CONFIGURATION GUIDE

Ruckus SmartZone Data Plane (vSZ-D/SZ100-D) Configuration Guide, 5.1.1

SmartZone Supporting 5.1.1

Part Number: 800-72209-001 Rev A
Publication Date: April 2019

Copyright, Trademark and Proprietary Rights Information

Export Restrictions

These products and associated technical data (in print or electronic form) may be subject to export control laws of the United States of America. It is your responsibility to determine the applicable regulations and to comply with them. The following notice is applicable for all products or technology subject to export control:

These items are controlled by the U.S. Government and authorized for export only to the country of ultimate destination for use by the ultimate consignee or end-user(s) herein identified. They may not be resold, transferred, or otherwise disposed of, to any other country or to any person other than the authorized ultimate consignee or end-user(s), either in their original form or after being incorporated into other items, without first obtaining approval from the U.S. government or as otherwise authorized by U.S. law and regulations.

Disclaimer

THIS CONTENT AND ASSOCIATED PRODUCTS OR SERVICES ("MATERIALS"), ARE PROVIDED "AS IS" AND WITHOUT WARRANTIES OF ANY KIND, WHETHER EXPRESS OR IMPLIED. TO THE FULLEST EXTENT PERMISSIBLE PURSUANT TO APPLICABLE LAW, ARRIS DISCLAIMS ALL WARRANTIES, EXPRESS OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE, TITLE, NON-INFRINGEMENT, FREEDOM FROM COMPUTER VIRUS, AND WARRANTIES ARISING FROM COURSE OF DEALING OR COURSE OF PERFORMANCE. ARRIS does not represent or warrant that the functions described or contained in the Materials will be uninterrupted or error-free, that defects will be corrected, or are free of viruses or other harmful components. ARRIS does not make any warranties or representations regarding the use of the Materials in terms of their completeness, correctness, accuracy, adequacy, usefulness, timeliness, reliability or otherwise. As a condition of your use of the Materials, you warrant to ARRIS that you will not make use thereof for any purpose that is unlawful or prohibited by their associated terms of use.

Limitation of Liability

IN NO EVENT SHALL ARRIS, ARRIS AFFILIATES, OR THEIR OFFICERS, DIRECTORS, EMPLOYEES, AGENTS, SUPPLIERS, LICENSORS AND THIRD PARTY PARTNERS, BE LIABLE FOR ANY DIRECT, INDIRECT, SPECIAL, PUNITIVE, INCIDENTAL, EXEMPLARY OR CONSEQUENTIAL DAMAGES, OR ANY DAMAGES WHATSOEVER, EVEN IF ARRIS HAS BEEN PREVIOUSLY ADVISED OF THE POSSIBILITY OF SUCH DAMAGES, WHETHER IN AN ACTION UNDER CONTRACT, TORT, OR ANY OTHER THEORY ARISING FROM YOUR ACCESS TO, OR USE OF, THE MATERIALS. Because some jurisdictions do not allow limitations on how long an implied warranty lasts, or the exclusion or limitation of liability for consequential or incidental damages, some of the above limitations may not apply to you.

Trademarks

ARRIS, the ARRIS logo, Ruckus, Ruckus Wireless, Ruckus Networks, Ruckus logo, the Big Dog design, BeamFlex, ChannelFly, EdgeIron, FastIron, HyperEdge, ICX, IronPoint, OPENG, SmartCell, Unleashed, Xclaim, ZoneFlex are trademarks of ARRIS International plc and/or its affiliates. Wi-Fi Alliance, Wi-Fi, the Wi-Fi logo, the Wi-Fi CERTIFIED logo, Wi-Fi Protected Access (WPA), the Wi-Fi Protected Setup logo, and WMM are registered trademarks of Wi-Fi Alliance. Wi-Fi Protected Setup™, Wi-Fi Multimedia™, and WPA2™ are trademarks of Wi-Fi Alliance. All other trademarks are the property of their respective owners.

Contents

Preface

Document Conventions

The following table lists the text conventions that are used throughout this guide.

TABLE 1 Text Conventions

Convention	Description	Example
`monospace`	Identifies command syntax examples	`device(config)# interface ethernet 1/1/6`
bold	User interface (UI) components such as screen or page names, keyboard keys, software buttons, and field names	On the **Start** menu, click **All Programs**.
italics	Publication titles	Refer to the *Ruckus Small Cell Release Notes* for more information.

Notes, Cautions, and Warnings

Notes, cautions, and warning statements may be used in this document. They are listed in the order of increasing severity of potential hazards.

NOTE
A NOTE provides a tip, guidance, or advice, emphasizes important information, or provides a reference to related information.

ATTENTION
An ATTENTION statement indicates some information that you must read before continuing with the current action or task.

CAUTION
A CAUTION statement alerts you to situations that can be potentially hazardous to you or cause damage to hardware, firmware, software, or data.

DANGER
A DANGER statement indicates conditions or situations that can be potentially lethal or extremely hazardous to you. Safety labels are also attached directly to products to warn of these conditions or situations.

Command Syntax Conventions

Bold and italic text identify command syntax components. Delimiters and operators define groupings of parameters and their logical relationships.

Convention	Description
bold text	Identifies command names, keywords, and command options.
italic text	Identifies a variable.
[ ]	Syntax components displayed within square brackets are optional. Default responses to system prompts are enclosed in square brackets.
{ **x** | **y** | **z** }	A choice of required parameters is enclosed in curly brackets separated by vertical bars. You must select one of the options.
x | **y**	A vertical bar separates mutually exclusive elements.
< >	Nonprinting characters, for example, passwords, are enclosed in angle brackets.
...	Repeat the previous element, for example, *member*[*member*...].
\	Indicates a “soft” line break in command examples. If a backslash separates two lines of a command input, enter the entire command at the prompt without the backslash.

Document Feedback

Ruckus is interested in improving its documentation and welcomes your comments and suggestions.

You can email your comments to Ruckus at ruckus-docs@arris.com.

When contacting us, include the following information:

- Document title and release number
- Document part number (on the cover page)
- Page number (if appropriate)

For example:

- Ruckus SmartZone Upgrade Guide, Release 5.0
- Part number: 800-71850-001 Rev A
- Page 7

Ruckus Product Documentation Resources

Visit the Ruckus website to locate related documentation for your product and additional Ruckus resources.

Release Notes and other user documentation are available at https://support.ruckuswireless.com/documents. You can locate the documentation by product or perform a text search. Access to Release Notes requires an active support contract and a Ruckus Support Portal user account. Other technical documentation content is available without logging in to the Ruckus Support Portal.

White papers, data sheets, and other product documentation are available at https://www.ruckuswireless.com.

Online Training Resources

To access a variety of online Ruckus training modules, including free introductory courses to wireless networking essentials, site surveys, and Ruckus products, visit the Ruckus Training Portal at https://training.ruckuswireless.com.

Contacting Ruckus Customer Services and Support

The Customer Services and Support (CSS) organization is available to provide assistance to customers with active warranties on their Ruckus products, and customers and partners with active support contracts.

For product support information and details on contacting the Support Team, go directly to the Ruckus Support Portal using https://support.ruckuswireless.com, or go to https://www.ruckuswireless.com and select **Support**.

What Support Do I Need?

Technical issues are usually described in terms of priority (or severity). To determine if you need to call and open a case or access the self-service resources, use the following criteria:

- Priority 1 (P1)—Critical. Network or service is down and business is impacted. No known workaround. Go to the **Open a Case** section.
- Priority 2 (P2)—High. Network or service is impacted, but not down. Business impact may be high. Workaround may be available. Go to the **Open a Case** section.
- Priority 3 (P3)—Medium. Network or service is moderately impacted, but most business remains functional. Go to the **Self-Service Resources** section.
- Priority 4 (P4)—Low. Requests for information, product documentation, or product enhancements. Go to the **Self-Service Resources** section.

Open a Case

When your entire network is down (P1), or severely impacted (P2), call the appropriate telephone number listed below to get help:

- Continental United States: 1-855-782-5871
- Canada: 1-855-782-5871
- Europe, Middle East, Africa, Central and South America, and Asia Pacific, toll-free numbers are available at https://support.ruckuswireless.com/contact-us and Live Chat is also available.
- Worldwide toll number for our support organization. Phone charges will apply: +1-650-265-0903

We suggest that you keep a physical note of the appropriate support number in case you have an entire network outage.

Self-Service Resources

The Ruckus Support Portal at https://support.ruckuswireless.com offers a number of tools to help you to research and resolve problems with your Ruckus products, including:

- Technical Documentation—https://support.ruckuswireless.com/documents

- Community Forums—https://forums.ruckuswireless.com/ruckuswireless/categories
- Knowledge Base Articles—https://support.ruckuswireless.com/answers
- Software Downloads and Release Notes—https://support.ruckuswireless.com/#products_grid
- Security Bulletins—https://support.ruckuswireless.com/security

Using these resources will help you to resolve some issues, and will provide TAC with additional data from your troubleshooting analysis if you still require assistance through a support case or RMA. If you still require help, open and manage your case at https://support.ruckuswireless.com/case_management.

About This Guide

About this Guide

This document describes the features and configuration required for setting up the Ruckus SmartZone 100 Data Plane (SZ100-D) and Ruckus Virtual SmartZone Data Plane (vSZ-D) on the network.

This guide is written for service operators and system administrators who are responsible for managing, configuring, and troubleshooting Ruckus devices. Consequently, it assumes a basic working knowledge of local area networks, wireless networking, and wireless devices.

NOTE
If release notes are shipped with your product and the information there differs from the information in this guide, follow the instructions in the release notes.

Most user guides and release notes are available in Adobe Acrobat Reader Portable Document Format (PDF) or HTML on the Ruckus Support Web site at https://support.ruckuswireless.com/contact-us.

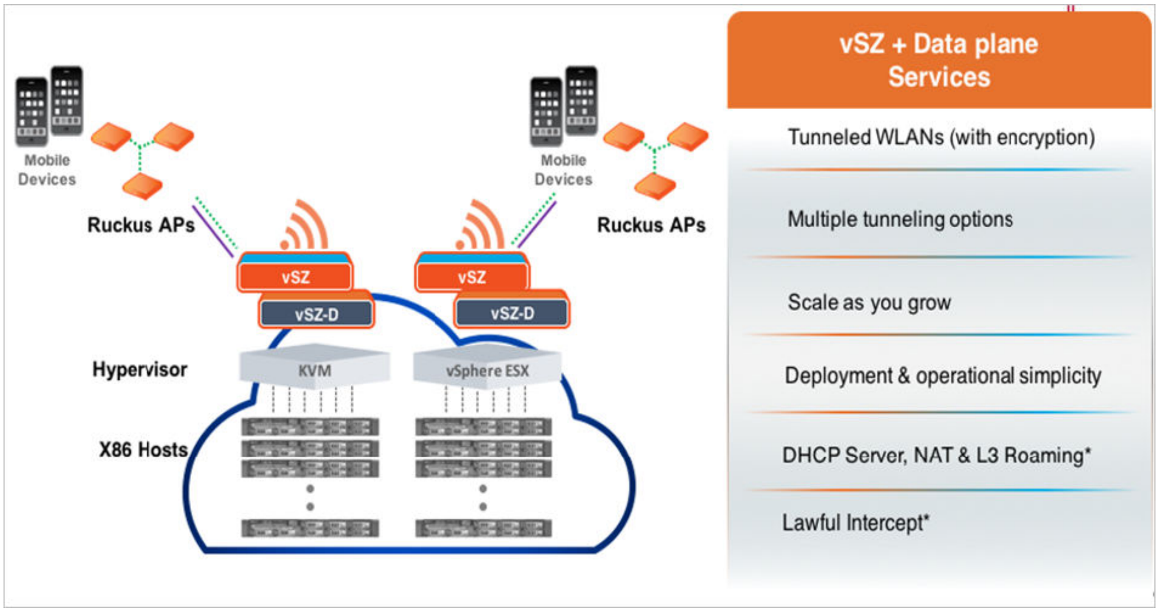
SmartZone Data Plane Features

Virtual SmartZone Data Plane and SmartZone 100 Data Plane Overview

The Ruckus Virtual SmartZone controller platform is the industry's most scalable Wi-Fi controller platform that enables service providers and enterprises to leverage virtualization technologies to deploy superior Wi-Fi management systems.

With the introduction of the Virtual Data Plane (vSZ-D) in SZ 3.2 release and SZ100-D in 5.1, the SmartZone platform launched sophisticated data plane capabilities. This is truly differentiated and distinguished offering that provides compelling business benefits for varied deployment scenarios.

FIGURE 1 vSZ-D/SZ100-D Services


Mobile Devices
Ruckus APs
Mobile Devices
Ruckus APs
vSZ
vSZ-D
vSZ
vSZ-D
Hypervisor
KVM
vSphere ESX
X86 Hosts
vSZ + Data plane Services
Tunneled WLANs (with encryption)
Multiple tunneling options
Scale as you grow
Deployment & operational simplicity
DHCP Server, NAT & L3 Roaming*
Lawful Intercept*

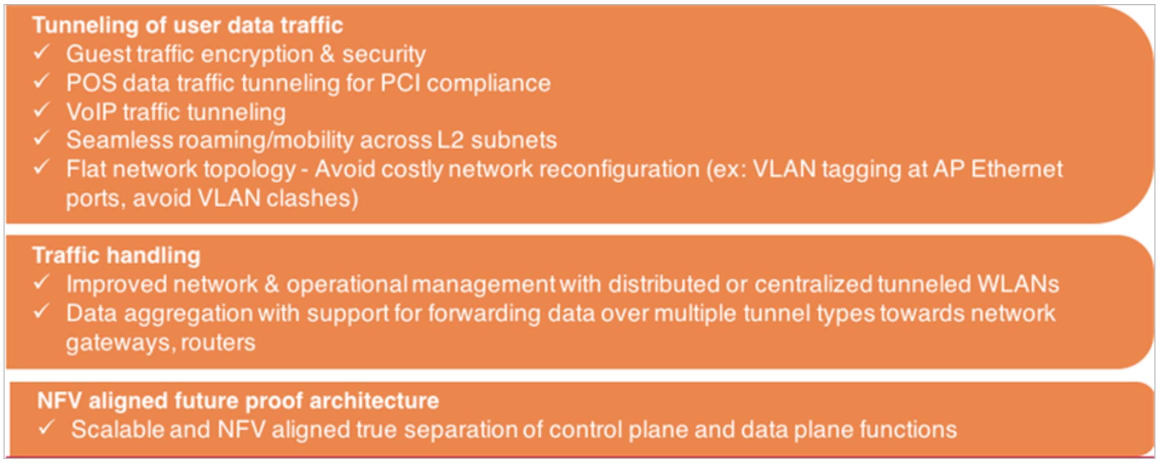
Features and Benefits

vSZ-D is a virtualized service to segregate and securely tunnel user data traffic.

NOTE
You can create a maximum of 2047 multicast groups on vSZ-D/SZ100-D.

Some of the key use cases for the vSZ-D/SZ100-D are:

FIGURE 2 Use cases



Tunneling of user data traffic

- ✓ Guest traffic encryption & security
- ✓ POS data traffic tunneling for PCI compliance
- ✓ VoIP traffic tunneling
- ✓ Seamless roaming/mobility across L2 subnets
- ✓ Flat network topology - Avoid costly network reconfiguration (ex: VLAN tagging at AP Ethernet ports, avoid VLAN clashes)

Traffic handling

- ✓ Improved network & operational management with distributed or centralized tunneled WLANs
- ✓ Data aggregation with support for forwarding data over multiple tunnel types towards network gateways, routers

NFV aligned future proof architecture

- ✓ Scalable and NFV aligned true separation of control plane and data plane functions

TABLE 2 Feature and Benefits

Feature	Benefit
Secure data plane tunneling	Manages the creation of aggregated user data streams through secure tunnel
Multiple Hypervisor Support	Supports the most widely deployed VMware and KVM hypervisors, applicable only to vSZ-D.
Dynamic data plane scaling	Supports 1Gbps, 10Gbps or even higher throughput capacities to support all types of enterprise and carrier deployments that can be dynamically tuned without needing software updates

TABLE 2 Feature and Benefits (continued)

Feature	Benefit
Seamless integration with vSZ controller	• Simple integration and management with vSZ controller clustering architecture enables support for multiple vSZ-D/SZ100-D instances • 10 vSZ-D/SZ100-D instances per vSZ instance • 40 vSZ-D/SZ100-D instances per vSZ cluster of 4 instances • The controller runs in Active/Active (3+1) mode for extremely high availability. • Each vSZ-D runs as an independent virtual machine instance that is managed by the controller. • With vSZ-D/SZ100-D Zone Affinity enabled, it is possible to support a distributed vSZ-D/SZ100-D instance on a per vSZ Zone basis.
Superior data plane functions	Encrypted tunnel aggregation from all types of WLANs (Captive portal, 802.1x, HS2.0), VLANs, DHCP Relay, DHCP Server, NAT, L3 Roaming, Lawful Intercept, IPv6 Support and NAT traversal between AP and vSZ-D/SZ100-D.
Scalable Deployment Architectures	Provides the ability to service distributed and centralized network configurations
Deployment and operational simplicity	Simple integration and management with vSZ-E and vSZ-H installations
Site level QoS and policy control	Service policy management and data stream (will be supported in a later release)

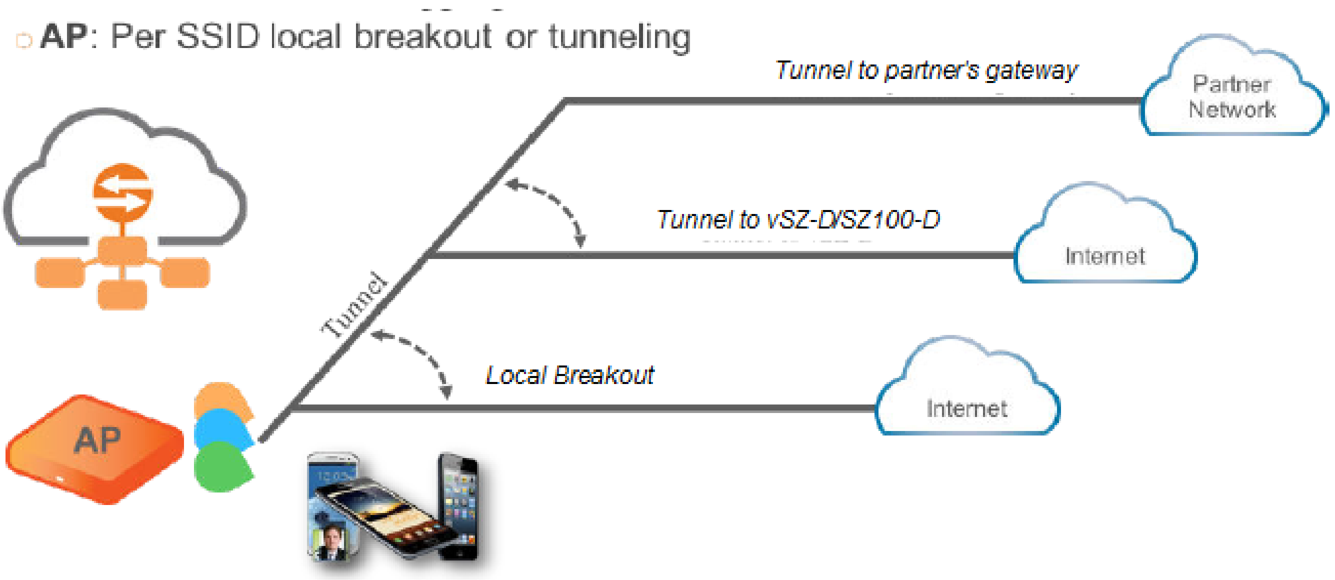
Tunneled WLANs and Flexible Traffic Redirection

Many WiFi deployments have requirements to support tunneled WLANs for guest isolation and encryption, POS data security, VoIP traffic management, and seamless roaming across L2 subnets. One of the most deployed and easily managed way to meet these requirements is to enable a flat network topology by tunneling traffic to a controller.

