Juniper Networks | Engineering Simplicity

vSRX Deployment Guide for Nutanix

Published
2020-12-28

Juniper Networks, Inc.
1133 Innovation Way
Sunnyvale, California 94089
USA
408-745-2000
www.juniper.net

vSRX Deployment Guide for Nutanix

YEAR 2000 NOTICE

Juniper Networks hardware and software products are Year 2000 compliant. Junos OS has no known time-related limitations through the year 2038. However, the NTP application is known to have some difficulty in the year 2036.

END USER LICENSE AGREEMENT

The Juniper Networks product that is the subject of this technical documentation consists of (or is intended for use with) Juniper Networks software. Use of such software is subject to the terms and conditions of the End User License Agreement ("EULA") posted at https://support.juniper.net/support/eula/. By downloading, installing or using such software, you agree to the terms and conditions of that EULA.

Table of Contents

About This Guide

Use this guide to install the vSRX Virtual Firewall in the Nutanix enterprise cloud. The purpose of this document is to help users launch vSRX instances on Nutanix AHV cluster.

The document does not provide configuration details required to bring up Nutanix cluster assuming a working Nutanix cluster is up and running, and accessible through Prism web GUI and Acropolis CLI.

After completing the installation and basic configuration procedures covered in this guide, refer to the Junos OS documentation for information about further software configuration.

1

CHAPTER

Overview

vSRX Overview

SUMMARY

In this topic you learn about vSRX architecture and its benefits.

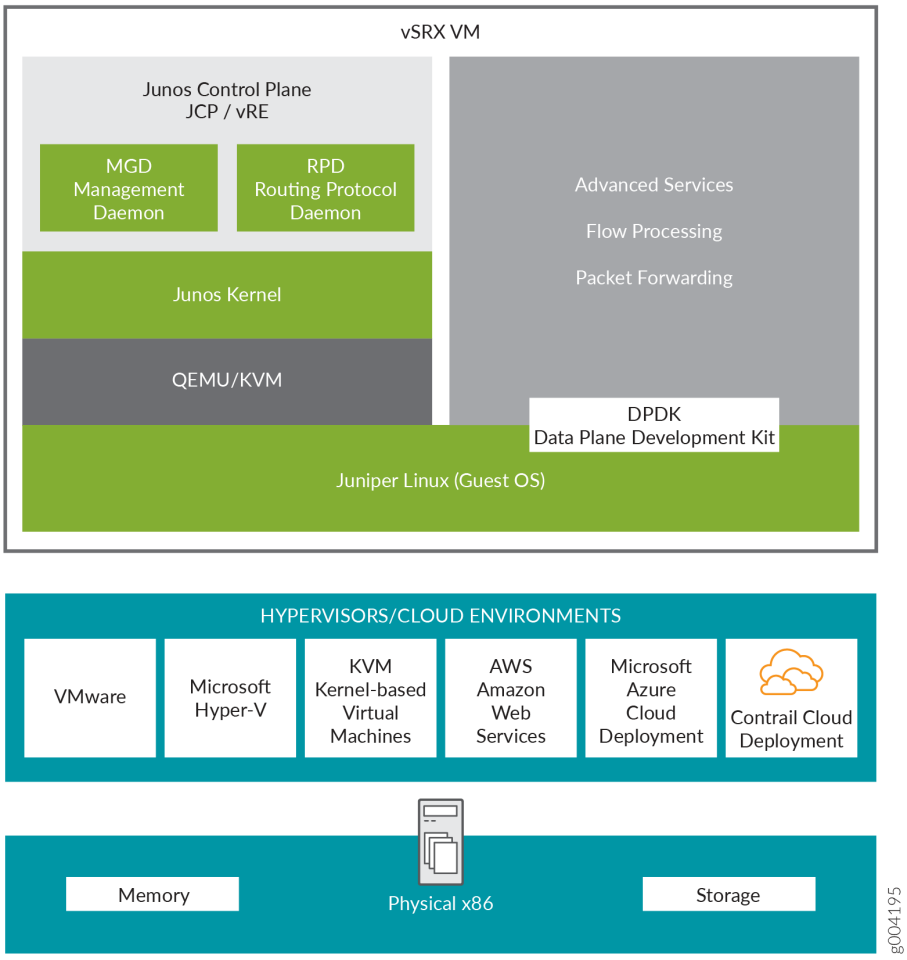
IN THIS SECTION

vSRX is a virtual security appliance that provides security and networking services at the perimeter or edge in virtualized private or public *cloud* environments. vSRX runs as a virtual machine (*VM*) on a standard x86 server. vSRX is built on the Junos operating system (Junos OS) and delivers networking and security features similar to those available on the software releases for the SRX Series Services Gateways.

The vSRX provides you with a complete Next-Generation Firewall (NGFW) solution, including core firewall, VPN, NAT, advanced Layer 4 through Layer 7 security services such as Application Security, intrusion detection and prevention (IPS), and UTM features including Enhanced Web Filtering and Anti-Virus. Combined with Sky ATP, the vSRX offers a cloud-based advanced anti-malware service with dynamic analysis to protect against sophisticated malware, and provides built-in machine learning to improve verdict efficacy and decrease time to remediation.

Figure 1 on page 3 shows the high-level architecture.

Figure 1: vSRX Architecture



vSRX includes the Junos control plane (JCP) and the packet forwarding engine (PFE) components that make up the data plane. vSRX uses one virtual CPU (vCPU) for the JCP and at least one vCPU for the PFE. Starting in Junos OS Release 15.1X49-D70 and Junos OS Release 17.3R1, multi-core vSRX supports scaling vCPUs and virtual RAM (vRAM). Additional vCPUs are applied to the data plane to increase performance.

Junos OS Release 18.4R1 supports a new software architecture vSRX 3.0 that removes dual OS and nested virtualization requirement of existing vSRX architecture.

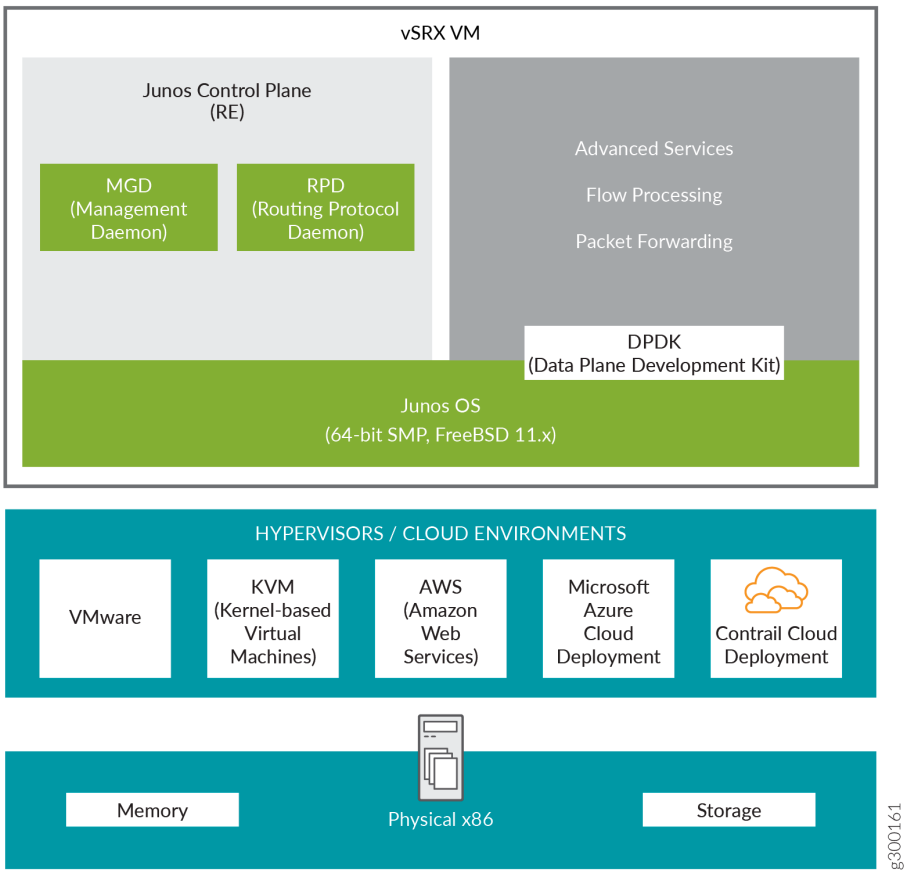
In vSRX 3.0 architecture, FreeBSD 11.x is used as the guest OS and the Routing Engine and Packet Forwarding Engine runs on FreeBSD 11.x as single virtual machine for improved performance and scalability. vSRX 3.0 uses DPDK to process the data packets in the data plane. A direct Junos upgrade from vSRX to vSRX 3.0 software is not supported.

vSRX 3.0 has the following enhancements compared to vSRX:

- Removed the restriction of requiring nested VM support in hypervisors.
- Removed the restriction of requiring ports connected to control plane to have Promiscuous mode enabled.
- Improved boot time and enhanced responsiveness of the control plane during management operations.
- Improved live migration.

Figure 2 on page 4 shows the high-level architecture for vSRX 3.0

Figure 2: vSRX 3.0 Architecture



Benefits

vSRX on standard x86 servers enables you to quickly introduce new services, deliver customized services to customers, and scale security services based on dynamic needs. vSRX is ideal for public, private, and hybrid cloud environments.

Some of the key benefits of vSRX in a virtualized private or public cloud multitenant environment include:

- *Stateful firewall* protection at the tenant edge
- Faster deployment of virtual firewalls into new sites
- Ability to run on top of various hypervisors and public cloud infrastructures
- Full routing, *VPN*, core security, and networking capabilities
- Application security features (including IPS and App-Secure)
- Content security features (including Anti Virus, Web Filtering, Anti Spam, and Content Filtering)
- Centralized management with Junos Space Security Director and local management with J-Web Interface
- Juniper Networks Sky Advanced Threat Prevention (Sky ATP) integration

Release History Table

Release	Description
15.1X49-D70	Starting in Junos OS Release 15.1X49-D70 and Junos OS Release 17.3R1, multi-core vSRX supports scaling vCPUs and virtual RAM (vRAM). Additional vCPUs are applied to the data plane to increase performance.

Understand vSRX Deployment with Nutanix

IN THIS SECTION

Nutanix Platform Overview

IN THIS SECTION

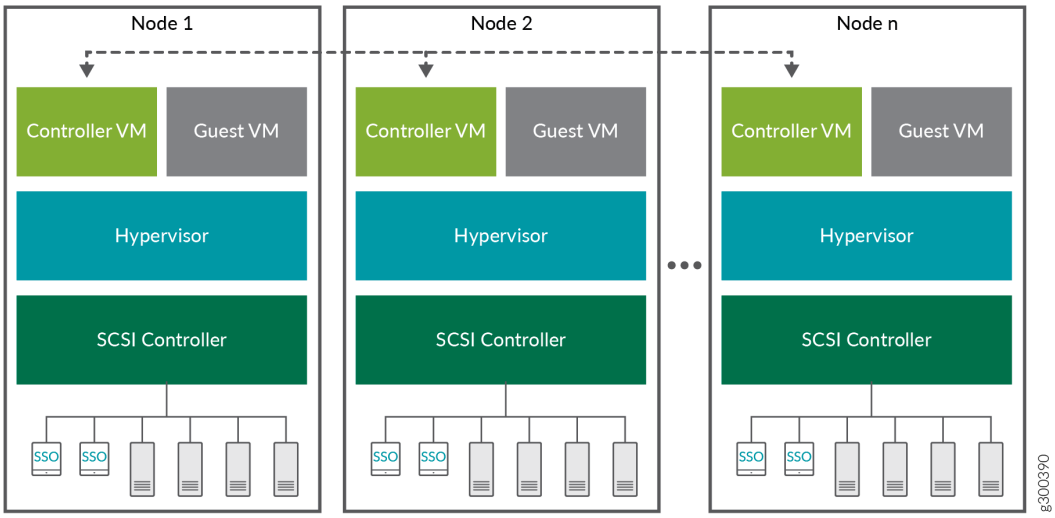
The Nutanix Virtual Computing Platform is a converged, scale-out compute and storage system that is purpose-built to host and store virtual machines (VMs).

All nodes in a Nutanix cluster converge to deliver a unified pool of tiered storage and present resources to VMs for seamless access. A global data system architecture integrates each new node into the cluster, allowing you to scale the solution to meet the needs of your infrastructure. Nutanix supports VMware vSphere (ESXi), Microsoft HyperV, Citrix XenServer, and Nutanix Acropolis hypervisor (AHV) (KVM-based).

The foundational unit for the cluster is a Nutanix node. Each node in the cluster runs a standard hypervisor and contains processors, memory, and local storage (SSDs and hard disks).

The Nutanix cluster has a distributed architecture, which means that each node in the cluster shares in the management of cluster resources and responsibilities. Within each node, there are software components that perform specific tasks during cluster operation. All components run on multiple nodes in the cluster, and depend on connectivity between their peers that also run the component. Most components also depend on other components for information.

A Nutanix Controller VM runs on each node, enabling the pooling of local storage from all nodes in the cluster.



Guest VM Data Management

VM data is stored locally, and replicated on other nodes for protection against hardware failure.

When a guest VM submits a write request through the hypervisor, that request is sent to the Controller VM on the host. To provide a rapid response to the guest VM, this data is first stored on the metadata drive, within a subset of storage. This cache is rapidly distributed across the 10-*Gigabit Ethernet* GbE network to other metadata drives in the cluster. Oplog data is periodically transferred to persistent storage within the cluster. Data is written locally for performance and replicated on multiple nodes for high availability.

When the guest VM sends a read request through the hypervisor, the Controller VM will read from the local copy first, if present. If the host does not contain a local copy, then the Controller VM will read across the network from a host that does contain a copy. As remote data is accessed, it will be migrated to storage devices on the current host, so that future read requests can be local.

Guest VM data management includes the following features:

- **MapReduce tiering**—Nutanix cluster dynamically manages data based on how frequently it is accessed. New data is saved on the SSD tier. Frequently accessed data is kept on the SSD tier and old data is migrated to the HDD tier.

  Automated data migration also applies to read requests across the network. If a guest VM repeatedly accesses a block of data on a remote host, the local controller VM migrates that data to the SSD tier of the local host. This migration not only reduces network latency, but also ensures that frequently accessed data is stored on the fastest storage tier.

- **Live migration**—Live migration of VMs, whether it is initiated manually or through an automatic process like vSphere DRS, is fully supported by the Nutanix Virtual Computing Platform. All hosts

within the cluster have visibility into shared Nutanix datastores through the Controller VMs. Guest VM data is written locally, and is also replicated on other nodes for high availability.

If a VM is migrated to another host, future read requests are sent to a local copy of the data, if it exists. Otherwise, the request is sent across the network to a host that does contain the requested data. As remote data is accessed, the remote data is migrated to storage devices on the current host, so that future read requests are local.

- **High availability (HA)**—The built-in data redundancy in a Nutanix cluster supports high availability provided by the hypervisor. If a node fails, all high-availability-protected VMs can be automatically restarted on other nodes in the cluster. The hypervisor management system, such as vCenter, selects a new host for the VMs, which might or might not contain a copy of the VM data.

- **Virtualization management VM high availability**—In virtualization management VM high availability, when a node becomes unavailable, VMs that are running on that node are restarted on another node in the same cluster.

  Typically, an entity failure is detected by its isolation from the network (the failure to respond to heartbeats). Virtualization management ensures that at most one instance of the VM is running at any point during a failover. This property prevents concurrent network and storage I/O that could lead to corruption.

  Virtualization management VM high availability implements admission control to help ensure that in case of node failure, the rest of the cluster has enough resources to accommodate the other VMs.

- **Datapath redundancy**—The Nutanix cluster automatically selects the optimal path between a hypervisor host and its guest VM data. The Controller VM has multiple redundant paths available, which makes the cluster more resilient to failures.

  When available, the optimal path is through the local Controller VM to local storage devices. In some situations, the data is not available on local storage, such as when a guest VM was recently migrated to another host. In those cases, the Controller VM directs the read request across the network to storage on another host through the Controller VM of that host.

