Release Notes: Junos® OS Release 15.1X49-D40 for the SRX Series

Release 15.1X49-D40
15 November 2016
Revision 14

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-D40 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-D40 supports SRX300, SRX320, SRX340, SRX345, SRX550 High Memory (SRX550M), SRX1500, vSRX, and 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).

Junos OS Release 15.1X49-D40 does not support SRX5400, SRX5600, or SRX5800 devices with the following cards:

- SRX5K-40GE-SFP I/O Card (IOC1)
- SRX5K-4XGE-XFP I/O Card (IOC1)
- SRX5K-FPC-IOC Flex I/O card (Flex IOC1)
- SRX5K-RE-13-20 Routing Engine (RE1)
- SRX5K-SCB Switch Control Board (SCB1)
- SRX5K-SPC-2-10-40 Services Processing Card (SPC1)

Junos OS Release 15.1X49-D40 does not support SRX1400, SRX3400, or SRX3600 devices.

Junos OS Release 15.1X49-D40 does not support SRX Series devices SRX100 through SRX650.

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-D40 for the SRX Series devices.

Release 15.1X49-D40 Software Features

Application Layer Gateways (ALGs)

- **TCP support for SIP ALG on SRX Series devices and vSRX instances**— Starting with Junos OS Release 15.1X49-D40, the SIP ALG supports TCP along with UDP. The TCP support reduces traffic to the server by eliminating the need to reregister or refresh the server frequently.

  [See Understanding the SIP ALG.]

AppSecure

- **AppQoS rate-limiting support on SRX5000 line devices with IOC2 and IOC3** —Starting with Junos OS Release 15.1X49-D40, the SRX5K-MPC (IOC2), the SRX5K-MPC3-100G10G (IOC3), and the SRX5K-MPC3-40G10G (IOC3) support AppQoS rate-limiting functionality.

  The rate-limiting functionality helps maintain a consistent level of throughput and packet loss sensitivity for different classes of traffic. AppQoS implements rate limiting on all egress PICs on the device. The rate-limiting configuration consists of two parameters, **bandwidth-limit** and **burst-size-limit**. The **bandwidth-limit** option defines the maximum number of kilobits per second that can traverse the port. The **burst-size-limit** option defines the maximum number of bytes that can traverse the port in a single burst. The **burst-size-limit** option reduces starvation of lower-priority traffic by ensuring a finite size for each burst.

  [See Understanding Application QoS (AppQoS).]

- **Custom application signatures**—Starting with Junos OS Release 15.1X49-D40, application identification supports custom (user-defined) application signatures for SRX Series devices and vSRX. Custom application signatures are unique to your environment and are not part of the predefined application package.

  Custom application signatures are required to bring visibility for unknown or unclassified applications, to identify applications over Layer 7 and transiting or temporary applications, and to achieve further granularity of known applications.

  SRX Series devices support the following types of custom signatures:

  - ICMP-based
  - IP protocol-based
  - Address-based
  - Layer 7-based

You can create custom application signatures using the CLI by specifying a name, a protocol (as applicable), the port where the application runs (as applicable), and the match criteria.

[See Understanding Junos OS Application Identification Custom Application Signatures.]

- **SSL Forward Proxy with Intel QuickAssist Technology (QAT) cryptography support for SRX1500 devices**—Starting with Junos OS Release 15.1X49-D40, hardware-based SSL acceleration capabilities are supported on SRX1500 devices to improve overall performance.

  The following functions are optimized with this enhancement:

  - Symmetric cryptography, which includes bulk cipher operations
  - Public Key (asymmetric) cryptography, which includes RSA operations.

  [See Configuring SSL Proxy.]

Authentication, Authorization and Accounting (AAA)

- **HTTPS support for firewall authentication and Web authentication**—Starting from Junos OS Release 15.1X49-D40, this feature is supported on SRX300, SRX320, SRX340, SRX345, SRX550M, and SRX1500 Services Gateways.

  Firewall authentication now supports the HTTPS protocol along with FTP, HTTP, and Telnet. This feature enhances HTTPS support for Web authentication. Unauthenticated HTTPS traffic is redirected to the Web authentication IP addresses of the incoming interfaces.

  HTTPS is the secure version of HTTP, the protocol over which data is sent between the user and the device that the user is connected to. All communications between the user and the connected devices are encrypted. HTTPS is often used to protect highly confidential online transactions like online banking and online shopping order forms.

  The following new CLI statements are part of this feature:

  - **ssl-termination-profile**—Specify the name of the SSL termination profile used for SSL offloading.
  - **web-redirect-to-https**—Redirect unauthenticated HTTP requests to the device's internal HTTPS webserver. If **web-redirect-to-https** is configured, the firewall redirects the unauthenticated HTTP traffic to the HTTPS Web authentication server's incoming interface .
  - **https**—Enable authentication through HTTPS. If **https** is selected, the system allows Web authentication for HTTPS traffic.
  - **redirect-to-https**—Redirect the HTTP Web authentication traffic to the HTTPS Web authentication service.

[See Firewall User Authentication Overview.]

Class of Service (CoS)

- **Support for logical interface policer on SRX Series devices and vSRX instances**—Starting with Junos OS Release 15.1X49-D40, the logical interface policer, also called an aggregate policer, is supported on all SRX Series devices and vSRX instances. The logical interface policer is a two-color or three-color policer that defines traffic rate limiting. You can apply a policer to input or output traffic for multiple protocol families on the same logical interface without needing to create multiple instances of the policer.

  To configure a single-rate two-color logical interface policer, include the **logical-interface-policer** statement at the **[edit firewall policer policer-name]** hierarchy level.

  To display a logical interface policer on a particular interface, issue the **show interfaces policers** operational mode command.

  [See Logical Interface (Aggregate) Policer Overview, Two-Color Policer Configuration Overview, and Example: Configuring a Two-Color Logical Interface (Aggregate) Policer.]

