Release Notes

Published
2025-12-12

Junos OS Release 25.2R1®

Introduction

Junos OS runs on the following Juniper Networks® hardware: ACX Series, cRPD, cSRX, EX Series, JRR Series, Juniper Secure Connect, MX Series, NFX Series, QFX Series, SRX Series, and vSRX. These release notes accompany Junos OS Release 25.2R1. They describe new and changed features, limitations, and known and resolved problems in the hardware and software.

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

Table of Contents

Introduction

Junos OS runs on the following Juniper Networks® hardware: ACX Series, cRPD, cSRX, EX Series, JRR Series, Juniper Secure Connect, MX Series, NFX Series, QFX Series, SRX Series, and vSRX. These release notes accompany Junos OS Release 25.2R1. They describe new and changed features, limitations, and known and resolved problems in the hardware and software.

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.

Authentication and Access Control

- **SSH enhancements for algorithm configuration (all Junos OS platforms)**—We've made the following updates to SSH algorithms:

  - The CLI command `set system services ssh ca-signature-algorithms` should be used to configure the signature algorithms that are allowed for certificate authorities (CAs) to use when signing certificates.

  - Under the `system services ssh hostkey-algorithm-list` hierarchy level, new options are introduced:

    - `set system service ssh hostkey-algorithm-list rsa-sha2-256`

    - `set system service ssh hostkey-algorithm-list rsa-sha2-512`

    These options enable RSA hostkey signatures using the SHA-256 hash algorithm and SHA-512 hash algorithm.

  - RSA signatures using the SHA-1 hash algorithm have been disabled by default. Consequently, the CLI command `set system services ssh hostkey-algorithm-list rsa` has been deprecated.

  [See hostkey-algorithm-list.]

Dynamic Host Configuration Protocol

- **Display physical interface and VLAN ID in DHCP relay and server binding outputs (all Junos OS and Junos OS Evolved platforms)**—You can view the physical interface and VLAN ID in the outputs of the following commands:

  - `show dhcp relay binding`

  - `show dhcp server binding`

  - `show dhcpv6 relay binding`

  - `show dhcpv6 server binding`

  The enhanced output now displays data for **Physical interface** and **VLAN** alongside existing data. This addition facilitates easy understanding of client's binding origin.

  [See https://www.juniper.net/documentation/us/en/software/junos/cli-reference/topics/ref/command/show-dhcp-relay-binding.html and https://www.juniper.net/documentation/us/en/software/junos/cli-reference/topics/ref/command/show-dhcp-server-binding-command.html.]

What's Changed

IN THIS SECTION

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

General Routing

- SSH key options for user account credentials. You can configure key-options <key-options> option at the set system login user user authentication [**ssh-rsa|ssh-ecdsa|ssh-ed25519** <ssh key> hierarchy level.

  [See login.]

- **Option allow-transients is set by default for the EZ-LAG commit script**—The EZ-LAG feature simplifies setting up EVPN multihoming configurations using a set of configuration statements and a commit script. The commit script applies transient configuration changes, which requires the `allow-transients` system commit scripts option to be set. Now the default system configuration sets the `allow-transients` option at the EZ-LAG commit script file level, removing the need to set this option manually. In earlier releases where this option isn't set by default, you must still configure the option explicitly either globally or only for the EZ-LAG commit script.

  [See Easy EVPN LAG Configuration Overview.]

User Interface and Configuration

- **Access privileges for request support information command (ACX Series, EX Series, MX Series,QFX Series, SRX Series Firewalls, and vSRX Virtual Firewall)**—The `request support information` command is designed to generate system information for troubleshooting and debugging purposes. Users with the specific access privileges `maintenance`, `view`, and `view-configuration` can execute request support information command.

- **Changes to the `show system storage` command output (ACX Series, EX Series, MX Series, QFX Series, and SRX Series)**—We've updated the `show system storage` command output to include only true (physical) storage and exclude any host/hypervisor level storage. In earlier releases, the output also includes a container/jail storage, which does not have a separate storage of its own.

  [See show system storage.]

- **Option to view combined disk space usage statistics for all configuration databases (ACX Series, EX Series, MX Series, QFX Series, SRX Series, and vSRX)**—The `show system configuration database usage` command provides the `merge` option. When you include the `merge` option, the command output displays combined disk space usage statistics for all configuration databases, including the static configuration database and all ephemeral configuration database instances.

  [See show system configuration database usage.]

Known Limitations

IN THIS SECTION

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

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

General Routing

- In the ACX platforms, family inet6 configuration is needed in core facing interface for VPNv6 traffic forwarding. PR1525348

Open Issues

There are no known issues in hardware or software in this release for ACX Series routers.

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

Resolved Issues

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

- [ACX7000 Series] DHCPv4/v6 packets may be dropped because DHCP packets are not routed to kernel after initial jdhcpd starts. PR1816246
- Serial Console Stops Working After Cable Reconnection. PR1838074
- Virtual port configuration not supported in ACX710. PR1840387
- Packets are forwarded with native VLAN tagged on ACX5448 and ACX710 platforms. PR1849241
- Inner VLAN tag DEI bit in VLAN header set . PR1850907
- The l2ald process crash is observed when same Type 5 MAC-IP received with same IP and different MAC. PR1852019
- EVPN/VPLS protocol configuration through CLI is not allowed on device. PR1852905
- Esi link state change causing bum traffic block. PR1853321
- IPv6 neighbor discovery with DHCP packet getting dropped when no-snoop option is enabled for DHCP Relay. PR1855624

- Layer 2 and layer 3 packet loss and bulk of syslog messages reported in MPLS scenarios. PR1859990
- The authd process crashes when /etc/resolv.conf file is empty. PR1860913
- The syslog message "RPD_DYN_CFG_SMID_REG_FAILED: Failed to open session database: -1" pops every 5 seconds. PR1865702
- The rpd process crashes and asserts are seen due to memory leak. PR1868085
- Transient traffic loss for CE in an EVPN MPLS setup with Multi-Homing. PR1874476

Subscriber Access Management

- Error message gets generated after you restart the device. PR1813456

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, EOL and EEOL:

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

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

For both EOL and EEOL releases, you can upgrade to the next three subsequent releases or downgrade to the previous three releases.

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

Table 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
End of Life (EOL)	24 months	End of Engineering + 6 months	Yes	No
Extended End of Life (EEOL)	36 months	End of Engineering + 6 months	Yes	Yes

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

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

Junos OS Release Notes for cRPD

IN THIS SECTION

What's New

There are no new features or enhancements to existing features in this release for cRPD.

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

IN THIS SECTION

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.

Platform and Infrastructure

- On all Junos, Junos OS Evolved, and cRPD platforms, due to deadlock in internal processes, BGP route advertisement fails leading to traffic disruption. PR1860786
- Unable establish gnmi session using Radius and TACACS authentication. PR1874078

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.

Device Security

- **Override default minimum TTL for DNS caching (cSRX, SRX Series Firewalls, and vSRX 3.0)**—Override the default minimum time-to-live value (TTL) value for fully qualified domain names (FQDNs) in the address book for DNS caching. This configuration ensures that DNS responses with TTL values lower or higher than 16 seconds are cached for their actual duration, rather than for the default minimum of 16 seconds. The system maintains default behavior for backward compatibility unless you reconfigure it. This feature offers more accurate DNS resolution and is particularly beneficial in environments where IP addresses change frequently.

  [See Override Default Minimum TTL for DNS Caching.]

- **Real-time DNS snooping for dynamic FQDN policy updates (cSRX, SRX1600, SRX2300, SRX4100, SRX4120, SRX4200, SRX4300, SRX4600, SRX4700, SRX5400, SRX5600, SRX5800, and vSRX 3.0)**—Domain Name System (DNS) snooping inspects and caches DNS responses in real time.

  After you enable DNS snooping, the firewall:

  1. Captures DNS response packets as traffic traverses the network.
  2. Extracts relevant DNS records.
  3. Builds a local cache mapping of fully qualified domain names (FQDNs) to IP addresses.

  The firewall keeps these mappings accurate and current for IPv4 or IPv6 traffic. Use this feature to implement real-time DNS mapping updates in environments with frequently changing DNS entries.

  [See DNS Snooping for Security Policies.]

- **DNS snooping and DNS module integration (cSRX, SRX1600, SRX2300, SRX4100, SRX4120, SRX4200, SRX4300, SRX4600, SRX4700, SRX5400, SRX5600, SRX5800, and vSRX 3.0)**—Use the integrated DNS-snooping cache in the Packet Forwarding Engine with the DNS module on the Routing Engine to unify entries from explicit DNS queries and DNS snooping in the data plane. The combined DNS cache remains accurate and relevant, helping you to apply DNS-based policies and destination network address translation (NAT) configurations effectively.

  The `show security dns-cache` command displays entries from both the DNS resolver and DNS snooping.

  [See DNS Snooping for Security Policies.]

Identity Aware Firewall

- **SAML-based firewall authentication (cSRX, SRX Series Firewalls, and vSRX 3.0)**—You can authenticate users through Security Assertion Markup Language (SAML)-based access profiles using your organization's identity provider (IdP) for firewall authentication. This method generates SAML requests and processes SAML assertions, enhancing the security and flexibility of user authentication. The integration supports single sign-on (SSO) using HTTP Redirect and HTTP POST

SAML bindings, providing benefits such as improved security and reduced password management. Include the `access-profile` *`profile-name`* statement under `set security policies from-zone` *`zone-name`* `to-zone` *`zone-name`* `policy` *`policy-name`* `then permit firewall-authentication user-firewall` hierarchy to enable SAML-based captive portal authentication.

To apply a default Secure Sockets Layer (SSL) termination profile, use the `set access firewall authentication user-firewall default-ssl-termination-profile` *`default-ssl-termination-profile`* command. Enable this configuration to enforce security for all access profiles.

[See user-firewall (Access Firewall-Authentication), default-ssl-termination-profile (Access), user-firewall, policy (Security Policies), SAML Authentication in Juniper Secure Connect, saml, and authentication-order (Access Profile).]

Network Management and Monitoring

- **Support for multiple gRPC servers hosting different service sets (EX2300, EX2300-C, EX2300-MP, EX2300-VC, EX3400, EX3400-VC, EX4000-8P, EX4000-12P, EX4000-12T, EX4000-12MP, EX4000-24MP, EX4000-48MP, EX4000-24P, EX4000-24T, EX4000-48P, EX4000-48T, EX4100-24MP, EX4100-24P, EX4100-24T, EX4100-48MP, EX4100-48P, EX4100-48T, EX4100-F-12P, EX4100-F-12T, EX4100-F-24P, EX4100-F-24T, EX4100-F-48P, EX4100-F-48T, EX4100-H-12MP, EX4100-H-12MP-DC, EX4100-H-24F, EX4100-H-24F-DC, EX4100-H-24MP, EX4100-H-24MP-DC, EX4300-MP, EX4300VC, EX4400-24MP, EX4400-24P, EX4400-24T, EX4400-24X, EX4400-48F, EX4400-48MP, EX4400-48MXP, EX4400-48P, EX4400-48T, EX4400-48XP, EX4600-VC, EX4650, EX4650-48Y-VC, EX9204, EX9208, EX9214, MX204, MX240, MX304, MX480, MX960, MX2008, MX2010, MX2020, MX10004, MX10008, cSRX, SRX300, SRX320, SRX340, SRX345, SRX380, SRX1500, SRX1600, SRX2300, SRX4100, SRX4200, SRX4300, SRX4600, SRX4700, SRX5400, SRX5600, SRX5800, and vSRX 3.0)**—You can configure multiple gRPC servers that host different sets of services on unique ports. Additionally, each server can support different certificates, listening addresses, and routing instances. You configure the gRPC servers at the `[edit system services http servers]` hierarchy level. Distributing gRPC services across different servers allows for better allocation of network resources, reducing the risk of port conflicts and optimizing server performance.

  [See Configure gRPC Services and 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 switches.

Authentication and Access Control

- **Support for selective server-reject VLAN in dot1x authentication** —You can enhance authentication processes with the Dot1x selective server-reject-vlan feature. When the RADIUS server rejects authentication, this feature allows 802.1x clients to attempt alternative authentication methods before being placed in the server-reject VLAN. [See https://www.juniper.net/documentation/us/en/software/junos/user-access/topics/concept/understand-802.1X-selective-server-reject-vlan.html]

- **LLDP-MED bypass for 802.1X authentication**— You can bypass the 802.1X authentication procedure for connecting multiple LLDP-MED end devices on dot1x enabled interfaces. [See https://www.juniper.net/documentation//us/en/software/junos/user-access/virtual-chassis/topics/concept/understanding-lldp-med-bypass.html]

- **Retaining dot1x cache information across reboots for persistent sessions**—You can ensure network access for clients authenticated via MAC-radius even after a device reboot using the persistent cache option. Enable this feature with the set protocol dot1x authenticator cache persistent command. This option saves session attributes to persistent storage, allowing clients to reconnect based on previously authenticated details, ensuring continuous access during power outages or server unavailability.

[See https://www.juniper.net/documentation/us/en/software/junos/user-access/topics/concept/understanding-server-fail-persistent-cache.html]

- **GRES support for 802.1X protocol**—You can ensure uninterrupted traffic flow during a Routing Engine failure using Graceful Routing Engine Switchover (GRES) support for the 802.1X protocol. The feature maintains client authentication states, preventing traffic loss and MAC learning disruptions. Use the CLI command show dot1x sync-pending-sessions to view unsynced authenticated sessions post-switchover and ensure proper session synchronization. This enhancement allows seamless transitions without client disconnections, ensuring continuous network access and stability. [See https://www.juniper.net/documentation/us/en/software/junos/user-access/understanding-graceful-routing-engine-switchover-support-for-802.1X.html]

- **Enhancements to per-service accounting over RADIUS and default service activation** —You can specify RADIUS accounting servers and intervals for individual services, enhancing control over service-specific accounting configurations. Additionally, you can configure a default service to activate when external RADIUS authentication servers are unreachable, ensuring service continuity. These configurations improve flexibility and reliability in managing service sessions and subscriber accounting. [See https://www.juniper.net/documentation/us/en/software/junos/user-access/understanding-per-service-radius-accounting-override-default-service-activation.html]

Class of Service

- **CoS support on IRB interfaces carrying EVPN-VXLAN traffic (EX4100, EX4300MP, and EX4400)**—EX4100, EX4300MP, and EX4400 switches support CoS features such as classification and rewrite on integrated routing and bridging (IRB) interfaces that carry EVPN-VXLAN traffic.

  [See **CoS Support on EVPN VXLANs**.]

EVPN

- **Configuration statements and `show` commands for troubleshooting EVPN with L2ALM context history (EX4100-24MP, EX4100-48MP, EX4400-24MP, EX4400-48MP, EX4650, MX204, MX240, MX304, MX480, MX960, MX2008, MX2010, MX2020, MX10003, MX10004, MX10008, MX10016, QFX5110, QFX5120-32C, QFX5120-48T, QFX5120-48Y, QFX5120-48YM, QFX10002, QFX10002-60C, QFX10008, and QFX10016)**—You can troubleshoot EVPN issues more effectively using updated configuration statements and `show` commands with Layer 2 Address Learning Manager (L2ALM) context history output. These tools assist in diagnosing and resolving Layer 2 learning and Ethernet switching context-related problems, enhancing your network management capabilities.

  [See l2-learning, ctxt-history, show l2-learning context-history, and show ethernet-switching context-history.]

- **Exception policy for enhanced OISM to avoid multicast traffic loss on packets with TTL=1 (EX4100-48MP, EX4100-24MP, EX4100-24T, EX4400-24MP, EX4400-24P, EX4400-24T, EX4400-24X, EX4400-48F, EX4400-48MP, EX4400-48P, EX4400-48T, EX4650, MX204, MX240,**

MX304, MX480, QFX5120-32C, QFX5120-48T, QFX5120-48T-VC, QFX5120-48Y, QFX5120-48Y-VC, and QFX5120-48YM)—Enhanced optimized intersubnet multicast (OISM) routes most multicast traffic on the OISM supplemental bridge domain (SBD) rather than on the source VLAN, even if the destination OISM device hosts the source VLAN. This extra routing decrements a packet's time-to-live (TTL) more than once, so packets with TTL=1 don't reach the receivers. To avoid this problem on enhanced OISM devices, use the following steps to configure the devices to use the source VLAN instead of the SBD to forward multicast data to remote receivers:

1. Configure a routing policy *policy-name* at the `[edit policy-options policy-statement]` hierarchy level to match the multicast groups (or sources and groups) for which to forward multicast traffic on the source VLAN.

2. Set the `forward-policy` *policy-name* option at the `[edit routing-instances` *VRF-instance-name* `protocols evpn oism enhanced forward-on-source-bridge-domain]` hierarchy level to enable forwarding on the source VLAN instead of on the SBD for the multicast groups (or sources and groups) that match the policy.

You can configure and apply multiple policies with the `forward-policy` option.

[See forward-on-source-bridge-domain and Enhanced OISM Exception Policy to Forward on Source VLAN Instead of SBD for Packets with TTL=1.]

- **New CLI option to prevent host entries from occupying LPM table space (EX4100-24MP, EX4100-24P, EX4100-24T, EX4100-48MP, EX4100-48P, EX4100-48T, EX4100-F-12P, EX4100-F-12T, EX4100-F-24P, EX4100-F-24T, EX4100-F-48P, EX4100-F-48T, EX4300-MP, EX4400-24MP, EX4400-24P, EX4400-24T, EX4400-24X, EX4400-48F, EX4400-48MP, EX4400-48P, EX4400-48T, EX4650, QFX5120-32C, QFX5120-48T, QFX5120-48T-VC, QFX5120-48Y, QFX5120-48Y-VC, and QFX5120-48YM)**—You can prevent host entries from occupying longest prefix match (LPM) table space by configuring the `no-host-as-lpm` CLI option. This option blocks additional host entries from overflowing into the LPM table, ensuring that routing for these hosts is based solely on LPM routes. To enable this feature, use the `set forwarding-options no-host-as-lpm` command and restart the Packet Forwarding Engine. This preservation of LPM table space allows for accommodating more subnet routes, enhancing routing efficiency.

  [See Host Entry Overflow Prevention.]

- **NTP-based DF election for Ethernet segments (EX4400-24T and QFX5120-48T)**—You can use the NTP-based designated forwarder (DF) election option to synchronize DF elections for multihomed Ethernet segments. This option supports existing DF election algorithms and aligns DF election timing across all devices in the segment. Use this feature to enhance network stability and performance by minimizing loops, duplicates, and traffic discarding.

  To enable this feature, configure the `df-election-ntp` option under the `protocol evpn` hierarchy. A newly defined BGP extended community with a time synchronization (T) bit communicates the Service Carving Time (SCT) for synchronized timing.

[See NTP-Based DF Election.]

- **Optimized EVPN-VXLAN DCI with enhanced OISM and an IPv6 underlay (EX4400-24MP, EX4400-24P, EX4400-24T, EX4400-24X, EX4400-48F, EX4400-48MP, EX4400-48P, EX4400-48T, EX4650, QFX5120-32C, QFX5120-48T, QFX5120-48T-VC, QFX5120-48Y, QFX5120-48Y-VC, and QFX5120-48YM)**—You can configure enhanced optimized intersubnet multicast (OISM) and seamless Data Center Interconnect (DCI) with EVPN-VXLAN instances on an IPv6 underlay. In EVPN-VXLAN DCI fabrics with enhanced OISM and an IPv6 underlay, DCI gateway (iGW) devices send EVPN Type 6 Selective Multicast Ethernet Tag (SMET) routes to remote iGW devices when hosts subscribe to multicast groups. iGW devices in the source data center selectively forward multicast traffic for a group across the DCI only if the remote data center has receivers subscribed to that group. Previously, the iGW devices always flooded multicast traffic across the interconnection even when the remote data center had no subscribed receivers.

  [See EVPN-VXLAN DCI Multicast with Enhanced OISM.]

- **Support for excluding specific MAC addresses from duplicate MAC detection (EX4100-24MP, EX4100-24T, EX4100-48MP, EX4300-MP, EX4400-24MP, EX4400-24P, EX4400-24T, EX4400-24X, EX4400-48F, EX4400-48MP, EX4400-48P, EX4400-48T, EX4650, QFX5120-32C, QFX5120-48T, QFX5120-48T-VC, QFX5120-48Y, QFX5120-48Y-VC, and QFX5120-48YM)**—You can configure an exclusion list for MAC addresses in EVPN networks to prevent legitimate MAC address movements from being marked as duplicates. Use `set protocols evpn mac-list` *`list_name`* `mac-address` *`mac_address_with_prefix_len`* to create the list and `set protocols evpn duplicate-mac-detection exclude-list` *`list_name`* to apply it. This feature helps maintain network stability by avoiding unnecessary duplicate MAC detection for specified addresses, particularly in scenarios involving virtual MAC configurations in redundant setups.

  [See EVPN Duplicate MAC Detection Exclusion Lists.]

Junos Telemetry Interface

- **Enhanced memory monitoring with configurable thresholds and improved alarm validation (EX2300-C, EX3400, EX4100-24P, EX4100-24T, EX4300-MP, EX4400-24MP, EX4400-24P, EX4400-24T, EX4400-48MP, EX4650, MX960, MX10003, MX10004, MX10008, MX10016, MX2008, MX2010, MX2020, SRX2300, SRX4200, SRX4300, SRX4600, SRX4700, and SRX5800)**—You can monitor system free pages and memory swap usage more efficiently to prevent issues related to memory shortages. The enhanced validation process reduces false alarm triggers. Additionally, you can set user-configurable thresholds for monitoring the virtual memory size (VSZ) of processes, with events categorized based on severity.

  Use the `set system monitor memory process (minor/major/critical)-event threshold <process-name> memory-limit <threshold>` command to configure these thresholds. Alarms are integrated with *eventd* and *alarmd* infrastructure and can be viewed using the `show system alarms` command. To view *jsysmond* events, use the `show system monitor memory events all` command.

[See https://www.juniper.net/documentation/us/en/software/junos/cli-reference/topics/ref/command/show-system-monitor-memory-events.html.]

- **Enhanced telemetry with multiple gRPC servers and multiport gRPC services (EX2300, EX2300-C, EX2300-MP, EX2300-VC, EX3400, EX3400-VC, EX4000-8P, EX4000-12P, EX4000-12T, EX4000-12MP, EX4000-24MP, EX4000-48MP, EX4000-24P, EX4000-24T, EX4000-48P, EX4000-48T, EX4100-24MP, EX4100-24P, EX4100-24T, EX4100-48MP, EX4100-48P, EX4100-48T, EX4100-F-12P, EX4100-F-12T, EX4100-F-24P, EX4100-F-24T, EX4100-F-48P, EX4100-F-48T, EX4100-H-12MP, EX4100-H-12MP-DC, EX4100-H-24F, EX4100-H-24F-DC, EX4100-H-24MP, EX4100-H-24MP-DC, EX4300-MP, EX4300VC, EX4400-24MP, EX4400-24P, EX4400-24T, EX4400-24X, EX4400-48F, EX4400-48MP, EX4400-48MXP, EX4400-48P, EX4400-48T, EX4400-48XP, EX4600-VC, EX4650, EX4650-48Y-VC, EX9204, EX9208, EX9214, MX204, MX240, MX304, MX480, MX960, MX2008, MX2010, MX2020, MX10004, MX10008, cSRX, SRX300, SRX320, SRX340, SRX345, SRX380, SRX1500, SRX1600, SRX2300, SRX4100, SRX4200, SRX4300, SRX4600, SRX4700, SRX5400, SRX5600, SRX5800, and vSRX 3.0)**—You can configure multiple gRPC servers with distinct services, listening addresses, and ports using the Junos Telemetry Interface. This feature enhances control over service management and telemetry data collection. You can also configure TLS certificates for secure communications. Use CLI commands to set listening addresses and ports and secure communications through TLS certificates. For example, you can configure a server to listen on a specific port and serve only designated gRPC services, enhancing flexibility and security in your telemetry setup.

- **Use Junos telemetry interface sensors to stream infrastructure and new-component environment data** —Junos OS supports these new sensors:

  - Relative humidity sensor:

    ```
    /components/component[name='FPC0']/properties/property[name='moisture']/
    ```

  - Two input and one output dry contact sensors:

    ```
    /components/component[name='FPC0']/properties/property[name='alarm-port-output0']/components/component[name='FPC0']/properties/property[name='alarm-port-input0']/components/component[name='FPC0']/properties/property[name='alarm-port-input1']
    ```

  You can also see information about dry contact and relative humidity by using the operational mode commands `show chassis environment` and `show chassis craft-interface`.

  For state sensors, see Junos YANG Data Model Explorer. For commands, see show chassis environment and show chassis craft-interface.

Layer 2 VPN

- **Layer 2 circuit support for aggregated Ethernet interfaces (EX4650 and QFX5120 line)**—You can use aggregated Ethernet interfaces when connecting to Layer 2 circuits. This feature provides the following benefits:

- Enhanced network resilience
- Load balancing across the member links
- Increased bandwidth capacity

[See Configuring Interfaces for Layer 2 Circuits and Aggregated Ethernet Interfaces.]

MAC Learning

- **Support to learn the MAC-IP information of the host (EX4000, EX4100, EX4400, and EX4650 switches)**—You can use MAC-IP snooping for non-EVPN VLANs to learn the MAC-IP information of the host. Use the new command `global-mac-ip-snooping` in the `[edit protocols l2-learning]` hierarchy to enable this feature. The `show ethernet-switching mac-ip-table` command output displays the MAC IP information. You can verify whether MAC-IP snooping is enabled for a VLAN by using the `show vlans extensive` command. You can disable the feature for a VLAN by using the new command `no-mac-ip-snooping` in the `[edit vlans <vlan-name> switch-options]` hierarchy.

  [See https://www.juniper.net/documentation/us/en/software/junos/cli-reference/topics/ref/statement/global-mac-ip-snooping-edit-protocols-l2-learning.html and https://www.juniper.net/documentation/us/en/software/junos/cli-reference/topics/ref/statement/no-mac-ip-snooping-edit-vlans-switch-options.html.]

Multicast

- **Flood IGMP/MLD reports to inter-switch links and enable immediate-leave on all host links (EX Series)**—You can flood IGMP/MLD reports to the Inter-switch Links (ISL) and prevent sending to Host Links (HL) by configuring the `flood-reports-to-inter-switch-interface` statement at the `edit protocols igmp-snooping vlan` or `edit bridge-domains protocols igmp-snooping` hierarchy level. Additionally, you can enable automatic immediate-leave on all host links by configuring the `immediate-leave-on-host-interface` statement under the `edit protocols igmp-snooping vlan` or the `edit bridge-domains protocols igmp-snooping` hierarchy.

  [See Flood Reports to Inter-switch Links and Automatic Immediate Leave on Host Links, flood-reports-to-inter-switch-interface, and immediate-leave-on-host-interface.]

Network Management and Monitoring

- **Support for multiple gRPC servers hosting different service sets (EX2300, EX2300-C, EX2300-MP, EX2300-VC, EX3400, EX3400-VC, EX4000-8P, EX4000-12P, EX4000-12T, EX4000-12MP, EX4000-24MP, EX4000-48MP, EX4000-24P, EX4000-24T, EX4000-48P, EX4000-48T, EX4100-24MP, EX4100-24P, EX4100-24T, EX4100-48MP, EX4100-48P, EX4100-48T, EX4100-F-12P, EX4100-F-12T, EX4100-F-24P, EX4100-F-24T, EX4100-F-48P, EX4100-F-48T, EX4100-H-12MP, EX4100-H-12MP-DC, EX4100-H-24F, EX4100-H-24F-DC, EX4100-H-24MP, EX4100-H-24MP-DC, EX4300-MP, EX4300VC, EX4400-24MP, EX4400-24P, EX4400-24T, EX4400-24X, EX4400-48F, EX4400-48MP, EX4400-48MXP, EX4400-48P, EX4400-48T, EX4400-48XP, EX4600-

VC, EX4650, EX4650-48Y-VC, EX9204, EX9208, EX9214, MX204, MX240, MX304, MX480, MX960, MX2008, MX2010, MX2020, MX10004, MX10008, cSRX, SRX300, SRX320, SRX340, SRX345, SRX380, SRX1500, SRX1600, SRX2300, SRX4100, SRX4200, SRX4300, SRX4600, SRX4700, SRX5400, SRX5600, SRX5800, and vSRX 3.0)—You can configure multiple gRPC servers that host different sets of services on unique ports. Additionally, each server can support different certificates, listening addresses, and routing instances. You configure the gRPC servers at the `[edit system services http servers]` hierarchy level. Distributing gRPC services across different servers allows for better allocation of network resources, reducing the risk of port conflicts and optimizing server performance.

[See Configure gRPC Services and server.]

- **IPv6 collector support for sFlow technology with EVPN-VXLAN (EX4100-48MP, EX4100-H-12MP, EX4100-H-24MP, EX4100-H-24F, EX4100-H-24F-DC, 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, EX4400-24MP, EX4400-24P, EX4400-24T, EX4400-24X, EX4400-48F, EX4400-48MP, EX4400-48MXP, EX4400-48XP, EX4400-48P, EX4400-48T, EX4650, QFX5120-32C, QFX5120-48T, QFX5120-48Y, and QFX5120-48YM)**—You can use IPv6 collector for sFlow technology to monitor known multicast traffic in EVPN-VXLAN deployments. The system supports both IPv4 and IPv6 traffic and includes management interface support for IPv6 collectors. With this functionality, you can efficiently monitor and analyze network performance across different interfaces.

  [See sFlow Support on Switches.]

- **Enhanced on-box memory monitoring with configurable thresholds and improved alarm validation (EX2300-C, EX3400, EX4100-24P, EX4100-24T, EX4300-MP, EX4400-24MP, EX4400-24P, EX4400-24T, EX4400-48MP, EX4650, MX960, MX10003, MX10004, MX10008, MX10016, MX2008, MX2010, MX2020, SRX2300, SRX4200, SRX4300, SRX4600, SRX4700, and SRX5800)**—You can monitor system free pages and excessive swap memory usage more efficiently to prevent memory shortage issues. The enhanced validation process reduces false alarm triggers.

