Release Notes: Junos® OS Release 15.1X49-D100 for the SRX Series

Release 15.1X49-D100
28 January 2019
Revision 4

Contents

Introduction

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

These release notes accompany Junos OS Release 15.1X49-D100 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/documentation/software/junos/.

NOTE: Junos OS Release 15.1X49-D100 supports the following devices: SRX300, SRX320, SRX340, SRX345, and SRX550 High Memory (SRX550M), SRX1500, SRX4100, SRX4200, SRX5400, SRX5600, and SRX5800 devices with host subsystems composed of either an SRX5K-RE-1800X4 (RE2) with an SRX5K-SCBE (SCB2), or an SRX5K-RE-1800X4 (RE2) with an SRX5K-SCB3 (SCB3), and vSRX.

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

New and Changed Features

This section describes the new features and enhancements to existing features in Junos OS Release 15.1X49-D100 for the SRX Series devices.

Release 15.1X49-D100 Software Features

AppSecure

- **AppTrack enhancements to support APBR for SRX Series devices and vSRX instances**—Starting from Junos OS Release 15.1X49-D100, the AppTrack feature is enhanced to include advanced policy-based routing (APBR) details. AppTrack, an application tracking tool, collects byte, packet, and duration statistics for application flows in the specified zone. As a part of the enhancement to support APBR, AppTrack syslog message now include destination interface details. A new AppTrack syslog message is introduced to include APBR profile, rule, and routing instance details. This message is generated for the session when APBR is applied to the session.

  In addition, the **show security application-tracking counters** command, which displays AppTrack counters, is updated to include a new counter to indicate the number of times a new route update log is generated.

  [See show security application-tracking counters and Understanding AppTrack.]

- **New cipher support on SSL proxy on SRX340, SRX345, SRX550M, SRX1500, SRX4100, SRX4200, SRX5400, SRX5600, and SRX5800 devices, and vSRX instances**—Starting in Junos OS Release 15.1X49-D100, new ECDHE (Elliptic Curve DHE) ciphers and RSA ciphers are introduced along with the existing ciphers in SSL proxy. Newly added ECDHE ciphers are supported to enable the Perfect Forward Secrecy (PFS) on SSL proxy.

  [See SSL Proxy Overview.]

Class of Service (CoS)

- **Support for port-based egress traffic shaping and policing on SRX Series devices**—Starting with Junos OS Release 15.1X49-D100, you can configure egress traffic shaping and policing at the physical port level, which limits the egress traffic rate of all logical interfaces on the port.

  [See shaping-rate (CoS Interfaces).]

- **Support for CoS on dl0 Interface on SRX320, SRX340, SRX345, and SRX550M devices**— Starting with Junos OS Release 15.1X49-D100, you can configure the following class of service (CoS) features on the dl0 interface for 4G wireless modems: behavior aggregate classifiers, multifield classifiers, policers, shapers, schedulers, and rewrite rules. The dialer interface, dl0, is a logical interface for configuring properties for modem connections.

  [See LTE Mini-PIM Overview.]

- **Support CoS on Logical Tunnel Interface in a Chassis Cluster on SRX300, SRX320, SRX340, SRX345, and SRX550M devices**— Starting with Junos OS Release 15.1X49-D100, queuing is supported on logical tunnel (LT) interfaces to allow CoS configuration.

  [See Class of Service.]

Dynamic Host Configuration Protocol (DHCP)

- **DHCPv6 enhancements to support RFC 6177 for SRX Series devices**— Starting with Junos OS Release 15.1X49-D100, new CLI commands are introduced to configure preferred prefix length and sub-prefix length in clients. A delegating router (DHCPv6 server) is provided with IPv6 prefixes and a requesting router (DHCPv6 client) requests one or more prefixes from the delegating router. When the client receives a valid DHCPv6 block it must then delegate to all active interfaces using a sub-prefix delegation.

  [See Administration Guide.]

Flow and Processing

- **Support for distributed BFD on SRX300, SRX320, SRX340, SRX345, and SRX1500**—Starting with Junos OS Release 15.1X49-D100, distributed Bidirectional Forwarding Detection (BFD) is supported. The distributed BFD protocol is a simple hello mechanism that detects failures in a network. Hello packets are sent at a specified, regular interval. A neighbor failure is detected when the routing device stops receiving a reply after a specified interval.

  The support for distributed BFD results in the following session scaling improvements:

  1. Up to four sessions on SRX300 and SRX320 devices
  2. Up to 50 sessions on SRX340 and SRX345 devices
  3. Up to 120 sessions on SRX1500 devices

  The supported failure detection interval has improved.

  To enable distributed BFD on the SRX340, SRX345, and SRX1500, use the **set chassis dedicated-ukern-cpu** command.

  To enable distributed BFD on the SRX300 and SRX320, use the **set chassis realtime-ukern-thread** command.

  [See Understanding BFD for Static Routes for Faster Network Failure Detection, Understanding Distributed BFD, dedicated-ukern-cpu (BFD), and realtime-ukern-thread (BFD).]

- **Preserving incoming fragment characteristics for SRX Series devices**—Starting in Junos OS Release 151.X49-D100, you can enable this feature to diminish the likelihood of packet fragmentation in the downstream data path. When the SRX Series device receives packet fragments, it must reassemble them into the whole datagram for application layer inspection. Before the datagram is transmitted, it must be broken down again into fragments. If this feature is enabled, the SRX Series device takes into account the characteristics of incoming fragments when setting the egress interface

maximum transmission unit (MTU) size. It identifies the maximum fragment size of all incoming fragments. It uses that information in conjunction with the existing MTU of the egress interface. The SRX Series device compares the two numbers. It takes the smaller number and uses it for the egress interface MTU size.

[See Understanding How Preserving Incoming Fragmentation Characteristics Can Improve Throughput.]

GPRS

- **Support for IPv6 address validation on user equipment for SRX1500, SRX4100, SRX4200, SRX5400, SRX5600, SRX5800 devices and vSRX instances**—Starting with Junos OS Release 15.1X49-D100, the device supports IPv6 address validation on a user equipment (for example, a cellphone). The user equipment accesses data through the mobile core network, and the information is carried in the GTP tunnel by GTP-U packets. The IP address of the user equipment is allocated during the GTP user tunnel creation. User equipment supports both IPv4 and IPv6 address types.

  [See Understanding IP Address Validation on GTP.]

Installation and Upgrade

- **Support for SSD slot on SRX340, SRX345, and SRX550M devices**—Starting in Junos OS Release 15.1X49-D100, the SSD slot in the device supports adding an external SSD disk for additional storage of log messages.

  [See Hardware Overview of SRX Series Services Gateways.]

- **Zero Touch Provisioning on SRX300, SRX320, SRX340, SRX345, SRX550M, and SRX1500 devices**– Starting from Junos OS 15.1X49-D100, ZTP is supported to automate the provisioning of the device configuration and software image with little or no manual intervention.

  ZTP on SRX Series devices is responsible for the initial bootup and configuration of the device when the device is powered on. When the SRX Series device boots up with the factory-default configuration, it connects to the server over the Internet and downloads the initial configuration and the latest Junos OS image from the server. The new image is installed first and then the initial configuration is applied and committed on the SRX Series device.

  [See Configuring Zero Touch Provisioning on SRX Series Devices.]

