Release Notes: Junos® OS Release 15.1X49-D130 for the SRX Series

Release 15.1X49-D130
31 January 2019
Revision 7

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-D130 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-D130 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-D130 for the SRX Series devices. For New and Changed Features information starting with Junos OS Release 15.1X49-D10 to Junos OS Release 15.1X49-D120, refer to the Release Notes listed in the Release 15.1X49 section at Junos OS for SRX Series page.

Release 15.1X49-D130 Software Features

Authentication and Access

- **IPv6 support for ClearPass (SRX Series, vSRX)**—Starting with Junos OS Release 15.1X49-D130, SRX Series devices can query ClearPass for identity information for newly generated IPv6 users, and ClearPass can push IPv6 user identity information to an SRX Series device. SRX Series devices also support the use of IPv6 addresses associated with source identities in security policies. In addition, you can configure a Web API client address with an IPv6 address and Web API supports IPv6 user entries obtained from ClearPass.

  [See Understanding the SRX Series Integrated ClearPass Authentication and Enforcement Feature and Understanding How ClearPass Initiates a Session and Communicates User Authentication Information to the SRX Series Device Using the Web API.]

Interfaces and Routing

- **NDP Proxy and DAD Proxy Support for SRX Series Devices**—Starting in Junos OS Release 15.1X49-D130, NDP proxy and DAD proxy are supported at the interface level on all SRX Series devices.

  Use the following commands to enable NDP and DAD proxies:

  - **set interfaces *interface-name* family inet6 proxy-ndp**
  - **set interfaces *interface-name* family inet6 proxy-dad**

  Use the following commands to disable NDP and DAD proxies:

  - **set protocols neighbor-discovery proxy-ndp no-proxy-on-resolve**
  - **set protocols neighbor-discovery proxy-dad no-proxy-on-resolve**

  The **show system statistics icmp6** command is enhanced to add the following statistics:

  - interface-restricted ndp proxy requests
  - interface-restricted dad proxy requests
  - interface-restricted ndp proxy responses
  - interface-restricted dad proxy conflicts
  - interface-restricted dad proxy duplicates

- interface-restricted ndp proxy resolve requests
- interface-restricted dad proxy resolve requests
- interface-restricted dad packets from same node dropped
- interface-restricted proxy packets dropped with nomac

[See Configuring Duplicate Address Detection Proxy and Configuring Neighbor Discovery Protocol Proxy.]

- **Support for Address Resolution Protocol (ARP) throttle and ARP detect [SRX5400, SRX5600, and SRX5800]**—Starting in Junos OS Release 15.1X49-D130, an ARP throttling mechanism is introduced for SRX Series devices.

  Excessive ARP processing results in high utilization of Routing Engine CPU resources, resulting in deprivation of CPU resources to other Routing Engine processes. To provide protection against excessive ARP processing, you can now use the following configuration statements:

  - **edit forwarding-options next-hop arp-throttle *seconds***
  - **edit forwarding-options next-hop arp-detect *milliseconds***

  

  CAUTION: We recommend that only advanced Junos OS users attempt to configure the ARP throttle and ARP detect feature. An improper configuration could result in high CPU utilization of the Routing Engine, which could affect other processes on your device.

  [See arp-throttle and arp-detect].

Related Documentation

- Changes in Behavior and Syntax on page 5
- Known Behavior on page 7
- Known Issues on page 13
- Resolved Issues on page 17
- Migration, Upgrade, and Downgrade Instructions on page 22

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-D130.

Authentication and Access Control

- **Support for Web Authentication (SRX Series)**—Starting with Junos OS Release 15.1X49-D130, you can configure the **timeout** option at **[edit access firewall-authentication web-authentication]** hierarchy level to configure a timeout value in seconds.

  Prior to Junos OS Release 15.1X49-D130, the default timeout value to process a web authentication was 3 seconds. For example, when you type a username and password in a browser for authentication, SRX Series device checks the user account in the database, and after 3 seconds your web browser displays a message **invalid username and password** even before the check is complete in the database. However, after 10 seconds, SRX Series device receives a response from the database that the user authentication is successful, but SRX Series device could not notify the user about successful authentication, due to 3 seconds timeout value.

  Now, with an enhancement to configure a timeout value for web authentication, if you configure the timeout value from 5 through 60 seconds, the browser waits for the SRX Series device to respond for the specified time.

Flow-Based and Packet-Based Processing

- **Increase in security zone limit (SRX300 and SRX320)**—Starting with Junos OS Release 15.1X49-D130, maximum number of security zones supported on SRX300 and SRX320 devices is increased from 16 zones to 32 zones.

