used along with EVPN Type 5 routes to identify domains through which routes have already passed.

  [See domain-path-id.]

- **Hard interface shutdown when a device detects EVPN core isolation conditions (EX4100-24MP, EX4400-24MP, MX304, MX10003, QFX5120-32C, QFX5120-48T, QFX5120-48Y, and QFX5120-48YM)**—Starting in Junos OS Release 23.2R1, you can configure a device to bring associated interfaces down (hard shutdown) when the device detects an EVPN core isolation event. In the CLI:

  1. Define a service tracking profile for detecting core isolation conditions.

2. Set the `link-down` service tracking action in the profile.

3. Assign the profile to the interfaces you want the device to bring down after it detects a core isolation condition.

We support core isolation service tracking on:

- Links to single-homed customer edge (CE) devices.
- Ethernet segment identifier (ESI) LAG member interfaces to multihomed CE devices.

[See network-isolation and network-isolation-profile.]

- **Simplified configuration for ESI LAGs with EVPN dual-homing (EX4100-48MP, EX4100-24MP, EX4100-48P, EX4100-48T, EX4100-24P, EX4100-24T, EX4100-F-48P, EX4100-F-24P, EX4100-F-48T, EX4100-F-24T, EX4100-F-12P, EX4100-F-12T, EX4300-MP, EX4400-24MP, EX4400-24P, EX4400-24T, EX4400-24X, 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 23.2R1, we support a new CLI statement hierarchy level, `[edit services evpn]`. Using statements at this hierarchy level, you can specify the device attributes and other parameters to configure an Ethernet segment in an EVPN fabric. This new configuration simplifies setting up EVPN fabrics with Ethernet segment identifier (ESI) link aggregation groups (LAGs) for dual-homing peer provider edge (PE) devices.

  When you commit a configuration at this hierarchy level, the device automatically invokes commit scripts to create a corresponding configuration on the device. You must specify some mandatory elements. You can also include optional elements. For optional elements that you don't specify, the automatic configuration scripts derive the optional elements (or the scripts use default parameters).

  The resulting automatic configuration includes the applicable configuration stanzas corresponding to the different elements you specify at the `[edit services evpn]` hierarchy level.

  The new hierarchy includes options to override some default parameters, and you can override the automatically configured settings by manually configuring the related statements.

Junos Telemetry Interface

- **EVPN remote route statistics (QFX5100 and QFX10002)**—Starting in Junos OS Release 23.2R1, we support streaming statistics for EVPN remote routes.

  [See Junos YANG Data Model Explorer.]

- **Support for OpenConfig multicast data model (ACX5448, ACX710, EX2300, EX2300-MP, EX2300-C, EX2300-VC, EX3400, EX3400-VC, EX4100, EX4100-MP, EX4300-MP, EX4300-VC, EX4400-MP, EX4400, EX4650, EX4650-VC, EX9214, MX204, MX240, MX304, MX150, MX480, MX960, MX2008, MX2010, MX2020, MX10003, MX10004, MX10008, MX10016, vMX, QFX10002-60C, QFX5110, QFX5110-VC, QFX5110-VCF, QFX5120, QFX5120-VC, QFX5200, QFX5210, QFX5500,**

QFX10002, QFX10008, and QFX10016)—Junos OS Release 23.2R1 introduces support for OpenConfig multicast data models **openconfig-pim.yang** (version 0.4.2) and **openconfig-igmp.yang** (version 0.3.0). This feature includes telemetry streaming of operational state data and configuration using OpenConfig.

See Junos YANG Data Model Explorer for state sensors and Mapping OpenConfig Multicast Commands to Junos Configuration for configuration.

- **Support for configuring the routing-instance and source address for each gRPC tunnel session (MX204, MX240, MX480, MX960, MX10003, MX10004, MX10008, MX10016, MX2008, MX2010, MX2020, VMX, and QFX5110)**—Starting with Junos OS Release 23.2R1, you can configure the routing instance and the source address for each gRPC remote procedure call (gRPC) tunnel session to dial out a connection to the tunnel server.

  To configure the routing instance, add the `routing-instance <routing-instance>` option and to configure the source address, add the `source-address <ip-address>` option in the `grpc-tunnel` configuration statement.

  If you do not configure a routing instance, the gRPC tunnel uses the default routing instance. If you do not configure the source address, the kernel picks the source address that can reach the tunnel server.

  [See gRPC Tunnels Overview and grpc-tunnel].

Precision Time Protocol (PTP)

- **Support for PTP G.8275.2.enh profile on QFX5120-48YM-8C switches**—Starting in Junos OS Release 23.2R1, you can enable the distribution of phase and time with partial timing support (PTS) through the Precision Time Protocol (PTP) G.8275.2.enh profile in QFX5120-48YM-8C switches.

  See https://www.juniper.net/documentation/us/en/software/junos/time-mgmt/topics/topic-map/ptp-profiles.html#id_vxn_ydt_rrb

Routing Policy and Firewall Filters

- **Support for loopback-firewallv6-optimization (QFX5210)**-Starting in Junos 23.2R1, `loopback-firewallv6-optimization` can be used to increase IPv6 loopback filter scale when scale of IPv4 loopback filters are used in EVPN VXLAN deployments.

  [See loopback-firewallv6-optimization.]

Routing Protocols

- **Support to activate BFD strict mode for BGP peer sessions (ACX5448, ACX710, cRPD, MX10003, MX10004, VRR, QFX5110, and QFX5200)**—Starting in Junos OS Release 23.2R1, we support the activation of BFD strict mode for BGP peer sessions that disallows BGP to establish a session until

BFD session is successfully established and has stabilized. With the BFD strict mode feature, you can prevent routing churn and minimize network interruption.

To activate BFD strict mode for BGP peer sessions, include the `strict-mode [bfd-wait-timeout <10-255 seconds>` CLI statement under `bfd-liveness-detection` at the `[edit protocols bgp group` *`group-name`* `neighbor` *`address`*] hierarchy level.

For example, use the following command to activate BFD strict mode for BGP peer sessions:

`set protocol bgp group` *`group-name`* `neighbor` *`address`* `bfd-liveness-detection [strict-mode [bfd-wait-timeout` *`10-255 seconds`*`]]`

[See Understanding BFD for BGP, bfd-liveness-detection (BGP).]

Additional Features

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

- **Ephemeral database support for configuring MSTP, RSTP, and VSTP** (ACX Series, EX Series, and QFX Series). You can configure the following protocols in the ephemeral configuration database:
  - Multiple Spanning Tree Protocol (MSTP)
  - Rapid Spanning Tree Protocol (RSTP)
  - VLAN Spanning Tree Protocol (VSTP)

  [See Unsupported Configuration Statements in the Ephemeral Configuration Database.]
- **Seamless EVPN-VXLAN stitching** (QFX10002-36Q, QFX10002-72Q, QFX10008, and QFX10016). We support the seamless stitching of unicast, broadcast, and unknown unicast routes.
- **View supported transceivers, optical interfaces, and DAC cables**—Select your product in the Hardware Compatibility Tool (HCT) to view the supported transceivers, optical interfaces, and direct attach copper (DAC) cables for your platform or interface module. We update HCT and provide the first supported release information when the optic becomes available.

What's Changed

IN THIS SECTION

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

General Routing

- **Multicast debug information added in EVPN options to request system information command (MX Series, QFX Series)**—The output from CLI command `request support information evpn-vxlan` now includes additional information to help debug EVPN multicast issues.

  [See request support information.]

- The connectivity fault management process (cfmd) runs only when the ethernet connectivity-fault-management protocol is configured.

- **Label for the hours unit of time displayed in output**— When there are zero minutes in the output for the `show system uptime` command, the label for the hours unit of time is displayed.

  [See show system uptime.]

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

- **The active-user-count is defined as a numeric integer value in ODL request output** — The output for the get-system-uptime-information ODL request contains information for the active-user-count. The active-user-count is now defined as a numeric integer value and avoids an invalid value type error.

  [See show system uptime.]

Network Management and Monitoring

- **Changes to the `show system yang package` (`get-system-yang-packages` RPC) XML output (ACX Series, EX Series, MX Series, QFX Series, SRX Series, vMX, and vSRX)**—The `show system yang package` command and `<get-system-yang-packages>` RPC include the following changes to the XML output:

  - The root element is `yang-package-information` instead of `yang-pkgs-info`.

- A yang-package element encloses each set of package files.
- The yang-pkg-id tag is renamed to package-id.
- If the package does not contain translation scripts, the Translation Script(s) (trans-scripts) value is none.

- **NETCONF server's <rpc-error> response changed when <load-configuration> uses operation="delete" to delete a nonexistent configuration object (ACX Series, EX Series, MX Series, QFX Series, SRX Series, vMX, and vSRX)**—In an earlier release, we changed the NETCONF server's <rpc-error> response for when an <edit-config> or <load-configuration> operation uses operation="delete" to delete a configuration element that is absent in the target configuration. We've reverted the changes to the <load-configuration> response.

- **Changes to the RPC response for <validate> operations in RFC-compliant NETCONF sessions (ACX Series, EX Series, MX Series, QFX Series, SRX Series, vMX, and vSRX)**—When you configure the rfc-compliant statement at the [edit system services netconf] hierarchy level, the NETCONF server emits only an <ok/> or <rpc-error> element in response to <validate> operations. In earlier releases, the RPC reply also includes the <commit-results> element.

Routing Protocols

- **Configure conserve-mcast-route-in-pfe option on OISM server leaf and border leaf devices in scaled EVPN-VXLAN fabrics to avoid multicast route exhaustion (QFX5130-32CD and QFX5700 switches)**—You can configure QFX5130-32CD and QFX5700 switches as optimized intersubnet multicast (OISM) server leaf or border leaf devices in an EVPN-VXLAN fabric. In scaled fabrics with many VLANs, EVPN instances, and multicast streams, you might see multicast traffic loss on these devices due to the limited size of the multicast snooping route tables in the PFE. To avoid this problem on QFX5130-32CD and QFX5700 switches with OISM in scaled environments, we require that you configure the conserve-mcast-routes-in-pfe option at the edit multicast-snooping-options oism hierarchy on these platforms. This option is available only on QFX5130-32CD and QFX5700 switches. Use this option when you configure these devices as server leaf or border leaf devices with OISM. Do not configure this option when you configure these devices as standalone assisted replication (AR) replicators with OISM.