Integrated User Firewall

- **Advanced user identity query for SRX Series devices**—Starting in Junos OS Release 15.1X49-D100, you can use the advanced user identities query feature which provides a solution that allows you to provision users locally and have their authentication information made available throughout your network for policy enforcement and reporting.

This feature:

- Relies on the Juniper Identity Management Service (JIMS) from which the SRX Series device obtains the user identity information.
- Allows you to obtain identity information for a range of users or, similar to the Aruba Clearpass query function, for an authenticated user based on the user's IP address.

[See Understanding the Advanced Query Feature for SRX Series Active Directory and Aruba ClearPass User Firewall Authentication.]

- **Timeout parameters for unauthenticated user authentication table entries for SRX Series devices**—Starting in Junos OS Release 15.1X49-D100, you can configure separate timeout values for invalid user authentication table entries. User entries for both active directory and Aruba ClearPass contain a timeout value after which the entry expires. When an invalid entry is created for an unauthenticated user attempting to log in, the current timeout value, which applies to all entries, applies to it. Active directory probes the unauthenticated user's workstation for identity information. SRX Series queries ClearPass for the authentication information. While the probe or query is taking place, the timeout value for the invalid user entry is counting down. To ensure that an invalid user entry does not expire during this period, this feature introduces new timeout parameters specifically for invalid user entries. Because they are separate features, individual entries are defined for Aruba ClearPass and for active directory. The active directory authentication table is a repository for both integrated user firewall and captive portal authentication.

  [See Understanding the Invalid Authentication Table Entry Timeout Setting.]

Interfaces

- **LTE support on SRX320, SRX340, SRX345, and SRX550M Services Gateways**—Starting with Junos OS Release 15.1X49-D100, wireless WAN connectivity over 3G and 4G/LTE networks is supported. The connectivity is provided by the LTE Mini-Physical Interface Module (Mini-PIM), which can be configured as a primary WAN or as a backup WAN to the primary wired network for the services gateways.

  [See Interfaces Feature Guide for Security Devices.]

- **MACsec support on SRX300, SRX320, SRX340 and SRX345 devices**—Starting in Junos OS Release 15.1X49-D100, Media Access Control Security (MACsec) is supported on all MACsec-capable ports of SRX300, SRX320, SRX340 and SRX345 devices.

  On SRX300 line devices MACsec is supported on the following ports:

  - SRX300 and SRX320: 2 ports (on two fixed SFP interfaces.)
  - SRX340 and SRX345: 16 ports (on eight fixed SFP interfaces + eight fixed Ethernet ports)

  [See Understanding Media Access Control Security (MACsec).]

- **PPPoE support SRX Series and vSRX instances**—Starting in Junos OS Release 15.1X49-D100, SRX series devices and vSRX support Point-to-Point Protocol over Ethernet (PPPoE). You can connect multiple hosts on an Ethernet LAN to a remote site through a single customer premises equipment (CPE) device. The hosts share a

common digital subscriber line (DSL), a cable modem, or a wireless connection to the Internet.

[See Understanding PPPoE Interfaces.]

- **RFC 4638 support for SRX300, SRX320, SRX340, SRX345, and SRX550M devices**—Starting in Junos OS Release 15.1X49-D100, you can use the PPP-Max-Payload option to override the default behavior of the PPPoE client by providing a maximum size that the PPP payload can support in both sending and receiving directions. The PPPoE server might allow the negotiation of an MRU larger than 1492 and the use of an MTU larger than 1492.

  [See Understanding MTU and MRU Configuration for PPP Subscribers.]

J-Web

- **J-Web support for Mini PIM FRU and integrated Mini PIM on SRX platforms**—Starting with Junos OS Release 15.1X49-D100, J-Web will support Mini PIM FRU and integrated Mini PIM on SRX320, SRX340, SRX345 and SRX550M, and SRX320 and SRX320 PoE platforms.
- **J-Web support for on-box reporting and other enhancements on SRX platforms**—Starting with Junos OS Release 15.1X49-D100, J-Web will support on-box reporting, such as, application and user usage, log mode stream, threat report, high risk application report, URL report, IPS report, IPS report, virus report, botnet report, advance malware report, and user Firewall. J-Web GUI is enhanced for a better user experience and new dashboard widgets are added on SRX300, SRX320, SRX340, SRX345, SRX320-poe, SRX550M, SRX1500, SRX4100, and SRX4200 platforms.

  The on-box reporting feature is enabled by default when you load the factory-default configurations on the SRX Series device with Junos OS Release 15.1X49-D100 or later.

  If you are upgrading your device from a Junos OS Release prior to Junos OS 15.1X49-D100, then the device inherits the existing configuration and the on-box reporting feature is disabled by default. You need to run the **set security log report** command and the **set security log mode stream** command to enable the on-box reporting feature on the device.

  Alternatively using J-Web, you can enable these commands in the Configure> Device Setup > Basic Settings > Logging page.
- **J-Web support for SSL Proxy and User Firewall on SRX platforms**—Starting with Junos OS Release 15.1X49-D100, J-Web will support SSL Proxy (SSL Forward Proxy Profile, Associate proxy profile to a security policy) and User Firewall (UserFW captive portal HTTPS redirect support, Active Directory profile) on SRX1500, SRX340, SRX345, SRX320-poe, SRX4100, and SRX4200 platforms.

Network Management and Monitoring

- **SNMP support for monitoring GRE keepalive status for all SRX Series devices and vSRX instances**—Starting with Junos OS Release 15.1X49-D100, you can monitor generic routing encapsulation (GRE) interface status using remote network management. In earlier releases, you had to use a CLI command to check GRE keepalive status. Now the SNMP MIB jnxOamMibRoot helps you to monitor GRE keepalive status using remote network management. When GRE keepalive status is changed, this SNMP MIB generates SNMP trap jnxOamGreKeepAliveTrapVars to send notifications.

  [See Enterprise-Specific SNMP MIBs Supported by Junos OS.]

System Logs

- **On-box reporting support on SRX300, SRX320, SRX340, SRX345, SRX550M, SRX1500, SRX4100, SRX4200 devices, and vSRX instances**—Starting with Junos OS Release 15.1X49-D100, the existing on-box logging functionality is modified to collect system traffic logs, analyzes the logs, and generate reports of these logs in the form of tables and graphs using the CLI.

  This feature is enabled by default when you load the factory-default configurations on the SRX Series device with Junos OS Release 15.1X49-D100 or later.

  If you are upgrading your device from a Junos OS Release prior to Junos OS 15.1X49-D100, then the device inherits the existing configuration and the on-box reporting feature is disabled by default. You need to run the **set security log report** command and the **set security log mode stream** command to enable the on-box reporting feature on the device.

  The feature allows the IT management teams to identify security information at a glance to quickly decide actions to be taken.

  [See System Log Monitoring and Troubleshooting Guide for Security.]

Unified Threat Management (UTM)

- **IPv6 support for UTM features on SRX Series devices**—Starting in Junos OS Release 15.1X49-D100, IPv6 pass-through traffic for HTTP, HTTPS, FTP, SMTP, POP3, IMAP protocols is supported for Sophos antivirus, Web filtering and Content filtering security features of UTM.

  [See Unified Threat Management Overview.]

