Release Notes: Junos® OS Release 12.3X48-D10 for the SRX Series

Release 12.3X48-D10
16 September 2015
Revision 5

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 12.3X48-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/.

New and Changed Features

This section describes the new features and enhancements to existing features in Junos OS Release 12.3X48-D10 for the SRX Series.

Software Features

Application Layer Gateways (ALGs)

- **MS-RPC ALG and Sun RPC ALG map table scaling for SRX Series devices**—Starting with Junos OS Release 12.3X48-D10, the MS-RPC ALG and Sun RPC ALG dynamically allocate new mapping entries instead of using a default size (512 entries). They also offer a flexible time-based RPC mapping entry that removes the mapping entry (auto-clean) without affecting the associated active RPC sessions, including both control session and data session.

  [See Understanding Sun RPC ALGs and Understanding Microsoft RPC ALGs.]

Chassis Cluster

- **Dual active-backup IPsec VPN chassis clusters for SRX1400, SRX3400, SRX3600, SRX5600, and SRX5800 devices**—Starting with Junos OS Release 12.3X48-D10, VPN tunnels can terminate on either node of an active/active chassis cluster pair. Both nodes in the chassis cluster can actively pass traffic through VPN tunnels at the same time.

  NOTE: Z-mode flows occur when traffic enters an interface on a chassis cluster node, passes through the fabric link, and exits through an interface on the other cluster node. They are not supported with dual active-backup IPsec VPN chassis clusters.

  [See Understanding Dual Active-Backup IPsec VPN Chassis Clusters.]

Flow-based and Packet-based Processing

- **Allowing embedded ICMP packets for SRX Series devices**—Starting with Junos OS Release 12.3X48-D10, security flow allows embedded ICMP packets to pass through your device even when there is no session match. By default, an embedded ICMP packet is dropped if it does not match any session. Use the **allow-embedded-icmp** statement at the **[edit security flow]** hierarchy level to enable this feature. Once enabled, all packets encapsulated in ICMP pass through and no policy affects this behavior. This feature is useful when you have asymmetric routing in your network and you want to use traceroute and other ICMP applications on your device.

  [See allow-embedded-icmp.]

- **Enhanced security flow session command for SRX Series devices**—Starting with Junos OS Release 12.3X48-D10, the following updates have been made to the **show security flow session** command:

  - A new option, **policy-id**, allows you to query the flow session table by policy ID.
  - New output flags have been added in the command output. The three available flags are **flag**, **natflag1**, and **natflag2**.

  [See show security flow session and show security flow session policy-id.]

- **Express Path (formerly known as services offloading) on the SRX5000 line MPC for SRX5400, SRX5600, and SRX5800 devices**—Starting with Junos OS Release 12.3X48-D10, the SRX5K-MPC supports 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.

  The following features are supported:

  - Support inter- and intra-Packet Forwarding Engine Express Path for IPv4
  - Per-wing statistics counter of bytes and packets sent out over the wing
  - LAG interfaces
  - NAT for IPv4
  - Active and backup chassis cluster

  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 Services Offloading Overview.]

- **Improved session close log for SRX Series devices**—Starting with Junos OS Release 12.3X48-D10, the session closed log message has been expanded to include information about the device sending the TCP RST. The new log message **session closed TCP [client | server] RST** simplifies troubleshooting by indicating whether it was the client or the server that sent the TCP RST.

  ```
  Jan 12 13:51:04 user@host RT_FLOW: RT_FLOW_SESSION_CLOSE: session closed TCP
  SERVER RST: 30.0.0.2/54584->50.0.0.2/8081 None 30.0.0.2/54584->50.0.0.2/8081
  None None None None 6 p1 green red 250003018 1(60) 1(40) 2 UNKNOWN UNKNOWN
  N/A(N/A) ge-11/0/0.0 UNKNOWN

  Jan 12 13:53:44 user@host RT_FLOW: RT_FLOW_SESSION_CLOSE: session closed TCP
  CLIENT RST: 30.0.0.2/46488->50.0.0.2/23 junos-telnet 30.0.0.2/46488->50.0.0.2/23
  None None None None 6 p1 green red 240003072 2(100) 1(60) 2 UNKNOWN UNKNOWN
  N/A(N/A) ge-11/0/0.0 UNKNOWN
  ```

  [See Junos OS System Log Reference for Security Devices.]

General Packet Radio Service (GPRS)

- **GTP GSN table ager for high-end SRX Series devices**—Starting with Junos OS Release 12.3X48-D10, one SRX Series device supports 100,000 GSN entries per SPU and 250,000 GSN entries per CP. Prior to this release, each entry was saved permanently. To prevent GSN entry exhaustion caused by frequent short-time roaming among countries, visiting GSNs are recorded when subscribers access the home GPRS core network from visiting countries. These entries are not deleted when the subscribers return home, but no further traffic is passed. The GTP GSN table ager causes the idling GSN entries to time out, preventing inactive GSNs from taking up too much space.

[See show security gprs gtp gsn statistics.]

- **SCTP association scaling for high-end SRX Series devices**—Starting with Junos OS Release 12.3X48-D10, the capacity of SCTP is enhanced from 5000 associations to 20,000 associations per SPU.

  [See Understanding Stream Control Transmission Protocol.]

IP Tunneling

- **IPv6 tunneling control for SRX Series devices**—Starting with Junos OS Release 12.3X48-D10, the IPv6 tunneling control feature introduces new screens for tunneled traffic based on user preferences. By default, all tunneling traffic is allowed by the screens unless the external IP encapsulation matches the block criteria of any existing screen. You must enable the screens to control, allow, or block the transit of tunneled traffic. The following new screens are introduced in this feature:
  - GRE 4in4 Tunnel
  - GRE 4in6 Tunnel
  - GRE 6in4 Tunnel
  - GRE 6in6 Tunnel
  - Bad Inner Header Tunnel
  - IPinIP 6to4relay Tunnel
  - IPinIP 6in4 Tunnel
  - IPinIP 6over4 Tunnel
  - IPinIP 4in6 Tunnel
  - IPinIP ISATAP Tunnel
  - IPinIP DS-Lite Tunnel
  - IPinIP 6in6 Tunnel
  - IPinIP 4in4 Tunnel
  - IPinUDP Teredo Tunnel

[See Understanding Screen IPv6 Tunneling Control.]