Flow and Processing

- **Central point architecture enhancements for flow supporting GTP/SCTP**—Starting in Junos OS Release 15.1X49-D40, the central point architecture is enhanced to fix the following issues:

  - To address GTP-C message rate-limiting to protect GGSN from GTP-C message flood.
  - To prevent GTP-C packet drop issues during SGSN handover.
  - To load-balance the GTP-U traffic handled by a GGSN and SGSN pair by distributing the traffic on all SPUs using the tunnel endpoint identifier (TEID)-based hash distribution. Use the **enable-gtpu-distribution** command to enable GTP-U session distribution.
  - To support even distribution of SCTP traffic association to load-balance the SCTP association distribution issue and to enhance SCTP data throughput. This is achieved by distributing SCTP traffic evenly across all SPUs.

  [See Understanding Central Point Architecture Flow Support for GTP and SCTP.]

- **Express Path support on SRX5000 line devices with IOC2 and IOC3 for IPv6**—Starting with Junos OS Release 15.1X49-D40, the SRX5K-MPC (IOC2), the SRX5K-MPC3-100G10G (IOC3), and the SRX5K-MPC3-40G10G (IOC3) support Express Path (formerly known as *services offloading*) for IPv6 traffic.

  Express Path is a mechanism for processing fast-path packets in the Trio chipset instead of in the SPU. This method reduces the long packet-processing latency that arises when packets are forwarded from network processors to SPUs for processing and back to IOCs for transmission. This method reduces the packet-processing latency that arises when packets are forwarded from network processors to SPUs for processing and back to IOCs for transmission.

[See Express Path Overview.]

- **LAG and LACP support on SRX5000 line devices with IOCs**—Starting with Junos OS Release 15.1X49-D40, the SRX5K-MPC (IOC2), the SRX5K-MPC3-100G10G (IOC3), and the SRX5K-MPC3-40G10G (IOC3) support LAG and LACP in Express Path mode.

  IEEE 802.3ad link aggregation enables you to group Ethernet interfaces to form a single, aggregated Ethernet interface, also known as a LAG or bundle. LAGs provide increased interface bandwidth and link availability by linking physical ports and load-balancing traffic crossing the combined interface. LACP provides a standardized means for exchanging information between partner (remote or far-end of the link) systems on a link.

  With this feature, you can configure LAG on an SRX Series device using the links from an IOC2 or an IOC3 in Express Path mode.

  [See LAG and LACP Support on SRX5000 Line Devices with I/O Cards (IOCs).]

- **Session limit performance enhancement on central point**—Starting in Junos OS Release 15.1X49-D40, the session limit on the central point can now support 1.6 million connections per second (cps) on SRX5000 line devices with 10 SPCs.

  The central point updates the session limit counter when the session ages out. Every session age out triggers a central point delete message and many such delete messages consume more time. The central point session limit performance is enhanced by replacing the central point delete message with specific screen report message and hence, saving the central point memory capacity.

  [See Understanding Central Point Session Limit Performance Enhancements.]

General Packet Radio Service (GPRS)

- **Central point architecture support for GTP**—Starting in Junos OS Release 15.1X49-D40, the central point architecture is enhanced to address the GTP-C message rate-limiting to protect GGSN from GTP-C message flood and to distribute GTP-U traffic handled by a GGSN and SGSN pair on all SPUs by switching to tunnel endpoint identifier (TEID)-based hash distribution.

  Previously, the GTP ALG used to drop incoming GTP-C packets if the GGSN or SGSN direction was not determined. Now, to prevent GTP-C packets from being dropped, a new flow session is created and the GTP-C traffic is allowed to pass even if the GGSN or SGSN direction is not determined. Later, the GGSN IP can be determined using the correct SPU to create the flow session, and the session must be migrated to the designated SPU.

  [See Understanding Central Point Architecture Support for GTP.]

- **Central point architecture support for SCTP**—Starting in Junos OS Release 15.1X49-D40, the central point architecture supports even distribution of SCTP traffic association to load-balance the SCTP association distribution issue and to enhance SCTP data throughput. This is achieved by distributing SCTP traffic evenly across all SPUs.

Currently, all sessions of a given SCTP association are hashed to the same SPU by the fixed per-association SCTP port pair. However, in some cases multiple SCTP associations share the same port pair, resulting in all SPU traffic being handled by one SPU. Now, a tag-based hash distribution is used to ensure even distribution of SCTP traffic from different SCTP associations among all SPUs.

[See Understanding Central Point Architecture Support for SCTP.]

- **GTP handover messages support for SRX5000 line**—Starting with Junos OS Release 15.1X49-D40, GTP handover messages are supported for the SRX5000 line of Services Gateways. During a handover procedure, SGSN context messages (request/response/acknowledge) or forward relocation messages, referred as handover messages, are sent between the new and the old MME/SGSN. PDP context information, acquired from handover messages, is set up on SRX Series devices when these messages are received. Subsequently, the GTP messages can be normally inspected according to the new PDP context.

  The following key features are supported:

  - Inter-MME/SGSN handover messages inspection
  - GTP PDP context/forwarding tunnel setup according to the information in handover messages
  - GTP-U inspection for forwarding data traffic
  - Support for PDP context update by updating or modifying messages with different versions
  - System log and counter for handover messages

  NOTE: **Handover between different GTP versions is supported.**

Layer 2 Features

- **LACP support in Layer 2 transparent mode for SRX5400, SRX5600, and SRX5800 devices**—Starting with Junos OS Release 15.1X49-D40, LACP is supported in Layer 2 transparent mode in addition to existing support in Layer 3 mode.

  When the SRX Series device uses LACP to bundle the member links, it creates high-speed connections, also known as *fat pipe*, with peer systems. Bandwidth can be increased by adding member links. Increased bandwidth is especially important for redundant Ethernet (reth) and aggregated Ethernet (ae) interfaces. LACP also provides automatic determination, configuration, and monitoring member links.

  LACP is compatible with other peers that run the 802.3ad LACP protocol. It automatically binds member links without manually configuring the LAG, thereby avoiding errors.