With the vSZ-D/SZ100-D , it is now possible to support tunneled WLANs on Ruckus APs that are managed by a vSZ controller. In addition, both the Ruckus APs and the vSZ-D/SZ100-D support encryption capabilities on tunnels for data protection. This is especially important when tunneling guest traffic and in use cases where the service provider or enterprise operator does not have control on the backhaul links.

FIGURE 3 Traffic redirection flexibility with the Virtual SmartZone platform

- **Controller or vSZ-D/SZ100-D:** Aggregate user data and tunneling
- **AP:** Per SSID local breakout of tunneling

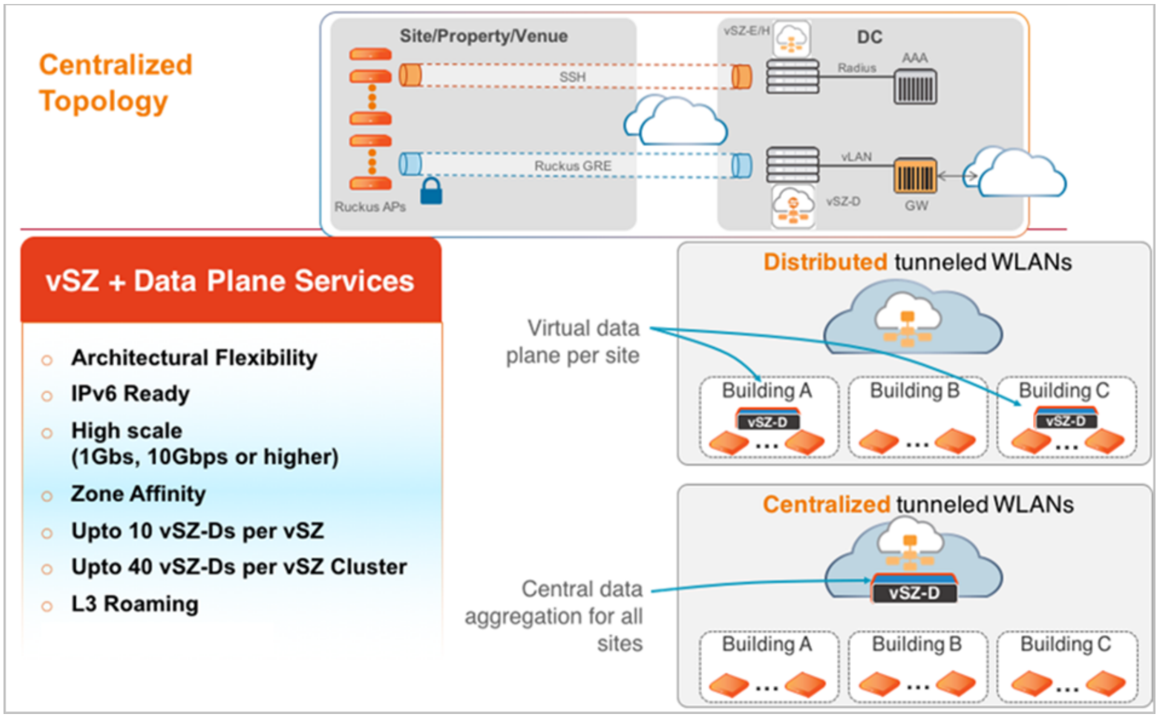


Architecture and Deployment Flexibility

Existing architectures for supporting tunneled WLANs involve tunneling data back into controllers. This results in architectures where a complete controller needs to be deployed on each site or all the tunneled WLAN traffic being backhauled into a centralized data center. This also results in dependencies on choices for controller platforms with different capacity profiles, which increase the capital and operating expenses of the entire solution without actually solving the real problem.

With the vSZ-D/SZ100-D , it is now possible to deploy the same software either on-premise (on cheaper COTS hardware) when needed, as well as deploy it at the data center (on higher end COTS hardware) and the entire Wi-Fi management controller by the vSZ controller.

FIGURE 4 Unmatched architecture flexibility


Centralized Topology
Site/Property/Venue
SSH
Ruckus GRE
Ruckus APs
vSZ-E/H
DC
Radius
AAA
vLAN
vSZ-D
GW
vSZ + Data Plane Services
Architectural Flexibility
IPv6 Ready
High scale (1Gbs, 10Gbps or higher)
Zone Affinity
Upto 10 vSZ-Ds per vSZ
Upto 40 vSZ-Ds per vSZ Cluster
L3 Roaming
Virtual data plane per site
Distributed tunneled WLANs
Building A
Building B
Building C
vSZ-D
Central data aggregation for all sites
Centralized tunneled WLANs
vSZ-D
Building A
Building B
Building C

IPv6 Address Support

The vSZ-D/SZ100-D supports IPv6 addresses for the data plane interface. The vSZ-D/SZ100-D also supports client IPv6 addresses for DHCP Relay only.

> **NOTE**
> vSZ-D/SZ100-D does not support IPv6 addresses for northbound soft-GRE tunnels.

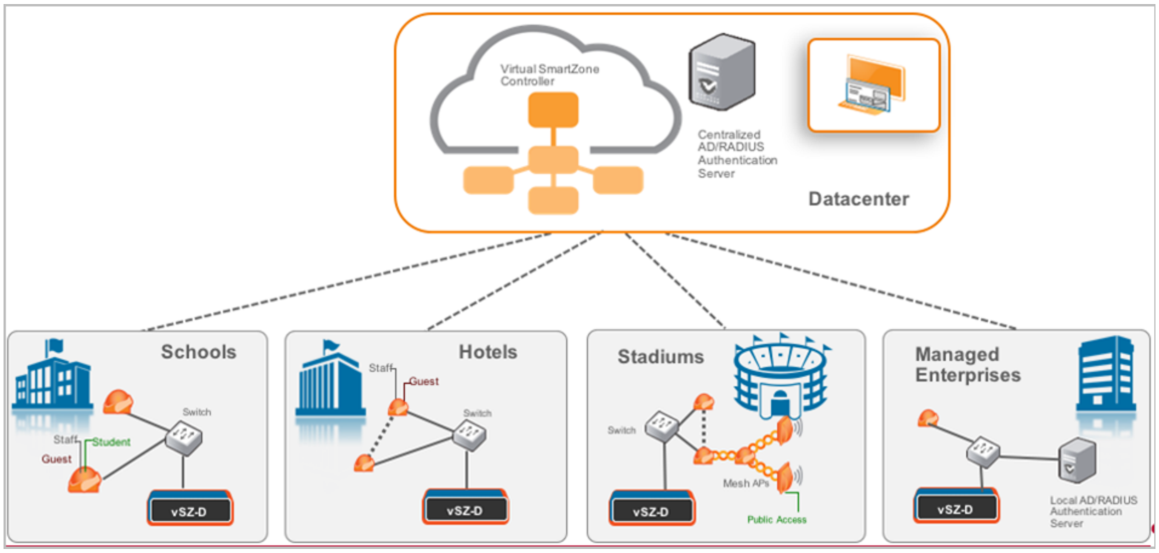
vSZ-D/SZ100-D Zone Affinity

vSZ-D/SZ100-D Zone Affinity is a new feature introduced in this release. It is now possible to dedicate vSZ-D/SZ100-D instance on a per distributed site basis.

This is especially useful for managed service providers and ISPs who manage remote distributed sites through a central or regional data center. In this architecture, the vSZ is in the provider's data center managing APs across all remote distributed sites.

On sites where there is a need for tunneling, they can introduce the vSZ-D/SZ100-D and bind them to that particular site so that all APs on that site shall tunnel traffic locally to the vSZ-D/SZ100-D on that site.

FIGURE 5 vSZ-D/SZ100-D Zone Affinity



DHCP Server and NAT Service on vSZ-D/SZ100-D

Highly scalable and optimized DHCP Server on vSZ-D/SZ100-D is designed from the ground up for WiFi networks. It also introduces NAT capability.

NOTE
DHCP Server/NAT function if enabled is supported only for wireless client IPv4 address assignment.

NOTE
DHCP Server and NAT service configuration is supported using AP and web user interface. Refer to Administrator Guide for configuring DHCP server and NAT service on the web interface.

DHCP Server

The DHCP Server is designed in-line in the data plane and provides extreme scale in terms of IP address assignment to clients. This feature is especially useful in high density and dynamic deployments like stadiums, train stations where large number of clients continuously move in & out of WiFi coverage. The DHCP server in the network needs to scale to meet these challenging requirements. The DHCP server on the vSZ-D/SZ100-D provides high scale IP assignment and management with minimal impact on forwarding latency. DHCP Server supports 64 pools with profile support.

NOTE
The DHCP service can scale for a maximum of 101K IP leases per data plane. You can incrementally add-on license on a per-group basis of two DPs.

NAT Service

With NAT service enabled, all the WiFi client traffic is NATed by vSZ-D/SZ100-D before being forwarded to the core network. Each vSZ-D/SZ100-D supports up to 16 public IP addresses for NAT. This feature essentially reduces the network overhead significantly since this reduces the MAC-table considerations on the UP-stream switches significantly. Again, very useful in high density deployments.

NOTE
Only single subnet is supported.

NOTE
The NAT service scales a maximum of 2 million sessions/ flows per Data Plane. You can incrementally add-on license on a per-Data Plane basis.

DHCP/NAT

DHCP/NAT functionality on SZ-managed APs and DPs (data planes) allows customers to reduce costs and complexity by removing the need for DHCP server/NAT router to provide IP addresses to clients. For data traffic aggregation and services delivery you can choose appropriate user profile for DHCP and NAT services on vSZ-D/SZ100-D.

AP-based DHCP/NAT

In highly distributed environments, particularly those with only a few APs per site, the ability for an AP or a set of APs to provide DHCP/NAT support to local client devices simplifies deployment by providing all-in-one functionality on the AP, which eliminates the need for a separate router and DHCP server for each site. It also eases site management by providing central control and monitoring of the distributed APs and their clients.

Three general DHCP scenarios are supported:

- SMB Single AP: DHCP is running on a single AP only. This AP also functions as the Gateway AP.
- SMB Multiple APs (<12): DHCP service is running on all APs, among which two of the APs will be Gateway APs. These two Gateway APs will provide the IP addresses as well as Internet connectivity to the clients via NAT.
- Enterprise (>12): For Enterprise sites, an additional on site vSZ-D/SZ100-D will be deployed at the remote site which will assume the responsibilities of performing DHCP/NAT functions. Therefore, DHCP/NAT service will not be running on any APs (they will serve clients only), while the DHCP/NAT services are provided by the onsite vSZ-D/SZ100-D.

Profile-based DHCP

The DHCP Server is designed in-line in the data plane and provides extreme scale in terms of IP address assignment to clients. This feature is especially useful in high density and dynamic deployments like stadiums, train stations where large number of clients continuously move in & out of WiFi coverage. The DHCP server in the network needs to scale to meet these challenging requirements. The DHCP server on the vSZ-D/SZ100-D provides high scale IP assignment and management with minimal impact on forwarding latency. DHCP Server supports 440K IP addresses and 64 pools with profile support.

NOTE
DHCP Server/NAT function if enabled is supported only for wireless client IPv4 address assignment.

Profile-based NAT

With NAT service enabled, all the WiFi client traffic is NATed by the vSZ-D/SZ100-D before being forwarded to the core network. Each vSZ-D/SZ100-D supports up to 990K ports and 16 public IP addresses for NAT. This feature essentially reduces the network overhead significantly since this reduces the MAC-table considerations on the UP-stream switches significantly. Again, very useful in high density deployments.

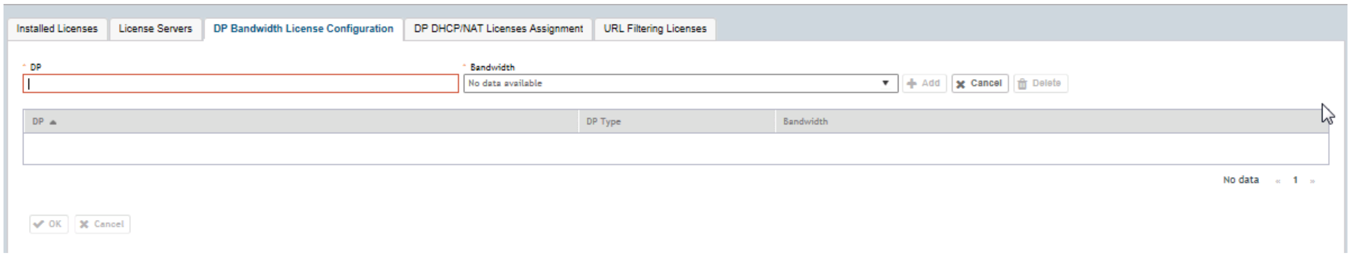
Configuring License Bandwidth

You can assign a license bandwidth for a data plane provided it is already approved. Each data plane can be configured with only one bandwidth license. Only vSZ-D support License Bandwidth.

1. Go to **Administration** > **Licenses**.

2. Select the **DP Bandwidth License Configuration** tab.

FIGURE 6 License Bandwidth Configuration



* DP

* Bandwidth: No data available

DP ▲	DP Type	Bandwidth

No data « 1 »

3. Select a DP from the Data Plane table, the **DP** name is automatically displayed.
4. From the **Bandwidth** drop-down menu, select one of the following bandwidth license:
   - 1Gbps (default)
   - 10Gbps for customers using 10G NIC card
   - Unlimited for customers using 40G NIC card.
5. Click **OK**. The data plane with the assigned license bandwidth is displayed.
6. Click **OK**.

   The message `Submitting form` appears, and the data plane is assigned a bandwidth.

You have successfully assigned a license bandwidth to the data plane.

Configuring the DHCP/NAT License Assignment

Creating DHCP License Assignment

Licensing needs to be created on a per SZ Controller Cluster basis. The default license, **CAPACITY-DP-SVDS-DEFAULT**, supports 1K DHCP address leases.

