Junos OS Release 17.3R1 for vSRX Release Notes

Release 17.3R1
8 February 2021
Revision 3

Contents

Introduction

This release note accompanies Junos OS Release 17.3R1 for vSRX. It describes new and changed features, known behavior, and known and resolved problems in the software.

vSRX is a virtual security appliance that provides security and networking services in virtualized private or public cloud environments. It runs as a virtual machine (VM) on x86 servers that support virtualization, and it enables advanced security and routing at the network edge in multitenant virtualized environments.

vSRX is built on Junos OS and delivers security and networking features similar to those available on SRX Series Services Gateways.

You can also find the vSRX release notes in the Juniper Networks TechLibrary, located at https://www.juniper.net/documentation/.

New and Changed Features

IN THIS SECTION

This section describes new features and enhancements to existing features in Junos OS Release 17.3R1 for vSRX.

New Features for Junos OS Release 17.3R1 for vSRX

Junos OS Release 17.3R1 for vSRX is at feature parity with Junos OS Release 15.1X49-D90 for vSRX.

This section describes new features in Junos OS Release 17.3R1 for vSRX.

vSRX on Microsoft Azure Cloud

Microsoft Azure Cloud support—Starting in Junos OS Release 17.3R1 for vSRX, you can add a vSRX virtual security appliance to a Microsoft Azure virtual network to provide networking security features. The vSRX protects the workloads that run within the virtual network on the Microsoft Azure Cloud.

[See vSRX Guide for Microsoft Azure Cloud]

> **NOTE:** For the initial release of vSRX on Microsft Azure, only the BYOL model is supported.

vSRX on Microsoft Hyper-V

Microsoft Hyper-V support—Starting in Junos OS Release 17.3R1 for vSRX, you can add a vSRX virtual security appliance to a Microsoft Hyper-V Server 2012 R2 or Hyper-V Server 2012 to provide networking security features for the virtualized server computing environment. The vSRX VM runs on Microsoft Hyper-V as a child partition.

[See vSRX Guide for Microsoft Hyper-V]

> **NOTE:** Please note that vSRX chassis clustering is not supported on Microsoft Hyper-V Server 2012 R2 or Hyper-V Server 2012.

vSRX on KVM Scale-Up Performance Enhancements

vSRX on KVM: support for 8 vCPUs and 16 GB vRAM and PCI passthrough support —Starting in Junos OS Release 17.3R1 for vSRX, the vSRX virtual appliance supports the following functionality 1 control plane vCPU, 8 data plane vCPUs, 16 GB vRAM, and Peripheral Component Interconnect (PCI) passthrough support (Intel XL710 NICs). In addition, vSRX now provides support for Intel X710/XL710 physical NICs for SR-IOV.

[See vSRX Guide for KVM.]

IDP

IPS signature package update (SRX Series and vSRX instances)—Starting in Junos OS Release 17.3R1, when you upgrade from Junos OS Release 12.3X48 or 15.1X49 to Junos OS Release 17.3 or downgrade

from Junos OS Release 17.3 to Junos OS Release 12.3X48 or 15.1X49, you must update the IPS signature package to avoid any IDP configuration commit failures. Update the IPS signature package by:

- Downloading the IPS signature package
- Installing the IPS signature package update when the download completes

> **NOTE:** When you upgrade from Junos OS Release 15.1X49 to Junos OS Release 17.3, the following warning message is displayed:
>
> **WARNING: A full install of the security package is required after reboot.**
>
> **WARNING: Please perform a full update of the security package using**
>
> **WARNING: "request security idp security-package download full-update"**
>
> **WARNING: followed by**
>
> **WARNING: "request security idp security-package install"**

[See Managing the IPS Signature Database (CLI).]

Junos OS XML API and Scripting

Support for Python language for commit, event, op, and SNMP scripts (SRX1500, SRX4100, SRX4200, SRX5400, SRX5600, and SRX5800 devices and vSRX instances)—Starting in Junos OS Release 17.3R1, you can author commit, event, op, and SNMP scripts in Python on devices that include the Python extensions package in the software image. Creating automation scripts in Python enables you to take advantage of Python features and libraries as well as leverage Junos PyEZ APIs supported in Junos PyEZ Release 1.3.1 and earlier releases to perform operational and configuration tasks on devices running Junos OS. To enable execution of Python automation scripts, which must be owned by either root or a user in the Junos OS **super-user** login class, configure the **language python** statement at the **[edit system scripts]** hierarchy level, and configure the filename for the Python script under the hierarchy level appropriate to that script type. Supported Python versions include Python 2.7.

[See Understanding Python Automation Scripts for Devices Running Junos OS.]

Management

Support for adding non-native YANG modules to the Junos OS schema (SRX345, SRX1500, SRX4100, SRX4200, SRX5400, SRX5600, and SRX5800 devices and vSRX instances)—Starting in Junos OS Release 17.3R1, you can load custom YANG models on devices running Junos OS to add data models that are not natively supported by Junos OS but can be supported by translation. Doing this enables you to extend the configuration hierarchies and operational commands with data models that are customized for your

operations. The ability to add data models to a device is also beneficial when you want to create device-agnostic and vendor-neutral data models that enable the same configuration or RPC to be used on different devices from one or more vendors. You can load custom YANG modules by using the request system **yang add** operational command.

[See Understanding the Management of Non-Native YANG Modules on Devices Running Junos OS.]