VPN

- **Support for SSL remote access VPNs by encapsulating IPsec traffic over TCP connections on SRX5400, SRX5600, and SRX5800 devices**—Starting with Junos OS Release 15.1X49-D100, SSL VPN connections from users running third-party NCP Exclusive Remote Access Client on Windows and MAC OS devices is supported. In many public hotspot environments, UDP traffic is blocked while TCP connections are allowed. To support these environments, SRX Series devices can encapsulate IPsec messages within a TCP connection. This implementation is compatible with the NCP Exclusive Remote Access Client, which can be downloaded from https://www.ncp-e.com/ncp-exclusive-remote-access-client/. A two-user license is supplied by default on SRX Series devices; a license must be purchased and installed for additional users.

  [See Understanding SSL Remote Access VPNs with NCP Exclusive Remote Access Client.]

- **Traffic selectors supported for IKEv2 site-to-site VPNs on SRX300, SRX320, SRX340, SRX345, SRX550M, SRX1500, SRX4100, SRX4200, SRX5400, SRX5600, and SRX5800 devices and vSRX instances**—Starting with Junos OS Release 15.1X49-D100, traffic selectors can be configured with IKEv2 site-to-site VPNs. A traffic selector is an agreement between IKE peers to permit traffic through a tunnel if the traffic matches a specified pair of local and remote addresses. Only traffic that conforms to a traffic selector is permitted through a security association (SA).

  [See Understanding Traffic Selectors in Route-Based VPNs.]

Release 15.1X49-D100 Hardware Features

Hardware

- The LTE Mini-Physical Interface Module (Mini-PIM) provides LTE support on the SRX320, SRX340, SRX345, and SRX550M devices. The LTE Mini-PIM supports wireless WAN connectivity over both 3G and 4G/LTE networks, and is available in two models based on the operating region:
  - SRX-MP-LTE-AE (North America and European Union)
  - SRX-MP-LTE-AA (Asia and Australia)

  The Mini-PIM supports up to two SIM cards and can be installed in any of the Mini-PIM slots on the devices. You can configure the Mini-PIM as a primary WAN or as a backup WAN to the primary wired network.

Related Documentation

- Changes in Behavior and Syntax on page 12
- Known Behavior on page 15
- Known Issues on page 20
- Resolved Issues on page 25
- Migration, Upgrade, and Downgrade Instructions on page 32

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-D100.

Application Layer Gateways (ALGs)

- In Junos OS Release 15.1X49-D90 and earlier, on all SRX Series devices, the custom application universal unique identifier (UUID) of Microsoft remote procedure call (MS-RPC) with leading zeros and the nil UUID (00000000-0000-0000-0000-000000000000) might match all TCP traffic and referenced policies allowing all TCP traffic instead of entering MS-RPC ALG check.

  Starting with Junos OS Release 15.1X49-D100, the custom application UUID with leading zeros does not match all TCP traffic and referenced policies, which will enter MS-RPC ALG check. This new application does not allow the nil UUID.

Authentication, Authorization and Accounting (AAA)

- Starting with Junos OS Release 15.1X49-D100, the **fingerprint-hash** option is added to the [**edit system service ssh**] hierarchy. The **fingerprint-hash** option is used to configure the hash algorithm used by the SSH server when displaying key fingerprints.
- Starting with Junos OS 15.1X49-D80, the **wins-server** option at the [**edit access profile *profile-name***] hierarchy level allows you to configure the IPv4 address of a Windows Internet Name Service (WINS) server.

CLI

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

Dynamic Host Configuration Protocol (DHCP)

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

  See the following for configuration changes:

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

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

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

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

General Packet Radio Service (GPRS)

- Starting with Junos OS Release 15.1X49-D100, on SRX5400, SRX5600, and SRX5800 devices, if the GTP profile is configured then the GTP module will select the anchor SPU for distributing the UDP traffic coming on port 2123 and 2152. If you do not configure the GTP profile, then the GTP module will not work and it will not select the anchor SPU for the UDP traffic on port 2123 and 2152.

Interfaces

- Starting with Junos OS Release 15.1X49-D100, the factory-default configuration of SRX320, SRX340, SRX345, and SRX550M devices has changed to enable the devices to automatically connect to the wireless network.

  When the device with the LTE Mini-PIM installed in slot 1 is powered on, the dialer interface is triggered to dial automatically. Note that this functionality is applicable only if the Mini-PIM is installed in slot 1. If the Mini-PIM is installed in any other slot, then you will need to manually configure the **cl-*slot-number*/0/0** interface to be associated with the dialer interface.

Flow-based and Packet-based Processing

- Starting with Junos OS Release 15.1X49-D100, for the SRX100, SRX110, SRX210, SRX220, SRX240, SRX300, SRX320, SRX340, SRX345, SRX550M, and SRX650 devices, the maximum capture size for packet captures is expanded to 1520 bytes to allow for captures of 1500 bytes of data and the 12-byte Juniper Ethernet header.

Security Policies

- Starting in Junos OS Release 15.1X49-D100, a new default application, **application junos-smtps**, has been added for secured email traffic using port 587 or 465. To view the new default policy, use the **show configuration groups junos-defaults applications** command.

Software Installation and Upgrade

- The Smart Download feature is used for downloading system software images and other files to SRX Series devices. If the download encounters errors, the system automatically tries to restart after an hour and continue the download from where it stopped. Starting with Junos OS Release 15.1X49-D100, the download retry is extended from 12 hours to 336 hours (2 weeks).

Layer 2 Ethernet Services

- Starting with Junos OS Release 15.1X49-D100, on SRX300, SRX320, SRX340, SRX345, SRX550M, and SRX550M devices, the default Layer 2 global mode configuration is changed from transparent-bridge to switching mode.

NOTE: You must explicitly configure Layer 2 transparent-bridge mode for the SRX300, SRX320, SRX340, SRX345, SRX550, and SRX550M devices that work in transparent mode. Use the command **set protocols l2-learning global-mode transparent-bridge** before rebooting the devices with Junos OS 15.1X49-D100 image.

Network Address Translation (NAT)

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

Routing Protocols

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

System Services

- Starting with Junos OS Release 15.1X49-D100, you can configure the **routing-instance** option at the [**edit system name-server *x.x.x.x***] hierarchy. This allows DNS queries to be originated for a specific source address and routing instance. This configuration resolves a domain name specified in the **set security ike gateway *gateway-name* address *domain-name*** configuration to an IP address. Only one source address can be configured for each name server. A routing instance can be configured for each source address. IPv6 source addresses are only supported for IPv6 DNS servers. You cannot configure an IPv6 source address for an IPv4 DNS server or an IPv4 source address for an IPv6 DNS server.

Related Documentation

- New and Changed Features on page 5
- Migration, Upgrade, and Downgrade Instructions on page 32
- Known Behavior on page 15
- Known Issues on page 20
- Resolved Issues on page 25

Known Behavior

This section contains the known behaviors, system maximums, and limitations in hardware and software in Junos OS Release 15.1X49-D100.

Ethernet Switching

- On SRX300, SRX320, SRX340, SRX345, SRX550M, and SRX1500 devices, VPLS traffic forwarding stops working after enabling ethernet switching configuration. This is current limitation. VPLS and ethernet-switching should not be configured together on the same device on the mentioned devices. As a workaround avoid using ethernet-switching configuration on these platforms when VPLS is enabled.

Firewall Authentication

- Firewall authentication cannot retrieve domain information from access profile configuration, such that firewall authentication will not push user domain information to juniper identity management service server in case user authenticates through web-authentication, pass-through, or web-redirect with a LDAP access profile.

