Release Notes: Junos® OS Release 15.1X49-D90 for the SRX Series

Release 15.1X49-D90
28 November 2017
Revision 4

Contents

Introduction

Junos OS runs on the following Juniper Networks® hardware: ACX Series, EX Series, M Series, MX Series, PTX Series, QFabric, QFX Series, SRX Series, and T Series.

These release notes accompany Junos OS Release 15.1X49-D90 for the SRX Series. They describe new and changed features, known behavior, and known and resolved problems in the hardware and software.

You can also find these release notes on the Juniper Networks Junos OS Documentation webpage, located at https://www.juniper.net/techpubs/software/junos/.

NOTE: Junos OS Release 15.1X49-D90 supports the following devices: SRX300, SRX320, SRX340, SRX345, and SRX550 High Memory (SRX550M), SRX1500, SRX4100, SRX4200, SRX5400, SRX5600, and SRX5800 devices with host subsystems composed of either an SRX5K-RE-1800X4 (RE2) with an SRX5K-SCBE (SCB2), or an SRX5K-RE-1800X4 (RE2) with an SRX5K-SCB3 (SCB3), and vSRX.

For more details about SRX 5400, SRX5600, and SRX5800 devices hardware and software compatibility, please see http://kb.juniper.net/KB30446. If you have any questions concerning this notification, please contact the Juniper Networks Technical Assistance Center (JTAC).

New and Changed Features

This section describes the new features and enhancements to existing features in Junos OS Release 15.1X49-D90 for the SRX Series devices.

Release 15.1X49-D90 Software Features

Flow-based and Packet-based Processing

- **Pre-fragmentation and post-fragmentation counters for SRX Series devices**—Starting in Junos OS Release 15.1X49-D90, packet fragmentation counters for IPsec tunnels are implemented to help you achieve optimum SRX Series performance. You can use the statistics made available by these counters to inform the procedures that you use to tune your system to avoid packet fragmentation. You can use the **show security flow session tunnel extensive**, **show security flow session tunnel summary**, and **show security flow statistics** commands to view fragmentation statistics information.

  [See Understanding the Fragmentation Counters Feature and Its Benefits]

User Access and Authentication

- **Ensured captive portal for unauthenticated users who use HTTP/HTTPS browsers for SRX Series devices**—Starting in Junos OS Release 15.1X49-D90, you can ensure that an unauthenticated user who issues an access request using an HTTP/HTTPS browser is presented with a captive portal interface to allow them to authenticate. It can happen that non-browser HTTP/HTTPS services running in the background at the same time can trigger captive portal authentication creating a race condition that suppresses presentation of the captive portal interface to the browser user. You specify the **auth-only-browser** parameter for firewall-authentication in security policies to direct it to ignore non-browser HTTP/HTTPS requests. You can also configure the **auth-user-agent** parameter to direct firewall authentication to check the User-Agent field in the browser header for information identifying content, such as **Opera**.

  [See Understanding How to Ensure That Firewall Authentication Provides Captive Portal Authentication to HTTPS/HTTP Browser Traffic]

Related Documentation

Changes in Behavior and Syntax

This section lists the changes in behavior of Junos OS features and changes in the syntax of Junos OS statements and commands from Junos OS Release 15.1X49-D90.

Authentication, Authorization and Accounting (AAA)

- Starting with Junos OS 15.1X49-D80, the **wins-server** option at the [**edit access profile *profile-name***] hierarchy level allows you to configure the IPv4 address of a Windows Internet Name Service (WINS) server.

CLI

- Starting with Junos OS Release 15.1X49-D60, the **modem1** option has been added to the **show wireless-wan adapter <adapter-name> modem** command. The **modem1** option displays details of the integrated modems on the CBA850 3G/4G/LTE Wireless WAN Bridge.

Dynamic Host Configuration Protocol (DHCP)

- Starting with Junos OS Release 15.1X49-D90, the factory-default configuration of SRX300, SRX320, SRX340, SRX345, and SRX550M devices has changed to allow small form-factor pluggable (SFP) ports to be configured as DHCP clients.

  See the following for configuration changes:

```
SRX300 / SRX320 / SRX320-POE
----------------------------
ge-0/0/0 and ge-0/0/7 (UNTRUST) - routed interfaces with DHCP client enabled
ge-0/0/1 - ge-0/0/6 - Ethernet Switching part of VLAN TRUST

SRX340 / SRX345
---------------------------
ge-0/0/0 and ge-0/0/15 (UNTRUST) - routed interfaces with DHCP client enabled
ge-0/0/1 - ge-0/0/14 - Ethernet Switching part of VLAN TRUST

SRX550M
---------------------------
ge-0/0/0 and ge-0/0/9 (UNTRUST) - Routed interface with DHCP client enabled
ge-0/0/1-5 (TRUST) - Routed interfaces with DHCP server enabled

Also enable RSTP protocol by default (set protocols rstp)
```

- Starting with Junos OS Release 15.1X49-D80, a new command, **force-discover**, is introduced to the DHCP client to force the DHCP client to send a DHCP discover packet after one to three failed **dhcp-request** attempts. The **force-discover** option ensures that the DHCP server will assign the same or a new IP address to the client. To ensure that this process does not fail in the event of a DHCP server outage, the **retransmission-attempt** value has been extended from a maximum of 6 to 50,000 attempts. No changes are made to the current default values.

  To start the new DHCP process, include the **force-discover** command in the [edit interfaces] hierarchy level. For example,

set interfaces ge-0/0/0 unit 0 family inet dhcp-client force-discover

- Starting with Junos OS Release 15.1X49-D60, the legacy DHCPD (DHCP daemon) configuration on all SRX Series devices is being deprecated and only the new JDHCP CLI will be supported. When you upgrade to Junos OS Release 15.1X49-D60 and later releases on a device that already has the DHCPD configuration, the following warning messages are displayed:

  WARNING: The DHCP configuration command used will be deprecated in future Junos releases.

  WARNING: Please see documentation for updated commands.

  To ensure uninterrupted service to existing user implementation of DHCP relay service, the following configuration items are identified as missing (edit and interface hierarchies) between the old DHCPD and the new JDHCPD configurations:

  set forwarding-options helpers bootp description
  set forwarding-options helpers bootp client-response-ttl
  set forwarding-options helpers bootp maximum-hop-count
  set forwarding-options helpers bootp minimum-wait-time
  set forwarding-options helpers bootp vpn
  set forwarding-options helpers bootp relay-agent-option
  set forwarding-options helpers bootp dhcp-option82

  and the interface hierarchy:

  set forwarding-options helpers bootp interface *interface-name* description
  set forwarding-options helpers bootp interface *interface-name* client-response-ttl
  set forwarding-options helpers bootp interface *interface-name* maximum-hop-count
  set forwarding-options helpers bootp interface *interface-name* minimum-wait-time
  set forwarding-options helpers bootp interface *interface-name* vpn
  set forwarding-options helpers bootp interface *interface-name* relay-agent-option
  set forwarding-options helpers bootp interface *interface-name* dhcp-option82

Flow-based and Packet-based Processing

- **Flow-based processing for IPv6 Traffic**—Starting with Junos OS Release 15.1X49-D70, on the SRX1500, SRX4100, and SRX4200 devices, flow-based processing for IPv6 traffic is enabled by default. Also, you do not need to reboot the device when you are switching modes between flow mode, packet mode, and drop mode.