User Interface and Configuration

Support for configuring the ephemeral database using the NETCONF and Junos XML protocols (SRX300, SRX320, SRX340, SRX345, SRX550M, SRX1500, SRX4100, SRX4200, SRX5400, SRX5600, and SRX5800 devices and vSRX instances)—Starting in Junos OS Release 17.3R1, NETCONF and Junos XML protocol client applications can configure the ephemeral configuration database, which is an alternate configuration database that enables multiple clients to simultaneously load and commit configuration changes on a device running Junos OS and with significantly greater throughput than when committing data to the candidate configuration database. Junos OS provides a default instance and up to eight user-defined instances of the ephemeral configuration database. The device's active configuration is a merged view of the committed configuration database and the configuration data in all instances of the ephemeral configuration database. Ephemeral configuration data is volatile and is deleted upon rebooting the device.

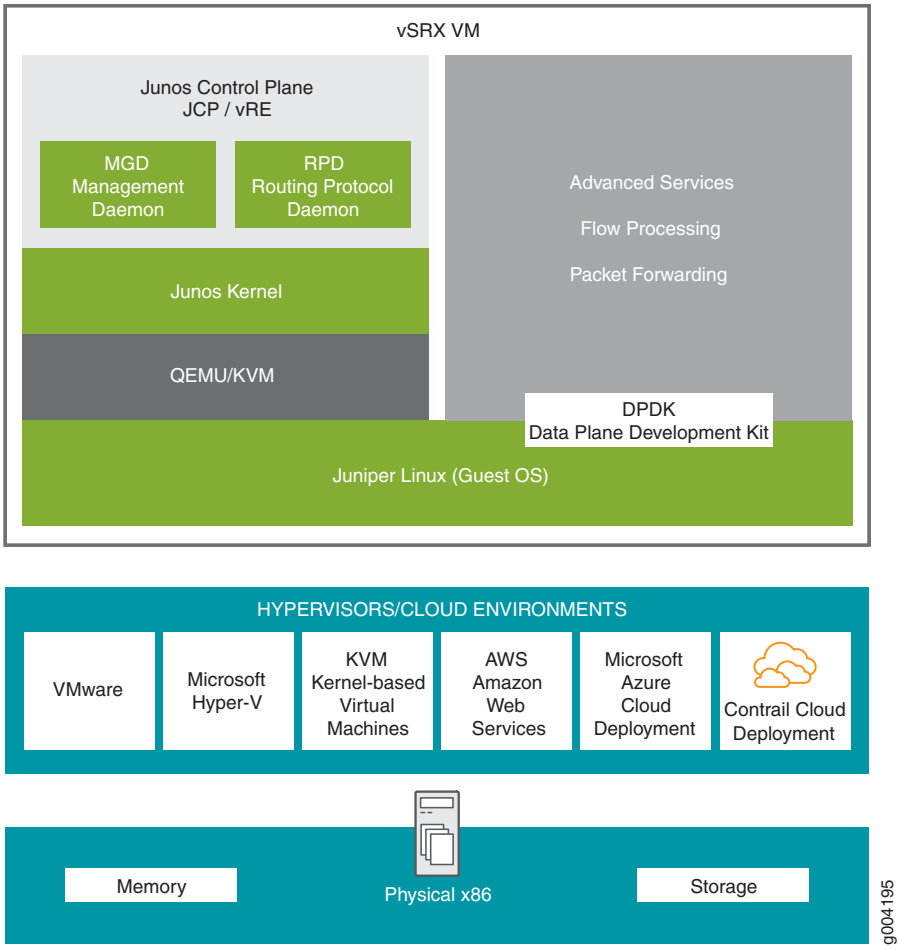
[See Understanding the Ephemeral Configuration Database.]

vSRX Architecture Illustration

vSRX Architecture

Figure 1 on page 7 is a high-level illustration of the vSRX architecture as of Junos OS Release 17.3R1.

Figure 1: vSRX Architecture



Supported Features

For details about Junos OS features supported on vSRX, see Feature Explorer: vSRX.

Supported Features References

Table 1 on page 8 lists documentation references to Junos OS features that are supported on vSRX. See "Known Behavior" on page 10 and SRX Series Features Not Supported on vSRX for specific support limitations.

NOTE: Some vSRX features require a license. See vSRX License Model Numbers for more details.

Table 1: Documentation References for Junos OS Features Supported on vSRX

Feature	Feature Documentation	vSRX Platform
Application Firewall (AppFW)	Application Firewall Overview	VMware, KVM, Contrail, AWS, Azure, and Hyper-V
Application Identification (AppID)	Understanding Application Identification Techniques	VMware, KVM, Contrail, AWS, Azure, and Hyper-V
Application Layer Gateways (ALGs)	ALG Overview	VMware, KVM, Contrail, AWS, Azure, and Hyper-V
Application Quality of Service (AppQoS)	Understanding Application QoS (AppQoS)	VMware, KVM, Contrail, AWS, Azure, and Hyper-V
Attack Detection and Prevention (ADP)	Attack Detection and Prevention Overview	VMware, KVM, Contrail, AWS, Azure, and Hyper-V
Chassis cluster support for Virtio driver	Chassis Cluster Overview	KVM
Chassis cluster support for VMXNET3 driver	Chassis Cluster Overview	VMware
Class of service (CoS)	Understanding Class of Service	VMware, KVM, Contrail, AWS, Azure, and Hyper-V
Dynamic Host Configuration Protocol (DHCP)	Understanding Interfaces	VMware, KVM, Contrail, AWS, Azure, and Hyper-V
Flow and packet processing	Juniper Networks Devices Processing Overview	VMware, KVM, Contrail, AWS, Azure, and Hyper-V
Intrusion Detection and Prevention (IDP)	Understanding Intrusion Detection and Prevention	VMware, KVM, Contrail, AWS, Azure, and Hyper-V
IPsec VPN	IPsec VPN Overview	VMware, KVM, Contrail, AWS, Azure, and Hyper-V

