Release Notes: Junos® OS Release 15.1X49-D140 for the SRX Series

Release 15.1X49-D140
31 January 2019
Revision 5

Contents

Introduction

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

These release notes accompany Junos OS Release 15.1X49-D140 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-D140 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-D140 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-D130, refer to the Release Notes listed in the Release 15.1X49 section at Junos OS for SRX Series page.

Release 15.1X49-D140 Software Features

General Packet Radio Service (GPRS)

- **GTP tunnel enhancements (SRX1500, SRX4100, SRX4200, SRX5400, SRX5600, SRX5800, and vSRX instances)**—Starting in Junos OS Release 15.1X49-D140, GTP is enhanced to update the GTP tunnel and session lifetime to avoid GTP tunnel timeout issues. Even if the GTP-U validation is disabled, the GTP-U traffic can refresh the GTP tunnel to avoid timeout. Only GTPv1 and GTPv2 tunnels, not GTPv0 tunnels, are refreshed by the GTP-U traffic. Before refreshing the GTP tunnel, you must enable the GTP-U distribution. The GTP-U tunnel has a session attach flag that is checked when scanning the GTP-U tunnels. If the session attach flag is present in the tunnel, the timer will not decrease and prevents the tunnel from being deleted while the tunnel is still in service.

NOTE: On SRX5400, SRX5600, and SRX5800 devices, the number of GTP tunnels supported per SPU is increased from 200,000 tunnels to 600,000 tunnels per SPU, for a total of 2,400,000 tunnels per SPC2 card.

Related Documentation

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-D140.

Chassis Cluster

- IP Monitoring—Starting with Junos OS Release 15.1X49-D140, on all SRX Series devices, if the reth interface is in bundled state, IP monitoring for redundant groups is not supported on the secondary node. This is because the secondary node sends reply

using the lowest port in the bundle which is having a different physical MAC address. The reply is not received on the same physical port from which the request is sent. If the reply comes on the other interface of the bundle, then the internal switch drops it.

- Power Entry Module—Starting with Junos OS Release 15.1X49-D140, when you use DC PEM on SRX Series devices operating in chassis cluster mode, the output of **show chassis power** command shows **DC input: 48.0 V input (57000 mV)**. The value **48.0 V input** is a fixed string and can be interpreted as a measured input voltage. The acceptable range of DC input voltage accepted by the DC PEM is 40 to 72 V. The **(57500 mV)** is a measured value, but is not related with the input. It is the actual output value of the PEM and the value is variable. The **DC input:** from **show chassis power** and **Voltage:** information from **show chassis environment pem** command output are removed for each PEM.

Intrusion Detection and Prevention (IDP)

- Custom Attack (SRX Series)—Starting with Junos OS Release 15.1X49-D140, the maximum number of characters allowed for a custom attack object name is 60. You can validate the statement using the CLI **set security idp custom-attack** command.

VPNs

- **Error message is displayed when a remote address of 0::0 (IPv6) is configured on site-to-site VPNs**—Starting with Junos OS Release 15.1X49-D140, on all SRX Series devices and vSRX instances, when you configure the traffic-selector with a remote address of 0::0 (IPv6), the following **"error: configuration check-out failed"** message is displayed when performing the commit and the configuration checkout fails.

Related Documentation

- New and Changed Features on page 4
- Known Behavior on page 5
- Known Issues on page 8
- Resolved Issues on page 13
- Migration, Upgrade, and Downgrade Instructions on page 18

Known Behavior

This section contains the known behaviors, system maximums, and limitations in hardware and software in Junos OS Release 15.1X49-D140.