  When IPv6 is configured on SRX300 Series devices, drop mode remains the default behavior because of memory constraints. In this case, you must reboot the device after changing the processing mode from the drop mode default to flow mode and between modes.

  Flow-based processing for IPv4 Traffic—The SRX Series device is enabled for flow-based forwarding for IPv4 traffic on all devices by default. For the SRX1500, SRX4100, SRX4200 devices and vSRX, you do not need to reboot the device when you are switching modes between flow mode, packet mode, and drop mode. For SRX300 Series devices, you *must* reboot the device when switching between flow mode, packet mode, and drop mode.

- **Source address for SRX5400, SRX5600, and SRX5800 devices and vSRX instances**—Starting with Junos OS 15.1X49-D60, management traffic can originate from a specific source address for Domain Name System (DNS) names.

  Consider the following when you configure the source address for DNS:

  - Only one source address can be configured as the source address for each DNS server name.
  - IPv6 source addresses are supported for IPv6 DNS servers, and only IPv4 addresses are supported for IPv4 DNS servers. You cannot configure an IPv4 address for an IPv6 DNS server or an IPv6 address for an IPv4 DNS server.

  To have all management traffic originate from a specific source address, configure the system name server and the source address. For example:

  ```
  user@host# set system name-server 5.0.0.1 source-address 4.0.0.3
  ```

Installation and Upgrade

- Starting with Junos OS Release 15.1X49-D80, on SRX5400, SRX5600, and SRX5800 devices, if the software image is installed from a USB device, a fips-error core is generated during bootup of the device. This core dump is harmless and does not affect any other functionality. To avoid this issue, after installing the software image using a USB, install the software image again using the Junos CLI.

Network Address Translation (NAT)

- Starting with Junos OS Release 15.1X49-D90, the number of addresses in NAT source pools with IPv6 prefixes are represented as zeros (0).This change ensures that when a configuration that includes a NAT source pool with IPv6 prefixes is committed, the capacity check is not exceeded, and the commit is successful. This change will be reflected in the output of the following commands when used on NAT source pools with IPv6 prefixes:

  - **show security nat resource-usage source-pool**—The **Avail** and **Total** fields are zero (0).
  - **show security nat source pool**—The **Total Addresses** field is 0.
  - **show security nat source summary**—The **Total Address** field is 0.

- Starting with Junos OS Release 15.1X49-D60, when you delete or modify a NAT rule, a NAT pool, or an interface address, the related NAT bindings might not be deleted immediately. In addition, the related session scan for the NAT rule and NAT pool might not be deleted as quickly as in previous releases.

Public Key Infrastructure

- Generating a public key infrastructure (PKI) signature of 512 bits for a digital certificate with Digital Signal Algorithm (DSA) or RSA encryption is being deprecated on SRX Series devices and vSRX instances:

  - Starting with Junos OS Release 15.1X49-D75, the **size 512** option is not supported in the CLI command **request security pki generate-key-pair certificate-id** *certificate-id-name* **type dsa**. Instead, the **size** must be **1024** (the default value), **2048**, or **4096**.
  - The **size 512** option is being deprecated in the CLI command **request security pki generate-key-pair certificate-id** *certificate-id-name* **type rsa** and will no longer be supported in a future release. Instead, the **size** must be **1024**, **2048** (the default value), or **4096**.

- The **request security pki local-certificate enroll** command now includes the **cmpv2** and **scep** keywords for CMPv2 and SCEP certificate enrollment. Each keyword has configurable options. In previous releases, SCEP enrollment parameters were entered after the **enroll** keyword. Starting with this release, SCEP enrollment parameters should be entered after the **scep** keyword. In a future release, SCEP enrollment parameters after the **enroll** keyword will be deprecated.

  The **auto-re-enrollment** configuration statement at the [**edit security pki**] hierarchy level now includes the **cmpv2** and **scep** keywords for automatic reenrollment of local certificates using CMPv2 or SCEP. Each keyword has configurable options. In previous releases, SCEP enrollment parameters were entered after the **set security pki auto-re-enrollment certificate-id** *certificate-id-name* statement. Starting with this release, SCEP reenrollment parameters should be entered after the **scep** keyword. In a future release, SCEP enrollment parameters after the **set security pki auto-re-enrollment certificate-id** *certificate-id-name* statement will be deprecated.

Routing Protocols

- Starting in Junos OS Release 15.1X49-D80, **authentication-key-chain** configuration is not supported on SRX devices.

System Logs

- Starting with Junos OS Release 15.1X49-D80, two new system log messages have been added to indicate memory-related problems on the interfaces to the DDR3 memory:
  - XMCHIP_CMERROR_DDRIF_INT_REG_CHKSUM_ERR_MINOR
  - XMCHIP_CMERROR_DDRIF_INT_REG_CHKSUM_ERR_MAJOR

  These error messages indicate that the XMCHIP on an Flexible PIC Concentrator (FPC) has detected a checksum error, which is causing packet drops.

  The following error threshold values classify the error as a major error or a minor error:
  - Minor error —> 5 errors per second
  - Major error —> 255 errors per second (maximum count)
- Starting in Junos OS Release 15.1X49-D70, new parameters are added to the structured log fields of the antivirus, antispam, content, and apppxy system log messages.

The following example shows the structured log fields of **AV_VIRUS_DETECTED_MT, ANTISPAM_SPAM_DETECTED_MT, CONTENT_FILTERING_BLOCKED_MT, APPPXY_RESOURCE_OVERUSED_MT, and APPPXY_SESSION_ABORT_MT** messages before Junos OS Release 15.1X49-D70:

AntiVirus: Virus detected: from <source-address>:<source-port> to <destination-address>:<destination-port> source-zone <source-zone-name> <filename> file <temporary-filename> virus <name> URL:<url> username <username> roles <roles>

AntiSpam: SPAM detected: <source-name> (<source-address>) <action> reason: <reason> username <username> roles <roles>

Content Filtering: <argument> (<profile-name> from <source-address> is <action> due to <reason> username <username> roles <roles>

ApplicationProxy: Suspicious client <source-address>:<source-port>->(<destination-address>:<destination-port>) used <percentage-value> connections, which exceeded the maximum allowed <maximum-value> connectionsusername <username> roles <roles>