VPNs

- **IKE Gateway Extended Authentication (XAuth)**—Starting with Junos OS Release 15.1X49-D130, on all SRX Series devices, and vSRX instances, the maximum number of characters allowed for an IKE gateway Extended Authentication (XAuth) client username is increased from 32 to 128.
- **Dead peer detection (DPD) interval parameter**—Starting with Junos OS Release 15.1X49-D130, on all SRX Series devices and vSRX instances, the permissible interval parameter range at which DPD messages are sent to the peer device is reduced from 10 through 60 seconds to 2 through 60 seconds. The minimum threshold parameter should be 3 seconds, when the DPD interval parameter is set less than 10 seconds.

Routing Protocols

- **Mechanism to retain elected PIM designated router on device recovery(SRX Series)**—Starting with Junos OS Release 15.1X49-D130, **nondr-stickydr** option is introduced at the following hierarchy levels to overcome the traffic loss during the designated router failover:
  - **[edit routing-instances routing-instance-name protocols pim interface *interface-name*]** to configure routing instance.
  - **[edit protocols pim interface *interface-name*]** to configure PIM master routing instance.

Prior to Junos OS Release 15.1X49-D130, when the designated router failed, a non designated router was elected and performed as the designated router. When the failed router recovered, the router was re-elected and performed as the designated router again. This process resulted in traffic loss during the designated router failover. This traffic loss is eliminated by enabling the **nondr-stickydr** option, which allows the elected designated router to continue as a designated router until the device undergoes an interface flap or a reboot.

NOTE: **Configuring designated router priority explicitly on an interface may return unexpected results.**

[See interface (Protocols PIM)].

Related Documentation

- Changes in Behavior and Syntax on page 5
- Known Behavior on page 7
- Known Issues on page 13
- Resolved Issues on page 17
- Migration, Upgrade, and Downgrade Instructions on page 22

Known Behavior

This section contains the known behaviors, system maximums, and limitations in hardware and software in Junos OS Release 15.1X49-D130.

Chassis Cluster

- On SRX4100 and SRX4200 devices, although the CLI is configurable, the following features are not supported: Group VPN, VPN Suite B, and encrypted control links when in a chassis cluster. PR1214410
- On SRX Series devices in a chassis cluster, when configuring Ethernet switching, the device reboots followed by a CLI warning message. Rebooting one node in the chassis cluster setup might lead to an asynchronized chassis cluster, and this might result in the device moving to database mode. PR1228473

Flow-Based and Packet-Based Processing

- On SRX550M devices, traffic processed by the serialization process is dropped when the maximum limit of serialization sessions (32,000) is exceeded. As a result, advanced services such as IDP, ALG, GTP, SCTP, and AppSecure are impacted. The limitation of maximum serialization sessions must be increased to 64,000. PR1061524
- On SRX5400, SRX5600, and SRX5800 devices, in a central point architecture, system logs are sent per second per SPU. Hence, the number of SPUs defines the number of system logs per second. PR1126885

- On SRX1500 devices, the log buffer size is increased to 30,000 in an event mode. When the log buffer size was 1000, the packet forwarding engine generated log bursts when there were more than 30 entries and more logs were dropped. PR1133757
- On SRX1500 devices, when Security Intelligence (SecIntel) is loading feed to a service card (packet forwarding engine), the log message prints a message showing data feed is loaded to pic 1. The pic 1 is incorrect because there is no pic 1 on SRX1500, it should be pic 0. PR1144765
- On SRX340 and SRX345 devices, half-duplex mode is not supported because BCM53426 does not support half-duplex mode. BCM5342X SoC port configurations, BCM53426 does not have QSGMII interface. Only the QSGMII port supports half-duplex mode. PR1149904
- On SRX5400 devices, if a user or group name contains the following characters: **"*" (ASCII 0x2a), "(" (ASCII 0x28), ")" (ASCII 0x29), "\" (ASCII 0x5c) and NUL (ASCII 0x00)**, the query from the device to the LDAP server will timeout and might lead to high CPU utilization. PR1157073
- On SRX Series devices, due to SRX5K-MPC (IOC2) lookup, the hardware engine counts one extra packet for each session wing installed in the SRX5K-MPC (IOC2) services offloading. The packet counters in the CLI for services offloading sessions from the SRX5K-MPC (IOC2) are always up by 1 compared to the SRX5K-MPC3-100G10G (IOC3), for the same Service offload scenario. PR1157158
- On SRX300, SRX320, SRX340, SRX345, and SRX1500 devices, the command **set system internet-options tcp-mss <value>** does not work in Junos OS Release 15.1X49. PR1213775
- On SRX300, SRX320, SRX340, SRX345, and SRX550M devices, after a certain period of enabling dot1x, multiple first message EAP frames with the same timestamp are transmitted. However, this does not affect any dot1x functionality. PR1245325
- Modem profile is not active until a profile is defined. You need to define a profile before selecting a profile. PR1254427
- On SRX Series devices, OSPF over GRE over IPsec is not supported on a device with a standalone central point. PR1274667
- On SRX Series devices, user firewall process useridd retries connecting to the autodiscovery server but fails to connect to the server. Due to this issue, the useridd is unable to handle other messages. Hence, the administrator must remove or deactivate those unused or incorrect user firewall configurations. PR1307851
- On SRX300, SRX320, SRX340, SRX345, and SRX550M devices, using an SFP-T module can cause an early linkup on connecting a device during the boot process. PR1314167

