Release Notes: Junos® OS Release 15.1X49-D10 for the SRX Series

Release 15.1X49-D10
03 January 2017
Revision 8

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-D10 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 now supports 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). Use the Junos OS Release 15.1X49 Release Notes and all the documentation for vSRX and for SRX5000 line devices with these specific host subsystem configurations (RE2 with SCB2 or RE2 with SCB3).

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

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

Junos OS Release 15.1X49 does not support branch SRX Series devices or SRX1400, SRX3400, or SRX3600 devices.

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-D10 for the SRX Series and in vSRX Release 15.1X49-D15.

Hardware Features

Security

- **Enhanced support for Switch Control Board and Modular Port Concentrators**—Starting with Junos OS Release 15.1X49-D10, the SRX5400, SRX5600, and SRX5800 Services Gateways support the third-generation Switch Control Board SRX5K-SCB3 (SCB3) and the Modular Port Concentrator (IOC3): SRX5K-MPC3-40G10G and SRX5K-MPC3-100G10G. These cards provide superior carrier-grade network performance and chassis cluster features, and greater throughput, interface density, Application Layer performance, and scalability. The SCB3 provides higher capacity traffic support, greater link speeds and fabric capacity, and improved services. The IOC3s enable faster processing and provide line rates of up to 240 Gbps per slot.

  [See Switch Control Board SRX5K-SCB3, SRX5K-MPC3-40G10G, and SRX5K-MPC3-100G10G.]

Software Features

Dynamic Host Configuration Protocol (DHCP)

- **DHCP Relay on VRF Support (vSRX)**—Starting with vSRX Release 15.1X49-D15, DHCP Relay is supported in routing-instances of type VPN routing and forwarding (VRF). VRF is used for Layer 3 VPN implementations. The VRF routing instance type has a VPN routing and forwarding table and a VPN forwarding table. Hence, there is a one-to-one mapping between an interface and a VRF instance.

  [See Administration Guide for Security Devices.]

- **DHCP Relay support for IPv6 (vSRX)**—Starting with vSRX Release 15.1X49-D15, vSRX supports DHCP Relay for IPv6. DHCP relay agent forwards incoming requests from BOOTP and DHCP clients to a specified BOOTP or DHCP server. Client requests can pass through virtual private network (VPN) tunnels. You cannot configure a single device interface to operate as both a DHCP client and a DHCP relay.

  [See Admininistration Guide for Security Devices.]

Flow-Based and Packet-Based Processing

- **Express Path (formerly known as services offloading) on the SRX5000 line IOC3**—Starting with Junos OS Release 15.1X49-D10, the SRX5K-MPC3-100G10G (IOC3) and the SRX5K-MPC3-40G10G (IOC3) support Express Path.

  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.

  To achieve the best latency result, both the ingress port and egress port of a traffic flow need to be on the same XM chip of the IOC3.

  NOTE: XL chip flow table lookup occurs only in ingress. Egress datapath packet handling is the same as supported in the previous release.

  NOTE: The services offloading feature is renamed to *Express Path* starting in Junos OS Release 12.3X48-D10. Currently, the documents still use the term *services offloading*.

  [See Express Path Overview, Enabling and Disabling Express Path, services-offload, np-cache (Flexible PIC Concentrator), and Example: Configuring SRX5K-MPC3-100G10G (IOC3) and SRX5K-MPC3-40G10G (IOC3) on an SRX5000 Line Device to Support Express Path.]

- **Fragmentation packet ordering using session cache**—Starting with Junos OS Release 15.1X49-D10, the IOCs (SRX5K-MPC [IOC2], SRX5K-MPC3-100G10G [IOC3], and

SRX5K-MPC3-40G10G [IOC3]) on SRX5400, SRX5600, and SRX5800 devices support fragmentation packet ordering using the session cache.

A session can consist of both normal and fragmented packets. With hash-based distribution, 5-tuple and 3-tuple keys can be used to distribute normal and fragmented packets to different SPUs. All the session packets are forwarded to the SPU. Due to latency, the SPU might not guarantee packet ordering. Session cache on the IOCs ensures fragmentation ordering.