Table 1: Documentation References for Junos OS Features Supported on vSRX *(continued)*

Feature	Feature Documentation	vSRX Platform
Multiprotocol Label Switching (MPLS)	MPLS Overview	VMware, KVM, Contrail, AWS, Azure, and Hyper-V
Multicast	Multicast Overview	VMware, KVM, and Contrail
Network Address Translation (NAT)	Introduction to NAT	VMware, KVM, Contrail, AWS, Azure, and Hyper-V
Routing protocols	Junos OS Routing Protocols Library	VMware, KVM, Contrail, AWS, Azure, and Hyper-V
Security building bocks	Understanding Security Basics	VMware, KVM, Contrail, AWS, Azure, and Hyper-V
Transparent mode	Ethernet Switching and Layer 2 Transparent Mode Overview	VMware, KVM, and Contrail
Unified Threat Management (UTM)	Unified Threat Management Overview	VMware, KVM, Contrail, AWS, Azure, and Hyper-V
User authentication	Understanding User Authentication for Security Devices	VMware, KVM, Contrail, AWS, Azure, and Hyper-V

Unsupported Features

While vSRX supports many of the Junos OS features supported on other SRX Series devices, not all features are supported. For information about Junos OS features that are not supported on vSRX, see SRX Series Features Not Supported on vSRX.

Changes in Behavior and Syntax

For the most complete and latest information about changes in command behavior and syntax applicable to all SRX Series platforms in Junos OS Release 17.3R1, see Changes in Behavior and Syntax for SRX.

Known Behavior

This section contains the known behaviors, system maximums, and limitations in hardware and software in Junos OS Release 17.3R1 for vSRX.

Chassis Cluster/High Availability

- In vSRX deployments, HA is not supported on Contrail, AWS, Microsoft Azure, and Microsoft Hyper-V.
- In KVM deployments using Virtio, when vSRX is operating in HA and sessions are established and closed at very high rates, some sessions might not get closed on the backup node. This issue is because of a Virtio driver limitation.

  Workaround: Reduce session establish rate to less than 300 cps.
- In KVM deployments using Virtio, when vSRX is operating in HA, packet loss is observed during an RG0 failover. This occurs because the MAC entry at the bridge layer cannot be updated by the HA mechanism because of a driver limitation. Packets must remain in the queue until they expire.

Interfaces and Routing

- In vSRX deployments, source MAC filtering is supported on Fast Ethernet and Gigabit Ethernet interfaces in Layer 3 standalone mode and redundant Ethernet interfaces in HA mode. However, support is not available on Aggregated Ethernet (AE), Fabric Ethernet, or Gigabit Ethernet interfaces in Layer 2 standalone mode.
- In vSRX deployments, the following configuration options are not supported: *services unified-access-control* and *protocols l2-learning global-mode switching*.
- In vSRX deployments, configuring XAuth with AutoVPN secure tunnel (st0) interfaces in point-to-multipoint mode and dynamic IKE gateways is not supported. However, XAuth is supported with shared IKE IDs.
- In vSRX deployments using VMware ESX, changing the default speed (1000 Mbps) or the default link mode (full duplex) is not supported on VMXNET3 vNICs.

Platform and Infrastructure

- VRRP is not supported on VMware hypervisors because of a VMware support limitation for virtual MAC addresses.
- In VMware deployments, a serial console port on the vSRX platform cannot be used through the network to redirect console messages to a telnet session because of an underlying infrastructure limitation. The console port can be configured; however, it is not usable.
- In a vSRX deployment in VMware ESXi 5.5 using VMXNET3 vNICs, a performance degradation (8 percent) is observed when more vNICs (approximately eight) are configured, compared with fewer vNICs (approximately three) across a single instance.
- DPDK does not provide an outgoing multicast traffic count on its interface. As a result, interface outgoing multicast packets are interpreted as incoming packets on the egress interface.
- In vSRX deployments, the vSRX VM does not support the use of Live Migration or vMotion as a means to move virtual machines from one host to another.

SR-IOV

- SR-IOV interfaces have both physical functions (PFs) and multiple virtual functions (VFs). When configuration parameters are modified on the VF, the PF driver has the option to accept or reject the change. As a security precaution, the generic PF driver that is part of standard hypervisors (both VMware and Linux) does not allow certain parameters to be configured. Parameters that cannot be changed include enabling promiscuous mode, enabling multicast, and allowing Jumbo frames. Because of this driver limitation, the following vSRX features are not supported in deployments that use SR-IOV interfaces:
  - High availability (HA)
  - IRB interfaces
  - IPv6 addressing
  - Jumbo frames
  - Layer 2 support
  - Multicast with other features such as OSPF and IPv6
  - Packet mode

  These limitations apply in deployments where the PF drivers cannot be updated or controlled. The limitations do not apply when vSRX is deployed on supported Juniper Networks devices.
- SR-IOV does not support all VMware features (see your VMware documentation).
- In either a Microsoft Azure or Microsoft Hyper-V deployment, SR-IOV is not supported.