Interfaces and Routing

- When a Digital Subscriber Line Access Multiplexer (DSLAM) is invoked for link fault management remote loopback in drop mode, the VDSL PPPOE interface goes down.
- 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 SRX Series devices, when IPv6 address is configured on a Layer 3 VLAN interface, in some rare scenarios, the VLAN interface might take longer to boot up during the device bootup. Then, the IPv6 duplicate address detection (DAD) cannot run successfully for a long time, which results in the IPv6 address remaining in a tentative state. PR967786
- On SRX Series devices, an IPv6 ping to an interface may not work if the interface is configured in a virtual routing instance and inet6 is the only family configured on the interface. PR1142936
- On all multi-thread SRX Series devices, when one of the interfaces is down, it could be a timing issue. For example, if one thread releases an interface resource because the interface is down, another thread might try to access this interface resource, resulting in a flowd process stop. PR1148796
- On SRX Series devices, after the user changes some interface configuration, a reboot warning message might appear. The warning message is triggered only when the configuration of the interface mode is changing from route mode to switch or mixed mode. This is a configuration-related warning message, so it might not reflect the current running state of the interface mode. PR1165345
- 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 the 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, use logical tunnel interface lt-0/0/0 as the destination interface option for an RPM probe server on the device. PR1257502

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. PR1138333
- On SRX Series devices in a chassis cluster, if you want to use J-Web to configure and commit the configurations, you must ensure that all other user sessions are logged out, including any CLI sessions. Otherwise, the configurations might fail. PR1140019
- On SRX1500 devices in J-Web, snapshot functionality (Maintain->Snapshot->Target Media->Disk ->Click Snap Shot) is not supported. PR1204587
- On SRX Series devices, DHCP relay configuration under the 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. The same bindings can be seen in the CLI using the **show dhcp** client binding command. PR1205915
- On SRX Series devices, if the configuration file is more than 5000 bytes, the following pages are not loaded successfully: Link Aggregation page at **Configure>Interface> Link Aggregation Zones** and Screens page at **Configure>Security>Zones/Screens**. PR1220052

- On SRX Series devices, you cannot upload a huge supported configuration file through J-Web (Maintain>config Management> Upload). The device displays the following error message: **Allowed memory size of 52428800 bytes exhausted (tried to allocate 18781489 bytes) in /html/core/junoscript.php on line 441**. PR1220059
- On SRX Series devices, you cannot create profiles for CL-1/0/0 using J-Web and the CLI. An error message, interface not found, is displayed. We recommended using only one LTE mPIM in the supported devices. PR1262543
- On SRX Series devices, log in to J-Web and navigate to Monitor>Services>DHCP> DHCP SERVER & DHCP RELAY. When you click the Help page icon, the Online Help page will display a 404 error message. PR1267751
- On SRX Series devices, adding 2000 global addresses at a time to the SSL proxy profile exempted addresses can cause the Web page to become unresponsive. PR1278087
- On SRX Series devices, validation is not checked when the UTM policy is detached from the firewall policy rule after an SSL proxy profile is selected. PR1285543

Layer 2 Ethernet Services

- 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 a specific MAC address learned at a 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 SRX1500 devices configured in Ethernet switching mode, only a few MAC entries are shown in the output of the **show ethernet-switching table** command, even after a MAC age-out time. This issue is applicable only when the MAC learning table has more than 17,000 MAC entries. PR1194667
- On SRX300, SRX320, SRX340, and SRX345 devices, you cannot launch the setup wizard after using the reset configuration button when the device is in Layer 2 transparent mode. You can launch the setup wizard by using the reset configuration button on the device when the device is in switching mode. PR1206189
- On SRX300, SRX320, SRX340, SRX345, SRX550M, and SRX1500 devices, VPLS traffic forwarding stops working after enabling the **ethernet-switching** configuration. VPLS and **ethernet-switching** must not be configured together on the same device. We recommend not using the **ethernet-switching** configuration on these devices when VPLS is enabled. PR1214803
- On SRX Series devices, a packet is not transited by the IRB interface when Layer 2 learning is in switching mode. PR1218376
- On SRX345 and SRX550M devices, frames carried with a priority bit on Tag Protocol Identifier (TPID) will be lost when the packet passes through with Layer 2 forwarding. PR1229021