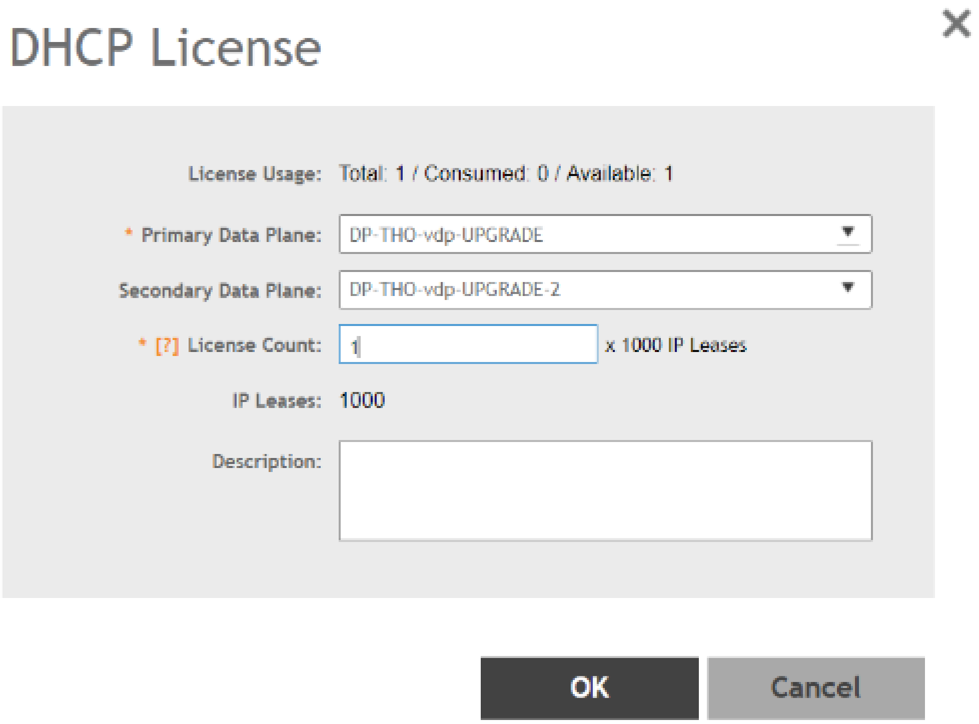
To create the DHCP License assignment:

1. Go to **Administration** > **Licenses**.
2. Select the **DP DHCP/NAT License Assignment** tab.

3. From the **DHCP License** area, click **Create**.

   The **DHCP License** form appears.

   FIGURE 7 DHCP License Assignment



License Usage: Total: 1 / Consumed: 0 / Available: 1

* Primary Data Plane: DP-THO-vdp-UPGRADE

Secondary Data Plane: DP-THO-vdp-UPGRADE-2

* [?] License Count: 1 x 1000 IP Leases

IP Leases: 1000

Description:

- **License Usage**: Lists the details of license consumption and availability.
- **Primary Data Plane**: Select the primary data plane from the drop-down. To remove the Data Plane from the DHCP license assignment, select **Clear**.
- **Secondary Data Plane**: Select the secondary data plane from the drop-down. To remove the Data Plane from the DHCP license assignment, select **Clear**.
- **License Count**: Enter the number of license. Range: 1 through 101.
- **IP Leases**: Lists the number of IPs assigned.
- **Description**: Enter a short description about the license assignment.

4. Click **OK**.

You have created the DHCP license assignment.

NOTE
To edit or remove the license assignment on the data plane, select the assignment from the list and click **Configure** or **Delete** respectively.

Creating NAT License Assignment

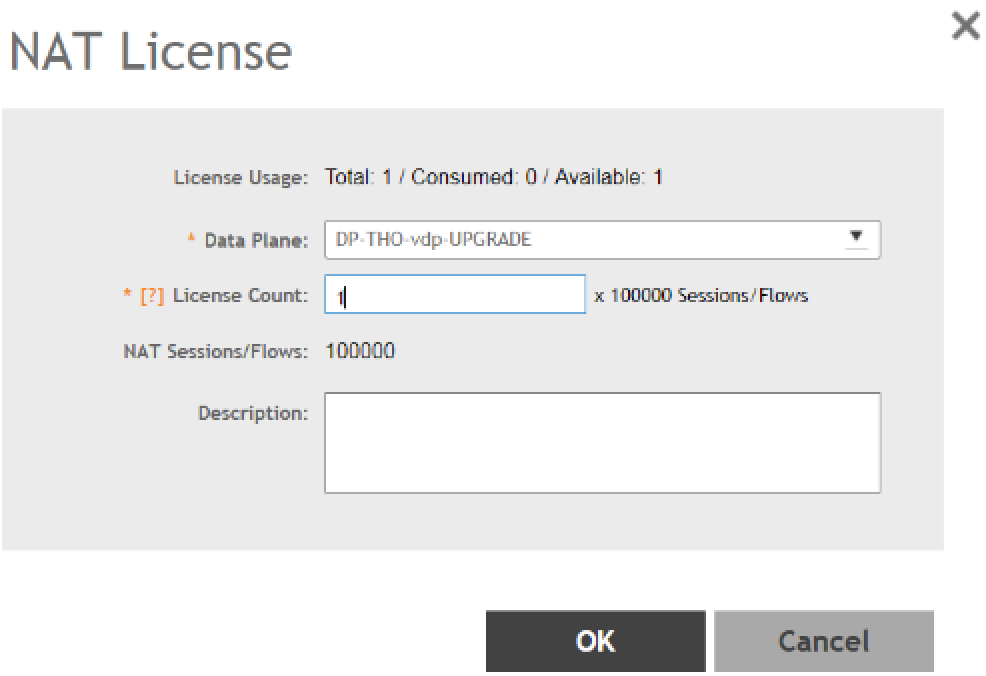
Licensing needs to be created on a per SZ Controller Cluster basis. The default license, **CAPACITY-DP-SNAT-DEFAULT**, supports 100K NAT sessions.

To create the NAT License assignment:

1. Go to **Administration** > **Licenses**.
2. Select the **DP DHCP/NAT License Assignment** tab.
3. From the **NAT License** area, click **Create**.

   The **NAT License** form appears.

   FIGURE 8 NAT License Assignment

   NAT License

   License Usage: Total: 1 / Consumed: 0 / Available: 1

   * Data Plane: DP-THO-vdp-UPGRADE

   * [?] License Count: 1 x 100000 Sessions/Flows

   NAT Sessions/Flows: 100000

   Description:

   - **License Usage**: Lists the details of license consumption and availability.
   - **Data Plane**: Select the data plane from the drop-down. To remove the Data Plane from the NAT license assignment, select **Clear**.
   - **License Count**: Enter the number of license for the data plane. Range: 1 through 20.
   - **NAT Sessions/Flows**: Lists the number of NAT sessions/flows.
   - **Description**: Enter a short description about the license assignment.
4. Click **OK**.

You have created the NAT license assignment.

> **NOTE**
> To edit or remove the license assignment on the data plane, select the assignment from the list and click **Configure** or **Delete** respectively.

L3 Roaming

Ruckus vSZ and vSZ-D/SZ100-D architecture now supports L3 Roaming without the need for additional mobility controllers.

The key use cases for L3 Roaming are well-understood,. Typically, a large WLAN network where APs are separated on different VLAN segments and there is a need for IP address preservation and potentially session persistence. Most common deployments are large campus networks designed with multiple switches and VLANs and there is a need to support L3 Roaming.

On vSZ-D/SZ100-D, Ruckus Wi-Fi can now support L3 Roaming with IP Address preservation. Below is the high level use case that describes the feature functions. A large network that is broken up into various campuses and there is a need to support L3 Roaming. Below figure depicts 2 campuses, which are L2 separated but need L3 Roaming.

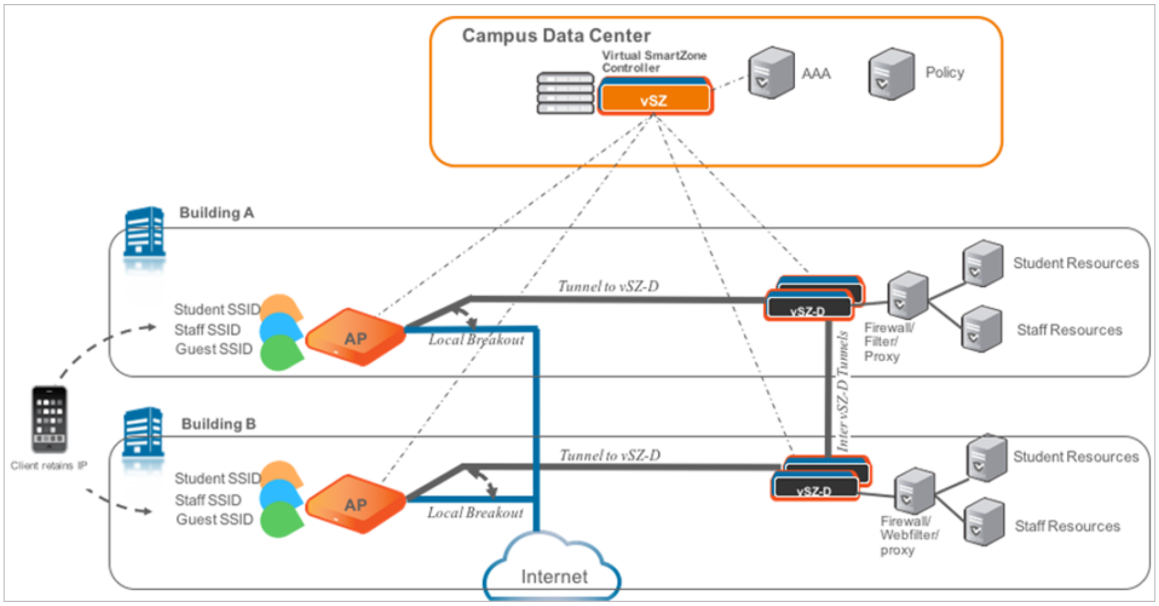
The APs in campus A setup a tunneled WLAN to the vSZ-D (Using Zone Affinity) and APs in building B setup a tunneled WLAN to the vSZ-D in their building.

Each vSZ-D/SZ100-D in the building can be configured to run a DHCP Server and NAT the traffic or be setup as a DHCP Relay. When a client roams from an AP in building A to an AP in building B, the vSZ-D/SZ100-D in building B detects the roaming event and forwards the traffic (or assigns the same IP back to the client) to the vSZ-D in building A (home vSZ-D/SZ100-D or anchor vSZ-D/SZ100-D) to ensure that service to the client is not interrupted.

One additional unique benefit of this architecture over other L3 Roaming solutions is that with this architecture, the roamer client can still have access to his home network resources (this is similar to mobile roaming on 3G/4G networks).

NOTE
Traffic between inter vSZ-D/SZ100-D tunnels in Figure 6 can be encrypted by enable "Tunnel Encryption.

FIGURE 9 Usage of L3 roaming



Editing L3 Roaming for a vSZ-D/SZ100-D

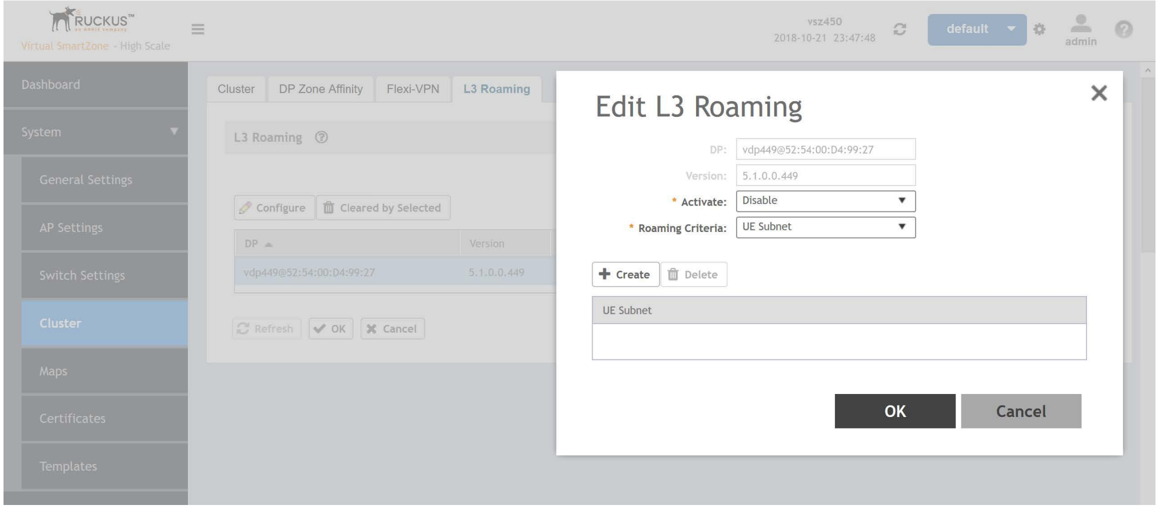
For L3 roaming to work without session break, the data planes between which the roaming happens must both be enabled with the L3 Roaming feature.

NOTE
If the IP address of the UE changes, then the session breaks.

1. Go to **System** > **Cluster**.
2. Select **L3 Roaming**.

   The **Enabling L3 Roaming** page is displayed.

FIGURE 10 Enabling L3 Roaming



Edit L3 Roaming

DP: vdp449@52:54:00:D4:99:27

Version: 5.1.0.0.449

* Activate: Disable

* Roaming Criteria: UE Subnet

UE Subnet

3. Click **Configure** to edit the L3 roaming settings.

   The **Edit L3 Roaming** page is displayed.
4. From **Activate**, you can enable the feature for the DP by selecting Enable or Disable from the drop-down menu.
5. From the **Roaming Criteria** list, select one of the following options to define the data format to establish connection between DPs: UE Subnet or WLAN VLAN.
6. Click **OK**.

   You have successfully enabled L3 roaming, and also set the roaming criteria based on which DPs would connect within the network.

You have enabled L3 roaming in the selected vSZ-D/SZ100-D.

Lawful Intercept

An important carrier class feature that is being introduced on the vSZ-D/SZ100-D is to support Lawful Intercept requirements.

These are slowly becoming mandatory and stringent on SP-WiFi deployments where Service Providers need to meet the CALEA standard requirements.

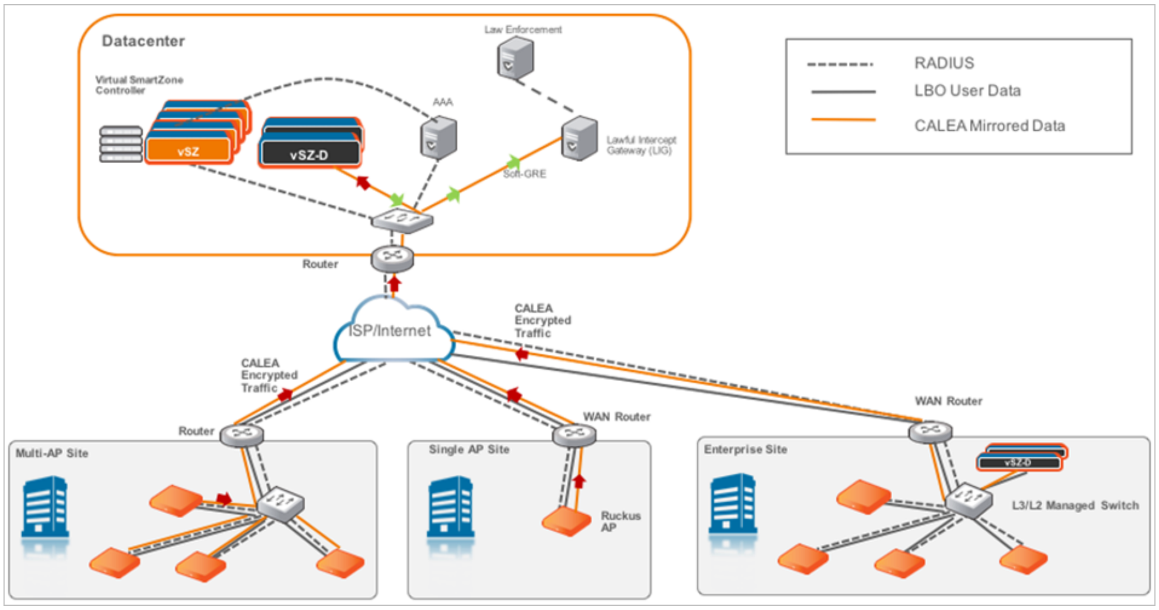
Ruckus vSZ-D/SZ100-D now supports the ability to identify a device that has a LI warrant issued against it and mirror the client data traffic to a LIG (Lawful Intercept Gateway) that is hosted in the SP's data center over L2oGRE.

The figure below illustrates the high level architecture that is supported for Lawful Intercept capabilities. It aslo depicts an architecture where smaller sites (with lesser number of APs) that do not need data tunneling to vSZ-D/SZ100-D (depicted as Multi-AP and Single AP sites) but need Lawful Intercept. On the other side is a large enterprise site with large number of APs and need tunneling (depicted as Enterprise site with vSZ-D/SZ100-D on premise) with Lawful intercept.

> **NOTE**
> As mentioned in this document, the flexibility of the Ruckus vSZ/vSZ-D architecture is that WiFi service providers can deploy the vSZ-D/SZ100-D only on premises where there is a need (typically larger venues) for tunneling.

The Ruckus architecture simply involves spinning up a vSZ-D/SZ100-D instance at the central data center and designate that vSZ-D/SZ100-D instance as a CALEA mirroring agent. All of this configuration is centrally managed through the vSZ. Once the network is setup appropriately, when a client device with a matching MAC address that has a warrant is detected on any of the access sites, the APs (or the vSZ-D/SZ100-D) will mirror the packets to the vSZ-D (CALEA Mirroring agent) in the DC which will then forward the traffic to the LIG (Lawful Intercept Gateway) either in the DC or SP DC.