  Additionally, you can set user-configurable thresholds to monitor the Virtual Memory Size (VSZ) of processes, with events categorized based on severity. Use the `set system monitor memory process minor/major/critical-event threshold` *`process-name`* `memory-limit` configuration statement to configure these thresholds.

  The system integrates alarms with the eventd and alarmd infrastructure, enabling you to view the alarms using the `show system alarms` command.

  Use the `show system monitor memory events all` and `show system monitor memory status all` commands to view all recorded events and the latest status on memory usage.

Services Applications

- **Flow based telemetry support for bridged traffic (EX4100, EX4100F, and EX4400)**—You now can use Flow Based Telemetry (FBT) on EX4100, EX4100F, and EX4400 switches to conduct per-flow level analytics on Layer 2 interfaces. This feature allows you to configure an inline monitoring services instance that collects and exports detailed flow information, including Layer 3 and Layer 4 attributes, to an external collector using an IPFIX template. FBT supports a range of attributes such as source and destination IP addresses, ports, and protocols, enhancing your network visibility and performance monitoring capabilities.

  [See Flow-Based Telemetry (EX4100, EX4100-F, and EX4400 Series).]

Virtual Chassis

- **Commit process optimization (EX4100-48MP, EX4100-24P, and EX4100-24T)—**Using the fast-synchronize feature, optimize the commit time on Junos OS EX Series Virtual Chassis devices. You can perform commit checks and commit activations in parallel across all Virtual Chassis members. You can validate the configuration only on the primary Virtual Chassis device where you perform the commit operation.

  [See commit (System) and Synchronizing Configurations Across Routing Engines.]

- **Synchronize Virtual Chassis configuration using SCP (EX4300-MP, EX4400-24MP, EX4400-24P, EX4400-24T, EX4400-24X, EX4400-48F, EX4400-48MP, EX4400-48MXP, EX4400-48XP, EX4400-48P, EX4400-48T, QFX5120-32C, QFX5120-48T, QFX5120-48T-VC, QFX5120-48Y, QFX5120-48Y-VC, and QFX5120-48YM)**—You can use Secure Copy Protocol (SCP) to securely transfer configuration data in a Virtual Chassis from the Virtual Chassis member in the primary Routing Engine role to a Virtual Chassis member in the backup Routing Engine role or line-card role. Synchronization occurs when a configuration is committed on the primary Virtual Chassis member, when a line-card member reboots, or when a new line-card member is added to the Virtual Chassis. When FIPS is enabled, the system uses SCP by default to synchronize configuration data.

  You must enable the `system commit config-sync-with-scp` configuration to use SCP for synchronization.

  [See Configure Synchronization of Configuration Data Using SCP in a Virtual Chassis.]

Additional Features

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

- **Filter-based forwarding for GBP-tagged traffic** (EX9204, EX9208, EX9214, MX240, MX304, MX480, MX960, MX10004, and MX10008)

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

- **Simplified configuration for ESI LAGs with EVPN dual homing (EZ-LAG)** (EX9204, EX9208, and EX9214)

[See Easy EVPN LAG (EZ-LAG) Configuration and evpn (Easy EVPN LAG Configuration).]

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

What's Changed

IN THIS SECTION

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

General Routing

- SSH key options for user account credentials. You can configure key-options key-options option at the set system login user user authentication **ssh-rsa|ssh-ecdsa|ssh-ed25519** ssh key] hierarchy level.

  [See login.]

- **Option `allow-transients` is set by default for the EZ-LAG commit script**—The EZ-LAG feature simplifies setting up EVPN multihoming configurations using a set of configuration statements and a commit script. The commit script applies transient configuration changes, which requires the `allow-transients` system commit scripts option to be set. Now the default system configuration sets the `allow-transients` option at the EZ-LAG commit script file level, removing the need to set this option manually. In earlier releases where this option isn?t set by default, you must still configure the option explicitly either globally or only for the EZ-LAG commit script.

  [See Easy EVPN LAG Configuration Overview.]

- **Changes to request system recover command syntax (EX Series)**—Options (all-members | local | member member-id) have been added to the request system recover command to specify the members for which the system needs to recover data.

  [See request system recover.]

- **Support for 4x10G uplink module**—You can use the 4x10G uplink module to support both 10G and 1G transceivers and interfaces. The device automatically detects the presence of a 10G or 1G transceiver and creates a physical interface of the corresponding speed.

  [See Port Speed on EX4400 Switches.]

Routing Protocols

- **Extension of traceoptions support for VLANs in IGMP/MLD snooping**— The `traceoptions` option is supported under the `[edit routing-instance protocols igmp-snooping vlan]` and `[edit routing-instance protocols mld-snooping vlan]`hierarchy. `traceoptions` can be enabled for both specific and all vlans.

  [See vlan (IGMP Snooping).]

User Interface and Configuration

- **Access privileges for request support information command (ACX Series, EX Series, MX Series, QFX Series, SRX Series Firewalls, and vSRX Virtual Firewall)**—The `request support information` command is designed to generate system information for troubleshooting and debugging purposes. Users with the specific access privileges `maintenance` , `view` , and `view-configuration` can execute request support information command.

- **Changes to the `show system storage` command output (ACX Series, EX Series, MX Series, QFX Series, and SRX Series)**—We've updated the `show system storage` command output to include only true (physical) storage and exclude any host/hypervisor level storage. In earlier releases, the output also includes a container/jail storage, which does not have a separate storage of its own.

  [See show system storage.]

- **Option to view combined disk space usage statistics for all configuration databases (ACX Series, EX Series, MX Series, QFX Series, SRX Series, and vSRX)**—The `show system configuration database usage` command provides the `merge` option. When you include the `merge` option, the command output displays combined disk space usage statistics for all configuration databases, including the static configuration database and all ephemeral configuration database instances.

[See show system configuration database usage.]

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.

General Routing

- On EX2300, EX3400, EX4300-48MP and EX4300, pause frame counters does not get incremented when pause frames are sent. PR1580560
- Carrier tranistions is not setting properly for channelized ports on non-DUT EX4400-48F for QSFP28-100G-AOC-30M 740-064980 of FINISAR.
- We cannot configure same output interface for multiple port-mirroring/analyzer instance. PR1873269

Open Issues

IN THIS SECTION

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

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

General Routing

- EX4100-24mp,48mp,24p/t,48p/t,F-24p/t,F-48-p/t: In an interop scenario, when using 1G SFP Optic on PIC-2, auto-negotiation should be disabled on the peer. PR1657766
- The interface of ge-x/0/1 port might go down after virtual-chassis split and merge on EX4300-VC. PR1745855
- EX4300MP: VC member status toggling between "Inactive" and "NotPrsnt" state after member downgrade. PR1751871
- Local or remote fault insertion from TG is failing. PR1789999
- Time Domain Reflectometry (TDR) support for detecting cable breaks and shorts aborts intermittently on some random ports. PR1820086
- It should not be a show-stopper for customer release, as there will be no impact on traffic, problem on displaying extra lanes in SNMP query. PR1844751
- When a poe bounce command is issued in quick succession for multiple ports, the 'poe enabled' logs may not be printed for some of the poe ports. This is a cosmetic issue and functionality works as expected. PR1845161
- A memory corruption issue can result random dense concentrator packet forwarding engine (dcpfe) process crashes on all Junos OS EX and QFX platforms configured with Virtual Extensible Local Area Network (VXLAN) configuration. PR1856424
- After multiple iterations of dc-pfe process restart, we may see interface with 10g-base-t transceiver (part# 740-123734) will not come up. PR1864715
- dhcp-snoop routes are not installed when IPSG group is full when IPv4 or IPv6 source guard is enabled along with DAI or NDI. When dhcp snooping binding entries exceed 512, even new bindings show up in the binding table, the dhcp-snoop route is not installed in HW. New bindings will be dropped due to DAI or NDI. This behavior is expected. As we are running out of space of FP entries in HW, routes are NOT installed beyond the scale. IPv4 and IPv6 uses the same VFP in HW. switch request pfe execute command `show filter hw groups` target fpc0 Unit:0 Group Information: VFP groups: Dynamic group id: 1. Pipe: 0 Entries: 1 Total_available: 512 Pri: 0 Def Entries: 0 VFP group for COS id: 143. Pipe: 0 Entries: 7 Total_available: 512 Pri: 2 Def Entries: 0 VFP group for DYN IPSG group id:

391. Pipe: 0 Entries: 512 Total_available: 512 Pri: 3 Def Entries: 0 full group with 512 entries. PR1878355

Platform and Infrastructure

- It is noticed that EX4300 switches after an upgrade of Junos from 21.2R3-SX to 21.4R3-SX may exhibit a higher CPU. Issue is resulting from fast path thread profiling code. It takes on an average 1 ms more for one fast path thread cycle, cumulatively overall fast path thread usage had increased. PR1794342
- On the EX4300, the egress Router Access Control List (eRACL) configured on the Layer 3 IPv6 interface with action count is not working.PR1848179
- VLAN Spanning Tree Protocol (VSTP), Bridge Protocol Data Units (BPDU) are dropped by EX4300 when the interface is configured in Service Provider style causing VSTP not to converge impacting the network traffic.PR1849492
- On all EX4300 series platforms, Packet Forwarding Engine process crashes and traffic via all the ports on this FPC could be impacted. PR1859134
- On EX4300 switches, Address Resolution Protocol (ARP) requests used for Media Access Control (MAC) learning are not handled correctly when MAC limiting features, such as the `mac-move-limit` configuration statements, are configured. These features change MAC learning from hardware-based to software-based. PR1873052

Resolved Issues

IN THIS SECTION

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

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

General Routing

- After ISSU upgrade, device is hanged and not able to perform any operations until USB recovery done on device. PR1703229
- EX3400: "Error:tvp_optics_eeprom_read: Failed to read eeprom for link" syslog error message. PR1757034
- API bcm_plp_mode_config_get(phy_name, plp_info, and speed, intf_type, r_clk, if_mode, aux) at tvp_bcm_mgig_phy_basic_init:433 -> -25" Error message is seen during image upgrade. PR1812228
- Packet drops when jumbo frames forwarded through ge interfaces configured for 10/100Mbps speed. PR1812891
- Complete packet loss will be observed for the inter-VLAN traffic in EVPN-VXLAN CRB scenario. PR1820830
- Interface goes down after a Data Centre Packet Forwarding Engine (dc-pfe) process restart in a Virtual Chassis environment on EX4400 platform. PR1823688
- The SFP 10GBASE-T part No. 740-083295 on platforms running Junos OS/Junos OS EVO is unable to detect a linkdown. PR1823771
- Random ports of EX4400 will not be created on upgrade or reboot. PR1825281
- On an EX4400 device with 4x25G Uplink module configured in 1GE or 25G speed, peer side of an interface with 10GBASE-T transceiver may remain up even when the IFD(xe-x/2/y) is not created. PR1831409
- EX2300/EX3400 : The status LED of uplink port is not working properly. PR1833177
- Continuous increment of tcpAttemptFails counter on Junos EX2300 and EX3400. PR1839618
- TDR test can cause a CPU hog and result in BFD flaps. PR1841117
- Memory leak is detected when interfaces are configured. PR1842546
- Junos OS and Junos OS Evolved: Receipt of a specifically malformed DHCP packet causes jdhcpd process to crash (CVE-2025-30648). PR1842682

- Media Access Control Security (MACsec) does not work properly after a transceiver is removed and re-inserted. PR1844354
- EX4100 looses connectivity with the directly connected management port of QFX5120-48Y series platform. PR1844709
- The push pop function on the QFX5120 and EX4650 is not correctly pushing the VLAN. PR1844853
- PEM mismatch alarms vanished after performing system reboot on member. PR1845365
- Interface not added back to AE bundle with multiple changes in single commit. PR1845370
- Baseline configuration commit takes more time with 256000 MAC configurations. PR1845657
- The error message will be seen on EX4100 platforms when deactivating/activating IRB interfaces. PR1846286
- Memory Leak: Memory leak is detected with rpd task blocks "rpd-trace". PR1846294
- Reachability issues are seen on interfaces that are aggregated without address-family. PR1847159
- Junos OS EX Series platform will display multiple intermittent Fan overspeed alarms. PR1848292
- EX4400: Storm-control is created for the GE interfaces for 4x10G uplink modules. PR1848338
- Handling AE Child Members, VT port properties reset when Access Port is destroyed. PR1849952
- EX4400 uplink ports (PIC 2) with the 4x25G uplink module may go down when SFPs (SFP+-10G-BX10-D/U or SFP+-10G-BX40-D/U) are inserted. PR1849992
- EX3400 Dot1x Radius accounting send incorrect value to the server for Acct-Input-Gigawords/ Acct-Output-Gigawords. PR1851299
- The l2ald process crash is observed when same Type 5 MAC-IP received with same IP and different MAC. PR1852019
- VoIP Phones are unable to receive an IP address with or without dot1x configuration. PR1852215
- Devices fail to obtain an IP address when DHCP Security Option 82 is enabled. PR1854253
- In Junos EX and QFX platforms, when ERPS protocol is enabled on a ISL trunk, the commit command fails. PR1855088
- PoE ports go down when only PSU in slot 1 is connected. PR1855409
- Traffic drop observed due to ECMP next-hop programming issue. PR1855990
- Error logs : "PFE_BRCM_COS_HALP_ERR: BRCM_COS_HALP" are observed and CoS not working on EX2300 switches. PR1856201

- Port mirroring fails due to mismatched analyzer and outgoing interface configuration. PR1856361
- Traffic drop is observed after removing the layer-2 policer from the IFL. PR1857934
- L2ald process crash is observed upon executing hidden command `show ethernet-switching debug-statistics fast-mac-update` in case the command doesn't have any output. PR1864295
- STP/MSTP/RSTP/VSTP convergence issue due to BPDU drop by l2cpd. PR1864371
- Default Route configured with Discard Next Hop on PFE instead of ECMP Next Hop after reboot. PR1867562
- Traffic will be dropped due to IPv4 header checksum mismatch on EX4400 platform. PR1870016
- RPD might crash when upgrading using no-validate. PR1870183
- EX9208: Syslog message 'JINSIGHTD_SENSOR_RESUBSCRIPTION' every 5 seconds. PR1873990

Layer 2 Ethernet Services

- Unable to assign an IP address on management interface with DHCP configuration even if DHCP is bound after a power cycle. PR1854827
- AE member not able to discover lost LACP peer connection leading to traffic drops. PR1874126

Platform and Infrastructure

- Traffic drops after link flap on active-active ESI setup with MAC pinning enabled. PR1846365
- User root is shown as incorrect after power cycle of the device. PR1855393
- STP/RSTP/MSTP/VSTP enters a disputed and blocked state when the anchor FPC of an AE link, with members distributed across multiple FPCs, goes offline. PR1870522

Routing Protocols

- Memory leak is seen when BGP is activated and deactivated. PR1849027
- BGP queue deadlock on Junos/Junos OS Evolved/cRPD platforms leading to route advertisement failure and traffic loss. PR1860786

User Interface and Configuration

- CLI core file is genarated when the size of buffer area (user input) increased to 1GB. PR1854070
- Unexpected issues such as login failures or disabled interfaces observed following abrupt reboot during commit operation. PR1861063

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, EOL and EEOL:

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

For both EOL and EEOL releases, you can upgrade to the next three subsequent releases or downgrade to the previous three releases.

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

Table 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
End of Life (EOL)	24 months	End of Engineering + 6 months	Yes	No
Extended End of Life (EEOL)	36 months	End of Engineering + 6 months	Yes	Yes

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

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

Junos OS Release Notes for 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, EOL and EEOL:

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

For both EOL and EEOL releases, you can upgrade to the next three subsequent releases or downgrade to the previous three releases.

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

Table 3: EOL and EEOL Releases

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

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

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

Junos OS Release Notes for Juniper Secure Connect

IN THIS SECTION

What's New

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

What's Changed

IN THIS SECTION

Learn about what changed in this release for Juniper Secure Connect.

VPNs

- **Support for iPadOS for prelogon compliance checks in Juniper Secure Connect (SRX Series, and vSRX3.0)**—You can configure prelogon compliance checks on your firewall to allow or reject endpoints running iPadOS. Use the `ipados` option at the `[edit security remote-access compliance pre-logon`

name `term` *name* `match platform]` hierarchy level to enforce these checks. This ensures that only compliant iPadOS devices are permitted access, enhancing the security of your network.

[See compliance (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: 25.2R1-S1

IN THIS SECTION

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

Hardware

- **New hot-swappable RCB for MX Series routers (JNP10K-RE3)**—We introduce a new hot-swappable routing control board (RCB), JNP10K-RE3, for the MX Series routers. This new generation RCB integrates the functions of a routing engine (RE) and control board (CB).

  The RE architecture gives a higher performance computing power by using a multi-core processor, higher memory, and storage infrastructure. Its input-output interfaces allow the software to interact with the rest of the system.

  The CB serves as a backbone of the chassis and the management plane, extending control and management interfaces to all FRUs in the system. It also provides class C timing to all line cards, and central timing function for the chassis, distributing system-wide timing while enabling compliance to Synchronous Ethernet (SyncE) and IEEE 1588.

  See the MX Hardware Guide for detailed information.

Table 4: JNP10K-RE3 RCB Feature Support

Feature	Description
Interfaces	Supported transceivers, optical interfaces, and DAC cables (MX10004 and MX10008)—Select your product in the Hardware Compatibility Tool to view supported transceivers, optical interfaces, and direct attach copper (DAC) cables for your platform or interface module. We update the HCT and provide the first supported release information when the optic becomes available.
Software Installation and Upgrade	• Support for firmware upgrade using the `request system firmware upgrade` CLI command. [See request system firmware upgrade.] • Secure boot and common BIOS support—The Secure Boot implementation is based on the UEFI 2.4 standard. The BIOS has been hardened and serves as a core root of trust. The BIOS updates, the bootloader, and the kernel are cryptographically protected. Secure boot is enabled by default on supported platforms. [See Junos OS Overview.] • Support for zero-touch provisioning (ZTP) and ZTP over WAN and management ports [See Zero Touch Provisioning.] • Support for secure zero-touch provisioning (SZTP) [See Secure Zero Touch Provisioning.]
User access and authentication administration	• Support for file-system encryption with Trusted Platform Module (TPM 2.0) [See Encryption with Trusted Platform Module.]

Chassis

- **RCB redundancy and chassis management support (MX10004 and MX10008)**—The MX10004 and MX10008 devices with JNP10K-RE3-128 or JNP10K-RE3-256 Routing Engine Control Boards (RCBs) support existing chassis management features and CLI commands. These devices support operation with two RCBs, where one RCB acts as the primary and the other as a backup. If you configure Graceful Routing Engine Switchover (GRES) and remove the primary RCB, the backup RCB becomes the primary RCB, ensuring continuous operation.

  [See Enabling Graceful Routing Engine Switchover.]

- **Routing Engine Board Resiliency (MX10004 and MX10008)**—We provide Routing Control Board (RCB) resiliency support for MX10004 and MX10008 devices with JNP10K-RE3-128 or JNP10K-RE3-256 RCBs. Resiliency enables the system to monitor component health, alert you of errors, and take appropriate action to restore normal operation based on error severity.

  [See Resiliency

Platform and Infrastructure

- **Enhanced VM host architecture support for new RCB (MX10004 and MX10008)**—The MX Series routers now support an enhanced VM host architecture. The enhanced VM host architecture integrates TVP and VM host.The integration of TVP and VM host has resulted in the creation of the enhanced VM host architecture. This architecture segregates platform-dependent components, platform-independent components, and guest applications.This approach makes platform and Packet Forwarding Engine activities independent of Junos OS. With this enhanced architecture, you can leverage the benefits of open-source software and drivers.

  [See VM Host Overview (Junos OS).]

Precision Time Protocol (PTP)

- **Support for Synchronous Ethernet, Synchronous Ethernet over LAG, G.8275.1, and G.8275.1 over LAG (MX Series)**—MX10004 and MX10008 routers with JNP10K-LC480 line cards support Synchronous Ethernet, Synchronous Ethernet over LAG, G.8275.1, and G.8275.1 over LAG.

  The G.8275.1 profile supports the architecture that is defined in ITU-T G.8275. The profile enables the distribution of phase and time with full timing support. You must ensure that all the devices in the network operate in combined or hybrid mode. In each of these modes, Precision Time Protocol (PTP) and Synchronous Ethernet are enabled on the devices.

  Synchronous Ethernet provides precise frequency synchronization over Ethernet networks, ensuring stable and reliable communication. It is crucial for time-sensitive applications.

  Link Aggregation Group (LAG) increases bandwidth and provides redundancy by combining multiple physical links into a single logical connection. This enhances network performance and ensures high availability in case one link fails.

[See Timing Features with JNP10K-LC480 and JNP10K-LC4800 Line Cards on MX10004 and MX10008.]

What's New: 25.2R1

IN THIS SECTION

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

Hardware

- **New MX10K-LC4802 line card (JNP10K-LC4802)**—The MX10K-LC4802 line card is a 36-port fixed configuration line card that provides a line-rate throughput of 4.8 Tbps. The MX10K-LC4802 has 32 QSFP28 ports that operate at a speed of 100 Gbps and four QSFP56-DD ports that operate at 400 Gbps.

  The MX10K-LC4802 plugs into the MX10004 and MX10008 routers horizontally in the front of the chassis. The line card is compatible with the JNP10004-SF2 (in the MX10004) and JNP10008-SF2 (in the MX10008) Switch Fabric Boards (SFBs).

  Table 5: MX10K-LC4802 Line Card Feature Support

Feature	Description
Chassis	Support for the following hardware components, platform features, and fabric functionalities for the new MX10K-LC4802 line card in MX10004 and MX10008 routers: • Support for platform resiliency [See Platform Resiliency.]
Interfaces	• QSFP to SFP+ adapter support on QSFP28 ports for 1GbE and 10GbE speeds. You can use the QSFP to SFP+ Adapter (QSA) on QSFP28 ports to support 1GbE and 10GbE speeds. This adapter enables you to connect higher-speed QSFP ports with lower-speed SFP or SFP+ ports, facilitating smooth and cost-effective network upgrades. The QSA ensures compatibility and flexibility in managing network transitions. • Supported transceivers, optical interfaces, and DAC cables —Select your product in the Hardware Compatibility Tool to view supported transceivers, optical interfaces, and direct attach copper (DAC) cables for your platform or interface module. We update the HCT and provide the first supported release information when the optic becomes available.

Table 5: MX10K-LC4802 Line Card Feature Support *(Continued)*

Feature	Description
MACsec	• Support for Media Access Control Security (MACsec), including AES-256 encryption, extended packet numbering, and fail-open mode. [See Configuring MACsec] • MACsec bounded delay protection. [See bounded-delay.]

Authentication and Access Control

- **SSH enhancements for algorithm configuration (all Junos OS platforms)**—We've made the following updates to SSH algorithms:

  - The CLI command `set system services ssh ca-signature-algorithms` should be used to configure the signature algorithms that are allowed for certificate authorities (CAs) to use when signing certificates.

  - Under the `system services ssh hostkey-algorithm-list` hierarchy level, new options are introduced:

    - `set system service ssh hostkey-algorithm-list rsa-sha2-256`

    - `set system service ssh hostkey-algorithm-list rsa-sha2-512`

    These options enable RSA hostkey signatures using the SHA-256 hash algorithm and SHA-512 hash algorithm.

  - RSA signatures using the SHA-1 hash algorithm have been disabled by default. Consequently, the CLI command `set system services ssh hostkey-algorithm-list rsa` has been deprecated.

  [See hostkey-algorithm-list.]

EVPN

- **Clone BGP routes between VRF RIBs (MX204, MX240, MX304, MX480, MX960, MX2008, MX2010, MX2020, MX10003, MX10004, MX10008, and MX10016)**—You can clone a primary or secondary BGP route from one virtual routing and forwarding (VRF) routing information base (RIB) to another VRF RIB. You can also clone the route from a VRF RIB to either the `inet.0` or `inet6.0` table.

  [See rib-exports (Routing Options) and rib-export-strip (Policy Options).]

- **Configuration statements and `show` commands for troubleshooting EVPN with L2ALM context history (EX4100-24MP, EX4100-48MP, EX4400-24MP, EX4400-48MP, EX4650, MX204, MX240, MX304, MX480, MX960, MX2008, MX2010, MX2020, MX10003, MX10004, MX10008, MX10016, QFX5110, QFX5120-32C, QFX5120-48T, QFX5120-48Y, QFX5120-48YM, QFX10002, QFX10002-60C, QFX10008, and QFX10016)**—You can troubleshoot EVPN issues more effectively using updated configuration statements and `show` commands with Layer 2 Address Learning Manager (L2ALM) context history output. These tools assist in diagnosing and resolving Layer 2 learning and Ethernet switching context-related problems, enhancing your network management capabilities.

  [See l2-learning, ctxt-history, show l2-learning context-history, and show ethernet-switching context-history.]

- **Exception policy for enhanced OISM to avoid multicast traffic loss on packets with TTL=1 (EX4100-48MP, EX4100-24MP, EX4100-24T, EX4400-24MP, EX4400-24P, EX4400-24T, EX4400-24X, EX4400-48F, EX4400-48MP, EX4400-48P, EX4400-48T, EX4650, MX204, MX240, MX304, MX480, QFX5120-32C, QFX5120-48T, QFX5120-48T-VC, QFX5120-48Y, QFX5120-48Y-VC, and QFX5120-48YM)**—Enhanced optimized intersubnet multicast (OISM) routes most multicast traffic on the OISM supplemental bridge domain (SBD) rather than on the source VLAN, even if the destination OISM device hosts the source VLAN. This extra routing decrements a packet's time-to-live (TTL) more than once, so packets with TTL=1 don't reach the receivers. To avoid this problem on enhanced OISM devices, use the following steps to configure the devices to use the source VLAN instead of the SBD to forward multicast data to remote receivers:

  1. Configure a routing policy *`policy-name`* at the `[edit policy-options policy-statement]` hierarchy level to match the multicast groups (or sources and groups) for which to forward multicast traffic on the source VLAN.

  2. Set the `forward-policy` *`policy-name`* option at the `[edit routing-instances` *`VRF-instance-name`* `protocols evpn oism enhanced forward-on-source-bridge-domain]` hierarchy level to enable forwarding on the source VLAN instead of on the SBD for the multicast groups (or sources and groups) that match the policy.

  You can configure and apply multiple policies with the `forward-policy` option.

  [See forward-on-source-bridge-domain and Enhanced OISM Exception Policy to Forward on Source VLAN Instead of SBD for Packets with TTL=1.]

- **Uplink protection for network isolation detection (MX204, MX240, MX304, MX480, MX960, MX10004, MX10008, MX2008, MX2010, and MX2020)**—With uplink protection support, you can manage network isolation by automatically shutting down Layer 2 (L2) interfaces when core isolation is detected and bringing them back up after the isolation state is cleared. This feature prevents the occurrence of traffic loops in L2 multiaccess BGP or EVPN services and improves traffic failover for multihomed customer edges during network disruptions. You can configure hold times to delay L2 interfaces' reactivation, allowing Layer 3 (L3) protocols to converge and routes to synchronize.

Additionally, maintenance options enable you to bring multiple L2 interfaces up or down collectively, facilitating easier network management.

[See Uplink Protection for Network Isolation.]

High Availability

- **Unified ISSU with enhanced mode for JNP10K-LC4802 line card (MX10004 and MX10008)**—The `in-service-upgrade enhanced-mode` CLI option ensures continuous traffic flow during software updates. Use the command `request system software in-service-upgrade enhanced-mode` to enable unified ISSU with enhanced mode and upgrade without disrupting traffic.

  [See How to Use Unified ISSU with Enhanced Mode.]

- **Support for VRRP tracking with BFD sessions (MX204, MX240, MX304, MX480, MX960, MX2008, MX2010, MX2020, MX10003, MX10004, MX10008, and MX10016)**—You can track the state of BFD sessions and dynamically adjust the VRRP priority based on the session status. For example, if a BFD session goes down, the VRRP priority is decreased, triggering an immediate switchover to the backup router. Use the `vrrp-group track` configuration option to configure VRRP tracking with BFD sessions. Use the `show vrrp track bfd` command to monitor the state and details of tracked BFD sessions.

  [See show vrrp track.]

- **Commit check for Routing Engine switchover (MX204, MX240, MX301, MX304, MX480, MX960, MX2008, MX2010, MX2020, MX10003, MX10004, MX10008, and MX10016)**—If a commit is in progress, Junos OS prohibits Routing Engine switchover until the commit completes. You can ensure that active commit operations do not interfere with a Routing Engine switchover by using the `request chassis routing-engine master switch check` command. This feature prevents system crashes and undefined states by blocking the switchover until the commit process is complete.

  [See request chassis routing-engine master.]

Juniper Extension Toolkit (JET)

- **JET support for ECMP with flex route destinations (MX304 and MX10003)**—The Juniper Extension Toolkit (JET) RIB Service API supports ECMP with a single flex route destination address that has multiple next-hop flexible tunnel profiles. In the flexible tunnel profiles, you no longer have to specify a flexible tunnel interface (FTI) to enable forwarding features and make the flex route reachable for ECMP routes. To enable this feature with the updated JET RIB Service API, see the `rib_service` proto definition file.

  [See Overview of JET APIs.]

Junos Telemetry Interface

- **Enhanced memory monitoring with configurable thresholds and improved alarm validation (EX2300-C, EX3400, EX4100-24P, EX4100-24T, EX4300-MP, EX4400-24MP, EX4400-24P, EX4400-24T, EX4400-48MP, EX4650, MX960, MX10003, MX10004, MX10008, MX10016, MX2008, MX2010, MX2020, SRX2300, SRX4200, SRX4300, SRX4600, SRX4700, and SRX5800)**—You can monitor system free pages and memory swap usage more efficiently to prevent issues related to memory shortages. The enhanced validation process reduces false alarm triggers. Additionally, you can set user-configurable thresholds for monitoring the virtual memory size (VSZ) of processes, with events categorized based on severity.