NOTE: Tentative sessions are created for all interfaces in a particular VLAN. If there is plenty of one-way traffic, numerous tentative sessions are created. When sessions reach the maximum limit, vector fails and packet loss might be seen.

- **Support for enhanced Layer 2 transparent bridge mode and switching mode**—Starting with Junos OS Release 15.1X49-D40, the enhanced Layer 2 transparent bridge mode and switching mode features are supported on SRX300, SRX320, SRX340, SRX345, and SRX550M devices.

  Use the **set protocols l2-learning global-mode (transparent-bridge | switching)** command to switch between the Layer 2 transparent bridge mode and switching mode. After switching the mode, you must reboot the device for the configuration to take effect.

  The layer 2 protocols supported in switching mode is Link Aggregation Control Protocol (LACP).

  NOTE:
  - LACP is not supported on SRX300 and SRX320 devices.
  - LACP is not supported in transparent bridge mode.

  You can now configure Layer 2 mode on redundant Ethernet interface. Use the following commands to define a redundant Ethernet interface:

  - **set interfaces *interface-name* ether-options redundant-parent *reth-interface-name***
  - **set interfaces *reth-interface-name* redundant-ether-options redundancy-group *number***

  [See global-mode (Protocols), and Layer 2 Bridging and Switching Overview.]

Multicast

- **IGMP Policy Behavior for Multicast Traffic on SRX Series devices**—Starting with Junos OS Release 15.1X49-D40, PIM policies on SRX Series devices are enhanced to remove the special policies configuration that used port number 2/2 to allow PIM protocol messages to pass through an SRX Series device that was acting as an intermediate router. The benefit of this enhancement is that, if attackers send multicast UDP packets using port pair 2/2, the packets no longer pass through the SRX Series device. You must now use the real port number in the packets to create a PIM data session and make sure that multicast flow works properly.

  Run the following commands to create the PIM data session at real port number along with the normal PIM configuration:

  set applications application PIM protocol pim

  set applications application MULTICAST_APP protocol udp

  set applications application MULTICAST_APP destination-port 5000-8000

  NOTE: The port number range is 5000-8000.

  Multicast Feature Guide for Security Devices

Network Address Translation (NAT)

- **IPv6-to-IPv6 Network Address Translation** —Starting in Junos OS Release 15.1X49-D40, stateless IPv6-to-IPv6 network prefix translation, which is compliant with RFC 6296, is provided for SRX300, SRX320, SRX345, SRX550M, and SRX1500 Series devices, and vSRX instances. This feature enables address independence and provides a one-to-one relationship between IPv6 addresses in an internal network and IPv6 addresses in an external network. This type of translation can be used to secure proprietary information, for example, by a mobile service provider using customers' phone numbers as IPv6 local host identifiers.

  [See IPv6 NAT Overview.]

Public Key Infrastructure

- **CMPv2 certificate enrollment protocol for vSRX instances and SRX300, SRX320, SRX340, SRX345, SRX550M, SRX1500, SRX5400, SRX5600, and SRX5800 devices** — Starting in Junos OS Release 15.1X49-D40, Certificate Management Protocol version 2 (CMPv2) can be used for certificate enrollment and reenrollment. CMPv2 supports RSA, DSA, and ECDSA certificates and is based on RFC 4210, *Internet X.509 Public Key Infrastructure Certificate Management Protocol (CMP)* and RFC 4211, *Internet X.509 Public Key Infrastructure Certificate Request Message Format*. Based on your deployment environment, you can use either Simple Certificate Enrollment Protocol (SCEP) or CMPv2 for certificate enrollment and reenrollment.

  [See Understanding Certificates and PKI.]

Sky Advanced Threat Prevention

- **Support for SRX1500 devices** —Junos OS Release 15.1X49-D40 and later releases support Sky Advanced Threat Prevention running on the SRX1500 device.

  [See Sky Advanced Threat Prevention Supported Platforms Guide]

- **Policy and statistic CLI** —Starting with Junos OS Release 15.1X49-D40, you can use CLI commands to configure Sky Advanced Threat Prevention policies, view Sky Advanced Threat Prevention statistics and status, and set trace options.

  [See Sky Advanced Threat Prevention CLI Reference Guide]

System Logging

- **Stream log based on category for SRX300, SRX320, SRX340, SRX345, SRX550M, and SRX1500 Series devices, and vSRX instances** —Starting with Junos OS Release 15.1X49-D40, when forwarding logs using stream mode, all the categories can be configured for sending specific category logs to different log servers. For stream mode log forwarding, the transport protocol used between Packet Forwarding Engine and the log server can be UDP, TCP, or TLS, and it is configurable. The transport protocol used between the Routing Engine and the log server can only be UDP.

  [See Understanding System Logging for Security Devices]

Unified Threat Management (UTM)

- **Enhanced Web Filtering (EWF) and Sophos Antivirus over SSL forward proxy support HTTPS traffic for SRX340, SRX345, SRX5400, SRX5600, and SRX5800 devices and vSRX instances**—Starting with Junos OS Release 15.1X49-D40, UTM EWF and Sophos Antivirus over SSL forward proxy support HTTPS traffic by intercepting HTTPS traffic passing through the SRX Series devices and vSRX instances. The security channel from the device is divided into one SSL channel between the client and the device and another SSL channel between the device and the HTTPS server. SSL forward proxy acts as the terminal for both channels and forwards the cleartext traffic to UTM. UTM extracts the URL and the file checksum information from the cleartext traffic. The Sophos Antivirus scanner determines whether to block or permit the requests.

  [See Enhanced Web Filtering Overview and Example: Configuring Sophos Antivirus Scanner with SSL Forward Proxy.]

Virtual Private Networks (VPNs)

- **Group VPNv2 servers and members supported on SRX300, SRX320, SRX340, SRX345, and SRX550M devices**— Junos OS Release 15.1X49-D40 provides Group VPNv2 server and members that are compliant with RFC 6407, *The Group Domain of Interpretation (GDOI)*. Group VPNv2 server clusters provide group controller/key server (GCKS) redundancy and scaling for compatible Group VPN members.