FIGURE 11 Usage of Lawful Intercept



Enabling Flexi VPN

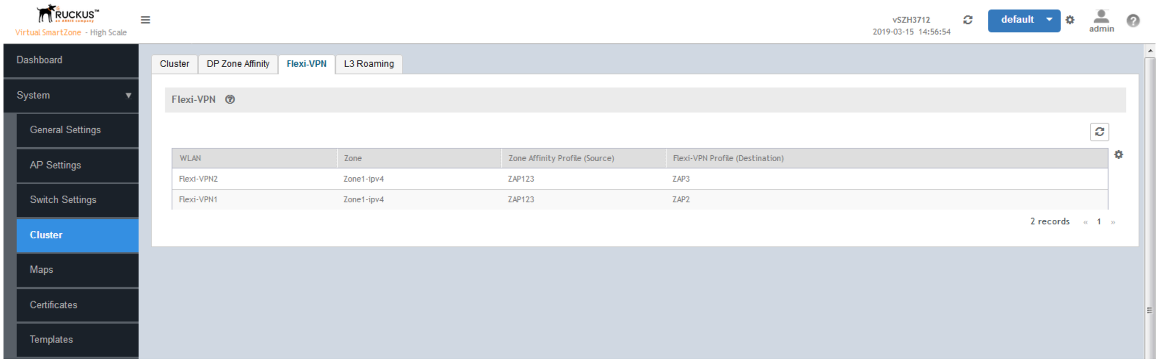
You can enable Flexi-VPN and limit the network resources that a UE can access. Flexi-VPN allows an administrator to customize the network topology, and is thereby able to control the network resources accessible to the end-user. This feature is only supported on vSZ-E and vSZ-H, and is enabled by purchasing the Flexi-VPN license.

1. Select **System** > **Cluster**.

2. Select **Flexi-VPN**.

   The **Flexi-VPN** status page is displayed.

   FIGURE 12 Enabling Flexi-VPN



WLAN	Zone	Zone Affinity Profile (Source)	Flexi-VPN Profile (Destination)
Flexi-VPN2	Zone1-ipv4	ZAP123	ZAP3
Flexi-VPN1	Zone1-ipv4	ZAP123	ZAP2

2 records « 1 »

NOTE
The Flexi-VPN option is available only if the Access-VLAN ID is configured in manual mode, and when VLAN Pooling, Dynamic VLAN and Core Network VLAN options, and Tunnel NAT are disabled.

NOTE
Flexi-VPN is activated when a Flexi-VPN profile is assigned to a WLAN.

NOTE
A maximum of 1024 WLAN IDs can be applied to a Flexi-VPN profile.
Flexi-VPN supports IPv4 addressing formats and Ruckus GRE tunnel protocol. It does not support IPv6 addressing formats.

The following record table indicates that the Flexi-VPN profile is successfully applied to the WLAN:

- WLAN: displays the name of the WLAN
- Zone: displays the name of the zone
- Zone Affinity Profile: displays the name of the source data plane from which tunneled traffic starts
- Flexi-VPN Profile: displays the name of the destination data plane to where the tunneled traffic terminates

Enabling Tunnel Encryption

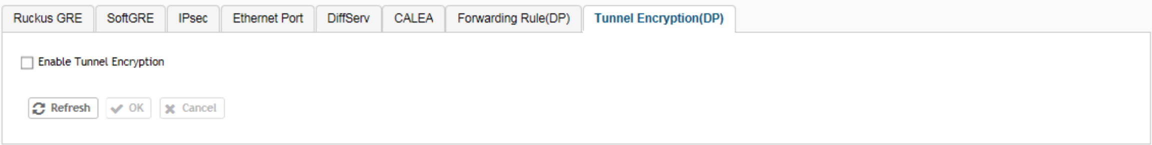
You can use the tunnel encryption feature to encrypt data for a private network, through a public network. This feature is available in vSZ-H and vSZ-E.

1. Go to **Services & Profiles** > **Tunnels and Ports**.

2. Select the **Tunnel Encryption(DP)** tab.

   The **Tunnel Encryption (DP)** page appears.

   FIGURE 13 Tunnel Encryption (DP)

   □ Enable Tunnel Encryption

3. Select the **Enable Tunnel Encryption** check-box.
4. Click **OK**.

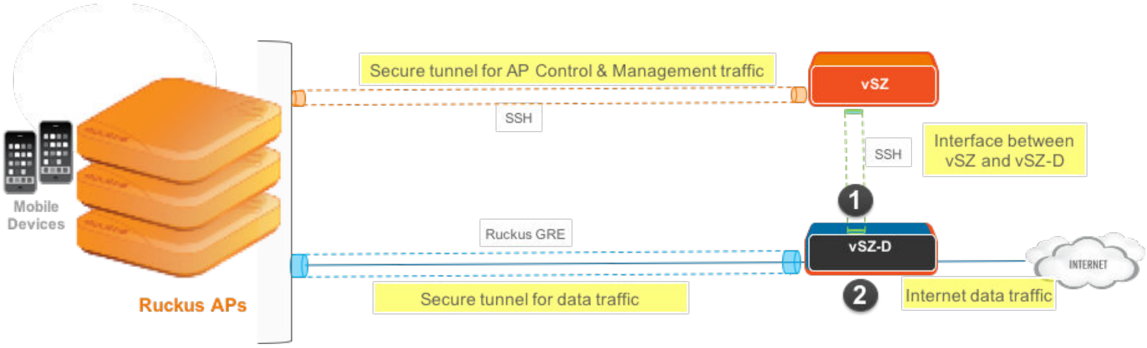
You have successfully enabled tunnel encryption.

Network Architecture

vSZ-D/SZ100-D requires at least two physical interfaces: one for control/management and another for data plane.

The control/management interface is used for communication with the vSZ controller, as well as the command line interface. The data plane interface is used to tunnel user data traffic from the APs.

FIGURE 14 vSZ-D logical interfaces


Secure tunnel for AP Control & Management traffic
SSH
vSZ
SSH
Interface between vSZ and vSZ-D
1
Mobile Devices
Ruckus GRE
vSZ-D
INTERNET
Secure tunnel for data traffic
2
Internet data traffic
Ruckus APs

The access layer (southbound) is used to tunnel traffic to and from managed APs. The following connections exist on the access layer.

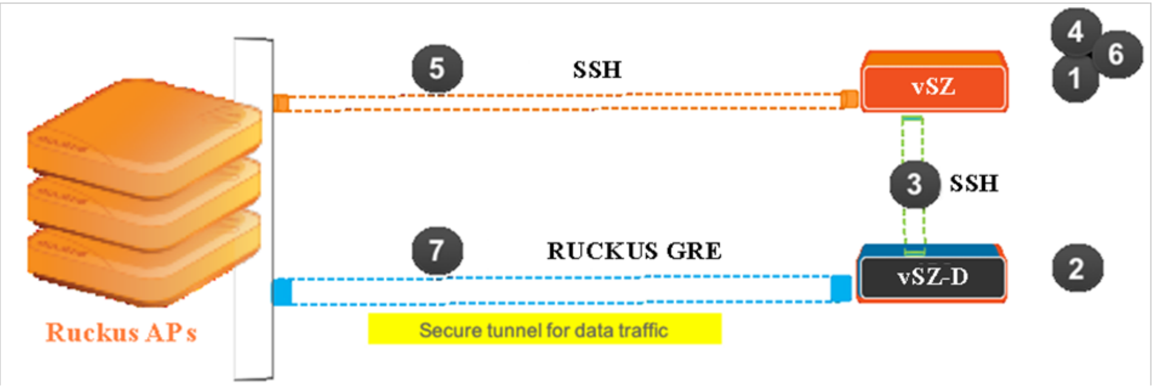
1. AP to and from vSZ-D/SZ100-D : Data plane, secured by Ruckus GRE tunnel.
2. vSZ to and from vSZ-D/SZ100-D : Control plane, for vSZ to manage vSZ-D/SZ100-D
3. AP to and from vSZ: Control plane, for vSZ to manage the AP

The core layer (northbound) is used by vSZ-D/SZ100-D to forward traffic to and from the core network.

Communication Workflow

The figure below captures a high level end-to-end communication flow between Ruckus APs, vSZ and vSZ-D/SZ100-D.

FIGURE 15 Communication workflow between Ruckus APs, vSZ, and vSZ-D/SZ100-D



The following are the steps seen in the above figure.

1. Update the vSZ controller to the latest release or perform a fresh install of the vSZ controller with the latest release

   NOTE
   If you are upgrading the vSZ controller and the vSZ-D/SZ100-D, Ruckus recommends the update of vSZ controller before the update of vSZ-D/SZ100-D

2. Install vSZ-D/SZ100-D and point it to the vSZ-E or vSZ-H controller by using the following options:
   - Set vSZ-E or vSZ-H control interface IP address or FQDN or configure the controller IP address via DHCP option 43.
   - For vSZ-E or vSZ-H configured with three (3) IP interfaces, the IP address to use is the vSZ control interface IP address.
3. The vSZ-D/SZ100-D management interface connects with the vSZ-E or vSZ-H controller control interface
4. The vSZ-E or vSZ-H controller administrator approves the vSZ-D/SZ100-D connection request
5. The vSZ informs the AP of the vSZ-D/SZ100-D data interface
6. The vSZ-D/SZ100-D is displayed as active and managed on vSZ-E or vSZ-H
7. AP establishes a Ruckus GRE tunnel with the vSZ-D/SZ100-D data interface when a tunnelling WLAN is configured

Figure 15 depicts logical network architecture. In real-world deployments, there may be network routers, gateways, firewalls and other devices; these typical network devices are not shown in the figure to focus on the vSZ-D/SZ100-D interfaces and communication protocol aspects between the various entities.

It is also important to note that support for distributed or centralized deployment topologies introduce NAT routers/gateway devices. The communication interfaces between Ruckus APs, vSZ and vSZ-D/SZ100-D are designed to support NAT traversal so as to support such NAT Deployment Topologies on page 33.

NAT Deployment Topologies

vSZ-D/SZ100-D supports several deployment topologies.

AP Behind NAT and vSZ-D/SZ100-D Behind NAT

When an AP is behind NAT, it is assumed that AP is sitting in the private world and wants to talk to vSZ-D/SZ100-D in the public world through NAT. The AP obtains its private IP address and communicate with the vSZ-D/SZ100-D through NAT. During communication with vSZ-D/SZ100-D, the NAT router will intercept the packet and change the source IP address (which is the AP IP address) to a public IP address and add a new source port number before forwarding the packet to vSZ-D/SZ100-D. vSZ-D/SZ100-D, in this case, is insensitive to the NAT router's operation. When the packet comes back from vSZ-D/SZ100-D to the AP, the NAT router will intercept the packet and translate the destination IP address and port number back to the appropriate (original) AP IP address and port number.

When vSZ-D/SZ100-D is behind NAT, it is assumed that vSZ-D/SZ100-D is sitting in the private world and wants to talk to the AP in the public world through NAT. In this case, it is needed to setup the NAT IP (public IP) and a port number pair in vSZ-D/SZ100-D "setup" process. vSZ picks up this public address and the associated port number and informs the AP that this is the vSZ-D/SZ100-D address/port (public-IP, port) pair to connect to.

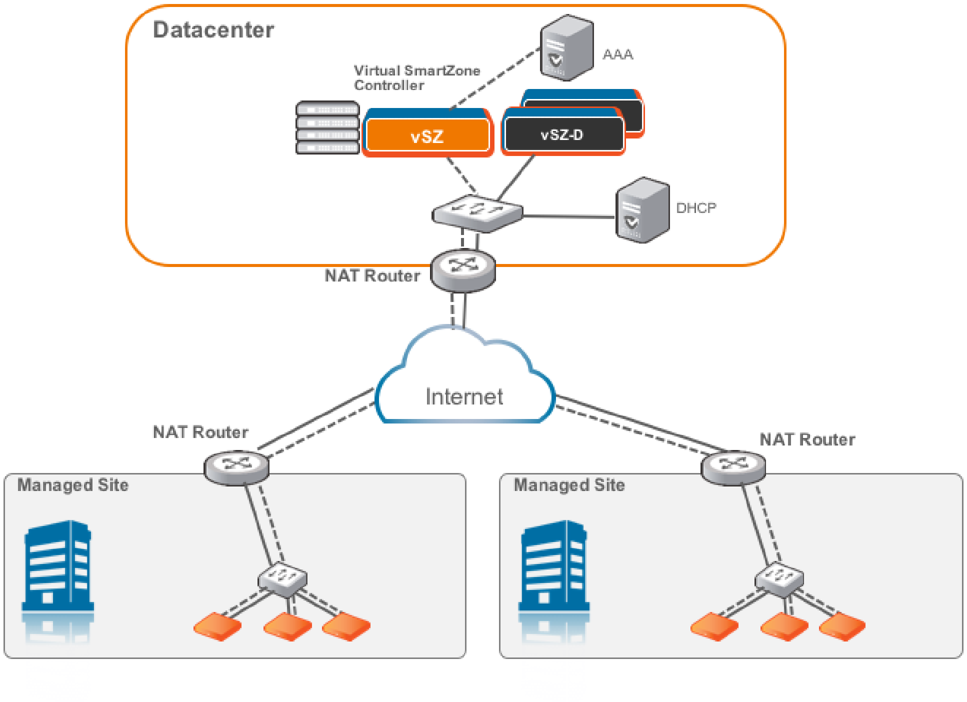
It is also needed to configure the NAT device and enter the port mapping, basically, (public-IP, port) <-> (private-IP, 23233) into NAT's rule table. Thus, when NAT receives the packet bound for vSZ-D/SZ100-D (sent to public-IP/port) from the AP, it will translate it to (private-IP, 23233) based on the rule table before sending it to vSZ-D/SZ100-D, and conversely, for packet from vSZ-D/SZ100-D, NAT router will look at the srcIP/srcPort (IP, 23233), and convert it to public IP address or port based on the rule table before sending it to AP.

NOTE
Both TCP and UDP protocols on port 23233 need to be forwarded as both are used (TCP is used for tunnel establishment and UDP for client data)

vSZ and vSZ-D/SZ100-D at Data Center Behind NAT

In this deployment topology, vSZ-D/SZ100-D and vSZ are co-located at the data center behind NAT, while Ruckus APs are on the access network behind NAT.

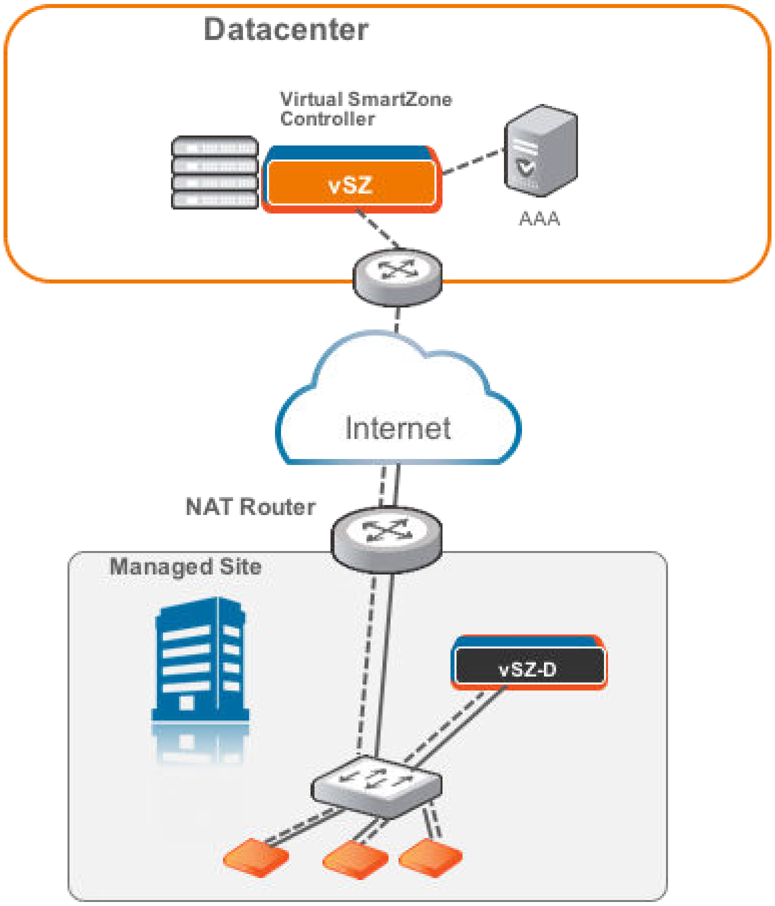
FIGURE 16 vSZ and vSZ-D/SZ100-D at data center behind NAT



vSZ-D/SZ100-D at Access Site with NAT

In this deployment topology, vSZ is at the data center and vSZ-D/SZ100-D is co-located with the Ruckus APs on the access network. In this scenario, there are NAT routers between vSZ and vSZ-D/SZ100-D/Ruckus APs.

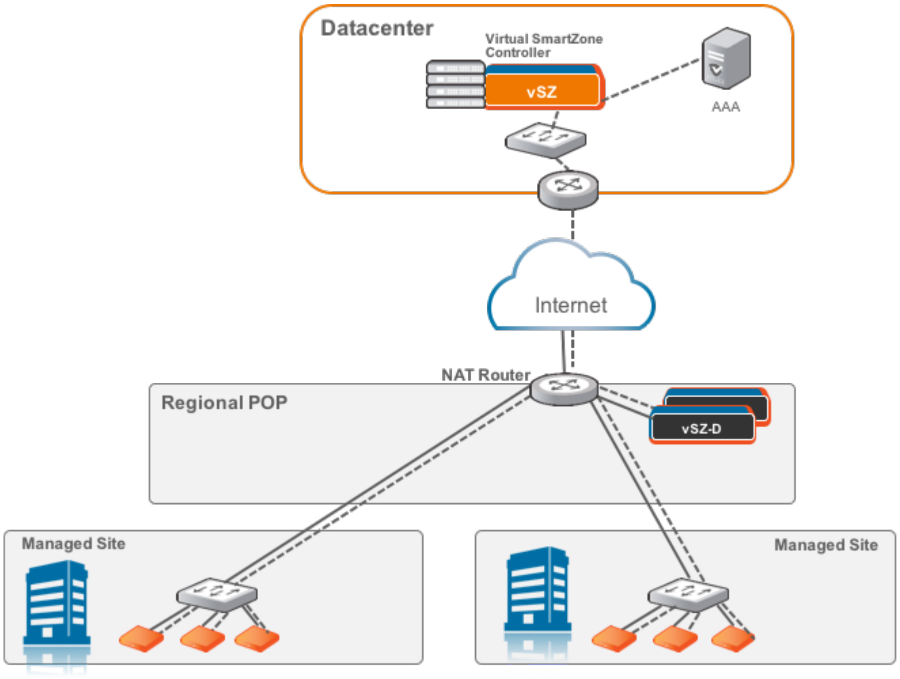
FIGURE 17 vSZ-D/SZ100-D at access site with a NAT router



vSZ-D/SZ100-D Behind NAT

In this deployment topology, vSZ is at the data center and vSZ-D/SZ100-D is in a distributed site but not co-located with the Ruckus APs within the access network. There are NAT routers between vSZ and vSZ-D/SZ100-D, and between vSZ-D/SZ100-D and Ruckus APs. The vSZ-D/SZ100-D port to communicate with vSZ control plane is port 22.