  Use the `set system monitor memory process (minor/major/critical)-event threshold <process-name> memory-limit <threshold>` command to configure these thresholds. Alarms are integrated with *eventd* and *alarmd* infrastructure and can be viewed using the `show system alarms` command. To view *jsysmond* events, use the `show system monitor memory events all` command.

  [See https://www.juniper.net/documentation/us/en/software/junos/cli-reference/topics/ref/command/show-system-monitor-memory-events.html.]

- **Enhanced telemetry with multiple gRPC servers and multiport gRPC services (EX2300, EX2300-C, EX2300-MP, EX2300-VC, EX3400, EX3400-VC, EX4000-8P, EX4000-12P, EX4000-12T, EX4000-12MP, EX4000-24MP, EX4000-48MP, EX4000-24P, EX4000-24T, EX4000-48P, EX4000-48T, EX4100-24MP, EX4100-24P, EX4100-24T, EX4100-48MP, EX4100-48P, EX4100-48T, EX4100-F-12P, EX4100-F-12T, EX4100-F-24P, EX4100-F-24T, EX4100-F-48P, EX4100-F-48T, EX4100-H-12MP, EX4100-H-12MP-DC, EX4100-H-24F, EX4100-H-24F-DC, EX4100-H-24MP, EX4100-H-24MP-DC, EX4300-MP, EX4300VC, EX4400-24MP, EX4400-24P, EX4400-24T, EX4400-24X, EX4400-48F, EX4400-48MP, EX4400-48MXP, EX4400-48P, EX4400-48T, EX4400-48XP, EX4600-VC, EX4650, EX4650-48Y-VC, EX9204, EX9208, EX9214, MX204, MX240, MX304, MX480, MX960, MX2008, MX2010, MX2020, MX10004, MX10008, cSRX, SRX300, SRX320, SRX340, SRX345, SRX380, SRX1500, SRX1600, SRX2300, SRX4100, SRX4200, SRX4300, SRX4600, SRX4700, SRX5400, SRX5600, SRX5800, and vSRX 3.0)**—You can configure multiple gRPC servers with distinct services, listening addresses, and ports using the Junos Telemetry Interface. This feature enhances control over service management and telemetry data collection. You can also configure TLS certificates for secure communications. Use CLI commands to set listening addresses and ports and secure communications through TLS certificates. For example, you can configure a server to listen on a specific port and serve only designated gRPC services, enhancing flexibility and security in your telemetry setup.

- **Telemetry sensor support for IFL and IFL set statistics from CUPS and user plane (MX204, MX240, MX304, MX480, MX960, MX10003, MX10004, and MX10008)**—You can monitor and export queue statistics and dynamic interface information for logical interfaces (IFLs) and logical interface sets (IFLsets) from the CUPS and user plane using telemetry sensor subscriptions. This feature enables you to collect and analyze queue statistics for IFLs and IFLsets efficiently. By leveraging the same sensor path tree and data model as integrated broadband network gateway (BNG), you can

seamlessly extract these statistics and send them to an external collector. This functionality enhances your ability to monitor and manage network performance effectively by providing detailed ON_CHANGE telemetry data. For sensor paths, see Junos YANG Data Model Explorer.

- **Telemetry support for native SRv6 data model in SRv6 manager (MX10004 and MX10008)**—You can enhance network telemetry by using the native Segment Routing for IPv6 (SRv6) data model for SRv6 base, facilitating detailed monitoring and management. The SRv6 manager in the routing protocol process (rpd) streams various XPaths from this model, providing comprehensive data about locators, node capabilities, and local SIDs. With this feature, you can efficiently monitor SRv6 performance metrics and improve network management and troubleshooting. Additionally, the `show srv6 local-sids`CLI operational command has been introduced to display a consolidated list of local segment identifiers (SIDs) allocated by various protocols and applications from the SRv6 manager.

  For a complete list of sensors, see Junos YANG Data Model Explorer.]

  .

- **OpenConfig telemetry sensors for DHCP relay statistics (MX204, MX304, MX150, MX480, MX960, MX10003, MX10004, MX10008, MX10016, MX2008, MX2010, and MX2020)**—You can monitor DHCP relay performance on your network by using OpenConfig telemetry sensors. For both DHCPv4 and DHCPv6, you can use only per-interface statistics sensors that stream data about total-dropped packets, invalid opcodes, and DHCP message types.This implementation supports comprehensive monitoring for Business Edge and Broadband Edge use cases, enabling you to track and aggregate critical DHCP relay statistics, ensuring efficient network management and troubleshooting.

  [See Junos YANG Data Model Explorer.]

- **Per-segment-list telemetry support for colored and uncolored SR-TE tunnels (MX10003, MX10004, MX10008, MX10016, and MX2008)**—You can configure per-segment-list sensors in segment routing–traffic engineering (SR-TE) tunnels to generate sensor IDs and collect traffic statistics from both ingress and transit points.The feature generates unique sensor IDs for each segment-list and provides the option to disable specific sensors.Additionally,updated SR-TE displays and route installations reflect per-path sensor information, ensuring comprehensive visibility and management of network telemetry.

  [See https://www.juniper.net/documentation/us/en/software/junos/interfaces-telemetry/topics/concept/srv6_traffic_sensor_telemetry.html.]

- **Leaf-level resource configuration support for data export in telemetry(MX301, MX304, MX480, MX960, MX10004, and MX10008)**—You can configure leaf-level resource paths for telemetry data export on network devices, reducing computational overhead and bandwidth usage. This feature supports selective querying of specific data elements,such as interface operational status or packet counters. The feature removes the need of exporting data for all instances of a resource. By focusing on relevant leaf devices, you obtain precise information efficiently, enhancing performance of telemetry collectors. Use the following XPath-based resource filters to further refine data queries for

sensors using advanced forwarding technologies to stream Packet Forwarding Engine performance data:

- Precise leaf such as `/interfaces/interface[name='et-1/0/35']/state/counters/in-pkts`
- Container within the path such as `/interfaces/interface[name='et-1/0/35']/state/counters/`
- List within the path `/interfaces/interface/`
- Exported leafs for `IFD/IFL/Queues`

Note that leaf-level support is applicable to both the RPC developed by Google (gRPC) and gRPC Network Management Interface (gNMI) transport modes. Leaf level subscription is not supported for leaf devices where configuration and exported paths are different.

- **XPath-based resource filtering support for Packet Forwarding Engine sensors on AFT platforms (MX301, MX304, MX480, MX960, MX10004, and MX10008)**— You can use XPath-based resource filtering to selectively export telemetry data from specific instances of network device components, reducing bandwidth usage and processing time. This feature supports precise paths, full wildcards, partial wildcards, and multilevel key options. For example, you can filter data using paths like `'/interfaces/interface[name=xe-0/0/0]'` or wildcards such as `'/interfaces/interface[name=*]'`. This functionality is particularly beneficial on fully loaded devices with numerous interfaces, enabling you to target the data of interest efficiently. Note that XPath based resource filtering is applicable to both the RPC developed by Google (gRPC) and gRPC Network Management Interface (gNMI) transport modes but not to the UDP transport mode.

  [See Junos YANG Data Model Explorer.]

- **SRv6 telemetry support (MX10004 and MX10008)**— You can manage complex networks by using Segment Routing for IPv6 (SRv6) telemetry, which provides essential tools and insights for high performance, security, and operational efficiency. This feature supports traffic sensor data streaming for IS-IS SRv6 segment identifiers (SIDs) or routes and SRv6 Traffic Engineering policies through a native YANG data model.By using these telemetry capabilities, you can monitor traffic statistics and enhance the management of SRv6 TE tunnels, ensuring robust network performance and reliability. Only the DEFAULT instance is supported for thistelemetry enhancement. For more information, see SRv6 and SRv6-TE Traffic Sensor Telemetry.

Layer 2 VPN

- **Added L2PT protocol support (MX204, MX240, MX304, MX480, MX960, MX10003, MX10004, MX10008, MX2008, MX2010, and MX2020)**—Use Layer 2 protocol tunneling (L2PT) to tunnel packets for multiple protocols. In addition to Cisco Discovery Protocol (CDP), VLAN Spanning Tree Protocol (VSTP), Per-VLAN Spanning Tree (PVST) protocol, Per-VLAN Spanning Tree Plus (PVST+) protocol, Spanning-Tree Protocol (STP), and VLAN Trunking Protocol (VTP) , you can configure L2PT to tunnel packets for the following protocols:

- Ethernet Local Management Interface (E-LMI)
- Generic Attribute Registration Protocol (GARP) VLAN Registration Protocol (GVRP)
- IEEE 802.1X authentication
- IEEE 802.3AH Operation, Administration, and Maintenance (OAM) link fault management (LFM)
- Link Aggregation Control Protocol (LACP)
- Link Layer Discovery Protocol (LLDP)
- Multiple MAC Registration Protocol (MMRP)
- Multiple VLAN Registration Protocol (MVRP)
- Unidirectional Link Detection (UDLD)
- VLAN Spanning Tree Protocol (VSTP)

[See protocol and Layer 2 Protocol Tunneling (L2PT).]

MACsec

- **MACsec with GRES and NSR (MX10004 and MX10008)**—Media Access Control Security (MACsec) support includes GRES and nonstop active routing (NSR) to provide nonstop MACsec service during a routing engine switchover. This feature is supported on the MIC-3D-20GE-SFP-EH, MIC-3D-20GE-SFP-E, and MIC-MACSEC-20GbE line cards.

  [See Configuring MACsec.]

- **Enable device to automatically adjust the MTU to include MACsec header (MX304, MX960, MX2020, MX10003, and MX10008)**—When Media Access Control Security (MACsec) is enabled on a physical interface or a logical interface, these devices can automatically adjust the maximum transmission unit (MTU) to include the MACsec header for that interface. If the device is using the default interface MTU when this feature is enabled, the device automatically increases the interface MTU to accommodate the MACsec header. If you (the network administrator) have configured a custom interface MTU, the device automatically reduces the protocol MTU to make space for the MACsec header instead. Use this feature to ensure the interface or protocol MTU is adjusted properly to account for the MACsec overhead. Without this feature, you need to adjust the interface and protocol MTU manually.

  To enable the device to automatically adjust the MTU, configure the `enable-auto-mtu-update` statement at the `[edit security macsec]` hierarchy level.

  [See Media MTU and Protocol MTU.]

Multichassis Link Aggregation (MC-LAG)

- **Support for active-standby bridging and VRRP over IRB in an MC-LAG (MX304 Universal Routing Platform, MPC10E-10C-MRATE, MPC10E-15C-MRATE, and MX2K-MPC11E modular port concentrators, and MX10K-LC9600 MX10K-LC4800 line cards)**—We introduce support for active-standby in a multichassis link aggregation (MC-LAG). In an MC-LAG topology, to make an active node inactive and enable a link switchover, you must configure the active-standby mode.

  [See Configuring Active-Active Bridging and VRRP over IRB in Multichassis Link Aggregation on MX Series Routers.]

Network Management and Monitoring

- **Support for multiple gRPC servers hosting different service sets (EX2300, EX2300-C, EX2300-MP, EX2300-VC, EX3400, EX3400-VC, EX4000-8P, EX4000-12P, EX4000-12T, EX4000-12MP, EX4000-24MP, EX4000-48MP, EX4000-24P, EX4000-24T, EX4000-48P, EX4000-48T, EX4100-24MP, EX4100-24P, EX4100-24T, EX4100-48MP, EX4100-48P, EX4100-48T, EX4100-F-12P, EX4100-F-12T, EX4100-F-24P, EX4100-F-24T, EX4100-F-48P, EX4100-F-48T, EX4100-H-12MP, EX4100-H-12MP-DC, EX4100-H-24F, EX4100-H-24F-DC, EX4100-H-24MP, EX4100-H-24MP-DC, EX4300-MP, EX4300VC, EX4400-24MP, EX4400-24P, EX4400-24T, EX4400-24X, EX4400-48F, EX4400-48MP, EX4400-48MXP, EX4400-48P, EX4400-48T, EX4400-48XP, EX4600-VC, EX4650, EX4650-48Y-VC, EX9204, EX9208, EX9214, MX204, MX240, MX304, MX480, MX960, MX2008, MX2010, MX2020, MX10004, MX10008, cSRX, SRX300, SRX320, SRX340, SRX345, SRX380, SRX1500, SRX1600, SRX2300, SRX4100, SRX4200, SRX4300, SRX4600, SRX4700, SRX5400, SRX5600, SRX5800, and vSRX 3.0)**—You can configure multiple gRPC servers that host different sets of services on unique ports. Additionally, each server can support different certificates, listening addresses, and routing instances. You configure the gRPC servers at the `[edit system services http servers]` hierarchy level. Distributing gRPC services across different servers allows for better allocation of network resources, reducing the risk of port conflicts and optimizing server performance.

  [See Configure gRPC Services and server.]

- **SNMP support for coherent ZR optics performance monitoring and threshold alerts (MX204, MX240, MX304 with MX304-LMIC16-BASE line card; MX480, MX960, and MX10003; MX10004, MX10008, MX10016 with MX10K-LC9600 line card; and MX2008, MX2010, MX2020 with MX2K-MPC11E line card)**—You can monitor the performance of coherent ZR optics (100ZR, 400ZR, 400ZR-M, and 400ZR-M-HP) and receive threshold crossing alerts by using SNMP. Retrieve real-time, historical, and statistical data for various performance parameters through SNMP get-requests. You also can receive trap notifications for threshold crossing alerts and clear events.

  Use the updated enterprise MIB named `Juniper-IFOPTICS-MIB` to comprehensively monitor and manage coherent ZR series transceivers.

[See https://www.juniper.net/documentation/us/en/software/junos/cli-reference/topics/ref/command/show-snmp-mib.html, https://www.juniper.net/documentation/us/en/software/junos/network-mgmt/topics/topic-map/snmp-mibs-supported-by-junos-os-and-junos-os-evolved.html#id_m4x_xqs_hyb, and SNMP MIB Explorer.]

- **Enhanced on-box memory monitoring with configurable thresholds and improved alarm validation (EX2300-C, EX3400, EX4100-24P, EX4100-24T, EX4300-MP, EX4400-24MP, EX4400-24P, EX4400-24T, EX4400-48MP, EX4650, MX960, MX10003, MX10004, MX10008, MX10016, MX2008, MX2010, MX2020, SRX2300, SRX4200, SRX4300, SRX4600, SRX4700, and SRX5800)**—You can monitor system free pages and excessive swap memory usage more efficiently to prevent memory shortage issues. The enhanced validation process reduces false alarm triggers.

  Additionally, you can set user-configurable thresholds to monitor the Virtual Memory Size (VSZ) of processes, with events categorized based on severity. Use the `set system monitor memory process minor/major/critical-event threshold` *`process-name`* `memory-limit` configuration statement to configure these thresholds.

  The system integrates alarms with the eventd and alarmd infrastructure, enabling you to view the alarms using the `show system alarms` command.

  Use the `show system monitor memory events all` and `show system monitor memory status all` commands to view all recorded events and the latest status on memory usage.

OpenConfig

- **OpenConfig telemetry sensors for DHCP relay statistics (MX150, MX204, MX304, MX480, MX960, MX10003, MX10004, MX10008, MX10016, MX2008, MX2010, and MX2020)**—You can monitor DHCP relay performance on your network by using OpenConfig telemetry sensors. Only per-interface statistics sensors are supported for both DHCPv4 and DHCPv6, including metrics such as total-dropped packets, invalid opcodes, and DHCP message types. This implementation supports comprehensive monitoring for Business Edge and Broadband Edge use cases, enabling you to track and aggregate critical DHCP relay statistics, ensuring efficient network management and troubleshooting.

  [See Junos YANG Data Model Explorer.]

Platform and Infrastructure

- **Enhanced VM host architecture support for new RCB (MX10004 and MX10008)**—The MX Series routers now support an enhanced VM host architecture. The integration of TVP and VM host has resulted in the creation of the enhanced VM host architecture. This architecture segregates platform-dependent components, platform-independent components, and guest applications. This approach helps platform and Packet Forwarding Engine activities happen independent of Junos OS and also enables you to leverage the benefits of open-source software and drivers.

  [See VM Host Overview (Junos OS).]

Precision Time Protocol (PTP)

- **Support for Synchronous Ethernet, Synchronous Ethernet over LAG, G.8275.1, and G.8275.1 over LAG (MX Series)**—MX10004 and MX10008 routers with JNP10K-LC4800 line cards support Synchronous Ethernet, Synchronous Ethernet over LAG, G.8275.1, and G.8275.1 over LAG.

  The G.8275.1 profile supports the architecture that is defined in ITU-T G.8275. The profile enables the distribution of phase and time with full timing support. You must ensure that all the devices in the network operate in combined or hybrid mode. In each of these modes, Precision Time Protocol (PTP) and Synchronous Ethernet are enabled on the devices.

  Synchronous Ethernet provides precise frequency synchronization over Ethernet networks, ensuring stable and reliable communication. It is crucial for time-sensitive applications.

  Link Aggregation Group (LAG) increases bandwidth and provides redundancy by combining multiple physical links into a single logical connection. This enhances network performance and ensures high availability in case one link fails.

  [See Timing Features with JNP10K-LC480 and JNP10K-LC4800 Line Cards on MX10004 and MX10008.]

Routing Options

- **Delete programmable RPD routes in CLI (MX Series)**—Delete programmable RPD (PRPD) routes in the CLI with the command `clear programmable-rpd route`. The following options are available for more precise control:

  - `client-id` (mandatory)
  - `destination` (optional)
  - `exact` (optional)
  - `table` (optional)
  - `VNI` (optional)

  [See clear programmable-rpd and programmable-rpd.]

- **Route limiter for flow specification at global family level (MX Series)**—Limit the number of flow specification routes at the global level across all routing instances for protection of flow specification filter resources. You can limit the flow routes at the IPv4 family level, IPv6 family level and at the global level. Use the new `/inet/inet6/global` option at the `[edit routing-options flow]` hierarchy level.

  [See Understanding BGP Flow Routes for Traffic Filtering.]

Routing Policy and Firewall Filters

- **Use policies to validate flow specification filters (MX Series)**—Use policies to validate the flow specification filters at the edge routers signalling flow routes over external BGP (EBGP) session to the peers. By configuring the policies, you can prevent the flow routes from accidentally or maliciously blocking protocol sessions. You can also prevent the admission of malformed, unsupported, or undesired flow routes coming from the source.

  Configure policies by specifying the match conditions and flow route actions at the `[edit policy-options flowspec-attribute]` hierarchy level.

  [See Configuring Policies for Flow Route Validation].

- **Policy to enable per-route-accounting on selective flow routes (MX Series)**—You can selectively enable individual counters for flow specification routes. Use the new policy action `flow route accounting` in the following statement format:

  ```
  set policy-options policy-statement < > term < > then flow-route-accounting
  ```

  [See flowspec-attribute].

- **New CLI option for flow family matching policy configuration (MX Series)**—The following new CLI options are available for configuring policies to match against specific family routes. Use these options at the `[edit policy-options policy-statement from family]`hierarchy level:

  `inet-flow`—IPv4 flow family

  `inet6-flow`—IPv6 flow family

  `inet-vpn-flow`—IPv4 VPN flow family

  `inet6-vpn-flow`—IPv6 VPN flow family

  [See flowspec-attribute].

Routing Protocols

- **BGP multipath prioritization with configurable priority queues (MX304)**—Use BGP multipath prioritization to prioritize critical routes in BGP multipath computations with queues of low, medium, and high priorities. This feature reduces multipath-calculation latency for operator-prioritized routes in overall route convergence during high load. Additionally, you can manage delayed forwarding information base (FIB) convergence that results from frequent routing changes.

  [See BGP Route Prioritization , multipath (Protocols BGP), and **prioritization**.]

- **BGP route leak prevention by using BGP roles and OTC attributes based on RFC 9234 (cRPD, MX204, MX240, MX301, MX304, MX480, MX960, MX10004, MX10008, MX2008, MX2010, and MX2020)**—You can prevent route leaks in BGP routing by using BGP roles and OTC attributes as

defined in RFC 9234. The feature ensures that routes from providers or peers are only propagated to customers, reducing misconfigurations and errors. The BGP speaker automatically sets the OTC based on its configured role, and then advertises a prefix based on the OTC presence in the BGP update message, making the configuration straightforward and minimizing manual intervention. With this feature, you can maintain intended routing policies and prevent network delays and denial-of-service (DoS) attacks.

[See BGP Route Leak Prevention and Detection, otc-local-role, and Supported Standards for BGP.]

- **Enhanced service route resolution for BGP multipath with list next hop (ACX5448, ACX5448-M, ACX5448-D, ACX710, MX204, MX240, MX304, MX480, MX960, MX10003, MX10004, MX10008, MX10016, MX2008, MX2010, and MX2020)**—This feature improves how service routes resolve over BGP multipath routes that use list-next hop structures. The resolver now tracks all contributing paths, not just the active one. When you configure service routes to rely on BGP multipath, RPD builds internal dependencies across each indirect next hop in the list. This ensures that your service route automatically re-resolves whenever any contributing path changes.

  Previously, inactive paths could change without triggering a re-resolution. To fix this issue, RPD now links multipath routes to their full set of contributing routes using a patricia tree structure. The resolver can now detect changes across the entire path set and update service routes as needed.

  You do not need to configure new CLI settings, but you must ensure that the BGP multipath list-nexthop command statement is enabled. You can use the updated `show route resolution list-nh` and `show krt indirect-next-hop` commands to inspect dependencies, contributing next hops, and the resulting forwarding decisions.

  This enhancement improves resolution accuracy, supports re-evaluation during inactive path changes, and strengthens overall routing consistency in hybrid internal BGP (iBGP) and external BGP (eBGP) environments.

  [See Understanding BGP Path Selection.]

- **IGP-Metric-Based AIGP Path Selection for Flex-Algo Topologies (MX Series)**—You can now use IGP metrics for AIGP path selection in SR-MPLS networks with flex-algorithm topologies, ensuring consistent low-latency routing across domains with different metric types. You can enable IGP metric computation for a flex-algorithm topology using the `compute-igp-metric` statement and assign multiple colors to a flex-algorithm with the `secondary-color` statement, both configured under `routing-options flex-algorithm <flex-algo-id>`. For finer control over route resolution, import policies can be managed within resolution schemes by using `import-policy-append` to add policies or `import-policy` to replace existing ones, configured under `routing-options resolution scheme <scheme-name>`. Additionally, policy statements now support the `actual-igp-cost` metric expression keyword, which allows precise adjustment of IGP metrics during route selection and is configured within `policy-options policy-statement <policy-name>`.

Serviceability

- **PacketIO process restart mechanism (MX Series with non-MPC line cards, such as LC480, LC4800, and LC9600)**—We've changed what happens after the PacketIO process crashes. When the PacketIO process crashes, instead of immediately rebooting the line card, the system attempts to restart the PacketIO process three times before rebooting the line card. During these restart attempts, traffic is disrupted and any host-bound traffic is expected to be dropped.

Services Applications

- **Soft Generic Routing Encapsultion (GRE) Capaility (MX304)**—The Soft GRE Capability enables advanced tunneling of Q-in-Q Ethernet frames across network infrastructure. This feature encapsulates and decapsulates Ethernet frames over GRE tunnels, preserving original Ethernet headers and MAC addresses for accurate traffic forwarding using VLAN tags.This feature supports dynamic tunnel creation, allowing automatic GRE tunnel formation without signaling protocols, thus simplifying setup and enhancing scalability.

  [See Tunnel and Encryption Services Interfaces User Guide for Routing Devices.]

- **Inline Carrier-Grade Network Address Translation (MX304, MX10004, MX10008)**—Inline Carrier-Grade Network Address Translation (CGNAT) integrates Network Address Port Translation (NAPT) directly into the Packet Forwarding Engine (PFE). Inline CGNAT can be implemented on an individual subscriber basis using RADIUS. This feature enables efficient address and port management through NAT44 (IPv4-to-IPv4) and NAT64 (IPv6-to-IPv4) translations, eliminating the need for external service cards located in the BNG chassis or an external SRX to perform the CGNAT function for BNG subscribers.

  [See Adaptive Services Interfaces User Guide for Routing Devices.]

- **Support for MAP-T solution (MX204, MX240, MX480, MX960, MX2010, MX2020, MX10004, and MX10008 with MX-SPC3)** —You can configure Mapping of Address and Port using Translation (MAP-T) as an inline service on MX Series routers with MPCs and MICs. MAP-T is a double stateless NAT64-based solution. The MAP-T solution uses IPv4-IPv6 translation as the form of IPv6 domain transport. The line cards on MX Series routers now support full reassembly of IPv4 and IPv6 packets for (MAP-T). We are introducing the following enhancements:

  - Maximum supported fragments per flow for full reassembly is increased to 32.
  - Maximum supported IP fragment size is increased to 9000 bytes.
  - Maximum IP packet size that can be fully reassembled is increased to 9000 bytes.

  [See https://www.juniper.net/documentation/us/en/software/junos/interfaces-next-gen-services/topics/topic-map/map-t-next-gen-interfaces.html#:~:text=The%20MAP%2DT%20functionality%20is,assigned%20IPv6%20MAP%20source%20address..]

Software Defined Networking (SDN)

- **Support for RHEL 9.4 in Junos node slicing (MX480, MX960, MX2008, MX2010, and MX2020)**—The external server-based Junos node slicing supports RHEL 9.4 as the host OS on x86 servers. If you are currently running RHEL 7.3 or earlier releases, we recommend that you upgrade your host OS to RHEL 9.4 before upgrading to Junos OS 25.2R1.

  [See Setting Up Junos Node Slicing].

- **Support for Ubuntu 24.04 in Junos node slicing (MX480, MX960, MX2008, MX2010, and MX2020)**—The external server-based Junos node slicing supports Ubuntu 24.04 as the host OS on x86 servers. If you are currently running Ubuntu 20.04 or earlier releases, we recommend that you upgrade your host OS to Ubuntu 24.04 before upgrading to Junos OS 25.2R1.

  [See Setting Up Junos Node Slicing].

Software Installation and Upgrade

- **Automatic firmware upgrade during initial boot (MX304)**—We support automatically upgrading the firmware for the Flexible PIC Concentrator (FPC) field-programmable gate array (FPGA) component. After you upgrade the software package, during the first boot of the new software, the system checks the version of that component's firmware. If the FPC FPGA firmware version in the router is lower than the version available in the new software, the system automatically installs the new firmware for that component.

- **Enhanced VM host architecture support for new RCB (MX240, MX480, MX960, MX2010, MX2020)**—The MX series routers now support the enhanced VM host architecture. The integration of TVP and VM host has resulted in the creation of the enhanced VM host architecture. This architecture segregates platform-dependent, platform-independent components, and guest applications. This approach helps platform and PFE activities happen independent of Junos OS and also allows us to leverage the benefits of open-source software and drivers.

  [See VM Host Overview (Junos OS).]

Source Packet Routing in Networking (SPRING) or Segment Routing

- **CoS propogation for SRv6 (IS-IS) (MX304, MX480, MX960, MX10004, and MX10008)**—We support CoS with Segment Routing for IPv6 (SRv6) to combine traffic prioritization and efficient routing. This enables better resource allocation and enhanced quality of service, resulting in a more reliable and responsive network. By default, we support uniform mode for CoS propogation, where the inner CoS value is propogated to the outer IPv6 header, that is, the SRv6 tunnel, for both classic and micro-SID (uSID) scenarios. CoS is also supported with the flex-algo SRv6 tunnels and the Segment Routing for IPv6–Traffic Engineering (SRv6-TE) tunnel.

  [See **Understanding SRv6 Network Programming in IS-IS Networks**.]

- **SRv6 unreachable prefix announcement (MX204, MX240, MX304, MX480, MX960, MX10003, MX10004, MX10008, MX10016, MX2008, MX2010, and MX2020)**—To maintain scalability and prevent overwhelming all nodes with every prefix, route summarization at Area Border Routers (ABRs) conceal local domain details. SRv6 condenses locators from remote domains and disseminates them into the core network, which can obscure local domain activities.

  A provider edge router does not immediately detect the loss of reachability when a remote edge device becomes unreachable, resulting in a traffic drop until BGP sends a status update. The ABR assigns a maximum metric to prefixes from unreachable devices, ensuring they leak across domains as Unreachable Prefix Advertisements (UPAs).

  To enable the UPA, include the `prefix-unreachable` statement at the `[edit protocols isis]` hierarchy level.

  [See prefix-unreachable.]

- **BGP-LS advertisements of PCE delegated and initiated SRv6-TE tunnels (MX960)**—Report static Segment Routing for IPv6–Traffic Engineering (SRv6-TE) tunnels with static segment list with micro SID (uSID) configuration to Path Computation Element (PCE). When the PCE controller provisions an SRv6-TE tunnel with uSIDs, BGP-LS advertises the SRv6-TE tunnel with its uSID segment list. This feature supports the SID Structure TLV 1252 and the SRv6 endpoint behavior TLV 1250, which are available in the PCE report. When the externally controlled and routed SRv6-TE receives a PCUpdate message with uSIDs from the controller, BGP-LS advertises the endpoint behavior of the uSIDs.

  [See **Enable Segment Routing for the Path Computation Element Protocol** and **SRv6-TE Tunnels with micro-SIDs in PCEP**.]

- **Support for SRv6-TE path computation (MX304 and MX960)**— Segment Routing for IPv6–Traffic Engineering (SRv6-TE) path computation enhances your IPv6 network's routing efficiency by enabling the local computation of SRv6-TE paths using both classic SIDs and micro SIDs (uSIDs). You can embed explicit paths within IPv6 packets, optimizing routing paths and reducing overhead. By default, SRv6-TE path computation prefers uSIDs over classic SIDs, resulting in paths that may consist entirely of micro SIDs, classic SIDs, or a combination of both.