IPv6

- **Transparent mode for IPv6 support extended for SRX Series devices**—The Transparent mode for IPv6 was supported on all high-end SRX Series devices. Starting with Junos OS Release 12.3X48-D10, transparent mode for IPv6 is also supported on all branch SRX Series devices.

  [See Understanding IPv6 Flows in Transparent Mode.]

Layer 2 Features

- **Secure wire mode and mixed mode (Layer 2 and Layer 3) support for SRX Series devices**—Starting with Junos OS Release 12.3X48-D10, secure wire mode and mixed mode are supported and the interface type of these modes is the same without cross talk. You can configure both Layer 2 and Layer 3 interfaces simultaneously using separate security zones. There is no routing among IRB interfaces or between IRB interfaces and Layer 3 interfaces. Also, the user logical system is not supported for Layer 2 traffic. However, you can configure the Layer 2 interface using the root logical system.

  As with mixed mode, in secure wire mode you can configure both Layer 3 and secure wire interfaces simultaneously. In fact, you can configure Layer 3, Layer 2, and secure wire interfaces simultaneously, without traffic cross talk between any two of the three configured interfaces.

  [See Understanding Mixed Mode (Layer 2 and Layer 3).]

Network Address Translation (NAT)

- **NAT64 IPv6 prefix to IPv4 address persistent translation for SRX Series devices**—Starting with Junos OS Release 12.3X48-D10, this feature, which is targeted at IPv6 mobile networks, is used with the dual-translation mechanism, 464XLAT, to enable IPv4 services to work over IPv6-only networks. It augments the existing NAT64 mechanism, which enables IPv6 clients to contact IPv4 servers by translating IPv6 addresses to IPv4 addresses (and vice versa). However, the existing NAT64 mechanism does not ensure a sticky mapping relationship for one unique end user. By configuring the new **address-persistent** option with a specific IPv6 prefix length for NAT64 translations in an IPv4 source NAT pool, a sticky mapping relationship is ensured between one specific IPv6 prefix and one translated IPv4 address.

  [See Understanding NAT64 IPv6 Prefix to IPv4 Address-Persistent Translation.]

PKI

- **Digital certificate validation for SRX Series devices**—Starting with Junos OS Release 12.3X48-D10, the PKI daemon on SRX Series devices performs X509 certificate policy, path, key usage, and distinguished name validation, as specified in RFC 5280, *Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile*.

  [See Understanding Digital Certificate Validation.]

Routing Protocols

- **Virtual Router Redundancy Protocol version 3 (VRRPv3) for branch SRX Series devices**—Starting with Junos OS Release 12.3X48-D10, the Internet protocol VRRP provides one or more backup devices when a statically configured device is used on a LAN. The devices share a virtual IP address, with one device designated as the primary devices and the others as backups.

  VRRP is the combination of both IPv4 and IPv6. The VRRPv3 feature supports IPv4 and IPv6 VRRP groups, including IPv6 traps. When you configure VRRP IPV6 groups, you must set the virtual-link-local address or link-local-address value explicitly. Otherwise, the address will be automatically generated.

  To enable VRRPv3, set the **version-3** statement at the **[edit protocols vrrp]** hierarchy level.

  NOTE: To avoid having multiple primary devices in the network, the VRRPv3 IPv4 devices switch to the backup state when they receive a VRRPv2 IPv4 advertisement packet. Additionally, to avoid having multiple primary devices in your IPv6 network that are caused by checksum differences, you need to disable VRRP for IPv6 on the backup devices before you perform the VRRPv2 to VRRPv3 upgrade.

  NOTE: When you enable VRRPv3, ensure that the protocol is enabled on all the VRRP devices in the network. This is because VRRPv3 does not interoperate with previous versions of VRRP.

[See Junos OS Support for VRRPv3.]

Security

- **Secure wire interface mode and forwarding for SRX Series devices**—Starting with Junos OS Release 12.3X48-D10, secure wire allows interfaces to be mapped one-to-one for ingress-to-egress forwarding. It differs from transparent and route modes in that there is no switching or routing lookup to forward traffic. Policies and upper-layer security features permit traffic to be forwarded through the device.

  This feature is available on Ethernet logical interfaces; both IPv4 and IPv6 addresses are supported. You can configure interfaces for access or trunk mode. Secure wire supports chassis cluster redundant Ethernet interfaces and virtual LAN tagging, but it does not support IRB interfaces. This feature does not support security features not supported in transparent mode, including NAT and IPsec VPN. It does support Layer 7 features, including AppSecure, IPS, and UTM.

  [See Understanding Secure Wire.]

Unified Threat Management (UTM)

- **Redirect Web filtering support for SRX Series devices**—The redirect Web filtering solution intercepts HTTP requests and sends them to an external URL filtering server, provided by Websense, to determine whether to block or permit the requests.

  [See Understanding Redirect Web Filtering.]

VPNs

- **Auto Discovery VPN (ADVPN) protocol for SRX Series devices**—Starting with Junos OS Release 12.3X48-D10, AutoVPN deployments can use the ADVPN protocol to dynamically establish spoke-to-spoke VPN tunnels. When passing traffic from one spoke to another spoke, the hub can suggest that the spokes establish a direct security association, or "shortcut," between each other. Shortcuts can be established and torn down dynamically, resulting in better network resource utilization and reduced reliance on a centrally located hub.