A session cache entry is allocated for normal packets of the session, and the 5-tuple key is used to find the fragmented packet. When the first fragmented packet is received, the IOC updates the session cache entry. The IOC forwards all subsequent packets to the SPU to ensure fragmentation packet ordering.

To enable session cache on the IOC, you need to run the **set chassis fpc *<fpc-slot>* np-cache** command.

[See Understanding Session Cache and Express Path Overview.]

- **Hash-based forwarding on the SRX5K-MPC3-40G10G (IOC3) and SRX5K-MPC3-100G10G (IOC3)**—Starting with Junos OS Release 15.1X49-D10, hash-based datapath packet forwarding is supported on the IOC3 to interconnect with all existing IOC and SPC cards for SRX5400, SRX5600, and SRX5800 devices.

  The IOC3 XL chip uses a hash-based method to distribute ingress traffic to a pool of SPUs by default. Selection of hash keys depends on application protocols.

  On a high-end SRX Series device, a packet goes through a series of events involving different components from ingress to egress processing. With the datapath packet forwarding feature, you can obtain quick delivery of I/O traffic over the SRX5000 line of devices.

  [See Understanding Load Distribution in High-End SRX Series Devices, hash-based, show security flow statistics, and show security flow status.]

- **Session cache and selective installation of session cache**—Starting with Junos OS Release 15.1X49-D10, the IOCs (SRX5K-MPC [IOC2], SRX5K-MPC3-100G10G [IOC3], and SRX5K-MPC3-40G10G [IOC3]) on SRX5400, SRX5600, and SRX5800 devices support session cache and selective installation of session cache.

  Session cache is used to cache a conversation between the network processor (NP) and the SPU on an IOC. A conversation could be a session, GTP-U tunnel traffic, IPsec VPN tunnel traffic, and so on. A conversation has two session cache entries, one for incoming traffic and the other for reverse traffic.

  The session cache table is extended to support the NP sessions as well. Express Path (formerly known as *services offloading*) traffic and the NP traffic share the same session cache table on the IOCs. The session cache on the IOC leverages the Express Path functionality.

  To optimize system resources and conserve session entries on IOCs, certain priority mechanisms are applied to both the flow module and the IOCs to selectively install the session cache.

  To enable session cache on the IOC, you need to run the **set chassis fpc *<fpc-slot>* np-cache** command.

[See Understanding Session Cache, Express Path Overview, and Understanding VPN Session Affinity.]

Interfaces and Chassis

- **SRX5K-MPC3-40G10G (IOC3) and SRX5K-MPC3-100G10G (IOC3)** —Starting with Junos OS Release 15.1X49-D10, the SRX5K-MPC3-40G10G (IOC3) and the SRX5K-MPC3-100G10G (IOC3) are introduced for SRX5400, SRX5600, and SRX5800 devices.

  These IOC3s provide the powerful SRX5000 line devices with superior networking and carrier grade chassis cluster features, interface density (scalable and upgradable), and high performance. Both IOC3s support up to an aggregated 240-Gbps IMIX throughput per slot, latency less than 10 microseconds, and higher Layer 7 (L7) performance.

  The two types of IOC3 MPCs, which have different built-in MICs, are the 24x10GE + 6x40GE MPC and the 2x100GE + 4x10GE MPC.

  The IOC3s do not support the following command to set a PIC to go offline or online:

  request chassis pic fpc-slot <fpc-slot> pic-slot <pic-slot> <offline | online> CLI command.

  All four PICs on the 24x10GE + 6x40GE cannot be powered on. A maximum of two PICs can be powered on at the same time.

  Use the **set chassis fpc <slot> pic <pic> power off** command to choose the PICs you want to power on.

  NOTE: Fabric bandwidth increasing mode is not supported on the IOC3.

  WARNING:

  On SRX5400, SRX5600, and SRX5800 devices in a chassis cluster, when the PICs containing fabric links on the SRX5K-MPC3-40G10G (IOC3) are powered off to turn on alternate PICs, always ensure that:

  - The new fabric links are configured on the PICs that are turned on. At least one fabric link must be present and online to ensure minimal RTO loss.
  - The chassis cluster is in active-backup mode to ensure minimal RTO loss, once alternate links are brought online.
  - If no alternate fabric links are configured on the PICs that are turned on, RTO synchronous communication between the two nodes stops and the chassis cluster session state will not back up, because the fabric link is missing. You can view the CLI output for this scenario indicating a bad chassis cluster state by using the **show chassis cluster interfaces** command.