  [See Understanding SRv6 TE Tunnel Local Path Computation].

Subscriber Management and Services

- **BNG subscriber redundancy on aggregated Ethernet interfaces with disabled Packet Forwarding Engines (MX304, MX960, and MX10004)**—You can enhance network reliability for broadband network gateway (BNG) subscribers by maintaining active sessions over aggregated Ethernet interfaces, ensuring service continuity even if a Packet Forwarding Engine fails. This feature supports DHCP, PPPoE, and L2TP and remains operational as long as one member link is active. It is compatible with the following configurations:

  - Active/Active mode

- Active/Standby
- Dynamic VLAN
- Static VLAN.

This redundancy improves user experience by minimizing service disruptions and ensuring uninterrupted connectivity. Disabling a Packet Forwarding Engine on a Flexible PIC Concentrator (FPC) does not affect other Packet Forwarding Engines on that FPC or other FPCs.. If you disable a Packet Forwarding Engine with an aggregated Ethernet member link, link aggregation group (LAG) or the aggregated Ethernet infrastructure redistributes the traffic on other member links.

[See Broadband Network Gateway (BNG) Subscriber Redundancy on Aggregated Ethernet (AE) Interfaces with Disabled PFEs.]

- **Wireless CUPS mobile edge support (MX240, MX304, MX480, and MX960)**—You can use the LC4800 and LC9600 line cards for the following non-anchor link configurations in the devices with user plane function (UPF) configuration:
  - **N3 mobile-edge:** Access-facing side to carry and steer uplink traffic to the UPF anchor card
  - **N4 mobile-edge:** Exchange tunneled traffic in addition to PFCP control traffic between the CPF and UPF
  - **N6 mobile-edge:** Core-facing side to carry and steer downlink traffic to the anchor card on the UPF
  - **N9 mobile-edge:** Uplink or downlink for GPRS tunneling protocol, user plane (GTP-U) tunnel switching between the I-UPF and A-UPF

  [See Junos Multi-Access User Plane Overview and MX Series Router as Junos Multi-Access User Plane.]

- **L2-BSA service on new-generation line cards (MX304-LMIC16 on MX304, MPC10E-10C and MPC10E-15C on MX960, MX10004, MX10008, and MX10016)** —Support for Layer-2 Bit Stream Access (L2-BSA) service on advanced forwarding toolkit (AFT)-based line cards, MX304-LMIC16 on MX304, and MPC trio based line cards MPC10E-10C and MPC10E-15C on MX960, MX10004, MX10008, and MX10016. This includes support for:
  - Inline L2-BSA.
  - Out-of-Band L2-BSA
  - Bring up of L2BSA subscribers
  - Bring down of L2BSA subscribers
  - Upstream packet flow

- Downstream packet flow
- Service providers can now provide 100-Mbps domain-specific language (DSL) speed VDSL2 with L2-BSA service for network service provider (NSP) partners.

[See Broadband Subscribers Access Network Overview.]

- **Support for PPPoE subscriber over softGRE tunnels on pseudowire interfaces over RLT(MX240, MX480, and MX960)**—You can extend subscriber services over softGRE tunnels to pseudowire subscriber interface over redundant logical tunnel (RLT) interfaces for Wi-Fi access gateway (WAG) deployments in a PPPoE dual-stack network. This feature enhances forwarding-path redundancy and supports active-active or active-backup modes. You can use VLAN-tagged or untagged Ethernet frames. Support is limited to line cards from MPC2 to MPC9.

  [See Wi-Fi Access Gateways.]

- **Load balancing based on tunnel identified in L2TPv3 header (MX204, MX240, MX304 MX480, MX960, MX2008, MX2010, MX2020, MX10003, MX10004, MX10008, and MX10016)**—These devices can load-balance packets based on the tunnel they belong to. When Layer 2 Tunneling Protocol version 3 (L2TPv3) packets are encapsulated in IP tunnels, the packet header includes a tunnel ID and a session ID that distinguishes the traffic flow that packet belongs to. The device uses this information in the L2TPv3 packet headers when performing the hash computations for load balancing. This feature enables the device to better manage traffic flows in L2TPv3-over-IP tunnels.

  To enable and disable L2TPv3-header based load balancing, use the `l2tp-tunnel-session-identifier` statement at the `[edit enhanced-hash-key family` *`family`*`]` hierarchy, where the family can be `inet` or `inet6`.

  [See l2tp-tunnel-session-identifier and Layer 2 Tunneling Protocol (L2TP).]

- **N+1 (DHCP Server and Relay) subscriber redundancy on BNG using Packet Forwarding Engine (MX304, MX480, MX960, MX10004, and MX10008)**

  —Optimize resource usage and defer full-service traffic handling until failover occurs, thus supporting higher subscriber density. This feature supports Packet Forwarding Engine over-subscription using pseudowire interfaces (MPLS PWHT and EVPN VPWS PWHT) across multiple chassis for access and DHCP in relay mode with external server addresses and in local server mode with locally assigned IP addresses. The backup Packet Forwarding Engine transitions from basic forwarding to full service during failover. The MPC7 and LC2103 line cards act as secondary line cards.

  Use the `service-activation-on-failover` mode to enable this feature.

  Use the `set system services subscriber-management redundancy group <group-name> interface <interface-name> standby-mode [hot-standby | service-activation-on-failover];` command.

  Enable one secondary device to back up multiple primary devices.

[See N+1 Redundancy Support for BNG.]

- **Support for creating access-line-identifier (ALI) based dynamic VLANs using unique source MAC Address for PPPoE Subscribers only (MX Series Routers)**—Service Provider deployments with multi-service access nodes (MSANs) that do not support agent circuit identifier (ACI) or agent remote identifier (ARI) insertion in PPPoE control packets can create ALI based dynamic VLANs using a single network-wide unique MAC address assigned to each household or access line. When a household has multiple PPPoE sessions, the MSAN performs MAC address translation such that all PPPoE sessions from a household have the same source MAC address. To allow multiple PPPoE sessions from the same source MAC address, the PPPoE `duplicate-protection` support is extended to include the `relay-session-id` tag along with source MAC to create a client address key to uniquely identify each PPPoE session. The PPPoE `short-cycle-protection` support is also extended to include `relay-session-id` tag along with source MAC to uniquely identify each PPPoE session.

  Use the `accept-no-ids mac address` option to trigger ALI based dynamic VLAN creation based on source MAC address. Use the `duplicate-protection include relay-session-id` option to include relay-session-id tag to uniquely identify each PPPoE session from a household with duplicate source MAC addresses.

  The following CLI show command outputs are updated:

  ```
  show subscribers detail

  show subscribers extensive

  show subscribers aci-interface-set

  show interface interface-set detail

  show pppoe interface-sets

  show interfaces

  show pppoe underlying-interfaces

  show pppoe lockout
  ```

  [See Access-Line-Identifier-Based Dynamic VLANs Overview.]

- **Support for static IPv4 subscribers over statically configured soft-GRE tunnels (MX240, MX480, MX960 with MPC5 and MPC7 line cards)**—Service Providers using Fixed Wireless LAN (WLAN) to provide network access to subscribers can now provision static IPv4 subscribers wherein IP address of the Customer Premises Equipment (CPE) router is statically configured on both the CPE and the Broadband Network Gateway (BNG) and the data is transmitted over statically configured soft-GRE tunnels. Control plane protocols such as PPPoE or DHCP do not run on the CPE to provision the CPE IP address. The soft-GRE tunnel is brought up by the configuration and will stay up as long as the

configuration is present on the router. The static subscriber requires the underlying soft-GRE tunnel to be present before it comes up. The static subscriber can access all BNG services including policers, Class of Service (CoS), accounting and more, based on the configuration. A static tunnel configuration must be defined under the `set services soft-gre` *gre-group* hierarchy with a tunnel name and remote address. These subscribers are associated with statically configured `demux1` logical interfaces with IPv4 prefixes, defined under the `set system services static-subscribers` hierarchy.

[See Static Subscribers Over Statically Configured Soft-GRE Tunnels.]

Additional Features

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

- **Access Gateway Function (AGF) support**(MX304, MX10004, and MX10008)

  [See AGF User Guide.]

- **Filter-based forwarding for GBP-tagged traffic** (EX9204, EX9208, EX9214, MX240, MX304, MX480, MX960, MX10004, and MX10008)

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

- **Multiple next hop support for inline active flow monitoring** (MX240, MX304, MX480, MX960, MX10004, MX10008, MX10016, MX2010, and MX2020, with line cards LC480, LC2101, LMIC16-BASE, LC4800, or LC9600)

  [See Understand Inline Active Flow Monitoring, ipv6-extended-attrib, and multi-bgp-path.]

- **Seamless stitching of Type 5 to Type 5 routes in EVPN-VXLAN** (MX240, MX304, MX480, MX960, MX10004, MX10008, MX10016, MX2010, and MX2020)

  [See Configuring Seamless Type-5 to Type-5 Stitching for EVPN-VXLAN.]

- **Support for consistent hashing** (MX304 and MX10003).Define a KRT export policy for consistent hashing on routes resolving over a flex route profile with multiple gateways. The policy applies to direct flows to the flex route IP address to maintain flow affinity.

  [See **Actions in Routing Policy Terms**

- **Support for stitching EVPN-VXLAN Type 5 with SRv6**(MX240, MX304, MX480, MX960, MX2010, MX2020, MX10004, and MX10008). We support stitching EVPN-VXLAN Type 5 route on IPv4 with an SRv6 micro-SID tunnel within the same data center using a Layer 3 VRF. The EVPN network in the data center is configured on IPv4 underlay networks. You can use both IPv4 and IPv6 data traffic from the CE device in the SRv6 tunnel that is stitched to EVPN-VXLAN tunnel.

> **NOTE:**
> You must include the `vrf-table-label` statement in the routing instance.

> **NOTE:**
> We support only one-to-one mapping of VRF Type 5 instances.

- Type 5 in EVPN-VXLAN

  [See EVPN Type 2 and Type 5 Route Coexistence Implementation.]

- Data Center Intercoonect (DCI) in EVPN-VXLAN

  [See Data Center Interconnect Design and Implementation Using IPVPN and Example: Configuring VXLAN Data Center Interconnect Using EVPN]

- Segment Routing for IPv6 (SRv6)

  [See SRv6 and Example: Configuring Layer 3 Services over SRv6 in BGP Networks.]

- **Support for file-system encryption with Trusted Platform Module (TPM 2.0)** (MX304)

  [See Encryption with Trusted Platform Module.]

-

What's Changed

IN THIS SECTION

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

General Routing

- **Changes to default behavior under forwarding-table (MX Series)**—The `ecmp-fast-reroute` and `indirect-next-hop-change-acknowledgements` commands are enabled by default under the [`edit routing-options forwarding-table`] hierarchy. You can verify these defaults by running the `show configuration routing-options forwarding-table` command in the operational mode.

  [See ecmp-fast-reroute .]

- SSH key options for user account credentials. You can configure key-options <key-options> option at the set system login user <user> authentication [ssh-rsa|ssh-ecdsa|ssh-ed25519] <ssh key> hierarchy level.

  [See login.]

- The `show subscribers extensive client-type dhcp | display xml validate` command has now been updated to display correct output instead of the `Duplicate data element` error message.

- **SFP Optics LOS alarms (MX Series)**— SFP Optics don't support Tx laser disabled alarm, Tx loss of signal functionality alarm, and Rx loss of signal alarm as diagnostics output.

  [See show interfaces diagnostics optics.]

- **G.8275.1 profile configuration with PTP, SyncE, and hybrid mode (Junos)]**— On all Junos platforms, when configuring the G.8275.1 profile, it is mandatory to configure Precision Time Protocol (PTP), Synchronous Ethernet (SyncE), and hybrid mode. Earlier, the system would not raise a commit error even if the required hybrid and SyncE configurations were missing while configuring G.8275.1 profile. However, going forward you will not be able to configure the G.8275.1 profile without configuring PTP, SyncE and hybrid mode to be compliant with the ITU-T standards.

  [See G.8275.1 Telecom Profile.]

- **Extension of traceoptions support for VLANs in IGMP/MLD snooping**—The `traceoptions` option is supported under the `edit routing-instance protocols igmp-snooping vlan` and `edit routing-instance protocols mld-snooping vlan`hierarchy. `traceoptions` can be enabled for both specific and all vlans.

  [See (IGMP Snooping) and vlan (MLD Snooping).]

Subscriber Access Management

- You can configure VLAN termination cause codes to specify RADIUS attribute values for different termination scenarios on JUNOS MX platforms supporting the Layer-2 Bitstream Access (L2BSA) feature. You can diagnose and manage network issues effectively by understanding the specific

reasons for VLAN termination. Ensure that the correct termination cause codes are sent by validating configuration and testing scenarios to correctly interpret network events. When a subscriber logs out, the system occasionally sends an incorrect termination cause value to RADIUS. The subscriber VLAN "Account-Terminate-Cause" in "Acct-Stop" message for different L2BSA subscriber logout error scenarios is modified to display correct reasons for termination.

[See VLAN Termination Causes and Code Values and show network-access aaa terminate-code.]

User Interface and Configuration

- **Access privileges for request support information command (ACX Series, EX Series, MX Series, QFX Series, SRX Series Firewalls, and vSRX Virtual Firewall)**—The `request support information` command is designed to generate system information for troubleshooting and debugging purposes. Users with the specific access privileges `maintenance`, `view` and `view-configuration` can execute request support information command.

- **Changes to the `show system storage` command output (ACX Series, EX Series, MX Series, QFX Series, and SRX Series)**—We've updated the `show system storage` command output to include only true (physical) storage and exclude any host/hypervisor level storage. In earlier releases, the output also includes a container/jail storage, which does not have a separate storage of its own.

  [See show system storage.]

- **Option to view combined disk space usage statistics for all configuration databases (ACX Series, EX Series, MX Series, QFX Series, SRX Series, and vSRX)**—The `show system configuration database usage` command provides the `merge` option. When you include the `merge` option, the command output displays combined disk space usage statistics for all configuration databases, including the static configuration database and all ephemeral configuration database instances.

  [See show system configuration database usage.]

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

- Pause frames counters does not get incremented when pause frames are sent.PR1580560
- This issue is caused because of the fact that peers-synchronize is configured, and master-password is configured to encrypt the config being sync'ed. However since there is no master-password configured on the peer device, the encrypted configuration cannot be decrypted (this is expected). This has not been supported from day-1, however a workaround can be done in order to get this to work. The workaround is to manually configure the same master password on the peer device manually. At a high level the problem is as follows: Consider there are two devices A and B in a peer-sync config 1. config on dev A contains secrets which need to be encrypted with the master password and synced with the device B 2. The master-password (juniper123+masterpassword) is configured on device A and the configuration is encrypted and written to /tmp/sync-peers.conf 3. The /tmp/sync-peers.conf is then synced to device B but device B does not have the same master-password configured which results in the config failing to decrypt. The master-password itself is not a part of the config-database. Additionally, it cannot be transmitted over an unencrypted HA Link, as this would lead to the master-password getting leaked. This is by design, and would be a security concern if it were to be transmitted across an unencrypted channel. Therefore, this work as designed. In order to work around this issue follow these steps: 1. configure the master-password on device B and commit the config 2. configure the same master-password on device A and commit the config and it should get sync'ed correctly.PR1805835
- M/Mx: ISIS session over MPC11 cards flapped due to "3-Way handshake failed" during ISSU (FRU upgrade stage - reboot phase)PR1809351
- On MX10008 and MX10016 platforms with JNP10K-LC480 Line Card installed, the remote end of the Ethernet link of the JNP10K-LC480 Line Card goes down when an ISSU (Unified In-Service Software Upgrade) is performed from Junos OS 24.4R2 (or earlier) to Junos OS 25.2R1 (or higher). This causes traffic disruption.PR1880150

Platform and Infrastructure

- An Authentication Bypass by Spoofing vulnerability in the RADIUS protocol of Juniper Networks Junos OS and Junos OS Evolved platforms allows an on-path attacker between a RADIUS server and

a RADIUS client to bypass authentication when RADIUS authentication is in use. Please refer to https://supportportal.juniper.net/JSA88210 for more information.PR1850776

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.

General Routing

- On the MX104 platform, when using snmpbulkget or snmpbulkwalk (for example, used by the SNMP server) on a chassisd-related component (for example, jnxOperatingEntry), chassis process (chassisd) high CPU usage and slow response might be seen because of a hardware limitation, which might also lead to a query timeout on the SNMP client. In addition, the issue might not be seen while using an SNMP query for interface statistics. As a workaround, to avoid the issue, use either of the following approaches: Use snmpget or snmpwalk instead of snmpbulkget or snmpbulkwalk and include the -t 30 option when doing the SNMP query. For example, snmpget -v2c -c XX -t 30. Use the -t 30 option with snmpbulkget or snmpbulkwalk. For example, snmpbulkget -v2c -c XX -t 30. PR1103870
- Multiple vulnerabilities have been resolved in MQTT (Message Queuing Telemetry Transport) included with Junos by fixing vulnerabilities found during external security research. Please refer to https://supportportal.juniper.net/JSA71655 for more information.PR1651519

- In an interop scenario, when using 1G SFP Optic on PIC-2, auto-negotiation should be disabled on the peer. PR1657766
- 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
- When LAG is configured with mixed speed interfaces switching to a secondary interface of different port speed, results in a few packet drops for a very short duration. PTP remains lock and there is no further functional impact. PR1707944
- In Netconf private edit configuration session, commit RPC fails when unprotect operation is performed. PR1751574
- On all Junos and Junos OS Evolved platforms, when rib-sharding is enabled and RT (Route Target) multipath routes containing both indirect and composite next-hop types are processed, the rpd (Routing Protocol Daemon) process will crash due to incorrect handling during the next-hop copy operation from RIB (Routing Information Base) shards to the main RIB thread. An rpd crash results in all routing protocols going down and causes a brief traffic disruption until the rpd process restarts.PR1757915
- PR1735843 has fixed a VM core with the reason "panic: deadlres_td_sleep_q: possible deadlock detected". The same issue might also be seen on all other JUNOS vmhost platforms but with a different root cause. PR1776854
- On MX104, the AFEB could crash and reboot following a change of PTP GM clock source, which affects traffic forwarding. PR1782868
- On MX platforms with MS-MPC/MS-MIC with IPsec (Internet Protocol Security) configured, IPsec traffic loss will be observed if an SA (Security Association) deletion request is sent by the peer just before the SA installation is completed. The issue happens in the scale scenario (4000 tunnels are configured, and when the SA count reaches up to 3900). PR1825835
- It should not be a show-stopper for customer release, as there will be no impact on traffic, problem on displaying extra lanes in SNMP query. PR1844751
- On MX10004 and MX10008 platforms with JNP10K-RE3 and LC480 line cards, when the device is set up with G8275.1 PTP(Precision time protocol) profile or SyncE (Synchronous Ethernet) and GRES, performing a GRES switchover causes DPLL-2 to go from "lock" to "unlock." This can lead to a loss of synchronization which can disrupt timing-sensitive services like PTP and SyncE. PR1848235
- On MX platforms with MPC5/MPC7 line cards when there are active pseudo wire subscribers and there is a change in the tunnel-services bandwidth configuration, FPC (Flexible Physical Interface Card Concentrators) crash is observed with the subsequent impact on the traffic.PR1849552.

- On SRX and MX platforms a rare occurrence issue causes a sudden reboot of the SPC3 (Services Processing Cards) in use leading to packet loss during the card offline period in the reboot process.PR1857890
- Mixed type of anchor PFE on APFE config is not supported. PR1861177
- On MX chassis with ULC with asymmetry configured on PTP slave ports, we see small spikes which in the TIE values which are more than the expected range. The TIE values however falls within the expected range after few seconds.PR1867423
- When a PTP source switchover event occurs either due to a LC reboot or optics removal on the peer side, we see 1 errored PTP packet on the slave end of a Hamilton LC. The errored packet does not cause any PTP performance issue and PTP quickly phase-aligns with new source.PR1869672
- On Juniper MX10003 platforms equipped with MIC1, interfaces using QSFP optics fail to come up or remain down after a connected third-party device is rebooted. This behavior results from a timing mismatch, where the software delays link initialization while waiting for a stable optical signal, potentially missing the brief window when the remote device restarts its transmit signal. This is an interoperability issue and may require manual intervention for service restoration.PR1876314
- Humidity Sensor CLI command is not applicable on MX10004 and MX10008 devices. The command has been suppressed in later releases. PR1909435
- Support for Virtium SSD firmware upgrade on MX10004 and MX10008 devices not available in Junos OS 25.2R1-S1 Release. Fixed in later releases. PR1907227
- On MX10004 and MX10008 devices, display-only issue in Junos CLI show chassis environment : current/power for some of the POLs are shown as 0, observed in 25.2R1-S1. Fixed in later releases. PR1916094

Interfaces and Chassis

- The commit failure "Change in hierarchical-scheduler mode is not allowed" (given in description) can be seen after multiple iterations of loading test config and overriding with baseline config.PR1849110

Layer 2 Ethernet Services

- Day-1 issue, DHCP subscribers are not going down when PFE is disabled where AE with single leg is present with BFD enabled.PR1837994

Network Management and Monitoring

- In some NAPT44 and NAT64 scenarios, Duplicate SESSION_CLOSE Syslog will be seen. PR1614358
- Issue is related to only user defined routing-instance. In this case DUT is connected to two remote-servers through the same Routing-instance. when the route for above connection is deleted and added back from the server side, stale connections are seen. This is because when routes are deleted SYN_SENT are not acknowledged but Application closes the socket. when the routes are again added, application creates new sockets and connects to the remote-server, at the same time Previous SYN_SENT got ack and moved to ESTABLISHED state. this causes stale connections. There is no impact-on functionality, Issue is seen only on Junos platform and for only user-defined RI. Infra code need to be changed to handle socket close error conditions that needs more code churn, time and thorough testing. PR1825311

Routing Protocols

- LDP OSPF are in synchronization state because the IGP interface is down with ldp-synchronization enabled for OSPF. user@host> show ospf interface ae100.0 extensive Interface State Area DR ID BDR ID Nbrs ae100.0 PtToPt 0.0.0.0 0.0.0.0 0.0.0.0 1 Type: P2P, Address: 10.0.60.93, Mask: 255.255.255.252, MTU: 9100, Cost: 1050 Adj count: 1 Hello: 10, Dead: 40, ReXmit: 2, Not Stub Auth type: MD5, Active key ID: 1, Start time: 1970 Jan 1 00:00:00 UTC Protection type: None Topology default (ID 0) -> Cost: 1050 LDP sync state: in sync, for: 00:04:03, reason: IGP interface down config holdtime: infinity. As per the current analysis, the IGP interface goes down because although LDP notified OSPF that LDP synchronization was achieved, OSPF is not able to take note of the LDP synchronization notification, because the OSPF neighbor is not up yet. PR1256434
- On all Junos and Junos Evolved platforms, the aggregate-bandwidth feature does not function as expected when the device is configured as a BGP (Border Gateway Protocol) Route Reflector (RR). Specifically, in scenarios involving BGP multipath bandwidth aggregation for routes originating from VRF (Virtual Routing and Forwarding) instances under the L3VPN (Layer 3 Virtual Private Network) address family. PR1877111

Services Applications

- An incorrect remote id received from peer results in AUTH failure and this fails the IKE SA setup. This immature IKE SA doesn't go for proper cleanup hence "Not matured" IKE SA piles UP. Restarting the kmd will clear the Not matured SAs.PR1797377

- On all MX platforms with MS-MPC (Multiservices Modular PIC Concentrator), when DPD (Dead Peer Detection) is enabled under IPsec/IKE (Internet Key Exchange) VPN settings and for any reason an IPsec SA (Security Association) is deleted, the kmd process crashes. Due to the kmd process restart some disruption in tunnel establishment is seen.PR1869769

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.

Authentication and Access Control

- Radius authentication is failing when Challenge Token is entered PR1862203

Class of Service (CoS)

- When CoS configurations for an Interface Device (IFD) are present both under the wildcard (applied via groups) and as specific configurations (applied directly under the class-of-service hierarchy) on Junos platform, the Interface Device (IFD) correctly takes the specific configurations as expected. However, the Interface Logical (IFL) over this IFD does not take the wildcard configuration from the group. PR1872595

EVPN

- Stale MAC entries may remain in the MAC table of EVPN routing instances after rapid MAC-IP move scenarios PR1833660
- RPD core-dump on 22.2R3-S4. PR1841965
- Few seconds traffic loss during previous DF coming back with EVPN-VPWS non-revertive DF preference feature enabled. PR1851659
- Using SRv6 or MPLS IPv6 encapsulation over EVPN instances causes IPv4 packets to be dropped PR1857154
- NTP DF election feature should support EVPN VPWS instances. PR1860135
- 'TLV type 00000052 not supported on IFL gr' seen repeatedly in syslog for EVPN routing-instance configured with gr- ifls. PR1870365

Forwarding and Sampling

- Error messages are observed and incorrect values are returned for SNMP requests for pfe traffic statistics PR1692411
- Incorrect color-aware srTCM marking with yellow packet loss priority. PR1837840
- MIB2D will see 100% CPU utilization due to MIB2D walk fail PR1856854
- MIB2D stucked at 100% on MX10003 PR1859894
- System becomes unresponsive or crash due to frequent filter changes in a scale scenario having mib2d process in use PR1872347

General Routing

- Junos OS: An unauthenticated attacker with local access to the device can create a backdoor with root privileges (CVE-2023-44194) PR1514925
- Multiple J-UKERN core files might be generated during the sanity test PR1641517
- Extremely fast interface flaps in MPC10E line-card causes cpu to hog which leads to fpc reboot. PR1727066
- Error message may occurs once in a while with full scale when 'clear bgp neighbor all' with all the services like EVPN, vrf etc being present. PR1744815
- MPC10E: Support of G.8275.1 PTP Hybrid mode with speed 400G PR1767930
- [./sw-vale-mx-indus] [generic] MX10004 :: LC480 line card crashed with reference to posix_interface_abort () at ../src/pfe/platform/linux/posix_interface.c:2729 PR1784824
- Speed change between 1G and 10G with traffic in high-priority queue on ports causes the link to go down PR1807277
- FPC crash due to race condition on MX platforms with LC480. PR1809644
- Tunnel source and destination in the same broadcast domain lead to traffic drops. PR1811488
- Complete packet loss will be observed for the inter-VLAN traffic in EVPN-VXLAN CRB scenario PR1820830
- Random ports of EX4400 will not be created on upgrade or reboot PR1825281

- In high-scale, high-load environments, the l2ald process may experience hangs during Apstra polling. PR1828741
- Commit error check-out failed does not get triggered when a complete bridge-domain is configured in instance-type vrf. PR1829886
- High FPC CPU utilisation and local MAC learning failure in EVPN-MPLS scenario due to rapid MAC moves PR1838335
- The MPC7/MX2K-MPC8E/MX2K-MPC9E line cards of the FPC gets stuck into HOST LOOPBACK WEDGE state post pfe-reset action triggered by any PFE major/fatal errors PR1839071
- Tactical Traffic Engineered load sharing utilization displays incorrect percentage on MX platforms PR1840503
- Major alarm "Host 0 bme1 : Ethernet Link to other RE Down" or log "CHASSISD_LINK_RE_ERROR_RECOVER: RE_TO_ORE iface recovery: bme1 is down" is seen when backup RE is removed PR1840810
- ISSU fail for the MPC2E/3E NG FPC result in FPC crash. PR1841400
- The "show chassis synchronization extensive" command output shows syncE is locked to both primary and secondary sources after switching between primary and secondary sources PR1841695
- MGeo Telemetry - Added cluster name and generation number to subsystem health sensor tree. PR1842439
- Unable to console to VNF using a non-root user from Juniper Device Manager PR1842451
- Memory leak is detected when interfaces are configured PR1842546
- Junos OS and Junos OS Evolved: Receipt of a specifically malformed DHCP packet causes jdhcpd process to crash (CVE-2025-30648) PR1842682
- Incorrect MTU value in the ICMP Next-Hop MTU field, regardless of the actual MTU of the outgoing interfaces PR1842744
- IGMP packets are not accepted on dynamic demux interface with additional configuration of all interfaces disabled under IGMP protocol. PR1843505
- Memory leak when deactivating/reactivating routing instances with vrf-table-label PR1843627
- vlan tagging in Q-in-Q is not handled correctly over EVPN-VxLAN PR1843817
- Memory leak is seen with rpd task blocks "nhlib_nexthops_004" PR1844160
- Stale MAC-IP entries are not cleared in an EVPN-VXLAN scenario when encapsulate-inner-vlan or decapsulate-accept-inner-vlan or both knobs are present. PR1844623

- High heap memory caused MX-SPC3 PIC to go offline. PR1844731
- Subscribers unable to connect in GNF setup PR1844934
- Unnecessary trace log files related to licenses are generated. PR1845079
- Interface not added back to AE bundle with multiple changes in single commit. PR1845370
- Traffic blackhole is observed for IPv4 /32 LDP prefixes advertised over BGP-LU when BGP sharding is configured PR1845425
- Incorrect warning message is seen post hyper-mode configuration change and mismatch of hyper-mode between FPC and RE impacts performance. PR1845497
- Baseline configuration commit takes more time with 256000 MAC configurations PR1845657
- PTP/SyncE config on Junos fusion port causes crashes PR1846115
- Continuous logging of alarms during a fiber cut with transport devices PR1846164
- Memory Leak: Memory leak is detected with rpd task blocks "rpd-trace" PR1846294
- When "set chassis redundancy failover on-re-to-fpc-stale" is configured unexpected master RE switchover will be seen if backup RE reboots resulting in traffic disruption PR1846557
- Some ports take longer than others to come back online when multiple ports experience simultaneous flap PR1847378
- MACSec fails after applying MACSec configuration on IFL and removing it. PR1847418
- Support FW_Continue with HW Segmented Filters on AFT TRIO platform PR1848740
- Routing-services enabled on PPPoE dynamic profile causes subscriber login failure for new subscribers. PR1848887
- Configuring BGP rib-sharding and generate route will cause rpd process to crash. PR1848971
- Time Error Spikes Observed During SyncE Source Switching Between Line Cards on MX10004 and MX10008 Systems with JNP10K-RE3 RCB and JNP10K-LC480 Modules. PR1849099
- The SNMP mib walk for lldpConfigManAddrPortsTxEnable fails. PR1849307
- The bbe-statsd process crash due to malformed PFE packets. 1849377
- FPC reboot due to memory leak from telemetry sensor installation/uninstallation. PR1849915
- Handling AE Child Members, VT port properties reset when Access Port is destroyed. PR1849952
- Telemetry query on /system xpaths does not work on QFX10002-36Q platform. PR1850033