Flow-based and Packet-based Processing

- OSPF over GRE over IPSec is not supported on SRX platforms with standalone CP.
- Advanced anti malware (AAMW) established sessions always use the configured AAMW parameters during the time of session establishment. Configuration changes do not affect the established sessions. For example, a sessions established when the verdict threshold is 5 will always have 5 as threshold, even if the verdict threshold changes to any other values during that sessions lifetime.
- FIPS core file is seen when you perform a firmware upgrade or downgrade. In a FIPS version Junos, file integrity checking application veriexec treats the new updated firmware file as corrupted Junos file. This is an expected behavior by design.
- On SRX Series device, if advanced anti-malware service (AAMW) is enabled, and SMTP(s) is configured in the AAMW policy, and fallback permit is enabled, under the long network latency between SRX deviceand AWS running Sky ATP service, there may be a file submission time-out. When the sending timeout occurs, there is a potential chance that the e-mail sent out from Outlook might stay in the outbox of the sender, and the receiver might not receive the e-mail.
- On SRX300, SRX320, SRX340, SRX345, and SRX550M devices, after certain period of enabling dot1x, multiple first message EAP frames with the same timestamp are transmitted. However, this does not affect any dot1x functionality.
- On SRX5400, SRX5600, and SRX5800 devices, in central point architecture, system logs are sent per second per SPU. Hence, the number of SPUs define the number of system logs per second.
- On SRX340 and SRX345 devices, fabric interfaces must be configured such that the Media Access Control Security (MACsec) configurations are local to the nodes. Otherwise, the fabric link will not be reachable.

General Packet Radio Service (GPRS)

- On SRX5000 Series devices, when you use the GTP inspection feature, during an ISSU from Junos OS Release 15.1X49-D10, 15.1X49-D20, or 15.1X49-D30 to Junos OS Release 15.1X49-D40 or later, GTPv0 tunnels will not be synchronized to the upgraded node.

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

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

Integrated User Firewall

- The SRX Series integrated user firewall feature for both ClearPass and active directory authentication will manage up to 2048 sessions for each user for whom there is a user identity and authentication entry in the authentication table. There might be additional sessions associated with a user beyond the 2048 supported sessions, but they are not managed by integrated user firewall. When an authentication entry in an authentication table is deleted, integrated user firewall only closes sessions that are associated with that entry. It will not close sessions that it does not manage. That is, sessions that are not associated with the authentication entry are not closed.

Interfaces and Routing

- On SRX1500 devices, when 1G SFP-T is used on the 1G SFP ports (ge-0/0/12 to ge-0/0/15), the ge interface does not operate at 100M speed.
- On SRX320, SRX340, SRX345, and SRX550M devices with LTE Mini-Physical Interface Module (Mini-PIM) for 4G/LTE wireless connection, modem profile is not active until a profile is defined. You need to define a profile before selecting a profile.
- You cannot create profiles for CL-1/0/0 using J-Web and CLI. An error message, **Interface not found** is displayed. It is recommended to use only one LTE mPIM in the supported SRX Series devices.

J-Web

- On SRX550M and SRX1500 devices, there is no option to configure Layer 2 firewall filters from J-Web, irrespective of the device mode.
- On SRX Series devices in chassis cluster, if you want to use J-Web to configure and commit the configurations, you must ensure that all other user sessions are logged out including any CLI sessions. Otherwise, the configurations might fail.
- If 2000+ global addresses are added at a time to SSL Proxy profile exempted addresses then J-Web page does not respond.

Software Installation and Upgrade

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

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

Platform and Infrastructure

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

USB Autoinstallation

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

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

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

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

Unified Threat Management (UTM)

- Transport of IPv6 packets between the SRX Series devices and cloud servers (Sophos antivirus, Enhanced Web filtering, Websense redirect, and Antispam filtering servers) is not supported.
- Websense redirect and antispam filtering do not support IPv6 traffic.

VPN

- When there are multiple traffic selectors configured for a route-based VPN, clear traffic may enter a VPN tunnel without matching a traffic selector if the IKE gateway external interface is moved to another virtual router (VR). The software does not handle the multiple asynchronous interface events generated when an IKE gateway external interface is moved to another VR. As a workaround, first deactivate the IPsec VPN tunnel and commit the configuration without that tunnel before moving the IKE gateway external interface to another VR.
- For the **member-threshold** statement at the [**edit security group-vpn server group** ***group-name***] hierarchy level, the maximum number you can configure for a group is dependent upon the group server platform. Also, the sum of the **member-threshold** numbers for all groups configured on the group server must not exceed the capacity of the group server platform.
- When a TCP encapsulation profile is used in an IKE gateway configuration, changing the virtual router (VR) of the external interface of that IKE gateway leads to an unknown behavior which can include (but is not limited to) failure of the VPN tunnel to be brought up. As a workaround, deactivate the TCP encapsulation profile in the IKE gateway configuration before moving the external interface of the IKE gateway to another VR.
- The group VPN server daemon might generate a coredump when the group VPN server configuration is committed for the first time or when the SRX device starts up with the group VPN server configuration.
- ISSU with VPN configuration is not supported when upgrading from a Junos OS release prior to 15.1X49-D75 to Junos OS Release 15.1X49-D75 and later releases. You can use ISSU with VPN configuration when upgrading from Junos OS Release 15.1X49-D75 to later releases. You can also use ISSU with VPN configuration to upgrade from Junos OS Release 15.1X49-D10 up to Junos OS Release 15.1X49-D70.
- On SRX5400, SRX5600, and SRX5800 devices, do not use ISSU if upgrading from Junos OS Release 15.1X49-D30 through Junos OS Release 15.1X49-D60, if using any VPN configurations.

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

Related Documentation

- New and Changed Features on page 5
- Changes in Behavior and Syntax on page 12
- Known Issues on page 20
- Resolved Issues on page 25

Known Issues

This section lists the known issues in hardware and software in Junos OS Release 15.1X49-D100.

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

Authentication and Access Control

- SRX5400, SRX5600, and SRX5800 devices support an additional check on the LDAP servers certificate during the TLS handshake for LDAP authentication by default. If the validation of the server certificate is not required, you can use the set access profile profile-name ldap-server ldap-server-ip-address no-tls-certificate-check command to ignore the validation of servers certificate and accept the certificate without checking. PR1218357
- On SRX Series devices, TLS1.0 and TLS1.1 SSL protocols are blocked because of reported security vulnerabilities. This change might affect users accessing J-Web, web authentication GUI or using Dynamic VPN through Pulse client, when using an older OS or lower version browsers where TLSv1.2 protocol is not supported. This change affects Junos OS Release 12.3X48-D55, 15.1X49-D100 and all higher SRX releases. PR1283812

Chassis Clustering

- On SRX1500 devices in a chassis cluster with Sky Advanced Threat Prevention (ATP) solution deployed, if you disable and then re-enable CRL checking of certificate validity, the system does not re-enable CRL checking. PR1144280
- On SRX550M devices in chassis cluster, traffic loss for about 10 seconds is seen when there is power failure on the active chassis cluster node. PR1195025
- This issue is happening in ISSU stage with special data pattern. When the issue happens, the number of Invalid auth entry Is around 5k and pending auth entry is reaching the maximum number 5k(in srx5000 platform). When ISSU is ongoing the related traffic will go through SRX box with some number. At this situation ISSU may fail. PR1284561