- Cloning vSRX VMs with SR-IOV interfaces is not supported. Instead of cloning a VM, instantiate a new vSRX VM from the .ova image (VMware hypervisors) or from the .qcow2 image (KVM hypervisors).
- In deployments using SR-IOV interfaces, Address Resolution Protocol (ARP) does not work when Jumbo frames are used on a physical NIC.
- In deployments using SR-IOV interfaces, packets are dropped when a MAC address is assigned to a vSRX Junos OS interface. This issue occurs because SR-IOV does not allow MAC address changes in either the PF or the VF.
- In KVM deployments using SR-IOV interfaces with a DPDK driver, the PF interface might go down and then come back up. In such circumstances, the vSRX might stay down even after the PF is back up because the Junos OS ge- interface does not receive an updated link state message from the VF interface.

  Workaround: Reboot the vSRX instance.
- In KVM deployments operating in SR-IOV mode with an Intel X710/XL710 NIC, note that there is no VLAN support for the vSRX interfaces in this configuration. This is due to an Intel card limitation with the X710 and XL710 NICs.

vSRX Limitations in Junos Space Security Director Integration with vSRX

The following vSRX features are not supported in Security Director:

- Application QoS (AppQoS)
- Layer 2 transparent mode
- Specific Security Director limitations with respect to Application Firewall (AppFW), IDP, and UTM features:
  - UTM database updates are not supported.
  - Application ID (AppID) custom signatures are not supported.
- The following vSRX features are not supported in Junos Space Security Director for IPsec and routing features:
  - Certificates for AutoVPN must be generated from the CLI.
  - All other IPsec settings can be configured using Junos Space Security Director.

Known Issues

This section lists the known issues in Junos OS Release 17.3R1 for vSRX.

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

Chassis Clustering

- In HA deployments, when the Routing Engine is busy and an RG0 manual failover is initiated, a control link failure occurs. A failed control link causes both control link detection methods (tcp keepalive and control link heart beat) to fail; it also results in an RG1+ failover. This situation might eventually lead to an RG1+ split brain condition. PR1085987
- In a cluster environment, when the primary node is shut down on VMware ESXi by the vSphere client, the remaining node state transitions from *Secondary* to *Ineligible* before changing to the *Primary* state. This change in state change can lengthen the delay to failover. PR1216447
- The vSRX HA control link might go down under high-traffic conditions, which disables the secondary node. PR1229172
- With vSRX instances running in a chassis cluster, when rebooting the primary node for redundancy-group 1+, traffic forwarding may stop for approximately a minute. PR1258502

  Workaround: First manually failover redundancy-group 1+ before rebooting a cluster node.
- A high-availability cold-sync failure might occur when using PCI passthrough as FAB. When this issue occurs, the vSRX might become unresponsive. PR1263056

  Workaround: Perform a manual failover for redundancy-group 1+ before rebooting a cluster node. If this does not resolve the issue, use Virtio as FAB.

Class of Service (CoS)

- On vSRX instances when classifiers, schedulers, and shapers are configured, the interface queue counters where these schedulers are applied do not match the expected number of packets. PR1083463

DHCP

- In vSRX deployments, when you exclude an assigned address from the DHCP pool on a DHCP server, the DHCP client gets the excluded address when you use the command **request dhcp client renew all**. This issue occurs because the CLIENT_EVENT_RECONFIGURE event, sent to the client when the **request dhcp client renew** command was issued, is handled by the client in the bound state. This issue is applicable only to DHCPv4 clients.

  Workaround: Clear the binding on the DHCP client by using the **clear dhcp client binding all** command, and then run the **request dhcp client renew all** command to get a new IP address.

  PR1094252

  PR1094257

Flow and Processing

- When vSRX FTP self-traffic crosses a virtual router, the FTP session might fail. PR1079190
- In vSRX deployments, traffic is dropped when a loopback address (lo0.0) and a generic routing encapsulation (GRE) physical interface are configured in different zones. PR1081171

  Workaround: Configure lo0.0 and GRE in the same zone, or use the IP address of the physical interface as the source IP address of the GRE interface.
- Because all DPDK vhost user vNICs on OVS are, by default, bound to the CPUs on Numa node 0, only the OVS poll mode driver (PMD) threads running on node 0 can poll packets on the vhost user NICs. For the performance test to be done on node 1, although you can add the CPU mask to use CPUs on Numa node 0 to poll the packet from the DPDK vhost user NICs, this action can seriously impact performance because of traffic across Numa nodes. PR1241975

  Workaround: A solution to this issues consists of two steps:

  1. Compile the DPDK with CONFIG_RTE_LIBRTE_VHOST_NUMA enabled:
     /config/common_base:556:CONFIG_RTE_LIBRTE_VHOST_NUMA=y

  2. Set the QEMU process to run on the Numa node 1 by adding **emulatorpin** elements to the XML file.

```
<cputune>
    <vcpupin vcpu='0' cpuset='45'/>
    <vcpupin vcpu='1' cpuset='46'/>
    <vcpupin vcpu='2' cpuset='47'/>
    <vcpupin vcpu='3' cpuset='48'/>
    <vcpupin vcpu='4' cpuset='49'/>
    <emulatorpin  cpuset='50-53'/>
 </cputune>
```

General Routing

- On vSRX platforms, when an interface is configured as a DHCP client using the dhcpd process, the DHCP discovers that the message cannot be sent out and the interface does not fetch the IP address. This occurs when the hostname is not configured. As a result, the DHCP client cannot not fetch an IP address. PR1073443

Interfaces and Routing

- RSVP neighbors are not established on a VMware ESXi host if NSX components are installed on that host. PR1092514
- On a VMware ESXi host, packets with VLAN do not cross over ESXi hosts when NSX components are installed through a Virtual Extensible LAN (VXLAN) port group. PR1092517
- When running VMware ESXi 5.5.0U3, in the **show chassis fpc detail** output, the current status of fpc0 shows that it is in cluster mode. Normally, the mode is displayed as online. PR1141998

  Workaround: Use VMware ESXi 5.5.0U2 or upgrade to VMware ESXi 6.0.
- When you operate the vSRX in transparent mode with VMware ESXi 5.1 as the host, some packet corruption might occur at the VMXNET3 driver level if TCP segmentation offload (TSO) is enabled on the host. PR1200051

  NOTE: This issue does not occur with VMware ESXi 5.5 and later.