  [See show chassis hardware (View) and show chassis fpc (View).]

- **Switch Control Board SRX5K-SCB3 (SCB3) with enhanced midplanes**—Starting with Junos OS Release 15.1X49-D10, the SRX5K-SCB3 (SCB3) with enhanced midplanes is introduced for SRX5400, SRX5600, and SRX5800 devices.

  The SCB3 provides the powerful SRX5000 line devices with superior networking and carrier grade chassis cluster features, interface density (scalable and upgradable), and high performance. The IOC3s support up to an aggregated 240-Gbps IMIX throughput per slot. To support this high throughput per slot, the SCB3 and enhanced midplanes are required to guarantee full-bandwidth connection.

  The SCB3 works only with the SRX5K-RE-1800X4(RE2), SRX5K-MPC (IOC2), the SRX5K-SPC-4-15-320 (SPC2), the SRX5K-MPC3-40G10G (IOC3), and the SRX5K-MPC3-100G10G (IOC3), with the standard midplanes and the enhanced midplanes.

  The SCB3 does not support mixed Routing Engines and SCBs, in-service software upgrade (ISSU), in-service hardware upgrade (ISHU), or fabric bandwidth increasing mode.

  To request that an SRX5K-SCB3 go online or offline, use the **request chassis cb (offline | online) slot slot-number** CLI command.

  [See show chassis hardware (View), show chassis environment cb, and request chassis cb.]

IPv6

- **Support for RPM probes with IPv6 sources and destinations (vSRX)**—Starting with vSRX Release 15.1X49-D15, vSRX supports IPv6 for Route Engine-based real-time performance monitoring (RE-based RPM). RPM is a mechanism that enables you to monitor network performance in real time and to assess and analyze network efficiency. RPM can now send and receive IPv6 probe packets to monitor performance on IPv6 networks. To specify the destination IPv6 address used for the probes, include the **target (url *ipv6-url* | address *ipv6-address*)** statement at the **[edit services rpm probe owner test *test-name*]** hierarchy level. To specify the source IPv6 address of the client from which the RPM probes are sent, include the **inet6-options source-address *ipv6-address*** statement at the **[edit services rpm probe owner test *test-name*]** hierarchy level.

  [See IPv6 RPM Probes, Guidelines for Configuring RPM Probes for IPv6, and Configuring IPv6 RPM Probes.]

- **TACACS+ IPV6 Support (vSRX)**—Starting with vSRX Release 15.1X49-D15, vSRX supports Terminal Access Controller Access Control System Plus (TACACS+) on the IPv6 protocol. TACACS+ is a protocol that allows a remote access server to communicate with an authentication server in order to determine if a user has access to the network. It handles authentication, authorization, and accounting (AAA) services.

  [See Administration Guide for Security Devices.]

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 (Ethernet switching) configuration statements and operational commands are not supported.

  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 for registered customers to help them become familiar with the enhanced Layer 2 CLI and to quickly convert existing switch-based CLI configurations to transparent mode 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.]

VPNs

- **IPsec VPN session affinity**—Starting with Junos OS Release 15.1X49-D10, the IOCs (SRX5K-MPC [IOC2], SRX5K-MPC3-100G10G [IOC3], and SRX5K-MPC3-40G10G [IOC3]) on SRX5400, SRX5600, and SRX5800 devices support IPsec session affinity for IPsec tunnel-based traffic.

  With the IOC, the flow module creates sessions for IPsec tunnel-based traffic before encryption and after decryption on its tunnel-anchored SPU and installs the session cache for the sessions so that the IOC can redirect the packets to the same SPU to minimize packet forwarding overhead.

  NOTE: To enable session cache on the IOC, you need to run the **set chassis fpc *<fpc-slot>* np-cache** command.

  To enable IPsec VPN affinity, use the **set security flow load-distribution session-affinity ipsec** command.