Layer 2 Ethernet Services

- On 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 does not send the second request, because the process detects that the first authentication did not occur. This delay causes memory leak on the authd process and the memory might be exhausted, generating a core file and preventing DHCP server service. High CPU usage on the Routing Engine might also be observed. PR1042818
- On SRX Series devices, the show arp command will show all the ARP entries learned from all interfaces. When Layer 2 global mode is switching, the ARP entries learned from IRB interface can only show one specific VLAN member port instead of the actual VLAN port learned in the ARP entries. PR1180949
- On SRX300, SRX320, SRX340, SRX345, and SRX550M devices, the current Ethernet switching MAC aging uses software to age out bulk learned MAC addresses. You cannot age out specific MAC address learned at specific time immediately after the configured age. Theoretically, the MAC address might age out close to two times the configured age out time. PR1179089
- On SRX345 and SRX550M devices, frame carried with priority bit on Tag Protocol Identifier (TPID) will be lost when packet passes through with Layer 2 forwarding. PR1229021

Flow-based and Packet-based Processing

- On SRX Series devices, when a device forwards traffic, a flowd core file is generated. This is a generic issue and does not impact any feature. PR1027306
- On SRX Series devices, the maximum-sessions value is displayed incorrectly. PR1094721
- On SRX1500 devices, the log buffer size is increased to 30,000 in event mode. When the log buffer size is 1000, the Packet Forwarding Engine generated logs rush when there were more than 30 entries and the logs are dropped. PR1133757
- On SRX550M devices, traffic loop is seen with MSTP for untag traffic from IxNetwork ports. Configuring native-vlan id on the interfaces connected to IxNetwork port will remove the loop. PR1259099
- On SRX300, SRX320, SRX340, and SRX345 devices, when the protocol packets flood into the device, the CPU usage is exhausted to process the BPDU frame which has higher priority than L3 protocol, such as, ICMP and IPv4. The CPU receives maximum number of frames. So, there is possibility that the CPU might exhaust during high traffic. PR1259793
- On SRX320, SRX340, SRX345, and SRX550M devices with LTE Mini-Physical Interface Module (Mini-PIM) for 4G/LTE wireless connection, IPv6 traffic triggered

dial-on-demand from configured static route is not supported on 15.1X49-D100 PR1273532

- On SRX345 devices, flowd core files are seen at mbuf_get_from_pool. PR1276848

Install and Upgrade

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

Interfaces and Chassis

- On SRX100, SRX110, and SRX210, if 3G modem is configured without 3G modem inserted. Junos may erroneously try to access the 3G thread and crash when it cannot find it. Traffic interruption will occur due to flowd crashes. When encountering this issue, please delete the 3G modem configuration to restore the issue. PR1151904
- On SRX Series devices, the NP error is displayed when service offline is enabled on NP-IOC. PR1210152
- On SRX300, SRX320, SRX340, SRX345, and SRX550M devices, use logical tunnel interface: lt-0/0/0 as the destination interface option for RPM probe-server. PR1257502

J-Web

- On SRX Series devices in J-Web, when you login to the Web-authentication page, BAD_PAGE_FAULT will be seen. PR1180787
- On SRX1500 devices in J-Web, snapshot functionality **Maintain > Snapshot > Target Media > Disk > Click Snap Shot** is not supported. PR1204587
- On SRX Series devices, DHCP relay configuration under **Configure > Services > DHCP > DHCP Relay** page is removed from J-Web in Junos OS Release 15.1X49-D60. The same DHCP relay can be configured using the CLI. PR1205911
- On SRX Series devices, DHCP client bindings under Monitor is removed for Junos OS Release 15.1X49-D60. The same bindings can be seen in CLI using the **show dhcp client binding** command. PR1205915
- On SRX4100 devices, a security policy page in J-Web does not load when it has 40000 firewall policy configuration. Navigate to **Configure > Security > Security Policy** page. PR1251714
- Login to J-Web Navigate to **Monitor > Services > DHCP > DHCP SERVER & DHCP RELAY** click the help page icon. Online help page throws a 404 error . PR1267751
- Sometimes Dashboard widget Applications, ThreatMap, Firewall Top Denies shows no data available when device is having huge data PR1282666
- CLI does not work for Chrome version > 42. You can use IE version 10 or version 11 or Firefox version 46+ browsers to use CLI. PR1283216
- Sometimes in Chrome or Firefox browser, Time Range slider does not work for all events as well as individual events PR1283536

- For every commit performed using J-Web, commit goes through but the J-Web pages always prompt the following message **"The configuration on the device is too large for J-Web to handle. Please use CLI to manipulate the configuration"** PR1286996
- Source NAT pool configuration from J-Web cannot be committed unless address range is entered. Since Add/Delete buttons are available from J-Web to add/delete source NAT pool address range is not visible now. You can perform these operations only through CLI.
  - Navigate to Configure -> Security -> NAT -> Source.
  - Click Source NAT Pools tab and enter pool name
  - While entering address range details for pool addresses, add/delete buttons are missing from the window.
  - So commit wont be successful unless address range is entered.
  - Customers can configure this part through cli using the **set security nat source pool <poolname> address <ip_addr> to <ip_addr>** to add and **delete security nat source pool <poolname> address <ip_addr> to <ip_addr>** to delete.

    PR1290722

Network Management and Monitoring

- After power-on or RG0 failover at SRX cluster, one RE does not reply for snmp request. PR1240178
- The syslog message from the secondary node will not reach a syslog server when reth I/F is source interface for it. PR1252128

Platform and Infrastructure

- On SRX Series devices, when a USB flash device with a mounted file system is physically detached by a user, the system might panic. PR695780
- On SRX210 or SRX220 chassis cluster, if a VLAN interface is configured as the interface of JDHCP server, then the DHCPDISCOVER message will be dropped on the switch chip, which results in the function of JDHCP server failure. PR1088134
- On SRX5800 devices, if the system service REST API is added to the configuration, though commit can be completed, all the configuration changes in this commit does not take effect. This occurs as the REST API daemon fails to come up and the interface IP is not available during bootup. The configuration is not read on the Routing Engine side. PR1123304
- On SRX Series devices, File Descriptor (FD) might leak on the httpd-gk process when system fails to connect to the mgd process management socket. PR1127512
- On high-end SRX Series devices, flowd process might crash and cause traffic outage if the services processing unit (SPU) CPU usage is higher than 80%. Therefore, some threads are in waiting status and the watchdog cannot be toggled timely causing the flowd process to crash. PR1162221

Routing Policy and Firewall Filters

- On SRX Series devices, if there are two routing instances, of instance type default and virtual router, when you change the instance type of one routing instance from default to virtual router after the routing policy is configured, the route is missing from the second routing instance. PR969944

Routing Protocols

- On SRX Series devices, RIP is supported in P2P DC mode over st0 interfaces. PR1141817
- On SRX Series devices, when OSPF dead-interval is lower than the default value, graceful restart might not work during manual RG0 failover or ISSU, causing service disruption. PR1216687

UTM

- Some traffic from web-cam contain non-standard HTTP boundary format, it will cause SRX UTM/SAV hold traffic/mbuf, later cause failover PR1283806