AppSecure

- 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 that you change the SSL-I configuration to enable or disable the certificate revocation list (CRL) checking instead of the CA profile configuration. PR1143462

- On SRX1500 devices in a chassis cluster with Sky ATP solution deployed, if you disable and then reenable CRL checking of certificate validity, the system does not reenable CRL checking. PR1144280

Chassis Cluster

- SRX5400, SRX5600, and SRX5800 devices operating in a chassis cluster might encounter the em0 or em1 interface link failure on either of the nodes, which results in split-brain condition. That is, both devices are unable to detect each other. If the failure occurs on the secondary node, the secondary node is moved to the disabled state.

  This solution does not cover the following cases:

  - em0 or em1 failure on primary node
  - HA process restart
  - Preempt conditions
  - Control link recovery

- On SRX1500 devices in a chassis cluster, the CRL check might fail because of the nonavailability of the CRL information for a CA profile. Because of the CRL check 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 SRX340 and SRX345 devices, half-duplex mode is not supported, because BCM53426 does not support half-duplex mode. BCM5342X SoC port configurations and BCM53426 do not have a QSGMII interface. Only the QSGMII port supports half-duplex mode. PR1149904

Flow-Based and Packet-Based Processing

- 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 event mode. When the log buffer size is 1000, the Packet Forwarding Engine generates log bursts when there are more than 30 entries and then more logs are dropped. PR1133757
- On SRX1500 devices, when Security Intelligence (SecIntel) is loading feed to a service card, the log message prints a message showing that the data feed is loaded to PIC 1. However, there is no PIC 1 on the device, so the data feed must be loaded to PIC 0. PR1144765
- On SRX5400 devices, if a user or a 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 might time out, leading to a high CPU utilization. PR1157073
- On SRX Series devices, because of the SRX5K-MPC (IOC2) lookup, the hardware engine counts one extra packet for each session wing installed in the SRX5K-MPC (IOC2) services-offload. The packet counters in the CLI for the servics-offload sessions

from the SRX5K-MPC (IOC2) are always up by 1, compared to the SRX5K-MPC3-100G10G (IOC3), for the same services-offload scenario. PR1157158

- On SRX Series devices, after a 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 changed from route mode to switch or mixed mode. This is a configuration-related warning message and might not reflect the current running state of the interface mode. PR1165345
- 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

Interfaces and Routing

- In Junos OS Release 15.1X49-D140, on SRX4100 and SRX4200 devices, you can get the NIC statistics (like, Total octets, Total packets, Unicast packets, Multicast packets, CRC/Align errors, FIFO errors, MAC pause frames) by executing **show interfaces extensive** CLI command.
- 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 an IPv6 address is configured on a Layer 3 VLAN interface, the VLAN interface might take longer to boot up during the device bootup. The IPv6 duplicate address detection (DAD) cannot run successfully for a long time, resulting in the IPv6 address remaining in a tentative state. PR967786
- On SRX1500 devices, when a 1G SFP-T is used on 1G SFP ports (ge-0/0/12 to ge-0/0/15), the ge interface does not operate at 100Mbps speed. PR1133384
- IPv6 ping to an interface might not work if the interface is configured in a virtual routing instance and inet6 is the only family configured on the interface. PR1142936
- 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

Layer 2 Ethernet Services

- 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

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 have a size 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 the CPU usage is very high (above 95 percent), there is a possibility that the connection between AAMW and PKID process can stop. In this case, the AAMW process remains in an initializing state until the connection is established. PR1142380

VPNs

- On SRX Series devices, in a Layer 3 VPN scenario, in selective packet mode the MPLS packet is dropping the VPN packet when it is at the end of the MPLS path. After parsing the MPLS header, the MPLS packet must go to the IP process. But, after adding the native VLAN ID, the next header parse is wrong in **fwdd_parse_lsi**. This issue occurs because the packet pointer is not updated, leading to the behavior with or without native VLAN ID. PR1204186

Related Documentation

- New and Changed Features on page 4
- Changes in Behavior and Syntax on page 4
- Known Issues on page 8
- Resolved Issues on page 13

Known Issues

This section lists the known issues in hardware and software in Junos OS Release 15.1X49-D140.