  Datapath redundancy also responds when a local Controller VM is unavailable. To maintain the storage path, the cluster automatically redirects the host to another Controller VM. When the local Controller VM comes back online, the datapath is returned to this VM.

vSRX Deployment with Nutanix Overview

IN THIS SECTION

This topic provides an overview of vSRX deployment on Nutanix Enterprise Cloud.

vSRX offers the same full-featured advanced security as the physical Juniper Networks SRX Series Services Gateways, but in a virtualized form factor. Handling speeds up to 100 Gbps, making it the industry's fastest virtual firewall. vSRX with Nutanix delivers:

- A single platform delivering high performance and predictable scale for any virtual workload.
- High-performance networking and security for scale-out virtual data centers.
- Flexibility with multi-hypervisor support (Hyper-V, ESXi, and Acropolis Hypervisor) and a full appliance portfolio for the right mix of compute and storage resources.
- VMs that keep running and are protected with VM-centric backups and integrated disaster recovery.
- Innovative Virtual Chassis Fabric architecture with automation capabilities for simplified management.

Manual, rigid, and static connectivity and security implementations might work in traditional network environments. In the multicloud era, however, where application requirements are highly dynamic, network security must be an agile and scalable partner to compute and storage.

Enterprise multiclouds typically employ perimeter security solutions like Nutanix Enterprise Cloud to block threats contained in north-south traffic entering or leaving the HCI. Effective as they are, these solutions cannot defend against threats introduced by compromised virtual machines (VMs) that infect east-west traffic flowing within the data center itself, between applications and services. If these threats are not identified and addressed in a timely manner, they could compromise mission-critical applications and lead to the loss of sensitive data, causing irreparable harm to revenue and reputation of an organization.

vSRX works with Nutanix Enterprise Cloud to provide advanced security, consistent management, automated threat remediation, and effective microsegmentation—delivering a secure and automated solution for defending today's multicloud environments.

The joint Juniper Networks-Nutanix hyperconverged solution helps enterprises secure their multicloud environments with advanced security, consistent management, automated threat remediation,

automation, and effective microsegmentation. Enterprises can now easily deploy a secure and automated multicloud without the overhead of operational and management complexity.

Nutanix provides on-demand services in the cloud. Services range from Infrastructure as a Service (IaaS) and Platform as a Service (SaaS), to Application and Database as a Service. Nutanix is a highly flexible, scalable, and reliable cloud platform. In Nutanix, you can host servers and services on the cloud as bring-your-own-license (BYOL) service.

Benefits of vSRX with Nutanix

- **Advanced security**—Protects the business by delivering advanced security services, including user and application firewall, advanced threat prevention, and intrusion prevention.
- **Microsegmentation**—Employs microsegmentation to secure applications and defend against lateral threat propagation in the enterprise multicloud. Protects virtual workloads through effective microsegmentation.

  Microsegmentation facilitates granular segmentation and control by applying security policies at the virtualized host level. From a security perspective, the more granular level at which a threat can be blocked, the more effective the defense will be in containing the threat's propagation. Administrators must augment their security solutions with microsegmentation and automated threat remediation, providing the visibility and control required to protect lateral data center traffic from common breaches.
- **Visibility**—Provides granular visibility and analytics into application, user, and IP behavior.
- **Automation**—Offers rich APIs and automation libraries from Nutanix and Juniper Networks to enable agile DevOps workflows; to deliver improved security response through unified automation of security and networking workflows.
- **Operational simplicity**—Streamlines and enables policy deployment and enforcement with single-pane management and simple, intuitive controls across multicloud deployments.

Understand vSRX Deployment with Nutanix AHV

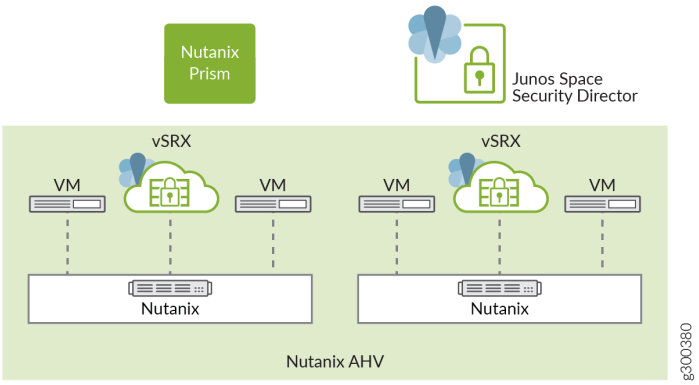
IN THIS SECTION

Nutanix Acropolis hyperconverged infrastructure (HCI) supports customer choice in virtualization solutions including VMware vSphere (ESXi), Microsoft HyperV, Citrix XenServer, and Nutanix AHV. AHV is a feature-rich Nutanix hypervisor. AHV is an enterprise-ready hypervisor based on proven open-source technology. Nutanix AHV is a license-free virtualization solution included with Acropolis that delivers enterprise virtualization ready for a multicloud world. With Acropolis and AHV, virtualization is tightly integrated into the Nutanix Enterprise Cloud OS rather than being layered on as a standalone product that needs to be licensed, deployed and managed separately.

Common tasks such as deploying, cloning, and protecting VMs are managed centrally through Nutanix Prism, rather than utilizing disparate products and policies in a piecemeal strategy.

Figure 3 on page 11 illustrates how security is provided for applications running in a private subnet of Nutanix Enterprise Cloud with AHV hypervisor.

Figure 3: vSRX Deployment in Nutanix Enterprise Cloud



The Nutanix AHV virtualization solution, including the tools you need to manage it, ships from the factory already installed and ready to go state so that you can have the system up and running as soon as you have racked the cluster and powered it on. When the system is up and running, you can maintain the environment through a simple HTML 5 Web UI. Prism Element, which is available on each cluster you deploy, integrates this UI with the overall Nutanix solution. You can access Prism Element through each individual Nutanix cluster through the cluster IP or any of the individual Nutanix Controller Virtual Machine (CVM) IP addresses. Prism Element requires no additional software; it is built into every Nutanix cluster and incorporates support for AHV.

If you prefer a more centralized mechanism for managing your deployment, Prism Central is available from the Nutanix portal or can be deployed directly from the Nutanix cluster. Prism Central is a robust optional software appliance VM that can run on ESXi, Hyper-V, or AHV.

Prism Central is both a platform and a hypervisor-agnostic management interface, providing an aggregate view of your deployed Nutanix clusters. In addition to allowing you to view and manage the cluster, Prism Central provides insight into VMs, hosts, disks, and containers or pooled disks.

Prism Central provides a single pane of glass for managing not only multiple Nutanix clusters, but also the native Nutanix hypervisor, AHV. Unlike other hypervisors, AHV requires no additional back-end applications or database to maintain the data rendered in the UI.

Prism runs on every node in the cluster, but like other components, it elects a leader. All requests are forwarded from the followers to the leader using Linux iptables. This allows administrators to access Prism using any Controller VM IP address. If the Prism leader fails, a new leader is elected. The leader also communicates with the ESXi hosts for VM status and related information. Junos Space Security Director manages vSRX Virtual Firewalls deployed on each node of a Nutanix AHV cluster, and it acts as a unified security policy manager to apply consistent policies across all vSRX VMs in Nutanix-based private and public clouds (AWS/Azure).

Traffic between VMs and applications is redirected through the vSRX, allowing next-generation firewall security services with advanced threat prevention to be provisioned. Security policies enforced on traffic inside the Nutanix Enterprise Cloud augment the Nutanix HCI with microsegmentation, blocking sophisticated threats that propagate laterally while identifying and controlling application and user access. This enables security administrators to isolate and segment mission-critical applications and data using zero trust security principles.

Components of vSRX Deployment with Nutanix

Joint solution with vSRX and Nutanix includes the following key components:

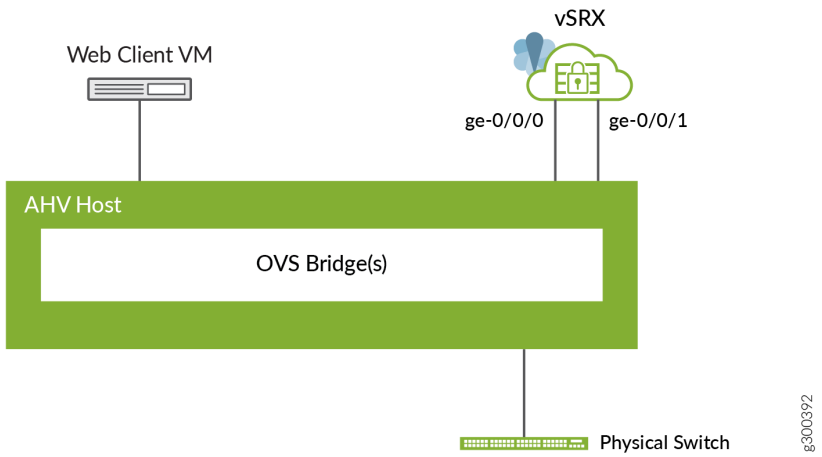
- **vSRX Virtual Firewall**—vSRX offers the same full-featured advanced security as the physical Juniper Networks SRX Series Services Gateways, but in a virtualized form.
- **Junos Space Security Director**—Junos Space Security Director allows network operators to manage a distributed network of virtual and physical firewalls from a single location. Serving as the management interface for the vSRX Virtual Firewall, Security Director manages the firewall policies on all vSRX instances. It includes a customizable dashboard with details, threat maps, and event logs, providing unprecedented visibility into network security. Remote mobile monitoring is also possible through a mobile application for Google Android and Apple iOS systems.
- **Nutanix AHV**—Nutanix AHV is an enterprise-class virtualization solution included with the Nutanix Enterprise Cloud OS, with no additional software components to license, install, or manage. Starting with proven open-source virtualization technology, AHV combines an enhanced datapath for optimal performance, security hardening, flow network virtualization, and complete management features to deliver a leaner yet more powerful virtualization stack, no costly shelfware, and lower virtualization costs.
- **Nutanix Manager (Nutanix Prism)**—Nutanix Prism is an end-to-end management tool for administrators to configure and monitor the Nutanix cluster and solutions for virtualized data center environments using the nCLI and the Web console. The end-to-end management capability streamlines and automates common workflows, eliminating the need for multiple management solutions across data center operations. Powered by advanced machine learning technology, Prism

analyzes system data to generate actionable insights for optimizing virtualization and infrastructure management.

Sample vSRX Deployment Using Nutanix AHV

A Sample vSRX deployment to provide security for applications running in a private subnet of Nutanix Enterprise Cloud with AHV hypervisor is shown in Figure 4 on page 13.

Figure 4: Sample vSRX Deployment in Nutanix Enterprise Cloud Using AHV



A vSRX image is loaded into the Linux-based kernel with Nutanix AHV virtualization solution as the hypervisor. AHV-based VMs support multitenancy, allowing you to run multiple vSRX VMs on the host OS. AHV manages and shares the system resources between the host OS and the multiple vSRX VMs.

NOTE: vSRX requires you to enable hardware-based virtualization on a host OS that contains an Intel Virtualization Technology (VT) capable processor.

The basic components of this deployment include:

- **Linux bridge**—Used for CVM control traffic
- **Open vSwitch (OVS) bridge(s)**—Used form VM traffic and to connect to physical ports
- **Physical switch**—Transports in or out traffic to the physical network ports on the host

RELATED DOCUMENTATION

- Requirements for vSRX on KVM
- Upgrade a Multi-core vSRX
- Install vSRX with KVM

Requirements for vSRX on Nutanix

IN THIS SECTION

These topics provide an overview of requirements for deploying a vSRX 3.0 instance on Nutanix.

System Requirements for Nutanix

IN THIS SECTION

This topic provides the system requirement details.

Table 1 on page 15 lists the system requirements for a vSRX 3.0 instance deployed on Nutanix.

Table 1: System Requirements for vSRX 3.0

Component	Specification and Details
Hypervisor support	AHV 5.9
Memory	4 GB
Disk space	16 GB
vCPUs	2
vNICs	Up to 8
vNIC type	Virtio

Interface Mapping for vSRX 3.0 on Nutanix

Table 2 on page 15 shows the vSRX 3.0 and Nutanix interface names. The first network interface is used for the out-of-band management (fxp0) for vSRX 3.0.

Table 2: vSRX 3.0 and Nutanix Interface Names

Interface Number	vSRX 3.0 Interface	Nutanix Interface
1	fxp0	eth0
2	ge-0/0/0	eth1
3	ge-0/0/1	eth2
4	ge-0/0/2	eth3

Table 2: vSRX 3.0 and Nutanix Interface Names *(Continued)*

Interface Number	vSRX 3.0 Interface	Nutanix Interface
5	ge-0/0/3	eth4
6	ge-0/0/4	eth5
7	ge-0/0/5	eth6
8	ge-0/0/6	eth7

We recommend putting revenue interfaces in routing instances as a best practice to avoid asymmetric traffic/routing, because fxp0 is part of the default (inet.0) table by default. With fxp0 as part of the default routing table, there might be two default routes needed: one for the fxp0 interface for external management access, and the other for the revenue interfaces for traffic access. Putting the revenue interfaces in a separate routing instance avoids this situation of two default routes in a single routing instance.

NOTE: Ensure that interfaces belonging to the same security zone are in the same routing instance. See KB Article - Interface must be in the same routing instance as the other interfaces in the zone.

vSRX 3.0 Default Settings on Nutanix

vSRX 3.0 requires the following basic configuration settings:

- Interfaces must be assigned IP addresses.
- Interfaces must be bound to zones.
- Policies must be configured between zones to permit or deny traffic.

Table 3 on page 17 lists the factory-default settings for security policies on the vSRX 3.0.

Table 3: Factory-Default Settings for Security Policies

Source Zone	Destination Zone	Policy Action
trust	untrust	permit
trust	trust	permit

> ⚠ **CAUTION**: Do not use the **load factory-default** command on a vSRX 3.0 Nutanix instance. The factory-default configuration removes the Nutanix preconfiguration. If you must revert to factory default, ensure that you manually reconfigure Nutanix preconfiguration statements before you commit the configuration; otherwise, you will lose access to the vSRX 3.0 instance. See *Configure vSRX Using the CLI* for Nutanix preconfiguration details.

Best Practices for Improving vSRX 3.0 Performance

Refer the following deployment practices to improve vSRX 3.0 performance:

- Disable the source/destination check for all vSRX 3.0 interfaces.
- Limit public key access permissions to 400 for key pairs.
- Ensure that there are no contradictions between Nutanix security groups and your vSRX 3.0 configuration.
- Use vSRX 3.0 NAT to protect your instances from direct Internet traffic.

Reference Requirements

Requirements for vSRX 3.0 with different types of Hypervisors are:

- **Requirements for vSRX on VMware**—See *Requirements for vSRX on VMware*
- **Requirements for vSRX on KVM-Based Hypervisor**—See *Requirements for vSRX on KVM*
- **Requirements for vSRX with Hype-V-Based Hypervisor**—See *Requirements for vSRX on Microsoft Hyper-V*

Junos OS Features Supported on vSRX with Nutanix

IN THIS SECTION

SRX Series Features Supported on vSRX

vSRX inherits most of the branch SRX Series features with the following considerations shown in Table 4 on page 18.

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 at: Feature Explorer: vSRX .

Table 4: vSRX Feature Considerations

Feature	Description
Application firewall	Supported
Deep packet inspection	Supported

Table 4: vSRX Feature Considerations *(Continued)*

Feature	Description
IDP	The IDP feature is subscription based and must be purchased. After purchase, you can activate the IDP feature with the license key. For SRX Series IDP configuration details, see: Understanding Intrusion Detection and Prevention for SRX Series In J-Web, use the following steps to add or edit an IPS rule: 1. Click **Security**>**IDP**>**Policy**>**Add**. 2. In the Add IPS Rule window, select **All** instead of **Any** for the Direction field to list all the FTP attacks.
J-Web	Supported
Layer 3 Routed Mode	Supported
Layer 2 Transparent mode	Supported
Screens	Supported
Secure wire	Supported
GPRS	Supported
Transparent mode	The known behaviors for transparent mode support on vSRX are: • The default MAC learning table size is restricted to 16,383 entries. • VMware vSwitch does not support MAC learning. It also floods traffic to the secondary node. The traffic is silently dropped by the flow on the secondary node. For information on configuring transparent mode vSRX, see: Layer 2 Bridging and Transparent Mode Overview.