  On the hub, configure **advpn suggester** at the [**edit security ike gateway *gateway-name***] hierarchy level. On spokes, configure **advpn partner** at the [**edit security ike gateway *gateway-name***] hierarchy level. ADVPN is supported with IKEv2 only.

  [See Understanding Auto Discovery VPN.]

- **AutoVPN with traffic selectors for SRX Series devices**—Starting with Junos OS Release 12.3X48-D10, AutoVPN hubs can be configured with multiple traffic selectors. This allows hubs to advertise spoke networks with different metrics.

  This feature includes the following added functionality:

  - AutoVPN hubs with traffic selectors can be configured with the st0 interface in point-to-point mode for both IKEv1 and IKEv2.

    NOTE: Dynamic routing protocols are not supported with traffic selectors with st0 interfaces in point-to-point mode.

- Traffic selectors are configured on the hub to protect traffic to spokes. Spokes can be non-SRX Series devices.

[See Understanding AutoVPN with Traffic Selectors.]

- **Enhanced VPN support for inactive-tunnel reporting and syslog for SRX Series devices**—Starting with Junos OS Release 12.3X48-D10, the methods used for debugging issues in VPN have been enhanced to improve the process in several ways. The use of CLI per-tunnel debugging, deleting the traceoptions configuration stanza after data collection is complete, and issuing the subsequent commit command are no longer required. Debugging can now be performed through Junos OS operational commands with the following VPN enhancements:
  - Information shown in the output of the **show security ipsec inactive-tunnel** command
  - System log messages

[See Understanding Tunnel Events.]

Related Documentation

- Changes in Behavior and Syntax on page 12
- Known Behavior on page 14
- Known Issues on page 16
- Resolved Issues on page 21
- Documentation Updates on page 27
- 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 12.3X48-D10.

IP Tunneling Screen

- Starting with Junos OS Release 12.3X48-D10, the syslog messages **RT_SCREEN_IP** and **RT_SCREEN_IP_LS** for the IP tunneling screen have been updated to include the tunnel screen attacks and log-without-drop criteria. The following list illustrates some examples of these new system log messages for each of the tunnel types:
  - **RT_SCREEN_IP: Tunnel GRE 6in4! source: 12.12.12.1, destination: 11.11.11.1, zone name: untrust, interface name: ge-0/0/1.0, action: alarm-without-drop**
  - **RT_SCREEN_IP: Tunnel GRE 6in6! source: 1212::12, destination: 1111::11, zone name: untrust, interface name: ge-0/0/1.0, action: drop**
  - **RT_SCREEN_IP: Tunnel GRE 4in4! source: 12.12.12.1, destination: 11.11.11.1, zone name: untrust, interface name: ge-0/0/1.0, action: drop**
  - **RT_SCREEN_IP_LS: [lsys: LSYS1] Tunnel GRE 6in4! source: 12.12.12.1, destination: 11.11.11.1, zone name: untrust, interface name: ge-0/0/1.0, action: alarm-without-drop**
  - **RT_SCREEN_IP_LS: [lsys: LSYS1] Tunnel GRE 6in6! source: 1212::12, destination: 1111::11, zone name: untrust, interface name: ge-0/0/1.0, action: drop**
  - **RT_SCREEN_IP_LS: [lsys: LSYS1] Tunnel GRE 4in4! source: 12.12.12.1, destination: 11.11.11.1, zone name: untrust, interface name: ge-0/0/1.0, action: drop**

Network Time Protocol

- Starting in Junos OS Release 12.3X48-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 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

- Maximum number of pre-authentication SSH packets—Starting with Junos OS Release 12.3X48-D10, you can limit the number of pre-authentication SSH packets that the SSH server will accept prior to user authentication. Use the **set system services ssh max-pre-authentication-packet *value*** command to set the maximum number of pre-authentication SSH packets that the server will accept.
- 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.

VPNs

- Starting with Junos OS Release 12.3X48-D10, multicast traffic is no longer supported on secure tunnel (st0) interfaces in Protocol Independent Multicast (PIM) point-to-multipoint mode.

  AutoVPN hubs are supported on SRX240, SRX550, SRX650, SRX1400, SRX3400, SRX5600, and SRX5800 devices. AutoVPN spokes are supported on SRX100, SRX210, SRX220, SRX240, SRX550, SRX650, and SRX1400 devices.

- Starting with Junos OS Release 12.3X48-D10, you no longer have to configure exactly matching traffic selectors on both the IKE initiator and responder. During IKE negotiation, the responder can accept from the initiator a proposed traffic selector that is a subset of the traffic selector configured on the responder. Traffic selector flexible matches are supported for both IKEv1 and IKEv2.

- Starting with Junos OS Release 12.3X48-D10, a single traffic selector configuration can result in multiple tunnels related to that traffic selector; this is referred to as multi-SA.

Related Documentation

- New and Changed Features on page 4
- Known Behavior on page 14
- Known Issues on page 16
- Resolved Issues on page 21
- Documentation Updates on page 27
- 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 12.3X48-D10.

Application Layer Gateways (ALGs)

- On all SRX Series devices, you can define the Sun RPC and MS RPC mapping entry ageout value using the **set security alg sunrpc map-entry-timeout *value*** and **set security alg msrpc map-entry-timeout *value*** commands. The ageout value ranges from 1 hour to 72 hours, and the default value is 32 hours.

  If either the Sun RPC ALG or the MS-RPC ALG service does not trigger the control negotiation even after 72 hours, the maximum RPC ALG mapping entry value times out and the new data connection to the service fails.

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.

General Packet Radio Service (GPRS)

- On all high-end SRX Series devices, unified ISSU is supported from Junos OS Release 12.1X45 to Junos OS Release 12.1X46 and from Junos OS Release 12.1X46 to Junos OS Release 12.3X48-D10. Unified ISSU is not supported from Junos OS Release 12.1X45 to Junos OS Release 12.3X48-D10.