Platform and Infrastructure

- On SRX5800 devices, if a global SOF policy (all session service-offload) is enabled, the connections per second (CPS) will be impacted due to IOC2 limitation. We

recommend using an IOC3 card if more sessions are required for SOF or lowering the SOF session amount to make sure IOC2 is capable of handling it. PR1121262

- On SRX5800 devices, if the system service REST API is added to the configuration, even though commit can be completed, all the configuration changes in this commit will not take effect. This occurs because the REST API fails to come up and the interface IP address is not available during bootup. The configuration is not read on the Routing Engine side. PR1123304

Software Installation and Upgrade

- On SRX5000 devices, in-service software upgrade (ISSU) is not supported when upgrading from earlier Junos OS releases to Junos OS Release 15.1X49. ISSU is supported when upgrading to Junos OS Release 15.1X49 and later.

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

Unified Threat Management (UTM)

- On SRX Series devices with Sophos Antivirus (SAV) configured, some files that are larger than the **max-content-size** might not go into fallback state. Instead, some protocols do not predeclare the content size. PR1005086
- On SRX1500 devices, when CPU usage is very high (above 95 percent), there is a possibility that the connection between the advanced anti-malware service (AAMW) process and the PKI process can break. In this case, the AAMW process remains in initializing state until the connection is established. PR1229021
- On SRX Series devices, if AAMW is enabled, and SMTP is configured in the AAMW policy with fallback permission enabled under the long network latency between the devices and AWS is running Sky ATP service, there might be a file submission timeout error. When sending the timeout error there is a possibility that the e-mail sent from Outlook might stay in the outbox of the sender, and the receiver might not receive the e-mail. PR1254088
- On SRX Series devices enabled with AAMW service and enrolled with Sky ATP Service running in the Cloud, if you enable the traceoption command using the **set services advanced-anti-malware traceoptions flag** process or the **set services advanced-anti-malware traceoptions flag all** command and keep committing configuration changes in AAMW, a core file might be generated on the AAMW process on the Routing Engine side of the device. The AAMW process later recovers automatically. PR1261881

Upgrade and Downgrade

- When you perform a firmware upgrade or downgrade, a FIPS core file is generated. In Junos OS FIPS mode, the file integrity checking application **veriexec** treats the new updated firmware file as a corrupted Junos OS file. This is an expected behavior by design. PR1268240

User Firewall and Authentication

- On SRX Series devices, firewall authentication cannot retrieve domain information from the access profile configuration. That is because the firewall authentication will not push user domain information to the Juniper identity management service server in case the user authenticates through web-authentication, pass-through, or web-redirect with an LDAP access profile. PR1281063

VPNs

- On SRX Series devices, if an IPsec VPN tunnel is established using IKEv2, due to bad SPI, a packet drop might be observed during a CHILD_SA rekey when the device is the responder for this rekey. PR1129903
- On SRX1500 devices, after you change the revocation configuration of a CA profile, the change cannot be populated to the SSL-I revocation check. We recommend changing the SSL-I configuration to enable or disable certificate revocation list (CRL) checking instead of CA profile configuration. PR1143462
- On SRX Series devices, the VPN monitoring feature is not working correctly in Junos OS Release 15.1X49-D40. PR1143955
- On SRX1500 devices in a chassis cluster, CRL check may fail due to nonavailability of CRL information for a **ca-profile**. As a result of the failure, if the CRL check is enabled for the connection to the Advanced Threat Prevention (ATP) cloud server, the connection cannot be established from the packet forwarding engine. PR1144265
- On SRX1500 devices in a chassis cluster with Sky Advanced Threat Prevention (ATP) solution deployed, if you disable and then reenable CRL checking of certificate validity, the system does not reenable CRL checking. PR1144280
- On SRX Series devices, when using point-to-multipoint IPsec VPN tunnels with dynamic routing over a tunnel, a ksyncd core might be observed after an RG0 failover on previous RG0 primary node if dynamic routing is removed from the VPN tunnel prior to RG0 failover. PR1170531
- On SRX Series devices, in a Layer 3 VPN scenario, in selective packet mode the MPLS packets are dropping the VPN packet when it is at the end of the MPLS path. So after parsing the MPLS header, the MPLS packet must go to the IP process. But after adding native VLAN ID, the next header parse is wrong in fwdd_parse_lsi. This is because the

packet pointer is not updated, leading to the behavior with or without native VLAN ID. PR1204186