  [See oism (Multicast Snooping Options.]

Known Limitations

IN THIS SECTION

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

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

General Routing

- During software validation, Junos OS mounts the new image and validates the configuration against the new image. Since the TVP-based QFX platforms (QFX5000 and QFX10000) are already mounting the maximum 4 disks during normal execution it cannot mount the extra disk for this purpose. Thus QFX currently does not support configuration validation during upgrade on QFX5000 so the syntax error appears when the image installation is triggered with **validation**. PR1421378
- Higher than expected loss and traffic null routes are seen during node failures with node protection on FTI interfaces for RSVP LSPs. PR1456350
- PFC is not supported across the FPCs with the HGOE VCPs. PR1709186
- Dot1x daemon read the configuration whenever there is change in time based license for the feature macsec. PR1713881

Infrastructure

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

Open Issues

IN THIS SECTION

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

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

General Routing

- VXLAN VNI (multicast learning) scaling on QFX5110 traffic issue is seen from VXLAN tunnel to Layer 2 interface. PR1462548
- PIM VXLAN does not work on the TD3 chipsets that enables the VXLAN flexflow. PR1597276
- When the remote end server or system reboots, QFX5100 platform ports with SFP-T 1G inserted might go into a hung state and remain in that state even after the reboot is complete. This might affect traffic after the remote end system comes online and resumes traffic transmission.PR1665800
- On QFX5100 platforms (both stand-alone and VC scenario) running Junos, occasionally during the normal operation of the device, PFE (Packet Forwarding Engine) can crash resulting in total loss of traffic. The PFE reboots itself following the crash. PR1679919
- On Junos QFX5100-Virtual Chassis (VC) and Virtual Chassis Fabric (VCF) platforms on upgrading Virtual Chassis Fabric (VCF) and toggling the interface, when FPC (Flexible PIC Concentrators) is disabled and rebooted, the member fails to join the virtual chassis and the interface remains disabled even after been enabled. PR1689499

- The `show chassis hardware` indicates duplicate entries for PSU and FAN tray after USB clean install or zeroize. PR1704106
- On all QFX5000 platforms, with VXLAN (Virtual Extensible LAN) configured and due to a stale next hop entry of vtep (vxlan tunnel end point) interface, dcpfe (Dense Concentrator Packet Forwarding Engine) process crash was observed. PR1712175
- In a VC of QFX5100-24Q with an expansion module EX4600-EM-8F, if VC is formed on 10G ports then after the reboot of VC, the 10G connections will be lost and the line card will show as not present. This will impact traffic on the 10G ports after connection is lost.PR1718062
- If we observe any slowness in accessing the VTY and could see any hogging or scheduler slip messages in syslog. It is advised to run the debug commands manually, instead of running it through RSI.PR1721297
- FRR with Type-1 ESI takes more time to converge as Type-1 ESI is build on partner systemid and adminkey. When the link goes down partner system ID is lost and interface is withdrawn from the ESI.PR1722348
- On the Junos QFX5200 platform, sometimes upon restarting the device the 100G link will not come up and will remain down, impacting the traffic flowing through it.PR1725116
- On all Junos OS and Junos OS Evolved platforms in the EVPN-VXLAN (Ethernet VPN-Virtual Extensible LAN) scenario, when the configuration statement `switch-options no-mac-learning` is configured, the MAC-IP entry will still be learned even though the MAC learning is disabled due to which the proxy ARP (Address Resolution Protocol) will not work properly on the leaf device and it will respond with a wrong MAC address for the ARP request.PR1727119
- On all Junos QFX5000 (except QFX5100) platforms, child links that are in LACP (Link Aggregation Control Protocol) detached state are up and accepting incoming traffic, expecting it to drop. PR1730076
- QFX5120 VSTP on VLAN-bridge might block all packets on **family inet/inet6** interfaces in SP style. PR1732718
- On all inserted FPCs of Junos OS based QFX10008 and QFX10016 platforms, due to SIB (Switch Interface Board) ASIC (Application-Specific Integrated Circuit) issue on fabric, packets are getting dropped and major errors **PECHIP_CMERROR_EPW_MISC_INT_EVENTS_CRC_ERR (0x2101aa)** are reported. These errors are not auto-cleared on a couple of FPCs.PR1734735
- On QFX5120-48YM-8C : PTP 1PPS measurement will not be supported. PR1736385
- In a combination of EX4650 connected to EX4400 and Junos OS based QFX5000 platforms connected to EX4400 using 25G-LR(Long Range) optics, FEC(Forward Error Correction) value mismatch between directly connected devices would cause the link to go down on Junos release version 20.4R3-S8 and above and leads to complete traffic loss. PR1738077

- On Junos OS QFX5000 platforms, no MAC-learning on the interface results in traffic drop due to hardware programming not being updated for the child interface under AE (Aggregated Ethernet) when encapsulation ethernet-bridge is configured on the AE interface associated with VxLAN (Virtual Extensible LAN) VLAN. PR1738205
- On Junos OS QFX5000 platforms in the EVPN-VxLAN scenario, due to high convergence time, traffic loss is more than expected when the uplink to the spine disabled (CLI initiated uplink failover). PR1738276
- On Junos OS QFX10000 platforms, on configuring diffServ code point (DSCP) classifier and when inet or inet6 is configured with custom dot1p on interface, default DSCP classifiers are not getting removed properly. PR1738981
- VXLAN VNI (multicast learning) scaling on QFX5110 traffic issue is seen from VXLAN tunnel to Layer 2 interface. PR1462548
- Pim VXLAN does not work on the TD3 chipsets that enables the VXLAN flexflow. PR1597276
- When the remote end server or system reboots, QFX5100 platform ports with SFP-T 1G inserted might go into a hung state and remain in that state even after the reboot is complete. This might affect traffic after the remote end system comes online and resumes traffic transmission. PR1665800
- On QFX5100 platforms (both stand-alone and VC scenario) running Junos OS, occasionally during the normal operation of the device, PFE (Packet Forwarding Engine) can crash resulting in total loss of traffic. The PFE reboots itself following the crash. PR1679919
- On Junos OS QFX5100 Virtual Chassis (VC) and Virtual Chassis Fabric (VCF) platforms on upgrading Virtual Chassis Fabric (VCF) and toggling the interface, when FPC (Flexible PIC Concentrators) is disabled and rebooted, the member fails to join the virtual chassis and the interface remains disabled even after been enabled. PR1689499
- The `show chassis hardware` indicates duplicate entries for PSU and FAN tray after USB clean install or zeroize. PR1704106

Infrastructure

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

Interfaces and Chassis

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

Layer 2 Ethernet Services

- On QFX5100 and QFX5110, vendor-id format might be incorrect for network ports. This does not impact the ZTP functionality or service. The DHCP client configuration is coming from two places, that is, AIU script and vsdk sandbox. The DHCP client configuration coming from AIU script has the serial ID in vendor ID where as the default configuration from sandbox does not have it. PR1601504
- In EVPN VXLAN topology with DHCP stateless relay (forward-only) configured at Layer 3 gateways, Jdhcpd broadcasts snooped unicast offer packets. That leads to the offer getting dropped on its way to the client and then the IP negotiation fails. PR1722082

Routing Protocols

- On all Junos OS and Junos OS Evolved platforms, if the nexthop of a flow route is the same as it was before when reconfiguring flow routes, memory leak occurs. High memory use of routing process daemon(rpd) is seen as a result of this leak. A kernel out of memory message is observed which results BGP flap. PR1742147

Virtual Chassis

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

Resolved Issues

IN THIS SECTION

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

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

EVPN

- In EVPN scenario, proxy-arp on IRB interfaces do not work as expected. PR1709007
- The generation of the VXLAN table appears to be lost after loading configuration. PR1712805

Forwarding and Sampling

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

General Routing

- JUNOS:JDI_FT_REGRESSION:PROTOCOLS:SWITCHING: INTERFACE : QFX10008:: while verifying em0 statistics interface speed is displaying in gbps instead of mbps. PR1589942
- Traffic failure with error message **Buffers are stuck on queue** after removing and attaching 100G QSFP. PR1641572
- VC members are reloading randomly. PR1671293

- QFX10000 series platforms generates error messages constantly and IPv6 routing is not performed when configured rpf-check and inet6 on VXLAN enabled interface and trying to resolve arp ndp. PR1677422
- DHCPv6 packets are not forwarded if it contains the trailer or extra bytes out of the IP stack. PR1688316
- Traffic loss is observed in IP fabric when there is a change in the underlay network. PR1688323
- There is change in `show pfe vxlan nh-usage` command output. PR1692596
- The l2cpd telemetry crash might be observed when the LLDP Netconf notification from external controllers along with Netconf services configuration is present on the device. PR1695057
- On QFX5110-VC-VCF platforms, traffic impact is seen when the firewall filter with DSCP action is enabled. PR1695820
- Traffic forwarding fails when deleting all Layer 2 related configurations. PR1695847
- Traffic drop is observed for the VCP ports when there is traffic congestion in the egress queues. PR1696119
- Adding more than 256 VLANs as name tags on the same interface results in dcd crash. PR1696428
- Assigning VNI to VLAN will cause a small number of packets lost on other VLANs on the same interface. PR1697244
- Local multicast traffic forwarding issue can be seen on QFX5000 in EVPN-VXLAN OISM setup. PR1697614
- Adaptive sampling will not work if the system clock is turned backward. PR1699585
- The BFD session will remain in init or down state in the Virtual Chassis scenario. PR1701546
- Aggregated Ethernet interface member with `vlan-id-list` configured not forwarding traffic. PR1701636
- License will be deleted due to multiple FPC reboot or switchover on QFX VC scenario. PR1703200
- High CPU utilization causes a latency or slowness issue on QFX platforms. PR1704489
- DCPFE crashes which leads to FPC restart. PR1706515
- The FPC crash can be seen on QFX5000 platforms during simultaneous soft and hard OIR of SFP. PR1707094
- The spine does not reply to RS messages coming through the VXLAN tunnel in the CRB scenario. PR1707679