ApplicationProxy: session from <source-address>:<source-port> to <destination-address>:<destination-port> aborted due to <error-message> (code <error-code>)

The following example shows **AV_VIRUS_DETECTED_MT, ANTISPAM_SPAM_DETECTED_MT, CONTENT_FILTERING_BLOCKED_MT, APPPXY_RESOURCE_OVERUSED_MT, and APPPXY_SESSION_ABORT_MT** messages in Junos OS Release 15.1X49-D70, indicating the newly added parameters in the structured log fields:

AntiVirus: Virus detected: <source-address>:<source-port>-><destination-address>:<destination-port> source-zone="<source-zone-name>" profile-name="<profile-name>" file="<filename>" temp_file="<temporary-filename>" virus="<name>" URL="<url>" username="<username>" roles="<roles>"

AntiSpam: SPAM detected: name="<source-name>" source-ip=(<source-address>) profile-name="<profile-name>" action="<action>" reason="<reason>" username="<username>" roles="<roles>"

Content Filtering: protocol="<argument>" <source-address>:<source-port>-><destination-address>:<destination-port> profile-name="<profile-name>" action="<action>" reason="<reason>" username="<username>" roles="<roles>"

ApplicationProxy: Suspicious client <source-address>:<source-port>->(<destination-address>:<destination-port>) used <current-connections> connections, which exceeded the maximum allowed <maximum-value> connections. policy-name <policy-name> username <username> roles <roles>

ApplicationProxy: session from <source-address>:<source-port> to <destination-address>:<destination-port> aborted due to <error-message> (code <error-code>), policy-name <policy-name>

VPN

- Starting with Junos OS Release 15.1X49-D90, if VPN session affinity is enabled on SRX5400, SRX5600, and SRX5800 devices, the tunnel overhead is calculated according to the negotiated encryption and authentication algorithms on the anchor Services Processing Unit (SPU). If the configured encryption or authentication changes, the tunnel overhead is updated on the anchor SPU when a new IPsec security association is established.
- Starting with Junos OS Release 15.1X49-D80, the **xauth access-profile** option is being deprecated at the [**edit security ike gateway *gateway-name***] hierarchy level, and will no longer be supported in a future release. A new configuration option **aaa access-profile** is added under [**edit security ike gateway *gateway-name***] hierarchy level for Extended Authentication (XAuth) and Extensible Authentication Protocol (EAP) authentication. Also, **AAA** replaces the **XAuth** field names in the outputs for the **show security ike active-peer**, **show security ike active-peer detail**, **show security ike security-association detail**, and **show security ipsec next-hop-tunnels** commands.
- The **show security dynamic-vpn client version** command is not supported for dynamic VPN.
- Starting with Junos OS Release 15.1X49-D70, a warning message is displayed if you configure the **establish-tunnels immediately** option at the [**edit security ipsec vpn *vpn-name***] hierarchy level on AutoVPN hubs with point-to-point tunnel interfaces. Committing the configuration will succeed, however the **establish-tunnels immediately** configuration is ignored. The state of the point-to-point tunnel interface will be up all the time.

  The **establish-tunnels immediately** option is not appropriate for AutoVPN hubs with point-to-point tunnel interfaces because multiple VPN tunnels may be associated with a single AutoVPN configuration.

Related Documentation

- New and Changed Features on page 4
- Resolved Issues on page 19
- Known Behavior on page 10
- Known Issues on page 15
- Migration, Upgrade, and Downgrade Instructions on page 23

Known Behavior

This section contains the known behaviors, system maximums, and limitations in hardware and software in Junos OS Release 15.1X49-D90.

Class of Service (CoS)

The following limitations apply to CoS support on VPN st0 interfaces:

- Currently, the maximum number for software queues is 2048. If the number of st0 interfaces exceeds 2048, not enough software queues can be created for all the st0 interfaces.
- Only route-based VPN can apply st0 CoS. Table 1 on page 11 describes the st0 CoS feature support for different types of VPN.

Table 1: CoS Feature Support for VPN

Classifier Features	Site-to-Site VPN (P2P)	ADVPN/AutoVPN (P2MP)
Classifiers, policers, and rewriting markers	Supported	Supported
Queueing, scheduling, and shaping based on st0 logical interfaces	Supported	Not supported
Queueing, scheduling, and shaping based on virtual channels	Supported	Supported

- On SRX300, SRX320, SRX340, SRX345, and SRX550M devices, one st0 logical interface can bind to multiple VPN tunnels. The eight queues for the st0 logical interface cannot reroute the traffic to different tunnels, so pre-tunneling is not supported.

  NOTE: **The virtual channel feature can be used as a workaround on SRX300, SRX320, SRX340, SRX345, and SRX550M devices.**

- When defining a CoS shaping rate on an st0 tunnel interface, consider the following restrictions:
  - The shaping rate on the tunnel interface must be less than that of the physical egress interface.
  - The shaping rate only measures the packet size that includes the inner Layer 3 cleartext packet with an ESP/AH header and an outer IP header encapsulation. The outer Layer 2 encapsulation added by the physical interface is not factored into the shaping rate measurement.
  - The CoS behavior works as expected when the physical interface carries the shaped GRE or IP-IP tunnel traffic only. If the physical interface carries other traffic, thereby lowering the available bandwidth for tunnel interface traffic, the CoS features do not work as expected.
- On SRX550M, SRX5400, SRX5600, and SRX5800 devices, bandwidth limit and burst size limit values in a policer configuration are a per-SPU, not per-system limitation. This is the same policer behavior as on the physical interface.

Ethernet Switching

- On SRX300, SRX320, SRX340, SRX345, and SRX550M devices, when you create an aggregated interface with two or more ports and if a link in the bundle goes down, the traffic forwarded through the same link will be rerouted two seconds later. This causes an outage for the traffic being sent to the link until reroute is complete.
- SRX300, SRX320, SRX340, SRX345, and SRX550M devices do not support Connectivity Fault Management (CFM) packet level filtering. SRX Series devices do not forward the Link Trace Messages (LTMs) packets through Layer 2 engine if any CFM MPs configured on the device. You must configure maintenance association intermediate points (MIPs) on the intermediate device to pass the LTM packets to the other device.
- In Junos OS Release 15.1X49-D40, the Three-color policer feature is not supported on SRX Series devices and vSRX instances.

Flow-based and Packet-based Processing

- On SRX5400, SRX5600, and SRX5800 devices, in central point architecture, system logs are sent per second per SPU. Hence, the number of SPUs define the number of system logs per second.
- On SRX340 and SRX345 devices, fabric interfaces must be configured such that the Media Access Control Security (MACsec) configurations are local to the nodes. Otherwise, the fabric link will not be reachable.