Table 4: vSRX Feature Considerations *(Continued)*

Feature	Description
UTM	The UTM feature is subscription based and must be purchased. After purchase, you can activate the UTM feature with the license key. For SRX Series UTM configuration details, see: Unified Threat Management Overview For SRX Series UTM antispam configuration details, see: Antispam Filtering Overview.

SRX Series Features Not Supported on vSRX

vSRX inherits many features from the SRX Series device product line. Table 5 on page 20 lists SRX Series features that are not applicable in a virtualized environment, that are not currently supported, or that have qualified support on vSRX.

Table 5: SRX Series Features Not Supported on vSRX

SRX Series Feature		vSRX Notes
Application Layer Gateways		
	Avaya H.323	Not supported
Authentication with IC Series devices		
	Layer 2 enforcement in UAC deployments	Not supported **NOTE**: UAC-IDP and UAC-UTM also are not supported.
Chassis cluster support		

Table 5: SRX Series Features Not Supported on vSRX *(Continued)*

SRX Series Feature		vSRX Notes
	Chassis cluster for VirtIO driver	Not supported **NOTE**: The link status of VirtIO interfaces is always reported as UP, so a vSRX chassis cluster cannot receive link up and link down messages from VirtIO interfaces.
	Dual control links	Not supported
	In-band and low-impact cluster upgrades	Not supported
	LAG and LACP (Layer 2 and Layer 3)	Not supported
	Layer 2 Ethernet switching	Not supported
	Low-latency firewall	Not supported
	SR-IOV interfaces	Not supported
Class of service		
	High-priority queue on SPC	Not supported
	Tunnels	Only GRE and IP-IP tunnels supported
Data plane security log messages (stream mode)		
	TLS protocol	Not supported

Table 5: SRX Series Features Not Supported on vSRX *(Continued)*

SRX Series Feature		vSRX Notes
Diagnostic tools		
	Flow monitoring cflowd version 9	Not supported
	Ping Ethernet (CFM)	Not supported
	Traceroute Ethernet (CFM)	Not supported
DNS proxy		
	Dynamic DNS	Not supported
Ethernet link aggregation		
	LACP in standalone or chassis cluster mode	Not supported
	Layer 3 LAG on routed ports	Not supported
	Static LAG in standalone or chassis cluster mode	Not supported
Ethernet link fault management		
	Physical interface (encapsulations)	
	ethernet-ccc **ethernet-tcc**	Not supported

Table 5: SRX Series Features Not Supported on vSRX *(Continued)*

SRX Series Feature		vSRX Notes
	extended-vlan-ccc **extended-vlan-tcc**	Not supported
	Interface family	
	ccc, tcc	Not supported
	ethernet-switching	Not supported
Flow-based and packet-based processing		
	End-to-end packet debugging	Not supported
	Network processor bundling	Not supported
	Services offloading	Not supported
Interfaces		
	Aggregated Ethernet interface	Not supported
	IEEE 802.1X dynamic VLAN assignment	Not supported
	IEEE 802.1X MAC bypass	Not supported
	IEEE 802.1X port-based authentication control with multisupplicant support	Not supported

Table 5: SRX Series Features Not Supported on vSRX *(Continued)*

SRX Series Feature		vSRX Notes
	Interleaving using MLFR	Not supported
	PoE	Not supported
	PPP interface	Not supported
	PPPoE-based radio-to-router protocol	Not supported
	PPPoE interface **NOTE**: Starting in Junos OS Release 15.1X49-D100 and Junos OS Release 17.4R1, the vSRX supports Point-to-Point Protocol over Ethernet (PPPoE) interface.	Not supported
	Promiscuous mode on interfaces	Only supported if enabled on the hypervisor
IP Sec and VPNs		
	Acadia - Clientless VPN	Not supported
	DVPN	Not supported
	Hardware IPsec (bulk crypto) Cavium/RMI	Not supported
	IPsec tunnel termination in routing instances	Supported on virtual router only

Table 5: SRX Series Features Not Supported on vSRX *(Continued)*

SRX Series Feature		vSRX Notes
	Multicast for AutoVPN	Not supported
IPv6 support		
	DS-Lite concentrator (also called Address Family Transition Router [AFTR])	Not supported
	DS-Lite initiator (also called Basic Bridging Broadband [B4])	Not supported
ISSU		Not supported
J-Web		
	Enhanced routing configuration	Not supported
	New Setup wizard (for new configurations)	Not supported
	PPPoE wizard	Not supported
	Remote VPN wizard	Not supported
	Rescue link on dashboard	Not supported
	UTM configuration for Kaspersky antivirus and the default Web filtering profile	Not supported

Table 5: SRX Series Features Not Supported on vSRX *(Continued)*

SRX Series Feature		vSRX Notes
Log File formats for system (control plane) logs		
	Binary format (binary)	Not supported
	WELF	Not supported
Miscellaneous		
	Hardware acceleration	Not supported
	Logical systems	Not supported
	Outbound SSH	Not supported
	Remote instance access	Not supported
	USB modem	Not supported
	Wireless LAN	Not supported
MPLS		
	circuit cross-connect (CCC) and translational cross-connect (TCC)	Not supported
	Layer 2 VPNs for Ethernet connections	Only if promiscuous mode is enabled on the hypervisor
Network Address Translation		

Table 5: SRX Series Features Not Supported on vSRX *(Continued)*

SRX Series Feature		vSRX Notes
	Maximize persistent NAT bindings	Not supported
Packet capture		
	Packet capture	Only supported on physical interfaces and tunnel interfaces, such as *gr*, *ip*, and *st0*. Packet capture is not supported on redundant Ethernet interfaces (*reth*).
Routing		
	BGP extensions for IPv6	Not supported
	BGP Flowspec	Not supported
	BGP route reflector	Not supported
	Bidirectional Forwarding Detection (BFD) for BGP	Not supported
	CRTP	Not supported
Switching		
	Layer 3 Q-in-Q VLAN tagging	Not supported
Transparent mode		
	UTM	Not supported

Table 5: SRX Series Features Not Supported on vSRX *(Continued)*

SRX Series Feature		vSRX Notes
Unified threat management		
	Express AV	Not supported
	Kaspersky AV	Not supported
Upgrading and rebooting		
	Autorecovery	Not supported
	Boot instance configuration	Not supported
	Boot instance recovery	Not supported
	Dual-root partitioning	Not supported
	OS rollback	Not supported
User interfaces		
	NSM	Not supported
	SRC application	Not supported
	Junos Space Virtual Director	Not supported

2

CHAPTER

Installing vSRX in Nutanix

Launch and Deploy vSRX in Nutanix AHV Cluster

IN THIS SECTION

Before you begin, you need a Nutanix account and an Identity and Access Management (IAM) role, with all required permissions to access, create, modify, and delete Nutanix cloud objects. You should also create access keys and corresponding secret access keys, X.509 certificates, and account identifiers. For better understanding of Nutanix terminologies and their use in vSRX deployments, see Understanding vSRX with Nutanix.

The topics in this section help you launch vSRX instances in a Nutanix AHV cluster.

Log In to Nutanix Setup

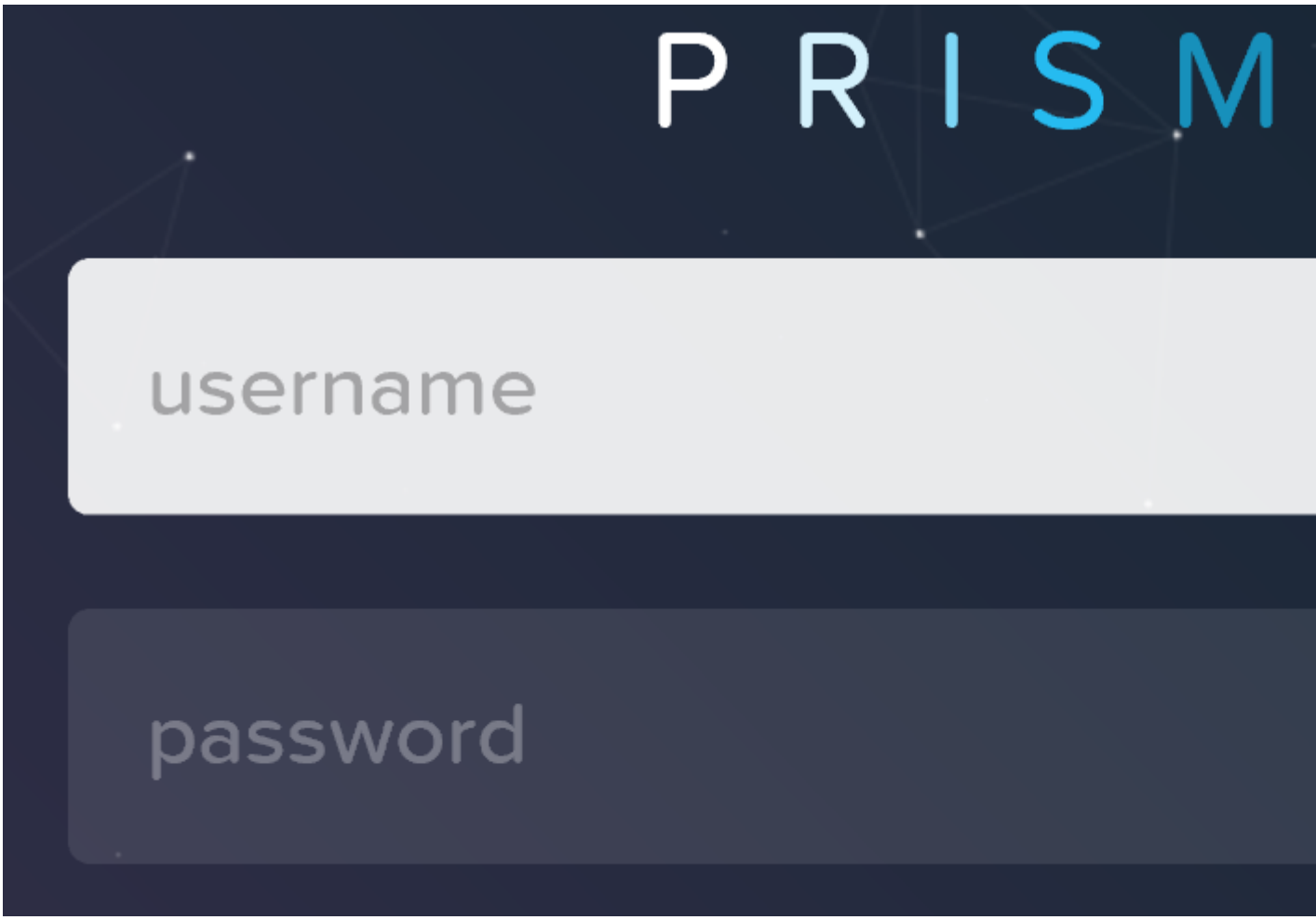
This topic provide details on how to log in to Nutanix setup.

Log in to the Nutanix Management Console.

NOTE: To access the Nutanix management console, remote access must be enabled on your local machine.

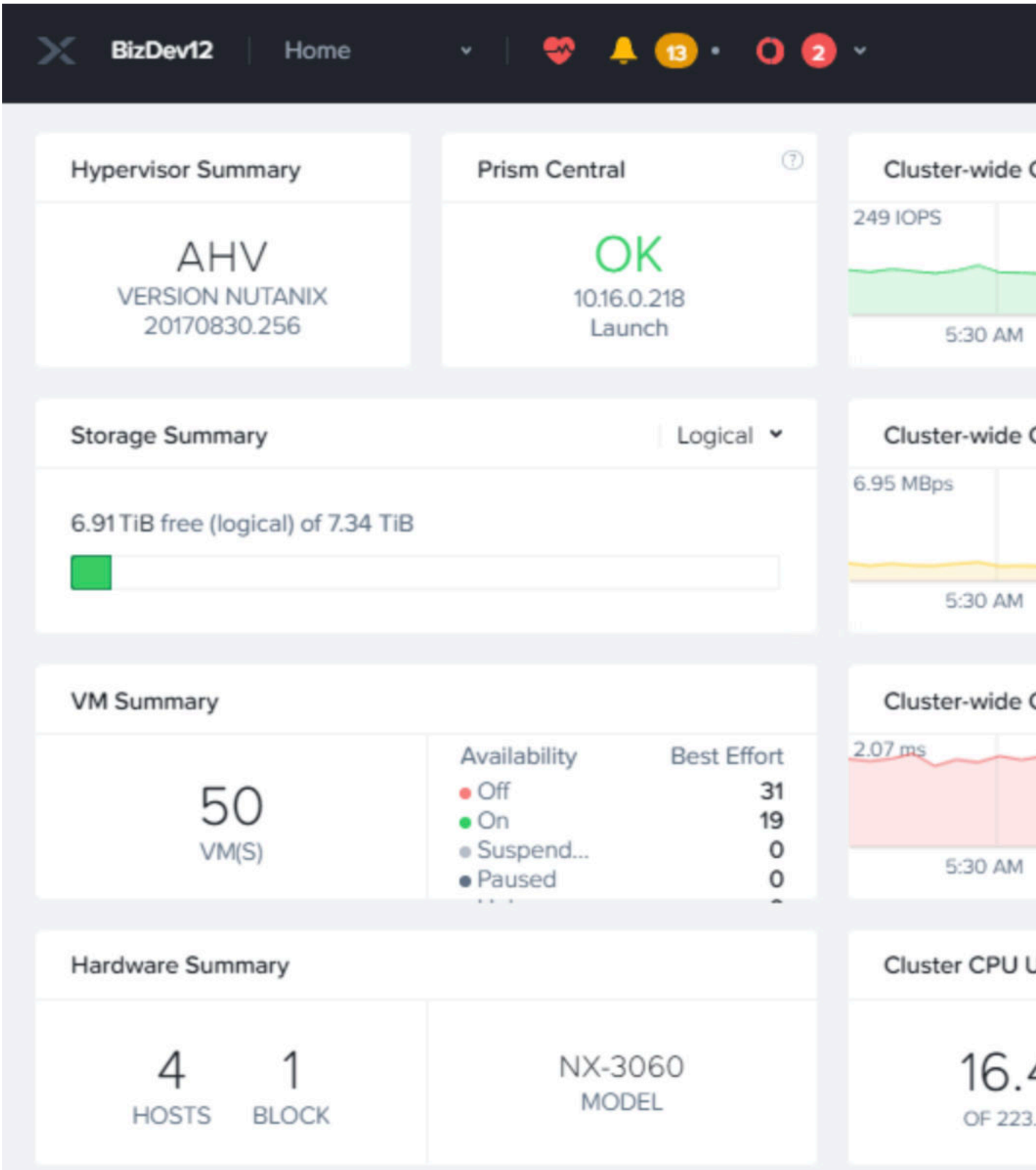
Once you have logged in to the remote Windows machine, you can access the Nutanix Prims Enable using your Web browser.

Figure 5: Prism Element Login Page



After you provide login details, the Nutanix Prism home page appears.

Figure 6: Initial Page of Prism Element



Adding a vSRX Image

Before you create a vSRX image, copy the image in the local machine from which the image can be accessed by Nutanix Prism Element. After copying, locally source the images from Prism GUI.

All the required vSRX images are available in the Juniper download page. After you copy the vSRX image on the local machine, complete the following steps to upload the image in Nutanix:

1. Click the **Image configuration** option from the **Tool** menu in the on top-right corner of the Prism home page.
2. Click the **Upload Image** tab.
3. Enter the required image details and provide a local file path under Image source. Wait for the image to be uploaded successfully.

Network Creation

This topic provides details on configuring the network for deploying vSRX VMs.

You can create a Routing Engine-FPC (RE-FPC) (or any other network) using the following steps:

1. At the top-right corner of the Nutanix Prism page, under Settings, click the **Network Configuration** option.
2. Click the **Create Network** button, add details for creating an internal network for RE-FPC communication, and click the **Save** button.

   A message appears, indicating that the RE-FPC internal network was successfully created.

> **NOTE**: In this deployment guide, all the the networks created on Nutanix setup are VLAN-based networks. Therefore, if you are deploying a Routing Engine and FPC on different hosts (compute nodes), the VLAN that is used by the RE-FPC internal networks must be part of the allowable VLAN range that is configured on the top-of-rack switch connecting the two machines.
>
> We tested the use case in which the Routing Engine and FPC were deployed on different hosts. However, for all our other tests, we deployed the Routing Engine and FPC on the same host.