  Group VPNv2 is an enhanced version of the group VPN feature supported on SRX100, SRX110, SRX210, SRX220, SRX240, SRX550, and SRX650 devices. Group VPNv2 servers and members do not interoperate with group VPN servers and members on these devices.

[See Group VPNv2 Overview.]

- **IKEv2 AES-GCM for SRX300, SRX320, SRX340, and SRX345 devices and SRX5400, SRX5600, and SRX5800 devices with SPC2 (SRX5K-SPC-4-14-320)** — Starting in Junos OS Release 15.1X49-D40, support is provided for Protocol Requirements for IP Modular Encryption (PRIME), an IPsec profile defined for public sector networks in the United Kingdom. PRIME uses AES-GCM rather than AES-CBC for IKEv2 negotiations. Both PRIME-128 and PRIME-256 cryptographic suites are supported.

  The following options are available:

  - The **encryption-algorithm** options **aes-128-gcm** and **aes-256-gcm** are available for proposals configured at the [**edit security ike proposal** ***proposal-name***] hierarchy level.
  - Predefined proposals **prime-128** and **prime-256** are available at the [**edit security ike policy** ***policy-name*** **proposal-set**] and [**edit security ipsec policy** ***policy-name*** **proposal-set**] hierarchy levels.

  [See Understanding Suite B and PRIME Cryptographic Suites.]

- **Auto Discovery VPN (ADVPN) suggester and partners supported on vSRX instances and SRX1500, SRX5400, SRX5600, and SRX5800 devices** — Starting in Junos OS Release 15.1X49-D40, vSRX instances and SRX1500, SRX5400, SRX5600, and SRX5800 devices can be configured as ADVPN suggesters or partners.

  NOTE: BGP and OSPF dynamic routing protocols are supported with AutoVPN. Only OSPF is supported with ADVPN.

  [See Understanding Auto Discovery VPN.]

Related Documentation

- Changes in Behavior and Syntax on page 13
- Known Behavior on page 17
- Known Issues on page 22
- Resolved Issues on page 24
- Migration, Upgrade, and Downgrade Instructions on page 28

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.

AppSecure

- On SRX Series devices, the following CLI statements are deprecated—rather than immediately removed—to provide backward compatibility and a chance to bring your configuration into compliance with the new configuration:

  edit services ssl termination profile ***profile-name*** **protocol-version ssl3**

edit services ssl initiation profile *profile-name* protocol-version ssl3

- On SRX300, SRX320, SRX340, and SRX345 devices, AppSecure is part of Juniper Networks Secure Edge software or IPS subscription license. A separate license key is not required on your device to download and install the AppID signature database updates, or to use other AppSecure features such as AppFW, AppQoS, and AppTrack.

Authentication, Authorization and Accounting (AAA)

- On SRX340 and SRX345 devices, the factory-default configuration has a generic HTTP configuration. To use **ge** and **fxp0** ports as management ports, you must use the **set system services web-management http** command. The Web management HTTP and HTTPS interfaces are changed to fxp0.0 and from **ge-0/0/1.0** through **ge-0/0/7.0**.

Chassis Cluster

- When an SRX Series device is operating in chassis cluster mode and encounters any IA-chip access issue in an SPC or an I/O Card (IOC), a minor FPC alarm will be activated to trigger redundancy group failover.
- Starting in Junos OS Release 15.1X49-D20, for all SRX Series devices, reth interface supports proxy ARP.

Interfaces and Routing

- **GRE keepalive time feature for SRX Series devices**—Starting in Junos OS Release 15.1X49-D30, the GRE keepalive time feature is supported on the GRE tunnel interface. You can configure the keepalives on a GRE tunnel interface using the **keepalive-time** and **hold-time** commands at the [**edit protocols oam gre-tunnel interface interface-name**] hierarchy level.

Layer 2 Features

- **Enhanced Layer 2 CLI**—Starting with Junos OS Release 15.1X49-D10, enhanced Layer 2 CLI configurations are supported on SRX5400, SRX5600, and SRX5800 devices. Legacy Layer 2 transparent mode configuration statements and operational commands are not supported. If you enter legacy configurations in the CLI, the system displays an error and fails to commit the configurations.

  For example, the following configurations are no longer supported:

  - **set bridge-domain**
  - **set interfaces ge-1/0/0 unit 0 family bridge**
  - **set vlans vlan-1 routing-interface**

  Use the SRX L2 Conversion Tool to convert Layer 2 CLI configurations to enhanced Layer 2 CLI configurations.

  The SRX L2 Conversion Tool is available at http://www.juniper.net/support/downloads/?p=srx5400#sw .

  For more information, refer to the Knowledge Base article at http://kb.juniper.net .

[See Enhanced Layer 2 CLI Configuration Statement and Command Changes.]

Multicast

- Starting with Junos OS Release 15.1X49-D40, for all SRX Series devices, configuration of patterns in standard PCRE format is supported in the custom attacks.

NAT

- Source NAT pool port configuration options—Starting with Junos OS Release 15.1X49-D40, the **port-overloading-factor** option and the **port-range** option at the [edit security nat source pool *source-pool-name* port] hierarchy level can be configured together. Prior to Release 15.1X49-D40, the options would overwrite each other.

  [See *port (Security Source NAT)*]

Network Time Protocol

- Starting in Junos OS Release 15.1X49-D10, on all SRX Series devices, when the NTP client or server is enabled in the [**edit system ntp**] hierarchy, the REQ_MON_GETLIST and REQ_MON_GETLIST_1 control messages supported by the monlist feature within the NTP client or server might allow remote attackers, causing a denial of service. To identify the attack, apply a firewall filter and configure the router's loopback address to allow only trusted addresses and networks.

Public Key Infrastructure

- 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.

Screen

- In Junos OS releases earlier than Junos OS Release 15.1X49-D20, the firewall generates a log for every packet that exceeds the source-ip-based or destination-ip-based threshold and triggers the source or destination session limit. This can lead to a flood of logs if a large number of packets is received every second after the threshold has been reached. For example, if the source or destination session limit has been reached and 100 additional packets arrive in the next second, 100 log messages are sent to the system log server.