VPN

- On SRX Series devices, if IPsec VPN tunnel is established using IKEv2, due to bad SPI, packet drop might be observed during CHILD_SA rekey when the device is the responder for this rekey. PR1129903
- On SRX5800 devices, when upgrading from Junos OS Release 15.1X49-D30 to 15.1X49-D35, 15.1X49-D40, and 15.1X49-D50 or from 15.1X49-D35, 15.1X49-D40, and 15.1X49-D50 to 15.1X49-D60 release, the ISSU fails for AutoVPN/ADVPN/DEP IPsec VPN tunnels. PR1201955
- On SRX5400, SRX5600, and SRX5800 devices, when CoS on st0 interface is enabled and the incoming traffic rate destined for st0 interface is higher than 300000 packets per second (pps) per SPU, the device might drop some of the high priority packets internally and shaping of outgoing traffic might be impacted. It is recommended that you configure appropriate policer on the ingress interface to limit the traffic below 300000 pps per SPU. PR1239021
- A loopback interface using two IP addresses can be used to create IPSec tunnels to two different remote peers on an Active/Passive SRX cluster as long as the 'local-address' parameter is defined under the IKE configuration with the appropriate loopback IP address for each remote peer. PR1266915

Related Documentation

- New and Changed Features on page 5
- Changes in Behavior and Syntax on page 12
- Known Behavior on page 15
- Migration, Upgrade, and Downgrade Instructions on page 32
- Resolved Issues on page 25

Resolved Issues

This section lists the issues fixed in hardware and software in Junos OS Release 15.1X49-D100.

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

Authentication and Access Control

- For a security policy with HTTP pass-through firewall authentication being configured, we recommend that you configure web-redirect for HTTP pass-through firewall authentication instead of using direct HTTP pass-through firewall authentication because web browser may automatically carry credential in subsequential request to target web-server. PR1230447
- A user session is disconnected due to aging out of a fwauth entry in spite of an existing session. PR1265571
- Once a session hit fails authentication entry, the entry might show a huge number instead of "Infinite". This issue does not have any impact on the traffic.PR1270461
- On SRX Series devices, when UAC (Unified Access Control) is used, the flowd process might fail under a race condition of operating internal connections between Routing Engine (RE) and Packet Forwarding Engine (PFE) for status synchronization. PR1271687

Chassis Clustering

- An interface is not synced between the RE and the PFE under HA cluster environment when some special CoS setting is configured. PR1248193
- In an SRX340 device cluster using Ethernet switching , ARP issues are seen. PR1259286
- Under a race condition, the interrupts on the routing engine may reuse resources that are not previously released, leading to a dead loop, and ultimately causing a watchdog to trigger the reboot of the SRX device. PR1256840
- On SRX345 device, sometimes it is observed that either on primary or the secondary node, the switching fab probe status is down in Layer 2 HA configuration. The Layer 2 HA traffic can work well under such state. This state moves to up on rebooting both nodes. PR1257617
- On SRX Series devices, when Advanced Anti-Malware (AAMW) service is enabled, enrolled with Sky ATP Service running in the cloud, and the user enables the traceoption with option flag daemon or flag. For example, set services advanced-anti-malware traceoptions flag daemon or set services advanced-anti-malware traceoptions flag all. If you commit the configuration changes in AAMW, there might be a coredump on Routing Engine (RE) AAMW daemon. The AAMW daemon recovers afterwards automatically. The coredump occurrence is rare. PR1261881
- SRX300 line devices and SRX1500 devices running version prior to Junos OS Release 15.1X49-D100, does not show any option to enable control-link-vlan PR1274601

- On SRX5400, SRX5600, and SRX5800 platforms, when IPsec VPN is configured with IPsec session-affinity enabled, the UDP traffic which destination port is 2123 or 2152 will be selected anchor by GTP module, even there is no GTP profile configured, which causes the IPsec VPN tunnel session and the clear-text session (UDP destination port is 2123 or 2152) to be installed on different SPUs. PR1277715
- On all SRX platforms with GTP inspection configured, a GTP control plane packet is dropped if it contains any Information Element (IE) more than once. For example when the RFSP Index IE appears twice in an SGSN Context Response, the packet will be dropped. PR1284311

Flow-based and Packet-based Processing

- Under IPv6 VRRP scenario, when a host sends router solicitation messages to VRRP virtual IPv6 address, the VRRP master replies router advertisement messages with physical MAC address instead of virtual MAC, the VRRP slave replies router advertisement messages with physical MAC address as well. As a result, the host has two default gateways installed and the host will send traffic directly to two devices but not to the VRRP virtual IP. This issue affects VRRP function and traffic. PR1108366
- On SRX Series devices, the software-NH value increases and causes the traffic outage. PR1190301
- On SRX devices with Selective Packet Services configured, multicast traffic might be sent out-of-order by the device. PR1246877
- On SRX1500 devices, if DPD is configured for tcp-encap sessions, then the effective DPD timeout must be increased to greater than 120 seconds. PR1254875
- On SRX Series devices, when Express Path (SOF) is enabled, the ASIC recalculates all the UDP checksum on I/O card (IOC) and causes traffic problem on the IPsec session. PR1254897
- On SRX300 line devices, sometimes auto-installation fails when you configure through Trivial File Transfer Protocol (TFTP) and the MAC address is incorrect . PR1258839
- On SRX Series devices, when RG0 failover occurs, the Point-to-Point Protocol over Ethernet (PPPoE) session is disconnected. PR1259316
- When using ECMP for load-balancing traffic over multiple links, in the case where IPv6 traffic is marked with ECN, not all packets belonging to the same TCP session may be forwarded over the same link. PR1265576
- On SRX Series devices, a core file is generated when traffic causes high memory usage and lot of memory allocation failures are observed at Deep Packet Inspection (DPI) module. The core file is difficult to reproduce and high memory usage might not always result in core file. The core file is generated due to buffering issues in DPI engine code when the application identification requires data to be buffered at engine. PR1266517
- If the same flow session traverse the same SRX multiple times and this flow session required TCP proxy on SRX, RG1+1 failover may cause high rate of TCP probe packets between the TCP proxies resulting in high SPU CPU utilization. PR1268740
- On all SRX Series devices, non-IPv4 packets are dropped if double GRE IPv4 encapsulation is used. PR1270070

- On all vSRX and SRX Series devices, when the DHCP or DHCP relay is configured, specially crafted packet might cause the flowd process to crash, halting or interrupting traffic from flowing through the device(s). PR1270493
- Multicast traffic was not working fine and noticed that at the egress interface (associated to a IRB interface) the destination MAC address were set all to "0". PR1276043
- SRX Series devices cannot record AD user in the AD table. This issue causes slow down of the processing speed for handling the eventlog with some ip-user mapping without username PR1274551
- The /var/log/wmtp file is not created by default on SRX1500 devices. PR1260810

Forwarding and Sampling

- SRRD daemon acts as a server for all JFlow clients. The JFlow clients can be either PFEs or PICs performing JFlow. The maximum number of JFlow clients were previously 32 and it has been increased to 64 in this release. PR1261783

Interfaces

- On SRX300, SRX320, SRX340, and SRX345 devices, the device reboots when Juniper USB with part number RE-USB-4G-S (740-028898) is inserted in the USB slot while the device is on. PR1214125
- On SRX1500 device, SFP+-10G-CU3M DAC cable connects to the xe interface, xe interface is not coming UP physically. PR1246725
- On Branch SRX devices, if an Aggregated Ethernet (AE) interface is changed from layer 2 (ethernet-switching) to layer 3, then ARP learning on this AE interface will fail. PR1258667
- On SRX1500, if software release 15.1X49-D70 or above is installed and you have a single PEM in slot 0, you will see an alarm saying PEM 1 is not present. PR1265795
- SFP-100BASE-BX10-U and SFP-100BASE-BX10-D does not support Digital Diagnostic Monitoring DDM, so "show interfaces diagnostics optics ge-X/X/X" command does not show any output PR1270908