  Workaround: Disable TSO in the data path on the VMware ESXi 5.1 host.

- The **monitor traffic** CLI command cannot be used to capture vSRX plain ping-to-host revenue ports traffic. All plain ping packets transmitted to revenue ports are handled on the srxpfe side, and vSRX revenue ports traffic will not be seen by RE using this command. However, traffic coming out from revenue ports can be seen by RE. Revenue ports refer to all ports except fxp0 and em0. PR1234321
- On vSRX, 10-Gigabit Ethernet interfaces are being displayed as 1-Gigabit Ethernet interfaces. PR1236912

  NOTE: This is a display issue and will be addressed in a future version of Junos OS.

- When performing a rapid disable interface/enable interface sequence on a vSRX (for example, when using a script), this action might trigger an Intel i40e-based NIC limitation where the NIC becomes unresponsive and is unable to receive packets. PR1253659

  Workaround: If possible, avoid using a script to perform a rapid disable interface/enable interface sequence on the vSRX. If you encounter this issue, login to the host and reload the Intel i40e driver to recover the NIC.
- In some cases, when you specify the **show interfaces gr-0/0/0 statistics detail** command, the show command output under Physical interface does not properly reflect the input and output packets or bytes in the Traffic statistics. PR1292261

Microsoft Azure

- Nested vmx (hardware virtualization support) is not supported for a vSRX that is deployed on Microsoft Azure. Please note that this has no impact to vSRX functionality, but it can slightly affect the bootup time and configuration commit time. PR1231270

Microsoft Hyper-V

- When you deploy a vSRX virtual security appliance on Windows Hyper-V Server 2012 (vSRX support for the Hyper-V hypervisor), if the bidirectional traffic of each port exceeds the capability of the vSRX, you might find that one vSRX port hangs and becomes unable to receive packets. PR1250285

  Workaround: Upgrade Windows Hyper-V Server 2012 to Windows Hyper-V Server 2012 R2.

Platform and Infrastructure

- In a KVM-based hypervisor, an attempt to save vSRX and restore it through the Virtual Machine Manager GUI causes the Virtual Routing Engine (VRE) to crash. The crash causes the vRE to go to DB mode. PR1087096

  Workaround: Use either **virsh destroy/start VM** or **nova stop/start/reboot VM** but not the Virtual Machine Manager GUI.

- In KVM deployments, virsh **reset** commands do not work. PR1087112
- The AWS snapshot feature cannot be used to clone vSRX instances. You can use the AWS snapshot feature to preserve the state of the VM so you can return to the same state when the snapshot was created. PR1160582
- vSRX uses DPDK to increase packet performance by caching packets to send in burst mode. Latency-sensitive applications must account for this burst operation. PR1087887
- APIC virtualization (APICv) does not work well with nested VMs such as those used with KVM. On Intel CPUs that support APICv (typically v2 models, for example E5 v2 and E7 v2), you must disable APICv on the host server before deploying vSRX. PR1111582

  Workaround: Disable APICv before deploying vSRX.

  Use the following commands to disable APICv on your host and verify that it is disabled:

```
sudo rmmod kvm-intel
sudo sh -c “echo ’options kvm-intel enable_apicv=n’ >> /etc/modprobe.d/dist.conf”
sudo modprobe kvm-intel
root@host:~# cat /sys/module/kvm_intel/parameters/enable_apicv
N
```

- In a KVM-based hypervisor deployment, you might encounter one or more of following issues: PR1263056
  - The vSRX may become unresponsive when Page Modification Logging (PML) is enabled in the host operating system (CentOS or Ubuntu) when using the Intel Xeon Processor E5 or E7 v4 family. This PML issue prevents the vSRX from successfully booting.
  - Traffic to the vSRX might drop or stop due to Intel XL710 driver-specific limitations. This behavior can be due to issues with the vSRX VM configuration (such as a MAC-VLAN or MAC-NUM limitation).

  Workaround: Perform the appropriate workaround to resolve the issues listed above:

  - If the vSRX becomes unresponsive due to a PML issue, we recommend that you disable the PML at the host kernel level. Depending on your host operating system, open the .conf file in your default editor and add the following line to the file: **hostOS# options kvm-intel nested=y enable_apicv=n pml=n**.
  - If the vSRX experiences loss of traffic due to Intel XL710 driver limitations, follow the recommended Intel XL710 guidelines to change the VM configuration to avoid these limitations. See Intel Ethernet Controller X710 and XL710 Family Documentation for the recommended guidelines.
- When deploying a vSRX instance in a KVM or Contrail environment with the vhost_net NIC driver, the vSRX might process and forward all unicast packets which were flooded to the port, regardless of the destination MAC address. PR1344700

  Workaround: For a vSRX on KVM deployment, insert **<driver name='qemu'/>** below **<model type='virtio'/>** in the VM XML definition file. For a vSRX on Contrail deployment, no workaround is available. To avoid packets from looping back out of the same interface, do not permit intra-zone traffic forwarding by the security policy.