General Packet Radio Service (GPRS)

- Starting in Junos OS Release 15.1X49-D40, the SCTP flow session utilizes a connection tag to more finely distribute SCTP traffic across SPUs on SRX5400, SRX5600, and SRX5800 devices that support the SCTP ALG. The connection tag is decoded from the SCTP vtag. A separate SCTP session will be created for each of the first three packets—that is, one session for INIT, INIT-ACK, and COOKIE-ECHO, respectively. Because, the reverse-direction traffic has its own session, the session can no longer match the existing forward-direction session and pass through automatically. Therefore, similar to the forward-direction policy, an explicit policy is needed for approving the reverse-direction SCTP traffic. In this scenario, the SCTP flow session requires a bidirectional policy configuration to be established for even a basic connection.
- On SRX5000 Series devices, when you use the GTP inspection feature, during an ISSU from Junos OS Release 15.1X49-D10, 15.1X49-D20, or 15.1X49-D30 to Junos OS Release 15.1X49-D40 or later, GTPv0 tunnels will not be synchronized to the upgraded node.

  For GTPv1 and GTPv2, the tunnels will be synchronized, but the timeout gets restarted.

  Beginning with Junos OS Release 15.1X49-D40, ISSU is fully supported with the GTP inspection feature enabled.

Interfaces and Routing

- On SRX1500 devices, when 1G SFP-T is used on the 1G SFP ports (ge-0/0/12 to ge-0/0/15), the ge interface does not operate at 100M speed.

Integrated User Firewall

- In Junos OS Release 15.1X49-D50, you cannot use the Primary Group, whether by its default name of Domain Users or any other name (if you happened to have changed it), in integrated user firewall configurations.

  When a new user is created in Active Directory, the user is added to the global security group Primary Group which is by default called Domain Users. The Primary Group is less specific than other groups created in Active Directory because all users belong to it. Consequently it can become very large.

Software Installation and Upgrade

- On SRX5000 Series devices, In-Service Software Upgrade (ISSU) is not supported for upgrading from earlier Junos OS releases to Junos OS Release 15.1X49. ISSU is supported for upgrading to successive Junos OS Release 15.1X49 releases and to major Junos OS releases.

  NOTE: SRX300 Series devices and SRX550M devices do not support ISSU.

Platform and Infrastructure

- On SRX5800 devices, if global SOF policy (all session service-offload) is enabled, the connections per second (CPS) will be impacted due to IOC2 limitation. It is recommended to use IOC3 card if more sessions are required for SOF or lower the SOF session amount to make sure IOC2 is capable of handling it.

USB autoinstallation

- On SRX300 Series Services Gateways on which the USB autoinstallation feature is enabled (the default configuration), removal of a USB storage device immediately after insertion is not supported.

  NOTE: USB autoinstallation is not supported on SRX1500, SRX4100, SRX4200, SRX5400, SRX5600, and SRX5800 devices.

  After you insert a USB storage device, Junos OS scans the device to check whether it contains the USB autoinstallation file. This process might take up to 50 seconds to complete depending on the quality of the USB storage device and the number and size of the files in the device. Removing the USB storage device while this process is running might cause the services gateway to reboot, the USB port to stop working, and data loss on the USB. We recommend that after inserting a USB storage device, you wait for at least 60 seconds before removing it.

  By issuing the **set system autoinstallation usb disable** command (which disables the USB autoinstallation feature) before you insert the USB device, you can reduce the waiting interval between insertion and removal of a USB storage device from 60 seconds to 20 seconds.

VPN

- If the IKE external interface is disabled then enabled, tunnels that use TCP connections with NCP Exclusive Remote Access Clients may not come up. If this occurs, reduce the TCP timeout for the client connections with the **inactivity-timeout** option at the [**edit applications application** *application-name*] hierarchy level. The **destination-port** configured at the [**edit applications application** *application-name*] hierarchy level must match the **ports** option configured at the [**edit security tcp-encap profile** *profile-name*] hierarchy level. The configuration application must then be specified in the **match application** configuration at the [**edit security policies from-zone** *from-zone* **to-zone** *to-zone* **policy** *policy-name*] hierarchy level.

  Tunnels that use TCP connections might not survive ISSU if the dead peer detection (DPD) timeout is not large enough. If you see this happening, increase the DPD timeout to a value greater than 120 seconds. The DPD timeout is a product of the configured DPD interval and threshold. For example, if the DPD interval is 32 and the threshold is 4, the timeout is 128.

- ISSU with VPN configuration is not supported when upgrading from a Junos OS release prior to 15.1X49-D75 to Junos OS Release 15.1X49-D75 and later releases. You can use ISSU with VPN configuration when upgrading from Junos OS Release 15.1X49-D75 to later releases. You can also use ISSU with VPN configuration to upgrade from Junos OS Release 15.1X49-D10 up to Junos OS Release 15.1X49-D70.

- On SRX Series devices, configuring RIP demand circuits over P2MP VPN interfaces is not supported.
- On SRX5400, SRX5600, and SRX5800 devices, do not use ISSU if upgrading from Junos OS Release 15.1X49-D30 through Junos OS Release 15.1X49-D60, if using any VPN configurations.

  As a workaround deactivate or remove all the VPN commands from the configuration before executing ISSU. If the workaround is used, all VPN tunnels and VPN traffic will be dropped during ISSU upgrade. Once ISSU has completed you may then re-enable the VPNs as before.

Related Documentation

- New and Changed Features on page 4
- Changes in Behavior and Syntax on page 5
- Known Issues on page 15
- Resolved Issues on page 19
- New and Changed Features on page 4

Known Issues

This section lists the known issues in hardware and software in Junos OS Release 15.1X49-D90.

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

Application Layer Gateways (ALGs)

- On SRX300 device, sometimes autoinstallation fails when you configure through Trivial File Transfer Protocol (TFTP) and the MAC address is incorrect . PR1258839

Ethernet Switching

- On SRX300, SRX320, SRX340, SRX345, and SRX550M devices, the current Ethernet switching MAC aging is using software to age out bulk learned MAC addresses. You cannot age out specific MAC address learned at specific time immediately after the configured age. The MAC address might be aged out close to two times the configured age out time. PR1179089
- On SRX1500 devices configured in Ethernet switching mode, only few MAC entries are shown in the output of **show ethernet-switching table** command, even after MAC age out time. This issue is applicable only when MAC learning table has more than 17000 MAC entries. PR1194667
- On SRX300, SRX320, SRX340, and SRX345 devices, you cannot launch setup wizard after using the reset configuration button when the device is in Layer 2 transparent mode. You can launch the setup wizard by using the reset configuration button on the device when the device is in switching mode. PR1206189

- On SRX345 and SRX550M devices, frame carried with priority bit on Tag Protocol Identifier (TPID) is lost when packet passes through with Layer 2 forwarding. PR1229021
- On SRX300, SRX320, SRX340, SRX345, and SRX550M devices, after certain period of enabling dot1x, multiple first message EAP frames with the same timestamp are transmitted. However, this does not affect any dot1x functionality. PR1245325
- On SRX345 device, sometimes it is observed that either on primary or the secondary node, the switching fab probe status is down in Layer 2 HA configuration. The Layer 2 HA traffic can work well under such state. This state moves to up on rebooting both nodes. PR1257617