  Starting in Junos OS Release 15.1X49-D20, the firewall generates only one log message every second irrespective of the number of packets that trigger the source or destination session limit.

  This behavior also applies to flood protection screens with TCP-Synflood-src-based, TCP-Synflood-dst-based, and UDP flood protection.

System Logs

- In Junos OS Release 15.1X49-D30 and earlier, the severity parameter for RT_SRC_NAT_PBA messages was “debug”.

  Starting in Junos OS Release 15.1X49-D40, the severity parameter has changed. The RT_SRC_NAT_PBA messages are now fixed with severity as “info”.

  The following example shows RT_SRC_NAT_PBA messages before Junos OS Release 15.1X49-D40:

  16:32:43.760393 In IP (tos 0x0, ttl 254, id 16957, offset 0, flags [none], proto: UDP (17), length: 218) 192.0.2.4.syslog > 192.0.2.2.syslog: SYSLOG, length: 190 Facility user (1), Severity debug (7)

  Feb 5 16:32:49 RT_NAT: RT_SRC_NAT_PBA_ALLOC: Subscriber 192.0.2.2 used/maximum [1/32] blocks, allocates port block [27200-27263] from 198.51.100.3 in source pool src-nat-pool-1 lsys_id: 0\012

  The following example shows RT_SRC_NAT_PBA messages in Junos OS Release 15.1X49-D40, indicating the change in the severity parameter:

  16:32:43.760393 In IP (tos 0x0, ttl 254, id 16957, offset 0, flags [none], proto: UDP (17), length: 218) 192.0.2.4.syslog > 192.0.2.2.syslog: SYSLOG, length: 190 Facility user (1), Severity info (6)

  Feb 5 16:32:49 RT_NAT: RT_SRC_NAT_PBA_ALLOC: Subscriber 192.0.2.2 used/maximum [1/32] blocks, allocates port block [27200-27263] from 198.51.100.3 in source pool src-nat-pool-1 lsys_id: 0\012

System Management

- During a load override, to enhance the memory for the commit script, you must load the configuration by applying the following commands before the commit step:
  set system scripts commit max-datasize 800000000
  set system scripts op max-datasize 800000000

- On all SRX Series devices in transparent mode, packet flooding is enabled by default. If you have manually disabled packet flooding with the **set security flow bridge**

no-packet-flooding command, then multicast packets such as OSPFv3 hello packets are dropped.

User Interface and Configuration

- You can configure only one rewrite rule for one logical interface. When you configure multiple rewrite rules for one logical interface, an error message is displayed and the commit fails.

VPNs

- Starting with Junos OS Release 15.1X49-D40, the **hmac-sha-256-96** option is deprecated at the [**edit security ipsec proposal *proposal-name* authentication-algorithm**] and [**edit security ipsec vpn *vpn-name* manual authentication algorithm**] hierarchy levels.
- Dynamic VPN is not supported in Junos OS 15.1X49 releases. Dynamic VPN is supported only in Junos OS Releases 12.3X48 and earlier on SRX100, SRX210, SRX220, SRX240, SRX550, and SRX650 devices.

Zones and Interfaces

- System services configuration option—Starting with Junos OS Release 15.1X49-D40, the **system-services** option at the **[edit security zones security-zone *zone-name* host-inbound-traffic]** hierarchy level and the **system-services** option at the **[edit security zones security-zone *zone-name* interfaces *interface-name* host-inbound-traffic]** hierarchy level no longer support the configuration of the Session Initiation protocol (SIP) system service.

  [See *system-services (Security Zones Interfaces)* and *system-services (Security Zones Host Inbound Traffic)*]

Related Documentation

- New and Changed Features on page 5
- Known Behavior on page 17
- Known Issues on page 22
- Resolved Issues on page 24
- Migration, Upgrade, and Downgrade Instructions on page 28

Known Behavior

This section contains the known behaviors, system maximums, and limitations in hardware and software in Junos OS Release 15.1X49-D40.

AppSecure

- On SRX Series devices, when you change the timeout value for the application system cache entries using the command **set services application-identification application-system-cache-timeout**, the cache entries need to be cleared to avoid inconsistency in timeout values of existing entries.

Attack Detection and Prevention (ADP)

- On all high-end SRX Series devices, the first path signature screen is performed first, followed by the fast path bad-inner-header screen.
- On all SRX Series devices, when a packet allow or drop session is established, the bad-inner-header screen is performed on every packet, because this screen is a fast path screen.

CLI

- On SRX5000 line devices, the following CLI statement is deprecated—rather than immediately removed—to provide backward compatibility and a chance to bring your configuration into compliance with the new configuration:

  set chassis fpc <*fpc-slot*> services offload

  The following new CLI statement replaces the deprecated CLI statement:

  set chassis fpc <*fpc-slot*> np-cache

Flow-based and Packet-based Processing

- On SRX Series devices, the default mode for processing traffic is flow mode. To configure an SRX Series device as a border router, you must change the mode from flow-based processing to packet-based processing. Use the **set security forwarding-options family mpls mode packet-based** statement to configure the SRX device to packet mode. You must reboot the device for the configuration to take effect.

General Packet Radio Service (GPRS)

- On SRX5000 line 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.

IP Monitoring

- On SRX5400, SRX5600, and SRX5800 devices, IP monitoring does not support MIC online/offline status.

Layer 2 Features

- **Layer 2 Bridging and Transparent Mode**— On all SRX Series devices, bridging and transparent mode are not supported on Mini-Physical Interface Modules (Mini-PIMs).
- In Junos OS Release 15.1X49-D40, the following features are not supported on SRX Series devices and vSRX instances:
  - Layer 2 transparent mode policer
  - Three-color policer

Network Address Translation (NAT)

- On high-end SRX Series devices, the number of IP addresses for NAT with port translation has been increased to 1M addresses since Junos OS Release 12.1X47-D10.