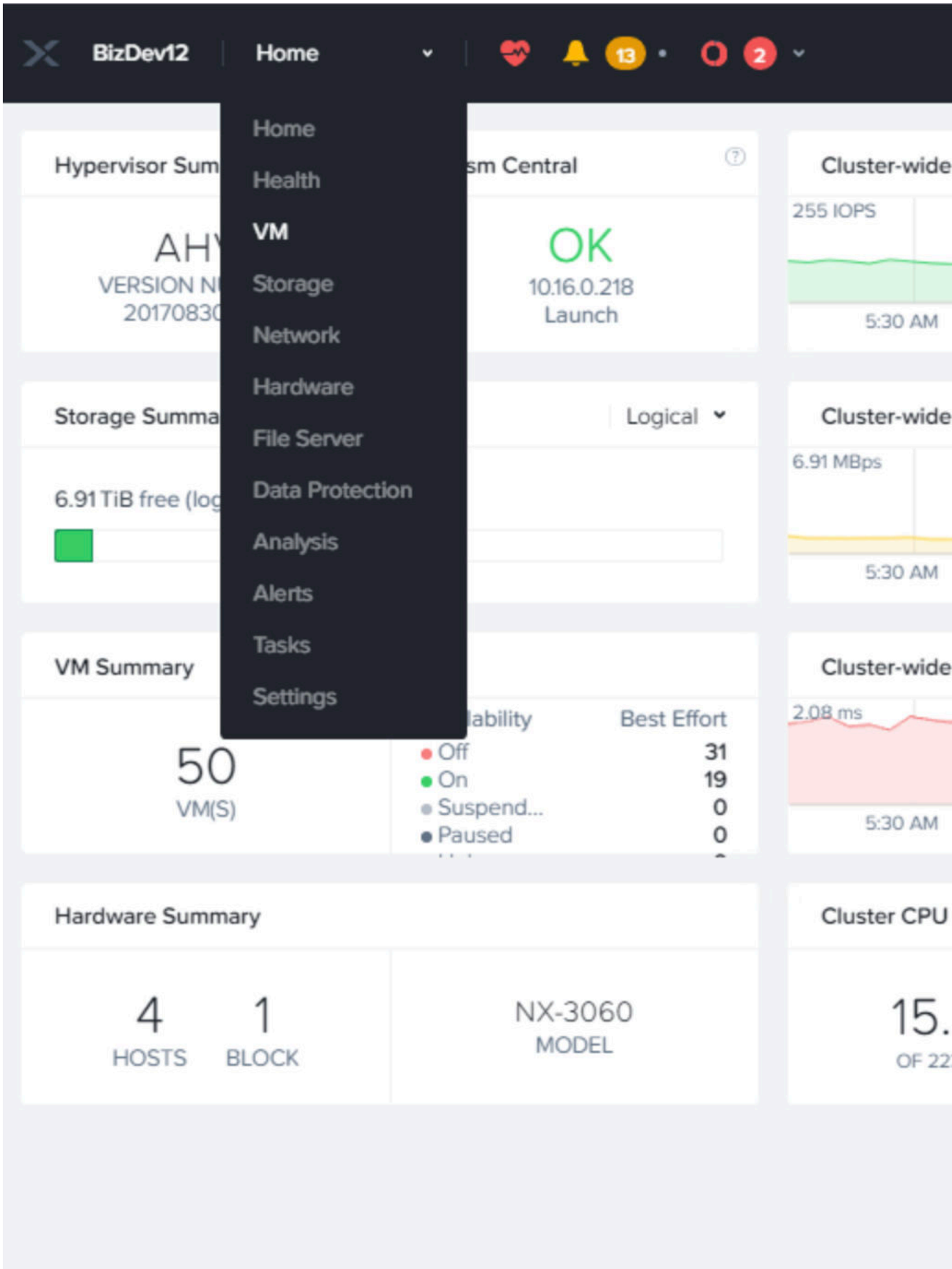
Create and Deploy a vSRX VM

This topic provides details on how to deploy a vSRX VM.

In Acropolis-managed clusters, you can create a new virtual machine (VM) through the Web console. When creating a VM, you can configure all of its components, such as number of vCPUs and memory, but you cannot attach a volume group to the VM. Attaching a volume group is possible only when you are modifying a VM.

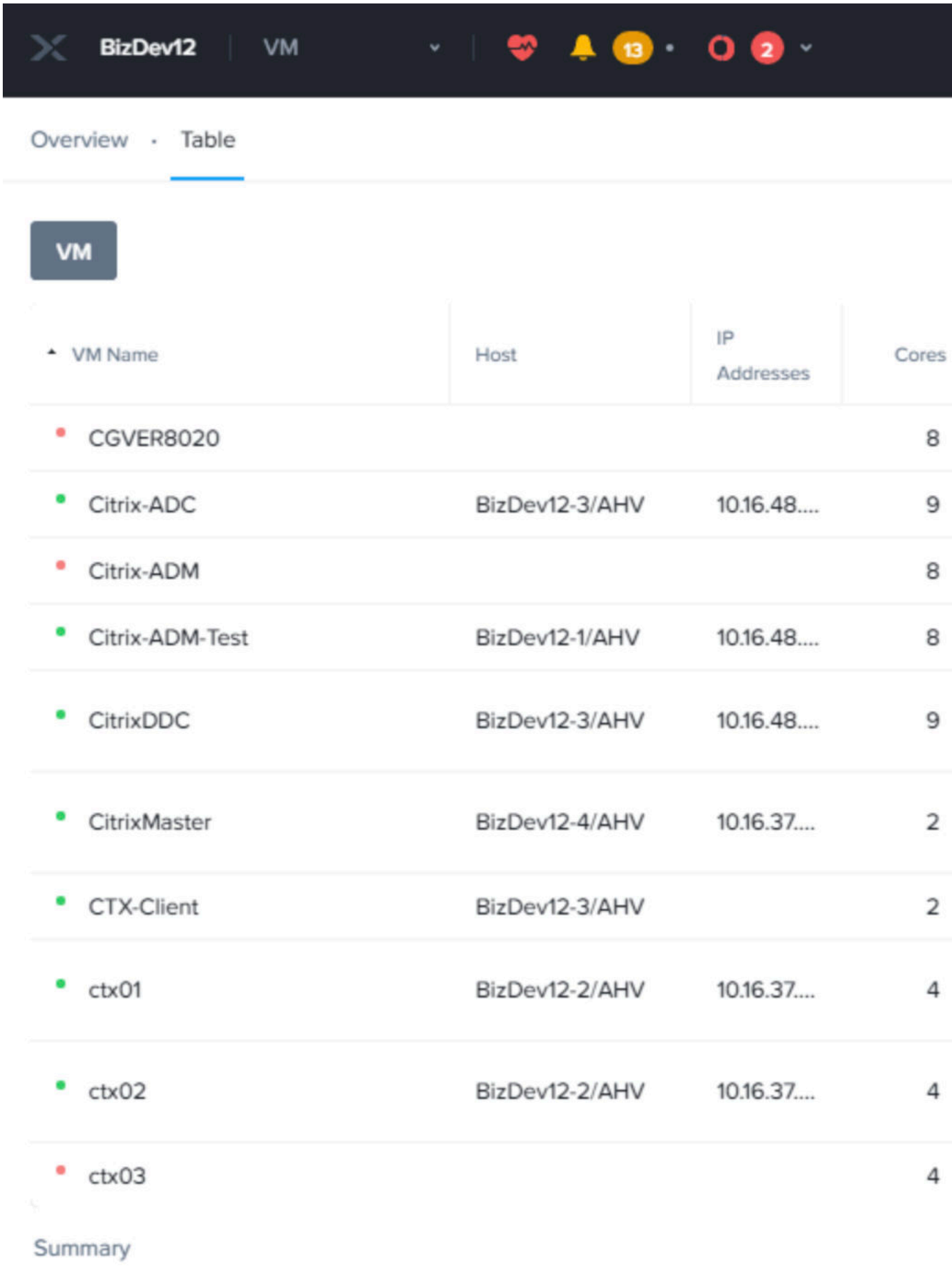
1. Click the **Home** menu at the top of the Prism home page and select the **VM** option from the drop-down list as as shown in Figure 7 on page 37.

Figure 7: VM Option Page



2. To create a VM, select the **VM** option under the Home tab (top-left corner) and click **+ Create VM** at the top-right side of the VM page as shown in Figure 8 on page 39.

Figure 8: VM Page



The Create VM page appears as shown in Figure 9 on page 42.

3. On the Create VM page, provide details of the indicated fields to create a vSRX VM as shown in Figure 9 on page 42 and click the **Save** button.

   - Name: Enter a name for the VM.
   - Description (optional): Enter a description for the VM.
   - vCPU(s): Enter the number of virtual CPUs to allocate to this VM.
   - Number of Cores per vCPU: Enter the number of cores assigned to each virtual CPU.
   - Memory: Enter the amount of memory to allocate to this VM.

- Select the time zone and update the compute details.

Figure 9: Create VM Page

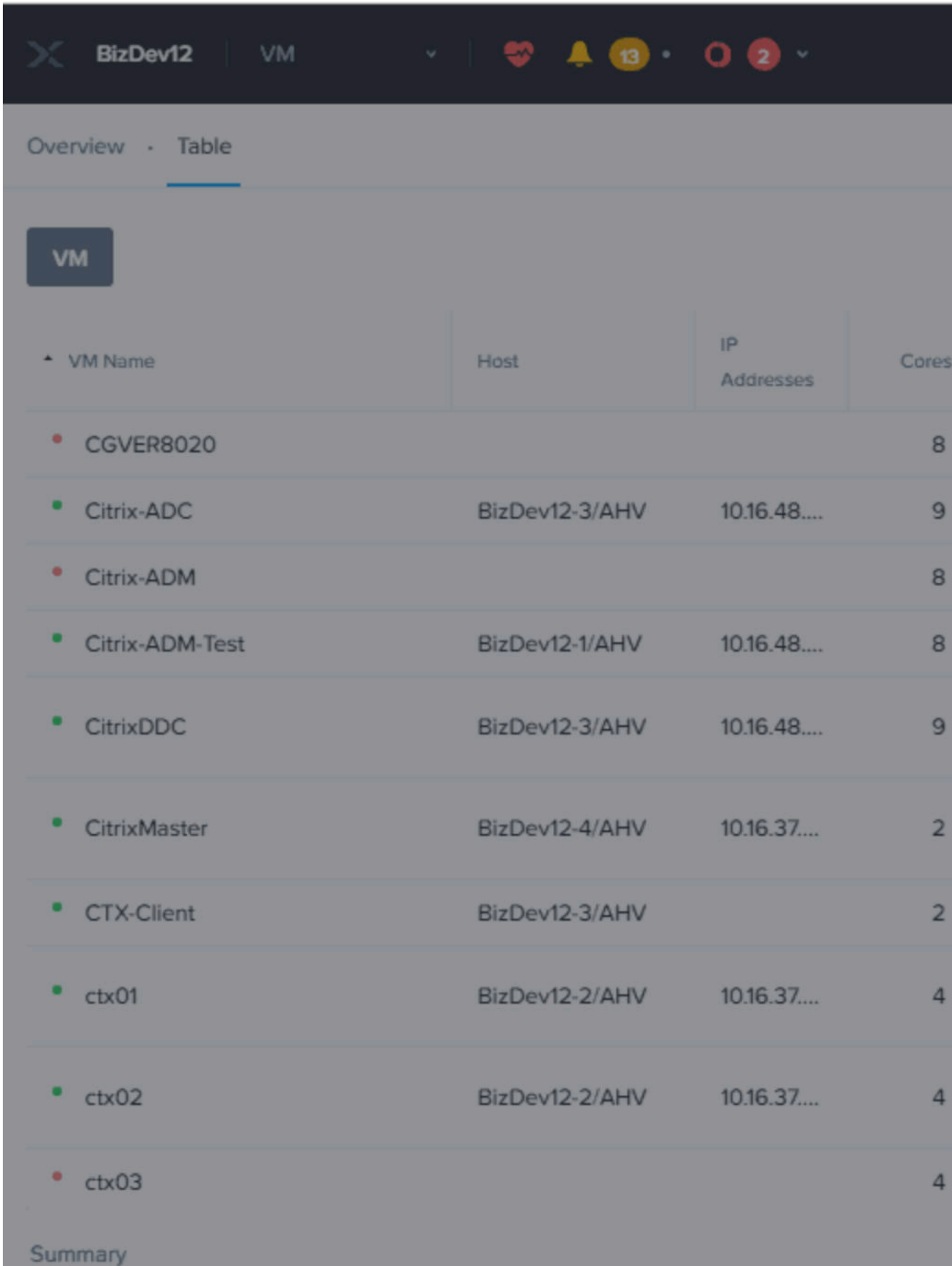
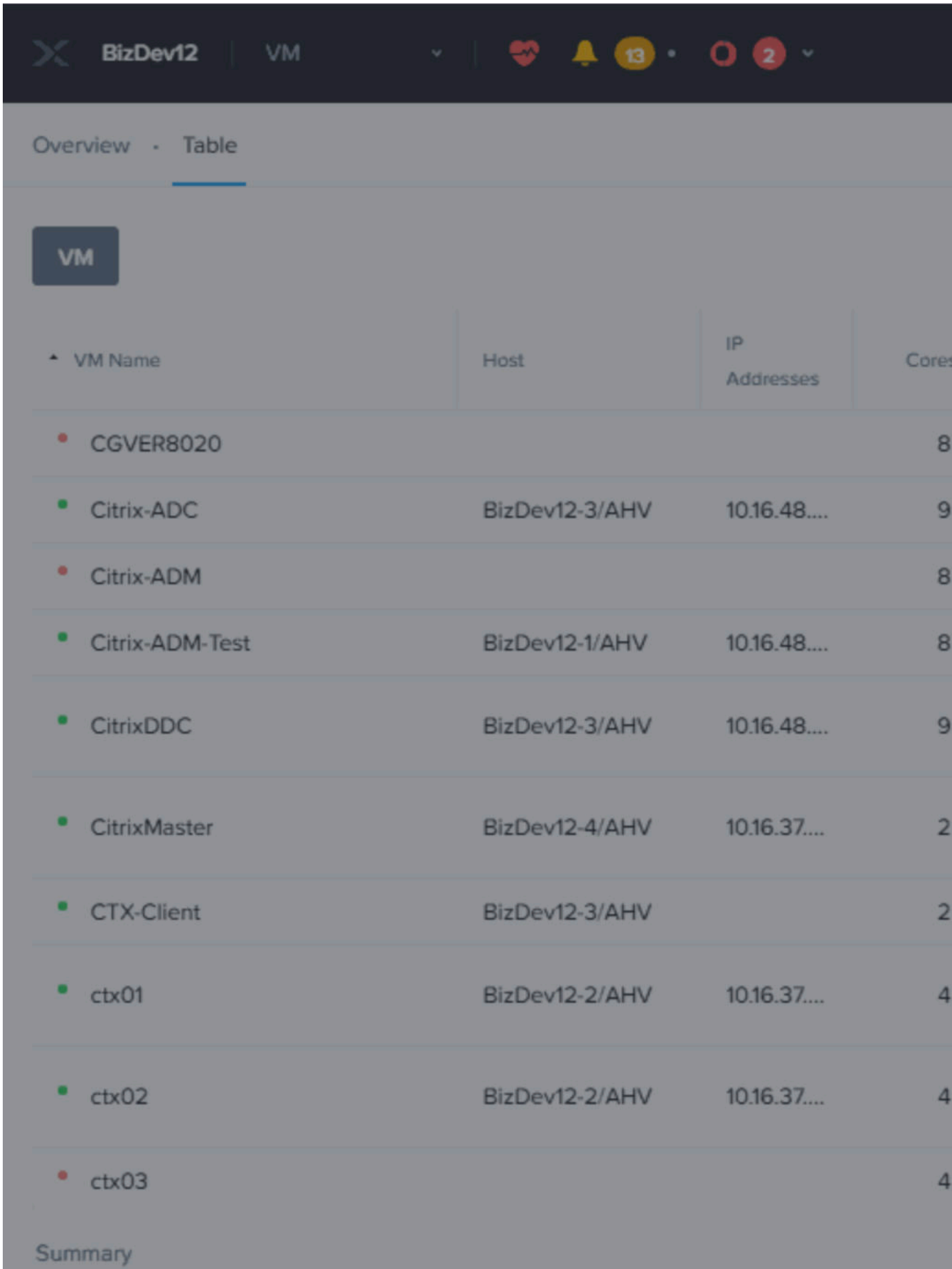
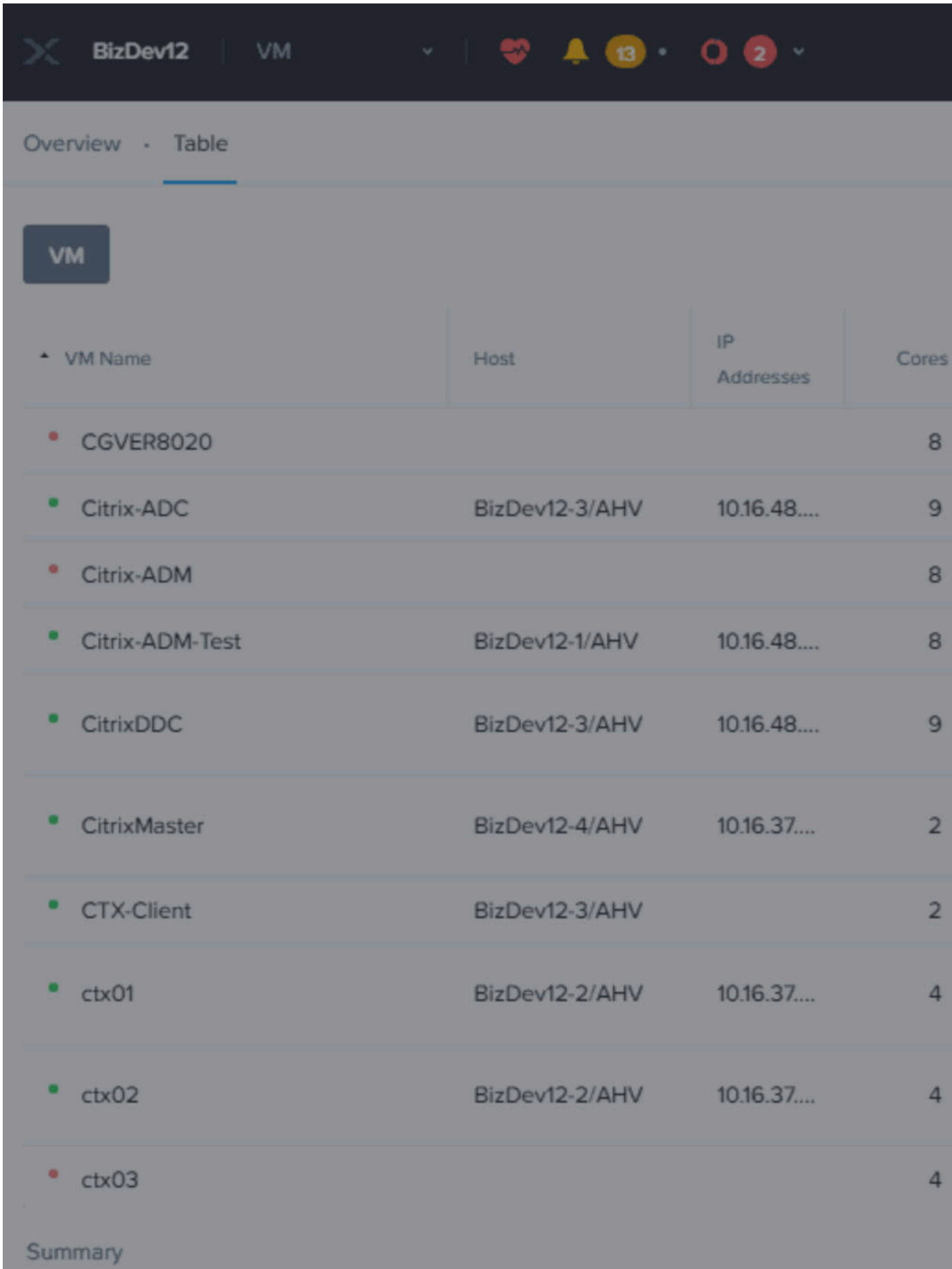