Layer 2 Features

- On all branch SRX Series devices, you cannot configure Ethernet switching and virtual private LAN service (VPLS) using mixed mode (Layer 2 and Layer 3).
- On all branch SRX Series devices, you must reboot the device when you configure bridge domain if the bridge domain was not already configured on the device.
- On all high-end SRX Series devices, you do not have to reboot the device when you configure bridge domain.
- On all branch SRX Series devices, configuring 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>***

VPNs

- On SRX Series devices, configuring XAuth with AutoVPN secure tunnel (st0) interfaces in point-to-multipoint mode and dynamic IKE gateways is not supported.
- On all SRX Series devices, the **disable** option is not supported on secure tunnel (st0) interfaces.
- RIP is not supported in point-to-multipoint (P2MP) VPN scenarios including AutoVPN deployments. We recommend OSPF or IBGP for dynamic routing when using P2MP VPN tunnels.

Related Documentation

- New and Changed Features on page 4
- Changes in Behavior and Syntax on page 12
- Known Issues on page 16
- Resolved Issues on page 21
- Documentation Updates on page 27
- Migration, Upgrade, and Downgrade Instructions on page 28

Known Issues

This section lists the known issues in hardware and software in Junos OS Release 12.3X48-D10.

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 high-end SRX Series devices, when you disable the services offloading feature, a warning message that the device will reboot is not generated. PR748673
- On SRX5600 devices in a chassis cluster, when the telnet program is running on either the primary or secondary Routing Engine connecting to SPUs on the Packet Forwarding Engine (PFE) side, the connection gets stuck because an incorrect source IP is used by the telnet program in the multichassis environment. When the connection gets stuck, specify the local chassis IP by using **-s** parameter as its source IP for the telnet program to connect to SPUs. PR923782
- On all branch SRX Series devices, the secondary node in a chassis cluster environment might crash or go into DB mode because of panic: rnh_index_alloc after frequent failover when IPsec with multipoint st0 interfaces are configured. This issue occurs when the st0 interface is in multipoint or point-to-multipoint (P2MP) mode. PR917719
- On all SRX Series devices, when you perform an in-service software upgrade (ISSU) from one Junos OS release version to another, the following error messages are displayed:

  Network security daemon: rtslib: ERROR kernel does not support all messages: expected 102 got 98, a reboot or software upgrade may be required

  Network security daemon: rtslib: WARNING version mismatch for msg unknown: expected 98 got 0, a reboot or software upgrade may be required

  These error messages are harmless and are generated during image checking, and the messages do not impact the ISSU. PR926661

CLI

- On all SRX Series devices, the output of the **show interfaces detail** and **show interfaces extensive** CLI commands for the SHDSL interface in EFM mode might not be displayed. PR1051641

Flow-based and Packet-based Processing

- On all branch SRX Series devices, reduced flow and packet performance and a drop in GRE and GRE IPsec are observed. PR682501
- On all branch SRX Series devices, IPsec tunnel reconnection might cause a memory leak.

As a workaround, upgrade to Junos OS Release 12.1X46-D35 and reduce the number of IPsec tunnel reconnections. PR1002738

Installation and Upgrade

- On SRX100, SRX110, SRX210, and SRX220 devices with 2-GB RAM (for H2/HE2 models), software upgrade to Junos OS Release 12.3X48-D10 fails if the upgrade is done from a release earlier than Junos OS Release 12.1X44-D40, 12.1X45-D30, or 12.1X46-D25. The following error message is displayed:

  WARNING: Package 12.3X48-Dxx is not compatible with this hardware

  As a workaround, you must upgrade to Junos OS Release 12.1X44-D40, 12.1X45-D30, 12.1X46-D25, 12.1X47-D10, or later and then upgrade to Junos OS Release 12.3X48-D10.

  Refer https://kb.juniper.net/tsb16646.

  PR987067

Interfaces and Routing

- On all SRX Series devices, when you connect to the device through wireless AP the secure access port incorrectly allows access to the MAC addresses that are not in the list of allowed MAC addresses. PR587163
- On all high-end SRX Series devices, LAG interface gratuitous ARP is neither generated nor sent out on the link when **gratuitous-arp-on-ifup** is configured. PR889851
- On all SRX Series devices, SFP interfaces ge-0/0/7, ge-0/0/8, and ge-0/0/9 on the 1-Gigabit Ethernet SYSIO card auto-negotiate to 10 gigabits per second. PR946581
- On SRX100H2 and SRX220H2 devices, when you enable vlan tagging on interfaces and commit the configuration, the interface speed and duplex mode might cause the interface to stop processing traffic. As a workaround, deactivate and then activate the affected interface. PR1003423
- On all high-end SRX Series devices, during route deletion on Packet Forwarding Engine, next-hop entries might not be deleted, these stale next-hops may continue to be used by sessions resulting in flowd process crash. PR1017037
- On all branch SRX Series devices, after enabling IEEE 802.1X, the connected devices on some ports might fail to be authenticated due to MAC authentication requests held on the eswd process. This issue might be seen on certain random ports, not all ports. PR1042294
- On SRX210 devices, when the device is configured over 200 VRRP groups, the Routing Engine CPU is very busy and you cannot run the VRRP show command, because it leads to a timeout error message. We recommend that you increase the advertisement interval of the VRRP PDU so that the pressure on the Routing Engine CPU is reduced. PR1054359
- On all branch SRX Series devices, VPLS session state is stuck in standby connection while testing VPLS over GRE over IPsec. PR1059801

- On all branch SRX Series devices, when interface monitor is enabled, the ppo.0 interface becomes inactive after disabling the reth interface. PR1060590
- On all branch SRX Series devices, when the speed of the physical member interfaces is 100 Mbps, you cannot ping to the reth interface.