- License expire error will be observed after upgrade. PR1708794
- BFD sessions flap on QFX platforms. PR1709664
- Ports with QSA adapter are down. PR1709817
- VC members are split when removing and inserting em0 cable. PR1709938
- FPC is down on QFX5000 after committing an IPv6 filter. PR1710704
- The message **fpc0 list_get_head, list has bad magic (0x0)** maybe output after the commit operation is complete. PR1710776
- The FPC will be offline after upgrading the system. PR1710855
- No alarm is raised when PSU is inserted with different airflow directions. PR1710952
- When a 100G transceiver is used as a VC port, the VC port will either not come up or come up as 40G. PR1711407
- DHCPv6 packets could not be forwarded if it contains the trailer or extra bytes out of the IP stack. PR1711525
- Traffic drop is observed in the EVPN-VXLAN scenario with Type-2 ESI tunnel. PR1711889
- VXLAN traffic gets dropped after new Layer 3 VLANs are created. PR1712405
- QSFP-100G-LR4-T2 optics will stay down after ISSU/TISSU. PR1713010
- QFX5120-32C: dcpfe core observed after restart layer 2-learning process. PR1713133
- Next-hop programming issue at Packet Forwarding Engine on Junos OS QFX10000 platforms when the member of unilist is in hold state. PR1713279
- The member interface will not be added to the AE (aggregate Ethernet) bundle if the link-speed of the AE interface does not match that of the member. PR1713699
- Traffic discarded after reboot. PR1714701
- VMcore crashes in a rare scenario. PR1714785
- Known multicast traffic is not forwarded when MLD snooping is enabled. PR1715429
- Untagged packets get dropped while adding a layer 3 logical unit to an interface with native VLAN configured. PR1715477
- IGML and MLD queries might get dropped if received on a non-primary Routing Engine VC member when IGMP and MLD snooping is enabled. PR1716902
- The dcpfe process crashes on QFX5000 devices. PR1716996

- Traffic loop is seen due to incorrect root bridge ID. PR1717267
- Traffic egressing over the EVPN-VXLAN tunnel will drop which has aggregate Ethernet interface as underlay. PR1718528
- ESI:FRR:L2ALD core at l2ald_vxlan_ifl_create_msg_build. PR1718534
- The rpd core is seen in the long-running devices with EVPN enabled. PR1723832
- Traffic loss is seen as Type 2 routes are not pushed even after withdrawing Type 5 routes. PR1723968
- BUM (Broadcast, Unknown Unicast, and Multicast) Traffic can be dropped in some instances. PR1727054
- The dcpfe process crash will be seen on the system. PR1721316
- Error message **%PFE-3: fpc0 Failed to get ifl for ifl index = XXX** is generated when receives DHCP packet through remote VTEP. PR1721318
- Unable to commit configs interface-mac-limit on sub-interfaces with vlan-tagging / flexible-vlan-tagging PR1723400
- QFX10000 not bridging multicast traffic with TTL=1 on same VLAN. PR1723433
- Packet Forwarding Engine crash is seen on Junos OS when file-logging is disabled. PR1723465
- ECMP traffic is not being forwarded on all QFX10002 platforms after software upgrade. PR1723545
- On QFX5000 platforms, the status of **ECMP Resilient Hashing** will not be displayed in output of CLI command `show forwarding-options enhanced-hash-key`. PR1725916
- Delete notifications for sub-interfaces missed in gRPC telemetry. PR1726205
- On all Junos OS platforms the l2ald process memory usage is seen to increase over time. PR1727954
- Traffic is impacted due to high CPU and dcpfe/fxpc crash (in some cases) in EVPN-VXLAN scenario. PR1730771
- SNMP polling Timeout due to OID 1.3.6.1.2.1.31.1.1.1.10.514 (ifInOctets.514). PR1732708

MPLS

- RPD(LDP) cores with configurations like BGP static routes or SR-TE routes in INET.0. PR1697498

Routing Policy and Firewall Filters

- Issue in committing more than 23, 4-byte AS on Junos OS platforms. PR1706143

Routing Protocols

- The BGP graceful-shutdown community is not advertised on Junos OS platforms. PR1699633
- The mcscnoopd process will be stuck in resync state after snooping configuration is deleted and added again immediately. PR1699784
- The IPv4 routes learnt over a link-local BGP session not advertised ahead to other BGP peers. PR1712406
- Unexpected behavior of bandwidth based metric for IS-IS protocol. PR1718734
- Multiple flaps of the interface will cause the BFD session to be down. PR1725971
- Junos OS and Junos OS Evolved: A BGP session will flap upon receipt of a specific, optional transitive attribute (CVE-2023-0026). PR1739919

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.

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

4. In the Install Package section of the Software tab, select the QFX Series Install Package for the 20.3 release.

   An Alert box appears.

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

   A login screen appears.

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

7. Download the software to a local host.

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

9. Install the new jinstall package on the device.

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

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

```
user@host> request system software add source/jinstall-host-qfx-5-x86-64-20.3-R1.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 20.3 `jinstall` package, you can issue the `request system software rollback` command to return to the previously installed software.

Installing the Software on QFX10002-60C Switches

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

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

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

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

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

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

For example:

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

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

For example:

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

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

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

Installing the Software on QFX10002 Switches

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

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

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

For example:

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

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

For example:

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

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

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

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

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

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

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

To install the software on re0:

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

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

For example:

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

To install the software on re1:

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

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

For example:

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

Reboot both Routing Engines.

For example:

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

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

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

Installing the Software on QFX10008 and QFX10016 Switches

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

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

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

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

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

2. From the command line, enter configuration mode:

   ```
   user@switch> configure
   ```

3. Disable Routing Engine redundancy:

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

4. Disable nonstop-bridging:

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

5. Save the configuration change on both Routing Engines:

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

6. Exit the CLI configuration mode:

```
user@switch# exit
```

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

12. Transfer routing control to the backup Routing Engine:

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

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

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

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

Routing Engine status:
  Slot 1:
```

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

Performing a Unified ISSU

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

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

Perform the following tasks:

- No Link Title
- No Link Title

Preparing the Switch for Software Installation

Before you begin software installation using unified ISSU:

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

  To verify that nonstop active routing is enabled:

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

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

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

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

Upgrading the Software Using Unified ISSU

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

To upgrade the switch using unified ISSU:

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

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

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

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

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

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

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

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

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

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

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

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

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

Upgrade and Downgrade Support Policy for Junos OS Releases 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 sixty months after the first general availability date and customer support for an additional six more months.

NOTE: The sixty months of support for EEOL releases is introduced in Junos OS 23.2 release and is available for all later releases. For releases prior to 23.2, the support for EEOL releases continues to be thirty six 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 21.2 to the next three releases – 21.3, 21.4 and 22.1 or downgrade to the previous three releases – 21.1, 20.4 and 20.3.

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, 21.2 is an EEOL release. Hence, you can upgrade from 21.2 to the next two EEOL releases – 21.4 and 22.2 or downgrade to the previous two EEOL releases – 20.4 and 20.2.

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
Standard End of Life (EOL)	24 months	End of Engineering + 6 months	Yes	No
Extended End of Life (EEOL)	60 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 SRX Series

IN THIS SECTION

What's New

IN THIS SECTION

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

To view features supported on the SRX platforms, view the Feature Explorer using the following links. To see which features were added in Junos OS Release 23.2R1, click the Group by Release link. You can collapse and expand the list as needed.

- SRX300
- SRX320
- SRX340
- SRX345
- SRX380
- SRX550 HM

- SRX1500
- SRX4100
- SRX4200
- SRX4600
- SRX5400
- SRX5600
- SRX5800

Authentication and Access Control

- **JIMS support FQDN as primary and secondary address (SRX1500, SRX4100, SRX4200, SRX4600, SRX5400, SRX5600, SRX5800, and vSRX3.0)**—Starting in Junos OS Release 23.2R1, you can get Fully Qualified Domain Names (FQDN) as primary & secondary support where each FQDN can have several entries per FQDN resolving one or more JIMS server for resilience purpose at `edit services user-identification identity-management connection (primary | secondary) address` hierarchy level.
  [See identity-management.]

- **JIMS support Junos PKI infrastructure (SRX1500, SRX4100, SRX4200, SRX4600, SRX5400, SRX5600, SRX5800, and vSRX3.0)**—Starting in Junos OS Release 23.2R1, you configure ca-profile under `set security pki` and assign `ca-profile` under JIMS by using `ca-profile` option at the `edit services user-identification identity-management connection (primary | secondary)` hierarchy level. You can perform CRL and OCSP checks based on settings under `set security pki` for the corresponding ca-profile.

  With the introduction of a new `ca-profile`, we will deprecate the existing `ca-certificate` option at the `edit services user-identification identity-management connection (primary | secondary)` hierarchy level.

  [See identity-management.]

Chassis Cluster-specific

- **Monitoring support for control links**(SRX5400, SRX5600, and SRX5800)—Starting in Junos OS Release 23.2R1, you can better maintain a chassis cluster by reviewing control port information. You can view information about high availability (HA) control port 0—a small form-factor pluggable (SFP) port on the Switch Control Board (SCB) card—of the local node in a chassis cluster.

  [See show-chassis-scb-ha-port .]