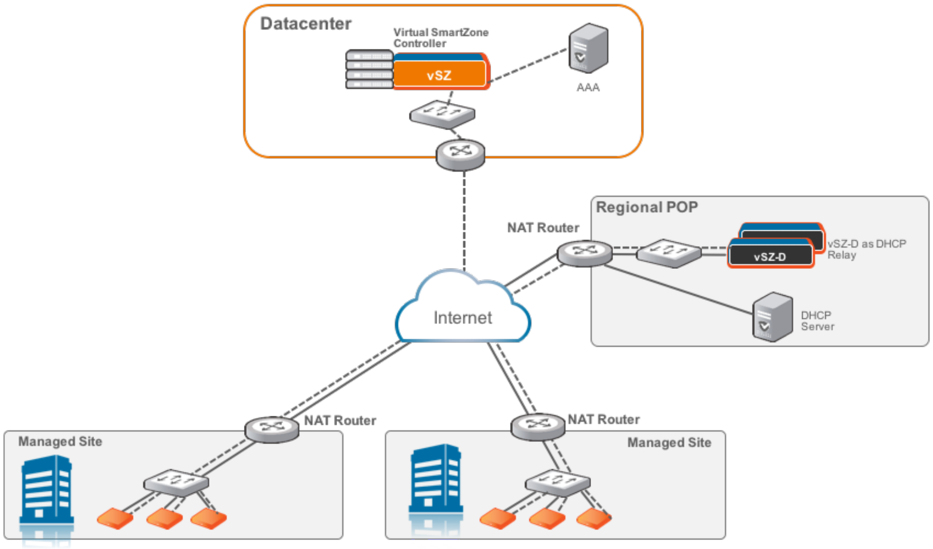
FIGURE 18 vSZ-D/SZ100-D behind a NAT router



DHCP Relay with NAT

Similar to the *vSZ-D/SZ100-D Behind NAT*, in this deployment topology, vSZ is at the data center and vSZ-D/SZ100-D is in a distributed site but not co-located with the Ruckus APs within the access network. There are NAT routers between vSZ and vSZ-D/SZ100-D, and between vSZ-D/SZ100-D and Ruckus APs. However, in this topology, the DHCP server assigning client IP addresses is on its own separate subnet. vSZ-D/SZ100-D provides the DHCP relay function to support such a network configuration.

FIGURE 19 DHCP relay with a NAT router

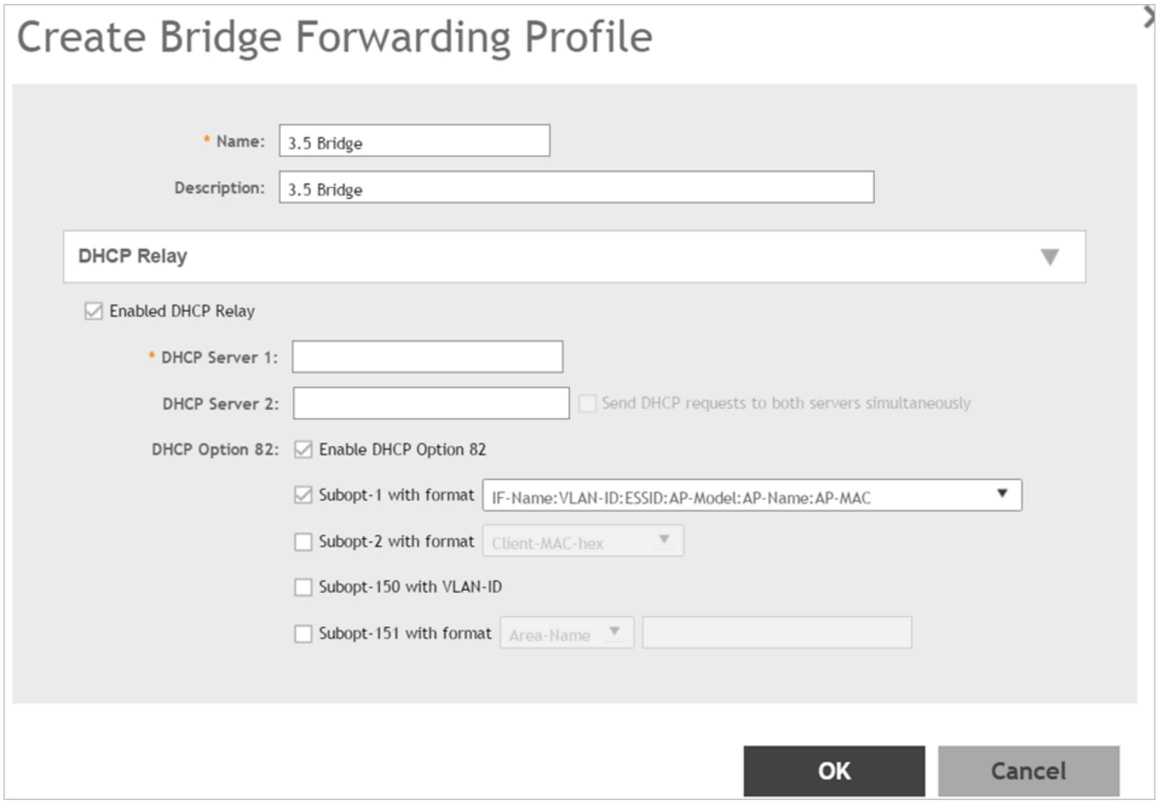


DHCP Option 82 and Bridge Profile

If you are enabling the DHCP Option 82 in WLAN configuration in the controller vSZ, it means that the AP is going to put DHCP Option 82 in the DHCP server and will send it to vSZ-D/SZ100-D. This is in the format `IF-Name:VLAN-ID:ESSID:AP-Model:AP-Name:AP-MAC`. If you want to give the users the option to choose what needs to be included in DHCP Option 82, you would need to create a *Bridge Service Profile* in the vSZ controller web interface. Follow the steps to create a *Bridge Service Profile*.

- Go to **vSZ controller web interface** > **Services & Profiles** > **Core Network Tunnel**
- Click on **Create** to add a **Bridge Forwarding Profile**
- Verify if the **DHCP Relay** is enabled.
- Add the **DHCP server** IP address
- Enable **DHCP Option 82** and choose the sub options based on your requirement or of the user. This will be taken care by vSZ-D/SZ100-D during DHCP packet relay to the DHCP server.

FIGURE 20 Creating Bridge Profile



Create Bridge Forwarding Profile

* Name: 3.5 Bridge

Description: 3.5 Bridge

DHCP Relay ▼

☑ Enabled DHCP Relay

* DHCP Server 1:

DHCP Server 2: □ Send DHCP requests to both servers simultaneously

DHCP Option 82: ☑ Enable DHCP Option 82

☑ Subopt-1 with format IF-Name:VLAN-ID:ESSID:AP-Model:AP-Name:AP-MAC ▼

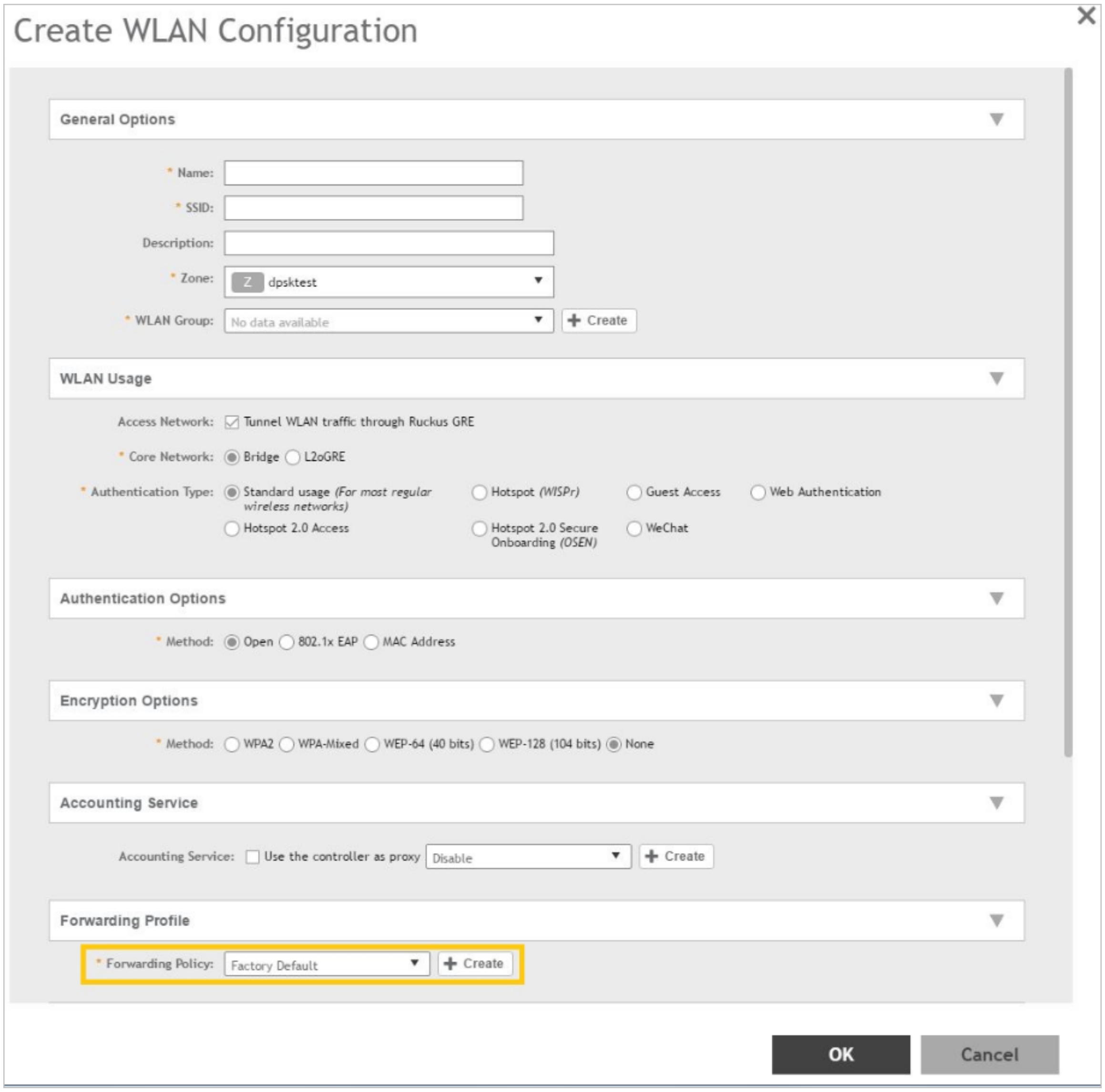
□ Subopt-2 with format Client-MAC-hex ▼

□ Subopt-150 with VLAN-ID

□ Subopt-151 with format Area-Name ▼

- Go to **vSZ controller web interface** > **Wireless LANs**
- Click on **Create** to add the following new WLAN configuration:
  - **Access Network** as **Tunnel WLAN traffic through Ruckus GRE**
  - **Core Network** as **Bridge**
  - **Authentication Options** > **Method**as **Open**
  - **Encryption Options** > **Method**as **None**
  - **Forwarding Policy** as **Factory Default** . Choose the forwarding policy as the bridge profile.
- Click **OK** to complete and save the configuration.

FIGURE 21 Creating a WLAN Configuration



Create WLAN Configuration

General Options

- * Name:
- * SSID:
- Description:
- * Zone: Z dpsktest
- * WLAN Group: No data available + Create

WLAN Usage

- Access Network: ☑ Tunnel WLAN traffic through Ruckus GRE
- * Core Network: ● Bridge ○ L2oGRE
- * Authentication Type: ● Standard usage *(For most regular wireless networks)* ○ Hotspot *(WISPr)* ○ Guest Access ○ Web Authentication ○ Hotspot 2.0 Access ○ Hotspot 2.0 Secure Onboarding *(OSEN)* ○ WeChat

Authentication Options

- * Method: ● Open ○ 802.1x EAP ○ MAC Address

Encryption Options

- * Method: ○ WPA2 ○ WPA-Mixed ○ WEP-64 (40 bits) ○ WEP-128 (104 bits) ● None

Accounting Service

- Accounting Service: □ Use the controller as proxy Disable + Create

Forwarding Profile

- * Forwarding Policy: Factory Default + Create

Hardware Requirements

vSZ-D supports auto scaling, which means the number of CPU cores can be expanded without needing a software update. Ruckus has tested from three to six CPU core allocations for the vSZ-D.

NOTE
The minimum memory and CPU requirements for vSZ have changed in this release. You may need to upgrade your infrastructure before upgrading. Please read carefully. This is the minimum requirement recommended. Refer to the Release Notes or the vSZ Getting Started Guide.

The following table lists the minimum hardware requirements recommended for running an instance of vSZ-D.

TABLE 3 vSZ-D hardware requirements

Hardware Component	Requirement
Hypervisor support required by Management Interface	VMWare ESXi 6.7 and later OR KVM (CentOS 7.4 64bit)
Processor	Intel Xeon E55xx and above. Recent Intel E5-2xxx chips are recommended
CPU cores	• Minimum 3 to 6 cores per instance dedicated for data plane processing. • DirectIO mode for best data plane performance. **NOTE** Actual throughput numbers will vary depending on infrastructure and traffic type. • vSwitch mode for flexibility
Memory	Minimum 6 Gb memory per instance
Disk space	10GB per instance
Ethernet interfaces	2
NICs that support Intel DPDK requiredby Data Interface	• Intel NICs igb, ixgbe • I350 • 82599EB, 82599, X520, 82599ES

Important Notes About Hardware Requirements

- If you change the number of CPU cores, you must reboot vSZ-D for the changes to take effect.
- The first core is always shared between Linux and NPE. Other cores are dedicated to NPE.
- vSZ-D requires two interfaces and these interfaces must be deployed on different subnets.
- The management interface of the vSZ-D can be any model as long as the NIC is supported by the hypervisor.
- The data interface needs to be Intel DPDK based.

Supported Modes of Operation

vSZ-D supports two modes of operation: direct IO mode and vSwitch mode.

For best performance, Ruckus recommends using the direct IO mode. SR-IOV mode is unsupported. Refer to the table below for mode of operation

NOTE
NICs assigned to direct IO cannot be shared. Moreover, VMware features such as vMotion, DRS, and HA are unsupported.

The hardware configuration for a single vSZ-D instance specified in the guide will scale to handle 10K tunnels (10K APs) and up to 10Gbps of throughput (unencrypted) with appropriate underlying Intel NIC cards (10G interfaces) in directIO mode of operation. This aligns with the number of Ruckus AP that a vSZ controller supports. Refer to the dimensioning table below.