Routing Protocols

- When the Bidirectional Forward Detection (BFD) protocol is configured over an IPv6 static route, the route remains in the routing table even after a session failure occurs. PR1109727

UTM

- In vSRX deployments configured with Sophos Antivirus, some files that are larger than the configured **max-content-size** might not go into fallback mode, and, after they are retransmitted several times, they might pass with a clean or an infected result. This issue is specific to a few protocols that do not send the content size before attempting to transmit files. PR1093984

VPN

- An error message might occur for **show** or **clear** commands if IPsec VPN is configured with over 1000 tunnels. PR1093872

  Workaround: Retry the commands.

- IPv6 firewall filters cannot be applied to virtual channels. PR1182367
- When IPsec is used with PKI authentication, the vSRX might unnecessarily send the entire certificate chain to the remote peer, potentially causing fragmentation of IKE messages. PR1251837

  Workaround: If possible, configure the remote peer to send the CERTREQ (certificate request) payload as part of the IKE exchange. The vSRX will examine the CERTREQ payload from the remote peer to determine what CAs the peer trusts and to compare them with the CAs trusted locally. This examination helps avoid sending the entire certificate chain to the peer.

- When configuring a manual route-based IPsec VPN, if you enable VPN monitoring this can cause the st0.* interface to go down, which results in VPN traffic being dropped. PR1259422

  Workaround: Enter the **restart ipsec-key-management** CLI command to restart the kmd process and restore the VPN service.

  > **NOTE:** When the kmd process is restarted, all existing phase 1 and phase 2 SA on the device will be cleared.

- With the **tcp-encap-profile** command configured in an environment with a virtual routing instance, there might be packet drops on a port 500-based IPsec tunnel. No issues are observed with Pathfinder (port 443) based IPsec tunnels. PR1263518
- In certain cases, when performing multiple high-availability failovers with a Pathfinder session, the vSRX might enter into an unresponsive state and send a reset connection to the NCP client, which terminates the connection. PR1263678

Resolved Issues

The Junos OS Release 17.3R1 for vSRX is at feature parity with Junos OS Release 15.1X49-D90 for vSRX. This section lists the issues that have been fixed in the Junos OS Release 17.3R1. See Junos OS Release 15.1X49-D90 for vSRX Release Notes for the complete list of the resolved issues in Junos OS Release 15.1X49-D90.

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

Microsoft Azure

- The Flexible PIC Concentrator (FPC) might become stuck on the Ready state after the vSRX is first deployed on Microsoft Azure Cloud. PR1262712

  Workaround: If this issue occurs, use the **restart chassis-control immediately** operational command to restart the chassis control daemon to bring the FPC back online.

Platform and Infrastructure

- The vSRX might experience a core dump when traffic causes high memory usage, which results in a significant number of memory allocation failures at the DPI module. The core dump is due to buffering issues occurring in the DPI engine. PR1266517
- In some instances, the vSRX interface might fail to get an IP address from the DHCP server. This behavior can occur because the DHCPOFFER message is dropped when another routing instance has the same client IP address of the YIADDR (Your IP Address) field in the DHCPOFFER message. PR1276149

Migration, Upgrade, and Downgrade Instructions

This section contains information about how to upgrade Junos OS for vSRX using the CLI. Upgrading or downgrading Junos OS can take several hours, depending on the size and configuration of the network.

You also can upgrade to Junos OS Release 17.3R1 for vSRX using J-Web (see J-Web) or the Junos Space Network Management Platform (see Junos Space).

Upgrading Software Packages

To upgrade the software using the CLI:

1. Download the Junos OS Release 17.3R1 for vSRX .tgz file from the Juniper Networks website. Note the size of the software image.

2. Verify that you have enough free disk space on the vSRX to upload the new software image.

```
root@vsrx> show system storage detail
Filesystem       1024-blocks       Used      Avail   Capacity   Mounted on
/dev/vtbd0s1a         512622     335984     135630        71%  /
devfs                      1          1          0       100%  /dev
/dev/md0              976542     976542          0       100%  /junos
/cf                   512622     335984     135630        71%  /junos/cf
devfs                      1          1          0       100%  /junos/dev/
procfs                     4          4          0       100%  /proc
/dev/vtbd1s1e        1650908         28    1518808         0%  /config
/dev/vtbd1s1f       14858326     746128   12923532         5%  /var
/dev/vtbd3s2           93552        714      92838         1%  /var/host
/dev/md1              328084       1184     300654         0%  /mfs
/var/jail           14858326     746128   12923532         5%  /jail/var
/var/log            14858326     746128   12923532         5%  /jail/var/log
devfs                      1          1          0       100%  /jail/dev
192.168.1.1:/var/tmp/corefiles    4661548    1367504    3034204   31%
/var/crash/corefiles
192.168.1.1:/var/volatile    8210120          8    8210112    0%  /var/log/host
192.168.1.1:/var/log    4661548    1367504    3034204     31%  /var/log/hostlogs
192.168.1.1:/var/local    4661548    1367504    3034204   31%  /var/db/host
192.168.1.1:/var/db/aamwd    4661548    1367504    3034204   31%  /var/db/aamwd
192.168.1.1:/var/db/secinteld    4661548    1367504    3034204   31%
/var/db/secinteld
192.168.1.1:/app_disk    1335984       2040    1248032     0%  /var/install_disk
```