Flow-based and Packet-based Processing

- **Service Offload (SOF) Out Of Order (OOO) Detection for TCP Traffic (SRX4600, SRX5400, SRX5600, and SRX5800)**—Starting in Junos OS Release 23.2R1, we support out- of-order packet (OOO) detection for TCP connections in midstream traffic during service offload (SOF) switchover.

  The OOO packet detection allows you to configure a TCP sequence threshold value for accepting OOO packets to allow SOF switchover. As long as the calculated OOO packet numbers are lower than the configured threshold, SOF takes effect immediately. If the calculated OOO packet numbers are greater than the configured threshold value, the packets are still forwarded to the SPU for processing. By default, the OOO detection feature is disabled. To enable the feature, use the `tcp-session-install-interval` and `tcp-seq-ooo-window` commands in the `[edit security forwarding-options services-offload]` hierarchy. The `tcp-seq-ooo-window` command is mandatory in the configuration.

  [See TCP Sessions.]

High Availability

- **Dynamic routing protocol support for IPsec VPN in Multinode High Availability (SRX1500, SRX4100, SRX4200, SRX4600, SRX5400, SRX5600, SRX5800, and vSRX3.0)**—Starting in Junos OS Release 23.2R1, you can enable dynamic routing protocols for IPsec VPN in a Multinode High Availability setup by configuring `node-local` tunnels.

  To configure node-local tunnels, you must specify the `set security ike gateway <name> node-local` statement in the IKE gateway configuration on both the SRX Series Firewalls in a Multinode High Availability setup.

  With dynamic routing protocols, you can add and remove IP prefixes in the network and automatically redistribute the prefixes to the network peers without changing the traffic selector configuration.

  See [IPsec VPN Support in Multinode High Availability].

J-Web

- **Support for allowed groups in LDAP (SRX1500, SRX4100, SRX4200, SRX4600, SRX5400, SRX5600, SRX5800, and vSRX3.0)**—Starting in Junos OS Release 23.2R1, J-Web supports **Allowed Groups** under the **LDAP** option in this navigation path: **Security Services** > **Firewall Authentication** > **Access Profile** > **Create Access Profile**. You can now configure groups that are allowed to sign in.

  [See Add an Access Profile.]

- **Support for LDAP (SRX1500, SRX4100, SRX4200, SRX4600, SRX5400, SRX5600, SRX5800, and vSRX3.0)**—Starting in Junos OS Release 23.2R1, J-Web supports the **LDAP** option in this navigation path: **Network** > **VPN** > **IPsec VPN** > **Create VPN** > **Remote Access** > **Juniper Secure Connect** > **Local Gateway**. Using LDAP, you can configure user authentication for an access profile.

[See Create a Remote Access VPN—Juniper Secure Connect and Add an Access Profile.]

- **Support for system logs (SRX1500, SRX4100, SRX4200, SRX4600, SRX5400, SRX5600, SRX5800, and vSRX3.0)**—Starting in Junos OS Release 23.2R1, we've added a new sub-menu, **System**, under the **Monitor** menu. From this sub-menu, you can navigate to monitor information about system events such as routine operations, failure and error conditions, and emergency or critical conditions.

  [See Monitor System.]

- **Support for compliance rules (SRX1500, SRX4100, SRX4200, SRX4600, SRX5400, SRX5600, SRX5800, and vSRX3.0)**—Starting in Junos OS Release 23.2R1:

  - We've added a new sub-menu, **Compliance**, under the **Network** menu. Use this sub-menu to create remote access pre-logon compliance policies in the SRX Series Firewall. You can associate only one compliance policy for a remote access connection profile. The Juniper Secure Connect application sends details to the SRX Series Firewall. The device performs pre-logon compliance checks and accepts or rejects a connection based on the pre-logon compliance rule match.

  - J-Web supports **Compliance** option under **Network** > **VPN** > **IPsec VPN** > **Create VPN** > **Remote Access** > **Juniper Secure Connect** > **Remote User**. Use this option to associate only one compliance rule for a remote access connection profile.

  [See About the Compliance Page and Create a Remote Access VPN—Juniper Secure Connect.]

- **Support for multiple device access (SRX1500, SRX4100, SRX4200, SRX4600, SRX5400, SRX5600, SRX5800, and vSRX3.0)**—Starting in Junos OS Release 23.2R1, you can now connect to the firewall from multiple devices at the same time. To enable multiple device user access through J-Web, navigate to **Network** > **VPN** > **IPsec VPN** > **Create VPN** > **Remote Access** > **Juniper Secure Connect** > **Remote User** > **Multi Device Access**.

  For configuring multiple device user access, ensure each of the remote devices (computers or smart devices) has a unique hostname.

  [See Create a Remote Access VPN—Juniper Secure Connect.]

- **Support for application bypass (SRX1500, SRX4100, SRX4200, SRX4600, SRX5400, SRX5600, SRX5800, and vSRX3.0)**—Starting in Junos OS Release 23.2R1, J-Web supports **Application Bypass** available in this path: **Network** > **VPN** > **IPsec VPN** > **Create VPN** > **Remote Access** > **Juniper Secure Connect** > **Remote User**. You can define Juniper Secure Connect remote client configuration parameters to bypass certain applications. Bypassing is based on domain names and protocols without passing through the remote access VPN tunnel. Administrator configures these parameters on the SRX Series Firewall which are pushed to client application after successful authentication.

  [See Create a Remote Access VPN—Juniper Secure Connect.]

Juniper Advanced Threat Prevention Cloud (ATP Cloud)

- **Support to delete a single country code from GeoIP-based dynamic addresses (SRX1500,SRX4100, SRX4200, SRX4600, SRX5400, SRX5600, SRX5800, and vSRX3.0)**—Starting in Junos OS Release 23.2R1, you can delete a single country code from an IP-based geolocation (GeoIP)–Dynamic Address Entry (DAE) configuration.

  In previous releases, when you delete a single country code from a GeoIP DAE, the SRX Series Firewall deletes all the country names, and then adds them back except the country code that you deleted. Now, you can use the same command to delete the country code. The SRX Series Firewall deletes the IP ranges related to the given country code only, without affecting the IP ranges of other countries.

  We've also updated the `show security dynamic-address` command to display the country code appended to the IP-based geolocation name.

  See [Configuring Juniper Advanced Threat Prevention Cloud With Geolocation IP].

Network Management and Monitoring

- **Support protobuf format**—Starting in Junos OS Release 23.2R1, Juniper Networks® SRX Series Firewalls support protocol buffers (protobuf) format to encode the security log. SRX Series Firewalls send the encoded security log to the target device. The logs are saved on the target and decoded for readability.

  The primary purpose of protobuf is to reduce the size of stream logs (compared to syslog and sd-syslog) and increase the events per second (EPS) ratings with the log server.

  [See Configure Protobuf Security Log Files.]

Platform and Infrastructure

- **Support for dynamic update of trusted CA bundle (SRX1500, SRX4100, SRX4200, SRX4600, SRX5400, SRX5600, SRX5800, vSRX 3.0 and NFX350)**—Starting in Junos OS Release 23.2R1, we support the dynamic update of default trusted CA certificates. With this feature, you have the latest list of default trusted CA certificates on Junos OS devices. You can easily download, install, and update the certificate bundle periodically.

  [See Dynamic Update of Trusted CA Certificates.]

Unified Threat Management (UTM)

- **Support for cache Preload for EWF (cSRX, SRX1500, SRX4100, SRX4200, SRX4600, SRX5400, SRX5600, SRX5800, and vSRX3.0)**—Starting in Junos OS Release 23.2R1, we support preloading of cache with the top-rated, frequently visited URL list along with the classification information at the system startup stage. This feature is useful if your Internet connect is slow and you experience high latency while accessing the Web due to the remote categorization service.

Because the Web-filter policy decision is based on the URL category information that is preloaded in the cache, you do not experience a lag even when you make the first request.

See [Enhanced Web Filtering]

- **Support for intelligent Web filtering profile selection (cSRX, SRX1500, SRX4100, SRX4200, SRX4600, SRX5400, SRX5600, SRX5800, and vSRX3.0)**—Starting in Junos OS Release 23.2R1, dynamic app information from Juniper Networks Deep Packet Inspection (JDPI) is used to retrieve policy information before the final policy match occurs. The Web filter profile is updated again after the final policy selection, based on the final application match.

  The Content Security profile that is retrieved based on the dynamic app information is more accurate than applying the default profile, which was the earlier approach.

  [See See Web Filtering]

VPNs

- **Support for dynamic update of trusted CA bundle (SRX1500, SRX4100, SRX4200, SRX4600, SRX5400, SRX5600, SRX5800, vSRX 3.0 and NFX350)**—Starting in Junos OS Release 23.2R1, we support the dynamic update of default trusted CA certificates. With this feature, you have the latest list of default trusted CA certificates on Junos OS devices. You can easily download, install, and update the certificate bundle periodically.

  [See Dynamic Update of Trusted CA Certificates.]

- **Support for additional platform for cryptographic acceleration techniques (SRX1500, SRX4100, SRX4200, SRX4600)**—Starting in Junos OS Release 23.2R1, the SRX Series Firewalls (SRX1500, SRX4100, SRX4200, SRX4600) offload the DH, ECDH and ECDSA cryptographic operations to the hardware cryptographic engine. We already support these operations on SRX5000 line of devices and vSRX 3.0. The SRX5000 line of devices continue to offload the cryptographic operations to the hardware cryptographic engine whereas the vSRX Virtual Firewall continues to offload these operations to a data plane CPU thread. This feature requires that the `junos-ike` package is installed on all the devices.

  [See Cryptographic acceleration support on SRX5K-SPC3 Card, SRX mid-range platforms and vSRX Virtual Firewall.]

What's Changed

IN THIS SECTION

Learn about what changed in this release for SRX Series.