- Traffic impact on MACsec enabled ports due to key length limit. PR1850387
- Host unreachable from the router with PPPoE when "routing-service" and "RPF-check" are enabled, and the route is learned via EBGP. PR1850562
- Packet duplication and flooding issues are seen when vpls bridge domain is configured on an aggregated Ethernet and label-switched interface across multiple line cards. PR1850604
- When BGP RIB Sharding is enabled, new BGP group/peer added gets stuck at Flags: <Sync InboundConvergencePending> PR1850620
- Chassis MX304 going offline due to Power-cycle. PR1850857
- Warning message is logged upon deleting VPLS neighbor PR1851083
- Erroneous data read from a temperature sensor caused MX304 to reboot. PR1851100
- EX3400 Dot1x Radius accounting send incorrect value to the server for Acct-Input-Gigawords/ Acct-Output-Gigawords PR1851299
- Packet drops are observed on rate-limited queues. PR1851317
- Observing stale entries under "show ptp phy-timestamping-interfaces. PR1851569
- Next-hop APIs to support LDP stitching cases over BGP routes pointing to list of indirects PR1851629
- After primary interface is explicitly disabled and then the VMhost is rebooted or clksyncd application is restarted, delay request packets are sent out of primary interface which is down, instead of secondary. PR1851730
- Intermittent traffic drops are seen due to large memory allocation for unidentified files. PR1851786
- [evpn_vxlan] [evpn_instance] ACX7100-32C :: JDI-RCT:l2ald core observed "hbt_descendent,hbt_delete ,l2ald_mac_ip_del_node" after loading the ERB Profile configs PR1852019
- Unintended reboots on QFX5120-48Y and EX4650-48Y platforms with Acbel PSU. PR1852227
- With rib-sharding enabled, IPFIX exports wrong SrcAS / DstAS fields PR1852278
- Memory leaks are seen in bbe-statsd process during the subscriber logout phase. PR1852532
- EVPN/VPLS protocol configuration through CLI is not allowed on device PR1852905
- On BNG CUPS controller loss of subscriber state is observed when cluster node restarts PR1853279

- On MX304 and MX platforms with MPC10,MPC11,LC9600 configured with Virtual Private LAN Service (VPLS) observe validation/installation errors logged by Advanced Forwarding Toolkit(AFT) in the PFE software. PR1853607
- Router flag is not getting set in Neighbor Advertisement message. PR1853868
- Devices fail to obtain an IP address when DHCP Security Option 82 is enabled PR1854253
- After the JNU config is deleted and added back jnuadmin's uid changes PR1854326
- Traffic drops are observed for v4ov6 traffic when next-hop information is not correctly configured on the backup RE during the switchover PR1854355
- jnud continues to further sync with the MX controller when the schema tar file failed to secure copy from satellite to the controller PR1854356
- The rpd gets struck with 100% CPU usage after enabling BGP RIB-Sharding PR1854481
- Slow commits and chassisd cores on backup RE. PR1854658
- Check for uniqueness of colors across flex-algorithm configurations. PR1855020
- On some FX platform parity error causes packet drop PR1855459
- ICMPv6 packets may be dropped instead of being translated using MAP-T <xref PR1855496
- IPv6 neighbor discovery with DHCP packet getting dropped when no-snoop option is enabled for DHCP Relay. PR1855624
- License is Missed Post System Reboot PR1855728.
- IPv4 Frameroutes with prefix length of less than /32 do not get applied. PR1855891
- During ISSU the repd experiences a process crash in the master RE during the image validation phase. PR1855947
- WAN Interfaces fail to receive hostbound traffic when OGE interface FIFO overflow error is detected PR1855966
- Aftd-trio core dump seen while removing subscribers (vbf) on an AFT based line card may result in a crash. PR1856393
- Input traffic on physical interface increases in the fabric statistics count despite locality bias feature configured. 1857225
- The chassisd process crash is seen after the device reboot when chassisd stalls after configuration commit. PR1857833
- Traffic drop is observed after removing the layer-2 policer from the IFL. PR1857934

- JUNOS_REG:: MX10008: After doing offline fpc, observing major alarms on FPC. PR1858079
- SPC3 SNMP : occasionally getting 0 value on jnxSpSvcSetIfCpuUtil, jnxSpSvcSetIfPctMemoryUsage andjnxSpSvcSetIfMemoryUsage64. PR1858550
- IPv6 link cannot be used for around 10 seconds after DAD finishing due to NS delay. PR1858741
- Route change is not synced after rpd restart due to rib-fib inconsistency PR1858750
- A momentary drop in traffic is observed when changes are applied on multipath SR-TE LSPs. PR1860334
- The rpd crash due to overlapping flow route updates in a single transaction PR1860888
- The authd process crashes when /etc/resolv.conf file is empty. PR1860913
- In an EVPN with IRB solution underlying NH change can cause packet drops on certain MX/EX platforms. PR1861020
- IS-IS enabled with BFD sessions go down when MACsec is enabled on IFL. PR1861054
- [MX] IPv6 Inline Distributed BFD sessions for ISIS fail to establish after applying CoS transmit-rate rate-limit configuration. PR1861238
- BGP PIC failover is taking longer than expected when IS-IS as an IGP enabled with LFA. PR1861451
- On srx4700, LACP is not coming up in distributed mode. PR1861483
- In BBE scenario the rebalancing event happens later than expected due to periodic rebalance interval miscalculation. PR1861619
- Random interfaces on MX304 remain in down state after an FPC reboot PR1861672
- FPC will crash in MX10003 during the Master switchover to RE1 or Master set to RE1. PR1863091
- On all Junos OS Evolved platforms, traffic loss will be seen after switching the LSP from SRTE to L-ISIS. PR1863248
- MAP-T translation does not work for upstream traffic. PR1863280
- Link error reported on one PFE(Packet Forwarding Engine) will also report error on other PFE. PR1863674
- Observing out-of-order packets when the TCP traffic gets passed over AE bundle and tunnelled via MPLSoUDP tunnel. PR1864237
- Due to race condition the FPC on MX platform crashes. PR1865576

- Traffic drop from subscriber will be observed when rpf-check knob is enabled under subscriber dynamic-profile with static underlying VLAN interface PR1865649
- The vms logical interface(s) remains down when inline-jflow is configured in the system PR1866570
- PPPoE subscriber login failures observed after interface flapping resulting in AC system errors on Junos MX Platforms PR1868007
- The rpd process crashes and asserts are seen due to memory leak. PR1868085
- After IPv6 tunnel is up and the iked daemon is restarted, post clearing of the IKE SA, ping from one end to the other end is not working as expected PR1869198
- Image validation fails during the Junos VM validation. PR1870082
- Link instability is seen on 4x10GSR and 40G-SR4 SFP modules from Finisar having high Rx output value. PR1870156
- RPD might crash when upgrading using no-validate. PR1870183
- Fragmented packets dropped in EVPN-MPLS scenario due to the IRB interface MTU limitation. PR1871420
- Filter-Based Forwarding (FBF) failed for over unicast IRB over AE on MX and EX platforms. PR1871698
- High memory and CPU usage due to unintended phone-home client activation. PR1871802
- The l2ald process crash is observed on non L2NG Junos platforms configured with "native-vlan-id" and "bridge-domains" on an IFL. PR1872280
- Packet loss or retransmissions observed on MX platforms using SFP-T transceivers PR1872743
- [MX] "smid ../../../../../../src/junos/lib/libsdb/licsubs/bsd12/liblicense_subs_os.c liblic_subs_total_active_licenses_in_use XXX" logs flood in license_flex_subs_trace.log. PR1873587
- The SPC3 card resets due to kernel memory exhaustion in MX Series platforms with highly scaled routing tables and Inline Active Flow Monitoring configured PR1873938
- EX9208: Syslog message 'JINSIGHTD_SENSOR_RESUBSCRIPTION' every 5 sec. PR1873990
- Transient traffic loss for CE in an EVPN MPLS setup with Multi-Homing. PR1874476
- JUNOS_REG: MX304 : Inline IKEv2 SA count verification failed, as IKE Security Associations did not come up following the rollback of the IPsec configuration. PR1876271
- The L2BSA subscriber fails to logout when "auto-configure-trigger" knob is edited on ANCP neighbour of MX platforms PR1877794

Infrastructure

- Memory leak is observed when Telemetry is configured. PR1865403

Interfaces and Chassis

- MTU configuration is not applied from the configuration group after commit and "warning" is seen PR1848768
- Routing instance knob for ICCP backup liveness detection PR1850316
- The jpppd process will crash with frequent subscribers login/logout PR1854387
- FPC process crash observed due to heap memory errors with Inline CFM and VLAN Normalisation PR1856132
- Observing traffic loss on PS service interface after deactivate and activate VPLS/EVPN instance type PR1858289

J-Web

- Unable to load J-Web after upgrading SRX when time zone is set to GMT+x or GMT-x. PR1851362

Layer 2 Features

- The snmp mib walk on jnxVplsPwBindTable fails with vpls routing-instances having multiple mesh-groups PR1806424

Layer 2 Ethernet Services

- DHCP-Relay short cycle protection can get stuck in Grace period PR1835753
- JDHCPD core @ ce_lease_time_compare GenAVLTreeDelete GenAVLTreeEntryDelete PR1835954
- DHCPv6 BLQ not working as expected PR1839348

- DHCPv6 Renew from a dual-stack CPE may be ignored if DHCP server is using DUID type 3 (DUID-LL) and DHCPv6 binding doesn't exist PR1843596
- AE member not able to discover lost LACP peer connection leading to traffic black-holing. PR1874126

MPLS

- Missing HELLO object in RSVP Hello messages after RE failovers in the NSR mode PR1792192
- RSVP authentication check fails if the length of the authentication-key is sixteen characters PR1850130
- The rpd process crashes due to memory exhaustion. PR1854623
- The "in-place-lsp-bandwidth-update" functionality does not work as expected. PR1854987
- Traffic loss will be observed when container-LSP with in-place-lsp-bandwidth-update configured. PR1857867
- RSVP-TE LSP path is not re-optimised to the path with best IGP metric. PR1859219
- The rpd with per-priority subscription configuration. PR1864823
- User traffic dropped after ISIS went down on one side with trapcode observed. PR1864949

Network Address Translation (NAT)

- The 'UI_CONFIGURATION_ERROR' error message is seen when a NAT rule-set has multiple rules PR1873928

Network Management and Monitoring

- Native junos modules in hello-message and yang modules in /var/run/db/yangs are not same PR1816904
- REST API doesn t work with passwords that includes the "%" character. PR1840232
- TCP session between syslog server and device remains in closed state PR1843602

- The eventd memory leak on Syslog over TLS with unconfigured PKI certificate PR1845058
- Unable to run event scripts for events: system_abnormal_shutdown/system_shutdown/ system_reboot_event PR1847814
- The eventd process crash occurs due to flooding of out of memory logs. PR1848106
- commit confirmed rpc request displays closing tag </commit-results> without opening tag <commit-results> in private mode PR1852868
- Syslog forwarding intermittently stops post DUT reboot on virtual devices. PR1853209
- SNMPV3 Engine-ID does not update to MAC address as configured PR1866948

Platform and Infrastructure

- On SRX300 series DHCP relay stops working and the device generates coredump after upgrading to JunOS 23.4R2-S2.1 PR1843935
- Traffic drops after link flap on active-active ESI setup with MAC pinning enabled PR1846365
- The standby router goes into the error state when the switchover is performed. PR1847307
- SCFD flow variation leads to error messages or process crash PR1848317
- The self-generated traffic on Junos platforms use the incorrect source IP with ECMP configuration PR1849296
- VPLS flooding is affected in mesh-group when one of the interfaces goes down PR1849854
- SCFD incorrectly decodes 802.1q tag as the source IP address for suspicious DHCPv4 flows PR1852259
- The forward next-hop for multicast is not updated during indirect next-hop change in VPLS PR1853874
- User root is shown as incorrect after power cycle of the device PR1855393
- ARP packet drops seen if proxy-arp restricted is configured on an IRB interface. PR1865605
- An IPv6 neighbor solicitation packet is dropped at the ingress PE router when it is received with more than two VLAN tags. 1874503
- FTP default mode changed from active to passive on 24.2R2 PR1874525
- ntp process may restart when issue the "show system ntp threshold" command PR1876690

Routing Policy and Firewall Filters

- Static route validation fails when using an interface-route leaked with rib-groups using "to rib <routing-instace-name>" as matching condition under rib-groups import-policy PR1849500

Routing Protocols

- The changes from instance-type DEFAULT_INSTANCE to others and vice versa will not be allowed PR1663776
- rt_instance memory leak on bulk configuration changes PR1832162
- BGP_PREFIX_THRESH_EXCEEDED warning message keeps flooding after accepted max prefix limit is reached PR1838490
- Link State of IS-IS IPv6 adjacency is not updated after FPC is restarted PR1847557
- The rpd crash on commit when configuring router-advertisement with DNS search label under 3 characters PR1847811
- Junos OS and Junos OS Evolved: Executing a specific CLI command when asregex-optimized is configured causes an rpd crash (CVE-2025-30652) PR1848929
- The CPU for the rpd stuck at 100% on Junos platforms PR1848939
- Memory leak is seen when BGP is activated and deactivated PR1849027
- BGP route still seen in routing table when route not available PR1849202
- L3VPN routes are not advertised to peer when BGP sessions with route-target filter flaps PR1849568
- Memory leak is observed when "graceful-shutdown" is configured PR1857801
- Incorrect subcode NOTIFICATION is sent when local interface is disabled for which multihop is configured for directly connected peer PR1859020
- BGP queue deadlock on Junos/Junos OS Evolved/cRPD platforms leading to route advertisement failure and traffic loss PR1860786
- The "advertise-inactive" configuration does not work as expected when "add-path multipath" is configured and negotiated with the neighbor PR1861799
- The rpd crash due to memory corruption in PIM/MSDP network PR1863470

- Valid BGP routes in RIB are displayed with verification state as Invalid PR1865114
- Too frequent LSP generation is observed on specific SR-LDP stitching scenario PR1865829
- Longer convergence is seen for a BGP neighbor having validation configured in its import policy PR1875144
- BGP updates missing graceful-shutdown community after quick sender knob flaps PR1877261
- rpd crash when changes are applied to as-path with dynamic-db in use PR1877288

Services Applications

- Traffic was lost on MX platforms following a Routing Engine failover PR1853304

Subscriber Access Management

- Error message is observed after device is restarted PR1813456
- CoA request failure from RADIUS over IPv6 PR1857161

User Interface and Configuration

- config rollback fails with commit error: Invalid XML from dfwd PR1829614
- On Junos OS Evolved platforms, HTTPS download fails when HTTPS URL is present in the configuration 1839955
- Multiple daemons crash upon ephemeral or static db commits PR1847834
- cli coredump genarated when the size of buffer area (user input) increased to 1GB PR1854070
- Unexpected issues such as login failures or disabled interfaces observed following abrupt reboot during commit operation 1861063

VPNs

- Master-encryption-password is not accessible when system is in FIPS mode PR1665506
- The MVPN traffic forwarding is affected when BGP PIC is enabled PR1861726
- IPSec tunnel inactive after multiple srg failovers on SRX platforms PR1868453

Migration, Upgrade, and Downgrade Instructions

IN THIS SECTION

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

Basic Procedure for Upgrading to Release 25.2R1

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

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

The installation process rebuilds the file system and completely reinstalls Junos OS. Configuration information from the previous software installation is retained, but the

contents of log files might be erased. Stored files on the routing platform, such as configuration templates and shell scripts (the only exceptions are the juniper.conf and ssh files might be removed. To preserve the stored files, copy them to another system before upgrading or downgrading the routing platform. For more information, see the Installation and Upgrade Guide.

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

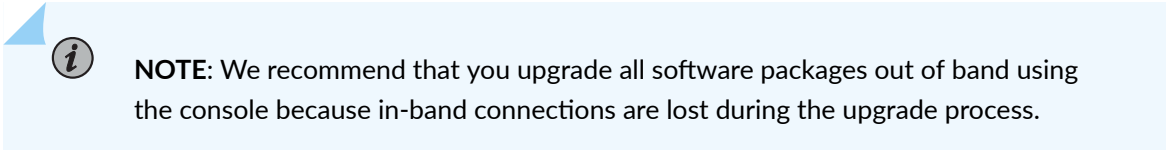
Procedure to Upgrade to Junos OS

To download and install Junos OS:

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

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

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



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-x86-32-25.2R1.9-signed.tgz
```

- For 64-bit Routing Engine version:

```
user@host> request system software add no-validate reboot source/junos-install-mx-x86-64-25.2R1.9-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-x86-32-25.2R1.x-limited.tgz
```

- For 64-bit Routing Engine version:

```
user@host> request system software add no-validate reboot source/junos-install-mx-x86-64-25.2R1.9-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*

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 25.2R1, in order to install a VM host image based on Wind River Linux 9, you must upgrade the i40e NVM firmware on the following MX Series routers:
  - MX240, MX480, MX960, MX2010, MX2020, MX2008, MX10016, and MX10008

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

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

Upgrade and Downgrade Support Policy for Junos OS Releases

We have two types of releases, EOL and EEOL:

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

For both EOL and EEOL releases, you can upgrade to the next three subsequent releases or downgrade to the previous three releases.

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

Table 6: EOL and EEOL Releases

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

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

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

Upgrading a Router with Redundant Routing Engines

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

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

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

Downgrading from Release 25.2R1

To downgrade from Release 25.2R1 to another supported release, follow the procedure for upgrading, but replace the 25.2R1 jinstall package with one that corresponds to the appropriate release.

NOTE: You cannot downgrade more than three releases.

For more information, see the Installation and Upgrade Guide.

Junos OS Release Notes for NFX Series

IN THIS SECTION

What's New

IN THIS SECTION

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

Authentication and Access Control

- **SSH enhancements for algorithm configuration (all Junos OS platforms)**—We've made the following updates to SSH algorithms:

- The CLI command `set system services ssh ca-signature-algorithms` should be used to configure the signature algorithms that are allowed for certificate authorities (CAs) to use when signing certificates.
- Under the `system services ssh hostkey-algorithm-list` hierarchy level, new options are introduced:
  - `set system service ssh hostkey-algorithm-list rsa-sha2-256`
  - `set system service ssh hostkey-algorithm-list rsa-sha2-512`

  These options enable RSA hostkey signatures using the SHA-256 hash algorithm and SHA-512 hash algorithm.
- RSA signatures using the SHA-1 hash algorithm have been disabled by default. Consequently, the CLI command `set system services ssh hostkey-algorithm-list rsa` has been deprecated.

[See hostkey-algorithm-list.]

What's Changed

IN THIS SECTION

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

General Routing

- SSH key options for user account credentials. You can configure key-options <key-options> option at the set system login user <user> authentication [ssh-rsa|ssh-ecdsa|ssh-ed25519] <ssh key> hierarchy level.

  [See login.]
- The `show subscribers extensive client-type dhcp | display xml validate` command has now been updated to display correct output instead of the `Duplicate data element` error message.

- **G.8275.1 profile configuration with PTP, SyncE, and hybrid mode (Junos)]**— On all Junos platforms, when configuring the G.8275.1 profile, it is mandatory to configure Precision Time Protocol (PTP), Synchronous Ethernet (SyncE), and hybrid mode. Earlier, the system would not raise a commit error even if the required hybrid and SyncE configurations were missing while configuring G.8275.1 profile. However, going forward you will not be able to configure the G.8275.1 profile without configuring PTP, SyncE and hybrid mode to be compliant with the ITU-T standards.

  [See G.8275.1 Telecom Profile.]

- **Extension of traceoptions support for VLANs in IGMP/MLD snooping**—The `traceoptions` option is supported under the `edit routing-instance protocols igmp-snooping vlan` and `edit routing-instance protocols mld-snooping vlan`hierarchy. `traceoptions` can be enabled for both specific and all vlans.

  [See (IGMP Snooping) and vlan (MLD Snooping).]

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.

General Routing

- On the NFXplatforms when one partition supports a Junos OS Release 23.4R1 image (supported on LTS19 operating sytem) and the other partition supports an image older than Junos OS Release 23.4R1 (supported on WRL8 operating system), the request vmhost reboot disk command is not executed as expected PR1753117..
- On the NFX350 devices, `srxpfe core` is seen.PR1792616.

VNFs

- On the NFX350 and NFX250 devices, VNF related SNMP traps are not generated when the client IP is configured.PR1868397.

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.

VNFs

- On the NFX350 with flex mode, traceoptions consume memory, which causes the the IKE (Internet Key Exchange) SAs (Security Associations) tunnel to be down for IPv6 with IKEv1. Users should enable selective traceoptions to allow other components to work with limited memory.

  PR1832087.

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.

Upgrade and Downgrade Support Policy for Junos OS Releases

We have two types of releases, EOL and EEOL:

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

For both EOL and EEOL releases, you can upgrade to the next three subsequent releases or downgrade to the previous three releases.

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

Table 7: EOL and EEOL Releases

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

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

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

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

Basic Procedure for Upgrading to Release 25.2

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

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 25.2R1:

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.

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.

Authentication and Access Control

- **SSH enhancements for algorithm configuration (all Junos OS platforms)**—We've made the following updates to SSH algorithms:

  - The CLI command `set system services ssh ca-signature-algorithms` should be used to configure the signature algorithms that are allowed for certificate authorities (CAs) to use when signing certificates.

  - Under the `system services ssh hostkey-algorithm-list` hierarchy level, new options are introduced:

    - `set system service ssh hostkey-algorithm-list rsa-sha2-256`

    - `set system service ssh hostkey-algorithm-list rsa-sha2-512`

    These options enable RSA hostkey signatures using the SHA-256 hash algorithm and SHA-512 hash algorithm.

  - RSA signatures using the SHA-1 hash algorithm have been disabled by default. Consequently, the CLI command `set system services ssh hostkey-algorithm-list rsa` has been deprecated.

  [See hostkey-algorithm-list.]

Dynamic Host Configuration Protocol

- **Display physical interface and VLAN ID in DHCP relay and server binding outputs (all Junos OS and Junos OS Evolved platforms)**—You can view the physical interface and VLAN ID in the outputs of the following commands:

  - `show dhcp relay binding`
  - `show dhcp server binding`
  - `show dhcpv6 relay binding`
  - `show dhcpv6 server binding`

  The enhanced output now displays data for **Physical interface** and **VLAN** alongside existing data. This addition facilitates easy understanding of client's binding origin.

  [See https://www.juniper.net/documentation/us/en/software/junos/cli-reference/topics/ref/command/show-dhcp-relay-binding.html and https://www.juniper.net/documentation/us/en/software/junos/cli-reference/topics/ref/command/show-dhcp-server-binding-command.html.]

EVPN

- **Configuration statements and `show` commands for troubleshooting EVPN with L2ALM context history (EX4100-24MP, EX4100-48MP, EX4400-24MP, EX4400-48MP, EX4650, MX204, MX240, MX304, MX480, MX960, MX2008, MX2010, MX2020, MX10003, MX10004, MX10008, MX10016, QFX5110, QFX5120-32C, QFX5120-48T, QFX5120-48Y, QFX5120-48YM, QFX10002, QFX10002-60C, QFX10008, and QFX10016)**—You can troubleshoot EVPN issues more effectively using updated configuration statements and `show` commands with Layer 2 Address Learning Manager (L2ALM) context history output. These tools assist in diagnosing and resolving Layer 2 learning and Ethernet switching context-related problems, enhancing your network management capabilities.

  [See l2-learning, ctxt-history, show l2-learning context-history, and show ethernet-switching context-history.]

- **Exception policy for enhanced OISM to avoid multicast traffic loss on packets with TTL=1 (EX4100-48MP, EX4100-24MP, EX4100-24T, EX4400-24MP, EX4400-24P, EX4400-24T, EX4400-24X, EX4400-48F, EX4400-48MP, EX4400-48P, EX4400-48T, EX4650, MX204, MX240, MX304, MX480, QFX5120-32C, QFX5120-48T, QFX5120-48T-VC, QFX5120-48Y, QFX5120-48Y-VC, and QFX5120-48YM)**—Enhanced optimized intersubnet multicast (OISM) routes most multicast traffic on the OISM supplemental bridge domain (SBD) rather than on the source VLAN, even if the destination OISM device hosts the source VLAN. This extra routing decrements a packet's time-to-live (TTL) more than once, so packets with TTL=1 don't reach the receivers. To avoid this problem on enhanced OISM devices, use the following steps to configure the devices to use the source VLAN instead of the SBD to forward multicast data to remote receivers:

1. Configure a routing policy *policy-name* at the `[edit policy-options policy-statement]` hierarchy level to match the multicast groups (or sources and groups) for which to forward multicast traffic on the source VLAN.

2. Set the `forward-policy` *policy-name* option at the `[edit routing-instances` *VRF-instance-name* `protocols evpn oism enhanced forward-on-source-bridge-domain]` hierarchy level to enable forwarding on the source VLAN instead of on the SBD for the multicast groups (or sources and groups) that match the policy.

You can configure and apply multiple policies with the `forward-policy` option.

[See forward-on-source-bridge-domain and Enhanced OISM Exception Policy to Forward on Source VLAN Instead of SBD for Packets with TTL=1.]

- **New CLI option to prevent host entries from occupying LPM table space (EX4100-24MP, EX4100-24P, EX4100-24T, EX4100-48MP, EX4100-48P, EX4100-48T, EX4100-F-12P, EX4100-F-12T, EX4100-F-24P, EX4100-F-24T, EX4100-F-48P, EX4100-F-48T, EX4300-MP, EX4400-24MP, EX4400-24P, EX4400-24T, EX4400-24X, EX4400-48F, EX4400-48MP, EX4400-48P, EX4400-48T, EX4650, QFX5120-32C, QFX5120-48T, QFX5120-48T-VC, QFX5120-48Y, QFX5120-48Y-VC, and QFX5120-48YM)**—You can prevent host entries from occupying longest prefix match (LPM) table space by configuring the `no-host-as-lpm` CLI option. This option blocks additional host entries from overflowing into the LPM table, ensuring that routing for these hosts is based solely on LPM routes. To enable this feature, use the `set forwarding-options no-host-as-lpm` command and restart the Packet Forwarding Engine. This preservation of LPM table space allows for accommodating more subnet routes, enhancing routing efficiency.

  [See Host Entry Overflow Prevention.]

- **NTP-based DF election for Ethernet segments (EX4400-24T and QFX5120-48T)**—You can use the NTP-based designated forwarder (DF) election option to synchronize DF elections for multihomed Ethernet segments. This option supports existing DF election algorithms and aligns DF election timing across all devices in the segment. Use this feature to enhance network stability and performance by minimizing loops, duplicates, and traffic discarding.

  To enable this feature, configure the `df-election-ntp` option under the `protocol evpn` hierarchy. A newly defined BGP extended community with a time synchronization (T) bit communicates the Service Carving Time (SCT) for synchronized timing.

  [See NTP-Based DF Election.]

- **Optimized EVPN-VXLAN DCI with enhanced OISM and an IPv6 underlay (EX4400-24MP, EX4400-24P, EX4400-24T, EX4400-24X, EX4400-48F, EX4400-48MP, EX4400-48P, EX4400-48T, EX4650, QFX5120-32C, QFX5120-48T, QFX5120-48T-VC, QFX5120-48Y, QFX5120-48Y-VC, and QFX5120-48YM)**—You can configure enhanced optimized intersubnet multicast (OISM) and seamless Data Center Interconnect (DCI) with EVPN-VXLAN instances on an IPv6 underlay. In EVPN-VXLAN DCI fabrics with enhanced OISM and an IPv6 underlay, DCI gateway (iGW) devices send EVPN Type

6 Selective Multicast Ethernet Tag (SMET) routes to remote iGW devices when hosts subscribe to multicast groups. iGW devices in the source data center selectively forward multicast traffic for a group across the DCI only if the remote data center has receivers subscribed to that group. Previously, the iGW devices always flooded multicast traffic across the interconnection even when the remote data center had no subscribed receivers.

[See EVPN-VXLAN DCI Multicast with Enhanced OISM.]

- **Support for excluding specific MAC addresses from duplicate MAC detection (EX4100-24MP, EX4100-24T, EX4100-48MP, EX4300-MP, EX4400-24MP, EX4400-24P, EX4400-24T, EX4400-24X, EX4400-48F, EX4400-48MP, EX4400-48P, EX4400-48T, EX4650, QFX5120-32C, QFX5120-48T, QFX5120-48T-VC, QFX5120-48Y, QFX5120-48Y-VC, and QFX5120-48YM)**—You can configure an exclusion list for MAC addresses in EVPN networks to prevent legitimate MAC address movements from being marked as duplicates. Use `set protocols evpn mac-list` *`list_name`* `mac-address` *`mac_address_with_prefix_len`* to create the list and `set protocols evpn duplicate-mac-detection exclude-list` *`list_name`* to apply it. This feature helps maintain network stability by avoiding unnecessary duplicate MAC detection for specified addresses, particularly in scenarios involving virtual MAC configurations in redundant setups.