  [See Understanding VPN Session Affinity, Enabling VPN Session Affinity, and session-affinity.]

vSRX (formerly Firefly Perimeter)

- **Enhancements to vSRX**—Starting with vSRX Release 15.1X49-D15, vSRX includes a new architecture based on Linux and Junos OS for performance and flexibility, DPDK packet I/O support for higher throughput, and SR-IOV vNIC and VMXNET 3 vNIC support for greater performance and hypervisor compatibility. SCSI virtual disk support has been added to existing IDE support.

  Other vSRX changes include:

- vSRX interfaces of 1 Gbps have a Class of Service (CoS) default delay buffer time of 1 second, a maximum buffer time of 32 seconds, and a maximum buffer size of 128 MB.
- On a logical vSRX interface, the sum of the guaranteed delay buffer sizes acts as a pool that can be shared among the queues that do not have a specific shaping rate.

Related Documentation

- Changes in Behavior and Syntax on page 10
- Known Behavior on page 12
- Known Issues on page 14
- Resolved Issues on page 16
- Documentation Updates on page 19
- Migration, Upgrade, and Downgrade Instructions on page 20

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-D10.

User Interface and Configuration

- Prior to Junos OS Release 15.1X49-D10, if you configured user-defined identifiers through the CLI using the reserved prefix, the commit would incorrectly succeed. Starting with Junos OS Release 15.1X49-D10 and later releases you cannot use "junos-" anywhere in the configuration except inside the "junos-defaults" group configurations. The CLI configurations will now exhibit the correct behavior by providing a commit error when “junos-“ is used.

Chassis Cluster

- When an SRX Series device is operating in chassis cluster mode and encounter any IA-chip access issue in an SPC or a I/O Card (IOC), a minor FPC alarm will be activated to trigger redundancy group failover.

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.]

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.

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.

Related Documentation

- New and Changed Features on page 4
- Known Behavior on page 12
- Known Issues on page 14
- Resolved Issues on page 16
- Documentation Updates on page 19
- Migration, Upgrade, and Downgrade Instructions on page 20

Known Behavior

This section contains the known behaviors, system maximums, and limitations in hardware and software in Junos OS Release 15.1X49-D10.

Application Identification and Tracking

- The application quality of service (AppQoS) feature is supported SRX5K-40GE-SFP I/O Card (IOC) and not supported on SRX5K-MPC (IOC2), SRX5K-MPC3-100G10G (IOC3), and SRX5K-MPC3-40G10G (IOC3).

Attack Detection and Prevention (ADP)

- On all branch SRX Series devices, the fast path bad-inner-header screen is always performed first, followed by the first path signature screen.
- 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

Layer 2 Features

- On all branch SRX Series devices, configuring the Layer 2 Ethernet switching family in transparent mode for an interface is not supported.

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>***

Software Installation and Upgrade

- On all SRX 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.

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 VPN interfaces is not supported.

Related Documentation

- New and Changed Features on page 4
- Changes in Behavior and Syntax on page 10
- Known Issues on page 14
- Resolved Issues on page 16
- Documentation Updates on page 19
- Migration, Upgrade, and Downgrade Instructions on page 20

Known Issues

This section lists the known issues in hardware and software in Junos OS Release 15.1X49-D10.

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 SRX5400, SRX5600, and SRX5800 devices, the SQL ALG is disabled by default in Junos OS Release 15.1X49-D10. PR1093193

Chassis Cluster

- On SRX5400, SRX5600, and SRX5800 devices, all interfaces of the RG0 secondary node go down when the connection between the kernel of the primary node and the ksyncd of the secondary node fails. PR1084660

Flow-Based and Packet-Based Processing

- On SRX5400, SRX5600, and SRX5800 devices in a chassis cluster with seven Services Processing Cards (SPCs) and multiple IPv6 policies (around 90 policies), when you reboot the device, flowd core files are generated. After the Switch Control Boards (SCBs) identify SPCs and initialize the SPC hardware, the Routing Engine policies are synchronized with the Packet Forwarding Engine. Therefore, one or more SPCs from either the primary node or the secondary node generate flowd core files. As a result, when all SPCs in the primary node or the secondary node undergo a reset, some of the flowd core files might again be generated. This issue does not occur after the chassis cluster is stable and all SPCs are online.