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, TLS version 1.0 and TLS version 1.1 SSL protocols are blocked because of reported security vulnerabilities. This change might affect users accessing J-Web or the Web authentication GUI, or using dynamic VPN through the Pulse client when using an older Junos OS version or lower version browsers where TLS version 1.2 protocol is not supported. This change affects Junos OS Release 15.1X49-D100 and all later releases. PR1283812

Chassis Clustering

- On SRX550M devices in a chassis cluster, traffic loss for about 10 seconds is observed when there is a power failure on the active chassis cluster node. PR1195025
- On SRX Series devices, RG1+ failover occurs because the FPC or SPU failure might trigger the MAC move protection on the neighbor switch. PR1333505
- For chassis cluster cold synchronization, the GTP-U session will be synchronized to a secondary device before the GTP-U tunnel, causing the GTP-U tunnel to not be linked with the corresponding GTP-U flow session. The GTP-U traffic does not refresh the GTP-U tunnel until a new session is created. If the old session does not age out on the primary device, all the GTP-U traffic will go through the fast path and no session creation event is triggered, then the GTP-U time out period, the tunnels on secondary device will age out earlier. PR1353791

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
- Memory leak might occur if the TCP proxy handles the traffic. This issue might cause traffic loss. PR1282647
- On SRX Series devices, sometimes the time range slider does not work for all events and individual events in the Google Chrome or the Firefox browser. PR1283536
- When the system processes, security intelligence is disabled and then enabled, the security intelligence works incorrectly. PR1284550
- On SRX300, SRX320, SRX340, and SRX345 devices, if there is power outage many times in a short period of time, the device might end up getting stuck in the loader prompt. PR1292962
- On SRX Series devices with chassis cluster enabled, the issue occurs when multicast traffic passes through the logical systems. The ingress interface of the multicast session in the first logical system is reth 2.0, which belongs to redundancy group 2. Redundancy

group 2 is active on node 1. The ingress interface of the multicast session in the second logical system will be the PLT interface, which belongs to redundancy group 1. The redundancy group 1 is active on node 0. So, the multicast session in the second logical system will be active on node 0. This might cause the multicast active or backup session to not be aligned with traffic forwarding. PR1295893

- On SRX Series devices, when you run the **clear nhdb statistics** command on an SPU PIC, the SPC might reset. PR1346320

Interfaces and Chassis

- On SRX300, SRX320, SRX340, SRX345, and SRX550M devices, for logical interface (IFL) scaling, without the **per-unit-scheduler** configured, the total number of IFLs is limited to 2048 and with the **per-unit-scheduler** configured on the IFD interface the total number of IFLs is limited to the CoS scheduler sub-unit upper limit, which is 2048. So, the IFL **max-number** for the **per-unit-scheduler** should be 2048 minus the number of physical interfaces. PR1138997
- If a 3G modem is configured without a 3G modem being inserted, the device might erroneously try to access the 3G thread and stop when the device cannot find the 3G thread. Traffic interruption might occur, causing the flowd process to stop. When this issue occurs, delete the 3G modem configuration to restore the issue. PR1151904
- When application tracking is configured on the zone with loopback interface, SSH to the loopback interface of the device works incorrectly. PR1343736

J-Web

- On SRX Series devices, DHCP relay configuration under **Configure > Services > DHCP > DHCP Relay** page is removed from the 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 SRX4100 devices, a security policy page in J-Web does not load when it has 40,000 firewall policies configured. Navigate to **Configure> Security> Security Policy** page. PR1251714
- On SRX Series devices, an issue occurs when you 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 displays a 404 error message. PR1267751
- 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 indicate that no data is available even when the device has a large amount of data. PR1282666
- On SRX Series devices, the CLI terminal does not work for Google Chrome version greater than 42. You can use Internet Explorer 10 or 11 or Mozilla Firefox 46 browsers to use the CLI terminal. PR1283216