TABLE 4 Hardware Dimensioning

Number of vSZ Instances	Number of vSZ-D Instances	Number of Ruckus APs	Number of Tunnels on vSZ-D	Maximum Throughput (Unencrypted)	Notes
1	1	10000	10000	10 Gbps	It is recommended to have 10G NICS on the vSZ-D considering the high number of Ruckus APs.
1	2	10000	5000 (10K maximum in case of failover)	10 Gbps	Tunnels are load-balanced towards the vSZ-D by the vSZ. This is useful when data plane redundancy is required. It is recommended to have 10G NICS on the vSZ-D considering the high number of Ruckus APs.
2	2	10000	5000 (10K maximum)	10 Gbps	Tunnels are load-balanced towards the vSZ-D by the vSZ. Each vSZ-Dmim tunnels.
2	4	10000	2500 (10K maximum)	10 Gbps	Tunnels are load-balanced towards the vSZ-D by the vSZ. Each vSZ-D instance can handle 10K maximim tunnels.
3	6	20000	3300 (10K maximum)	10 Gbps	Tunnels are load-balanced towards the vSZ-D by the vSZ. Each vSZ-D instance can handle 10K maximim tunnels.
4	8	30000	3750 (10K maximum)	10 Gbps	Tunnels are load-balanced towards the vSZ-D by the vSZ. Each vSZ-D instance

TABLE 4 Hardware Dimensioning (continued)

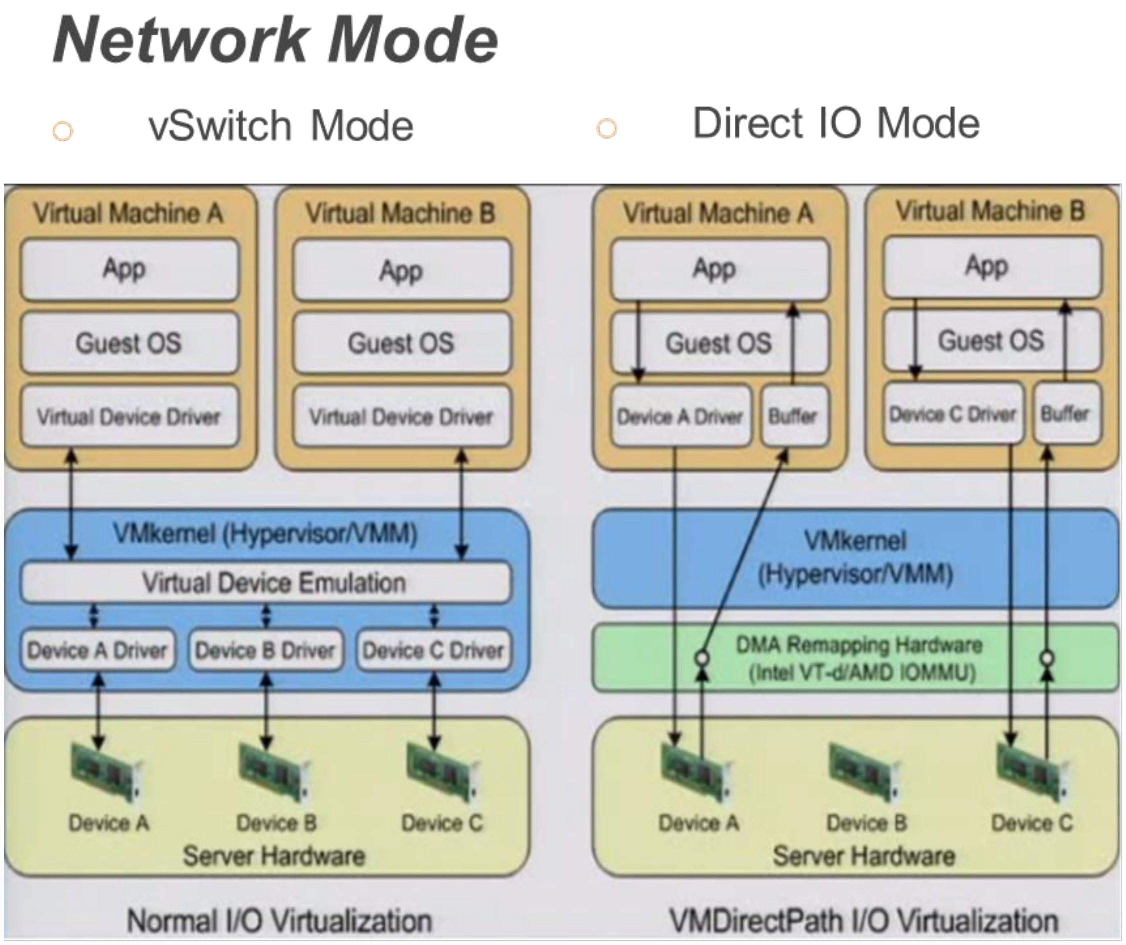
Number of vSZ Instances	Number of vSZ-D Instances	Number of Ruckus APs	Number of Tunnels on vSZ-D	Maximum Throughput (Unencrypted)	Notes
					can handle 10K maximim tunnels.

TABLE 5 Mode of Operation

Hypervisor	Number of CPUs	Memory (GB)	Hard Disk (GB)	Number of Tunnels	Tunnel Bandwidth (Intel NIC-10 G) (Unencrypted)	Packet Size (Bytes)
Vmware (DirectIO)	3	6	10	1000	17.6 Gbps	1400
Vmware (DirectIO)	6*	6	10	10000	6.3 Gbps	Random
Vmware (DirectIO)	3	6	10	10000	4.5 Gbps	Random

NOTE
Refer to the vSZ-D Performance Recommendations on page 107 chapter for encryption and vSwitch impacts.

NOTE
* vSZ-D needs to increase the CPUs to 6 for sustaining the 10GB line rate in random-byte traffic when the encryption is enabled. Encrypted requires 6 cores and unencrypted requires 3 cores



Network Mode

- vSwitch Mode
- Direct IO Mode

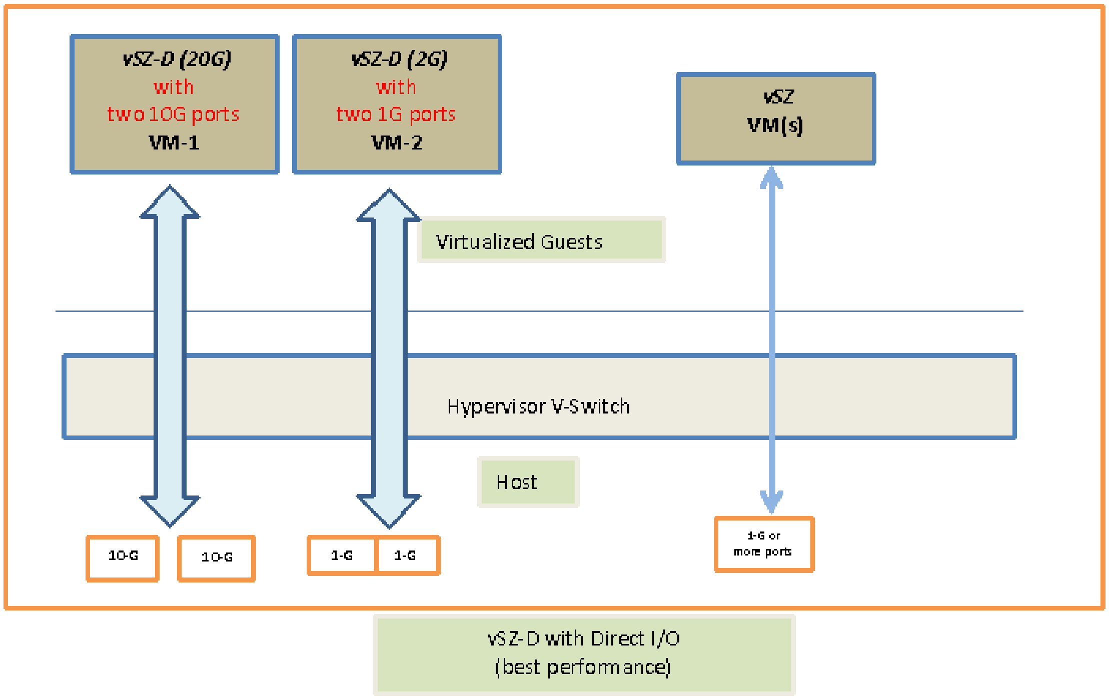
The figure below depicts a sample configuration in DirectIO mode. This is the recommended deployment model for the vSZ-D for best performance benefits. In this setup, cores as well as the NICs are dedicated to the vSZ-D VM only for best performance.

NOTE
In this setup, the vSZ-D data plane interfaces directly with the DPDK NIC, completely bypassing the vSwitch

vSZ-D with DirectI/O

NOTE
The figure below depicts multiple virtual data plane instances for reference purposes only.

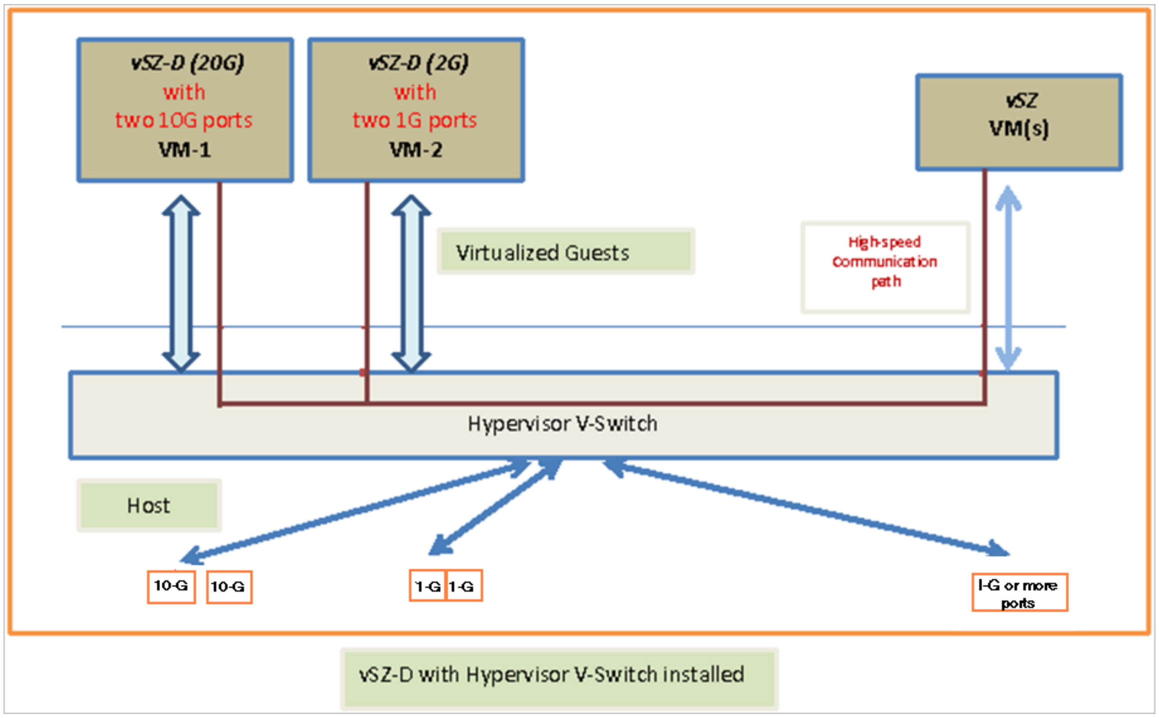
It also depicts a vSZ controller instance running as a separate VM. These VMs can be running on the same underlying host or potentially different hosts.



vSZ-D with Hypervisor vSwitch Installed

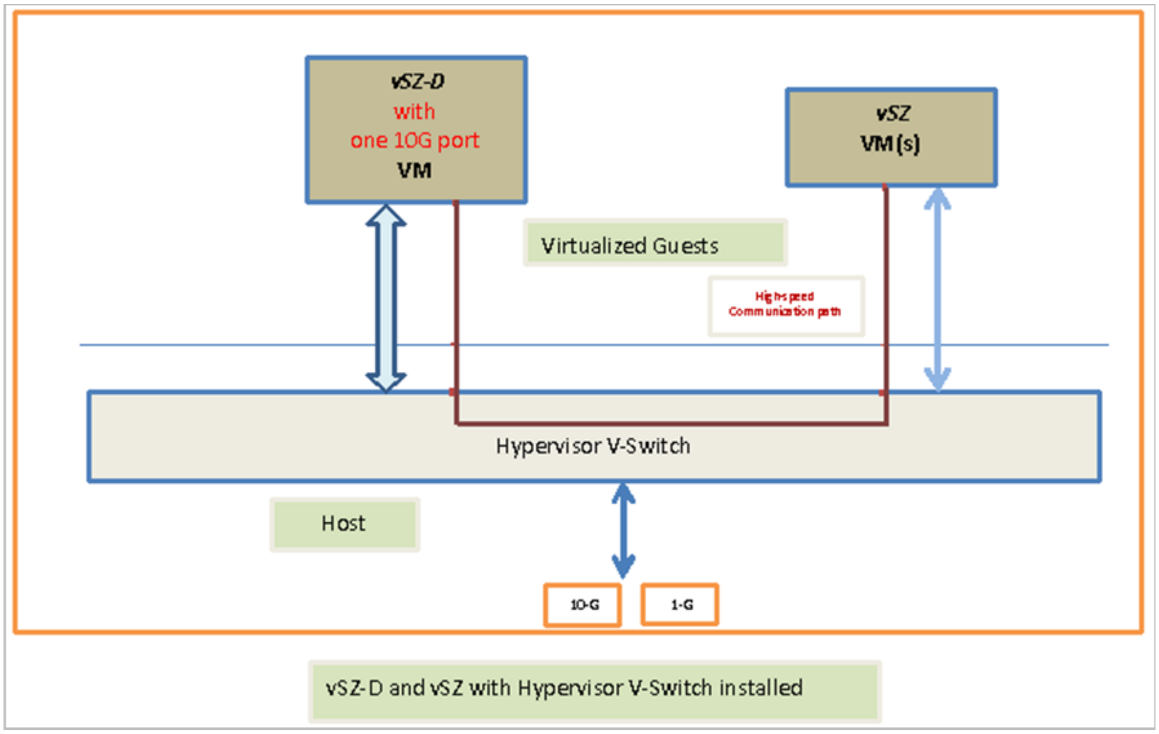
The figure below depicts a sample setup via the vSwitch.

NOTE
The figure below depicts multiple virtual data plane instances for reference. It also depicts a vSZ controller instance running as a separate VM.



vSZ-D and vSZ with Hypervisor vSwitch Installed

The figure below depicts an architecture where vSZ and vSZ-D are running on the same underlying host.



Recommended NICs and Operation Modes

The following table lists the modes of operation and network interface cards (NICs) that have been tested by Ruckus. Other NICs that support Intel DPDK architectures may or may not work.

TABLE 6 Recommended NICs and operation modes

Interface	Mode	Supported NIC Driver		NIC Model
Control / management	vSwitch	E1000		I350 Broadcom BCM5720
Data	Direct IO	1GB	igb	I350
		10GB	ixgbe	82599EB
				82599 82599ES
				X520
	vSwitch	VMware	VMXNET3	--
		KVM	Virtio	--

Hypervisor Configuration

This section covers hypervisor-specific configurations that Ruckus recommends and other settings that you may need to fine tune.

Supported Hypervisors

Unlike the vSZ controller, vSZ-D can only be installed on specific versions of VMware and KVM.

The tables below list the hypervisors and versions on which vSZ and vSZ-D can and cannot be installed.

TABLE 7 vSZ and vSZ-D supported hypervisors

	vSZ	vSZ-D
VMware 5.1	Supported from 2.5	
VMware 5.5 and later	Supported from 3.0	Supported from 3.2
KVM CentOS 6.5 64-bit	Supported from 2.5	
KVM CentOS 7.0 64-bit	Supported from 3.0	Supported from 3.2
Hyper-V	Supported from 3.2	
Azure	Supported from 3.2	
GCE	Supported from 3.2	

General Configuration

Ruckus offers the following general configuration recommendations.

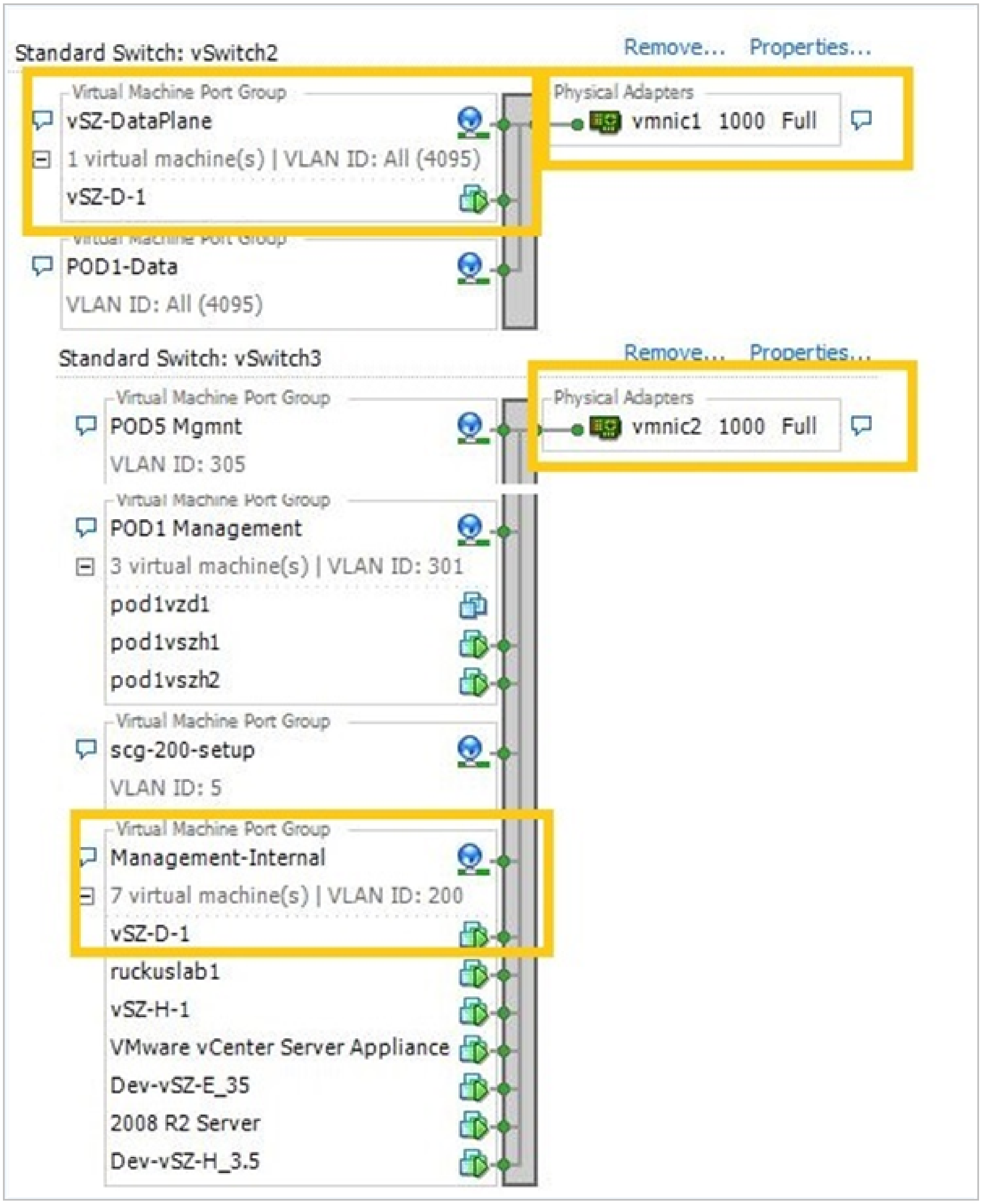
TABLE 8 General vSZ-D configuration recommendations

Component	Minimum Recommendation
Recommended reserved memory	Minimum 6144MB
Recommended number of CPU cores	Minimum three CPU cores. For improved performance in a large-scale deployment, allocate six CPU cores.
Configuration via DirectIO or through vSwitch	To enable passthrough on NIC devices, configure DirectIO mode in ESXi in **Advanced Settings**.