3. Optionally, free up more disk space if needed to upload the image.

```
root@vsrx> request system storage cleanup
 List of files to delete:

         Size Date         Name
    11B Feb  7 23:21 /var/jail/tmp/alarmd.ts
  3631B Feb 11 01:02 /var/jail/tmp/events-table.txt
 173.3K Feb  9 15:49 /var/jail/tmp/httpd.core.0.gz
    46B Mar  8 01:31 /var/jail/tmp/jweb-users.xml
  96.6K Apr 14 10:21 /var/log/chassisd.0.gz
  99.8K Apr 13 18:10 /var/log/chassisd.1.gz
 101.9K Apr 13 02:19 /var/log/chassisd.2.gz
 101.3K Apr 12 10:43 /var/log/chassisd.3.gz
  91.6K Apr 13 20:45 /var/log/hostlogs/auth.log.1.gz
  91.7K Apr 10 22:15 /var/log/hostlogs/auth.log.2.gz
  92.0K Apr  7 23:45 /var/log/hostlogs/auth.log.3.gz
  91.8K Apr  5 01:00 /var/log/hostlogs/auth.log.4.gz

<output omitted>
```

> **NOTE:** If this command does not free up enough disk space, see [SRX] Common and safe files to remove in order to increase available system storage for details on safe files you can manually remove from vSRX to free up disk space.

4. Use FTP, SCP, or a similar utility to upload the Junos OS Release 17.3R1 for vSRX .tgz file to **/var/tmp** on the local file system of your vSRX VM. For example:

```
root@vsrx> file copy ftp://username:prompt@ftp.hostname.net/pathname/
junos-vsrx-17.3R1.9.tgz /var/tmp
```

5. From operational mode, install the software upgrade package:

```
root@vsrx> request system software add /var/tmp/junos-srx-ffp-
junos-vsrx-17.3R1.9.tgz no-copy no-validate reboot

Installing package '/var/tmp/junos-vsrx-17.3R1.9.tgz' ...
Verified junos–boot–vsrx–17.3R1.9tgz signed by PackageProduction_15_1_0
Verified junos-vsrx-17.3R1.9.tgz signed by PackageProduction_15_1_0
Available space: 849286 require: 4714
```

```
Saving boot file package in /var/sw/pkg/junos-boot-vsrx-17.3R1.9.tgz
JUNOS 17.3 will become active at next reboot
Saving package file in /var/sw/pkg/junos-vsrx-17.3R1.9.tgz  ...
Saving state for rollback ...
Rebooting ...
shutdown: [pid 2535]
Shutdown NOW!

*** FINAL System shutdown Message from root@vsrx ***
System going down IMMEDIATELY

root@vsrx>
```

If no errors occur, Junos OS reboots automatically to complete the upgrade process.

6. You have successfully upgraded to Junos OS Release 17.3R1 for vSRX. Now log in and use the **show version** command to verify the upgrade.

```
vsrx (ttyd0)

login: root
password:
-- JUNOS 17.3 built 2017-08-15  23:57:11 UTC
root@vsrx>
root@vsrx> cli
root@vsrx>
root@vsrx> show version
Hostname: vsrx
Model: vSRX
JUNOS Software Release  [17.3]
```

Validating the OVA Image

If you have downloaded a vSRX .ova image and need to validate it, see Validating the vSRX .ova File for VMware.

Note that only .ova (VMware platform) vSRX images can be validated. The .qcow2 vSRX images for use with KVM cannot be validated the same way. File checksums for all software images are, however, available on the download page.

System Requirements

IN THIS SECTION

System Requirements by Environment

The topics below provide detailed system environment requirement specifications for each supported environment.

- System Requirements for vSRX on AWS
- System Requirements for vSRX on Contrail
- System Requirements for vSRX on KVM
- System Requirements for vSRX on Microsoft Azure
- System Requirements for vSRX on Microsoft Hyper-V
- System Requirements for vSRX on VMware

> **NOTE:** For certain vSRX instance deployments (for example, KVM, VMware, or Contrail), you can scale the performance and capacity of a vSRX instance by increasing the number of vCPUs or the amount of vRAM allocated to the vSRX, but you cannot scale down an existing vSRX instance to a smaller setting.

Hardware Recommendations

Table 2 on page 25 lists the hardware specifications for the host machine that runs the vSRX virtual machine (VM). For additional hardware guidance with respect to a specific software environment, see the *System Requirements* topics listed in the previous section.

Table 2: Hardware Specifications for the Host Machine

Component	Specification
Host memory size	4 GB, 8 GB, 16 GB. **NOTE:** Starting in Junos OS Release 15.1X49-D90 and Junos OS Release 17.3R1, the 16-GB host memory size is supported for vSRX on KVM.
Host processor type	x86_64 multicore CPU **NOTE:** DPDK requires Intel Virtualization VT-x/VT-d support in the CPU. See *About Intel Virtualization Technology*.
Physical NIC	• Intel X710/XL710, X520/540, or 82599 physical NICs for SR-IOV on vSRX • Intel XL710 physical NICs for PCI passthrough support on vSRX Starting in Junos OS Release 15.1X49-D70 and Junos OS Release 17.3R1, use Intel 82599 physical NICs in pass-through mode to scale the multicore vSRX. Starting in Junos OS Release 15.1X49-D90 and Junos OS Release 17.3R1, in a KVM deployment you can use SR-IOV (X710/XL710) physical NICs to scale the multicore vSRX. In addition, PCI passthrough (Intel XL710) support is available for vSRX on KVM.