The SRX5000 line, however, supports a maximum of 384M translation ports and cannot be increased. To use 1M IP addresses, you must confirm that the port number is less than 384. The following CLI commands enable you to configure the twin port range and limit the twin port number:

- **set security nat source pool-default-twin-port-range *<low>* to *<high>***

- **set security nat source pool sp1 port range twin-port** *<low>* **to** *<high>*

Platform and Infrastructure

- On all high-end SRX Series devices, when you enable a global services offloading policy utilizing IOC2 line-cards, the connections per second (CPS) rate might be reduced. It is recommended to utilize IOC3 line-cards to maximize the CPS rate, or, alternatively, lower the session count to ensure that the IOC2 is capable of scaling. As a workaround, identify the sessions that must be off-loaded and only enable services off-loading on those sessions.

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, SRX550M, and SRX1500 devices do not support ISSU.

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.

  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

- On a high-end SRX Series device, VPN monitoring of an externally connected device (such as a PC) is not supported. The destination IP address for VPN monitoring must be a local interface on the high-end SRX Series device.
- On SRX Series devices, configuring RIP demand circuits over P2MP VPN interfaces is not supported.

Related Documentation

- New and Changed Features on page 5
- Changes in Behavior and Syntax on page 13
- Known Issues on page 22
- Resolved Issues on page 24
- Migration, Upgrade, and Downgrade Instructions on page 28

Known Issues

This section lists the known issues in hardware and software in Junos OS Release 15.1X49-D40.

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

Chassis Cluster

- On all SRX Series devices in a chassis cluster, when you simultaneously reboot both the nodes, the secondary node might come up in the ineligible state. After all line cards of the primary node are online, the fabric recovery procedure changes the secondary node from ineligible to the normal secondary state. PR1104249
- On SRX1500 devices in a chassis cluster with Sky Advanced Threat Prevention (ATP) solution deployed, if you disable and then reenable CRL checking of certificate validity, the system does not reenable CRL checking.

  As a workaround, reboot the SRX1500 device to reenable CRL checking. PR1144280
- On all branch SRX Series devices, chassis cluster with Layer 2 switching mode configurations does not work. PR1161372

Flow and Processing

- On all branch SRX Series devices, traffic does not pass with the maximum number of Interface Logicals (IFLs) 8 queues. PR1138997
- On all high-end SRX Series devices, due to SRX5K-MPC (IOC2) lookup, the hardware engine counts one extra packet for each session wing installed in the SRX5K-MPC (IOC2) Express Path. The packet counters in CLI for Express Path sessions from the SRX5K-MPC (IOC2) are always up by 1 compared to the SRX5K-MPC3-100G10G (IOC3), for the same Express Path scenario. PR1157158
- On all SRX Series devices, for some designed traffic, session limit SPU entries from the same source IP address do not distribute among all SPUs evenly. Some central point session limit entries might leak, which might lead to an inaccurate session limit. PR1161277
- On SRX300 and SRX320 devices, LACP is not supported. PR1165015

IDP

- On all SRX Series devices, when Sky Advanced Threat Protection (ATP) inline blocking and IDP are configured together in the same security policy, Sky ATP inline blocking is not supported, but files are still submitted to the cloud for scanning. In this scenario IDP functionality is not affected, and IDP functions normally. PR1144843

Interfaces

- On SRX1500 devices, when 1G SFP-T is used on the 1G SFP ports (ge-0/0/12 to ge-0/0/15), it does not come up at 100M speed. PR1133384
- On SRX300, SRX320, SRX340, and SRX345 devices, when you change the interface mode from 10m/no-auto-10m/no-auto to 100m/no-auto-100m/no-auto, interfaces might be down on both the sides.

  As a workaround, delete the configuration on the interface and reconfigure the 100m/no-auto interface mode. PR1165942

J-Web

- On all SRX Series devices in chassis cluster, if you want to use J-Web to configure and commit some of the configurations, you must ensure that all other user sessions are logged out including any CLI sessions. Otherwise, the configurations might fail.

  As a workaround, run the **request system logout terminal <tty> user <all>** command. PR1140019

Layer 2 Features

- On branch SRX Series devices in chassis cluster, enhanced Layer 2 does not fully support VPLS. When the logical interface is up or down, some message handlers related to Layer 2 might be triggered, which attempt to process VPLS-related route changes. As VPLS is not fully supported in Layer 2, this might cause an assertion failure. PR1167439
- On branch SRX Series devices, enhanced Layer 2 CLI configurations such as, **input-traffic-control-profile**, **output-traffic-control-profile**, **scheduler-map**, and **shaping-rate** cannot be configured on the IRB interfaces. Therefore, traffic controlling and traffic shaping is not supported on IRB interfaces. PR1170472

Unified Threat Management (UTM)

- On all high-end SRX Series devices, under high connections per second (cps) and UTM Sophos antivirus traffic, the device might ramp up to 99 percent CPU usage because of a central lock of object cache memory allocation. There is no clear boundary, because the allocation race condition varies.

  As a workaround, reducing traffic cps might lower the high CPU usage. PR967739

VPNs

- On all SRX Series devices, on the hub side, the AutoVPN tunnel fails to come up if the establish-tunnel command is configured. PR1160948
- On all branch SRX Series devices, the IRB interface cannot be used as an external interface with IPsec VPN. PR1166714
- On high-end SRX Series devices, when upgrading from 15.1X49-D30 to 15.1X49-D35, 15.1X49-D40 and 15.1X49-D50 and from 15.1X49-D35, 15.1X49-D40 and 15.1X49-D50 to 15.1X49-D60 release, the ISSU breaks for all VPN configuration. PR1201955

Related Documentation

- New and Changed Features on page 5
- Changes in Behavior and Syntax on page 13
- Known Behavior on page 17
- Resolved Issues on page 24
- Migration, Upgrade, and Downgrade Instructions on page 28

Resolved Issues

This section lists the issues fixed in hardware and software in Junos OS Release 15.1X49-D40.