- On SRX Series devices, the second client was getting disconnected when the assigned IP address of the first client is changed with the local firewall authentication server. PR1246131

Related Documentation

- Changes in Behavior and Syntax on page 5
- Known Behavior on page 7
- Known Issues on page 13
- Resolved Issues on page 17
- Migration, Upgrade, and Downgrade Instructions on page 22

Known Issues

This section lists the known issues in hardware and software in Junos OS Release 15.1X49-D130.

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 server's 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 server's 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 the J-Web, or the Web authentication GUI or using dynamic VPN through the Pulse client, when using an earlier Junos OS release or a earlier version browser on which the TLSv1.2 protocol is not supported. This change affects Junos OS Release 12.3X48-D55, Junos OS Release 15.1X49-D100, and all later Junos OS releases. PR1283812

Chassis Clustering

- On SRX1500 devices in a chassis cluster with the Sky Advanced Threat Prevention (ATP) solution deployed, if you disable and then reenable CRL checking of certificate validity, the system does not reenable CRL checking. PR1144280
- On SRX550M devices in a chassis cluster, traffic loss for about 10 seconds is seen when there is a power failure on the active chassis cluster node. PR1195025
- On SRX Series devices, in rare situations, RG1+ failover due to FPC/SPU failure might trigger MAC move protection on the neighbor switch. PR1333505

Dynamic Host Configuration Protocol

- On SRX Series devices configured as a DHCP server (using the jdhcp process), when the DHCP server gets a new request from a client and applies an IP address from the authentication process, the jdhcp process communicates with authentication process 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 authentication process will indefinitely wait for the second authentication request. However, the jdhcp 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 authentication 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

Flow-Based and Packet-Based Processing

- On SRX Series devices, the NP error is displayed when service offline is enabled on the NP-IOC. PR1210152
- On SRX Series devices, sometimes the time range slider does not work for all events or individual events in the Google Chrome or Firefox browser. PR1283536
- On SRX Series devices with chassis cluster enabled, an issue occurs when multicast traffic goes across logical systems. The ingress interface of the multicast session in the first logical system is reth2.0, which belongs to redundancy group 2. Redundancy group 2 is active on node 1. The ingress interface of multicast session in the second logical system is the PLT interface, which belongs to redundancy group 1. Redundancy group 1 is active on node 0. So the multicast session in the second logical system will be active on node 0. As a result, the multicast session activation and backup are not aligned with traffic forwarding. As a workaround, make redundancy group 1 and redundancy group 2 active on the same node. PR1295893
- FTP using Microsoft NLB does not work correctly in Layer 2 transparent mode. PR1341446
- On SRX1500, SRX4100, and SRX4200 devices, if the Sky ATP cloud feeds updates, the packet forwarding engine might stop causing intermittent traffic loss. PR1315642
- On SRX550M devices, the front panel alarm LED turns red after an RG0 failover was triggered by the flowd process even though there was no system alarm or chassis alarm. PR1338396

Interfaces and Chassis

- On SRX300, SRX320, SRX340, SRX345, and SRX550M devices, for IFLs (logical interfaces) scaling:
  - Without **per-unit-scheduler** configured, the total number of logical interfaces is limited to 2048.

  - With **per-unit-scheduler** configured on the IFD interface, (physical interface), the total number of logical interfaces is limited to the CoS scheduler subunit number which is limited to 2048.

  So, the maximum number of logical interfaces with **per-unit-scheduler** configured should be 2048 minus the number of physical interfaces that are up (with at least one logical interface up and a maximum of 128). PR1138997

- On SRX Series devices, if 3G modem is configured without having a 3G modem inserted, Junos OS might erroneously try to access the 3G thread and stop when it cannot find it. Traffic interruption might occur because the flowd process might stop. As a workaround, delete the 3G modem configuration. PR1151904

Intrusion Detection and Prevention (IDP)

- On SRX Series devices, the output of **show security idp status** command does not accurately reflect the number of decrypted SSL or TLS sessions being inspected by IDP. PR1304666