  After you reboot the device, some SPUs might stay in offline state and generate flowd core files.

  As a workaround, do the following:

  1. Disable the control and fabric links.
  2. Deactivate the IPv6 policies and then reboot the affected node.
  3. After all images are online and the chassis cluster is stable, activate the IPv6 policies.

  PR1089272

- On SRX5400, SRX5600, and SRX5800 devices, in order to prevent all decapsulated cleartext packets going from the IPsec tunnel to the central point and to improve throughput, all cleartext sessions related to the IPsec tunnel attempt to install a forward session in an anchor SPU on the high-end SRX Series device. Thus, the anchor SPU will have more sessions than the non-anchor SPU. When the forward session's deleted message is lost without retransmission, the forward session's life is longer than that of the cleartext session. PR1105704

J-Web

- On SRX5400, SRX5600, and SRX5800 devices, when you go to the Monitor>NAT>Source NAT page and click the Resource Usage tab, all Pool type values in the grid are displayed as PAT. J-Web fails to recognize the non-PAT pool. PR1036621
- On SRX5400, SRX5600, and SRX5800 devices, you cannot create a new rule set of CoS for an existing security policy through J-Web. PR1095759
- On SRX5400, SRX5600, and SRX5800 devices, when you log in to J-Web using logical system credentials, you cannot monitor the CPU profile on the Dashboard page. PR1097008

Platform and Infrastructure

- On SRX5400, SRX5600, and SRX5800 devices, the cscript data memory limit is exceeded when you run an op, event, or commit script. The cscript process restarts and generates a core file due to a segmentation fault in the libxml2 library, causing the script to not run successfully and possibly causing the commit to fail.

  As a workaround, when you run the script, adjust the maximum amount of memory allocated for the data segment as follows:

  set system scripts commit max-datasize

  set system scripts op max-datasize

  set event-options event-script

  PR722161
- On SRX5400, SRX5600, and SRX5800 devices, the wrong IP information **Unknown IP version: 0** is displayed in a few load-balancing thread (LBT) and packet-ordering thread (POT) logs triggered by fragmentation. PR1032647

Security

- On SRX5400, SRX5600, and SRX5800 devices, Junos OS Release 15.1X49-D10 uses newer versions of OpenSSL that have improved security features. These features consume higher amounts of memory per session. For example, when you use SSL forward proxy, the session scaling numbers are less compared to Junos OS Release 12.1X47 and Junos OS Release 12.3X48 session scaling numbers. PR1084348

System Logging

- On SRX5400, SRX5600, and SRX5800 devices in a chassis cluster, when you run the **request system configuration rescue save** command, the following error message is displayed: **command is not valid on the srx5800**. However, the functionality works as expected. PR1097154

VPNs

- On SRX5400, SRX5600, and SRX5800 devices with dynamic VPN configured, the key management process (KMD) might crash when an IKE payload with a different port number is received. PR1080326

Related Documentation

- New and Changed Features on page 4
- Changes in Behavior and Syntax on page 10
- Known Behavior on page 12
- Resolved Issues on page 16
- Documentation Updates on page 19
- Migration, Upgrade, and Downgrade Instructions on page 20

Resolved Issues

This section lists the issues fixed in hardware and software in Junos OS Release 15.1X49-D10.

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 SRX5400, SRX5600, and SRX5800 devices with H.323 ALG and NAT enabled to process H.323 traffic, if H.323 calls contain the same source IP address and port number but in different positions, then some of the unidirectional sessions of H.323 might be seen. As a result, calls related to the H.323 ALG fail. PR1069067

Chassis Cluster

- On SRX5400, SRX5600, and SRX5800 devices, traffic outage might occur with hardware errors (IA PIO errors). When the devices are configured in a chassis cluster, the hardware errors (IA PIO errors) do not trigger RG1+ failover. This fix is used to raise an FPC minor alarm to trigger the RG1+ to switch over for a chassis cluster. PR1080116

Class of Service (CoS)