  As a workaround, disable and reenable the member interface, and then the ping to the reth interface will be successful. PR1060633
- On all branch SRX Series devices, you must configure the **forwarding-options sampling** or **forwarding-options packet-capture** option before enabling sampling on interfaces. PR1063002

Intrusion Detection and Prevention (IDP)

- On all branch SRX Series devices, when IDP and Express Anitvirus (EAV) are configured under very high stress, application traffic might coredump. PR1019401
- On all branch SRX Series devices, severity for the IDP report changes from log severity to threat severity. PR1040118
- On all SRX Series devices, an active IDP session might not be fetched by the **show security flow session idp** and **show security flow session summary idp** commands. This issue occurs only when both IDP and AppID are enabled. PR1045587

J-Web

- On all branch SRX Series devices, when you configure the J-Web setup wizard while creating a new configuration and apply the configuration, the changes are not reflected on all devices, As a result, the device displays the configuration change alert and sends a message for you to commit the configuration.

  As a workaround, when you configure the J-Web setup wizard while creating a new configuration, you must perform a commit operation after applying the configuration. PR1058434

Logical Systems

- On SRX3600 devices, logical systems with the policy count option displayed the statistics after a **show** command, or the counter stopped incrementing if both redundant groups were not on the same node as a result of failover. PR782546

MIBs

- On all high-end SRX Series devices, there are compilation issues with the mib-jnx-license, mib-jnx-sp-nat, and mib-jnx-subscriber MIBs. PR794327

Network Address Translation (NAT)

- On all SRX Series devices, H245 address payload on H323 ALG **CS:Alerting** and **CS:Connect** messages are not translated for traffic with static NAT on the ALG. PR1022197

Platform and Infrastructure

- On all high-end SRX Series devices, when use multicast and there are more than 600 copies of a multicast packet for a multicast group, the flowd process might crash while committing a change of multicast configuration. PR986592

System Logging

- On all branch SRX Series devices, when you configure the TCP connections of the system log stream with a value greater than 1 (for example, a value of 3), fail over the redundancy groups, clear the log connections, and re-create the TCP log connections, the TCP connections value is decremented, and the value is reduced to 2. PR1038113
- On all SRX Series devices, user/role information is not populated in IP-Action logs. The user/role information is populated in Attack logs. PR1055075

Unified Threat Management (UTM)

- On all high-end SRX Series devices, network processor offloading and Unified Threat Management (UTM) cannot coexist at the same time. Network processor offloading is disabled automatically when UTM is enabled. This issue occurs due to a memory capacity limitation. PR1059527

VPNs

- On all branch SRX Series devices, in dynamic VPN setup, when Junos Pulse clients are connected to the device the clients are authenticated successfully and will receive IP address information from the device. But, the clients will not receive the secondary DNS information even though the secondary DNS information is configured on the device. PR1016125
- On all high-end SRX Series devices, when using point-to-multipoint (P2MP) automatic NHTB IPsec tunnels, routes using next-hop IP that is in the st0.x subnet are incorrectly marked as active prior to the VPN tunnel establishment. PR1042462

Related Documentation

- New and Changed Features on page 4
- Changes in Behavior and Syntax on page 12
- Known Behavior on page 14
- Resolved Issues on page 21
- Documentation Updates on page 27
- Migration, Upgrade, and Downgrade Instructions on page 28

Resolved Issues

This section lists the issues fixed in hardware and software in Junos OS Release 12.3X48-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 all SRX Series devices with the SIP ALG and NAT enabled, if you place a call on hold or off hold many times, each time with different media ports, the resource in the call is used, resulting in one-way audio. Tearing down the call clears the resource, and following calls are not affected. PR1032528
- On all SRX Series devices with MSRPC ALG enabled, the flowd process might crash when ALG processes the MSRPC traffic which contains invalid Class IDs (CLSIDs) and unknown interface IDs (IIDs). PR1036574
- On all SRX Series devices with the SIP ALG and NAT enabled, the SIP ALG does not execute IP translation for the retransmitted 183 session progress messages. In this scenario, the SIP call will fail when the device receives the first 183 session progress messages without SDP information, but the retransmitted 183 session progress messages contains SDP information. PR1036650
- On all SRX Series devices, the DNS ALG does not terminate the session when a truncated DNS reply is received, so the session remains active until high timeout of 10~50 is reached. PR1038800
- On all branch SRX Series devices, SIP ALG code has been enhanced to support RFC 4566 regarding the SDP lines order and to avoid issues of no NAT in owner filed (O line) in some circumstances. PR1049469

Chassis Cluster

- On all high end SRX Series devices configured in a chassis cluster, after performing an ISSU upgrade on a chassis cluster containing IDP detector configuration, the FPCs on one node might remain in offline state. PR920216
- On SRX5400, SRX5600, and SRX5800 devices with SPC II cards installed, when IP spoofing is enabled, after the device under test (DUT) is rebooted, the address books in the Packet Forwarding Engine will be removed and not pushed back into the Packet Forwarding Engine. Due to this issue, IP spoofing does not work after the reboot. PR1025203
- On SRX Series devices in chassis cluster Z mode (except SRX110 device), if static NAT or destination NAT is configured, and in the NAT rule the IP address of the **incoming interface** is used as a matching condition for the **destination-address**, then the traffic matching the NAT rule is discarded. PR1040185
- On all high-end SRX Series devices in chassis cluster mode when the mbuf usage is more than 80 percent, the device will automatically fail over. To avoid UTM

traffic-overwhelmed system mbuf usage on the device, UTM function will be not enabled on the new session when system buf usage is as high as 75 percent. When usage is down, UTM function could still continue to run on the new session. PR1035986

- On all SRX Series devices in chassis cluster mode, during control plane RG0 failover, a policy resynchronisation operation compares the policy message between the Routing Engine and the Packet Forwarding Engine. However, some fields in the security policy data message are not processed. Data for unprocessed fields might be treated differently and cause the flowd process to crash. PR1040819