  [See EVPN Duplicate MAC Detection Exclusion Lists.]

IPv6

- **Route-based proxy neighbor discovery for VM gateways (QFX5110, QFX5120-32C, QFX5120-48T, QFX5120-48Y, QFX5120-48YM, QFX5200, QFX5210 switches)**—Use route-based proxy neighbor discovery to address network connectivity issues between hosts on different physical networks. This approach enables the gateway to send its MAC address to the source host, facilitating communication over routes instead of Layer 2 switching. By maintaining host routes in the routing table, you can ensure reachability and redistribute routes into BGP or interior gateway protocols (IGPs). Note that, the QFX5000 series supports proactive Address Resolution Protocol (ARP) detection, but doesn't support proactive IPv6 neighbor learning. You can use this method only with default routing tables.

  [See NDP Proxy Support For User Routes.]

Layer 2 VPN

- **Layer 2 circuit support for aggregated Ethernet interfaces (EX4650 and QFX5120 line)**—You can use aggregated Ethernet interfaces when connecting to Layer 2 circuits. This feature provides the following benefits:
  - Enhanced network resilience
  - Load balancing across the member links
  - Increased bandwidth capacity

[See Configuring Interfaces for Layer 2 Circuits and Aggregated Ethernet Interfaces.]

MAC Learning

- **Support to learn the MAC-IP information of the host (QFX5120 switches)**—You can use MAC-IP snooping for non-EVPN VLANs to learn the MAC-IP information of the host. Use the new command `global-mac-ip-snooping` in the `[edit protocols l2-learning]` hierarchy to enable this feature. The `show ethernet-switching mac-ip-table` command output displays the MAC IP information. You can verify whether MAC-IP snooping is enabled for a VLAN by using the `show vlans extensive` command. You can disable the feature for a VLAN by using the new command `no-mac-ip-snooping` in the `[edit vlans <vlan-name> switch-options]` hierarchy.

  [See https://www.juniper.net/documentation/us/en/software/junos/cli-reference/topics/ref/statement/global-mac-ip-snooping-edit-protocols-l2-learning.html and https://www.juniper.net/documentation/us/en/software/junos/cli-reference/topics/ref/statement/no-mac-ip-snooping-edit-vlans-switch-options.html.]

Multicast

- **New options introduced for the `show multicast snooping route` command (QFX5110 and QFX5120-32C)**—We now support the `l3-irb-elaboration` and `evpn-core-nh-route` options for the `show multicast snooping route` command. The command output displays the entries in the multicast forwarding table that were learned from snooping through integrated routing and bridging (IRB) or EVPN.

  [See https://www.juniper.net/documentation/us/en/software/junos/cli-reference/topics/ref/command/show-multicast-snooping-route-command.html.]

Network Management and Monitoring

- **1:N port mirroring for sending a source packet to multiple Layer 2 destinations (QFX5120-32C, QFX5120-48T, QFX5120-48Y, QFX5120-48YM, QFX5200, and QFX5210)**—You can use the 1:N port mirroring feature to mirror traffic to multiple Layer 2 destinations. This feature requires either one or both of the following configurations:

  - A port-mirroring instance that is based on a firewall filter. Use the configuration statements in the `[edit forwarding-options port-mirroring instance]` hierarchy.
  - A native analyzer. Use the configuration statements in the `[edit forwarding-options analyzer]` hierarchy.

  For both the configuration methods, you must also configure next-hop groups with a group type of `layer-2` to direct the mirrored packets to their destinations.

  [See 1:N Port Mirroring to Multiple Destinations on Switches.]

- **Enhancement to hardware resource threshold monitoring for capacity planning (QFX5120-32C, QFX5120-48T, QFX5120-48Y, and QFX5120-48YM)**—You can monitor additional hardware resources for capacity planning by using the hardware resource threshold monitoring feature. Use the `system packet-forwarding-options hw-resource-monitor resource-list` configuration statement at the `[edit]` hierarchy level to create a list of hardware resources that you want to monitor. Once configured, periodic resource monitoring occurs at the polling interval you set.

  [See Configure Hardware Resource Threshold Monitoring for Capacity Planning and resource-list (Network Management).]

- **IPv6 collector support for sFlow technology with EVPN-VXLAN (EX4100-48MP, EX4100-H-12MP, EX4100-H-24MP, EX4100-H-24F, EX4100-H-24F-DC, 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, EX4400-24MP, EX4400-24P, EX4400-24T, EX4400-24X, EX4400-48F, EX4400-48MP, EX4400-48MXP, EX4400-48XP, EX4400-48P, EX4400-48T, EX4650, QFX5120-32C, QFX5120-48T, QFX5120-48Y, and QFX5120-48YM)**—You can use IPv6 collector for sFlow technology to monitor known multicast traffic in EVPN-VXLAN deployments. The system supports both IPv4 and IPv6 traffic and includes management interface support for IPv6 collectors. With this functionality, you can efficiently monitor and analyze network performance across different interfaces.

  [See sFlow Support on Switches.]

Software Installation and Upgrade

- **Support of routing-instance option (QFX Series)**—The routing-instance option is newly introduced for the request system software add command on QFX5110, QFX5110-VC, QFX5110-VCF, QFX5120-32C, QFX5120-48T, QFX5120-48T-VC, QFX5120-48Y, QFX5120-48Y-VC, QFX5120-48YM, QFX5200, QFX5210, and QFX10002 devices. Use this option to specify the routing-instance to download the package for installation.

  [See request system software add (Junos OS).]

Virtual Chassis

- **Synchronize Virtual Chassis configuration using SCP (EX4300-MP, EX4400-24MP, EX4400-24P, EX4400-24T, EX4400-24X, EX4400-48F, EX4400-48MP, EX4400-48MXP, EX4400-48XP, EX4400-48P, EX4400-48T, QFX5120-32C, QFX5120-48T, QFX5120-48T-VC, QFX5120-48Y, QFX5120-48Y-VC, and QFX5120-48YM)**—You can use Secure Copy Protocol (SCP) to securely transfer configuration data in a Virtual Chassis from the Virtual Chassis member in the primary Routing Engine role to a Virtual Chassis member in the backup Routing Engine role or line-card role. Synchronization occurs when a configuration is committed on the primary Virtual Chassis member, when a line-card member reboots, or when a new line-card member is added to the Virtual Chassis. When FIPS is enabled, the system uses SCP by default to synchronize configuration data.

  You must enable the `system commit config-sync-with-scp` configuration to use SCP for synchronization.

[See Configure Synchronization of Configuration Data Using SCP in a Virtual Chassis.]

What's Changed

IN THIS SECTION

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

General Routing

- SSH key options for user account credentials. You can configure key-options <key-options> option at the set system login user user authentication **ssh-rsa|ssh-ecdsa|ssh-ed25519** <ssh key> hierarchy level.

  [See login.]

- **Changes to `show system alarms` command output (QFX5130 and QFX5220)**—When the current version of the firmware is less than the minimum supported version, you can now see alarms for this mismatch in the output of the command. These alarms were not shown previously. For example, when you have a firmware version mismatch, you should now see output similar to the following:

```
user@host> show system alarms 18 alarms currently active Alarm time Class Description
2024-09-09 04:55:00 PDT Minor CHASSIS 0 BIOS ROM minimum supported firmware version mismatch
2024-09-09 04:55:20 PDT Minor CHASSIS 0 Fan CPLD minimum supported firmware version mismatch
2024-09-09 04:55:19 PDT Minor CHASSIS 0 Optics CPLD minimum supported firmware version
mismatch
```

- **Option allow-transients is set by default for the EZ-LAG commit script**—The EZ-LAG feature simplifies setting up EVPN multihoming configurations using a set of configuration statements and a commit script. The commit script applies transient configuration changes, which requires the `allow-`

transients system commit scripts option to be set. Now the default system configuration sets the allow-transients option at the EZ-LAG commit script file level, removing the need to set this option manually. In earlier releases where this option isn't set by default, you must still configure the option explicitly either globally or only for the EZ-LAG commit script.

[See Easy EVPN LAG Configuration Overview.]

- **Reset high-power optics(QFX5130-32CD, QFX5130-48C, QFX5130-48CM, QFX5220-32CD, QFX5220-128C, QFX5230, and QFX5240)**—Junos OS automatically shuts down high-power optics upon Fire Shutdown threshold breach. Use the request interface optics-reset command to re-enable normal operation.

  [See request interface optics-reset.]

EVPN

- **Duplicate MAC detection timeout (QFX5000 Series switches and EX4650 switches)**—The default setting for auto-recovery-time is 5 minutes on these platforms only.

  [See duplicate-mac-detection.]

User Interface and Configuration

- **Access privileges for request support information command (ACX Series, EX Series, MX Series, QFX Series, SRX Series Firewalls, and vSRX Virtual Firewall)**— The request support information command is designed to generate system information for troubleshooting and debugging purposes. Users with the specific access privileges maintenance, view, and view-configuration can execute request support information command.

- **Changes to the show system storage command output (ACX Series, EX Series, MX Series, QFX Series, and SRX Series)**—We've updated the show system storage command output to include only true (physical) storage and exclude any host/hypervisor level storage. In earlier releases, the output also includes a container/jail storage, which does not have a separate storage of its own.

  [See show system storage.]

- **Option to view combined disk space usage statistics for all configuration databases (ACX Series, EX Series, MX Series, QFX Series, SRX Series, and vSRX)**—The show system configuration database usage command provides the merge option. When you include the merge option, the command output displays combined disk space usage statistics for all configuration databases, including the static configuration database and all ephemeral configuration database instances.

[See show system configuration database usage.]

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

- Channelized interfaces leds are not properly represented in `show chassis led`.PR1720502
- Problem: Performing VC split and Merge operation causes traffic to be affected for Broadcast, Unknown-unicast and Multicast traffic. RCA: When the link is brought down, each FPC will try to re-synchronize the IFDs, in addition resources are busy with updating for the new role. This can cause some synchronization issues with for IFDs/IFLs and other such lists. Test: This can be seen by the VTY command `show ifd brief` and `show ifl brief` for all the FPCs Workaround: It is recommended to wait at least 240 seconds after splitting the VC ad merging it back again. This ensures that the system can get enough time to synchronize the IFDs/IFLs etc. from the kernel.PR1867979

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

- In a QFX51200-48YM-8C VC setup, after a a primaryship switch over fan tray of linecard might not be displayed in show chassis hardware and show chassis environment. There is no functional impact. PR1758400
- There exists a hidden CLI upgrade option to do "clean-install". This has been enabled in 23.4R2-S3 and Mainline from 25.1R1 onwards. Using CLI upgrade with this option will do a "nist" compliant secure-erase for SATA disks. This method of CLI upgrade needs to be used with caution since this will wipe clean all configs/logs/files on the SATA FS and re-install the image.PR1847058
- There is an inconsistency in the way auto channelization works. Based on the peer status it might split up unexpectedly. So for configuration which requires a specific speed/channelization we recommend setting the port manually. PR1852964
- A memory corruption issue can result random dcpfe (dense concentrator packet forwarding engine) process crashes on all Junos QFX and EX platforms configured with VXLAN (Virtual Extensible Local Area Network) configuration. PR1856424
- On QFX10K2-60C switches, if traffic is coming from MPLS and going towards EVPN VXLAN tunnel (problem with the next-hop via ARP/IPV6 NDP to reach final destination IP) then traffic drop will be seen. PR1861501
- On QFX10002-60C platforms when ECMP is required to get multiple-path to multiple hosts connected, and with IPV6 address configured as a destination address, the destination MAC rewrite process fails, due to the unilist nexthop for IPv6 destination is getting overwritten. This leads the IPv6 packets to the host, to get dropped over the ECMP routes. PR1865354

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.

General Routing

- JDI_REG::QFX5200:: After ISSU upgrade, device is hanged and not able to perform any operations until USB recovery done on device. PR1703229
- The remote end of port JNP-SFPP-10GE-T doesn't shut down when the hardware is rebooted using request system reboot. PR1820286
- The SFP 10GBASE-T part No. 740-083295 on platforms running Junos is unable to detect a linkdown. PR1823771
- On an EX4400 device with 4x25G Uplink module configured in 1GE or 25G speed, peer side of an interface with 10GBASE-T transceiver may remain up even when the IFD(xe-x/2/y) is not created. PR1831409
- VRRP fails on 802.1Q VLAN Layer 3 logical interface on QFX10002-60C. PR1834429
- QFX5000: DHCP6 solicit packets are hitting CPU Queue 28 instead of DHCP queue 17. PR1837638
- The VXLAN ARP packets goes to the ARP queue 34 after disabling ARP suppression. PR1840251
- QFX5210/AS7816 lpm ip route install failed due to table full unit 0. PR1841913
- Incorrect MTU value in the ICMP Next-Hop MTU field, regardless of the actual MTU of the outgoing interfaces. PR1842744
- VLAN tagging in Q-in-Q is not handled correctly over EVPN-VxLAN. PR1843817
- The push pop function on the QFX5120 and EX4650 is not correctly pushing the VLAN. PR1844853
- Unnecessary trace log files related to licenses are generated. PR1845079

- Interface flap between the QFX5120 and QFX5210 with QSFP-100G-LR4-T2 optics. PR1845158
- QFX5000 TVP platforms clean-install support with nist compliant secure-erase. PR1847058
- Handling AE Child Members, VT port properties reset when access port is destroyed. PR1849952
- Telemetry query on /system xpaths does not work on QFX10002-36Q platform. PR1850033
- Duplication of DHCP request packets when unicast to VRRP gateway. PR1850203
- The l2ald process crash is observed when same Type 5 MAC-IP received with same IP and different MAC. PR1852019
- The dcpfe crash will be seen on Junos QFX5200 platforms due to route churn. PR1854995
- Warning message 'Too many VLAN-IDs on untagged interface' is seen when 2049 VLANS are configured on trunk LAG interface. PR1855085
- On some QFX platform parity error causes packet drop. PR1855459
- Traffic drop observed due to ECMP next-hop programming issue. PR1855990
- Port mirroring fails due to mismatched analyzer and outgoing interface configuration. PR1856361
- On particular QFX and EX devices firewall filter counters display double the actual packet count. PR1863813
- L2ald process crash is observed upon executing hidden command `show ethernet-switching debug-statistics fast-mac-update` in case the command doesn't have any output. PR1864295
- The dcpfe crash is seen in the EVPN-VXLAN scenario. PR1865432
- Command `show pfe vxlan` is not supported on QFX5200 devices. PR1866130
- Traffic loss is seen due to ECMP resource exhaustion on QFX5200, even after ECMP group usage is lower than the threshold. PR1870380
- ON QFX5000 platforms a log is required for route leaking when destination table hits a platform limitation. PR1876359

EVPN

- RPD core-dump on 22.2R3-S4. PR1841965
- Few seconds traffic loss during previous DF coming back with EVPN-VPWS non-revertive DF preference feature enabled. PR1851659

Interfaces and Chassis

- Routing instance knob for ICCP backup liveness detection. PR1850316
- The jpppd process will crash with frequent subscribers login/logout. PR1854387

Layer 2 Ethernet Services

- Unable to assign an IP address on management interface with DHCP configuration even if DHCP is bound after a power cycle. PR1854827
- DNS resolution will fail for DNS entries written to **resolv.conf**. PR1872292

Platform and Infrastructure

- FTP default mode changed from active to passive on 24.2R2. PR1874525

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

4. In the Install Package section of the Software tab, select the QFX Series Install Package for the 25.2 release.

   An Alert box appears.

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

   A login screen appears.

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

7. Download the software to a local host.

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

9. Install the new jinstall package on the device.

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

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

```
user@host> request system software add source/jinstall-host-qfx-5-x86-64-25.2-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 25.2 `jinstall` package, you can issue the `request system software rollback` command to return to the previously installed software.

Installing the Software on QFX10002-60C Switches

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

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

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

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

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

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

For example:

```
user@switch> request vmhost software add /var/tmp/junos-vmhost-install-qfx-x86-64-25.2R1.9.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-
x86-64-25.2R1.9.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-x86-64-25.2R1.n-secure-signed.tgz reboot
```

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

For example:

```
user@switch> request system software add ftp://ftpserver/directory/jinstall-host-qfx-10-f-x86-64-25.2R1.n-secure-signed.tgz reboot
```

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

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

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

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-
x86-64-25.2R1.n-secure-signed.tgz
```

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

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

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

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-
x86-64-25.2R1.n-secure-signed.tgz
```

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

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

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

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

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

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

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

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

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

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

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

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

```
  Slot 0:
    Current state                  Master
    Election priority              Master (default)

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

Performing a Unified ISSU

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

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

Perform the following tasks:

- "Preparing the Switch for Software Installation" on page 115
- "Upgrading the Software Using Unified ISSU" on page 116

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-x86-64-25.2R1.n-secure-signed.tgz`.

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

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

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

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

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

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

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

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

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

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

Upgrade and Downgrade Support Policy for Junos OS Releases

We have two types of releases, EOL and EEOL:

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

For both EOL and EEOL releases, you can upgrade to the next three subsequent releases or downgrade to the previous three releases.

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

Table 8: EOL and EEOL Releases

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

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

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

Junos OS Release Notes for SRX Series

IN THIS SECTION

What's New

IN THIS SECTION

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

Hardware

- **New SRX4700 Firewall**—The SRX4700 is a 1-RU fixed form-factor firewall offering next-generation firewall capabilities. The SRX4700 targets medium to large enterprise edge, campus edge, data center edge firewall, data center core firewall, and secure VPN concentrator or router for distributed enterprise use cases. These use cases include SD-WAN, and service provider roaming firewall, N6/Gi firewall, distributed security gateway, and core security gateway.

Table 9: SRX4700 Firewall Feature Support

Feature	Description

Chassis	• Chassis management support. The SRX4700 supports chassis management features, such as:
	  • Facilitate maintenance and system upgrades.
	  • Manage voltage and temperature sensors to improve system reliability and stability.
	  • Offer clear visual indicators through LED control for system components, aiding quick diagnostics and status evaluations.
	  • Optimize thermal management by adjusting fan speeds based on conditions, extending hardware lifespan, and assuring optimal operating conditions. Use the `show chassis enhanced-temperature-thresholds` command to view the temperature threshold values.
	[See show chassis enhanced-temperature-thresholds and Chassis-Level User Guide.]

Class of service (CoS)	• Support for CoS [See Understanding Class of Service.]

Table 9: SRX4700 Firewall Feature Support *(Continued)*

Feature	Description
Hardware	• The SRX4700 is a compact 1-RU form factor, high-performance, next generation firewall offering scalable security services. The firewall supports 1.4-Tbps Internet mix (IMIX) throughput, making it ideal for service providers, cloud providers, and large enterprises. In addition, enterprises can deploy the SRX4700 as data center core and data center edge firewalls and as a secure SD-WAN hub. The SRX4700 is a 1-U chassis with the following ports: • Two 400GbE QSFP-DD ports • Ten 100GbE QSFP28 ports • Sixteen 50GbE SFP56 ports • Two 1GbE SFP HA ports [See SRX4700 Firewall Hardware Guide.]

Table 9: SRX4700 Firewall Feature Support *(Continued)*

Feature	Description

High availability (HA) and resiliency	• Support for BFD
	  • Support up to 3 x 300-millisecond (ms) failure detection time
	  • Support up to 100 BFD sessions
	  [See Understanding BFD for Static Routes for Faster Network Failure Detection and Understanding How BFD Detects Network Failures.]
	• Support for Multinode High Availability (MNHA) in active/backup mode in routing, hybrid, and default gateway deployments.
	  [See Multinode High Availability.]
	• Support for IPsec VPN tunnels in an MNHA setup
	  [See IPsec VPN Support in Multinode High Availability.]
	• Resiliency support for platform components on SRX4700 devices
	  [See Resiliency.]

Table 9: SRX4700 Firewall Feature Support *(Continued)*

Feature	Description
Install and Upgrade	• Support for firmware (`jfirmware`) [See Installing and Upgrading Firmware, request system firmware upgrade, and show system firmware.] • Support for BIOS, Secure Boot, and bootloader [See Upgrading the Boot Loader on SRX Series Devices and Junos OS Overview.] • Support for secure zero-touch provisioning (SZTP) [See Secure Zero Touch Provisioning and Generate Secure ZTP Vouchers.] • Support for switching between SZTP and ZTP [See Switching between Secure Zero Touch Provisioning and Zero Touch Provisioning.]
Interfaces	• Port configuration and supported speeds. SRX4700 features a Packet Forwarding Engine logically divided into two identical Physical Interface Cards (PICs). Each PIC provides 14 front-panel ports configured with a mix of high-speed interfaces (1x400GbE, 5x100GbE, and 8x50GbE) ensuring a high-density networking solution for various high-throughput applications. [See Port Speed on SRX Series Firewalls.]

Table 9: SRX4700 Firewall Feature Support *(Continued)*

Feature	Description
Junos telemetry interface	Support for telemetry streaming with operational state sensors under the following resource paths: • **/junos/events** • **/junos/task-memory-information/** • **/interfaces/** • **/components/** • **/network-instances/network-instance/protocols/protocol/bgp/** • **/network-instances/network-instance/protocols/protocol/isis/levels/level/** • **/network-instances/network-instance/protocols/protocol/isis/interfaces/interface/** • **/network-instances/network-instance/mpls** • **/lacp/** • **/lldp/** • **/arp-information/** • **/nd6-information/** • **/ipv6-ra/** [See Junos YANG Data Model Explorer.]
J-Web	• J-Web support. You can monitor, configure, troubleshoot, and manage SRX4700 Firewalls using J-Web. [See The J-Web Setup Wizard, Dashboard Overview, Monitor Interfaces, and About Reports.]

Table 9: SRX4700 Firewall Feature Support *(Continued)*

Feature	Description
Layer 7 security features	• Support for advanced policy-based routing (APBR) [See Advanced Policy-Based Routing.] • Support for application identification (AppID) [See Application Identification.] • Support for application quality of experience (AppQoE) [See Application Quality of Experience.] • Support for application quality of service (AppQoS) [See Application QoS.] • Support for Content Security [See Content Security Overview.] • Support for intrusion detection and prevention (IDP) [See Intrusion Detection and Prevention Overview.] • Support for Juniper ATP Cloud [See File Scanning Limits.] • Support for Juniper Networks Deep Packet Inspection-Decoder (JDPI-Decoder) [See Juniper Networks Deep Packet Inspection-Decoder (JDPI-Decoder).] • Support for SSL proxy [See SSL Proxy.]

Table 9: SRX4700 Firewall Feature Support *(Continued)*

Feature	Description
MACsec	• Support for Media Access Control Security (MACsec) on physical interfaces for Layer 3 traffic. This implementation of MACsec supports: • Alignment with IEEE 802.1AE and IEEE 802.1X-2010 standards • Static connectivity association key (CAK) mode with preshared keys (PSKs) • Switch-to-switch port protection • The encryption types GCM-AES-128, GCM-AES-256, GCM-AES-XPN-128, and GCM-AES-XPN-256 • Revenue port in standalone mode [See Configuring MACsec.]
Optics	• Select your product in the Hardware Compatibility Tool to view supported transceivers, optical interfaces, and direct attach copper (DAC) cables for your platform or interface module. We update the HCT and provide the first supported release information when the optic becomes available [See Hardware Compatibility Tool.]

Table 9: SRX4700 Firewall Feature Support *(Continued)*

Feature	Description
Services applications	• Express Path [See Express Path Overview and enhanced-mode.] • Support for Application Layer Gateway (ALG) [See ALG Overview.] • Support for DNS [See Understanding and Configuring DNS, DNS ALG, DNS Proxy Overview, DNS Names in Address Books, and DNSSEC Overview.] • Support for user authentication [See User Authentication Overview.] • Support for security policies [See Configuring Security Policies.] • Support for security zones [See Security Zones.] • Support for Network Address Translation (NAT) [See NAT Configuration Overview.] • Support for screens options for attack detection and prevention [See Screens Options for Attack Detection and Prevention.] • Support for traffic processing [See Traffic Processing on SRX Series Firewalls Overview.] • Support for integrated user firewall [See Configure Integrated User Firewall.]

Table 9: SRX4700 Firewall Feature Support *(Continued)*

Feature	Description
	• Support for PowerMode IPsec (PMI) [See PowerMode IPsec.] • Support for DHCP [See DHCP Overview.] • Support for GTP and SCTP [See Monitoring GTP Traffic and SCTP Overview.] • Support for on-box reporting [See report (Security Log).] • Support for inline active flow monitoring [See Understand Inline Active Flow Monitoring.] • Support for TWAMP [See Understand Two-Way Active Measurement Protocol.] • Support for RPM [See Real-Time Performance Monitoring for SRX Devices.] • Support for logical systems [See Logical Systems Overview.]

- **New SRX4120 Firewall**—The SRX4120 Firewall provides next-generation firewall capabilities and advanced threat detection and mitigation. This firewall is ideal for small-medium enterprise edge, campus edge, data center edge firewall and secure VPN router deployments for distributed enterprise use-cases.

Table 10: Features Supported on SRX4120 Firewall

Feature	Description
Chassis	• Support for chassis management and temperature monitoring infrastructure [See Chassis-Level User Guide.]
Chassis Cluster	• Support for ISSU and dual control links with MACsec [See Upgrading a Chassis Cluster Using In-Service Software Upgrade and Media Access Control Security (MACsec) on Chassis Cluster.]
Class of service (CoS)	• Support for CoS [See Understanding Class of Service.]

Hardware	• The SRX4120 is a 1-U chassis with the following ports. All the ports are MACsec capable ports:
	  • Eight 10Gigabit-Ethernet (GbE) BASE-T ports
	  • Eight 10GbE SFP+ ports
	  • Four 1/10/25GbE SFP28 ports
	  • Two 40/100GbE QSFP28 ports
	  • Two 1GbE SFP high availability ports
	
	To install the SRX4120 hardware and perform initial software configuration, routine maintenance, and troubleshooting, see SRX4120 Firewall Hardware Guide.
	
	[See Feature Explorer for the complete list of features for any platform.]

Table 10: Features Supported on SRX4120 Firewall *(Continued)*

Feature	Description

High availability (HA) and resiliency	• Support for BFD
	  • Support up to 3 x 300 msec failure detection time
	  • Support up to 100 BFD sessions
	  [See Understanding BFD for Static Routes for Faster Network Failure Detection and Understanding How BFD Detects Network Failures.]
	• Support for MNHA
	  [See Multinode High Availability.]

Interfaces	Supports four PICs (PIC 0, PIC 1, PIC 2, and PIC 3) with the following interfaces: • PIC 0 has eight Base-T interfaces • PIC 1 has eight SFP+ interfaces • PIC 2 has four SFP28 interfaces • PIC 3 has two QSFP28 interfaces The Junos OS creates PIC 0 ports by default. You can channelize the QSFP28 (PIC 3) ports into 4x25 Gbps and 4x10 Gbps. [See Port Speed on SRX Series Firewalls.]

Table 10: Features Supported on SRX4120 Firewall *(Continued)*

Feature	Description
Junos Telemetry Interface	Junos telemetry interface (JTI) streaming support for the following sensors: • System log messages (/junos/events/) • Memory utilization for routing protocol tasks (/junos/task-memory-information/) • Interfaces (/interfaces/) • Hardware operational states for Routing Engine, power supply units (PSUs), switch fabric boards, control boards, switch interface boards, MICs, and PICs (/components/) • Sensor for flow sessions (/junos/security/spu/flow/) [See Junos YANG Data Model Explorer.]

Table 10: Features Supported on SRX4120 Firewall *(Continued)*

Feature	Description
Layer 7 security features	• Support for advanced policy-based routing (APBR) [See Advanced Policy-Based Routing.] • Support for application identification (APPID) [See Application Identification.] • Support for application quality of experience (AppQoE) [See Application Quality of Experience.] • Support for application quality of service (AppQoS) [See Application QoS.] • Support for Content Security [See Content Security Overview.] • Support for intrusion detection and prevention (IDP) [See Intrusion Detection and Prevention Overview.] • Support for Juniper Advanced Threat Prevention (ATP) Cloud [See File Scanning Limits.] • Support for Juniper Networks Deep Packet Inspection-Decoder (JDPI) [See Overview.] • Support for Cloud Access Security Broker (CASB) [See Cloud Access Security Broker (CASB).] • Support for SSL proxy

Table 10: Features Supported on SRX4120 Firewall *(Continued)*

Feature	Description
	[See SSL Proxy.]
MACsec	• Support for Media Access Control Security (MACsec) [See Understanding Media Access Control Security (MACsec).]
Network management and monitoring	• Support for the filter based packet capture which captures the real-time data packets traveling over the network. Support for datapath debugging is not yet available. [See Example: Configure a Firewall Filter for Packet Capture.]

Table 10: Features Supported on SRX4120 Firewall *(Continued)*

Feature	Description
Services applications	• Support for Application Layer Gateway (ALG) [See ALG Overview.] • Support for Domain Name System (DNS) [See Understanding and Configuring DNS, DNS ALG, DNS Proxy Overview, DNS Names in Address Books, and DNSSEC Overview.] • Support for user authentication [See User Authentication Overview.] • Support for security zones [See Security Zones.] • Support for Network Address Translation (NAT) [See NAT Overview.] • Support for screens options for attack detection and prevention [See Screens Options for Attack Detection and Prevention.] • Support for traffic processing [See Traffic Processing on SRX Series Firewalls Overview.] • Support for user identity [See Identity Aware Firewall.] • Support for PowerMode IPsec (PMI) [See PowerMode IPsec.] • Support for DHCP [See DHCP Overview.]