J-Web

- On SRX Series devices, when you add new IP address to firewall filter, the J-Web PHP memory does not overflow. PR1253482
- On SRX340 and SRX345 devices, on the Setup Wizard default mode, an address pool is created for a management IP network even if you change the default management IP address in the default-setup mode. PR1259742

- Sending SNMP traps with Dynamic VPN clients are failing to authenticate. Regular traps are not possible. Using event-options creates events but does not create and send traps. PR1263628
- Navigate to **Configure**->**Security**->**ALG** page and add the required ALG configurations. After this step, while navigating to other J-Web pages, page display will appear blank. Similarly, this issue is applicable for **Configure**->**Ipsec VPN**->**Global settings** options, **Configure**->**Security**->**Forwarding mode** page. Refresh the browser to access J-Web again. This issue might repeat again while editing or deleting configuration in the specified pages. You need to refresh the browser to access J-Web, anytime this issue is seen.PR1269762

Layer 2 Ethernet Services

- In the DHCPv4 or DHCPv6 relay environment with large scaled environment (in this case, 50-60K subscribers), and the system is under stress (many simultaneous operations). The subscribers might get stuck in RELEASE state with large negative lease time. PR1125189
- On SRX series in switching mode, SRX only transfers traffic up to 1Gbps from IRB interface. PR1228605
- Multiple hops would be seen when performing L2 traceroute.This issue can be triggered when there are loops in the topology and performing chassis fpc/dcd/ppmd deamon restart. PR1243213
- ISIS for SRX300 line devices is not working for multi-access topology. PR1274555

Network Address Translation (NAT)

- On SRX devices, when NAT is configured, the nsd process might show a memory leak after a NAT configurations are changed and committed. PR1260409
- On SRX Series devices, when source-address match condition for static NAT is configured, the NSD process might fail if the address book contains too many addresses. PR1272477

Network Management and Monitoring

- After power-on or RG0 failover at SRX cluster, one RE does not reply to SNMP request. PR1240178
- Syslog message from the secondary node will not reach a syslog server when reth I/F is the source interface. PR1252128

Platform and Infrastructure

- On SRX Series devices in a chassis cluster, if sampling is used, the flowd process fails and core files are seen on both the nodes, when route is updated through dynamic protocols, such as BGP. PR1249254
- On SRX5600 and SRX5800, in Junos releases 15.1X49-D70 to 15.1X49-D90, if a second Routing-Engine (RE) is present which is running a Junos release below 15.1X49-D70,

the command 'show chassis hardware' will trigger a resource leak which causes CLI commands to fail and SSH to the device to fail and you may see this message on the console: "kern.ipc.maxpipekva exceeded; see tuning(7)". This issue is accelerated when using SkyATP Advanced Anti Malware feature or when performing the command 'show chassis hardware' often. PR1254576

- On SRX Series devices, when you configure **http-get** Real-time Performance Monitoring (RPM) probes, the URL is lost in the get message. For example:

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

PR1256865

- On SRX Series devices, the error message abnormal timer recovery is displayed frequently in the logs, without any service impact. PR1260274
- On SRX Series devices, additional UI_CFG_AUDIT messages are logged for private configuration session and does not have adverse effect to the operational state of the device. PR1261147

Routing Policy and Firewall Filters

- Starting in Junos OS Release 15.1X49-D100, a new default application, application junos-smtps, has been added for secured email traffic using port 587 or 465. To view the new default policy, use the show configuration groups junos-defaults applications command. PR1273725

Routing Protocols

- When BGP is used and graceful restart is configured, packet drop is seen when routing process is restarted. PR1239186

Unified Threat Management (UTM)

- On all SRX platforms, when using UTM (includes Anti-Spam, Content-Filtering, and Anti-Virus) scanning on email protocol traffic, the e-mail flow may stop at some point. UTM traceoptions then indicate "MIME deadloop detected". PR1265992
- On SRX Series devices, when http-reassemble is configured, non-http traffic over port 80 might be blocked by UTM Web filter, such as Real-Time Messaging Protocol (RTMP) traffic over port 80. PR1267317
- On SRX5K device in chassis cluster, mgd CPU usage will go up around 90% when one of following commands are run **show security utm anti-virus status fpc**, **show security utm anti-virus status fpc fpc-slot <no>** or, **show security utm anti-virus status fpc pic-slot <no>**.PR1277772
- When trying to download complete mailbox from mail server over POP3, with sophos-av enabled on SRX, the download stops after a few mails (from 7-150). Everything works fine, with complete mail box downloaded with AV disabled. No errors or fallback counters shown as increased. Just in the UTM trace the "MIME deadloop detected" message will be displayed. PR1278134

User Interface and Configuration

- On all Junos platforms, inserting a policy after a deactivated policy, does not work. PR1254376

VLAN Infrastructure

- On SRX300 line devices in transparent mode, some of fragmented IPv4 multicast packets are dropped. PR1274455

VPNs

- Due to product limitation, second client is getting disconnected when assigned-IP of first client is changed with Local FW authentication server. PR1246131
- On SRX Series devices, traffic loss is seen after adding traffic selector in a IPsec VPN. PR1249908

- On SRX Series devices in a chassis cluster, in a rare condition while modifying IPsec VPN configuration, file mismatch of "/var/etc/vpn_tunnel.id" between both nodes is seen. Performing RG0 failover results in the kmd process failure on the new primary node. PR1250178
- On SRX1500 devices in a chassis cluster, IP leak might occur under the following scenarios:
  - In case of IKEv1, it is possible for an IPsec VPN tunnel to be active without an active IKEv1 phase 1 SA. Since the assigned IP address associated with an IPsec VPN tunnel (for a user) is stored in the record of phase 1 SA, if HA RG0 failover occurs while there is no active IKEv1 phase SA exist for an IPsec VPN tunnel. The assigned IP address will be released to the authd daemon when the IPsec VPN tunnel is disconnected.
  - In case a remote access IPsec VPN tunnel is cleared (for both IKEv1 and IKEv2), the assigned IP address is kept for 30 seconds before it is released back to the authd within an additional 2 minutes. If HA failover occurs during this time before the IP is received at the authd, there will be an IP address leak.
  - If a new IP is assigned by authd daemon after every user is authenticated, regardless of the user already having an IP assigned from an early authentication. In case of IKEv1, authentication occurs at every IKE phase 1 SA rekey. If the KMD daemon restarts immediately (within 2 minutes) after an IKEv1 phase 1 SA rekey, there is a possibility that the newly assigned IP has not been released to authd daemon yet.