Flow-based and Packet-based Processing

- On SRX1500 devices, the log buffer size is increased to 30,000 in event mode. When the log buffer size was 1000, the Packet Forwarding Engine generated logs burst when there were more than 30 entries and more logs were dropped. PR1133757
- On SRX5400, SRX5600, SRX5800 devices with IOC2 cards installed and np-cache feature enabled, low performance might be seen when fragmented traffic is present. PR1193769
- On SRX300, SRX320, SRX340, and SRX345 devices, the device reboots when Juniper USB with part number RE-USB-4G-S (740-028898) is inserted in the USB slot while the device is on. PR1214125
- On SRX1500, SRX4100, and SRX4200 devices, the RPM firewall counter increases the best-effort traffic class when **probe-type**, **tcp-ping**, and **dscp-code-points** CS7 are configured. PR1212678
- On SRX300, SRX320, SRX340, SRX345, and SRX550M devices, use logical tunnel interface: lt-0/0/0 as the destination interface option for RPM probe-server in device box.PR1257502
- On SRX300, SRX320, SRX340, and SRX345 devices, when the protocol packets flooded into device, the CPU usage is exhausted to process the BPDU frame which has higher priority than L3 protocol, such as, ICMP and IPv4. On the device, the CPU process to receive maximum number of frames and might exhaust during high traffic. PR1259793

Interfaces and Routing

- On SRX300, SRX320, SRX340, SRX345, and SRX550M devices, for IFLS (logical interface) scaling:
  - Without **per-unit-scheduler** configured, total IFL number is limited to 2048.
  - With **per-unit-scheduler** configured on the IFD interface: total IFL number is limited to CoS scheduler sub-unit upper limit (2048). So, IFL max-number for **per-unit scheduler** should be 2048 minus the number of physical interface (which is up with at least one logical interface up, maximum number is 128). PR1138997
- On SRX5600 devices, when CoS on st0 interface is enabled and the incoming traffic rate destined for st0 interface is higher than 300000 packets per second (pps) per SPU, the device might drop some of the high priority packets internally and shaping of

outgoing traffic might be impacted. It is recommended that you configure appropriate policer on the ingress interface to limit the traffic below 300000 pps per SPU. PR1239021

- On SRX550M devices, traffic loop is seen with MSTP for untag traffic from IxNetwork ports. Configuring **native-vlan id** on the interfaces connected to IxNetwork port removes the loop. PR1259099

J-Web

- On SRX Series devices in chassis cluster, if you want to use J-Web to configure and commit the configurations, you must ensure that all other user sessions are logged out including any CLI sessions. Otherwise, the configurations might fail. PR1140019
- On SRX1500 devices in J-Web, snapshot functionality **Maintain > Snapshot > Target Media > Disk > Click Snap Shot** is not supported. PR1204587
- On SRX Series devices, DHCP relay configuration under **Configure > Services > DHCP > DHCP Relay** page is removed from J-Web in Junos OS Release 15.1X49-D60. The same DHCP relay can be configured using the CLI. PR1205911
- On SRX Series devices, DHCP client bindings under Monitor is removed for Junos OS Release 15.1X49-D60. The same bindings can be seen in CLI using the **show dhcp client binding** command. PR1205915
- On SRX Series devices, if the load is more than 5000 bytes then the J-Web responds slowly and the navigation of pages takes more time. PR1222010
- On SRX4100 devices, a security policy page in J-Web does not load when it has 40000 firewall policy configuration. Navigate to **Configure > Security > Security Policy** page. PR1251714
- On SRX Series devices, the help pages for **Monitor>DHCP Server** and **Monitor>DHCP Relay** are not displayed. PR1267751

Network Address Translation (NAT)

- On SRX Series devices, if dead-peer-detection is configured, in a rare circumstances (under multiple failover), the **tcp-encap** sessions might be cleared. Refresh establishes a new **tcp-encap** sessions. PR1267273

Platform and Infrastructure

- On SRX Series devices, when a USB flash device with a mounted file system is physically detached by a user, the system might panic in such situation. This is a known FreeBSD issue which is resolved in version 7.3 and later. PR695780
- On SRX5800 devices, if the system service REST API is added to the configuration, though commit can be completed, all the configuration changes in this commit does not take effect. This occurs as the REST API daemon fails to come up and the interface IP is not available during bootup. The configuration is not read on the Routing Engine side. PR1123304

- On SRX4100 and SRX4200 devices, although the CLI is configurable, the following features are not supported: Group VPN, VPN Suite B, and encrypted control links when in chassis cluster. PR1214410
- On SRX Series devices, a core file is generated when traffic causes high memory usage and lot of memory allocation failures are observed at Deep Packet Inspection (DPI) module. The core file is difficult to reproduce and high memory usage might not always result in core file. The core file is generated due to buffering issues in DPI engine code when the application identification requires data to be buffered at engine. PR1266517

Unified Threat Management (UTM)

- On SRX Series devices with Sophos Antivirus (SAV) configured, some files that have size larger than the **max-content-size** might not go into fallback state. Instead, some protocols do not predeclare the content size. PR1005086
- On SRX Series devices, if Advanced Anti-Malware service (AAMW) is enabled, and SMTP is configured in the AAMW policy, and fallback permit is enabled, under the long network latency between device and AWS running Sky ATP service, there might be a file submission timeout. When the sending timeout happens, there is a potential chance that the e-mail sent out from the outlook stays in the outbox of the sender, and the receiver does not receive the e-mail. PR1254088

Upgrade and Downgrade

- On SRX550M devices, when upgrading from Junos OS Release 15.1X49-D30 to a later version, upgrade fails. PR1237971

VPN

- On SRX Series devices, if IPsec VPN tunnel is established using IKEv2, due to bad SPI, packet drop might be observed during CHILD_SA rekey when the device is the responder for this rekey. PR1129903
- On SRX Series devices, RIP is supported in P2P DC mode over st0 interfaces. PR1141817
- On SRX5800 devices, when upgrading from Junos OS Release 15.1X49-D30 to 15.1X49-D35, 15.1X49-D40, and 15.1X49-D50 or from 15.1X49-D35, 15.1X49-D40, and 15.1X49-D50 to 15.1X49-D60 release, the ISSU fails for AutoVPN/ADVPN/DEP IPsec VPN tunnels. PR1201955
- On SRX1500 devices, if DPD is configured for**tcp-encap** sessions, then the effective DPD timeout must be increased to greater than 120 seconds. PR1254875

Related Documentation

- New and Changed Features on page 4
- Migration, Upgrade, and Downgrade Instructions on page 23
- Changes in Behavior and Syntax on page 5
- Known Behavior on page 10
- Resolved Issues on page 19

Resolved Issues

This section lists the issues fixed in hardware and software in Junos OS Release 15.1X49-D90.