Figure 10: VM Compute Details Page



4. To attach a disk to the vSRX VM, click the **+ Add New Disk** option on the **Create VM** page as shown in Figure 11 on page 45.

Figure 11: VM Disk Details Page



5. The **Add Disk** page appears as shown in Figure 12 on page 48. Select the vSRX Junos Image.

   Do the following in the indicated fields and click on the **Add** button:

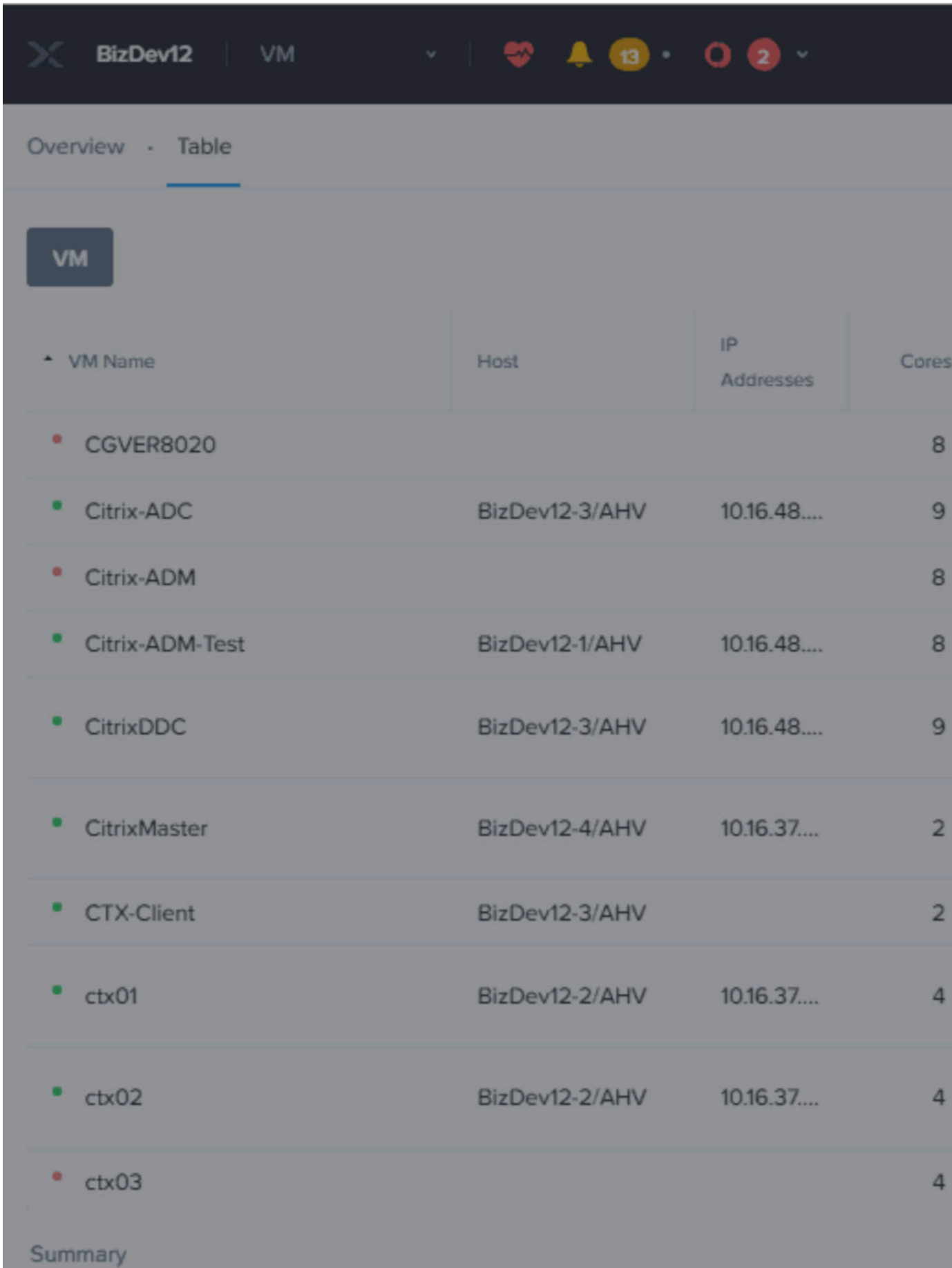
   - Type: Select the type of storage device, **DISK** or **CDROM**, from the drop-down list. The following fields and options vary depending on whether you choose DISK or CDROM.
   - Operation: Specify the device contents from the drop-down list.
     - Select **Clone from ADSF file** to copy any file from the cluster that can be used as an image onto the disk.
     - Select **Empty CDROM** to create a blank CD device. (This option appears only when CD is selected in the previous field.) A CD device is needed.
     - Select **Allocate on Container** to allocate space without specifying an image. (This option appears only when DISK is selected in the previous field.) Selecting this option means you are allocating space only. You have to provide a system image later from a CD or other source.
     - Select **Clone from Image Service** to copy an image that you have imported by using the image service feature onto the disk.
   - Bus Type: Select the bus type from the drop-down list. The choices are IDE, SCSI, or SATA.
   - Path: Enter the path to the desired system image.

     NOTE: Field for entering the path appears only when Clone from ADSF file is selected. This file specifies the image to copy. For example, enter the pathname as /container_name/iso_name.iso. For example to clone an image from myos.iso in a container named crt1, enter /crt1/myos.iso. When a user types the container name (/container_name/), a list appears of the ISO files in that container (If one or more ISO files had previously been copied to that container).

   - Image: Select the image that you have created by using the image service feature. This field appears only when Clone from Image Service is selected. This field specifies the image to copy.
   - Size: Enter the disk size in GiBs. This field appears only when Allocate on Container is selected.
   - When all the field entries are correct, click the **Add** button to attach the disk to the VM and return to the Create VM page.

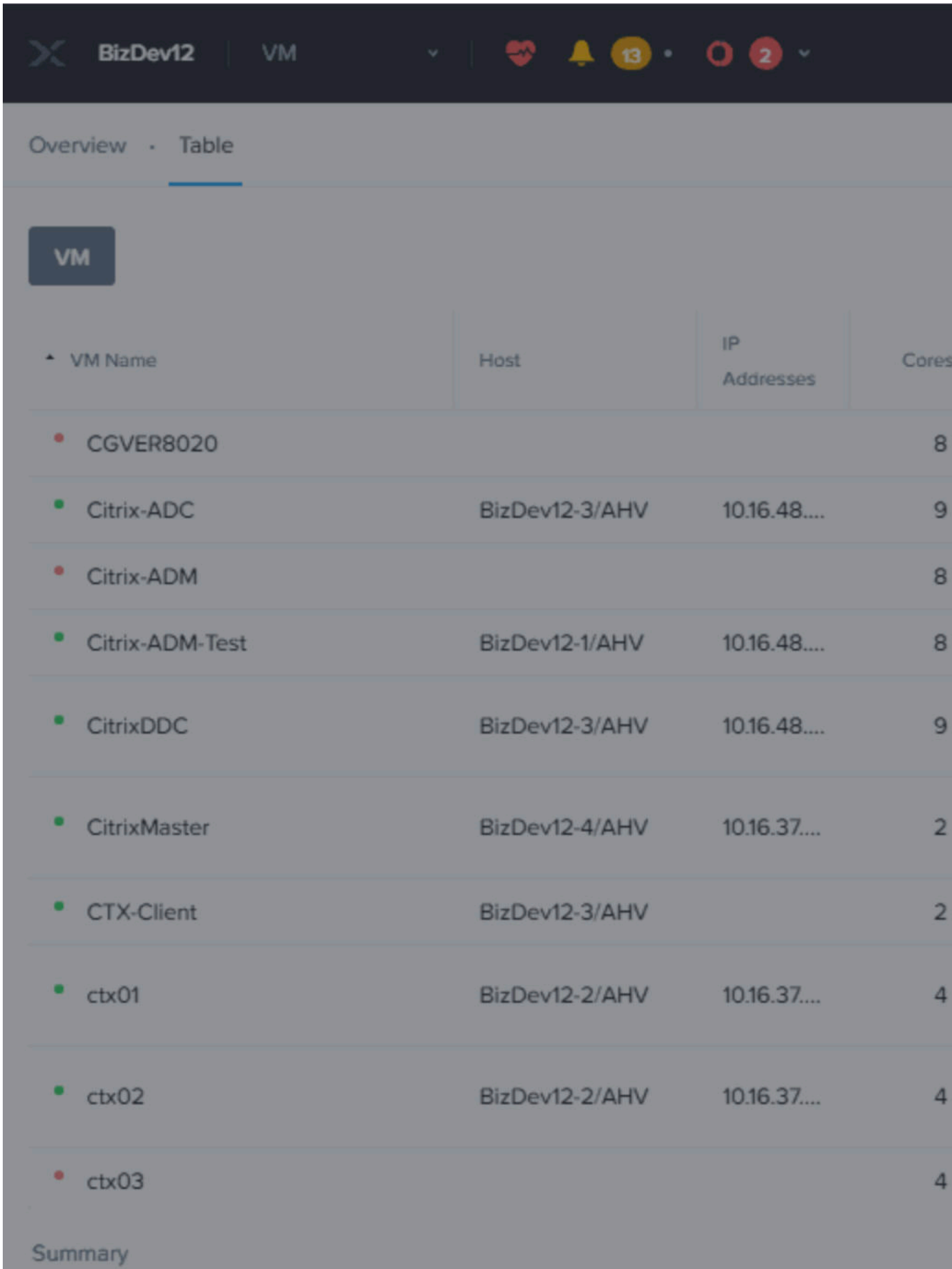
- Repeat Step "5" on page 46 to attach additional devices to the VM.

Figure 12: Add Disk Details Page



6. To create a network interface for the vSRX VM, click the **+ Add New NIC** option in the Create VM page as shown in Figure 13 on page 50. Add the NICs required.