Layer 2 Ethernet Services

- On SRX Series devices configured as a DHCP server (using the jdhcpd process), when the DHCP server receives 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

Logical Systems

- On SRX Series devices with chassis cluster enabled and logical systems configured, when any ALG (except DNS ALG) is enabled and NAT is configured for the ALG sessions, the flowd process on the secondary node might stop. PR1343552

Platform and Infrastructure

- On SRX Series devices running FreeBSD 6-based Junos OS software, the system might panic when a USB flash drive with a mounted file system is physically detached by a user. PR695780
- On SRX5800 devices, even though the system service REST API is configured and committed, all the configuration changes in this commit will not take effect. This issue occurs because the REST API process fails to come up and the interface IP address is not available during startup. The configuration is not read by the Routing Engine. PR1123304
- On SRX Series devices, the flowd process might stop and cause traffic outage if the SPU CPU usage is higher than 80 percent. Therefore, some threads are in waiting status and the watchdog cannot be toggled timely, causing the flowd process to stop. PR1162221
- On SRX Series devices, the mgd core files are generated during RPC communication between the SRX Series device and Junos Space or CLI with % present in the description or annotation. PR1287239
- On SRX5600 and SRX5800 devices in a chassis cluster, when a secondary Routing Engine is installed to enable dual control links, the **show chassis hardware** command might display the same serial number for both the Routing Engines on both the nodes. PR1321502

Unified Threat Management (UTM)

- On SRX Series devices, if advanced anti-malware service (AAMW) is enabled, and the SMTP is configured in the AAMW policy with fallback permission enabled under the long network latency between the devices and AWS 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 remain in the outbox of the sender, and the receiver might not receive the e-mail. PR1254088

- In case failover occurs while the device is handling many concurrent Web authentications, the httpd CPU usage might be high. PR1352133

Upgrade and Downgrade

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

VPNs

- On SRX Series devices, if an IPsec VPN tunnel is established using IKEv2 because of bad SPI, packet drop might be observed during the **CHILD_SA rekey** when the device is the responder for this rekey. PR1129903
- On SRX1500 devices in a chassis cluster with Sky ATP solution deployed, if you disable and then reenable the CRL checking of certificate validity, the system does not reenable the CRL checking. PR1144280
- On SRX Series devices, the VPN monitoring feature is not working correctly in Junos OS Release 15.1X49-D40. Use 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 st0 interface is higher than 3,00,000 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. We recommend that you configure the appropriate policer on the ingress interface to limit the traffic below 3,00,000 pps per SPU. PR1239021
- On SRX Series devices, in case 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 trigger through other mechanisms such as traffic or by peer. PR1287168
- In Junos OS Release 15.1X49-D140, if the CA profile name has a dot "." then the PKI process faces issues if it is restarted at any point. PR1351727

Related Documentation

- New and Changed Features on page 4
- Changes in Behavior and Syntax on page 4
- Known Behavior on page 5
- Resolved Issues on page 13
- Migration, Upgrade, and Downgrade Instructions on page 18

Resolved Issues

This section lists the issues fixed in hardware and software in Junos OS Release 15.1X49-D140. For Resolved Issues information starting with Junos OS Release 15.1X49-D10 to Junos OS Release 15.1X49-D130, 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 Identification

- On SRX devices, application identification is inconsistent for UDP based bidirectional traffic applications. PR1346180

Application Layer Gateways (ALGs)

- The flowd process generates a core file when the SIP ALG is enabled. PR1352416
- SIP calls might drop because of the 10,000 limit per SPU. PR1337549

Authentication and Access Control

- On SRX Series devices, the sessions might close because of the **idle Timeout junos-fwauth-adapter** error log message. PR1330926
- The uacd process is unstable after upgrading to Junos OS Release 12.3X48 and later releases. PR1336356
- On SRX Series devices, the **show version detail** command returns an error message: **Unrecognized command (user-ad-authentication)** while configuring the useridd settings. PR1337740
- A new configuration is available to configure the web-authentication timeout. PR1339627