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

Resolved Issues

Application Identification and Tracking

- On SRX Series devices, when Express Path (SOF) is enabled, the ASIC recalculates all the UDP checksum on I/O Card IOC and causes traffic problem on the IPsec session. PR1254897

Chassis Clustering

- On SRX1500 devices in a chassis cluster, the SFP+-10G-CU3M DAC cable connects to the XE interface as the XE interface do not come UP physically. PR1246725
- On SRX Series devices in a chassis cluster, sometimes it is observed that modifying IPsec VPN configuration might cause file mismatch of **/var/etc/vpn_tunnel.id** between both primary and secondary nodes. The kmd process crashes on the new primary node after RG0 failover. PR1250178
- On SRX345 device in a chassis cluster, when ethernet-switching is configured utilizing RETH and switching fabric (swfab) interfaces, the ARP table might be updated incorrectly and show MAC addresses being learnt through incorrect interfaces. The ethernet-switching table continues to show the correct information during the issue. PR1252965
- On SRX Series devices, user firewall feature causes the memory leak on data plane. All the data plane memory can be used up and traffic failure might occur. PR1255022
- On SRX devices in a chassis cluster, IRB interface does not work in switching mode. PR1259286
- On SRX Series devices, when manual route-based IPsec VPN is configured, and enabled the VPN monitoring, might cause the st0 interface down, which results in VPN traffic dropping. PR1259422

CLI

- On SRX1500 devices, traces cannot be enabled or disabled through the CLI options under **tcp-encap traceoptions**. PR1252544

Dynamic Host Configuration Protocol (DHCP)

- On SRX Series devices, user might get stuck in **RELEASE** state with large negative lease time. This issue occurs due to the DHCP IPv4 or DHCP IPv6 relay environment with large scaled environment, and the system is under stress. PR1125189

Ethernet Switching

- Starting with Junos OS Release 15.1X49-D40 and later, on SRX5400, SRX5600 and SRX5800 devices, some CLI commands are missed in the Request Support Information (RSI) script. PR1236874
- On SRX5400, SRX5600, and SRX5800 devices, if fab 0 and fab 1 interfaces are changed, the device might drop STP Bridge Protocol Data Unit (BPDU) on RG1+ primary node in transparent mode. PR1243887
- On SRX300, SRX320, SRX340, and SRX345 devices, if an Aggregated Ethernet (AE) interface is changed from layer 2 to layer 3, then the ARP learning on this AE interface fails. PR1258667
- On SRX Series devices, when RG0 failover occurs, the Point-to-Point Protocol over Ethernet (PPPoE) session is disconnected. PR1259316

Flow-based and Packet-based Processing

- On SRX5600 device, the DNS and WIN IPs are in reverse order in active-peer output when configured at access level and access profile level. PR1252186
- On SRX Series devices, when you configure **http-get** Real-time Performance Monitoring (RPM) probes, the URL is lost in the get message. For example:

```
services {
    rpm {
        probe Keepalive {
            test http-GET {
                probe-type http-get;
                target url http://customerB.net;
                probe-count 1;
                probe-interval 5;
                test-interval 300;
                history-size 10;
            }
        }
    }
}
```

  PR1256865

- On SRX Series devices, the IPv6 address is detected duplicate on RETH interface when doing inet6 address configurations and failing over at the same time. The Domain

Name System (DNS) is sending packets from old primary and received from new primary node due to manual operation. Use configuration **set interfaces rethx unit xx family inet6 dad-disable** command to disable DAD function. PR1257109

- On SRX345 device, when you use the NCP remote access client with the TCP encapsulation (Pathfinder) setting enabled, only one Data Plane Redundancy Group (RG1+) can be used. When you use multiple RG1+ and packets traverse the fabric link (Z-mode traffic), packets are dropped. PR1263443
- On SRX Series devices, when http-reassemble is configured, non-http traffic over port 80 might be blocked by UTM Web filter, such as Real-Time Messaging Protocol (RTMP) traffic over port 80. PR1267317

Interfaces and Routing

- On SRX5400, SRX5600, and SRX5800 devices, when a new API tunnel between SNMP and Routing Engine (RE) is established, SNMP is linked to common RE while device uses JSSG RE. In this scenario, the related interfaces are not set. PR1253672
- On SRX Series devices, when Virtual Router Redundancy Protocol (VRRP) advertisements are sent in between L2 and VLAN interface from peer but not received properly, can cause a VRRP split brain condition. PR1254800

J-Web

- On SRX Series devices, when you add new IP address to firewall filter, the J-Web PHP memory does not overflow. PR1253482
- On SRX Series devices, when you view interfaces in J-Web **Configure > Interfaces > Ports**, the output does not show Zone for some interfaces. PR1255781
- On SRX340 and SRX345 devices, on the Setup Wizard default mode, an address pool is created for a management IP network even if you change the default management IP address in the **default-setup** mode. PR1259742

Multicast

- On SRX Series devices with Selective Packet Services configured, multicast traffic might be sent out-of-order by the device. PR1246877

Platform and Infrastructure

- On SRX Series devices, when using administrative users with restricted permissions, you might be unable to rollback to a certain version. PR1206074
- On SRX Series devices, the secondary node in a chassis cluster environment might crash or go into DB mode, displaying the **panic:rnh_index_alloc** message. This issue is sometimes observed in a chassis cluster environment with multipoint st0.x interface configured, and the tunnel interfaces flaps according to IPsec idle-timeout or IPsec VPN-monitor. PR1244491

- On SRX Series devices, watchdog issue happens if routing engine fails to update the watchdog timer every 3 minutes. The watchdog reboots the device. PR1256840
- On SRX Series devices, the error message **abnormal timer recovery** is displayed frequently in the logs, without any service impact. PR1260274

Public Key Infrastructure

- On SRX Series devices, the error message **timeout communicating with pki-service daemon** is displayed when you create local certificate with ECDSA key pair. For example:
  - user@host# request security pki generate-key-pair certificate-id <name> size 384 type ecdsa.
  - user@host# request security pki local-certificate generate-self-signed certificate-id <name> digest sha-256 domain-name aaa.com subject CN=X, O=X, C=X add-ca-constraint.
  - In PKI trace is noticed that it is failing to sign x509 certificate. For example, **ERROR: X509V3_EXT_conf_nid() failed for extn=hash. self_signed_x509: ERROR: add_ext() failed for extn 'hash'. self_signed_x509: cannot sign the x509**. PR1259867

Unified Threat Management (UTM)