Figure 13: Add New NIC Option

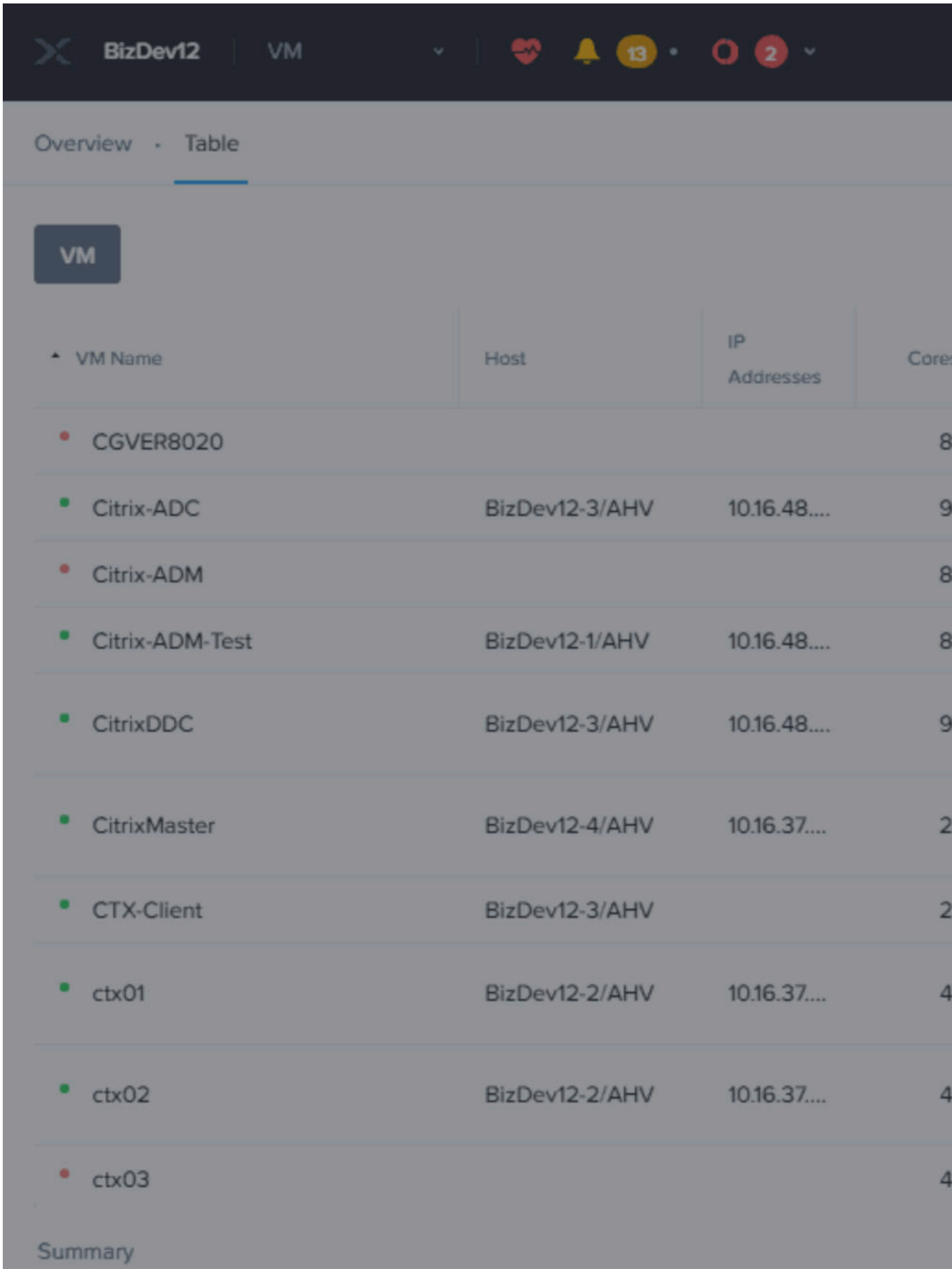


The Create NIC page appears as shown in Figure 14 on page 53. Do the following in the indicated fields:

- VLAN Name: Select the target virtual LAN from the drop-down list.
- VLAN ID: This is a read-only field that displays the VLAN ID.
- VLAN UUID: This is a read-only field that displays the VLAN UUID.
- Network Address/Prefix: This is a read-only field that displays the network IP address and prefix.
- IP Address: Enter an IP address for the VLAN. This field appears only if the NIC is placed in a managed network. Entering an IP address in this field is optional when the network configuration provides an IP pool. If the field is left blank, the NIC is assigned an IP address from the pool.
- When all the field entries are correct, click the **Add** button to create a network interface for the VM and return to the Create VM page.

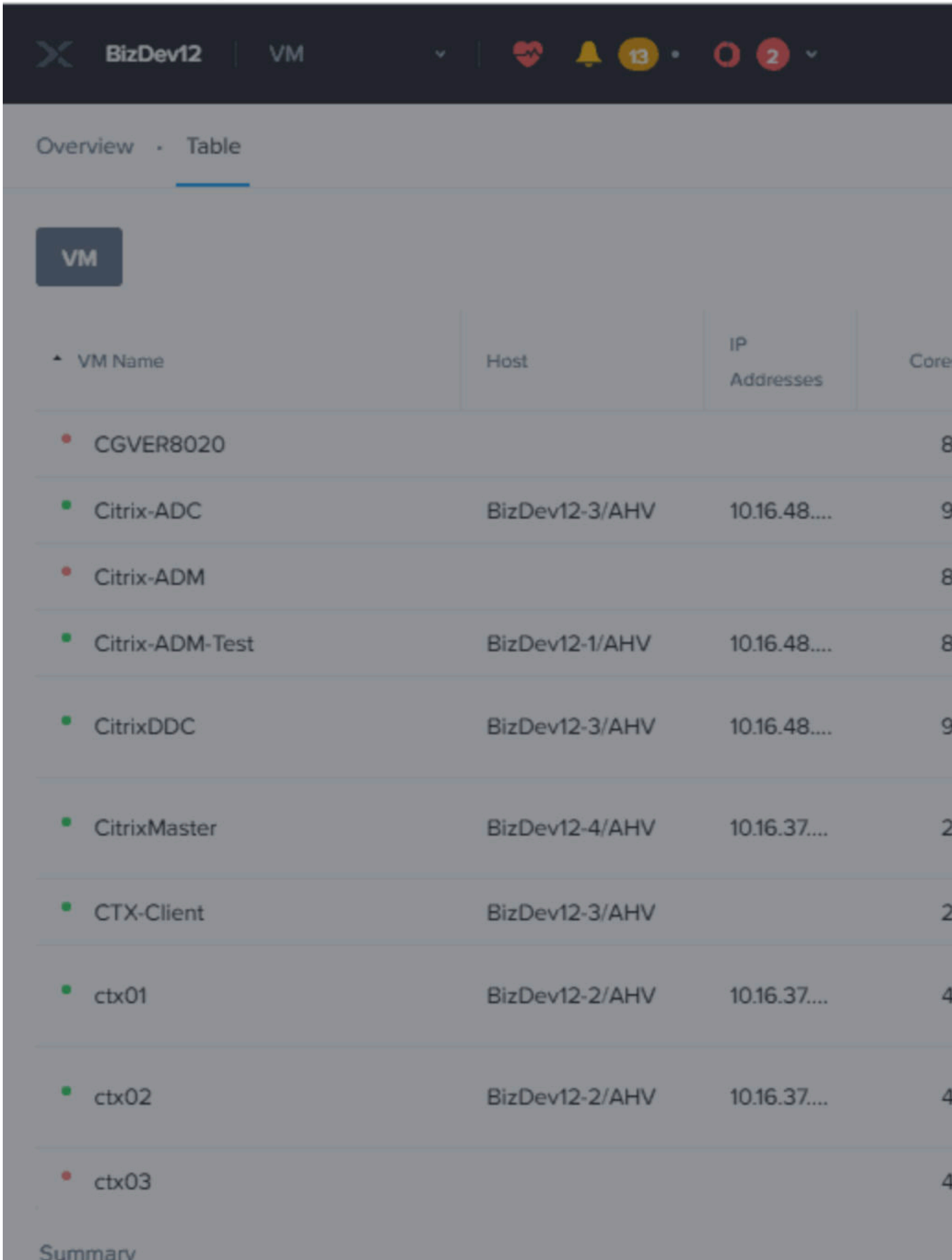
- Repeat this Step "6" on page 49 to create additional network interfaces for the VM.

Figure 14: Create NIC Page



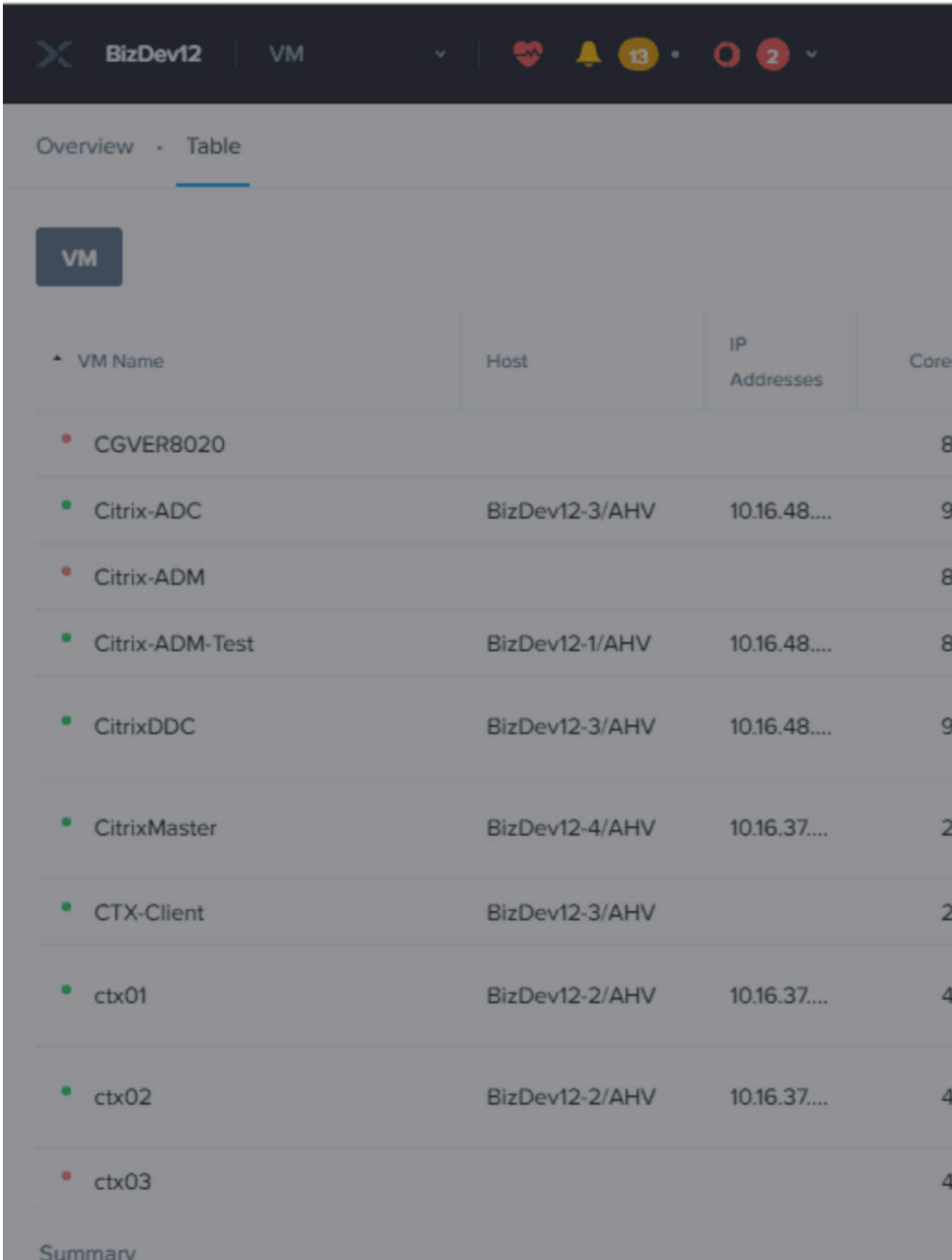
Repeat Step "6" on page 49 and add more VLANs and NICs as needed.

Figure 15: Adding More VLANs and NICs



7. (Optional) If host affinity is needed, click **Set Affinity**..

Figure 16: VM Host Affinity Page



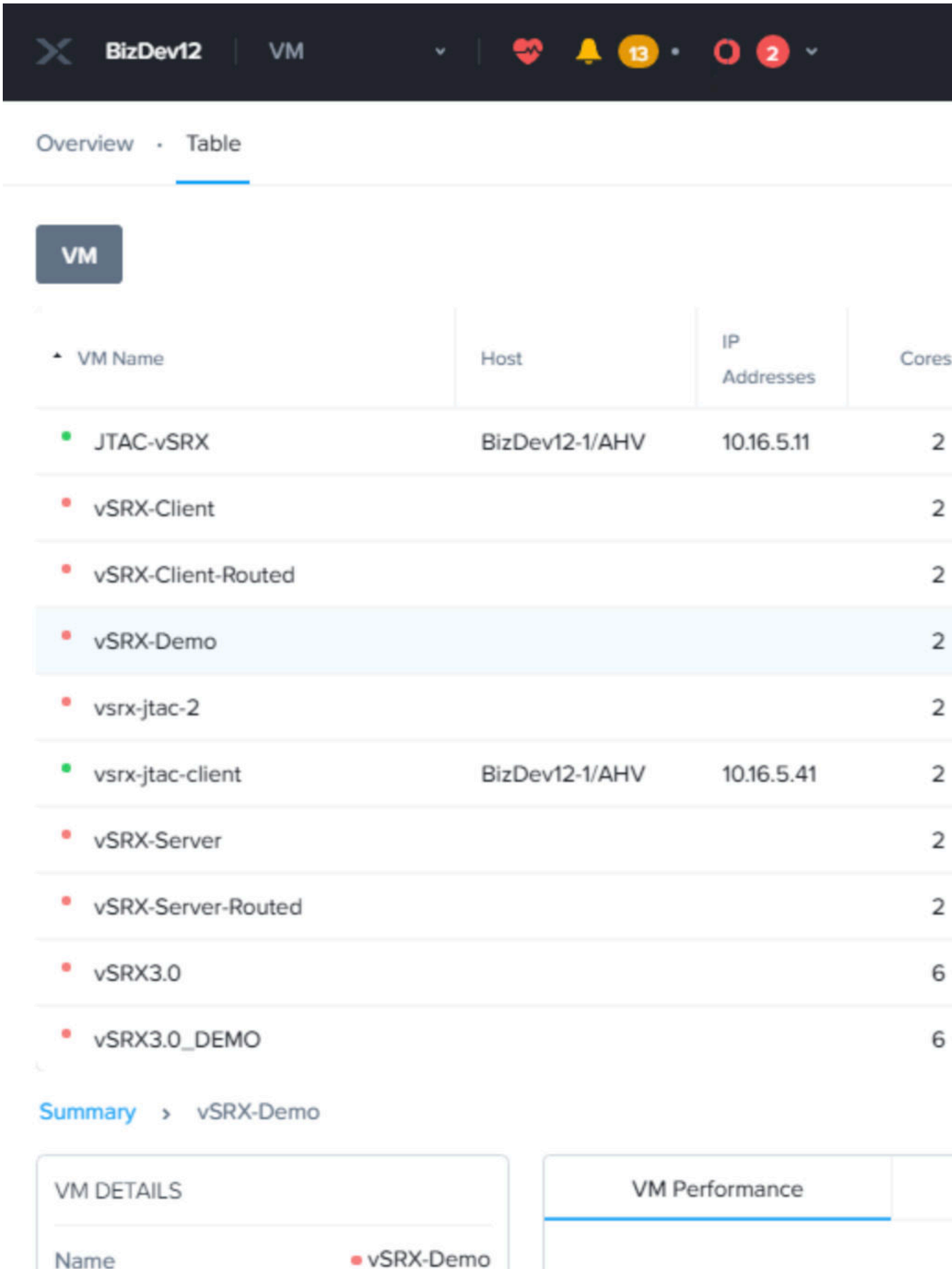
8. To customize the VM by using Cloud-init (for Linux VMs) or Sysprep (for Windows VMs), select the **Custom Script** check box.
9. When all the field entries are correct, click the **Save** button to create the VM and close the Create VM page.

Power on the vSRX VMs

This topic provides you details on how to power on vSRX VMs.