VMware Specific Configuration

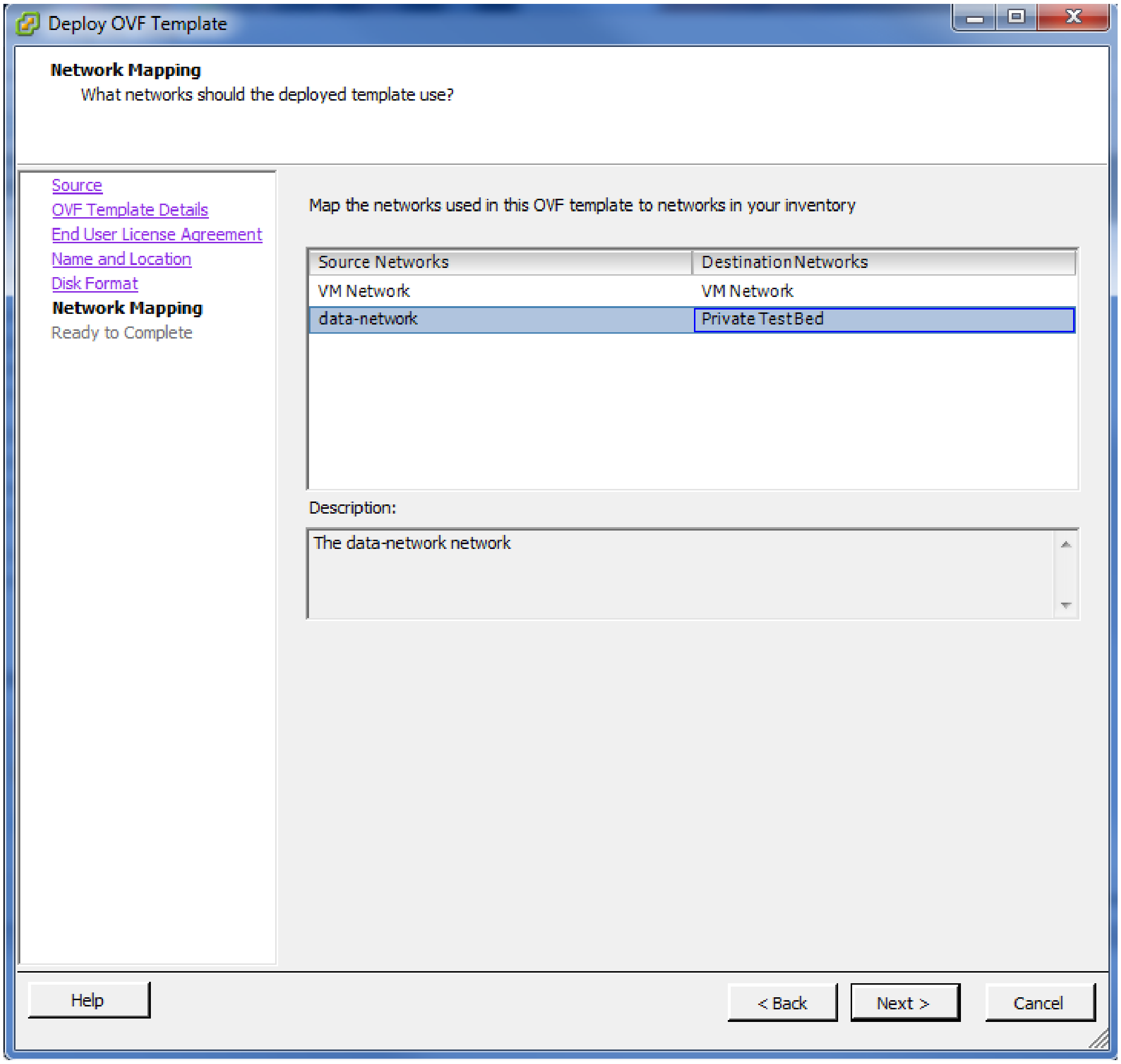
If you are installing vSZ-D on VMware, read these VMware specific configuration recommendations from Ruckus.

- Deploy vSZ-D on a machine that has at least two physical NICs. Alternatively, deploy to two vSwitch instances with dedicated physical NICs.



Standard Switch: vSwitch2
Remove...
Properties...
Virtual Machine Port Group
vSZ-DataPlane
1 virtual machine(s) | VLAN ID: All (4095)
vSZ-D-1
Physical Adapters
vmnic1 1000 Full
Virtual Machine Port Group
POD1-Data
VLAN ID: All (4095)
Standard Switch: vSwitch3
Remove...
Properties...
Virtual Machine Port Group
POD5 Mgmnt
VLAN ID: 305
Physical Adapters
vmnic2 1000 Full
Virtual Machine Port Group
POD1 Management
3 virtual machine(s) | VLAN ID: 301
pod1vzd1
pod1vszh1
pod1vszh2
Virtual Machine Port Group
scg-200-setup
VLAN ID: 5
Virtual Machine Port Group
Management-Internal
7 virtual machine(s) | VLAN ID: 200
vSZ-D-1
ruckuslab1
vSZ-H-1
VMware vCenter Server Appliance
Dev-vSZ-E_35
2008 R2 Server
Dev-vSZ-H_3.5

- When deploying an instance of vSZ-D using an OVA file, you must assign the management and data interfaces to two different network groups (vSwitch) on different subnets.



Network Mapping

What networks should the deployed template use?

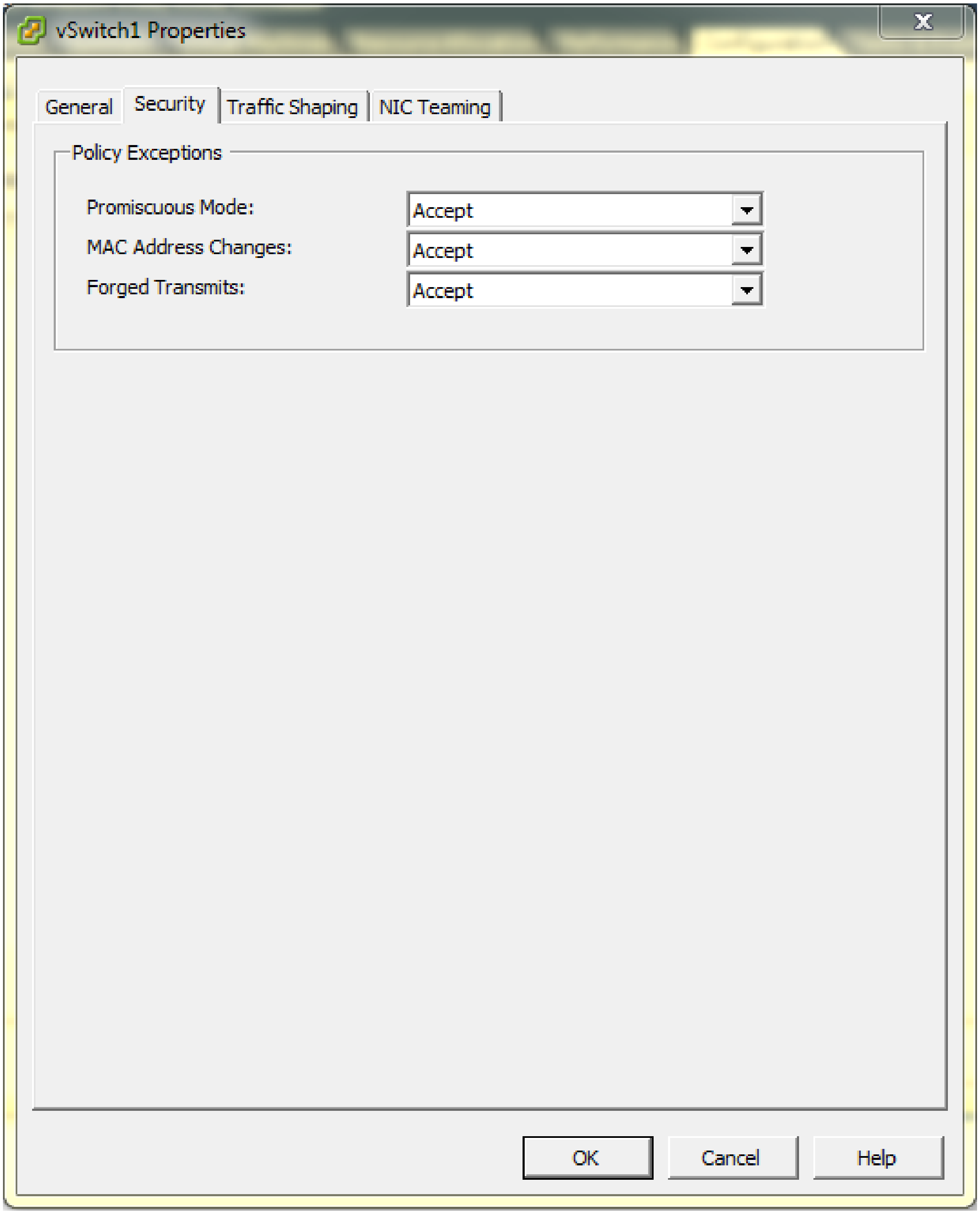
Map the networks used in this OVF template to networks in your inventory

Source Networks	Destination Networks
VM Network	VM Network
data-network	Private Test Bed

Description:

The data-network network

- Enable **Promiscuous** mode in vSwitch Config.



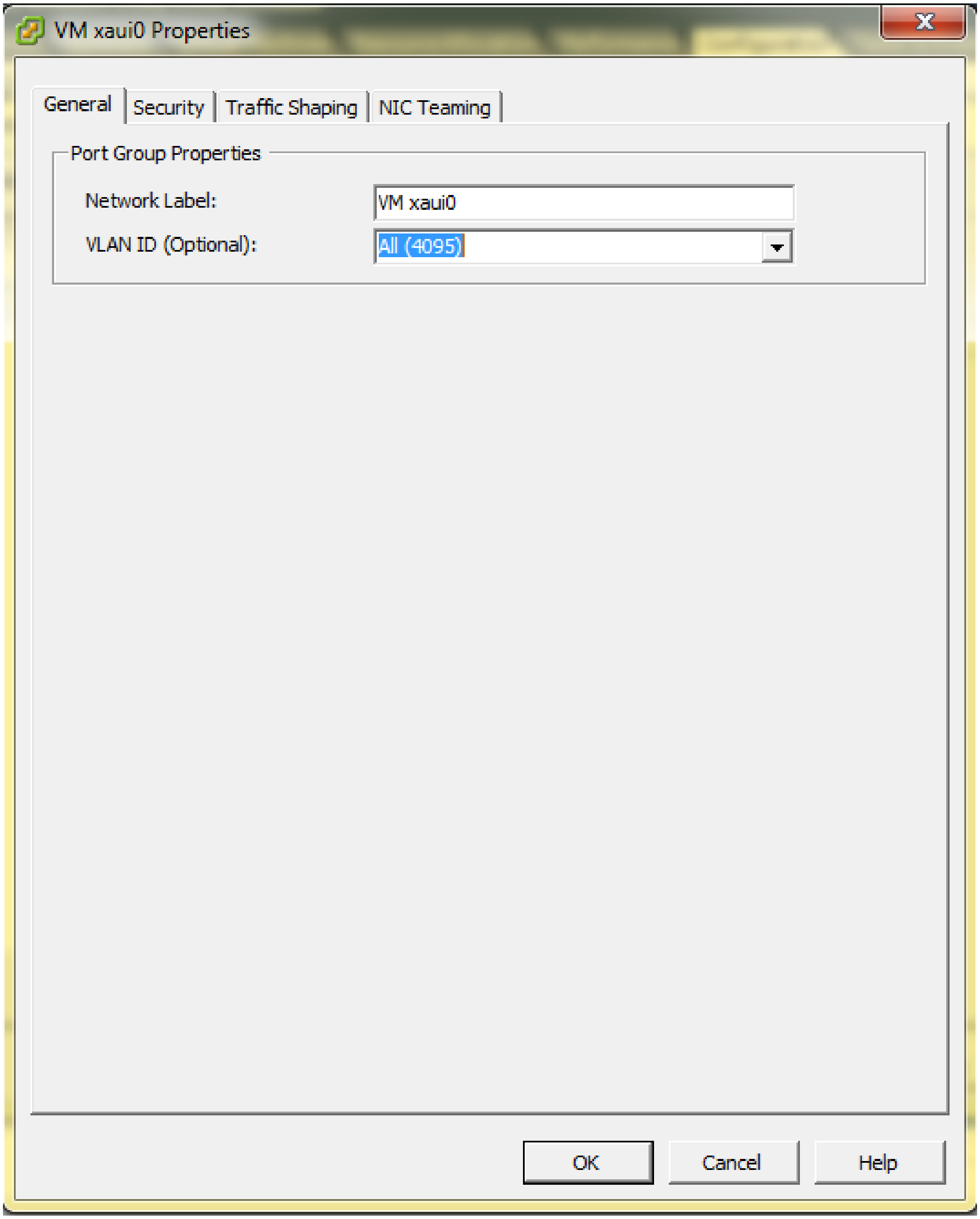
Policy Exceptions

Promiscuous Mode: Accept

MAC Address Changes: Accept

Forged Transmits: Accept

- In **vSwitch Config**, enable VLAN ID for **All**.



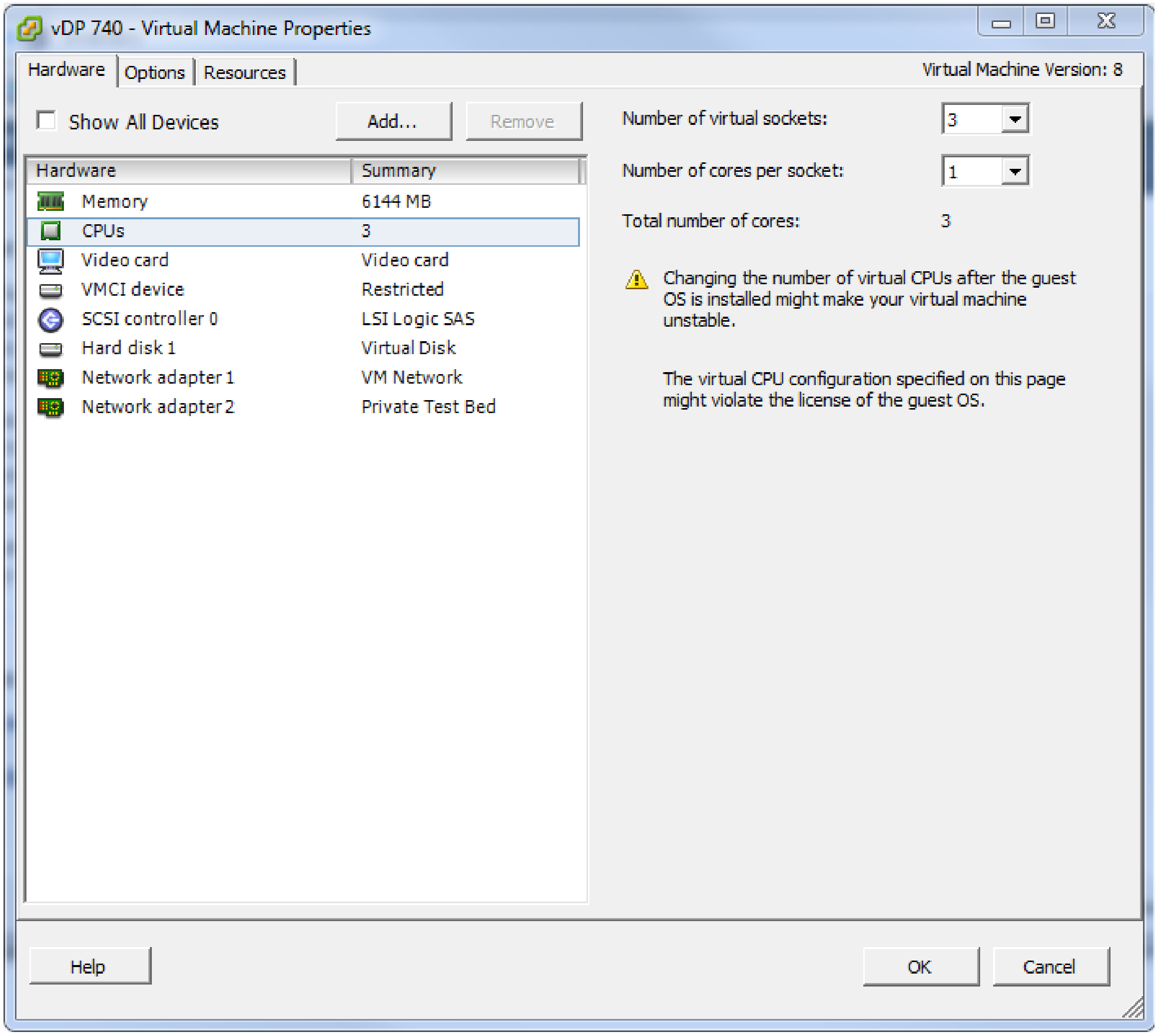
VM xaui0 Properties

Port Group Properties

Network Label: VM xaui0

VLAN ID (Optional): All (4095)

- After the vSZ-D instance is ready, modify the number of CPU cores (if needed) before powering on vSZ-D.