Network Management and Monitoring

- **Changes to the `show system yang package` (`get-system-yang-packages` RPC) XML output (ACX Series, EX Series, MX Series, QFX Series, SRX Series, vMX, and vSRX)**—The `show system yang package` command and `<get-system-yang-packages>` RPC include the following changes to the XML output:
  - The root element is `yang-package-information` instead of `yang-pkgs-info`.
  - A `yang-package` element encloses each set of package files.
  - The `yang-pkg-id` tag is renamed to `package-id`.
  - If the package does not contain translation scripts, the Translation Script(s) (`trans-scripts`) value is `none`.
- **NETCONF server's `<rpc-error>` response changed when `<load-configuration>` uses `operation="delete"` to delete a nonexistent configuration object (ACX Series, EX Series, MX Series, QFX Series, SRX Series, vMX, and vSRX)**—In an earlier release, we changed the NETCONF server's `<rpc-error>` response for when an `<edit-config>` or `<load-configuration>` operation uses `operation="delete"` to delete a configuration element that is absent in the target configuration. We've reverted the changes to the `<load-configuration>` response.
- **Changes to the RPC response for `<validate>` operations in RFC-compliant NETCONF sessions (ACX Series, EX Series, MX Series, QFX Series, SRX Series, vMX, and vSRX)**—When you configure the `rfc-compliant` statement at the `[edit system services netconf]` hierarchy level, the NETCONF server emits only an `<ok/>` or `<rpc-error>` element in response to `<validate>` operations. In earlier releases, the RPC reply also includes the `<commit-results>` element.

Platform and Infrastructure

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

Routing Policy and Firewall Filters

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

Known Limitations

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

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

Infrastructure

- When upgrading from releases before Junos OS Release 21.2 to Junos OS Release 21.2 and onward, validation and upgrade might fail. The upgrade requires using the no-validate option to complete successfully. https://kb.juniper.net/TSB18251. PR1568757
- On SRX380, the autonegotiation status on the 1G or 10G ports may be incorrectly displayed as Incomplete. This has no impact to traffic. PR1703002
- BCM5342X SOC port configurations, BCM53426 don't have QSGMII interface. Only the QSGMII port supports half-duplex mode. SRX340 and SRX345 have only SGMII interface, hence half-duplex is not supported. PR1716094

Open Issues

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

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

Infrastructure

- SRX550HM interfaces LED of ge-0/0/6-9 will auto turn off after device bootup some minutes.PR1634965
- Earlier implementation of kvmclock with vDSO which helps avoid the system call overhead for user space applications had problem of time drift, the latest set of changes takes care of initializing the clock after all auxiliary processors are launched so that the clock initialization is accurate.PR1691036
- FIPS mode is not supported in this release for SRX SME devices.PR1697999
- Mount Command from Shell mode is not supported for nfs in BSD12 based SRX320, SRX300, SRX345, SRX340, and SRX380 platforms. PR1701361
- On SRX platforms, log streaming to the Juniper Security Director Cloud fails on TLS when DNS re-query is performed.PR1708116
- For case when input traffic is more and output traffic is expected equal to maximum capacity of egress interface, please set the shaping explicitly equal to interface maximum capacity if default shaping does not work. PR1712964

- On SRX platforms, Interface speed stays 100Mbps when removing speed and duplex command separately. PR1715247
- In DNS response packets from the DNS server, the DNS flags do not have RA (Recursion Available) enabled. SRX discovers that this RA flag is disabled, and processes it as an error. The SRX then sends another DNS query to the second DNS server.PR1716171
- On SRX4600 and SRX5K platforms, the L2 channel error counter will increase when some unknown family packets received by interfaces.PR1729284

J-Web

- Certificate Management issues. As a workaround, you can use CLI to create, delete, or re-enroll certificates. PR1738316

VPNs

- Tunnel debugging configuration is not synchronized to the backup node. It needs to be configured again after RG0 failover. PR1450393
- First time when we add this command the existing active connections are not changed, only the new connection after this command will be taken into effect. PR1608715

Resolved Issues

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

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

Application Layer Gateways (ALGs)

- H.323 traffic failure caused by RAS packet drops when incorrect route lookup performed. PR1688986
- The first FTPS session will not work on SRX5000 line leading to a traffic drop.PR1715918
- SIP ALG not working and traffic is dropped. PR1728638

Authentication and Access Control

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

Chassis Clustering

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

Class of Service (CoS)

- QoS scheduler map incorrect when using wildcard interface configuration: " interface unit * " starting with Junos OS Release 21.1. PR1734013

Flow-Based and Packet-Based Processing

- VPN logs in monitor hierarchy on J-Web not being seen. PR1691095
- Packet loss is observed for IPsec sessions when PMI is enabled. PR1692885
- The core files are generated when user is changing interface configuration. PR1704623
- A flowd process stops on SRX4100, SRX4200, SRX4600, vSRX, and SRX5000 line with SPC3 card when a route is changed frequently. PR1705996
- The IPv6 source-level fragmented SCTP packets passing through an IPsec tunnel will be dropped. PR1708876
- The traffic will fail when accessing the routing instance interface IP from external IP. PR1719437
- IPv6 Neighbor Discovery is failing on VLAN tagging interface. PR1720570

General Routing

- Security log verification is failing as the contents of binary log file in logical systems are not as expected. PR1587360
- SRX4600 packet drop or srxpfe generates core files. PR1620773
- BGP down due to BFD expired; failover restored services. PR1630981
- On SRX5600 and SRX5800, the SNMP MIB queries may result in occasional response timeouts. PR1631149

- IMAP or IMAPS email permitted counter is not incremented in AAMW email statistics while testing whole email block. PR1646661
- No system or chassis alarm will be seen when device booting from backup partition. PR1646943
- The show fwauth user details is not displaying group information. PR1659115
- SRX4600 HA might not failover properly due to a hardware failure. PR1683213
- On all Junos logical systems the RPD process stops due to JET client invoking RPC handled by RPD process. PR1692738
- IPsec tunnel is not getting established back after the execution of clear security ike sa command. PR1694604
- TCP packet drops are seen when services-offload is enabled. PR1702138
- The flowd process stops and generates core files when TLS 1.3 session ticket is received on SSL-I. PR1705044
- Unable to onboard SRX on a Yang based Orchestrator. PR1705679
- TX would be stuck and no packet can be transferred by the SPC3 card. PR1706756
- Setting the security log profile without a category or stream will lead to srxpfe process stops. PR1708777
- The ECDSA certificate based websites are not accessible when the SSL proxy is enabled from Junos OS Release 22.1R1 onwards. PR1709386
- SRX4600 doesn't support aggregated Ethernet interfaces. PR1711467
- The targeted-broadcast feature will not work on some SRX platforms. PR1711729
- Continuous vmcores observed on the secondary node when committing set system management-instance command. PR1712727
- The fabric link flapped which initiated a Packet Forwarding Engine pause. PR1713263
- RA can be sent in response to an invalid RS. PR1713485
- Continuous vmcores observed on the secondary node when committing the "set system management-instance" command. PR1713759
- The firewall web-authentication feature will not work after enabling Juniper secure connect. PR1714845
- The NSD process may report an error message. PR1715297

- The SSL session drops because of the wrong SNI value. PR1716893
- Errors seen under interfaces in slot0 option. PR1717095
- The srxpfe core has been seen on secondary SRX during ISSU. PR1717503
- The flowd process stops when the web proxy packet reinjection fails. PR1719703
- With SD-WAN configuration on SRX, flowd process generates core files if APBR rule is not attached to SLA. PR1719965
- Local route is not added in the secondary FIB and KRT queue is stuck. PR1721032
- Configuration download failing for FQDN style realm name + no default-profile knob with previous versions of Juniper Secure Connect client. PR1721631
- Nstraced process is running high on the primary node after the Junos OS upgrade. PR1727122

Interfaces and Chassis

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

Intrusion Detection and Prevention (IDP)

- Network outage caused during change in IDP policy. PR1705491

J-Web

- The address-book address-book name attach zone is unexpectedly removed when address-book entry is added or removed by J-Web. PR1712454
- Exclude selected is unexpectedly enabled in security policy configuration. PR1735314

Layer 2 Ethernet Services

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

Network Address Translation (NAT)

- ICMP based traceroute is not showing any hops after SRX when SRX is configured with NAT64. PR1706541

- Some sessions will not be deleted when the NAT rule is deleted from the system. PR1712738

Network Management and Monitoring

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

Platform and Infrastructure

- After RG0 failover, node priority are set to zero for node0 with relinquish monitoring failure. PR1670772
- The vmcores can be seen on SRX5000 line when the fxp0 interface is configured under management-instance. PR1714002

Routing Policy and Firewall Filters

- Packet drops are seen for SRX destined traffic with self-traffic-policy. PR1698021
- Security policies go out of synchronize during ISSU. PR1698508
- The flowd process stops when the security policy updated with changing IP address related to the FQDN. PR1713576
- The NSD process stops when ISSU is performed on the cluster. PR1724777
- Traffic impact is observed when the security policy is configured with a huge number of addresses and on addition or deletion of these policies. PR1725567

Routing Protocols

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

Unified Threat Management (UTM)

- utmd core has seen at commit when *.* or *.*.* is configured at url-pattern. PR1715260
- Memory leak is observed on all Junos SRX platforms with http-persist and http-reassembly configuration. PR1725359

User Interface and Configuration

- The mustd process crash might be observed with persist-group-inheritance. PR1638847

VPNs

- Routes flapping when configuration changes are applied to custom routing instance. PR1654516
- IKE cookies didn't change in rekey lifetime expire cases after manual failover. PR1690921
- IPsec VPNs will disconnect after ISSU. PR1696102
- Cold synchronize status of MNHA nodes may go into INCOMPLETE state after bootup. PR1710374
- The iked process stops when VPN tunnels parameters are not matching. PR1716092
- ISSU is aborted and flowd process pause is observed. PR1722122

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.

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 sixty months after the first general availability date and customer support for an additional six more months.