Table 10: Features Supported on SRX4120 Firewall *(Continued)*

Feature	Description
	• Support for GPRS Tunneling Protocol (GTP) and Stream Control Transmission Protocol (SCTP) [See Monitoring GTP Traffic and SCTP Overview.] • Support for on-box reporting [See report (Security Log).] • Support for inline active flow monitoring [See Understand Inline Active Flow Monitoring.] • Support for Two-Way Active Measurement Protocol (TWAMP) [See Understand Two-Way Active Measurement Protocol.] • Support for real-time performance monitoring (RPM) [See Real-Time Performance Monitoring for SRX Devices.] • Support for logical systems [See Logical Systems Overview.]
Software Installation and Upgrade	• Support for BIOS, Secure Boot and boot loader [See Secure Boot.] • Support for Jfirmware [See request system firmware upgrade and show system firmware.] • Support for secure ZTP [See Secure Zero Touch Provisioning.]

Table 10: Features Supported on SRX4120 Firewall *(Continued)*

Feature	Description
User access and authentication administration	• Support for trusted platform module [See SZTP Infrastructure Components.]

Authentication and Access Control

- **SSH enhancements for algorithm configuration (all Junos OS platforms)**—We've made the following updates to SSH algorithms:

  - The CLI command `set system services ssh ca-signature-algorithms` should be used to configure the signature algorithms that are allowed for certificate authorities (CAs) to use when signing certificates.

  - Under the `system services ssh hostkey-algorithm-list` hierarchy level, new options are introduced:

    - `set system service ssh hostkey-algorithm-list rsa-sha2-256`

    - `set system service ssh hostkey-algorithm-list rsa-sha2-512`

    These options enable RSA hostkey signatures using the SHA-256 hash algorithm and SHA-512 hash algorithm.

  - RSA signatures using the SHA-1 hash algorithm have been disabled by default. Consequently, the CLI command `set system services ssh hostkey-algorithm-list rsa` has been deprecated.

  [See hostkey-algorithm-list.]

Device Security

- **Override default minimum TTL for DNS caching (cSRX, SRX Series Firewalls, and vSRX 3.0)**—Override the default minimum time-to-live value (TTL) value for fully qualified domain names (FQDNs) in the address book for DNS caching. This configuration ensures that DNS responses with TTL values lower or higher than 16 seconds are cached for their actual duration, rather than for the default minimum of 16 seconds. The system maintains default behavior for backward compatibility unless you reconfigure it. This feature offers more accurate DNS resolution and is particularly beneficial in environments where IP addresses change frequently.

  [See Override Default Minimum TTL for DNS Caching.]

- **Real-time DNS snooping for dynamic FQDN policy updates (cSRX, SRX1600, SRX2300, SRX4100, SRX4120, SRX4200, SRX4300, SRX4600, SRX4700, SRX5400, SRX5600, SRX5800, and vSRX 3.0)**—Domain Name System (DNS) snooping inspects and caches DNS responses in real time.

  After you enable DNS snooping, the firewall:

  1. Captures DNS response packets as traffic traverses the network.
  2. Extracts relevant DNS records.
  3. Builds a local cache mapping of fully qualified domain names (FQDNs) to IP addresses.

  The firewall keeps these mappings accurate and current for IPv4 or IPv6 traffic. Use this feature to implement real-time DNS mapping updates in environments with frequently changing DNS entries.

  [See DNS Snooping for Security Policies.]

- **DNS snooping and DNS module integration (cSRX, SRX1600, SRX2300, SRX4100, SRX4120, SRX4200, SRX4300, SRX4600, SRX4700, SRX5400, SRX5600, SRX5800, and vSRX 3.0)**—Use the integrated DNS-snooping cache in the Packet Forwarding Engine with the DNS module on the Routing Engine to unify entries from explicit DNS queries and DNS snooping in the data plane. The combined DNS cache remains accurate and relevant, helping you to apply DNS-based policies and destination network address translation (NAT) configurations effectively.

  The `show security dns-cache` command displays entries from both the DNS resolver and DNS snooping.

  [See DNS Snooping for Security Policies.]

- **Transparent web proxy with HTTP/2 support and application traffic exemption (SRX380, SRX320, SRX340, SRX345, SRX1600, SRX2300, SRX4100, SRX4120, SRX4200, SRX4300, and vSRX3.0)**—Use transparent web proxy to route traffic through an external proxy server without client awareness or additional configuration. You can exempt specific application traffic from the proxy, moving the traffic directly to the webserver. Transparent web proxy also supports HTTP/2, enabling secure HTTPS traffic relay without decryption. This functionality enhances the quality of service for specified applications by transparently mediating between the client and the webserver.

  [See Transparent Web Proxy.]

Dynamic Host Configuration Protocol

- **Display physical interface and VLAN ID in DHCP relay and server binding outputs (all Junos OS and Junos OS Evolved platforms)**—You can view the physical interface and VLAN ID in the outputs of the following commands:

  - `show dhcp relay binding`
  - `show dhcp server binding`

- `show dhcpv6 relay binding`
- `show dhcpv6 server binding`

The enhanced output now displays data for **Physical interface** and **VLAN** alongside existing data. This addition facilitates easy understanding of client's binding origin.

[See https://www.juniper.net/documentation/us/en/software/junos/cli-reference/topics/ref/command/show-dhcp-relay-binding.html and https://www.juniper.net/documentation/us/en/software/junos/cli-reference/topics/ref/command/show-dhcp-server-binding-command.html.]

Ethernet Switching and Bridging

- **Forwarding L3 broadcast IP packets and sending copies to Routing Engine (SRX300, SRX320, SRX340, SRX345, SRX380, SRX1500, SRX1600, SRX2300, and SRX4300)**—Integrated routing and bridging (IRB) interfaces support forwarding of Layer 3 (L3) broadcast packets on the egress interface. Additionally, you can use the IRB interfaces on these devices to send a copy of the IP broadcast packets to the Routing Engine.

  [See targeted broadcast and show interfaces irb.]

High Availability

- **MNHA support for Express Path (SRX4600, SRX5400, SRX5600, SRX5800 [IOC3, IOC4])**—Express Path, formerly services offloading, in Multinode High Availability (MNHA) (SRG0 and SRG1+) reduces latency and ensures seamless packet forwarding post failover. MNHA creates stateful and static services offloading sessions on the other node for immediate readiness, prevents premature session aging, preserves session integrity, and manages first packet processing during primary role transitions. The system also terminates and reinstalls services offload sessions in the newly failed node for accurate management. MNHA systems in Layer 3 (Routing) mode support this functionality.

  [See Express Path Overview.]

Identity Aware Firewall

- **Optimized session report mechanism in user firewall authentication (SRX Series Firewalls and vSRX 3.0)**—An optimized session report mechanism enhances user firewall authentication performance by reducing Routing Engine delays. The mechanism updates the authentication entry timeout on the Routing Engine and reduces the number of messages that the Packet Forwarding Engine must send for session report updates. Firewall administrators benefit from the faster, accurate session reporting and gain overall system efficiency.

  [See show services user-identification authentication-table.]

- **SAML-based firewall authentication (cSRX, SRX Series Firewalls, and vSRX 3.0)**—You can authenticate users through Security Assertion Markup Language (SAML)-based access profiles using your organization's identity provider (IdP) for firewall authentication. This method generates SAML

requests and processes SAML assertions, enhancing the security and flexibility of user authentication. The integration supports single sign-on (SSO) using HTTP Redirect and HTTP POST SAML bindings, providing benefits such as improved security and reduced password management. Include the `access-profile` *`profile-name`* statement under `set security policies from-zone` *`zone-name`* `to-zone` *`zone-name`* `policy` *`policy-name`* `then permit firewall-authentication user-firewall` hierarchy to enable SAML-based captive portal authentication.

To apply a default Secure Sockets Layer (SSL) termination profile, use the `set access firewall authentication user-firewall default-ssl-termination-profile` *`default-ssl-termination-profile`* command. Enable this configuration to enforce security for all access profiles.

[See user-firewall (Access Firewall-Authentication), default-ssl-termination-profile (Access), user-firewall, policy (Security Policies), SAML Authentication in Juniper Secure Connect, saml, and authentication-order (Access Profile).]

Interfaces

- **PPPoE family configuration on a physical interface (SRX300, SRX320, SRX340, SRX345, and SRX380)**—When you configure PPPoE encapsulation on a physical interface, the interface supports only PPPoE because the PPPoE encapsulation cannot support other protocol families. To enable the interface to support multiple protocol families, configure a new PPPoE family, such as IPv4 or IPv6.

  [See Configuring Point-to-Point Protocol over Ethernet.]

Juniper Advanced Threat Prevention Cloud (ATP Cloud)

- **DoT support with SSL forward proxy (SRX Series Firewalls and vSRX Series Firewall)**—Use DNS over TLS (DoT) with SSL forward proxy to decrypt the DNS traffic. Use DNS filtering, domain generation algorithm (DGA) detection, and DNS tunneling detection to filter malicious domains, enhancing threat detection and privacy. To leverage DNS security with DoT, configure SSL proxy profile, manage certificates, and set up security policies. You can monitor traffic by using the DNS statistics commands.

  [See show services security-intelligence dns-statistics, Enable DNS SecIntel Detection, Enable DNS DGA Detection, Enable DNS Tunnel Detection, Configure DNS Sinkhole and Configuring SSL Proxy.]

J-Web

- **Simplified J-Web UI (SRX Series Firewalls and vSRX 3.0)**—

  The J-Web user interface is streamlined to include only the essential features needed for initial setup, basic connectivity, and troubleshooting of your SRX Series Firewall.

  [See Juniper Web Device Manager Overview.]

- **Optional J-Web application package (SRX Series Firewalls and vSRX 3.0)**—J-Web for SRX Series Firewalls is now available as an optional package named `jweb-srx-app`. This package is bundled with Junos OS but not installed by default. To use J-Web, you need to install the package by using the CLI.

  [See Access the J-Web User Interface.]

- **Modified J-Web UI (SRX1600, SRX2300, SRX4300, and SRX4700)**—You can use the J-Web interface on the firewalls to support the limited SKU version of the Junos OS image. This update removes the following options, which are related to data plane cryptography, from the J-Web UI:

  - **Dashboard** > **VPN Monitoring**
  - **Dashboard** > **IPsec VPNs (IKE Peers)**
  - **Network** > **VPN**
  - **Monitor** > **Network** > **IPsec VPN**
  - **Monitor** > **Logs** > **VPN Logs**

  [See Dashboard Overview, About the IPsec VPN Page, Monitor IPsec VPN, and Monitor VPN.]

- **J-Web support for SRX4120 Firewall (SRX4120)**—You can use the J-Web UI for initial setup, basic connectivity, and troubleshooting of your SRX Series Firewalls.

  [See The J-Web Setup Wizard, Dashboard Overview, and Configure Basic Settings.]

Junos Telemetry Interface

- **Enhanced memory monitoring with configurable thresholds and improved alarm validation (EX2300-C, EX3400, EX4100-24P, EX4100-24T, EX4300-MP, EX4400-24MP, EX4400-24P, EX4400-24T, EX4400-48MP, EX4650, MX960, MX10003, MX10004, MX10008, MX10016, MX2008, MX2010, MX2020, SRX2300, SRX4200, SRX4300, SRX4600, SRX4700, and SRX5800)**—You can monitor system free pages and memory swap usage more efficiently to prevent issues related to memory shortages. The enhanced validation process reduces false alarm triggers. Additionally, you can set user-configurable thresholds for monitoring the virtual memory size (VSZ) of processes, with events categorized based on severity.

  Use the `set system monitor memory process (minor/major/critical)-event threshold <process-name> memory-limit <threshold>` command to configure these thresholds. Alarms are integrated with *eventd* and *alarmd* infrastructure and can be viewed using the `show system alarms` command. To view *jsysmond* events, use the `show system monitor memory events all` command.

  [See https://www.juniper.net/documentation/us/en/software/junos/cli-reference/topics/ref/command/show-system-monitor-memory-events.html.]

- **Enhanced telemetry with multiple gRPC servers and multiport gRPC services (EX2300, EX2300-C, EX2300-MP, EX2300-VC, EX3400, EX3400-VC, EX4000-8P, EX4000-12P, EX4000-12T,**

EX4000-12MP, EX4000-24MP, EX4000-48MP, EX4000-24P, EX4000-24T, EX4000-48P, EX4000-48T, EX4100-24MP, EX4100-24P, EX4100-24T, EX4100-48MP, EX4100-48P, EX4100-48T, EX4100-F-12P, EX4100-F-12T, EX4100-F-24P, EX4100-F-24T, EX4100-F-48P, EX4100-F-48T, EX4100-H-12MP, EX4100-H-12MP-DC, EX4100-H-24F, EX4100-H-24F-DC, EX4100-H-24MP, EX4100-H-24MP-DC, EX4300-MP, EX4300VC, EX4400-24MP, EX4400-24P, EX4400-24T, EX4400-24X, EX4400-48F, EX4400-48MP, EX4400-48MXP, EX4400-48P, EX4400-48T, EX4400-48XP, EX4600-VC, EX4650, EX4650-48Y-VC, EX9204, EX9208, EX9214, MX204, MX240, MX304, MX480, MX960, MX2008, MX2010, MX2020, MX10004, MX10008, cSRX, SRX300, SRX320, SRX340, SRX345, SRX380, SRX1500, SRX1600, SRX2300, SRX4100, SRX4200, SRX4300, SRX4600, SRX4700, SRX5400, SRX5600, SRX5800, and vSRX 3.0)—You can configure multiple gRPC servers with distinct services, listening addresses, and ports using the Junos Telemetry Interface. This feature enhances control over service management and telemetry data collection. You can also configure TLS certificates for secure communications. Use CLI commands to set listening addresses and ports and secure communications through TLS certificates. For example, you can configure a server to listen on a specific port and serve only designated gRPC services, enhancing flexibility and security in your telemetry setup.

Network Address Translation (NAT)

- **NAT IPv6 translations offloading to NPU (SRX4600, SRX5400, SRX5600, and SRX5800)**—You can enhance the efficiency of Network Address Translation (NAT) IPv6 translations on SRX Series Firewalls by offloading these tasks to the network processing unit (NPU). This includes handling IPv6 to IPv4, IPv4 to IPv6, and IPv6 to IPv6 translations. Offloading these processes to the NPU decreases the CPU load on the SPU, resulting in improved performance for NAT data packet processing. Consequently, this optimizes the handling of non-ALG traffic and ensures seamless communication between IPv4 and IPv6 networks.

  [See IPv6 NAT Overview]

Network Management and Monitoring

- **Support for multiple gRPC servers hosting different service sets (EX2300, EX2300-C, EX2300-MP, EX2300-VC, EX3400, EX3400-VC, EX4000-8P, EX4000-12P, EX4000-12T, EX4000-12MP, EX4000-24MP, EX4000-48MP, EX4000-24P, EX4000-24T, EX4000-48P, EX4000-48T, EX4100-24MP, EX4100-24P, EX4100-24T, EX4100-48MP, EX4100-48P, EX4100-48T, EX4100-F-12P, EX4100-F-12T, EX4100-F-24P, EX4100-F-24T, EX4100-F-48P, EX4100-F-48T, EX4100-H-12MP, EX4100-H-12MP-DC, EX4100-H-24F, EX4100-H-24F-DC, EX4100-H-24MP, EX4100-H-24MP-DC, EX4300-MP, EX4300VC, EX4400-24MP, EX4400-24P, EX4400-24T, EX4400-24X, EX4400-48F, EX4400-48MP, EX4400-48MXP, EX4400-48P, EX4400-48T, EX4400-48XP, EX4600-VC, EX4650, EX4650-48Y-VC, EX9204, EX9208, EX9214, MX204, MX240, MX304, MX480, MX960, MX2008, MX2010, MX2020, MX10004, MX10008, cSRX, SRX300, SRX320, SRX340, SRX345, SRX380, SRX1500, SRX1600, SRX2300, SRX4100, SRX4200, SRX4300, SRX4600, SRX4700, SRX5400, SRX5600, SRX5800, and vSRX 3.0)**—You can configure multiple gRPC servers that host different sets of services on unique ports. Additionally, each server can support different

certificates, listening addresses, and routing instances. You configure the gRPC servers at the `[edit system services http servers]` hierarchy level. Distributing gRPC services across different servers allows for better allocation of network resources, reducing the risk of port conflicts and optimizing server performance.

[See Configure gRPC Services and server.]

- **Enhanced on-box memory monitoring with configurable thresholds and improved alarm validation (EX2300-C, EX3400, EX4100-24P, EX4100-24T, EX4300-MP, EX4400-24MP, EX4400-24P, EX4400-24T, EX4400-48MP, EX4650, MX960, MX10003, MX10004, MX10008, MX10016, MX2008, MX2010, MX2020, SRX2300, SRX4200, SRX4300, SRX4600, SRX4700, and SRX5800)**—You can monitor system free pages and excessive swap memory usage more efficiently to prevent memory shortage issues. The enhanced validation process reduces false alarm triggers.

  Additionally, you can set user-configurable thresholds to monitor the Virtual Memory Size (VSZ) of processes, with events categorized based on severity. Use the `set system monitor memory process minor/major/critical-event threshold` *`process-name`* `memory-limit` configuration statement to configure these thresholds.

  The system integrates alarms with the eventd and alarmd infrastructure, enabling you to view the alarms using the `show system alarms` command.

  Use the `show system monitor memory events all` and `show system monitor memory status all` commands to view all recorded events and the latest status on memory usage.

VPNs

- **Remote access support (SRX4700)**—You can use remote access for IPsec VPN on SRX4700 devices to enhance security,using Juniper® Secure Connect. Juniper Secure Connect is a client-based SSL-VPN application that facilitates secure connections and access to protected network resources from any location. This feature helps you achieve dynamic, flexible, and adaptable connectivity, extending visibility and enforcement from client to cloud through secure VPN connections.

  [See Juniper Secure Connect.]

- **Support for inline IPsec (SRX4700)**—The firewall uses the Packet Forwarding Engine ASIC to encrypt and decrypt IPsec traffic by default. This inline processing of IPsec traffic within the Packet Forwarding Engine offloads the CPU. The CPU handles only PowerMode IPsec (PMI) and IPsec VPN with Quick Assist Technology (QAT) tasks, improving overall IPsec VPN throughput.

  [See Inline IPsec Overview, show security ipsec security-associations, and ipsec (Security).]

Additional Features

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

- **Support for firewall filter flexible match conditions** (SRX4700)

  [See Firewall Filter Flexible Match Conditions.]

- **Supported transceivers, optical interfaces, and DAC cables (SRX4700)**. Select your product in the Hardware Compatibility Tool to view supported transceivers, optical interfaces, and direct attach copper (DAC) cables for your platform or interface module. We update the HCT and provide the first supported release information when the optical transceiver becomes available.

What's Changed

IN THIS SECTION

Learn about what changed in this release for SRX Series.

Application Security

- **Deprication of ssl-version in custom signatures (SRX Series)**—The ssl-version in SSL context-based custom signatures is deprecated in application signature package version 3796 and later. You can use the ssl-protocol-version option instead. The ssl-version option is deprecated-rather than immediately

removed- to provide backward compatibility and an opportunity to bring your configuration into compliance with the new configuration.

[See [Custom Application Signatures for Application Identification and context.]

- **Configuration Limits for SSL Proxy Profiles**—Starting in this release, we have updated the limits for Trusted CA certificates, Server certificates, and URL categories in both SSL forward proxy and SSL reverse proxy configurations. These changes ensure compliance with the maximum configuration blob size limit of 56,986 bytes.

  Changes in limit size:

  - Trusted CA certificate/server certificates: maximum limit—400 (changed from 1024)
  - URL categories: maximum limit—800 (unchanged)

  Configuration statements:

```
user@host# set services ssl proxy profile profile-name trusted-ca (all | [ca-profile] )
user@host# set services ssl proxy profile profile-name server-certificate
user@host# set services ssl proxy profile profile-name whitelist-url-categories [whitelist
url categories]
```

  NOTE: In the reverse proxy configuration, ensure combined size of server certificates and URL categories does not exceed 56,986 bytes. If the combined size exceeds the limit, the following error message is displayed during commit:

```
ERROR: Maximum blob size (56986 bytes) exceeded...current blob size is 57014 bytes.
400 Server certs are taking 54400 bytes, and 27 URL categories are taking 1728 bytes.
```

  This error provides a breakdown of memory usage, helping you adjust the configuration accordingly.

  [See [Configuring SSL Proxy].]

Content Security

- **Sophos antivirus configuration for ISSU (SRX Series)**—To use the Sophos antivirus while performing an in-service software upgrade (ISSU), remove the following configuration options.

- `edit security utm default-configuration anti-virus forwarding-mode holdset`
- `edit security utm default-configuration anti-virus forwarding-mode inline-tap`

This caution applies only to ISSU upgrades and not to standalone upgrades. Once you complete the ISSU, you can re-enable the above configurations. The Sophos antivirus feature perform as usual when both devices come up.

[See Sophos Antivirus Configuration Overview.]

Chassis Clustering

- Define a redundancy mode.
  - `active-active: primary and secondary nodes in active mode.`
  - `active-backup: primary in active, secondary in backup mode.`

JIMS

- For push-to-identity-management to successfully push the authentication entry to JIMS, you must configure JIMS and verify that JIMS status is online.

  [See push-to-identity-management and Configuration of JIMS with SRX Series Firewall.]

Juniper Secure Connect

- **Support for iPadOS for prelogon compliance checks in Juniper Secure Connect (SRX Series, and vSRX3.0)**—You can configure prelogon compliance checks on your firewall to allow or reject endpoints running iPadOS. Use the `ipados` option at the `[edit security remote-access compliance pre-logon` *`name`* `term` *`name`* `match platform]` hierarchy level to enforce these checks. This ensures that only compliant iPadOS devices are permitted access, enhancing the security of your network.

  [See compliance (Juniper Secure Connect).]

Network Address Translation (NAT)

- Support for NAT debugging (SRX Series Firewalls and vSRX) To debug NAT-related issues, use the nat option with the request support information security-components command.

  [See request support information.]

PKI

- SSH key options for user account credentials. You can configure key-options `key-options` option at the set system login user `<user> authentication [ssh-rsa|ssh-ecdsa|ssh-ed25519] <ssh key>` hierarchy level.

  [See login.]

- **Certificate enrollment system logs (Junos)**—We've added system logs to notify if there is an SCEP and CMPv2 certificate failure. On SCEP certificate enrollment failure, you can see the PKID_SCEP_EE_CERT_ENROLL_FAIL message. On CMPv2 certificate enrollment failure, you can see the PKID_CMPV2_EE_CERT_ENROLL_FAIL message.

  [See System Log Explorer.]

Platform and Infrastructure

- **Alarm added to indicate failure in writing the security logs to traffic logs (SRX4700)**—We've introduced alarms indicating a failure in writing the security logs to traffic logs due to disk corruption or a read/write error. The alarms are displayed in the output of the show command `show system alarms`.

Security Policies

- **Secure Web Proxy Renamed as Transparent Web Proxy (SRX380, SRX320, SRX340, SRX345, SRX1600, SRX2300, SRX4100, SRX4200, SRX4300, and vSRX3.0)**—Starting in Junos OS Release 25.2R1, we've renamed the secure web proxy as transparent web proxy. If you are planning to upgrade to Junos OS Release 25.2R1 and later releases, note the following points regarding using proxy functionality:

  All existing secure web proxy related CLI statements and commands are deprecated. That is—Starting in Junos OS Release 25.2R1 secure web proxy functionality is deprecated— rather than immediately removed—to provide backward compatibility and an opportunity to bring your configuration into

compliance with the new configuration. As a part of this change, the `[edit services web-proxy secure-proxy]` hierarchy and all the configuration options under this hierarchy are deprecated. That is, the hierarchy for transparent proxy configuration statements has changed from `set services web-proxy secure-proxy` to `set services web-proxy transparent-proxy`.

To migrate, you will need to replace existing command hierarchies with the new ones as shown in the following table.

Table 11: Secure Web Proxy Hierarchy Replacements

Previous Hierarchy (Secure Web Proxy)	New Hierarchy (Transparent Web Proxy)
`set services web-proxy secure-proxy`	`set services web-proxy transparent-proxy`
`set security policies from-zone trust to-zone untrust policy apply_webproxy then permit application-services web-proxy profile-name <trans-proxy-profile-name>`	`set security policies from-zone trust to-zone untrust policy apply_webproxy then permit application-services transparent-proxy profile-name <trans-proxy-profile-name>`

These adjustments ensure that your configurations are up-to-date and ready to take advantage of the new features.

[See Transparent Web Proxy (Junos OS version 25.2R1 and later releases) and Secure Web Proxy (Junos OS version before Junos OS 25.2R1)].

User Interface and Configuration

- **Access privileges for request support information command (ACX Series, EX Series, MX Series, QFX Series, SRX Series Firewalls, and vSRX Virtual Firewall)**—The `request support information` command is designed to generate system information for troubleshooting and debugging purposes. Users with the specific access privileges `maintenance` , `view` , and `view-configuration` can execute request support information command.

- **Changes to the `show system storage` command output (ACX Series, EX Series, MX Series, QFX Series, and SRX Series)**—We've updated the `show system storage` command output to include only true (physical) storage and exclude any host/hypervisor level storage. In earlier releases, the output also includes a container/jail storage, which does not have a separate storage of its own.

  [See show system storage.]

- **Option to view combined disk space usage statistics for all configuration databases (ACX Series, EX Series, MX Series, QFX Series, SRX Series, and vSRX)**—The `show system configuration database usage`

command provides the `merge` option. When you include the `merge` option, the command output displays combined disk space usage statistics for all configuration databases, including the static configuration database and all ephemeral configuration database instances.

[See show system configuration database usage.]

- **`netconf ssh` is removed from the factory-default device configuration (SRX300, SRX320, SRX340 , SRX345, and SRX380)**—To enhance security, we've removed the `netconf ssh` statement at the `[edit system services]` hierarchy level from the factory-default device configuration. To use this service, you can explicitly configure the statement.

VPNs

- **Global option to disable inline IPsec hardware offloading (SRX4700)**—You can disable hardware offloading of IPsec tunnel processing in the Packet Forwarding Engine ASIC. Use the comman `set security ipsec hw-offload-disable` to globally disable this inline IPsec processing of packets. When you configure the statement, the firewall processes IPsec tunnels in CPU instead of the Packet Forwarding Engine ASIC. This statement replaces the previous hidden option `no-hw-offload` at the `edit security ipsec` hierarchy level. This global configuration provides a streamlined approach to managing IPsec hardware offloading settings at the firewall level.

  [See ipsec (Security).]

- **Deprecation of weak algorithms in IPsec VPN (SRX Series and vSRX 3.0)**—We've deprecated the weak algorithms in IKE and IPsec proposals. You'll no longer be able to use the following algorithms:

  Table 12: Deprecated Junos CLI Options

Type	Algorithm	Junos CLI Statement
Encryption Algorithm in IKE Proposal	`des-cbc` and `3des-cbc`	`set security ike proposal` *`name`* `encryption-algorithm`
Authentication Algorithm in IKE Proposal	`md5` and `sha1`	`set security ike proposal` *`name`* `authentication-algorithm`
DH Group in IKE Proposal	`group1`, `group2`, and `group5`	`set security ike proposal` *`name`* `dh-group`
Encryption Algorithm in IKE Proposal	`des-cbc` and `3des-cbc`	`set security ipsec proposal` *`name`* `encryption-algorithm`

Authentication Algorithm in IKE Proposal	`hmac-md5-96` and `hmac-sha1-96`	`set security ipsec proposal` *name* `authentication-algorithm`

You will receive a warning message if you configure these deprecated algorithms explicitly. As an alternative, we recommend that you configure the stronger algorithms to enhance the security in IPsec VPN.

[See proposal (Security IKE, and proposal (Security IPsec).]

- **Default installation of junos-ike package on additional platforms (SRX1500, SRX4100, SRX4200, SRX4600, and vSRX3.0)**—The `junos-ike` package is installed by default on SRX1500, SRX4100, SRX4200, SRX4600, and vSRX3.0 firewalls, ensuring the default support for `iked` process for IPsec VPN service. This aligns with the existing default installation of the package on SRX5000 line with Routing Engine 3 (SRX5K-SPC3 with RE3). You can delete the `junos-ike` package using the command `request system software delete junos-ike`. This runs the `kmd` process on these firewalls, allowing flexible management of your security infrastructure.

  [See IPsec VPN Feature Support with New Package.]

- **Support for iPadOS for prelogon compliance checks in Juniper Secure Connect (SRX Series, and vSRX3.0)**—You can configure prelogon compliance checks on your firewall to allow or reject endpoints running iPadOS. Use the `ipados` option at the `[edit security remote-access compliance pre-logon` *name* `term` *name* `match platform]` hierarchy level to enforce these checks. This ensures that only compliant iPadOS devices are permitted access, enhancing the security of your network.

  [See compliance (Juniper Secure Connect).]

Known Limitations

IN THIS SECTION

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

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

Platform and Infrastructure

- The peers-synchronize is configured, and master-password is configured to encrypt the config being synchronized. However, since there is no master-password configured on the peer device, the encrypted configuration cannot be decrypted. PR1805835
- An Authentication Bypass by Spoofing vulnerability in the RADIUS protocol of Juniper Networks Junos OS and Junos OS Evolved platforms allows an on-path attacker between a RADIUS server and a RADIUS client to bypass authentication when RADIUS authentication is in use. Refer to https://supportportal.juniper.net/JSA88210. PR1850776

VPNs

- All ARI-TS routes in Forwarding Table are dead after loading baseline and test configurations. PR1858312

Open Issues

IN THIS SECTION

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.