J-Web

- On SRX4100 devices, a security policy page in J-Web does not load when it has 40,000 firewall policy configurations. As a workaround, navigate to Configure> Security> Security Policy page. PR1251714
- On SRX Series devices, you cannot view the custom log files created for event logging in J-Web. PR1280857
- On SRX Series devices, the Dashboard widget applications, ThreatMap, and Firewall Top Denies shows no data available even when the device has huge amount of data. PR1282666
- On SRX Series devices, the CLI terminal does not work for Google Chrome versions later than 42. As a workaround, use internet Explorer 10 or 11 or Firefox 46. PR1283216
- On SRX Series devices running Junos OS Release 15.1X49-D100 or later, the zone drop-down menu does not list the available zone. Therefore, zone address book or sets cannot be configured. PR1308684
- On SRX Series devices, IPsec VPN tunnels go down when configuration is committed from Junos Space, Junos script or J-Web. PR1308684

Platform and Infrastructure

- On SRX Series devices running FreeBSD 6-based Junos OS software, when a USB flash device with a mounted file system is physically detached by a user, the system might panic. The issue is resolved with FreeBSD 10 and later. Contact JTAC for confirmation if system is running FreeBSD 10 or later. PR695780
- On SRX5800 devices, if the system service REST API is added to the configuration, though the commit can be completed, all the configuration changes in this commit will not take effect. This occurs because the REST API process fails to come up and

the interface IP is not available during bootup. The configuration is not read on the Routing Engine side. PR1123304

Unified Threat Management (UTM)

- On SRX1500 devices, when CPU usage is very high (above 95 percent), there is possibility that the connection between the AAMW process and PKID process can break. In this case, the AAMW process remains in initializing state until the connection is established. PR1142380
- On SRX Series devices, AAMW established sessions always use the configured AAMW parameters at the time of session establishment. The configuration changes will not retroactively affect the already established sessions. For example, a session established when the verdict threshold is 5 will always have 5 as the threshold even if the verdict threshold changes to other values during the session lifetime. PR1270751

Upgrade and Downgrade

- On SRX550M devices, upgrade fails when you upgrade from Junos OS Release 15.1X49-D30 to a later Junos OS release. PR1237971
- On SRX1500, SRX4100, and SRX4200 devices, while performing a Junos OS software upgrade or downgrade from Junos OS Release 15.1X49-D120 using the **unlink** option, the installation of the new software image fails. PR1325527

VPNs

- On SRX Series devices, the VPN monitoring is not working correctly in Junos OS Release 15.1X49-D40. As a workaround, use the dead peer detection (DPD) to check peer liveliness. PR1163751
- On SRX5400, SRX5600, and SRX5800 devices, when CoS is enabled on the st0 interface and the incoming traffic rate destined for the st0 interface is higher than 300,000 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. As a workaround, configure the appropriate policer on the ingress interface to limit the traffic below 300,000 pps per SPU. PR1239021
- On SRX Series devices, if multiple traffic selectors are configured for a peer with IKEv2 reauthentication, only one traffic-selector will rekey at the time of IKEv2 reauthentication. The VPN tunnels of the remaining traffic selectors will be cleared without immediate rekey. New negotiation of those traffic selectors might be triggered through other mechanisms such as traffic or by peer. PR1287168
- On SRX Series devices, when the VPN monitoring feature is enabled, the st interfaces go down immediately. PR1295896
- On SRX Series devices, IPsec traffic statistics counters return 32-bit values, which might quickly overflow. PR1301688
- On SRX Series devices, IPsec VPN tunnels might go down when you commit the configuration from Junos Space, Junos script, or J-Web. PR1317664

Related Documentation

- Changes in Behavior and Syntax on page 5
- Known Behavior on page 7
- Known Issues on page 13
- Resolved Issues on page 17
- Migration, Upgrade, and Downgrade Instructions on page 22

Resolved Issues

This section lists the issues fixed in hardware and software in Junos OS Release 15.1X49-D130. For Resolved Issues information starting with Junos OS Release 15.1X49-D10 to Junos OS Release 15.1X49-D120, refer to the Release Notes listed in the Release 15.1X49 section at Junos OS for SRX Series page.