CLI

- On all SRX Series devices, the configurations of group junos-defaults are lost after a configuration rollback. As a result, the **commit** command fails. PR1052925

Dynamic Host Configuration Protocol (DHCP)

- On all SRX Series devices configured as a DHCP server (using the jdhcpd process), when the DHCP server gets a new request from a client and applies an IP address from the authentication process (authd), the jdhcpd process communicates with authd twice as expected (once for the DHCP discovery message and once for the DHCP request message). If the authentication fails in the first message, the authd process will indefinitely wait for the second authentication request. However, the jdhcpd process never sends the second request, because the process detects that the first authentication did not occur. This causes memory leak on the authd process, and the memory might get exhausted, generating a core file and preventing DHCP server service. High CPU usage on the Routing Engine might also be observed. PR1042818

Flow-Based and Packet-Based Processing

- On all SRX Series devices, after a failover, there is a reroute process for each existing session on the newly active device. The reroute is delayed and is triggered by the first packet hitting an existing session. If multiple packets of the same session come in at once, and are picked up by different threads for processing, only one thread will run the reroute, while the other threads have to wait for the result before forwarding the packet. This waiting period penalizes traffic for other sessions and affects the overall throughput. Therefore, such packets will be dropped instead of waiting in order to optimize the overall system fairness and throughput. This drop does not affect newly created sessions, because that is a different data path. PR890785
- On all SRX Series devices, when composite next hop is used, RSVP session flap might cause an ifsate mismatch between the master Routing Engine and the backup Routing Engine, leading to a kernel crash on the master Routing Engine. PR905317
- On all SRX Series devices, when you configure **http-get** RPM probes to measure the website response, the probes might fail because the HTTP server might incorrectly interpret the request coming from the device. PR1001813
- On all branch SRX Series devices, I2C bus might hang due to read and write error with the same mutex and the following alarm message is displayed:

  2014-06-26 00:18:23 SAST Major SRXSME Chassis Fan Tray Failure

2014-06-26 00:17:46 SAST Minor PEM 1 Absent
2014-06-26 00:17:46 SAST Minor PEM 0 Absent

PR1006074

- On all branch SRX Series devices, the USB modem link goes down if you configure the init-command-string **\n** to **** and **n** 2 characters. PR1020559
- On all multiple thread-based SRX Series devices (SRX240 and above), if IDP, AppSecure, ALG, GTP, or the SCTP feature, which is required for serialization flow processing is enabled, the device might encounter an issue where two flow threads work on the same session at the same time for the serialization flow processing. This issue might cause memory corruption, and then result in a flowd process crash. PR1026692
- On all high-end SRX Series devices, when you forward traffic, a flowd core file is generated. PR1027306
- On all branch SRX Series devices, when you enable **flexible-vlan-tagging**, the return traffic might be dropped on the tagged interface with the following message: **packet dropped, pak dropped due to invalid l2 broadcast/multicast addr**". PR1034602
- On all SRX Series devices, when WebTrends Enhanced Log File (WELF) format is configured for the security log, the device generates very long WELF-formatted logs (for example, logs more than 1000 bytes). When the log is truncated on the Packet Forwarding Engine and sent to the Routing Engine, memory corruption occurs, causing the flowd process to crash. This issue generally occurs when UTM Web filtering is configured. PR1038319
- On all SRX Series devices, when a primary IP address of an interface changes, some IPsec tunnels terminated on that interface might go down. PR1044620

Hardware

- On all branch SRX Series devices, the message **twsi0: Device timeout on unit 1** fills the console on soft reboot. PR1050215

Installation and Upgrade

- On SRX650 devices, if the u-boot revision is 2.5 or later, installing the Junos OS release image from TFTP in loader mode fails. PR1016954
- On all high-end SRX Series devices, AES-GCM is not compatible with previous Junos OS releases. After you upgrade the Junos OS release on the VPN node (SRX Series device), the VPN tunnel that uses AES-GCM for encryption might not reboot. PR1037432

Interfaces and Routing

- On all branch SRX Series devices configured as a CHAP authentication client, in a PPPoE over ATM LLC encapsulation scenario, the connection might not be established because of an incorrect sequence of messages being exchanged with the second LNS. PR1027305
- On SRX210 and SRX220 devices, broadcast packets might not be sent to the Routing Engine after system initialization. PR1029424
- On all SRX Series devices, PIM register messages are not sent from the outgoing interface because the wrong outgoing interface is selected during route lookup. PR1031185
- On SRX1400, SRX3400, and SRX3600 devices, memory leak occurs on the Control Plane Processor (CPP) logical interfaces are deleted and the interprocess communication messages are received by the CPP. High memory usage on the CPP might be seen in an interface flapping situation. PR1059127

J-Web

- On all branch SRX Series devices, J-Web sets a limitation on the size of the configuration fetched from a device to avoid memory exhaustion. When the configuration size exceeds this limitation, J-Web fails to load the configuration on Junos OS Release 12.3X48-D10. PR1037073
- On all branch SRX Series devices, security policy log or security policy count is not displayed when the match condition is **RT_FLOW_SESSION**. PR1056947

Layer 2 Transparent Mode

- On all SRX Series devices in Layer 2 transparent mode, the flowd process might generate a core file when two packets of the same connection are received in a short time before the flow session is created, and destination MAC address lookup succeeds for these two packets. PR1025983

Network Address Translation (NAT)

- On all SRX Series devices, when source NAT is configured, the ports are allocated randomly by default. In rare circumstances, the global random port table of source pools or interfaces becomes damaged by certain services or traffic. This damage can result in low-range ports being assigned a higher priority in sessions. Ports might be reused quickly, causing application access failure. PR1006649
- On all SRX Series devices, when persistent NAT is enabled, allocation of resource (port) for an incoming session failed. The session reference count for that binding increases constantly even if no more sessions are associated with it. This results in stale entries in the persistent NAT binding table, which causes persistent NAT table exhaustion. PR1036020