Chassis Clustering

- IP monitoring is working incorrectly when one node is in secondary-hold and the priority of the primary node becomes 0. PR1330821
- After the primary node or the secondary node restarts, the FPC module goes offline on the secondary node. PR1340116

Class of Service (CoS)

- Packets go out of order on SPC2 cards with IOC1 or FIOC cards. PR1339551

Dynamic Host Configuration Protocol (DHCP)

- JDHCP process drops the request packet if the request packet has option 55 (0) PAD included. PR1201413

Flow-Based and Packet-Based Processing

- A memory leak might occur in the appidd process while updating an application signature package. PR1308863
- If the Sky ATP cloud feed updates, the Packet Forwarding Engine might stop causing intermittent traffic loss. PR1315642
- Periodic PIM register loop is observed during switch failure. PR1316428
- The MPC cards might drop traffic in the event of high temperatures. PR1325271
- The FPC is dropped or hangs in the present state when the intermittent control link heartbeat is observed. PR1329745
- The IPv6 traffic works incorrectly on the SRX5K-MPC3-100G10G (IOC3) with the NP cache feature. PR1331401
- NTP synchronization fails and switches to a local clock. PR1331444
- Simultaneous commit on the device triggers configuration integrity check failure and halts the device when the Trusted Platform Module (TPM) feature is used. PR1332605
- If the Trusted Platform Module (TPM) is enabled, the configuration integrity failure occurs when there is a power loss for few seconds after the commit. PR1351256
- SRX1500 fan speed often fluctuates. PR1335523
- The **show vlans detail no-forwarding** command in the RSI does not display any information, because the **no-forwarding** option is not supported. PR1336267
- Two-way active measurement protocol (TWAMP) client, when configured in a routing instance, does not work after a reboot. PR1336647
- On the front panel LED, the red alarm goes on after an RG0 failover is triggered when the flowd process stops. PR1338396
- The flowd process might stop when the syn-proxy function is used. PR1343920
- SRX1500 devices might encounter a failure while accessing the SSD drive. PR1345275
- The REST API is not working on the SRX320-POE device. PR1347539
- The Packet Forwarding Engine might suddenly stop forwarding traffic if the Layer 2 switching is configured. PR1348635

- File download stops over a period of time when the TCP proxy is activated through the antivirus or Sky ATP. PR1349351
- When a J-Flow related configuration is deleted, the forwarding plane begins to drop packets. PR1351102

Interfaces and Routing

- Incorrect ingress packet per second is observed on the MPLS enabled interface. PR1328161
- On SRX Series devices in a chassis cluster, the IRB interface does not send an ARP request after clearing the ARP entries. PR1338445
- Packet reorder occurs on the traffic received on the PPP interface. PR1340417
- On SRX1500 devices in a chassis cluster, when the PPPoE interface is configured over the ae or the reth interface, reboot of the cluster nodes might occur. PR1341968
- On SRX Series devices, when the VPLS interface receives a broadcast frame, the device sends this frame back to the sender. PR1350857

Intrusion Detection and Prevention (IDP)

- The control plane CPU utilization is high when the IDP feature is in use. PR1283379
- The IDP PCAP feature has been improved. PR1297876
- The output of the **show security idp status** command does not accurately reflect the number of decrypted SSL or TLS sessions being inspected by the IDP. PR1304666
- If IDP and SSL forward proxy whitelist are configured together, the device might generate a core file. PR1314282
- Unable to load the IDP policy because not enough heap memory is available. PR1347821

J-Web

- In J-Web when you click the **SKIP TO JWEB OPTIONS**, the Google Chrome browser automatically redirects. PR1284341
- The zone drop-down list does not include the available zones; hence the zone address book or address sets cannot be configured. PR1308684
- Unable to delete the dynamic VPN user configuration. PR1348705
- Security policies search button on the J-Web does not work with Internet Explorer version 11. PR1352910