- On SRX5400, SRX5600, and SRX5800 devices, the CoS rewrite rules do not work for VPN traffic if the rules are configured with **loss priority high**. This occurs when the packets are reinjected into the IPsec tunnel encapsulation process. PR1085654

General Packet Radio Service (GPRS)

- On SRX5400, SRX5600, and SRX5800 devices, when GPRS tunneling protocol version 2 (GTPv2) is configured, GTPv2 might fail to create control sessions. PR1029284

Flow-Based and Packet-Based Processing

- On SRX5400, SRX5600, and SRX5800 devices in a chassis cluster, when RG0 resides on a different node, RG1+ traffic sent out by the Routing Engine (RG0 node) is dropped. PR1059901
- On SRX5400, SRX5600, and SRX5800 devices, when the SPU works in high stress, the internal event queue becomes full and the event is lost. Because there is no retransmission mechanism for the internal event, this leads to a stuck session. The stuck session is recovered by up layer applications. For example, when the TCP session of the log module is stuck, the log message cannot be sent. After 30 seconds, the log module detects this and restarts the new connection to send the log message.

  As a workaround, for next-generation SPCs, the maximum concurrent sessions that need Layer 7 processing are 3000 per SPU. This number varies for different platforms. PR1060529
- On SRX5400, SRX5600, and SRX5800 devices, when you run the **show security policies hit-count** command, the Routing Engine memory is overwritten, resulting in an nsd process crash. This issue occurs when security policies are not synchronized between the Routing Engine and the data plane. PR1069371
- On SRX5400, SRX5600, and SRX5800 devices, the flowd process might crash when the multicast traffic processes the route lookup failure. PR1075797

- On SRX5400, SRX5600, and SRX5800 devices, if there are any configuration changes made to the interface (for example, when you add a new unit for an interface), an internal interface-related object will be freed and reallocated. However, in a rare condition, some packets queued in the system might refer to the freed object, causing the flowd process to crash. PR1082584
- On SRX5400, SRX5600, and SRX5800 devices, the flowd process might crash because of a 64-bit unaligned memory access. PR1085153

Network Address Translation (NAT)

- On SRX5400, SRX5600, and SRX5800 devices, the entry's timeout value of ALG is configured larger than the timer wheel's maximum timeout value (7200 seconds). However, this entry cannot be inserted into the timer wheel. As a result, an ALG persistent NAT binding leak occurs. PR1088539

Unified Threat Management (UTM)

- On SRX5400, SRX5600, and SRX5800 devices running Junos OS Release 15.1X49-D10 or later releases with Enhanced Web Filtering (EWF) configured, if the UTM EWF category object updating the data plane fails, the UTM EWF category object will not be updated anymore. This issue occurs during the system initialization process of an SRX Series chassis cluster. PR1073198

Related Documentation

- New and Changed Features on page 4
- Changes in Behavior and Syntax on page 10
- Known Behavior on page 12
- Known Issues on page 14
- Documentation Updates on page 19
- Migration, Upgrade, and Downgrade Instructions on page 20

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.

Layer 2 Bridging and Transparent Mode for Security Devices

- Starting in Junos OS Release 15.1X49-D10, the *Layer 2 Bridging and Switching Feature Guide for Security Devices* guide is retitled to *Layer 2 Bridging and Transparent Mode for Security Devices*.
- Although Ethernet switching is not supported in Junos OS Release 15.1X49-D10, the *Layer 2 Bridging and Transparent Mode for Security Devices* guide retains content about Ethernet switching.
- Starting in Junos OS Release 15.1X49-D10, the term *bridge-domain* is changed to *VLAN*. However, the documents still use the term *bridge-domain* in topics.

Related Documentation

- New and Changed Features on page 4
- Changes in Behavior and Syntax on page 10
- Known Behavior on page 12
- Known Issues on page 14
- Resolved Issues on page 16
- Migration, Upgrade, and Downgrade Instructions on page 20

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, 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 enhanced Layer 2 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 .