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 all SRX Series devices with MS-RPC ALG enabled, in heavy MS-RPC traffic environment, ALG traffic might fail because of the ASL groups being used up. PR1120757

Chassis Cluster

- On all SRX Series devices in chassis clusters, when you configure the MAC address on the reth interface using the **set interfaces reth* mac *** command, all reth member interfaces use the manually specified MAC address. When you use the **deactivate interfaces reth* mac** command, the reth interface will change to the default MAC address, but the reth member interfaces will remain in the manually specified MAC address. This scenario causes traffic issues on the reth interface. PR1115275

CLI

- On SRX5400, SRX5600, and SRX5800 devices, ICMP Out Errors with a rate of 10,000 per second are generated when you issue the **show snmp mib get decimal 1.3.6.1.2.1.5.15.0** command. PR1063472
- On SRX1500 devices, when the dual power modules are plugged in, and one of them does not have power, the **show chassis hardware** command displays the wrong power module status. PR1138203

Class of Service (CoS)

- On all SRX Series devices, on all multithreads, when an interface is down, a timing issue occurs in which one thread releases the interface resource (because the interface is down) while another thread is attempting to access the interface. As a result, the flowd process crashes. PR1148796

Dynamic Host Configuration Protocol (DHCP)

- On SRX1500 devices, when the **show dhcpv6 client** command is issued, the CLI hangs after restarting the DHCP service with DHCPv6 clients. PR1142711
- On SRX1500 devices, when multiple interfaces end up having the same DUID-EN format for the DHCPv6 client interface, some interfaces might not receive the address information from the DHCP server. PR1142768
- On all branch SRX Series devices, the DHCPv4 server is not supported on the IRB interface in switching mode PR1166338

Flow-Based and Packet-Based Processing

- On all high-end SRX Series devices, traffic is dropped because the traffic flow skips source NAT before handling session-affinity for IPsec tunnel traffic. PR1137926
- On all SRX Series devices, IPv6 host-inbound traffic destined to xnm-ssl and xnm-clear-text services will be dropped even if xnm-ssl and xnm-clear-text are permitted in host-inbound-traffic. PR1147446

- On all SRX Series devices, using MS Windows as a client, when you download a large file using the SRX Series antivirus, the download speed might be suboptimal, because the client throttles the incoming flow by decreasing its TCP window size. PR1155228

General Routing

- On an SRX Series device configured as a DHCP server, the device will not send DHCP option 125 unless the DHCP client requests it. This behavior does not comply to the RFC definition. According to RFC 3925, the DHCP server should send option 125 without the client's request. PR1116940

Interfaces

- On SRX1500, SRX5400, SRX5600, and SRX5800 devices, in a redundant Ethernet (reth) interface that has two or more member interfaces on each node, when one of the member interfaces goes down, traffic might be incorrectly forwarded through the backup node. PR1131769

J-Web

- On all high-end SRX Series devices, in J-Web, configured content of the DHCP Monitor page is not visible as expected. PR1148026

Network Address Translation (NAT)

- On all high-end SRX Series devices, for a device running NAT traffic in high-stress conditions, continuous chassis cluster failover might result in a minor central point session leak. However, other than the wasted sessions caused by the leak, this issue has no other effects on the device. PR1141695
- On all high-end SRX Series devices when port-block allocation (PBA) NAT is configured, the last port-block might be released too early, without considering the configured active-block timeout value. PR1146288
- On all branch SRX Series devices, the Layer 3 VLAN interface does not support NAT, because the IRB interface cannot be used by NAT. PR1166334

Platform and Infrastructure

- On SRX5600 and SRX5800 devices with an SRX5K-RE-13-20 Routing Engine (RE1), in dual control link configuration, the secondary control link (em1) interface stays down when the Routing Engine installed in slot 1 is installed with Junos OS Release 12.1X47-D10 or later. PR1077999
- On SRX1500 devices, when one of the fans fail, the system generates a major alarm and a system log message is generated. However, the state LED and the alarm LED are both shown as OFF instead of red. PR1142191

- On all branch SRX Series devices, memory leaks on the mib2d process are seen during polling of SNMP OID .1.3.6.1.2.1.54.1 (SYSAPPLMIB). PR1144377
- On all SRX Series devices, when automatic installation is enabled using the **set system autoinstallation** command, unit 0 logical interface is configured for physical interfaces that are up. This might result in failure of CLI commands that do not allow unit 0 logical interface configuration. This issue might cause the interface-control (dcd) process to crash, resulting in improper installation of the interface-related configurations. PR1147657

Routing Policy and Firewall Filters

- On all SRX Series devices, the definition of the **alg** option (under a term of an application) and the **application-protocol** option (under an application) are separated. As a result, there is a difference in the application list under these two configuration hierarchies. PR895547
- On all high-end SRX Series devices, predefined application sets can only be invoked in the root logical system; they cannot be invoked in the custom logical system. PR1075409
- On all high-end SRX Series devices, when multiple address books containing DNS names are defined in multiple logical systems (LSYSs), and the address books are invoked in security policies, an issue might occur in which the DNS address update is correct in the DNS cache, but the DNS address is not updated in security policies. PR1132681

Services Applications

- On all high-end SRX Series devices, the name of the ICMP6 big packet is changed to junos-icmp6-packet-too-big instead of junos-icmp6-packet-to-big. PR917007

Unified Threat Management (UTM)

- On all SRX Series devices, the Enhanced Web Filtering (EWF) module is bypassed if the TCP session starts with a TCP SYN packet that has multiple flags turned on in its header (for example, SYN+ECN+CWR). PR1144200
- On all SRX Series devices, if a custom routing instance is used to connect the server of UTM Enhanced Web Filtering, when the server is configured using an IP address (**set security utm feature-profile web-filtering juniper-enhanced server host *.*.*.*)**, it will use the wrong routing instance to connect the server. When the server is configured using a URL, it might use the wrong routing instance to connect the server when the Web filtering configuration is changed. As a result, the connection fails. PR1159827