Layer 2 Ethernet Services

- The default gateway route might be lost after an RG0 failover in a chassis cluster. PR1334016

Network Address Translation (NAT)

- Arena utilization on an FPC increases and then resumes to a normal value. PR1336228

Platform and Infrastructure

- The SRX4200 devices continuously logs the chassisd messages **pem_tvp_periodic cbd=8f51000 slot=0, state=1**. PR1292700
- IPsec VPN tunnels might go down when you commit the configuration from Junos Space, Junos OS script, or J-Web. PR1317664
- The output of the **show chassis environment pem** and the **show chassis power** commands do not show the DC input value correctly. PR1323256
- The following log is generated every 5 seconds: **No Port is enabled for FPC# on node0**. PR1335486
- The PPMD process might stop under certain conditions after an upgrade. PR1335526
- In RSI, a mandatory argument is missing for the **request pfe execute** and the **show usp policy counters** commands. PR1341042

Routing Policy and Firewall Filters

- DNS name entries in policies might not be resolved if the routing instance is configured under a system name-server. PR1347006
- If many custom applications are configured in the policies, the flowd process might stop. PR1347822

Routing Protocols

- OpenSSL Security Advisory [07 Dec 2017]. Refer to https://kb.juniper.net/JSA10851 for more information. PR1328891
- Mechanism is needed to hold down PIM-designated router election on device recovery. PR1343967
- Dedicated BFD does not work on SRX Series devices. PR1347662
- A new CLI command is required to prevent traffic loss during a disaster recovery failover scenario. PR1352589

System Logs

- The log messages on GUMEM parity error are observed seen for MPC or FPC with XM chipset. PR1200503

- The following log messages are displayed on the device: **L2ALM Trying peer/master connection, status 26**. PR1317011

Upgrade and Downgrade

- On SRX1500, SRX4100, and SRX4200 devices, downgrading from Junos OS Release 17.4 to Junos OS Release 15.1X49 or Junos OS Release 17.3 results in the factory-default configuration being loaded on the device. PR1330180
- Junos OS upgrade failed with an unlink option on the TVP device. PR1344449
- The command **show system firmware** displays the old firmware image. PR1345314

VPNs

- IPsec traffic statistics counters return 32-bit values, which might quickly overflow. PR1301688
- Auto Discovery VPN (ADVPN) tunnels might flap with the spoke error **no response ready yet**, leading to IKEv2 timeout. PR1305451
- For FIPS conformance, the PKI process syslog must be generated during key-pair deletion. PR1308364
- The IPsec VPN connections might be affected by changing the assignment of the duplicate IP address on multiple interfaces. PR1330324
- The kmd core files might be observed when all the VPNs are down. PR1336368
- The IPsec replay error for Z-mode traffic is observed. PR1349724
- Policy-based VPN is not working with the virtual router. PR1350123

Related Documentation

- New and Changed Features on page 4
- Changes in Behavior and Syntax on page 4
- Known Behavior on page 5
- Known Issues on page 8
- Migration, Upgrade, and Downgrade Instructions on page 18

Documentation Updates

There are no errata or changes in Junos OS Release 15.1X49-D140 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 18

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

- New and Changed Features on page 4
- Changes in Behavior and Syntax on page 4
- Known Behavior on page 5
- Known Issues on page 8
- Resolved Issues on page 13

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

31, January 2019—Revision 5— Junos OS 15.1X49-D140 – SRX Series.

28, January 2019—Revision 4— Junos OS 15.1X49-D140 – SRX Series.

12, July 2018—Revision 3— Junos OS 15.1X49-D140 – SRX Series.

14, June 2018—Revision 2— Junos OS 15.1X49-D140 – SRX Series.

30, May 2018—Revision 1— Junos OS 15.1X49-D140 – SRX Series.