Security

- OpenSSL released a Security Advisory that included CVE-2014-3566 known as the "POODLE" vulnerability. The SSL protocol 3.0 (SSLv3) uses nondeterministic CBC padding, which makes it easier for man-in-the-middle attackers to obtain clear text data through a padding oracle attack. OpenSSL is upgraded to support for SSL 3.0 fallback protection (TLS_FALLBACK_SCSV). Refer to JSA10656 for more information. PR1033938

System Logging

- On all high-end SRX Series devices, if the stream mode logging has incomplete configuration for multiple streams, after reboot the system might not send out stream logs to the properly configured streams. PR988798

Unified Threat Management (UTM)

- On all SRX Series devices, when UTM Sophos antivirus is enabled and a file that is not supported by Sophos antivirus is transferred through SMTP, the device might not be able to handle the last packet, and mail will be on hold. When packets are later sent on this session, the packet that was on hold will be handled by the device and the system will return to normal state. PR1049506

VPNs

- On all SRX Series devices, a certificate-based IKEv2 tunnel cannot be set up if remote identity is configured as wildcard (*) for the IKE gateway. PR968614
- On SRX Series devices with IPsec VPN configured using IKEv1, the device can hold only two pairs of IPsec SA per tunnel. When the third IPsec SA rekey occurs, the oldest IPsec SA is deleted. Due to this mechanism, a looping of IPsec SA rekey might occur. For example, when a VPN peer contains incorrect configuration that has more than two proxy IDs matching only one proxy ID on a device, the rekey looping issue might cause the flowd process to crash on multiple thread-based SRX Series platforms (SRX240 devices and higher). PR996429
- On all branch SRX Series devices, in group VPN setups, all the already registered members might suddenly disappear from the key server due to memory leak. PR1023940
- On all branch SRX Series devices, when IPsec VPN is enabled using IKE version 2 and a distinguished name is used to verify the IKEv2 phase 1 remote identity, a remote peer initiates IKEv2 Phase 1 Security Association (SA) renegotiation (SRX Series devices work as responders), the new negotiated VPN tunnel might stay in "inactive" state on the data plane, causing IPsec VPN traffic loss. PR1028949

- On all branch SRX Series devices in a Dynamic End Point (DEP) VPN scenario, the VPN tunnel might stay in down state after you change the user-at-hostname value. PR1029687
- On all branch SRX Series devices, when you reboot the device in an AutoVPN configuration mode, the VPN tunnel does not come up and reports a private key error message. PR1032840

Related Documentation

- New and Changed Features on page 4
- Changes in Behavior and Syntax on page 12
- Known Behavior on page 14
- Known Issues on page 16
- Documentation Updates on page 27
- Migration, Upgrade, and Downgrade Instructions on page 28

Documentation Updates

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

IPsec VPN Feature Guide for Security Devices

- The traffic selector feature referred to as reverse route insertion (RRI) is now called auto route insertion (ARI). ARI is the automatic insertion of a static route based on the remote IP address configured in a traffic selector.

  [See Understanding Auto Route Insertion.]

Various Guides

- Some Junos OS user, reference, and configuration guides—for example the Junos Software Routing Protocols Configuration Guide, Junos OS CLI User Guide, and Junos OS System Basics Configuration Guide—mistakenly do not indicate SRX Series device support in the "Supported Platforms" list and other related support information; however, many of those documented Junos OS features are supported on SRX Series devices. For full, confirmed support information about SRX Series devices, please refer to Feature Explorer at http://pathfinder.juniper.net/feature-explorer/.

Related Documentation

- New and Changed Features on page 4
- Changes in Behavior and Syntax on page 12
- Known Behavior on page 14
- Known Issues on page 16
- Resolved Issues on page 21
- 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.

NOTE: Upgrading to Junos OS Release 12.1X47-D10 or later is not supported on the J Series devices or on the versions of the SRX100 and SRX200 lines with less than 2GB memory. If you attempt to upgrade one of these devices to Junos OS 12.1X47-D10 or later, installation will be aborted with the following error message:

ERROR: Unsupported platform <platform-name >for 12.1X47 and higher

For more information, refer to the Knowledge Base article at http://kb.juniper.net/TSB16632.

- Upgrading and Downgrading Among Junos OS Releases on page 29
- Upgrading an AppSecure Device on page 31
- Network and Security Manager Support on page 31
- Upgrade and Downgrade Scripts for Address Book Configuration on page 31

Upgrading and Downgrading Among Junos OS Releases

All Junos OS releases are listed in sequence on the JUNOS Software Dates & Milestones webpage:

http://www.juniper.net/support/eol/junos.html

To help in understanding the examples that are presented in this section, a portion of that table is replicated here. See Table 1 on page 29. Note that releases footnoted with a 1 are Extended End-of-Life (EEOL) releases.

Table 1: Junos Software Dates & Milestones

Product	FRS Date
Junos 12.3X48[1]	03/06/2015
Junos 12.1X47[2]	08/18/2014
Junos 12.1X46[123]	12/30/2013
Junos 12.1X45[2]	07/17/2013
Junos 12.1X44[12]	01/18/2013
Junos 12.1	03/28/2012
Junos 11.4[1]	12/21/2011
Junos 11.3	08/15/2011
Junos 11.2	08/03/2011
Junos 11.1	03/29/2011
Junos 10.4[1]	12/08/2010
Junos 10.3	08/15/2010
Junos 10.2	05/28/2010
Junos 10.1	02/15/2010
Junos 10.0[1]	11/04/2009
Junos 9.6	08/06/2009
Junos 9.5	04/14/2009
Junos 9.4	02/11/2009

Table 1: Junos Software Dates & Milestones *(continued)*

Product	FRS Date
Junos 9.3[1]	11/14/2008
Junos 9.2	08/12/2008
Junos 9.1	04/28/2008
Junos 9.0	02/15/2008
Junos 8.5[1]	fwd-srns-context

You can directly upgrade or downgrade between any two Junos OS releases that are within three releases of each other.