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)

- Unexpected SIP ALG behavior might occur after upgrading to Junos OS Release 12.3X48. PR1328266
- When the SIP ALG is enabled and NAT is configured, the device might reboot after a core file is generated. PR1330254

Authentication and Access Control

- Incomplete RSI is displayed on the configuration. PR1329967

Chassis Cluster

- On SRX5400, SRX5600, and SRX5800 devices, node 0 fabric errors caused a split-brain state and traffic loss on the device. PR1296866
- On SRX1500, SRX4100, and SRX4200 devices, ISSU might fail if LACP and interface monitoring are configured. PR1305471
- The **Route-change-timeout** does not work as expected in an active-active cluster. PR1314162
- When services offloading feature is enabled, the device changes TCP checksum value to 0x0000. PR1317650
- Inaccurate J-Flow records might be observed for output interface and the next hop. PR1332666

CLI

- CLI options are available to manage the packet forwarding engine handling the ARP throttling for NHDB resolutions. PR1302384

Dynamic Host Configuration Protocol (DHCP)

- JDHCP process drops the request packet if the request packet has option 55 (0) PAD included. PR1201413
- On SRX300 line devices the DHCP client cannot obtain an IP address. PR1317197

Flow-Based and Packet-Based Processing

- No alarm is generated when the FPC reports the **FI: Cell underflow** error. PR1076299
- Packet-forwarding traffic is stopped when a transient memory parity error is in an MPC Endpoint Mapper (EPM) port-group wedge. PR1220019
- If destination NAT and session affinity are configured with multiple traffic selectors in IPsec VPN, the traffic selector match might fail. PR1309565
- The flowd process might stop and generate a core file during failover between node 0 and node 1. PR1311412
- The IPsec tunnel might fail to establish if the **datapath-debug** configuration includes the **preserve-trace-order** option or the **record-pic-history** option or both options. PR1311454
- SRX Series device, drop packets with reason **Drop pak on auth policy, not authed**. PR1312676
- When you commit configuration changes involving deletion of the routing instance with the application tracking and the session-close log enabled for the zone, the packet forwarding engine generates a core file. PR1312757
- The flowd process might generate a core file if SSL firewall proxy profile is configured with a whitelist. PR1313451
- The flowd process might stop and generate a core file when advanced policy-based routing (APBR) is used. PR1314554
- On SRX550M devices, **phone-home.core.0.gz** is generated after the zeroization procedure. PR1315367
- Periodic PIM register loop during switch failure. PR1316428
- On SRX Series devices, the **fin-invalidate-session** command does not work when the services offloading feature is enabled on the device. PR1316833
- Return traffic through the routing instance might drop intermittently after changing the zone and routing-instance configuration on the st0.x interface. PR1316839
- The default route is lost after the system returns to zero. PR1317630
- The flowd process stops when AppQoS is configured on the device. PR1319051

- The OSPF peers are unable to establish neighbors between the LT interfaces of the logical systems. PR1319859
- Inaccurate J-Flow records were seen for the output interface and next hop. PR1322538
- Flowd core files are generated on both nodes, causing an outage. PR1324476
- The software next-hop table is full with **RT_PFE: NH IPC op 1 (ADD NEXTHOP) failed, err 6 (No Memory) peer_class 0, peer_index 0 peer_type 10**. PR1326475
- On SRX Series devices, the Sky ATP advance anti-malware service plane was disconnecting and not reconnecting. PR1329238
- The FPC is dropped or gets stuck in present state when intermittent control link heartbeats are seen. PR1329745
- On SRX Series devices, the sessions might close because of the "idle Timeout junos-fwauth-adapter" logs. PR1330926
- The IPv6 traffic does not work as expected on IOC3 with the services offloading (NP cache) feature. PR1331401

In-service Software Upgrade (ISSU)

- ISSU between two Junos OS 15.1X49 releases might fail and generate a flowd core file. PR1320030
- The ISSU upgrade might fail due to the packet forwarding engine generating a core file. PR1328665

Interfaces and Chassis

- Unable to add IRB and AE interface. PR1310791
- An error does not occur at each commit or commit check if autonegotiation is disabled but the speed and duplex are not configured on the interface. PR1316965
- If an interface is configured with the Ethernet switching family, we recommend that you do not configure **vlan-tagging**. PR1317021
- The interface might be brought down by IP monitoring at the time of committing a configuration due to incorrect interface status computing. PR1328363
- Mechanism to hold down PIM designated router election on device recovery. PR1343967

Intrusion Detection and Prevention (IDP)

- IDP policy compilation can be triggered even if changes unrelated to IDP are done to the configuration. PR1283379
- The IDP PCAP feature is enhanced as follows:
  - The first valid **packet-log-id** value will no longer be zero.
  - The algorithm for assigning the **packet-log-id** is improved to reduce the duplicate entries and ID rollover events among devices with multiple SPUs.