NOTE: The sixty months of support for EEOL releases is introduced in Junos OS 23.2 release and is available for all later releases. For releases prior to 23.2, the support for EEOL releases continues to be thirty six 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 21.2 to the next three releases – 21.3, 21.4 and 22.1 or downgrade to the previous three releases – 21.1, 20.4 and 20.3.

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, 21.2 is an EEOL release. Hence, you can upgrade from 21.2 to the next two EEOL releases – 21.4 and 22.2 or downgrade to the previous two EEOL releases – 20.4 and 20.2.

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)	60 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

What's New

IN THIS SECTION

Learn about new features introduced in this release for vMX.

Junos Telemetry Interface

- **IS-IS configuration using OpenConfig (MX204, MX240, MX304, MX150, MX480, MX960, MX10003, MX10004, MX10008, MX10016, MX2008, MX2010, MX2020, and vMX)**—Junos OS Release 23.2R1 introduces support for new configuration paths based on OpenConfig data model **openconfig-isis.yang** version 1.0.0.

  See Mapping OpenConfig ISIS Commands to Junos Configuration.

- **Support for configuring the routing-instance and source address for each gRPC tunnel session (MX204, MX240, MX480, MX960, MX10003, MX10004, MX10008, MX10016, MX2008, MX2010, MX2020, VMX, and QFX5110)**—Starting with Junos OS Release 23.2R1, you can configure the routing instance and the source address for each gRPC remote procedure call (gRPC) tunnel session to dial out a connection to the tunnel server.

  To configure the routing instance, add the `routing-instance <routing-instance>` option and to configure the source address, add the `source-address <ip-address>` option in the `grpc-tunnel` configuration statement.

  If you do not configure a routing instance, the gRPC tunnel uses the default routing instance. If you do not configure the source address, the kernel picks the source address that can reach the tunnel server.

  [See gRPC Tunnels Overview and grpc-tunnel].

- **Telemetry streaming for IS-IS protocol based on OpenConfig data model (MX204, MX240, MX304, MX150, MX480, MX960, MX10003, MX10004, MX10008, MX10016, MX2008, MX2010, MX2020, and vMX)**—Starting in Junos OS Release 23.2R1, the data model for IS-IS is compliant with OpenConfig. The node type for **/network-instances/network-instance/protocols/protocol/** is defined as a list which contains user-configurable keys for the protocol name and identifier.

  [See Junos YANG Data Model Explorer.]

MPLS

- **Support for bound metrics and bandwidth for PCC Initiated/Delegated type LSPs (RSVP-TE and SR-TE) per RFC5440 (ACX5448, ACX5448-M, ACX5448-D, ACX710, MX204, MX240, MX304, MX150, MX480, MX960, MX10003, MX10004, MX10008, MX10016, MX2008, MX2010, MX2020, and vMX)**—Starting in Junos OS Release 23.2R1, we support metric object and bandwidth object for bounded constraints in a Path Computation Element Protocol (PCEP) connection for Segment Routing label-switched paths (SR-LSPs). Both metric object and bandwidth object are optional objects in PCEP, and can be present in PCInit, PCUpd, and PCRpt PCEP messages.

  To configure bounded metric values for an LSP controller, you can enter `igp-metric-bound <val> | te-metric-bound <val> | delay-metric-bound <val>` at the `[edit protocols mpls label-switched-path <lsp-name> lsp-external-controller controller-name]` hierarchy level.

  To configure bounded metric values for compute profiles, you can enter `bound-metric igp <val> | bound-metric te <val> | bound-metric delay <val>` at the `[edit protocols source-packet-routing compute-profile compute-profile-name]` hierarchy level.

  To use the maximum SR-MPLS segment identifier (SID) depth, use the `set protocols pcep maximum-srmpls-segment-list-depth <val>` configuration.

  To propogate the list, use the `set protocols pcep propagate-lsp-max-segment-list-depth` configuration.

[See lsp-external-controller, compute-profile, and pcep.]

- **Support to report bandwidth and reservation priority for delegated and PCE-initiated segment routing–traffic engineering (SR-TE) LSPs in Path Computation Element Protocol (ACX5448, ACX5448-M, ACX5448-D, ACX710, MX150, MX204, MX240, MX304, , MX480, MX960, MX2008, MX2010, MX2020, MX10003, MX10004, MX10008, MX10016, and vMX)**—Starting in Junos OS Release 23.2R1, we support the reporting of bandwidth and reservation priority for delegated segment routing–traffic engineering (SR-TE) label-switched paths (LSPs). For Path Computation Client (PCE)-initiated SR-TE LSPs, once the bandwidth, setup priority, and reservation priority request is received from the controller, the Path Computation Client (PCC) reports the same information to the controller.

  NOTE: You can configure bandwidth and reservation priority in PCC only for delegated SR-TE LSPs and not for undelegated and PCE-initiated SR-TE LSPs.

  To configure the `bandwidth-requested` and `bandwidth-reservation-priority` for delegated SR-TE LSPs, include the `bandwidth-requested | bandwidth-reservation-priority` configuration statement at the `[edit protocols source-packet-routing compute-profile` *`compute-profile-name`*`]` hierarchy level.

  [See Reporting Path Optimization Metrics in PCEP.]

Network Management and Monitoring

- **Support for ephemeral database cyclic versioning and resizing (MX240, MX480, MX960, MX2010, MX2020, MX10004, MX10008, MX10016, and vMX)**—Starting in Junos OS Release 23.2R1, Junos devices implement cyclic versioning and database resizing to more effectively manage the space used by the ephemeral configuration database. The cyclic version value defines the number of versions of an ephemeral database for which the system stores deleted configuration objects. During a commit operation, the system reclaims the space occupied by objects deleted in the previous database version relative to the current database version as determined by the cyclic version value. You can also configure the device to resize the database when its size exceeds certain thresholds. With effective space management, you can prevent the database from hitting the maximum database size and improve performance by reducing database fragmentation.

  [See Managing Ephemeral Configuration Database Space.]

Routing Protocols

- **Enhancements to show ospf spring and ospf database commands (MX240, MX480, MX960, MX2010, MX2020, and vMX)**— Starting in Junos OS Release 23.2R1, we have enhanced the `show ospf spring` and `show ospf database` commands to display the following additional segment-routing information:

- `show ospf spring sid-database`—Displays the segment identifier (SID) database with prefix and index of native segment routing nodes.
- `show ospf spring prefix-sid-map`—Displays segment routing mapping server (SRMS) advertisements
- `show ospf database opaque-area ext-link link-addr` *`link-address`*—Displays the specific extended-link link-state advertisements (LSAs) based on the link-address.
- `show ospf database opaque-area ext-prefix prefix` *`prefix/len`*—Displays the specific extended-prefix link-state advertisement based on the prefix

[See show ospf database, show-ospf-spring-sid-database], show-ospf-spring-prefix-sid-map.

What's Changed

IN THIS SECTION

Learn about what changed in this release for vMX.

Network Management and Monitoring

- **Changes to the `show system yang package` (`get-system-yang-packages` RPC) XML output (ACX Series, EX Series, MX Series, QFX Series, SRX Series, vMX, and vSRX)**—The `show system yang package` command and `<get-system-yang-packages>` RPC include the following changes to the XML output:
  - The root element is `yang-package-information` instead of `yang-pkgs-info`.
  - A `yang-package` element encloses each set of package files.
  - The `yang-pkg-id` tag is renamed to `package-id`.
  - If the package does not contain translation scripts, the Translation Script(s) (`trans-scripts`) value is `none`.
- **NETCONF server's `<rpc-error>` response changed when `<load-configuration>` uses `operation="delete"` to delete a nonexistent configuration object (ACX Series, EX Series, MX Series, QFX Series, SRX Series,**

vMX, and vSRX)—In an earlier release, we changed the NETCONF server's <rpc-error> response for when an <edit-config> or <load-configuration> operation uses operation="delete" to delete a configuration element that is absent in the target configuration. We've reverted the changes to the <load-configuration> response.

- **Changes to the RPC response for <validate> operations in RFC-compliant NETCONF sessions (ACX Series, EX Series, MX Series, QFX Series, SRX Series, vMX, and vSRX)**—When you configure the rfc-compliant statement at the [edit system services netconf] hierarchy level, the NETCONF server emits only an <ok/> or <rpc-error> element in response to <validate> operations. In earlier releases, the RPC reply also includes the <commit-results> element.

Known Limitations

There are no known limitations in hardware or software in this release for vMX.

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

Open Issues

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

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

Resolved Issues

IN THIS SECTION

Learn about the issues fixed in this release for vMX.

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

Platform and Infrastructure

- Traffic drop seen for some streams in intra-as srte color only IPv6 tunneling with sharding on VMX10008 and VMX304. PR1695669
- PFE syslog tags are missing for the command help syslog "^PFE_?". PR1707504
- Total LSP count mismatch on path computation client after PCCD restart. PR1714158

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.

Junos OS Release Notes for vRR

IN THIS SECTION

What's New

IN THIS SECTION

Learn about new features introduced in this release for vRR.

Junos Telemetry Interface

- **Upgrade of OpenConfig BGP models (MX480 and vRR)**—Junos OS Release 23.2R1 supports an upgrade for the following OpenConfig BGP models to version 9.1.0:

  - **openconfig-bgp-global.yang**
  - **openconfig-bgp-neighbor.yang**
  - **openconfig-bgp-peer-group.yang**

  The upgraded models introduce new leaves for operational state sensors and configuration.

  See Junos YANG Data Model Explorer for state sensors and Mapping OpenConfig BGP Commands to Junos Configuration for configuration.