Upgrading an AppSecure Device

For devices implementing AppSecure services, use the **no-validate** option when upgrading from Junos OS Release 11.2 or earlier to Junos OS 11.4R1 or later. The application signature package used with AppSecure services in previous releases has been moved from the configuration file to a signature database. This change in location can trigger an error during the validation step and interrupt the Junos OS upgrade. The **no-validate** option bypasses this step.

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 22).

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.

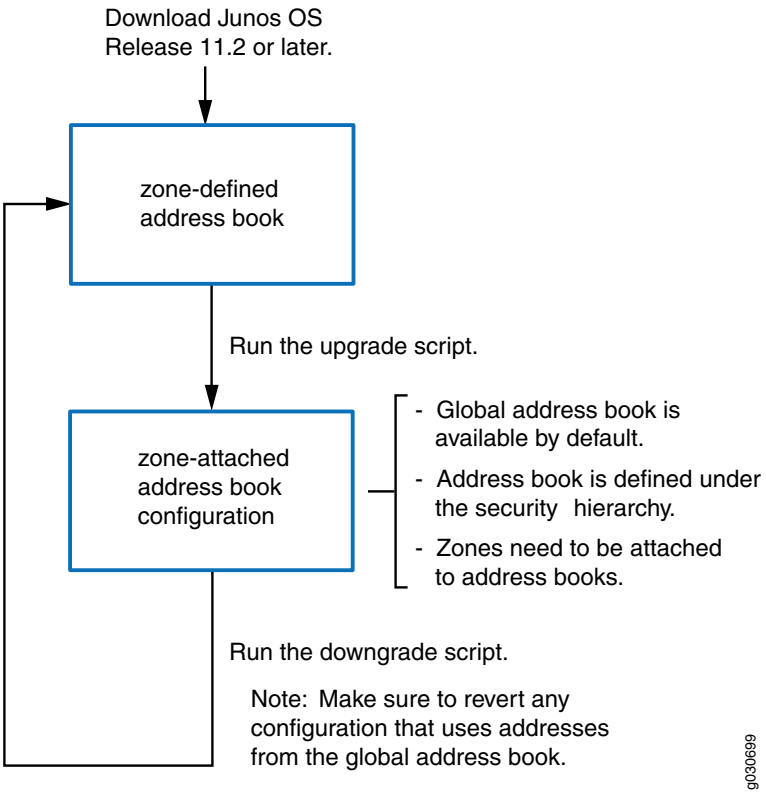
  After upgrading to the zone-attached address book configuration:

  - 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 10.0, 10.4, and 11.4 are EEOL releases. You can upgrade from Junos OS Release 10.0 to Release 10.4 or even from Junos OS Release 10.0 to Release 11.4. However, you cannot upgrade directly from a non-EEOL release that is more than three releases ahead or behind. For example, you cannot directly upgrade from Junos OS Release 10.3 (a non-EEOL release) to Junos OS Release 11.4 or directly downgrade from Junos OS Release 11.4 to Junos OS Release 10.3.

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 additional information about how to upgrade and downgrade, see the Installation and Upgrade Guide for Security Devices.

Related Documentation

- New and Changed Features on page 4
- Changes in Behavior and Syntax on page 10
- Known Behavior on page 12
- Known Issues on page 14
- Resolved Issues on page 16

Product Compatibility

- Hardware Compatibility on page 23
- Transceiver Compatibility for SRX Series Devices on page 24

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 send your comments to techpubs-comments@juniper.net, 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 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.

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 https://www.juniper.net/cgi-bin/docbugreport/.

Revision History

03 January, 2017—Revision 8— Junos OS 15.1X49-D10 – SRX Series.

15 November, 2016—Revision 7— Junos OS 15.1X49-D10 – SRX Series.

12 April, 2016—Revision 6— Junos OS 15.1X49-D10 – SRX Series.

17 March, 2016—Revision 5— Junos OS 15.1X49-D10 – SRX Series.

29 December, 2015—Revision 4— Junos OS 15.1X49-D10 – SRX Series.

11 August, 2015—Revision 3— Junos OS 15.1X49-D10 – SRX Series.

31 July, 2015—Revision 2— Junos OS 15.1X49-D10 – SRX Series.

30 June, 2015—Revision 1— Junos OS 15.1X49-D10 – SRX Series.