NOTE:

- For VMware, you can check for CPU and other hardware compatibility here: http://www.vmware.com/resources/compatibility/search.php?deviceCategory=cpu
- For KVM, we recommend that you enable hardware-based virtualization on the host machine. You can verify CPU compatibility here: http://www.linux-kvm.org/page/Processor_support

To determine the Junos OS features supported on vSRX, 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 here:

Feature Explorer: vSRX

Best Practices Recommendations

vSRX deployments can be complex, and there is a great deal of variability in the specifics of possible deployments. The following recommendations might apply to and improve performance and function in your particular circumstances.

NUMA Nodes

The x86 server architecture consists of multiple sockets and multiple cores within a socket. Each socket also has memory that is used to store packets during I/O transfers from the NIC to the host. To efficiently read packets from memory, guest applications and associated peripherals (such as the NIC) should reside within a single socket. A penalty is associated with spanning CPU sockets for memory accesses, which might result in nondeterministic performance. For vSRX, we recommend that all vCPUs for the vSRX VM are in the same physical non-uniform memory access (NUMA) node for optimal performance.

CAUTION: The Packet Forwarding Engine (PFE) on the vSRX will become unresponsive if the NUMA nodes topology is configured in the hypervisor to spread the instance's vCPUs across multiple host NUMA nodes. vSRX requires that you ensure that all vCPUs reside on the same NUMA node.

We recommend that you bind the vSRX instance with a specific NUMA node by setting NUMA node affinity. NUMA node affinity constrains the vSRX VM resource scheduling to only the specified NUMA node.

PCI NIC-to-VM Mapping

If the node on which vSRX is running is different from the node to which the Intel PCI NIC is connected, then packets will have to traverse an additional hop in the QPI link, and this will reduce overall throughput. On a Linux host OS, install the **hwloc** package and use the **lstopo** command to provide information about relative physical NIC locations. On a VMware ESX Server, use the **esxtop** command to view information about relative physical NIC locations. On some servers where this information is not available or not supported, refer to the hardware documentation for the slot-to-NUMA node topology.

Mapping Virtual Interfaces to a vSRX VM

To determine which virtual interfaces on your Linux host OS map to a vSRX VM:

1. Use the **virsh list** command on your Linux host OS to list the running VMs.

```
hostOS# virsh list
```

```
Id    Name                           State
----------------------------------------------------
9     centos1                        running
15    centos2                        running
16    centos3                        running
48    vsrx                           running
```

```
50    1117-2                         running
51    1117-3                         running
```

2. Use the **virsh domiflist *vsrx-name*** command to list the virtual interfaces on that vSRX VM.

   `hostOS#` **virsh domiflist vsrx**

```
Interface  Type       Source     Model       MAC
-------------------------------------------------------
vnet1      bridge     brem2      virtio      52:54:00:8f:75:a5
vnet2      bridge     br1        virtio      52:54:00:12:37:62
vnet3      bridge     brconnect  virtio      52:54:00:b2:cd:f4
```

> **NOTE:** The first virtual interface maps to the fxp0 interface in Junos OS.

RELATED DOCUMENTATION

- About Intel Virtualization Technology
- DPDK Release Notes

Finding More Information

For the latest, most complete information about known and resolved issues with the Junos OS, see Juniper Networks Problem Report Search application at:

https://prsearch.juniper.net

Juniper Networks Feature Explorer is a Web-based application that helps you to explore and compare Junos OS feature information to find the correct software release and hardware platform for your network. Find Feature Explorer at:

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

Juniper Networks Content Explorer is a Web-based application that helps you explore Juniper Networks technical documentation by product, task, and software release, and download documentation in PDF format. Find Content Explorer at:

https://www.juniper.net/documentation/content-applications/content-explorer/

Documentation Feedback

We encourage you to provide feedback, comments, and suggestions so that we can improve the documentation. You can provide feedback by using either of the following methods:

- Online feedback rating system—On any page of the Juniper Networks TechLibrary site at https://www.juniper.net/documentation/index.html, simply click the stars to rate the content, and use the pop-up form to provide us with information about your experience. Alternately, you can use the online feedback form at https://www.juniper.net/documentation/feedback/.
- E-mail—Send your comments to techpubs-comments@juniper.net. Include the document or topic name, URL or page number, and software version (if applicable).

Requesting Technical Support

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

- JTAC policies—For a complete understanding of our JTAC procedures and policies, review the *JTAC User Guide* located at 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://www.juniper.net/customers/support/
- Search for known bugs: https://prsearch.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://www.juniper.net/customers/csc/software/
- Search technical bulletins for relevant hardware and software notifications: https://kb.juniper.net/InfoCenter/
- Join and participate in the Juniper Networks Community Forum: https://www.juniper.net/company/communities/
- 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, see https://www.juniper.net/support/requesting-support.html.

Revision History

8 February 2021—Revision 3— Junos OS 17.3R1 – vSRX.

31 January 2019 —Revision 2— Junos OS 17.3R1 – vSRX.

25 August 2017 —Revision 1— Junos OS 17.3R1 – vSRX.

Copyright © 2017 Juniper Networks, Inc. All rights reserved.

Juniper Networks, the Juniper Networks logo, Juniper, and Junos are registered trademarks of Juniper Networks, Inc. and/or its affiliates in the United States and other countries. All other trademarks may be property of their respective owners.

Juniper Networks assumes no responsibility for any inaccuracies in this document. Juniper Networks reserves the right to change, modify, transfer, or otherwise revise this publication without notice.