- On SRX Series devices, when Advanced Anti-Malware (AAMW) service is enabled, enrolled with Sky ATP Service running in the cloud, and the user enables the traceoption with option **flag daemon** or **flag**. For example, **set services advanced-anti-malware traceoptions flag daemon** or **set services advanced-anti-malware traceoptions flag** all. If you commit the configuration changes in AAMW, there might be a coredump on Routing Engine (RE) AAMW daemon. The AAMW daemon recovers afterwards automatically. The coredump occurrence is rare. PR1261881

VPN

- On SRX Series devices in an IPv6 VRRP scenario, when a host sends **router solicitation** messages to VRRP virtual IPv6 address, the VRRP master replies **router advertisement** messages with physical MAC address instead of virtual MAC address, and the VRRP slave replies **router advertisement** messages with physical MAC address. As a result, the host has two default gateways installed and sends traffic directly to two devices instead of VRRP virtual IP. This issue affects the VRRP function and traffic. PR1108366
- On SRX5400, SRX5600, and SRX5800 devices, the st0 interface global counter statistics is not incrementing and keeps zero, although traffic passes through the tunnel sub-interfaces such as st0.0 and st0.1. PR1171958
- On SRX1500 devices in a chassis cluster, IP leak might occur under the following scenarios:
  - In case of IKEv1, it is possible for an IPsec VPN tunnel to be active without an active IKEv1 phase 1 SA. Since the assigned IP address associated with an IPsec VPN tunnel (for a user) is stored in the record of phase 1 SA, if HA RG0 failover occurs while there is no active IKEv1 phase SA exist for an IPsec VPN tunnel, the assigned IP address will be released to the authd daemon when the IPsec VPN tunnel is disconnected.

- In case a remote access IPsec VPN tunnel is cleared (for both IKEv1 and IKEv2), the assigned IP address is kept for 30 seconds before it is released back to the authd within an additional 2 minutes. If HA failover occurs during this time before the IP is received at the authd, there will be an IP address leak.
- If a new IP is assigned by authd daemon after every user is authenticated, regardless of the user already having an IP assigned from an early authentication. In case of IKEv1, authentication occurs at every IKE phase 1 SA rekey. If the KMD daemon restarts immediately (within 2 minutes) after an IKEv1 phase 1 SA rekey, there is a possibility that the newly assigned IP has not been released to authd daemon yet. This will lead to the leak of that IP. PR1252181

Related Documentation

- New and Changed Features on page 4
- Migration, Upgrade, and Downgrade Instructions on page 23
- Changes in Behavior and Syntax on page 5
- Known Behavior on page 10
- Known Issues on page 15

Documentation Updates

This section lists the errata and changes in the software documentation.

- In Junos OS Release 15.1X49-D90 there are no new J-Web features in this release. The J-Web online help for this release is the same as for Release 15.1X49-D80
- Information about MIBs is available in SNMP MIBS Explorer. On the Junos OS for SRX Series page, click **SNMP MIB Explorer** to view MIBs information. Use the MIBs Explorer to search for and view information about various MIBs, MIB objects, and SNMP notifications that are supported on Juniper Networks devices.
- Information about system log messages is available in System Log Explorer. On the Junos OS for SRX Series page, click **System Log Explorer** to view system log information. Use the System Log Explorer to search for and view information about various system log messages.

Migration, Upgrade, and Downgrade Instructions

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.

- Upgrade for Layer 2 Configuration on page 24
- Upgrade and Downgrade Scripts for Address Book Configuration on page 24

Upgrade for Layer 2 Configuration

Starting with Junos OS Release 15.1X49-D10 and later, only enhanced Layer 2 CLI configurations are supported. If your device was configured earlier for Layer 2 transparent mode, then you must convert the legacy configurations to Layer 2 next-generation CLI configurations.

For details on how to migrate from Junos OS Release 12.3X48-D10 and earlier releases to Junos OS Release 15.1X49-D10 and later releases, refer to the Knowledge Base article at http://kb.juniper.net/InfoCenter/index?page=content&id=KB30445.

Upgrade and Downgrade Scripts for Address Book Configuration

Beginning with Junos OS Release 12.1, you can configure address books under the **[security]** hierarchy and attach security zones to them (zone-attached configuration). In Junos OS Release 11.1 and earlier, address books were defined under the **[security zones]** hierarchy (zone-defined configuration).

You can either define all address books under the **[security]** hierarchy in a zone-attached configuration format or under the **[security zones]** hierarchy in a zone-defined configuration format; the CLI displays an error and fails to commit the configuration if you configure both configuration formats on one system.

Juniper Networks provides Junos operation scripts that allow you to work in either of the address book configuration formats (see Figure 1 on page 25).

About Upgrade and Downgrade Scripts

After downloading Junos OS Release 12.1, you have the following options for configuring the address book feature:

- **Use the default address book configuration**—You can configure address books using the zone-defined configuration format, which is available by default. For information on how to configure zone-defined address books, see the Junos OS Release 11.1 documentation.
- **Use the upgrade script**—You can run the upgrade script available on the Juniper Networks support site to configure address books using the new zone-attached configuration format. When upgrading, the system uses the zone names to create address books. For example, addresses in the trust zone are created in an address book named **trust-address-book** and are attached to the trust zone. IP prefixes used in NAT rules remain unaffected.

  After upgrading to the zone-attached address book configuration:

  - You cannot configure address books using the zone-defined address book configuration format; the CLI displays an error and fails to commit.

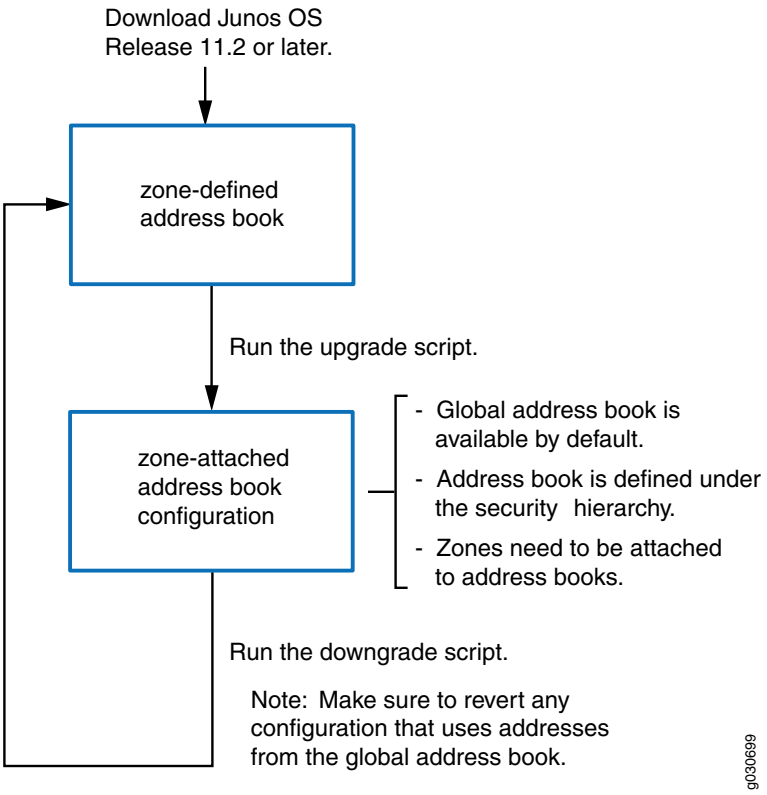
- You cannot configure address books using the J-Web interface.