- **Upgrade of OpenConfig BGP RIB models (ACX5448, ACX710, MX204, MX240, MX150, MX480, MX960, MX10003, MX10004, MX10008, MX10016, MX2008, MX2010, MX2020, vRR)**—Junos OS Release 23.2R1 supports operational state sensors based on the latest OpenConfig BGP RIB data models:

  - **openconfig-rib-bgp-attributes.yang (version 0.8.1)**
  - **openconfig-rib-bgp-ext.yang (version 0.6.0)**
  - **openconfig-rib-bgp-shared-attributes.yang (version 0.8.1)**
  - **openconfig-rib-bgp-table-attributes.yang (version 0.8.1)**
  - **openconfig-rib-bgp-tables.yang (version 0.8.1)**
  - **openconfig-rib-bgp-types.yang (version 0.5.0)**
  - **openconfig-rib-bgp.yang (version 0.8.1)**

The following model versions are no longer supported:

- **openconfig-rib-bgp-ext.yang (version 0.2.0)**
- **openconfig-rib-bgp-types.yang (version 0.2.0)**
- **openconfig-rib-bgp.yang (version 0.2.0)**

See Junos YANG Data Model Explorer.

Routing Protocols

- **Support to activate BFD strict mode for BGP peer sessions (ACX5448, ACX710, cRPD, MX10003, MX10004, VRR, QFX5110, and QFX5200)**—Starting in Junos OS Release 23.2R1, we support the activation of BFD strict mode for BGP peer sessions that disallows BGP to establish a session until BFD session is successfully established and has stabilized. With the BFD strict mode feature, you can prevent routing churn and minimize network interruption.

  To activate BFD strict mode for BGP peer sessions, include the `strict-mode [bfd-wait-timeout <10-255 seconds>` CLI statement under `bfd-liveness-detection` at the `[edit protocols bgp group` *`group-name`* `neighbor` *`address`*] hierarchy level.

  For example, use the following command to activate BFD strict mode for BGP peer sessions:

  `set protocol bgp group` *`group-name`* `neighbor` *`address`* `bfd-liveness-detection [strict-mode [bfd-wait-timeout` *`10-255 seconds`*`]]`

  [See Understanding BFD for BGP, bfd-liveness-detection (BGP).]

What's Changed

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

Known Limitations

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

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

To learn more about common BGP or routing known limitations in Junos OS 23.2R1, see "Known Limitations" on page 53 for MX Series routers.

Open Issues

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

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

Resolved Issues

Learn about the issues fixed in this release for vRR.

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

General Routing

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

Junos OS Release Notes for vSRX

IN THIS SECTION

What's New

IN THIS SECTION

Learn about new features introduced in this release for vSRX.

Authentication and Access Control

- **JIMS support FQDN as primary and secondary address (SRX1500, SRX4100, SRX4200, SRX4600, SRX5400, SRX5600, SRX5800, and vSRX3.0)**—Starting in Junos OS Release 23.2R1, you can get Fully Qualified Domain Names (FQDN) as primary & secondary support where each FQDN can have several entries per FQDN resolving one or more JIMS server for resilience purpose at `edit services user-identification identity-management connection (primary | secondary) address` hierarchy level.
  [See identity-management.]

- **JIMS support Junos PKI infrastructure (SRX1500, SRX4100, SRX4200, SRX4600, SRX5400, SRX5600, SRX5800, and vSRX3.0)**—Starting in Junos OS Release 23.2R1, you configure ca-profile under `set security pki` and assign `ca-profile` under JIMS by using `ca-profile` option at the `edit services user-identification identity-management connection (primary | secondary)` hierarchy level. You can perform CRL and OCSP checks based on settings under `set security pki` for the corresponding ca-profile.

  With the introduction of a new `ca-profile`, we will deprecate the existing `ca-certificate` option at the `edit services user-identification identity-management connection (primary | secondary)` hierarchy level.

  [See identity-management.]

High Availability

- **Dynamic routing protocol support for IPsec VPN in Multinode High Availability (SRX1500, SRX4100, SRX4200, SRX4600, SRX5400, SRX5600, SRX5800, and vSRX3.0)**—Starting in Junos OS Release

23.2R1, you can enable dynamic routing protocols for IPsec VPN in a Multinode High Availability setup by configuring `node-local` tunnels.

To configure node-local tunnels, you must specify the `set security ike gateway <name> node-local` statement in the IKE gateway configuration on both the SRX Series Firewalls in a Multinode High Availability setup.

With dynamic routing protocols, you can add and remove IP prefixes in the network and automatically redistribute the prefixes to the network peers without changing the traffic selector configuration.

See [IPsec VPN Support in Multinode High Availability].

J-Web

- **Support for allowed groups in LDAP (SRX1500, SRX4100, SRX4200, SRX4600, SRX5400, SRX5600, SRX5800, and vSRX3.0)**—Starting in Junos OS Release 23.2R1, J-Web supports **Allowed Groups** under the **LDAP** option in this navigation path: **Security Services** > **Firewall Authentication** > **Access Profile** > **Create Access Profile**. You can now configure groups that are allowed to sign in.

  [See Add an Access Profile.]

- **Support for LDAP (SRX1500, SRX4100, SRX4200, SRX4600, SRX5400, SRX5600, SRX5800, and vSRX3.0)**—Starting in Junos OS Release 23.2R1, J-Web supports the **LDAP** option in this navigation path: **Network** > **VPN** > **IPsec VPN** > **Create VPN** > **Remote Access** > **Juniper Secure Connect** > **Local Gateway**. Using LDAP, you can configure user authentication for an access profile.

  [See Create a Remote Access VPN—Juniper Secure Connect and Add an Access Profile.]

- **Support for compliance rules (SRX1500, SRX4100, SRX4200, SRX4600, SRX5400, SRX5600, SRX5800, and vSRX3.0)**—Starting in Junos OS Release 23.2R1:

  - We've added a new sub-menu, **Compliance**, under the **Network** menu. Use this sub-menu to create remote access pre-logon compliance policies in the SRX Series Firewall. You can associate only one compliance policy for a remote access connection profile. The Juniper Secure Connect application sends details to the SRX Series Firewall. The device performs pre-logon compliance checks and accepts or rejects a connection based on the pre-logon compliance rule match.

  - J-Web supports **Compliance** option under **Network** > **VPN** > **IPsec VPN** > **Create VPN** > **Remote Access** > **Juniper Secure Connect** > **Remote User**. Use this option to associate only one compliance rule for a remote access connection profile.

  [See About the Compliance Page and Create a Remote Access VPN—Juniper Secure Connect.]

- **Support for multiple device access (SRX1500, SRX4100, SRX4200, SRX4600, SRX5400, SRX5600, SRX5800, and vSRX3.0)**—Starting in Junos OS Release 23.2R1, you can now connect to the firewall from multiple devices at the same time. To enable multiple device user access through J-Web,

navigate to **Network** > **VPN** > **IPsec VPN** > **Create VPN** > **Remote Access** > **Juniper Secure Connect** > **Remote User** > **Multi Device Access**.

For configuring multiple device user access, ensure each of the remote devices (computers or smart devices) has a unique hostname.

[See Create a Remote Access VPN—Juniper Secure Connect.]

- **Support for application bypass (SRX1500, SRX4100, SRX4200, SRX4600, SRX5400, SRX5600, SRX5800, and vSRX3.0)**—Starting in Junos OS Release 23.2R1, J-Web supports **Application Bypass** available in this path: **Network** > **VPN** > **IPsec VPN** > **Create VPN** > **Remote Access** > **Juniper Secure Connect** > **Remote User**. You can define Juniper Secure Connect remote client configuration parameters to bypass certain applications. Bypassing is based on domain names and protocols without passing through the remote access VPN tunnel. Administrator configures these parameters on the SRX Series Firewall which are pushed to client application after successful authentication.

  [See Create a Remote Access VPN—Juniper Secure Connect.]

Juniper Advanced Threat Prevention Cloud (ATP Cloud)

- **Support to delete a single country code from GeoIP-based dynamic addresses (SRX1500,SRX4100, SRX4200, SRX4600, SRX5400, SRX5600, SRX5800, and vSRX3.0)**—Starting in Junos OS Release 23.2R1, you can delete a single country code from an IP-based geolocation (GeoIP)–Dynamic Address Entry (DAE) configuration.

  In previous releases, when you delete a single country code from a GeoIP DAE, the SRX Series Firewall deletes all the country names, and then adds them back except the country code that you deleted. Now, you can use the same command to delete the country code. The SRX Series Firewall deletes the IP ranges related to the given country code only, without affecting the IP ranges of other countries.

  We've also updated the `show security dynamic-address` command to display the country code appended to the IP-based geolocation name.

  See [Configuring Juniper Advanced Threat Prevention Cloud With Geolocation IP].

Network Management and Monitoring

- **Support protobuf format**—Starting in Junos OS Release 23.2R1, Juniper Networks® SRX Series Firewalls support protocol buffers (protobuf) format to encode the security log. SRX Series Firewalls send the encoded security log to the target device. The logs are saved on the target and decoded for readability.

  The primary purpose of protobuf is to reduce the size of stream logs (compared to syslog and sd-syslog) and increase the events per second (EPS) ratings with the log server.

  [See Configure Protobuf Security Log Files.]

Platform and Infrastructure

- **Support for Geneve flow infrastructure with AWS GWLB (vSRX 3.0)** —Starting in Junos OS Release 23.2R1, you can integrate vSRX Virtual Firewall (vSRX) 3.0 with Amazon Web Services (AWS) Gateway Load Balancer (GWLB) service that uses the Geneve protocol encapsulation for transparent routing of packets between GWLB and virtual appliances.

  With this feaure, you can use vSRX 3.0 as a transit router or a tunnel endpoint device in various cloud deployments.

  [See Geneve Flow Infrastructure on vSRX 3.0 and AWS Gateway Load Balancing with Geneve.]

- **Support for dynamic update of trusted CA bundle (SRX1500, SRX4100, SRX4200, SRX4600, SRX5400, SRX5600, SRX5800, vSRX 3.0 and NFX350)**—Starting in Junos OS Release 23.2R1, we support the dynamic update of default trusted CA certificates. With this feature, you have the latest list of default trusted CA certificates on Junos OS devices. You can easily download, install, and update the certificate bundle periodically.