  PR1252181
- On SRX5600 device, the DNS and WIN IPs are in reverse order in active-peer output when configured at access level and access profile level. PR1252186
- On SRX1500 devices, traces cannot be enabled or disabled through the CLI options under 'tcp-encap traceoptions'. PR1252544
- On SRX platforms, when st0 interface is moved from one routing instance to another routing instance, packet loss is observed. PR1255593
- On all SRX Series devices, when manual route-based IPsec VPN is configured, enabling VPN monitoring will cause the st0.* interface to go down, which results in VPN traffic drop. PR1259422
- On SRX Series devices, the error message timeout communicating with pki-service daemon is displayed when you create local certificate with ECDSA key pair. For example: user@host# request security pki generate-key-pair certificate-id <name> size 384 type ecdsa. ? user@host# request security pki local-certificate generate-self-signed certificate-id <name> digest sha-256 domain-name aaa.com subject CN=X, O=X, C=X add-ca-constraint. ? In PKI trace is noticed that it is failing to sign x509 certificate. For example, ERROR: X509V3_EXT_conf_nid() failed for extn=hash. self_signed_x509: ERROR: add_ext() failed for extn 'hash'. self_signed_x509: cannot sign the x509. PR1259867
- On SRX5400, SRX5600, and SRX5800 platforms running on Junos OS Release 15.1X49-D80, when traffic-selector is used, the flow session running through a traffic-selector based IPsec VPN tunnel might be deleted unexpectedly, and the Tunnel

establishment Per Second (TPS) of IPsec VPN has 19% drop comparing to the previous Junos OS Release. PR1266596

- Manual NHTB does not work on 15.1X releases. We see following error on IKE traces, "Internal Error: Manual NHTB add failed".PR1266797
- On SRX Series devices, if traffic-selector is configured, the IKE redundant gateway failover fails. PR1270000
- On all SRX Series devices, CRL download fails when missing content-length field in http header and CRL occupies are in at least 2 packets. PR1278631

Related Documentation

- New and Changed Features on page 5
- Migration, Upgrade, and Downgrade Instructions on page 32
- Changes in Behavior and Syntax on page 12
- Known Behavior on page 15
- Known Issues on page 20

Documentation Updates

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

- Information about MIBs is available in SNMP MIBS Explorer. On the Junos OS for SRX Series page, click **SNMP MIB Explorer** to view MIBs information. Use the MIBs Explorer to search for and view information about various MIBs, MIB objects, and SNMP notifications that are supported on Juniper Networks devices.
- Information about system log messages is available in System Log Explorer. On the Junos OS for SRX Series page, click **System Log Explorer** to view system log information. Use the System Log Explorer to search for and view information about various system log messages.

Migration, Upgrade, and Downgrade Instructions

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

- Upgrade for Layer 2 Configuration on page 32
- Upgrade and Downgrade Scripts for Address Book Configuration on page 33

Upgrade for Layer 2 Configuration

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

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

Upgrade and Downgrade Scripts for Address Book Configuration

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

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

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

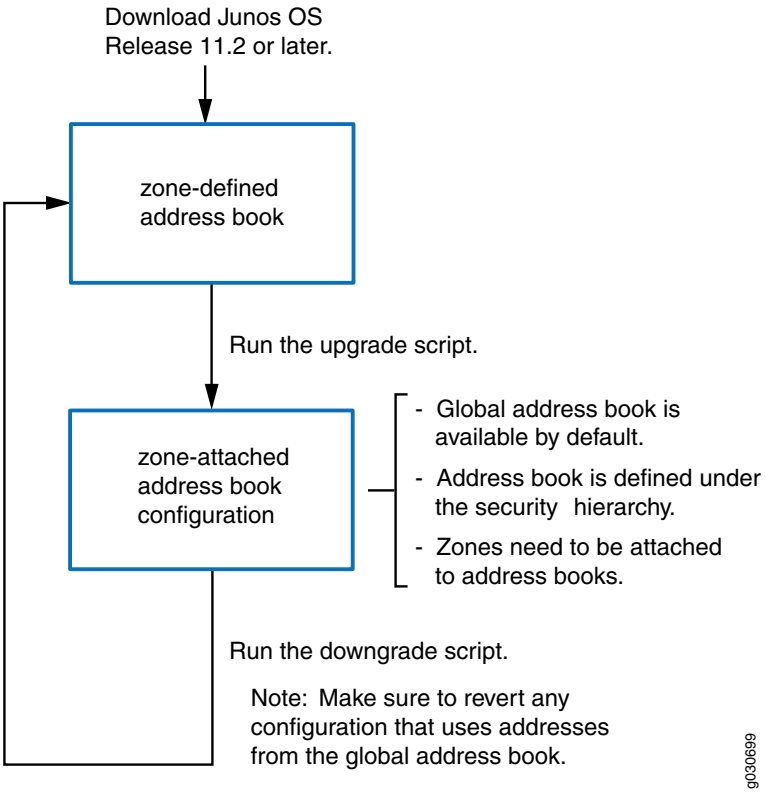
  - You cannot configure address books using the zone-defined address book configuration format; the CLI displays an error and fails to commit.
  - You cannot configure address books using the J-Web interface.

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

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

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

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

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

Related Documentation

- New and Changed Features on page 5
- Changes in Behavior and Syntax on page 12
- Known Behavior on page 15
- Known Issues on page 20
- Resolved Issues on page 25

Product Compatibility

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

Hardware Compatibility

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

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

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

To access Software Release Notifications for Junos OS Service Releases, visit our Knowledge Center at https://support.juniper.net/support/. You'll need to log in to your Juniper Account. From the Knowledge Center, search by the specific release number, for example 17.4R1-S2. Use the Software Release Notifications to download software, and learn about known and resolved issues for specific service releases.

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 https://apps.juniper.net/feature-explorer/.

Documentation Feedback

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

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

Requesting Technical Support

Technical product support is available through the Juniper Networks Technical Assistance Center (JTAC). If you are a customer with an active J-Care or JNASC support contract, or are covered under warranty, and need post sales technical support, you can access our tools and resources online or open a case with JTAC.

Technical product support is available through the Juniper Networks Technical Assistance Center (JTAC). If you are a customer with an active J-Care or Partner Support Service support contract, or are covered under warranty, and need post-sales technical support, you can access our tools and resources online or open a case with JTAC.

- JTAC policies—For a complete understanding of our JTAC procedures and policies, review the *JTAC User Guide* located at https://www.juniper.net/us/en/local/pdf/resource-guides/7100059-en.pdf.
- Product warranties—For product warranty information, visit https://www.juniper.net/support/warranty/.
- JTAC hours of operation—The JTAC centers have resources available 24 hours a day, 7 days a week, 365 days a year.

Self-Help Online Tools and Resources

For quick and easy problem resolution, Juniper Networks has designed an online self-service portal called the Customer Support Center (CSC) that provides you with the following features:

- Find CSC offerings: https://support.juniper.net/support/
- Search for known bugs: https://kb.juniper.net/
- Find product documentation: https://www.juniper.net/documentation/
- Find solutions and answer questions using our Knowledge Base: https://kb.juniper.net/
- Download the latest versions of software and review release notes: https://support.juniper.net/support/downloads/

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

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

Opening a Case with JTAC

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

- Use the Case Management tool in the CSC at https://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 https://support.juniper.net/support/requesting-support/.

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/documentation/feedback/.

Revision History

28 January 2019—Revision 4— Junos OS 15.1X49-D100 – SRX Series.

27, June 2018—Revision 3— Junos OS 15.1X49-D100 – SRX Series.

19, July 2017—Revision 2— Junos OS 15.1X49-D100 – SRX Series.

05, July 2017—Revision 1— Junos OS 15.1X49-D100 – SRX Series.