For information on how to configure zone-attached address books, see the Junos OS Release 12.1 documentation.

- **Use the downgrade script**—After upgrading to the zone-attached configuration, if you want to revert to the zone-defined configuration, use the downgrade script available on the Juniper Networks support site. For information on how to configure zone-defined address books, see the Junos OS Release 11.1 documentation.

NOTE: Before running the downgrade script, make sure to revert any configuration that uses addresses from the global address book.

Figure 1: Upgrade and Downgrade Scripts for Address Books



Running Upgrade and Downgrade Scripts

The following restrictions apply to the address book upgrade and downgrade scripts:

- The scripts cannot run unless the configuration on your system has been committed. Thus, if the zone-defined address book and zone-attached address book configurations are present on your system at the same time, the scripts will not run.
- The scripts cannot run when the global address book exists on your system.

- If you upgrade your device to Junos OS Release 12.1 and configure logical systems, the master logical system retains any previously configured zone-defined address book configuration. The master administrator can run the address book upgrade script to convert the existing zone-defined configuration to the zone-attached configuration. The upgrade script converts all zone-defined configurations in the master logical system and user logical systems.

  NOTE: You cannot run the downgrade script on logical systems.

For information about implementing and executing Junos operation scripts, see the *Junos OS Configuration and Operations Automation Guide*.

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

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

You can upgrade or downgrade to the EEOL release that occurs directly before or after the currently installed EEOL release, or to two EEOL releases before or after. For example, Junos OS Release 12.3X48 is an EEOL release. You can upgrade from Junos OS Release 12.1X46 to Release 12.3X48 or even from Junos OS Release 12.3X48 to Release 15.1X49-D10. For upgrading from Junos OS Release 12.1X47-D15 to Junos OS Release 15.1X49-D10, ISSU is supported. However, you cannot upgrade directly from a non-EEOL release that is more than three releases ahead or behind.

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

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

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

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

Related Documentation

- New and Changed Features on page 4
- Changes in Behavior and Syntax on page 5
- Known Behavior on page 10
- Known Issues on page 15
- Resolved Issues on page 19

Product Compatibility

This section lists the product compatibility for any Junos SRX mainline or maintenance release.

Hardware Compatibility

To obtain information about the components that are supported on the device, and special compatibility guidelines with the release, see the SRX Series Hardware Guide.

To determine the features supported on SRX Series devices in this release, use the Juniper Networks Feature Explorer, a Web-based application that helps you to explore and compare Junos OS feature information to find the right software release and hardware platform for your network. Find Feature Explorer at http://pathfinder.juniper.net/feature-explorer/.

Transceiver Compatibility for SRX Series Devices

We strongly recommend that only transceivers provided by Juniper Networks be used on SRX Series interface modules. Different transceiver types (long-range, short-range, copper, and others) can be used together on multiport SFP interface modules as long as they are provided by Juniper Networks. We cannot guarantee that the interface module will operate correctly if third-party transceivers are used.

Please contact Juniper Networks for the correct transceiver part number for your device.

Finding More Information

For the latest, most complete information about known and resolved issues with the Junos OS, see the Juniper Networks Problem Report Search application at http://prsearch.juniper.net.

For regulatory compliance information about Common Criteria, FIPS, Homologation, RoHS2, and USGv6 for Juniper Networks products, see the Juniper Networks Compliance Advisor.

Juniper Networks Feature Explorer is a Web-based application that helps you to explore and compare Junos OS feature information to find the correct software release and hardware platform for your network. Find Feature Explorer at http://pathfinder.juniper.net/feature-explorer/.

Juniper Networks Content Explorer is a Web-based application that helps you explore Juniper Networks technical documentation by product, task, and software release, and download documentation in PDF format. Find Content Explorer at http://www.juniper.net/techpubs/content-applications/content-explorer/.

Documentation Feedback

We encourage you to provide feedback, comments, and suggestions so that we can improve the documentation. You can send your comments to techpubs-comments@juniper.net, or fill out the documentation feedback form at https://www.juniper.net/cgi-bin/docbugreport/. If you are using e-mail, be sure to include the following information with your comments:

- Document or topic name
- URL or page number
- Software release version (if applicable)

Requesting Technical Support

Technical product support is available through the Juniper Networks Technical Assistance Center (JTAC). If you are a customer with an active J-Care or JNASC 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.

Technical product support is available through the Juniper Networks Technical Assistance Center (JTAC). If you are a customer with an active J-Care or Partner Support Service 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 http://www.juniper.net/us/en/local/pdf/resource-guides/7100059-en.pdf.
- Product warranties—For product warranty information, visit http://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: http://www.juniper.net/customers/support/
- Search for known bugs: http://www2.juniper.net/kb/
- Find product documentation: http://www.juniper.net/techpubs/
- Find solutions and answer questions using our Knowledge Base: http://kb.juniper.net/
- Download the latest versions of software and review release notes: http://www.juniper.net/customers/csc/software/

- Search technical bulletins for relevant hardware and software notifications: http://kb.juniper.net/InfoCenter/
- Join and participate in the Juniper Networks Community Forum: http://www.juniper.net/company/communities/
- Open a case online in the CSC Case Management tool: http://www.juniper.net/cm/

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

Opening a Case with JTAC

You can open a case with JTAC on the Web or by telephone.

- Use the Case Management tool in the CSC at http://www.juniper.net/cm/.
- 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, visit us at http://www.juniper.net/support/requesting-support.html.

If you are reporting a hardware or software problem, issue the following command from the CLI before contacting support:

```
user@host> request support information | save filename
```

To provide a core file to Juniper Networks for analysis, compress the file with the **gzip** utility, rename the file to include your company name, and copy it to **ftp.juniper.net/pub/incoming**. Then send the filename, along with software version information (the output of the **show version** command) and the configuration, to **support@juniper.net**. For documentation issues, fill out the bug report form located at http://www.juniper.net/techpubs/feedback/.

Revision History

28, November 2017—Revision 4— Junos OS 15.1X49-D90 – SRX Series.

29, June 2017—Revision 3— Junos OS 15.1X49-D90 – SRX Series.

23, May 2017—Revision 2— Junos OS 15.1X49-D90 – SRX Series.

27, April 2017—Revision 1— Junos OS 15.1X49-D90 – SRX Series.