PR1297876

- The file descriptor might leak during the automatic update of the security package. PR1318727

J-Web

- J-Web authentication fails when a password includes a backslash. PR1316915
- J-Web dashboard was displaying the last updated time incorrectly. PR1318006
- J-Web display problems occur for security policies. PR1318118
- J-Web was not displaying wizards on the dashboard. PR1330283

Layer 2 Ethernet Services

- Starting in Junos OS Release 15.1X49-D130, in DHCP relay configuration the **vpn** option name has been renamed to **source-ip-change**. PR1318487
- On SRX1500 devices, VLAN popping and pushing does not work over Layer 2 circuits. PR1324893

Network Management and Monitoring

- SRX300 line devices become unresponsive due to the **/cf/var: filesystem full** error. PR1289489

Platform and Infrastructure

- SRX Series devices require sensor-specific temperature thresholds to be implemented on the device. PR1199447
- An I2C bus timeout causes SFP thread hogging and MPC restart. PR1260517
- On SRX5400, SRX5600, and SRX5800 devices, The packet captured by datapath-debug on an IOC2 card might be truncated. PR1300351
- Inconsistent flow-control status on the reth interface is observed. PR1302293
- Internal host directory **/var/tmp/** might fail to mount on SRX4100 and SRX4200 devices. PR1311733
- On SRX1500 devices, when the power supply fails, the trap sent might contain incorrect information. PR1315937
- On SRX5400, SRX5600, and SRX5800 devices, SPC2 XLP stops processing packets in the ingress direction after repeated RSI collections. PR1326584
- NTP synchronization fails and switches to local clock. PR1331444

Routing Policy and Firewall Filters

- The number of address objects per policy for SRX5400, SRX5600, and SRX5800 devices is increased from 4096 to 16,000. PR1315625

Routing Protocols

- Dedicated BFD does not work on SRX Series devices. PR1312298
- On a chassis cluster device with BMP configured, the rpd process might stop when it gracefully terminates. PR1315798

Software Installation and Upgrade

- The **request system reboot node in/at** command results in an immediate reboot instead of rebooting at the allotted time. PR1303686

User Firewall and Authentication

- The JIMS server stops responding to requests from SRX Series devices. PR1311446
- User firewall has a command to fetch the user-group mapping from the active directory server. PR1327633

User Interface and Configuration

- Deactivated security policy is unexpectedly moved after committing a new policy configuration. PR1248882

Unified Threat Management (UTM)

- The whitelist function in **syn-flood** does not work. PR1332902

Switching

- Double VLAN tagging (**vlan-tags**) is not configurable after an upgrade to Junos OS Release 12.3X48. PR1310410

Unified Threat Management (UTM)

- New configuration is available to configure the web-authentication timeout. PR1339627

VPNs

- Occasionally, next-hop tunnel binding (NHTB) is not installed during rekey for VPN using IKEv1. PR1281833
- SSL firewall proxy does not work if root-ca has fewer than four characters. PR1319755

- Assignment of duplicate IP on multiple interfaces can affect the VPN connection. PR1330324
- SNMP for **jnxIpSecTunMonVpnName** does not work. PR1330365

Related Documentation

- Changes in Behavior and Syntax on page 5
- Known Behavior on page 7
- Known Issues on page 13
- Resolved Issues on page 17
- Migration, Upgrade, and Downgrade Instructions on page 22

Documentation Updates

There are no errata or changes in Junos OS Release 15.1X49-D130 for the SRX Series documentation.

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 and Downgrade Support Policy for Junos OS Releases and Extended End-Of-Life Releases on page 22

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

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

You can upgrade or downgrade to the EEOL release that occurs directly before or after the currently installed EEOL release, or to two EEOL releases before or after. For example, Junos OS Releases 12.3X48, 15.1X49, 17.3 and 17.4 are EEOL releases. You can upgrade from Junos OS Release 15.1X49 to Release 17.3 or from Junos OS Release 15.1X49 to Release 17.4. However, you cannot upgrade directly from a non-EEOL release that is more than three releases ahead or behind.

Upgrade from Junos OS Release 17.4 to successive Junos OS Release, 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

- Changes in Behavior and Syntax on page 5
- Known Behavior on page 7
- Known Issues on page 13
- Resolved Issues on page 17
- Migration, Upgrade, and Downgrade Instructions on page 22

Product Compatibility

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

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

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

31, January 2019—Revision 7— Junos OS 15.1X49-D130 – SRX Series.

28, January 2019—Revision 6— Junos OS 15.1X49-D130 – SRX Series.

12, July 2018—Revision 5— Junos OS 15.1X49-D130 – SRX Series.

07, June 2018—Revision 4— Junos OS 15.1X49-D130 – SRX Series.

03, May 2018—Revision 3— Junos OS 15.1X49-D130 – SRX Series.

22, March 2018—Revision 2— Junos OS 15.1X49-D130 – SRX Series.

08, March 2018—Revision 1— Junos OS 15.1X49-D130 – SRX Series.