  [See Dynamic Update of Trusted CA Certificates.]

Unified Threat Management (UTM)

- **Support for cache Preload for EWF (cSRX, SRX1500, SRX4100, SRX4200, SRX4600, SRX5400, SRX5600, SRX5800, and vSRX3.0)**—Starting in Junos OS Release 23.2R1, we support preloading of cache with the top-rated, frequently visited URL list along with the classification information at the system startup stage. This feature is useful if your Internet connect is slow and you experience high latency while accessing the Web due to the remote categorization service.

  Because the Web-filter policy decision is based on the URL category information that is preloaded in the cache, you do not experience a lag even when you make the first request.

  See [Enhanced Web Filtering]

- **Support for intelligent Web filtering profile selection (cSRX, SRX1500, SRX4100, SRX4200, SRX4600, SRX5400, SRX5600, SRX5800, and vSRX3.0)**—Starting in Junos OS Release 23.2R1, dynamic app information from Juniper Networks Deep Packet Inspection (JDPI) is used to retrieve policy information before the final policy match occurs. The Web filter profile is updated again after the final policy selection, based on the final application match.

  The Content Security profile that is retrieved based on the dynamic app information is more accurate than applying the default profile, which was the earlier approach.

  [See See Web Filtering]

VPNs

- **Support for dynamic update of trusted CA bundle (SRX1500, SRX4100, SRX4200, SRX4600, SRX5400, SRX5600, SRX5800, vSRX 3.0 and NFX350)**—Starting in Junos OS Release 23.2R1, we support the dynamic update of default trusted CA certificates. With this feature, you have the latest list of default trusted CA certificates on Junos OS devices. You can easily download, install, and update the certificate bundle periodically.

  [See Dynamic Update of Trusted CA Certificates.]

What's Changed

IN THIS SECTION

Learn about what changed in this release for vSRX.

Network Management and Monitoring

- **Changes to the `show system yang package` (`get-system-yang-packages` RPC) XML output (ACX Series, EX Series, MX Series, QFX Series, SRX Series, vMX, and vSRX)**—The `show system yang package` command and `<get-system-yang-packages>` RPC include the following changes to the XML output:

  - The root element is `yang-package-information` instead of `yang-pkgs-info`.
  - A `yang-package` element encloses each set of package files.
  - The `yang-pkg-id` tag is renamed to `package-id`.
  - If the package does not contain translation scripts, the Translation Script(s) (`trans-scripts`) value is `none`.

- **NETCONF server's `<rpc-error>` response changed when `<load-configuration>` uses `operation="delete"` to delete a nonexistent configuration object (ACX Series, EX Series, MX Series, QFX Series, SRX Series,**

vMX, and vSRX)—In an earlier release, we changed the NETCONF server's <rpc-error> response for when an <edit-config> or <load-configuration> operation uses operation="delete" to delete a configuration element that is absent in the target configuration. We've reverted the changes to the <load-configuration> response.

- **Changes to the RPC response for <validate> operations in RFC-compliant NETCONF sessions (ACX Series, EX Series, MX Series, QFX Series, SRX Series, vMX, and vSRX)**—When you configure the rfc-compliant statement at the [edit system services netconf] hierarchy level, the NETCONF server emits only an <ok/> or <rpc-error> element in response to <validate> operations. In earlier releases, the RPC reply also includes the <commit-results> element.

Platform and Infrastructure

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

Routing Policy and Firewall Filters

- **Syslogs to capture commit warning messages related to traffic loss prevention over VPN (SRX Series, vSRX, and NFX Series)**—Configuration commit warnings such as warning: Policy 'traditional' does not

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

Known Limitations

There are no known limitations in hardware or software in this release for vSRX.

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

Open Issues

Learn about open issues in this release for vSRX.

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

Infrastructure

- Earlier implementation of kvmclock with vDSO which helps avoid the system call overhead for user space applications had problem of time drift, the latest set of changes takes care of initializing the clock after all auxiliary processors are launched so that the clock initialization is accurate.PR1691036
- On SRX platforms, log streaming to the security director cloud fails on TLS when DNS re-query is performed. PR1708116
- In DNS response packets from the DNS server, the DNS flags do not have RA enabled. SRX discovers that this RA flag is disabled, and processes it as an error. The SRX then sends another DNS query to the second DNS server. PR1716171

Resolved Issues

Learn about the issues fixed in this release for vSRX.

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

Application Layer Gateways (ALGs)

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

Chassis Clustering

- Traffic loss after RG1 failover. PR1726753

Flow-Based and Packet-Based Processing

- When PMI mode is enabled, Uplink-incoming-interface-name not updated properly though link switch is successful by APBR as well as symmetric routing maintained. PR1692062
- High latency and packet drops will be observed with the transmit-rate exact option enabled for one or more schedulers of an IFL or IFD. PR1692559
- Packet loss is observed for IPsec sessions when PMI is enabled. PR1692885
- Packets are dropped because flow sessions will not be created for the MPLS routed traffic. PR1703678
- TCP session timeout seen on GRE tunnel. PR1708646
- The inet6 packet mode drops traffic significantly compared to the flow mode. PR1733819

Platform and Infrastructure

- VLAN tagging does not work for vSRX3.0 on HyperV Windows Server 2019 Datacenter. PR1711440
- RSI does not collect PFE related commands on vSRX3.0 in chassis cluster. PR1711733
- Multiple useridd core seen while upgrading to latest image with userid configuration. PR1717276
- The flowd process pause is observed when the web proxy packet reinjection fails. PR1719703
- Configuration download failing for FQDN style realm name and no default-profile knob with previous versions of Juniper Secure Connect client. PR1721631
- Unable to Connect Sky ATP. PR1727437

Services Applications

- Flowd process generates core files when type 5 EVPN is configured. PR1704061

VPNs

- Change in few fields of IKE_VPN_UP_ALARM_USER and IKE_VPN_DOWN_ALARM_USER syslogs of IKED. PR1657704
- IPsec VPNs will disconnect after ISSU. PR1696102

Migration, Upgrade, and Downgrade Instructions

IN THIS SECTION

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

You also can upgrade to Junos OS Release 23.2R1 for vSRX using J-Web (see J-Web) or the Junos Space Network Management Platform (see Junos Space).

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 21.1R1 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 21.1R1 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-x86-64-20.4-2020-10-12.0_RELEASE_20.4_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-
x86-64-20.4-2020-10-12.0_RELEASE_20.4_THROTTLE.tgz no-copy no-validate reboot
Verified junos-vsrx-x86-64-20.4-2020-10-12.0_RELEASE_20.4_THROTTLE signed by
PackageDevelopmentEc_2017 method ECDSA256+SHA256
THIS IS A SIGNED PACKAGE
WARNING:     This package will load JUNOS 20.4 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-20.4-2020-10-12.0_RELEASE_20.4_THROTTLE.tgz
Extracting the package ...
total 975372
-rw-r--r-- 1 30426 950 710337073 Oct 19 17:31 junos-srx-mr-
vsrx-20.4-2020-10-12.0_RELEASE_20.4_THROTTLE-app.tgz
-rw-r--r-- 1 30426 950 288433266 Oct 19 17:31 junos-srx-mr-
vsrx-20.4-2020-10-12.0_RELEASE_20.4_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-20.4-2020-10-12.0_RELEASE_20.4_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-20.4-2020-10-12.0_RELEASE_20.4_THROTTLE-linux.tgz ...
upgrade_platform: Input package /var/tmp/junos-srx-mr-
vsrx-20.4-2020-10-12.0_RELEASE_20.4_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-20.4-2020-10-12.0_RELEASE_20.4_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-20.4-2020-10-12.0_RELEASE_20.4_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 21.1R1 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 20.4-2020-10-12.0_RELEASE_20.4_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: 20.4-2020-10-12.0_RELEASE_20.4_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 sixty months after the first general availability date and customer support for an additional six more months.

> **NOTE:** The sixty months of support for EEOL releases is introduced in Junos OS 23.2 release and is available for all later releases. For releases prior to 23.2, the support for EEOL releases continues to be thirty six 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 21.2 to the next three releases – 21.3, 21.4 and 22.1 or downgrade to the previous three releases – 21.1, 20.4 and 20.3.

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, 21.2 is an EEOL release. Hence, you can upgrade from 21.2 to the next two EEOL releases – 21.4 and 22.2 or downgrade to the previous two EEOL releases – 20.4 and 20.2.

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)	60 months	End of Engineering + 6 months	Yes	Yes

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

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

Licensing

In 2020, Juniper Networks introduced a new software licensing model. The Juniper Flex Program comprises a framework, a set of policies, and various tools that help unify and thereby simplify the

multiple product-driven licensing and packaging approaches that Juniper Networks has developed over the past several years.

The major components of the framework are:

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

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

Finding More Information

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

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

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

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

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

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

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

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

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

Requesting Technical Support

IN THIS SECTION

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

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

Self-Help Online Tools and Resources

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

- Find CSC offerings: https://www.juniper.net/customers/support/
- Search for known bugs: https://prsearch.juniper.net/
- Find product documentation: https://www.juniper.net/documentation/
- Find solutions and answer questions using our Knowledge Base: https://kb.juniper.net/
- Download the latest versions of software and review release notes: https://www.juniper.net/customers/csc/software/

- Search technical bulletins for relevant hardware and software notifications: https://kb.juniper.net/InfoCenter/
- Join and participate in the Juniper Networks Community Forum: https://www.juniper.net/company/communities/
- Create a service request online: https://myjuniper.juniper.net/

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

Creating a Service Request with JTAC

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

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

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

Revision History

1 September 2023—Revision 4, Junos OS Release 23.2R1.

20 July 2023—Revision 3, Junos OS Release 23.2R1.

5 July 2023—Revision 2, Junos OS Release 23.2R1.

23 June 2023—Revision 1, Junos OS Release 23.2R1.