1. Use the Table drop-down list to search for VMs as shown in Figure 17 on page 60.

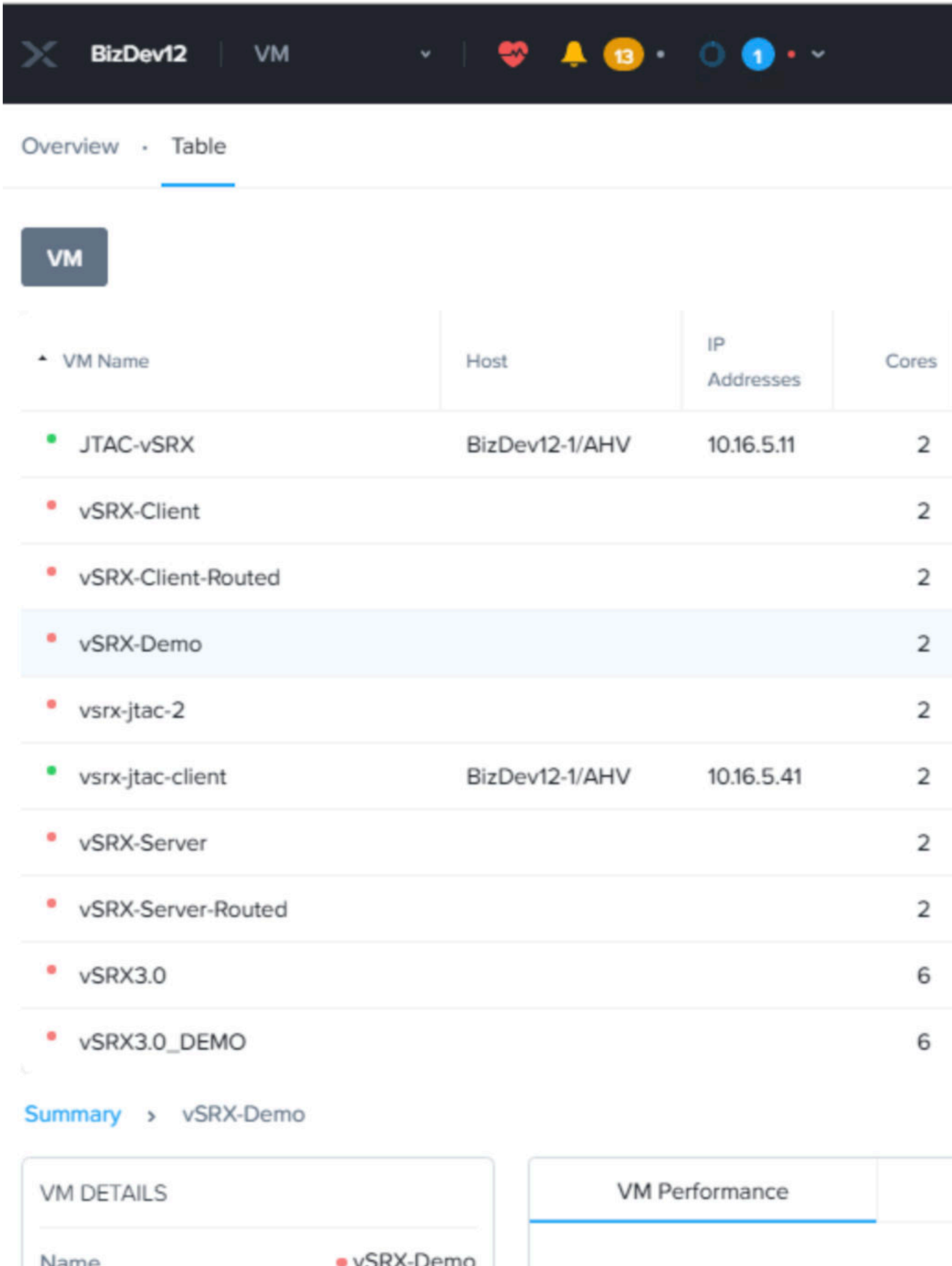
Figure 17: Powering on VMs



2. Click the **Power on** option (see Figure 17 on page 60) for each VM.

All the VMs will turn on as shown in Figure 18 on page 63

Figure 18: Power on VM Confirmation Page

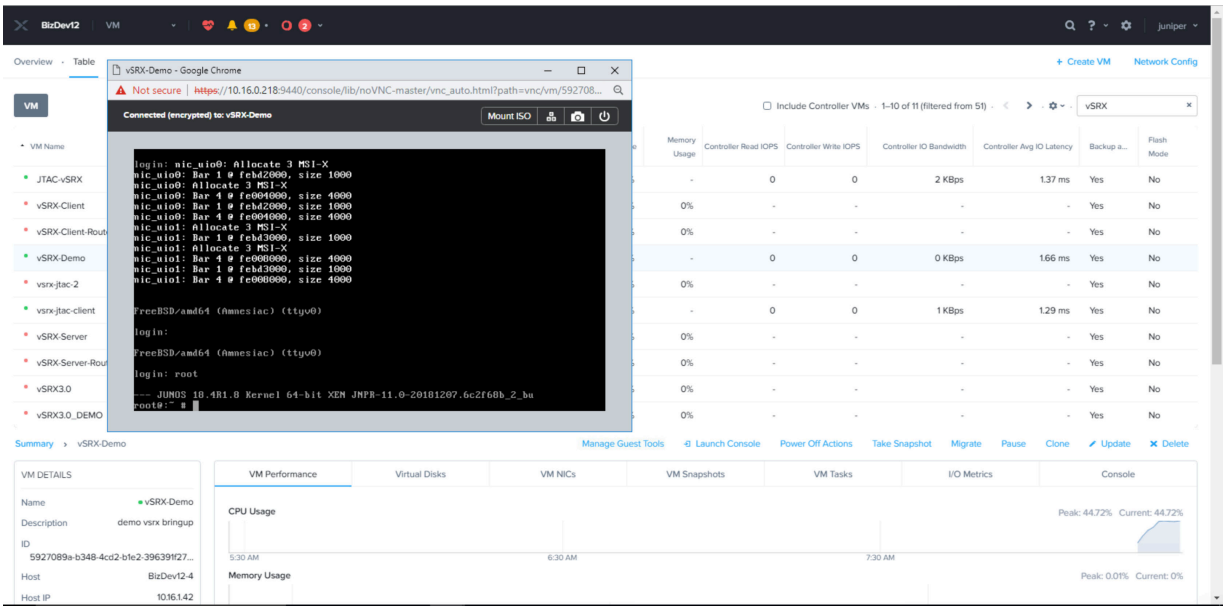


Launch vSRX VM Console

This topic explains how to launch the vSRX VM console.

Click the **Launch Console** option at the bottom of screenshot as shown in Figure 19 on page 64 to launch the VM console.

Figure 19: Launch Console Page



RELATED DOCUMENTATION

- Day One: vSRX on KVM

Upgrade the Junos OS for vSRX Software Release

You can upgrade the Junos OS for vSRX software using the CLI. Upgrading or downgrading Junos OS can take several hours, depending on the size and configuration of the network. Download the desired Junos OS Release for the **vSRX.tgz** file from the Juniper Networks website.

You also can upgrade using J-Web (see J-Web) or the Junos Space Network Management Platform (see Junos Space).

For the procedure on upgrading a specific Junos OS for vSRX software release, see the *Migration, Upgrade, and Downgrade Instructions* topic in the release-specific *vSRX Release Notes* available on the vSRX TechLibrary webpage.

CHAPTER 3

Configuring and Managing vSRX with Nutanix

vSRX Configuration and Management Tools

SUMMARY

This topic provides an overview of the various tools available to configure and manage a vSRX VM once it has been successfully deployed.

IN THIS SECTION

Understanding the Junos OS CLI and Junos Scripts

Junos OS CLI is a Juniper Networks specific command shell that runs on top of a UNIX-based operating system kernel.

Built into Junos OS, Junos script automation is an onboard toolset available on all Junos OS platforms, including routers, switches, and security devices running Junos OS (such as a vSRX instance).

You can use the Junos OS CLI and the Junos OS scripts to configure, manage, administer, and troubleshoot vSRX.

Understanding the J-Web Interface

The *J-Web* interface allows you to monitor, configure, troubleshoot, and manage vSRX instances by means of a Web browser. J-Web provides access to all the configuration statements supported by the vSRX instance.

Understanding Junos Space Security Director

As one of the Junos Space Network Management Platform applications, Junos Space Security Director helps organizations improve the reach, ease, and accuracy of security policy administration with a scalable, GUI-based management tool. Security Director automates security provisioning of a vSRX

instance through one centralized Web-based interface to help administrators manage all phases of the security policy life cycle more quickly and intuitively, from policy creation to remediation.

RELATED DOCUMENTATION

- CLI User Interface Overview
- J-Web Overview
- Security Director
- Mastering Junos Automation Programming
- Spotlight Secure Threat Intelligence

Configure vSRX Using the CLI

To configure the vSRX instance using the CLI:

1. Verify that the instance is powered on.
2. Log in using the username and password credentials for your vSRX VM deployment.
3. Start the CLI.

```
root#cli
root@>
```

4. Enter configuration mode.

```
configure
[edit]
root@#
```

5. Set the root authentication password by entering a *cleartext* password, an encrypted password, or an SSH public key string (*DSA* or *RSA*).

```
[edit]
root@# set system root-authentication plain-text-password
New password: password
Retype new password: password
```

6. Configure the traffic interfaces.

```
[edit]
root@# set interfaces ge-0/0/0 unit 0 family inet address assigned_ip/netmask
root@# set interfaces ge-0/0/1 unit 0 family inet address assigned_ip/netmask
```

> **NOTE**: Configuration of the management interface fxp0 for the vSRX is not necessary, because it is configured during vSRX VM deployment. Do not change the configuration for interface fxp0 and the default routing table or you will lose connectivity.

7. Configure routing interfaces to isolate management network and traffic network.

```
[edit]
root@# set routing-instances vsrx-vr1 instance-type virtual-router
root@# set routing-instances vsrx-vr1 interface ge-0/0/0.0
root@# set routing-instances vsrx-vr1 interface ge-0/0/1.0
```

8. Verify the configuration changes.

```
[edit]
root@# commit check
configuration check succeeds
```

9. Commit the current configuration to make it permanent and to avoid the possibility of losing connectivity to the vSRX instance.

```
[edit]
root@# commit confirmed
commit confirmed will be automatically rolled back in 10 minutes unless
confirmed
commit complete
# commit confirmed will be rolled back in 10 minutes
```

10. Commit the configuration to activate it on the instance.

```
[edit]
root@# commit
commit complete
```

11. Optionally, use the **show** command to display the configuration to verify that it is correct.

NOTE: Certain Junos OS software features require a license to activate the feature. To enable a licensed feature, you need to purchase, install, manage, and verify a license key that corresponds to each licensed feature. To conform to software feature licensing requirements, you must purchase one license per feature per instance. The presence of the appropriate software unlocking key on your virtual instance allows you to configure and use the licensed feature. See Managing Licenses for vSRX for details.

RELATED DOCUMENTATION

- Junos OS for SRX Series
- CLI User Guide

Configure vSRX Using the J-Web Interface

IN THIS SECTION

Access the J-Web Interface and Configuring vSRX

Use the Junos OS CLI to configure, at a minimum, the following parameters before you can access a vSRX VM using J-Web:

> ⚠ **CAUTION**: Do not change the configuration for interface fxp0 and default routing table or you will lose connectivity to the vSRX instance.

To configure vSRX using the *J-Web* Interface:

1. Launch a Web browser from the management instance.
2. Enter the vSRX fxp0 interface IP address in the Address box.
3. Specify the username and password.
4. Click **Log In**, and select the **Configuration Wizards** tab from the left navigation panel. The J-Web Setup wizard page opens.
5. Click **Setup**.

   You can use the Setup wizard to configure the vSRX VM or edit an existing configuration.

   - Select **Edit Existing Configuration** if you have already configured the wizard using the factory mode.
   - Select **Create New Configuration** to configure the vSRX VM using the wizard.

     The following configuration options are available in the guided setup:

     - Basic

       Select **basic** to configure the vSRX VM name and user account information as shown in Table 6 on page 71.

       - Instance name and user account options

         Table 6: Instance Name and User Account Information

Field	Description
Instance name	Type the name of the instance. For example: **vSRX**.

Table 6: Instance Name and User Account Information *(Continued)*

Field	Description
Root password	Create a default root user password.
Verify password	Verify the default root user password.
Operator	Add an optional administrative account in addition to the root account. User role options include: • **Super User**: This user has full system administration rights and can add, modify, and delete settings and users. • **Operator**: This user can perform system operations such as a system reset but cannot change the configuration or add or modify users. • **Read only**: This user can only access the system and view the configuration. • **Disabled**: This user cannot access the system.

- Select either **Time Server** or **Manual**. Table 7 on page 72 lists the system time options.

Table 7: System Time Options

Field	Description
Time Server	
Host Name	Type the hostname of the time server. For example: **ntp.example.com**.
IP	Type the IP address of the time server in the IP address entry field. For example: **192.0.2.254**.
NOTE: You can enter either the hostname or the IP address.	

Table 7: System Time Options *(Continued)*

Field	Description
Manual	
Date	Click the current date in the calendar.
Time	Set the hour, minute, and seconds. Choose **AM** or **PM**.
Time Zone (mandatory)	
Time Zone	Select the time zone from the list. For example: GMT Greenwich Mean Time GMT.

- Expert

  a. Select **Expert** to configure the basic options as well as the following advanced options:

  - Four or more internal zones
  - Internal zone services
  - Application of security policies between internal zones

  b. Click the **Need Help** icon for detailed configuration information.

  You see a success message after the basic configuration is complete.

Apply the Configuration

To apply the configuration settings for vSRX:

1. Review and ensure that the configuration settings are correct, and click **Next**. The Commit Configuration page appears.
2. Click **Apply Settings** to apply the configuration changes to vSRX.
3. Check the connectivity to the vSRX instance because you might lose connectivity if you have changed the management zone IP. Click the URL for reconnection instructions on how to reconnect to the instance.
4. Click **Done** to complete the setup.

After successful completion of the setup, you are redirected to the J-Web interface.

> **CAUTION**: After you complete the initial setup, you can relaunch the J-Web Setup wizard by clicking **Configuration>Setup**. You can either edit an existing configuration or create a new configuration. If you create a new configuration, the current configuration in vSRX will be deleted.

Add vSRX Feature Licenses

Certain Junos OS software features require a license to activate the feature. To enable a licensed feature, you need to purchase, install, manage, and verify a license key that corresponds to each licensed feature. To conform to software feature licensing requirements, you must purchase one license per feature per instance. The presence of the appropriate software unlocking key on your virtual instance allows you to configure and use the licensed feature.

To understand more about vSRX Licenses, see, Licenses for vSRX. Please refer to the Licensing Guide for general information about License Management. Please refer to the product Data Sheets for further details, or contact your Juniper Account Team or Juniper Partner.

Managing Security Policies for Virtual Machines Using Junos Space Security Director

SUMMARY

This topic provides you an overview of how you can manage security policies for VMs using security director.

Security Director is a Junos Space management application designed to enable quick, consistent, and accurate creation, maintenance, and application of network security policies for your security devices, including vSRX instances. With Security Director, you can configure security-related policy management including IPsec VPNs, firewall policies, NAT policies, IPS policies, and UTM policies. and push the configurations to your security devices. These configurations use objects such as addresses, services,

NAT pools, application signatures, policy profiles, VPN profiles, template definitions, and templates. These objects can be shared across multiple security configurations; shared objects can be created and used across many security policies and devices. You can create these objects prior to creating security configurations.

When you finish creating and verifying your security configurations from Security Director, you can publish these configurations and keep them ready to be pushed to all security devices, including vSRX instances, from a single interface.

The Configure tab is the workspace where all of the security configuration happens. You can configure firewall, IPS, NAT, and UTM policies; assign policies to devices; create and apply policy schedules; create and manage VPNs; and create and manage all the shared objects needed for managing your network security.

RELATED DOCUMENTATION

- Security Director

Software Receive Side Scaling

IN THIS SECTION

Overview

Contemporary NICs support multiple receive and transmit descriptor queues (multi-queue). On reception, a NIC can send different packets to different queues to distribute processing among CPUs. The NIC distributes packets by applying a filter to each packet that assigns it to one of a small number of logical flows. Packets for each flow are steered to a separate receive queue, which in turn can be processed by separate CPUs. This mechanism is generally known as Receive-side Scaling (RSS). The goal of RSS technique is to increase performance uniformly. RSS is enabled when latency is a concern or whenever receive interrupt processing forms a bottleneck. Spreading load between CPUs decreases queue length. For low latency networking, the optimal setting is to allocate as many queues as there are

CPUs in the system (or the NIC maximum, if lower). The most efficient high-rate configuration is likely the one with the smallest number of receive queues where no receive queue overflows due to a saturated CPU. You can improve bridging throughput with Receive Side Scaling.

As per flow thread affinity architecture each flow thread (FLT) polls for packet from dedicated receiving queue of NIC and process the packets until run to completion. Therefore, flow threads are bound to NIC receiving (RX) and transmitting (TX) queues for packet processing to avoid any disagreement. Hence, NIC must have same number of RX and TX queues as number of vSRX data plane CPU to support multi core vSRX flavors. Software RSS (SWRSS) removes this limitation of NIC HW queues to run vSRX multi-core flavors by implementing software-based packet spraying across various FLT thread.

Software RSS offloads the handling of individual flows to one of the multiple kernel, so the flow thread that takes the packets from the NIC can process more packets. Similar to RSS, network throughput improvement when using SWRSS has a linear correlation with CPU utilization.

In SWRSS, each NIC port is initialized with equal or lesser number of hardware RX/TX queues as that of I/O threads. I/O threads are determined based on total data-path CPU and minimum of NIC queues among all the NIC interface in vSRX. For example, if I/O thread is computed as 4, then number of HW queue per NIC port can be less or equal to 4 queues.

If NICs do not have sufficient number of queues as FLT threads in vSRX instances supported, then Software RSS (SWRSS) is enabled by flowd data-path. SWRSS implements software model of packet distribution across FLTs after obtaining the packets from NIC receiving queues. By removing NIC HW queue limitation, SWRSS helps to scale vCPUs by supporting various vSRX instance types.