Content Security

- Avira is not supported for SRX4700 in Junos OS release 24.4R1-S2. PR1851627

General Routing

- Multiple vulnerabilities have been resolved in MQTT included with Junos by fixing vulnerabilities found during external security research. Refer to https://supportportal.juniper.net/JSA71655. PR1651519
- Right after rebooting one of SRX4600 at high availability setup, CTL link might keep down. PR1802158
- On SRX4100 and SRX4200 devices, MNHA Conn State and ICL are down after 48+ hours of device being up with background traffic due to BFD flaps at regular intervals. PR1822662
- On SRX4600 device, if a few high-priority queues handle excessive traffic, those queues can become stuck, leading to packet drops. PR1823577
- On SRX300 line of devices configured with native-vlan-id, after upgrading an SRX300 line of devices to Junos OS release 23.4R1 or higher, the native-vlan-id option disappears from the interface settings. If native-vlan-id was set before the upgrade, the device keeps the setting but it does not apply it to the interface. Deleting native-vlan-id causes a syntax error. The native-vlan-id feature doesn't work, and if a custom VLAN ID (other than 1) is used then traffic for that VLAN will be affected. PR1847366
- CLI show security firewall-authentication users all-logical-systems-tenants shows null output for all-logical-systems-tenants filter, use show security firewall-authentication users all instead. PR1849954
- On SRX Series Firewall and MX platforms a rare occurrence issue causes a sudden reboot of the SPC3 in use leading to packet loss during the card offline period in the reboot process.PR1857890

Network Management and Monitoring

- Multiple stale sessions occur when two hosts use the same user-defined instance and routes are added or deleted on the server side. PR1825311

Resolved Issues

IN THIS SECTION

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

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

Application Layer Gateways (ALGs)

- The SRX Series Firewall might experience a flowd process stop and generate core file when the ALG feature is enabled. PR1852968

Chassis Clustering

- Traffic through IPsec VPN tunnel halts or stops after back to back failover until rekey occurs. PR1842874
- MNHA ICL IPsec encryption link went down permanently after rebooting connected router through which ICL was established before. During this state IKE process got stuck at ~70% on MNHA active node. PR1850967

- Post chassis-control restart on one of MNHA node, node goes into OFFLINE [SP] status with SRG in INELIGIBLE state and does not recover from this state. PR1873432

Content Security

- The utmd process stops when EWF or NG web-filtering is configured on SRX Series Firewall with scaled custom URLs. PR1841370
- FPC stops when web filtering type set to juniper-enhanced or NG-juniper. PR1854519

Flow-Based and Packet-Based Processing

- AppQoS rate limit in PMI mode on SRX5000 line of devices and SRX4600 might drop packets unexpectedly. PR1828819
- GRE traffic is getting blocked due to a software programming issue and MTU going below minimum value. PR1834338
- Type 5 VXLAN traffic drops are observed when SRX Series Firewall run as L3-VNI gateway and the ingress and egress traffic goes to the same Type-5 VXLAN peer. PR1847419
- SRX Series Firewall with chassis cluster configured experience flowd process stops due to a race condition in multicast session handling. PR1854492
- Data Plane CPU on one device spikes up to 95% during primary node system reboot. PR1856521
- The flowd process stops when service offload and system stats are enabled. PR1859062
- Security forwarding process pause might occur when multicast traffic triggers a route resolution request that needs to be processed for a pending session. PR1859163
- SRX4700 custom application session inactive timeout is half of the configured value. PR1865294
- Packet Forwarding Engine pause is observed when Packet Forwarding Engine processes the traffic passing through the dedicated fabric link. PR1872613
- The TCP session is not closing properly on the SRX4600 and SRX5000 line of devices after receiving the FIN-ACK message causing packets to drop for new session if reusing same source port. PR1873580
- A flowd process might stop on SRX Series Firewall in L2 transparent mode. PR1878164

General Routing

- Multiple J-UKERN core files might be generated during the sanity test. PR1641517
- ifHCOutOctets unexpected spikes in value. PR1706125
- RTO traffic loss and accumulation of session on secondary node is observed when RTO traffic not evenly distributed to all FLT (Flow Thread) threads. PR1819911
- On SRX4600 device with heavy traffic, the FPGA drop packets. PR1823577
- On SRX Series Firewall MLD groups are successfully formed however egress traffic is not being forwarded as expected. PR1828211
- The SRX1500 drops the packet if MTU matches the MRU of the receiving device. PR1831955
- The IDP security-packages install is throwing 'Attack DB Update Failed' error and AppID stops working. PR1832094
- Custom application detection fails for L4 traffic after upgrade due to uncompiled signatures. PR1833667
- AE interfaces not coming up if configured with flexible-vlan-tagging and output-vlan-map. PR1838033
- In FIPS mode, kernel panics at MipsSwitchFPState and reboots generating a vmcore. PR1838923
- Once we enable, mvrp on the dut interface DVLAN learning is not happening to r0 and r1. PR1839275
- The load-balance hash-key forwarding persists when switching to Layer 3-only. PR1842873
- Application crash is observed due to insufficient memory when a large numbers of JFlow entries are created. PR1843679
- Unnecessary trace log files related to licenses are generated. PR1845079
- SRX Series Firewall Packet Forwarding Engine pause is observed with source-identity enabled. PR1845506
- Auto-re-enrollment for local certificate once fail, not trigger again on SRX Series Firewall. PR1845573
- Security-metadata streaming is impacted due to dynamic-filter issue. PR1845645
- Packet drops are observed in the VPLS environment on SRX380 device in packet mode. PR1845997

- FPC0 will not transition to Online and might generate chassis alarm "FPC 0 Hard errors" in SRX4600 devices deployed in chassis cluster. PR1846340
- Local or peer device's interface reflects down after SRX380 device reboot. PR1848557
- It is not recommended to restart chassisd using CLI command restart chassis-control in MNHA setup. PR1849108
- The redundant Ethernet reserved buffer increases when redundant Ethernet interface is activated. PR1849364
- The commit command failed due to a speed mismatch between the Ten-Gigabit Ethernet (XE) port and the aggregated Ethernet (AE) interface to which it belongs. PR1851261
- Intermittent traffic drops are seen due to large memory allocation for unidentified files. PR1851786
- Flexible-vlan-tagging option is missing under interface hierarchy on SRX300 line of devices. PR1853238
- PIM IP ESP packet fragments dropped in SRX Series Firewall. PR1854130
- The nsd process stop responding on SRX Series Firewall during cluster reboot, failover, or policy addition causes traffic outage. PR1857379
- The chassisd process pause is seen after the device reboot when chassisd stalls after configuration commit PR1857833
- Security logs report messages for logical system are not generated. PR1860597
- Packet drops can occur when packets are received with a size equal to the default MRU. PR1863576
- CoS shaping is not functional on IRB interfaces when the SRX1600 is in switching mode PR1868103
- Hostname with apostrophe causing connection failures. PR1869192
- Commit delay due to incomplete MACsec PSK configuration. PR1873885
- Unexpected primary role assignment after nodes 0 reboot. PR1877323

J-Web

- Created address-set in global address book is not visible in J-Web. PR1805828
- Junos image upload progress message is not displayed. PR1844395
- Unable to load J-Web after upgrading when time zone is set to GMT+x or GMT-x. PR1851362

- VPN fails due to file descriptor issue. PR1858466
- Upgrade and Downgrade will fail from J-Web in SRX4600. PR1876075

Network Address Translation (NAT)

- New CLI for RSI updated to collect more NAT information. PR1825372

Network Management and Monitoring

- SNMPV3 Engine-ID does not update to MAC address as configured. PR1866948

Platform and Infrastructure

- On SRX300 series DHCP relay stops working and the device generates core files after upgrading to JunOS 23.4R2-S2.1. PR1843935
- The self-generated traffic on Junos platforms uses the incorrect source IP with ECMP configuration. PR1849296

Routing Policy and Firewall Filters

- The show security match-policies command results in a timeout error. PR1809563
- Security flow sessions are impacted during ISSU. PR1838698
- The mgd process pause is observed during large amount of configurations. PR1847877
- Deny traffic log message is not generated for persistent NAT traffic. PR1869988
- Protocols involved with TCP/IP on an lsi interface have issues as TCP 3-way handshake cannot be completed. PR1871431

Routing Protocols

- The rpd process stop on commit when configuring router-advertisement with DNS search label under 3 characters. PR1847811

VLAN Infrastructure

- Traffic drops are observed when SRX380 platform is configured in L2 transparent-bridge mode. PR1852047
- Packet Forwarding Engine stops responding due to invalid cached next hop during reinjection on SRX5000 like of devices. PR1856200

VPNs

- Master-encryption-password is not accessible when system is in FIPS mode. PR1665506
- The flowd process stops responding on SRX5000 line of devices with multiple line cards in MNHA scenario. PR1839665
- ICL connection getting established with wrong source interface IP when trying to establish ICL connection between pub-broker and sub-broker with loopback interface IP's. This resulting in IPsec session sync failure between master and backup MNHA devices. PR1840788
- The show chassis high-availability information CLI says SRG1 control plane state as ready ICL connection between Pub-Broker Sub-broker is not established properly and IPsec sessions are not synchronize between primary and Standby MNHA peers. PR1840803
- IPsec sa configuration entries on node0 Packet Forwarding Engine are empty when configured from secondary node. PR1846168
- IKED generates core files during a restart or failover event. PR1848834
- To renegotiate VPN with the correct gateway when the active tunnel goes down. PR1851652
- Recommended command to failover from Primary to Backup node. PR1861056
- On rare circumstances the kmd or iked process stops responding when the device is too overloaded to generate a random number after repeated attempts PR1864322.
- Post reboot, IPsec VPN is not coming up over MNHA active/active deployment. PR1864758

- Recommended command to failover from Primary to Backup node. PR1866890
- Type 5 EVPN traffic is dropped when PMI is disabled or not supported. PR1867040
- IPsec tunnel inactive after multiple srg failovers. PR1868453

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, EOL and EEOL:

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

For both EOL and EEOL releases, you can upgrade to the next three subsequent releases or downgrade to the previous three releases.

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

Table 13: EOL and EEOL Releases

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

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

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

Junos OS Release Notes for vSRX

IN THIS SECTION

What's New

IN THIS SECTION

Learn about new features introduced in this release for vSRX.

Authentication and Access Control

- **Authentication options for dynamic address feed downloads (SRX Series Firewalls and vSRX 3.0)**—You can authenticate dynamic address feed servers before downloading feeds into the vSRX 3.0.. Use the new authentication options, `user-name` and `password`, to securely obtain feeds from local or remote webservers. This feature facilitates automatic scaling of business operations and Layer 7 services.

  To configure this authentication, use:

  - `set security dynamic-address feed-server` *`feed-server`* `user-name` *`user-name`*
  - `set security dynamic-address feed-server` *`feed-server`* `password` *`password`*

  [See Configuring Security Policies, dynamic-address | Junos OS | Juniper Networks, and show security dynamic-address | Juniper Networks.]

- **SSH enhancements for algorithm configuration (all Junos OS platforms)**—We've made the following updates to SSH algorithms:

  - The CLI command `set system services ssh ca-signature-algorithms` should be used to configure the signature algorithms that are allowed for certificate authorities (CAs) to use when signing certificates.
  - Under the `system services ssh hostkey-algorithm-list` hierarchy level, new options are introduced:

- `set system service ssh hostkey-algorithm-list rsa-sha2-256`
- `set system service ssh hostkey-algorithm-list rsa-sha2-512`

  These options enable RSA hostkey signatures using the SHA-256 hash algorithm and SHA-512 hash algorithm.

- RSA signatures using the SHA-1 hash algorithm have been disabled by default. Consequently, the CLI command `set system services ssh hostkey-algorithm-list rsa` has been deprecated.

[See hostkey-algorithm-list.]

Device Security

- **Override default minimum TTL for DNS caching (cSRX, SRX Series Firewalls, and vSRX 3.0)**—Override the default minimum time-to-live value (TTL) value for fully qualified domain names (FQDNs) in the address book for DNS caching. This configuration ensures that DNS responses with TTL values lower or higher than 16 seconds are cached for their actual duration, rather than for the default minimum of 16 seconds. The system maintains default behavior for backward compatibility unless you reconfigure it. This feature offers more accurate DNS resolution and is particularly beneficial in environments where IP addresses change frequently.

  [See Override Default Minimum TTL for DNS Caching.]

- **Real-time DNS snooping for dynamic FQDN policy updates (cSRX, SRX1600, SRX2300, SRX4100, SRX4120, SRX4200, SRX4300, SRX4600, SRX4700, SRX5400, SRX5600, SRX5800, and vSRX 3.0)**—Domain Name System (DNS) snooping inspects and caches DNS responses in real time.

  After you enable DNS snooping, the firewall:

  1. Captures DNS response packets as traffic traverses the network.
  2. Extracts relevant DNS records.
  3. Builds a local cache mapping of fully qualified domain names (FQDNs) to IP addresses.

  The firewall keeps these mappings accurate and current for IPv4 or IPv6 traffic. Use this feature to implement real-time DNS mapping updates in environments with frequently changing DNS entries.

  [See DNS Snooping for Security Policies.]

- **DNS snooping and DNS module integration (cSRX, SRX1600, SRX2300, SRX4100, SRX4120, SRX4200, SRX4300, SRX4600, SRX4700, SRX5400, SRX5600, SRX5800, and vSRX 3.0)**—Use the integrated DNS-snooping cache in the Packet Forwarding Engine with the DNS module on the Routing Engine to unify entries from explicit DNS queries and DNS snooping in the data plane. The combined DNS cache remains accurate and relevant, helping you to apply DNS-based policies and destination network address translation (NAT) configurations effectively.

The `show security dns-cache` command displays entries from both the DNS resolver and DNS snooping.

[See DNS Snooping for Security Policies.]

- **Transparent web proxy with HTTP/2 support and application traffic exemption (SRX380, SRX320, SRX340, SRX345, SRX1600, SRX2300, SRX4100, SRX4120, SRX4200, SRX4300, and vSRX3.0)**—Use transparent web proxy to route traffic through an external proxy server without client awareness or additional configuration. You can exempt specific application traffic from the proxy, moving the traffic directly to the webserver. Transparent web proxy also supports HTTP/2, enabling secure HTTPS traffic relay without decryption. This functionality enhances the quality of service for specified applications by transparently mediating between the client and the webserver.

  [See Transparent Web Proxy.]

Dynamic Host Configuration Protocol

- **Display physical interface and VLAN ID in DHCP relay and server binding outputs (all Junos OS and Junos OS Evolved platforms)**—You can view the physical interface and VLAN ID in the outputs of the following commands:

  - `show dhcp relay binding`
  - `show dhcp server binding`
  - `show dhcpv6 relay binding`
  - `show dhcpv6 server binding`

  The enhanced output now displays data for **Physical interface** and **VLAN** alongside existing data. This addition facilitates easy understanding of client's binding origin.

  [See https://www.juniper.net/documentation/us/en/software/junos/cli-reference/topics/ref/command/show-dhcp-relay-binding.html and https://www.juniper.net/documentation/us/en/software/junos/cli-reference/topics/ref/command/show-dhcp-server-binding-command.html.]

Identity Aware Firewall

- **Optimized session report mechanism in user firewall authentication (SRX Series Firewalls and vSRX 3.0)**—An optimized session report mechanism enhances user firewall authentication performance by reducing Routing Engine delays. The mechanism updates the authentication entry timeout on the Routing Engine and reduces the number of messages that the Packet Forwarding Engine must send for session report updates. Firewall administrators benefit from the faster, accurate session reporting and gain overall system efficiency.

  [See show services user-identification authentication-table.]

- **SAML-based firewall authentication (cSRX, SRX Series Firewalls, and vSRX 3.0)**—You can authenticate users through Security Assertion Markup Language (SAML)-based access profiles using your

organization's identity provider (IdP) for firewall authentication. This method generates SAML requests and processes SAML assertions, enhancing the security and flexibility of user authentication. The integration supports single sign-on (SSO) using HTTP Redirect and HTTP POST SAML bindings, providing benefits such as improved security and reduced password management. Include the `access-profile` *`profile-name`* statement under `set security policies from-zone` *`zone-name`* `to-zone` *`zone-name`* `policy` *`policy-name`* `then permit firewall-authentication user-firewall` hierarchy to enable SAML-based captive portal authentication.

To apply a default Secure Sockets Layer (SSL) termination profile, use the `set access firewall authentication user-firewall default-ssl-termination-profile` *`default-ssl-termination-profile`* command. Enable this configuration to enforce security for all access profiles.

[See user-firewall (Access Firewall-Authentication), default-ssl-termination-profile (Access), user-firewall, policy (Security Policies), SAML Authentication in Juniper Secure Connect, saml, and authentication-order (Access Profile).]

Juniper Advanced Threat Prevention Cloud (ATP Cloud)

- **DoT support with SSL forward proxy (SRX Series Firewalls and vSRX Series Firewall)**—Use DNS over TLS (DoT) with SSL forward proxy to decrypt the DNS traffic. Use DNS filtering, domain generation algorithm (DGA) detection, and DNS tunneling detection to filter malicious domains, enhancing threat detection and privacy. To leverage DNS security with DoT, configure SSL proxy profile, manage certificates, and set up security policies. You can monitor traffic by using the DNS statistics commands.

  [See show services security-intelligence dns-statistics, Enable DNS SecIntel Detection, Enable DNS DGA Detection, Enable DNS Tunnel Detection, Configure DNS Sinkhole and Configuring SSL Proxy.]

Network Management and Monitoring

- **Support for multiple gRPC servers hosting different service sets (EX2300, EX2300-C, EX2300-MP, EX2300-VC, EX3400, EX3400-VC, EX4000-8P, EX4000-12P, EX4000-12T, EX4000-12MP, EX4000-24MP, EX4000-48MP, EX4000-24P, EX4000-24T, EX4000-48P, EX4000-48T, EX4100-24MP, EX4100-24P, EX4100-24T, EX4100-48MP, EX4100-48P, EX4100-48T, EX4100-F-12P, EX4100-F-12T, EX4100-F-24P, EX4100-F-24T, EX4100-F-48P, EX4100-F-48T, EX4100-H-12MP, EX4100-H-12MP-DC, EX4100-H-24F, EX4100-H-24F-DC, EX4100-H-24MP, EX4100-H-24MP-DC, EX4300-MP, EX4300VC, EX4400-24MP, EX4400-24P, EX4400-24T, EX4400-24X, EX4400-48F, EX4400-48MP, EX4400-48MXP, EX4400-48P, EX4400-48T, EX4400-48XP, EX4600-VC, EX4650, EX4650-48Y-VC, EX9204, EX9208, EX9214, MX204, MX240, MX304, MX480, MX960, MX2008, MX2010, MX2020, MX10004, MX10008, cSRX, SRX300, SRX320, SRX340, SRX345, SRX380, SRX1500, SRX1600, SRX2300, SRX4100, SRX4200, SRX4300, SRX4600, SRX4700, SRX5400, SRX5600, SRX5800, and vSRX 3.0)**—You can configure multiple gRPC servers that host different sets of services on unique ports. Additionally, each server can support different certificates, listening addresses, and routing instances. You configure the gRPC servers at the `[edit system services http servers]` hierarchy level. Distributing gRPC services across different servers allows

for better allocation of network resources, reducing the risk of port conflicts and optimizing server performance.

[See Configure gRPC Services and server.]

Platform and Infrastructure

- **Enhanced CPU core allocation for Routing Engine (vSRX 3.0)**—You can enhance system stability and performance in vSRX 3.0 by configuring even numbers of CPU cores for the Routing Engine. When you launch vSRX 3.0 instances with even numbers of CPU cores configured, by default two CPU cores are allocated to the Routing Engine. This allocation enhances system stability and ensures the efficient operation of both the Routing Engine and Packet Forwarding Engine. For systems with an odd number of CPU cores, only one core is allocated to the Routing Engine.

  The `set security forward-options resource-manager cpu re <n>` command is now deprecated. You cannot manually configure the number of CPU cores on the Routing Engine because the default assignment automatically allocates these cores.

  Use the `show security forward-options resource-manager settings` to verify the RE CPU core count.

  [See Junos OS Features Supported on vSRX Virtual Firewall, resource-manager (Forwarding-options), and show security forward-options resource-manager.]

What's Changed

IN THIS SECTION

Learn about what changed in this release for vSRX.

Juniper Secure Connect

- **Support for iPadOS for prelogon compliance checks in Juniper Secure Connect (SRX Series, and vSRX3.0)**—You can configure prelogon compliance checks on your firewall to allow or reject endpoints running iPadOS. Use the `ipados` option at the `[edit security remote-access compliance pre-logon` *`name`* `term` *`name`* `match platform]` hierarchy level to enforce these checks. This ensures that only compliant iPadOS devices are permitted access, enhancing the security of your network.

  [See compliance (Juniper Secure Connect).]

Network Address Translation (NAT)

- Support for NAT debugging (SRX Series Firewalls and vSRX) To debug NAT-related issues, use the nat option with the request support information security-components command.

  [See request support information.]

User Interface and Configuration

- **Access privileges for request support information command (ACX Series, EX Series, MX Series, QFX Series, SRX Series Firewalls, and vSRX Virtual Firewall)**—The `request support information` command is designed to generate system information for troubleshooting and debugging purposes. Users with the specific access privileges `maintenance`, `view`, and `view-configuration` can execute request support information command.

- **Option to view combined disk space usage statistics for all configuration databases (ACX Series, EX Series, MX Series, QFX Series, SRX Series, and vSRX)**—The `show system configuration database usage` command provides the `merge` option. When you include the `merge` option, the command output displays combined disk space usage statistics for all configuration databases, including the static configuration database and all ephemeral configuration database instances.

  [See show system configuration database usage.]

VPNs

- **Deprecation of weak algorithms in IPsec VPN (SRX Series and vSRX 3.0)**—We've deprecated the weak algorithms in IKE and IPsec proposals. You'll no longer be able to use the following algorithms:

Table 14: Deprecated Junos CLI Options

Type	Algorithm	Junos CLI Statement
Encryption Algorithm in IKE Proposal	des-cbc and 3des-cbc	set security ike proposal *name* encryption-algorithm
Authentication Algorithm in IKE Proposal	md5 and sha1	set security ike proposal *name* authentication-algorithm
DH Group in IKE Proposal	group1, group2, and group5	set security ike proposal *name* dh-group
Encryption Algorithm in IKE Proposal	des-cbc and 3des-cbc	set security ipsec proposal *name* encryption-algorithm
Authentication Algorithm in IKE Proposal	hmac-md5-96 and hmac-sha1-96	set security ipsec proposal *name* authentication-algorithm

You will receive a warning message if you configure these deprecated algorithms explicitly. As an alternative, we recommend that you configure the stronger algorithms to enhance the security in IPsec VPN.

[See proposal (Security IKE, and proposal (Security IPsec).]

- **Default installation of junos-ike package on additional platforms (SRX1500, SRX4100, SRX4200, SRX4600, and vSRX3.0)**—The junos-ike package is installed by default on SRX1500, SRX4100, SRX4200, SRX4600, and vSRX3.0 firewalls, ensuring the default support for iked process for IPsec VPN service. This aligns with the existing default installation of the package on SRX5000 line with Routing Engine 3 (SRX5K-SPC3 with RE3). You can delete the junos-ike package using the command request system software delete junos-ike. This runs the kmd process on these firewalls, allowing flexible management of your security infrastructure.

  [See IPsec VPN Feature Support with New Package.]

- **Support for iPadOS for prelogon compliance checks in Juniper Secure Connect (SRX Series, and vSRX3.0)**—You can configure prelogon compliance checks on your firewall to allow or reject endpoints running iPadOS. Use the ipados option at the [edit security remote-access compliance pre-logon *name* term *name* match platform] hierarchy level to enforce these checks. This ensures that only compliant iPadOS devices are permitted access, enhancing the security of your network.

  [See compliance (Juniper Secure Connect).]

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

IN THIS SECTION

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.

General Routing

- On SRX300 line of devices configured with native-vlan-id, after upgrading an SRX300 line of devices to Junos OS release 23.4R1 or higher, the native-vlan-id option disappears from the interface settings. If native-vlan-id was set before the upgrade, the device keeps the setting but it does not apply it to the interface. Deleting native-vlan-id causes a syntax error. The native-vlan-id feature doesn't work, and if a custom VLAN ID (other than 1) is used then traffic for that VLAN will be affected. PR1847366

Resolved Issues

IN THIS SECTION

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.

Content Security

- Change in content-filter return codes when action is block and notification is protocol-only. PR1845496

General Routing

- RTO traffic loss and accumulation of session on secondary node is observed when RTO traffic not evenly distributed to all FLT threads. PR1819911
- Dedicated-offload-cpu requires a full restart of vSRX 3.0 in Junos OS Release 24.4R1. PR1842550
- Auto-re-enrollment for local certificate once fail, not trigger again. PR1845573
- vSRX 3.0 kernel panic when deployed in Qemu version 8.1 and above. PR1845886
- Intermittent traffic drops are seen due to large memory allocation for unidentified files. PR1851786

- PIM IP ESP packet fragments are dropped. PR1854130
- Split brain scenario is observed on vSRX 3.0 with public cloud MNHA deployment. PR1855010
- Missing vCPU after downgrading from Junos OS release 25.2 to lower versions. PR1871397
- The srxpfe process stops responding on vSRX platform after set disables on the ge- interface and then rollback. PR1874848
- On vSRX 3.0 platforms, MNHA link fails to come up when MNHA ICL tunnel is enabled alongside dedicated-offload-cpu. PR1875491

Flow-Based and Packet-Based Processing

- In vSRX orphan backup sessions will exhaust session resources due to high backup session timeout value. PR1846897
- Type 5 VXLAN traffic drops are observed when SRX Series Firewall run as L3-VNI gateway and the ingress and egress traffic goes to the same Type-5 VXLAN peer. PR1847419
- Data Plane CPU on one device spikes up to 95% during primary node system reboot in SRX cluster PR1856521

Network Address Translation (NAT)

- New CLI for RSI updated to collect more NAT information. PR1825372

Platform and Infrastructure

- FTP default mode changed from active to passive on Junos OS release 24.2R2. PR1874525

Routing Policy and Firewall Filters

- Failed inter-process communication results in higher heap and buffer usage which impacts the functionality of processes. PR1823591
- RT_FLOW_SESSION_CLOSE carries encrypted field as 'UNKNOWN" for ssl traffic. PR1879078

VPNs

- ICL connection getting established with wrong source interface IP when trying to establish ICL connection between pub-broker and sub-broker with loopback interface IP's. This resulting in IPsec session sync failure between master and backup MNHA devices. PR1840788
- The show chassis high-availability information CLI says SRG1 control plane state as Ready ICL connection between Pub-Broker Sub-broker is not established properly and IPsec sessions are not synchronize between primary and standby MNHA peers. PR1840803
- IPsec tunnel distribution table on the Routing Engine is not cleaned up hitting SRXPFE generates core files when DPD is configured. PR1850526
- On vSRX 3.0 platforms IPsec tunnels do not redistributed with dedicated-offload-cpu knob enabled. PR1860693

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 25.2R1 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 25.2R1 for vSRX .tgz** file from the Juniper Networks website. Note the size of the software image.
2. Verify that you have enough free disk space on the vSRX instance to upload the new software image.

```
root@vsrx> show system storage
       Filesystem             Size       Used      Avail  Capacity   Mounted on
       /dev/vtbd0s1a          694M       433M       206M       68%  /
       devfs                  1.0K       1.0K         0B      100%  /dev
       /dev/md0               1.3G       1.3G         0B      100%  /junos
       /cf                    694M       433M       206M       68%  /junos/cf
       devfs                  1.0K       1.0K         0B      100%  /junos/dev/
```

```
        procfs                  4.0K       4.0K          0B      100%  /proc
        /dev/vtbd1s1e           302M        22K       278M        0%  /config
        /dev/vtbd1s1f           2.7G        69M       2.4G        3%  /var
        /dev/vtbd3s2             91M       782K        91M        1%  /var/host
        /dev/md1                302M       1.9M       276M        1%  /mfs
        /var/jail               2.7G        69M       2.4G        3%  /jail/var
        /var/jails/rest-api       2.7G        69M       2.4G      3%  /web-api/var
        /var/log                2.7G        69M       2.4G        3%  /jail/var/log
        devfs                   1.0K       1.0K          0B      100%  /jail/dev
        192.168.1.1:/var/tmp/corefiles       4.5G       125M       4.1G    3%  /var/crash/
corefiles
        192.168.1.1:/var/volatile       1.9G       4.0K       1.9G    0%  /var/log/host
        192.168.1.1:/var/log       4.5G       125M       4.1G     3%  /var/log/hostlogs
        192.168.1.1:/var/traffic-log       4.5G       125M       4.1G    3%  /var/traffic-log
        192.168.1.1:/var/local       4.5G       125M       4.1G    3%  /var/db/host
        192.168.1.1:/var/db/aamwd       4.5G       125M       4.1G    3%  /var/db/aamwd
        192.168.1.1:/var/db/secinteld       4.5G       125M       4.1G    3%  /var/db/secinteld
```

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

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

```
<
output omitted>
```

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

4. Use FTP, SCP, or a similar utility to upload the Junos OS Release 25.2R1 for vSRX .tgz file to **/var/crash/corefiles/** on the local file system of your vSRX VM. For example:

```
root@vsrx> file copy ftp://username:prompt@ftp.hostname.net/pathname/
junos-vsrx-x86-64-20.4-2020-10-12.0_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 25.2R1 for vSRX.

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

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

```
--- JUNOS 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, EOL and EEOL:

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

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

For both EOL and EEOL releases, you can upgrade to the next three subsequent releases or downgrade to the previous three releases.

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

Table 15: EOL and EEOL Releases

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

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

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

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

13 December 2025—Revision 12, Junos OS Release 25.2R1-S1.

3 December 2025—Revision 11, Junos OS Release 25.2R1.

1 October 2025—Revision 10, Junos OS Release 25.2R1.

25 September 2025—Revision 9, Junos OS Release 25.2R1.

12 August 2025—Revision 8, Junos OS Release 25.2R1.

7 August 2025—Revision 7, Junos OS Release 25.2R1.

6 August 2025—Revision 6, Junos OS Release 25.2R1.

23 July 2025—Revision 5, Junos OS Release 25.2R1.

22 July 2025—Revision 4, Junos OS Release 25.2R1.

4 July 2025—Revision 3, Junos OS Release 25.2R1.

1 July 2025—Revision 2, Junos OS Release 25.2R1.

30 June 2025—Revision 1, Junos OS Release 25.2R1.