VPNs

- On all high-end SRX Series devices, when a lot of VPN tunnels are established (for example, 12,500 VPN tunnels on an SRX5400), committing VPN-related configurations might cause the VPN configuration to be out-of-sync between the Routing Engine and the SPUs. The issue is caused by intermittent IPC failure. PR1129473

- On all branch SRX Series devices acting as a hub-and-spoke, after system rebooting, some IPsec VPN tunnels might not be established. PR1132925
- On SRX5400, SRX5600, and SRX5800 devices configured in a chassis cluster with tunnels that use AES-GCM, failovers result in reestablishment of the tunnels. PR1153214

Related Documentation

- New and Changed Features on page 5
- Changes in Behavior and Syntax on page 13
- Known Behavior on page 17
- Known Issues on page 22
- Migration, Upgrade, and Downgrade Instructions on page 28

Documentation Updates

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

Unified Threat Management (UTM)

- Starting from Junos OS Release 15.1X49-D10, Kaspersky Antivirus, Express Antivirus, and Surf Control integrated features are not supported on all SRX Series devices and vSRX instances. These features are not supported from Junos OS release 15.1x49-D10 onwards. However, the *UTM Feature Guide for Security Devices* retains the content about the unsupported features.

Related Documentation

- New and Changed Features on page 5
- Changes in Behavior and Syntax on page 13
- Known Behavior on page 17
- Known Issues on page 22
- Resolved Issues on page 24
- Migration, Upgrade, and Downgrade Instructions on page 28

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

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 30).

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:

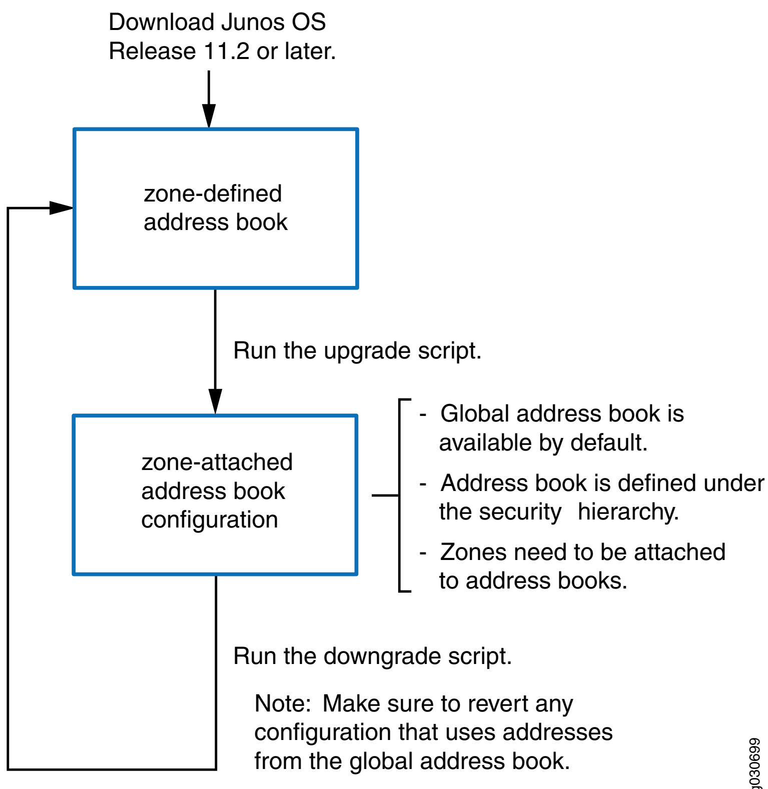
  - You cannot configure address books using the zone-defined address book configuration format; the CLI displays an error and fails to commit.
  - You cannot configure address books using the J-Web interface.

  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 Releases 12.1X44, 12.1X46, and 12.3X48 are EEOL releases. You can upgrade from Junos OS Release 12.1X44 to Release 12.1X46 or even from Junos OS Release 12.1X44 to Release 12.3X48. 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.

Related Documentation

- New and Changed Features on page 5
- Changes in Behavior and Syntax on page 13
- Known Behavior on page 17
- Known Issues on page 22
- Resolved Issues on page 24

Product Compatibility

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.

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 provide feedback by using either of the following methods:

- Online feedback rating system—On any page at the Juniper Networks Technical Documentation site at http://www.juniper.net/techpubs/index.html, simply click the stars to rate the content, and use the pop-up form to provide us with information about your experience. Alternately, you can use the online feedback form at http://www.juniper.net/techpubs/feedback/.
- E-mail—Send your comments to **techpubs-comments@juniper.net**. Include the document or topic name, URL or page number, and software version (if applicable).

Requesting Technical Support

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/customers/support/downloads/710059.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: https://www.juniper.net/alerts/
- 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 located at https://tools.juniper.net/SerialNumberEntitlementSearch/.

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.

Revision History

15, November 2016—Revision 14— Junos OS 15.1X49-D40 – SRX Series.

06, October 2016—Revision 13— Junos OS 15.1X49-D40 – SRX Series.

27, September 2016—Revision 12— Junos OS 15.1X49-D40 – SRX Series.

27, July 2016—Revision 11— Junos OS 15.1X49-D40 – SRX Series.

23, June 2016—Revision 10— Junos OS 15.1X49-D40 – SRX Series.

13, June 2016—Revision 9— Junos OS 15.1X49-D40 – SRX Series.

30, May 2016—Revision 8— Junos OS 15.1X49-D40 – SRX Series.

19, May 2016—Revision 7— Junos OS 15.1X49-D40 – SRX Series.

26, April 2016—Revision 6— Junos OS 15.1X49-D40 – SRX Series.

13, April 2016—Revision 5— Junos OS 15.1X49-D40 – SRX Series.

12, April 2016—Revision 4— Junos OS 15.1X49-D40 – SRX Series.

30, March 2016—Revision 3— Junos OS 15.1X49-D40 – SRX Series.

29, March 2016—Revision 2— Junos OS 15.1X49-D40 – SRX Series.

23, March 2016—Revision 1— Junos OS 15.1X49-D40 – SRX Series.