During the I/O operation the packets are fetched from receiving queues of NIC ports and packet classification is performed. Followed by distribution of packets to FLT threads virtual queues. These virtual queues are implemented over DPDK ring queue. In the transmission path, SWRSS fetches the packets from virtual transmitting queues of FLT threads and pushes these packets to NIC transmitting queues for transmit.

Number of SWRSS I/O threads are selected based on total CPU and number of NIC queues found in vSRX instances. Mix mode of operation with HWRSS and and SWRSS is not supported.

Understanding Software Receive Side Scaling Configuration

This topic provide you details on types of Software Receive Side Scaling (SWRSS) and its configuration.

SWRSS supports two modes of operation and it gets enabled based on number of data-path CPU needed. These modes are Shared IO mode and dedicated IO mode. These modes are enabled based on number of data-path CPUs needed. vSRX and vSRX3.0 supports dedicated I/O mode only.

In dedicated I/O mode flowd process creates dedicated I/O threads for I/O operation. Based on number of required I/O threads for vSRX, I/O thread is associated to a dedicated NIC port. NIC ports receiving

and transmitting queue is then bonded to each I/O thread in round robin method for uniform distribution and to avoid I/O thread locks. Each dedicated I/O thread pulls the packets in burst mode from NIC receiving queue and distributes to FLT threads and vice versa for TX path for packet transmit.

SWRSS is enabled based on the number of vCPUs. If NIC does not have sufficient number of queues as flow thread (FLT) in vSRX with different vCPUs, then Software RSS (SWRSS) is enabled by flowd process.

SWRSS is not enabled in the following scenarios:

- When the NIC has sufficient number of hardware RX or TX queues for required PFE data-path CPU.
- When the vSRX (based on number of vCPUs) and NIC result the smaller number of FLT CPUs as that obtained in nearest hardware RSS (HWRSS) mode. In such scenario, vSRX will be enabled with HWRSS mode which results more FLT CPU than SWRSS mode, providing better packet processing throughput.
- SWRSS is not recommended for vSRX with certain type of NIC that supports lesser number of NIC queues than needed to run dedicated IO thread. In such cases, SWRSS is enabled but extra CPUs are attached to FLT CPU, until I/O CPUs are completely utilized.

If SWRSS is not enabled use the **set security forwarding-options receive-side-scaling software-rss mode enable** command to enable SWRSS. When you run this command SWRSS will be enabled by force regardless of the NIC RSS or the number of vCPUs. If you do not enable SWRSS using the CLI then enabling of SWRSS automatically is decided based on the default ratio of FLT: IO (4:1).

To configure the number of required IO threads, use the **set security forwarding-options receive-side-scaling software-rss io-thread-number** ***<1-8>*** command. To view the actual number of vCPUs assigned to IO flow threads use the **show security forwarding-options resource-manager** command.

You can decide enabling of SWRSS automatically or by force based on the architecture and conception of IO thread and worker thread. Enabling SWRSS impacts the performance, so we recommend that the number of IO thread should be changed only if required and until the performance impact bottleneck point is reached.

GTP Traffic with TEID Distribution and SWRSS

IN THIS SECTION

Overview GTP Traffic Distribution with TEID Distribution and SWRSS

IN THIS SECTION

The topic provides an overview of asymmetric fat tunnel solution for GTP traffic with TEID distribution and SWRSS.

With TEID-based hash distributions feature, the GTP packets would be distributed to the flow thread according to the hash value calculated by TEID. The algorithm of hash calculation is same as GTP distribution in flow module, which ensures the GTP packets would not be reinjected again in the flow process.

There is a 4-byte field inside GTP payload called tunnel endpoint identifier (TEID), which is used to identify different connections in the same GTP tunnel.

A fat GTP tunnel carries data from different users. IPsec tunnels on the security gateway could be a fat tunnel due to the fat GTP tunnel. vSRX can create one GTP session with a high-bandwidth of GTP traffic. However, the throughput is limited to one core processor's performance.

If you use TEID-based hash distribution for creating GTP-U sessions, then you can:

- Enable vSRX and vSRX 3.0 instances to process asymmetric fat tunnels for parallel encryption on multiple cores for one tunnel.
- You can split a fat GTP session to multiple sessions and distribute them to different cores. This helps to increase the bandwidth for fat GTP tunnel.

The TEID based hash distribution creates GTP-U sessions to multiple cores. The clear text traffic acts as a fat GTP tunnel. This helps a fat GTP session to split into multiple slim GTP sessions and handle them on multiple cores simultaneously.

GTP Traffic Performance with TEID Distribution and SWRSS

vSRX instances support Software Receive Side Scaling (SWRSS) feature. SWRSS is a technique in the networking stack to increase parallelism and improve performance for multi-processor systems. If NICs do not have sufficient number of queues as flow thread (FLT), based on vSRX type, then Software RSS (SWRSS) is enabled by flowd process.

With Software Receive Side Scaling (SWRSS) support on vSRX and vSRX 3.0, you can assign more vCPUs to the vSRX regardless of the limitation of RSS queue of underlying interfaces.

Based on SWRSS you can improve the GTP traffic performance using Tunnel endpoint identifier (TEID) distribution and asymmetric fat tunnel solution by:

- Assigning specific number of vCPUs for input output flow usage—With SWRSS enabled, you can assign more vCPUs for input/output (IO) threads when the IO threads are less. Or you can assign less vCPUs for IO threads if the flow process is consuming more vCPU. Use the **set security forwarding-options receive-side-scaling software-rss io-thread-number <io-thread-number>**.

- Distributing the packets to flow threads according to the TEID inside the packet, which would avoid reinjecting the packets in flow process—This feature is enabled when both SWRSS is enabled and when you configure the **set security forwarding-process application-services enable-gtpu-distribution** command.

  With this feature, the GTP packets would be distributed to the flow thread according to the hash value calculated by TEID. The algorithm of hash calculation is same as GTP distribution in flow module, which ensures the GTP packets would not be reinjected again in flow process.

- Utilizing fragment matching and forwarding mechanism in input/output thread when GTPU distribution is enabled—This mechanism ensures that all the fragments of the same packet would be distributed to one flow thread according to the TEID.

  SWRSS uses IP pair hash to distribute packets to flow threads. For GTP traffic with GTPU distribution enabled, TEID distribution is used to distribute packets to the flow threads. For fragmented packets, TEID cannot be retrieved from non-first fragments. This will require fragment matching and forwarding logic to ensure all fragments are forwarded to the flow thread based on TEID.

Enabling GTP-U TEID Distribution with SWRSS for Asymmetric Fat Tunnels

The following configuration helps you enable PMI and GTP-U traffic distribution with SWRSS enabled.

Before you begin, understand:

- SWRSS concepts and configurations.
- How to establish PMI and GTP-U

With Software Recieve Side Scaling (SWRSS) enabled, you can assign more vCPUs for input/output (IO) threads when the IO threads are less. Or you can assign less vCPUs for IO threads if the flow process is consuming more vCPU. You can configure the number of IO threads required. With SWRSS is enabled and IO threads configured, reboot the vSRX for configuration to take effect. After IO threads are configured, distribute the GTP traffic to the configured IO threads according to TEID-based hash distribution for splitting a fat GTP session to multiple slim GTP sessions and process them on multiple cores in parallel.

NOTE: When PMI mode is enabled with TEID distribution and SWRSS support, performance of PMI is improved. If you want to enable PMI mode then run the **set securtiy flow power-mode-ipsec** command.

The following steps provide you details on how to enable SWRSS, configure IO threads, enable PMI mode for GTP sessions with TEID distribution for obtaining asymmetric fat tunnels:

1. SWRSS is enabled by default when NICs do not have sufficient number of queues as flow thread (FLT) based on vSRX type, then Software RSS (SWRSS) is enabled by flowd process. But, when SWRSS is not enabled use the following CLIs to enable. When you run this command SWRSS will be be enabled by force regardless of the NIC RSS or number of vCPUs.

   Enable SWRSS.

   ```
   [edit]
   user@host# set security forwarding-options receive-side-scaling software-rss mode enable
   ```

2. Configure the number of IO threads required. In this configuration we are configuring eight IO threads. The assigned number of vCPUs would be assigned for IO threads, and the rest vCPUs would be assigned for flow thread.

   ```
   [edit]
   user@host# set security forwarding-options receive-side-scaling software-rss io-thread-number 8
   ```

3.

   ```
   [edit security]
   user@host# set flow power-mode-ipsec
   ```

4. Configure GTP-U session distribution.

```
[edit security]
user@host# set forwarding-process application-services enable-gtpu-distribution
```

5. From the configuration mode, confirm your configuration by entering the **show** command.

```
[edit security]
user@host# show
forwarding-options {
    receive-side-scaling {
        software-rss {
             mode enable;
        io-thread-number 8;
flow {
    power-mode-ipsec;
}
forwarding-process {
    application-services {
        enable-gtpu-distribution;
    }
}
```

From the operational mode run the following command to view the actual number of vCPUs assigned to IO/flow threads.

```
show security forward-options resource-manager settings
```

```
------------------------------------------------------------------------
Owner         Type                     Current settings      Next settings
SWRSS-IO      CPU core number          2                     2
SWRSS         SWRSS mode               Enable                Enable
```

6. Commit the configuration.

```
[edit security]
user@host# commit
```

7. Reboot the vSRX for the configuration to take effect. After rebooting the whole device, PFE would check the IO-thread value according to the NIC RSS queue and its memory.

CHAPTER 4

vSRX in Nutanix Use Cases

Example: Configuring NAT for vSRX

IN THIS SECTION

This example shows how to configure vSRX to NAT all hosts behind the vSRX instance in the Nutanix virtual private cloud (VPC) to the IP address of the vSRX egress interface on the untrust zone. This configuration allows hosts behind vSRX in a cloud network to access the Internet.

Before You Begin

Ensure that you have installed and launched a vSRX instance in a Nutanix VPC.

Overview

A common cloud configuration includes hosts that you want to grant access to the Internet, but you do not want anyone from outside your cloud to get access to your hosts. You can use vSRX in a Nutanix VPC to NAT traffic inside the Nutanix VPC from the public Internet.

Configuring NAT

IN THIS SECTION

Procedure

Step-by-Step Procedure

To configure NAT on the vSRX instance:

1. Log in to the vSRX console in configuration edit mode.
2. Set the IP addresses for vSRX revenue interfaces.

```
set interfaces ge-0/0/0 unit 0 family inet address 10.0.10.197/24
set interfaces ge-0/0/1 unit 0 family inet address 10.0.20.1/24
```

3. Set up the untrust security zone.

```
set security zones security-zone untrust host-inbound-traffic system-services https
set security zones security-zone untrust host-inbound-traffic system-services ssh
set security zones security-zone untrust interfaces ge-0/0/0.0
```

4. Set up the trust security zone.

```
set security zones security-zone trust host-inbound-traffic system-services https
set security zones security-zone trust host-inbound-traffic system-services ssh
set security zones security-zone trust host-inbound-traffic system-services ping
set security zones security-zone trust interfaces ge-0/0/1.0
```

5. Set up the security policies.

```
set security policies from-zone trust to-zone untrust policy test match source-address any
set security policies from-zone trust to-zone untrust policy test match destination-address any
set security policies from-zone trust to-zone untrust policy test match application any
set security policies from-zone trust to-zone untrust policy test then permit
```

6. Configure NAT.

```
set security nat source rule-set SNAT_RuleSet from zone trust
set security nat source rule-set SNAT_RuleSet to zone untrust
set security nat source rule-set SNAT_RuleSet rule SNAT_Rule match source-address 0.0.0.0/0
```

```
set security nat source rule-set SNAT_RuleSet rule SNAT_Rule then source-nat interface
commit
```

5

CHAPTER

Monitoring and Troubleshooting

Monitoring

IN THIS SECTION

This topic provides details on how you can monitor your vSRX instances using SNMP.

Monitoring helps in maintaining the reliability, availability, and performance of your vSRX instances and your Nutanix solutions. You should collect monitoring data from all your Nutanix solutions so that you can easily debug any multi-point failure.

Monitoring vSRX Instances Using SNMP

You can monitor your vSRX instance details such as health and storage at instance level, using SNMP monitoring.

For details on SNMP monitoring, refer the SNMP MIB information in the MIB Explorer at: https://apps.juniper.net/mib-explorer/.

You can also find all the applicable SNMP OIDs from the Juniper MIB from the vSRX CLI, using the **show snmp mib walk 1.3.6.1.4.1.2636** command.

Some examples of useful OID's for monitoring system health are:

```
jnxOperatingCPU.1.1.0.0
jnxOperating5MinAvgCPU.1.1.0.0
jnxFwddMicroKernelCPUUsage.0
jnxFwddRtThreadsCPUUsage.0
jnxHrStoragePercentUsed.1
jnxJsNodeCurrentTotalSession.0
jnxJsNodeMaxTotalSession.0
jnxJsNodeSessionCreationPerSecond.0
```

NOTE: For monitoring storage capacity on the vSRX instance you can use SNMP monitoring. Using SNMP monitoring, you can be notified for any vSRX instance storage that is impacted. The storage related OID indicates the storage percentage, which is used to detect the storage capacity.

For best practices for enabling SNMP monitoring in Junos, see https://www.juniper.net/documentation/en_US/junos/topics/ task/configuration/snmp-best-practices-basic-config.html.

Troubleshooting

IN THIS SECTION

This topic provides details on how you can troubleshoot your vSRX instances.

Chassis Cluster

- **Ping Issue**—When ping does not work over ge or reth interfaces after the vSRX is brought up in a chassis cluster . The default NIC type is kNormal . You need to change the NIC type as kDirectNic to make it work in chassis cluster environment. Use the command **vm.nic_update R-vSRX3 50:6b:8d:7b:19:89 type=kDirectNic** to change the NIC type.

Deployment

- **Hypervisor Detection**—When vSRX detects AHV as Hyper-V, run the **CMD: acli vm.update <VM_name>disable_branding=true** command and **CMD: acli**

vm.update<VM_name>extra_flags=enable_hyperv_clock=0 command for vSRX to detect the hypervisor as KVM.

Backup and Recovery

This topic provides details on how you can backup and recover your configuration files in case of instance or service failure, both externally within Nutanix and locally on your vSRX instance console

To save the vSRX configuration file locally, perform the following steps:

1. Log into the vSRX instance and go to the configuration mode.
2. Execute the command **save /var/tmp/ *<file-name>***

   The current vSRX configurations are et saved in the above mentioned path.
3. Using your Secure Copy Protocol (SCP) client, download the saved configuration files to your local system.

For backup and recovery of configuration files within Nutanix:

NOTE: You must have an FTP server that is accessible from the vSRX instance.

1. Run the below configuration.

```
External example  system {
      archival {
        configuration {
            transfer-on-commit;
            archive-sites {
                "ftp://username:password@192.168.1.10";
                }
            }
      }
}
```

2. You can then run and commit the following configuration command on the vSRX instance.

```
set system archival configuration transfer-on-commit archive-sites ftp://
username:password@<FTP_Server_IP_Address> .
```

Finding the Software Serial Number for vSRX

You need the software serial number to open a support case or to renew a vSRX license.

The serial number is a unique 14-digit number that Juniper Networks uses to identify your particular software installation. You can find the software serial number in the Software Serial Number Certificate attached to the e-mail that was sent when you ordered your Juniper Networks software or license. You can also use the show system license command to find the software serial number.

Use the **show system license** command to find the vSRX software serial number.

```
vsrx> show system license
```

```
License usage:
                                Licenses     Licenses    Licenses    Expiry
  Feature name                       used    installed      needed
  Virtual Appliance                     1            1           0    58 days

Licenses installed:
  License identifier: E420588955
  License version: 4
  Software Serial Number: 20150625
  Customer ID: vSRX-JuniperEval
  Features:
    Virtual Appliance - Virtual Appliance
      count-down, Original validity: 60 days

  License identifier: JUNOS657051
  License version: 4
  Software Serial Number: 9XXXXAXXXXXXX9
  Customer ID: MyCompany
  Features:
```

```
    Virtual Appliance - Virtual Appliance
      permanent
```

For more information, see Licenses for vSRX