- Example: Direct release upgrade

  Release 10.3 → *(bypassing Releases 10.4 and 11.1)* Release 11.2

To upgrade or downgrade between Junos OS releases that are more than three releases apart, you can upgrade or downgrade first to an intermediate release that is within three releases of the desired release, and then upgrade or downgrade from that release to the desired release.

- Example: Multistep release downgrade

  Release 11.3 → *(bypassing Releases 11.2 and 11.1)* Release 10.4 → Release 10.3

Juniper Networks has also provided an even more efficient method of upgrading and downgrading using the Junos OS EEOL releases. EEOL releases generally occur once a calendar year and can be more than three releases apart. For a list of, EEOL releases, go to http://www.juniper.net/support/eol/junos.html.

You can directly upgrade or downgrade between any two Junos OS EEOL releases that are within three EEOL releases of each other.

- Example: Direct EEOL release upgrade

  Release 9.3 (EEOL) → *(bypassing Releases 10.0 [EEOL] and 10.4 [EEOL])* Release 11.4 (EEOL)

To upgrade or downgrade between Junos OS EEOL releases that are more than three EEOL releases apart, you can upgrade first to an intermediate EEOL release that is within three EEOL releases of the desired EEOL release, and then upgrade from that EEOL release to the desired EEOL release.

- Example: Multistep release upgrade using intermediate EEOL release

  Release 8.5 (EEOL) → *(bypassing Releases 9.3 [EEOL] and 10.0 [EEOL])* Release 10.4 (EEOL) → Release 11.4 (EEOL)

You can even use a Junos OS EEOL release as an intermediate upgrade or downgrade step if your desired release is several releases later than your current release.

- Example: Multistep release upgrade using intermediate EEOL release

  Release 9.6 → Release 10.0 (EEOL) → Release 10.2

For additional information about how to upgrade and downgrade, see the *Junos OS Installation and Upgrade Guide*.

Upgrading an AppSecure Device

Use the no-validate Option for AppSecure Devices.

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.

Network and Security Manager Support

Network and Security Manager (NSM) support for SRX Series Services Gateways with Junos OS 12.3X48-D10 is available only with NSM versions 2012.2R6 / 2012.1R10 and later. For additional information, see Network and Security Manager documentation.

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 33).

- About Upgrade and Downgrade Scripts on page 32
- Running Upgrade and Downgrade Scripts on page 33
- Upgrade and Downgrade Support Policy for Junos OS Releases and Extended End-Of-Life Releases on page 34

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.

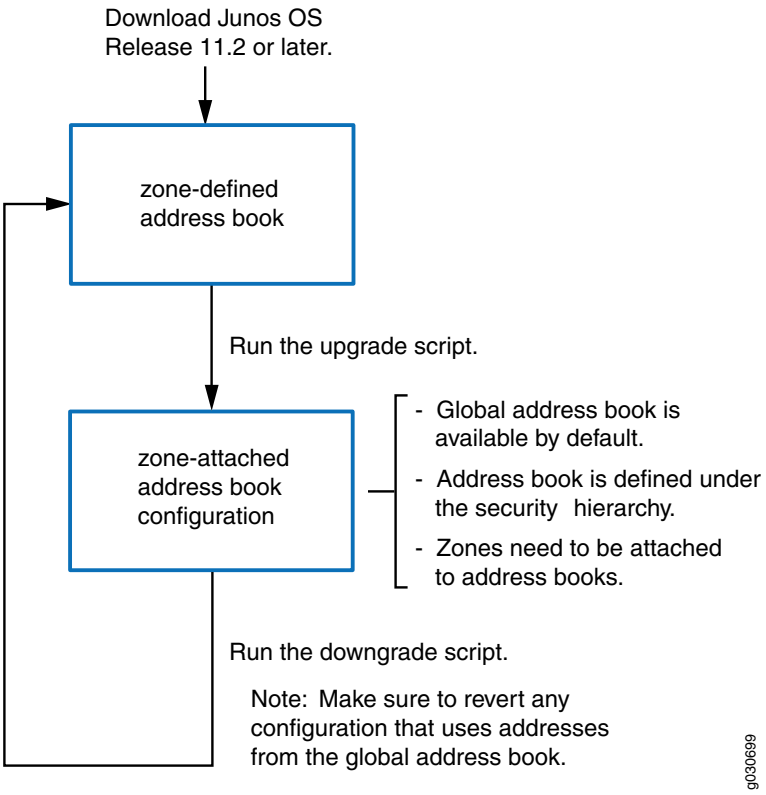
  After upgrading to the zone-attached address book configuration:

  - 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.

Related Documentation

- New and Changed Features on page 4
- Changes in Behavior and Syntax on page 12
- Known Behavior on page 14
- Known Issues on page 16
- Resolved Issues on page 21
- Documentation Updates on page 27

Product Compatibility

- Hardware Compatibility on page 34
- Transceiver Compatibility for SRX Series Devices on page 35

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 http://www.juniper.net/techpubs/feedback/. If you are using e-mail, be sure to include the following information with your comments:

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

Requesting Technical Support

Technical product support is available through the Juniper Networks Technical Assistance Center (JTAC). If you are a customer with an active J-Care or JNASC support contract, or are covered under warranty, and need postsales 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/.

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

16, September 2015—Revision 5— Junos OS 12.3X48-D10 – SRX Series.

25, June 2015—Revision 4— Junos OS 12.3X48-D10 – SRX Series.

15, April 2015—Revision 3— Junos OS 12.3X48-D10 – SRX Series.

18, March 2015—Revision 2— Junos OS 12.3X48-D10 – SRX Series.

05, March 2015—Revision 1— Junos OS 12.3X48-D10 – SRX Series.