Hardware	Summary
Memory	6144 MB
CPUs	3
Video card	Video card
VMCI device	Restricted
SCSI controller 0	LSI Logic SAS
Hard disk 1	Virtual Disk
Network adapter 1	VM Network
Network adapter 2	Private Test Bed

Number of virtual sockets: 3

Number of cores per socket: 1

Total number of cores: 3

⚠ Changing the number of virtual CPUs after the guest OS is installed might make your virtual machine unstable.

The virtual CPU configuration specified on this page might violate the license of the guest OS.

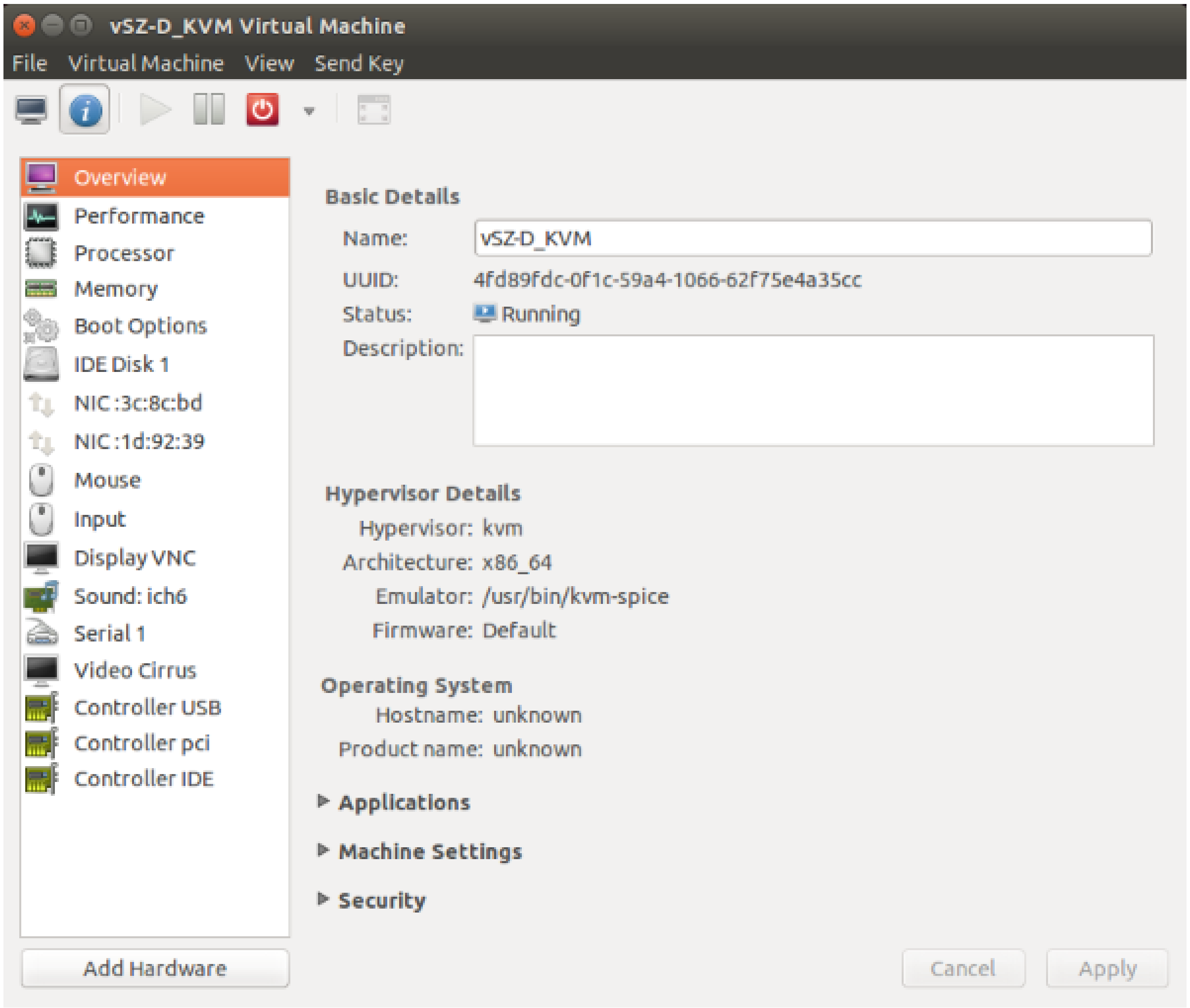
- For advanced CPU and memory resource configuration recommendations, refer to the *vSphere Resource Management Guide*, which is available on the VMware website.

KVM Specific Configuration

If you are installing a KVM on VMware, read these KVM specific configuration recommendations from Ruckus.

Hypervisor Detail

You can view the details of the hypervisor.



Basic Details

Name: vSZ-D_KVM

UUID: 4fd89fdc-0f1c-59a4-1066-62f75e4a35cc

Status: Running

Description:

Hypervisor Details

Hypervisor: kvm

Architecture: x86_64

Emulator: /usr/bin/kvm-spice

Firmware: Default

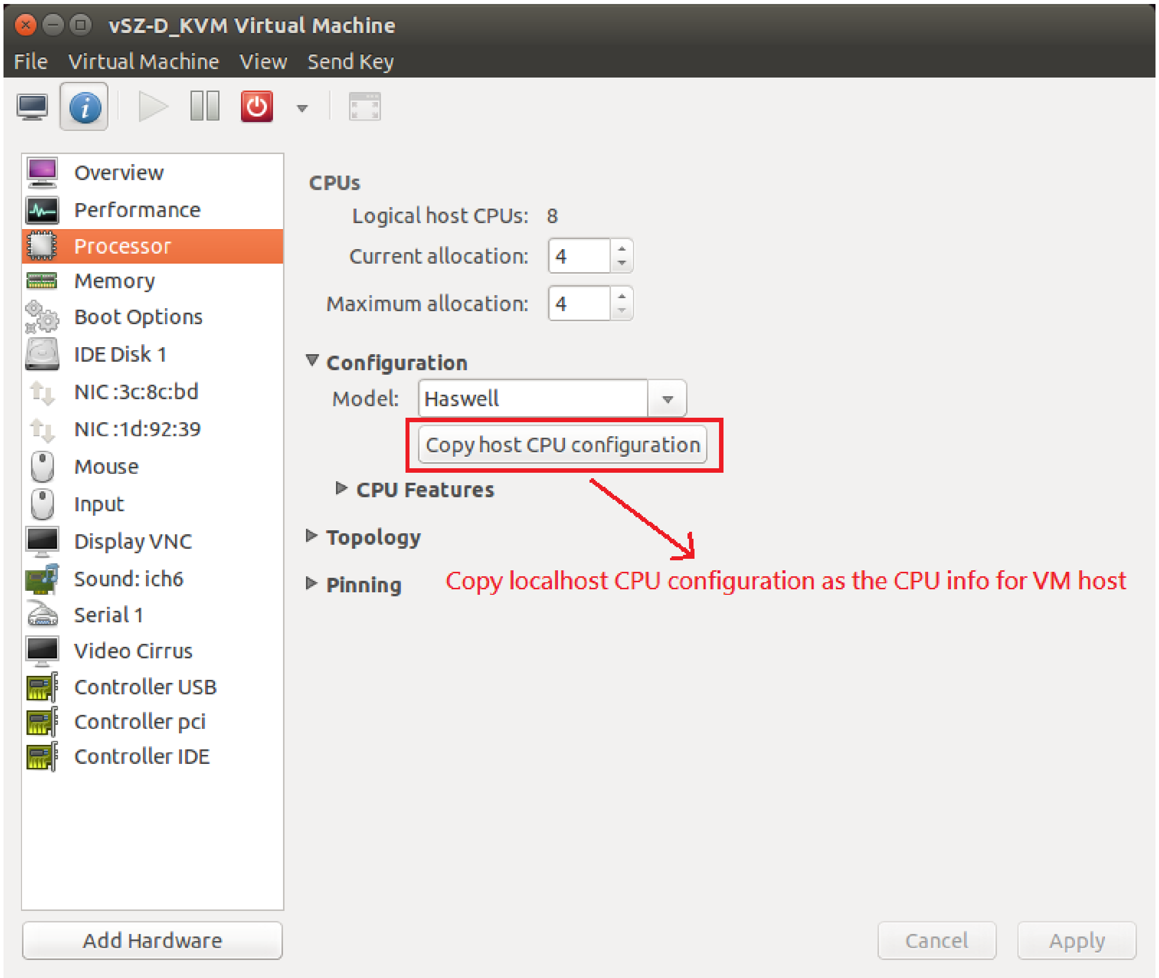
Operating System

Hostname: unknown

Product name: unknown

CPU Type

When selecting the CPU model, make sure you select one that is higher than Intel Core 2 Duo. On Linux, you can this information in `/proc/cpuinfo`.



Logical host CPUs: 8

Current allocation: 4

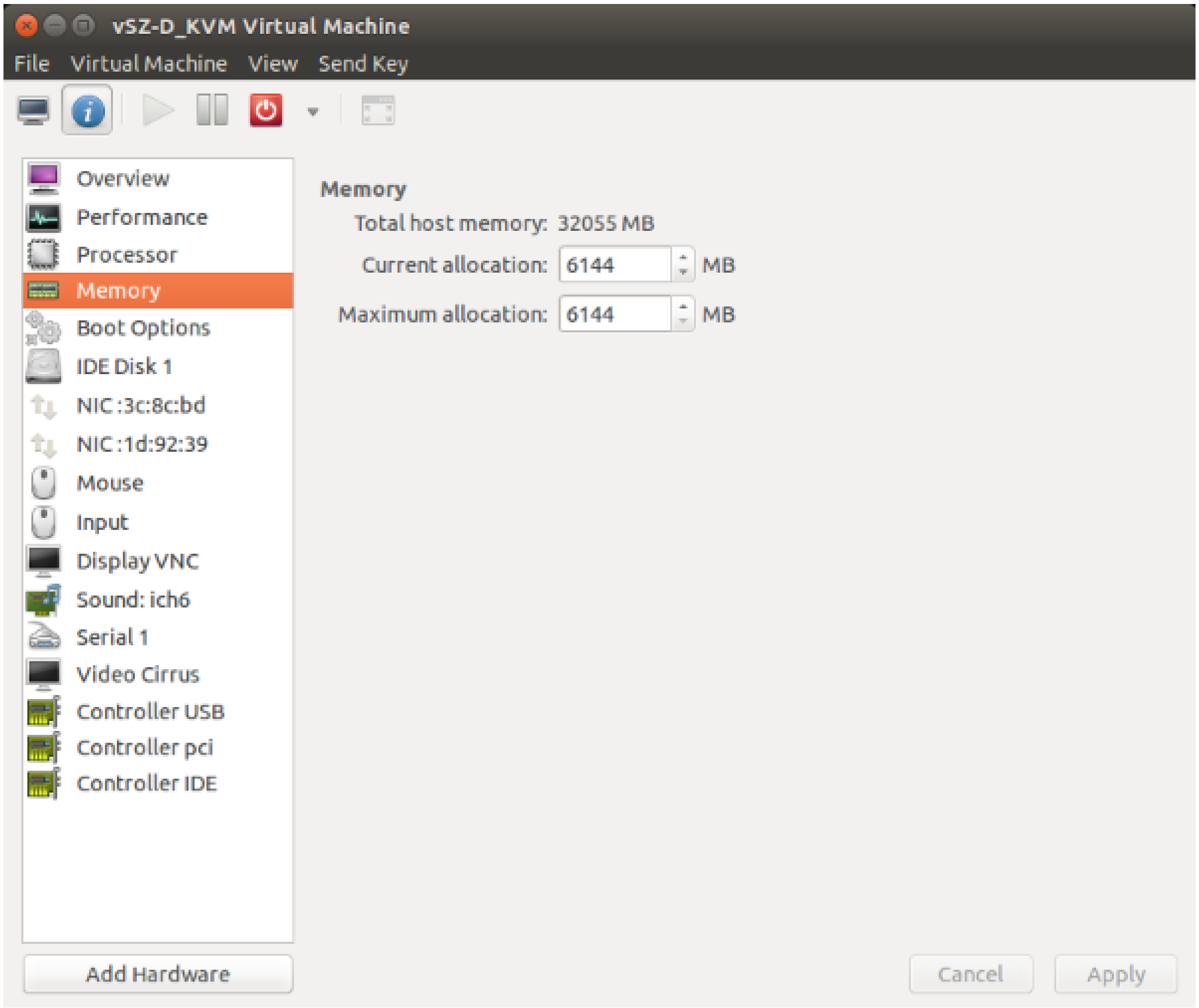
Maximum allocation: 4

Model: Haswell

Copy localhost CPU configuration as the CPU info for VM host

Memory Allocation

You must allocate a minimum of 6G (6144 MByte) memory for vSZ-D.



Memory

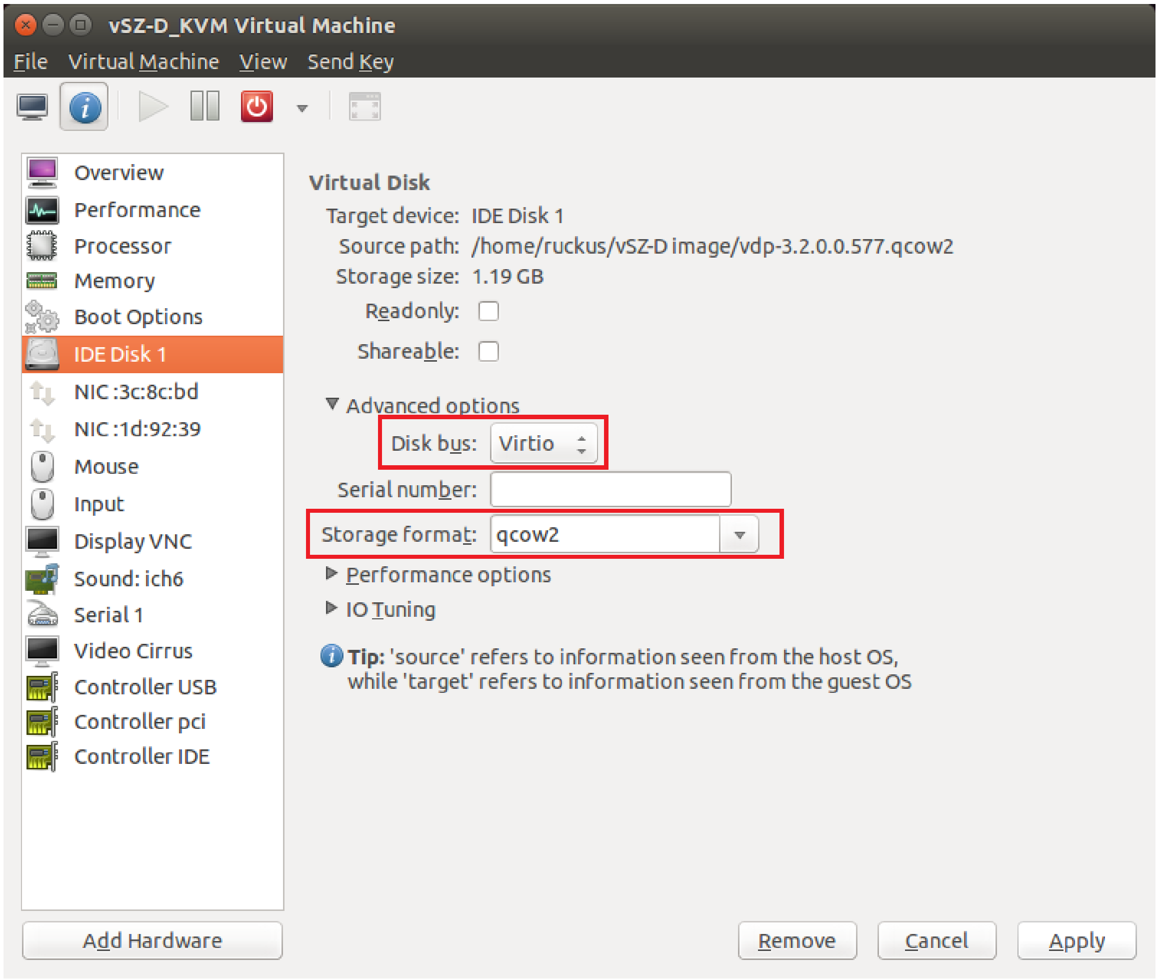
Total host memory: 32055 MB

Current allocation: 6144 MB

Maximum allocation: 6144 MB

Disk Configuration

Ruckus recommends using Virtio as the disk bus and qcow2 as the storage format.



Virtual Disk

Target device: IDE Disk 1

Source path: /home/ruckus/vSZ-D image/vdp-3.2.0.0.577.qcow2

Storage size: 1.19 GB

Readonly: □

Shareable: □

▼ Advanced options

Disk bus: Virtio

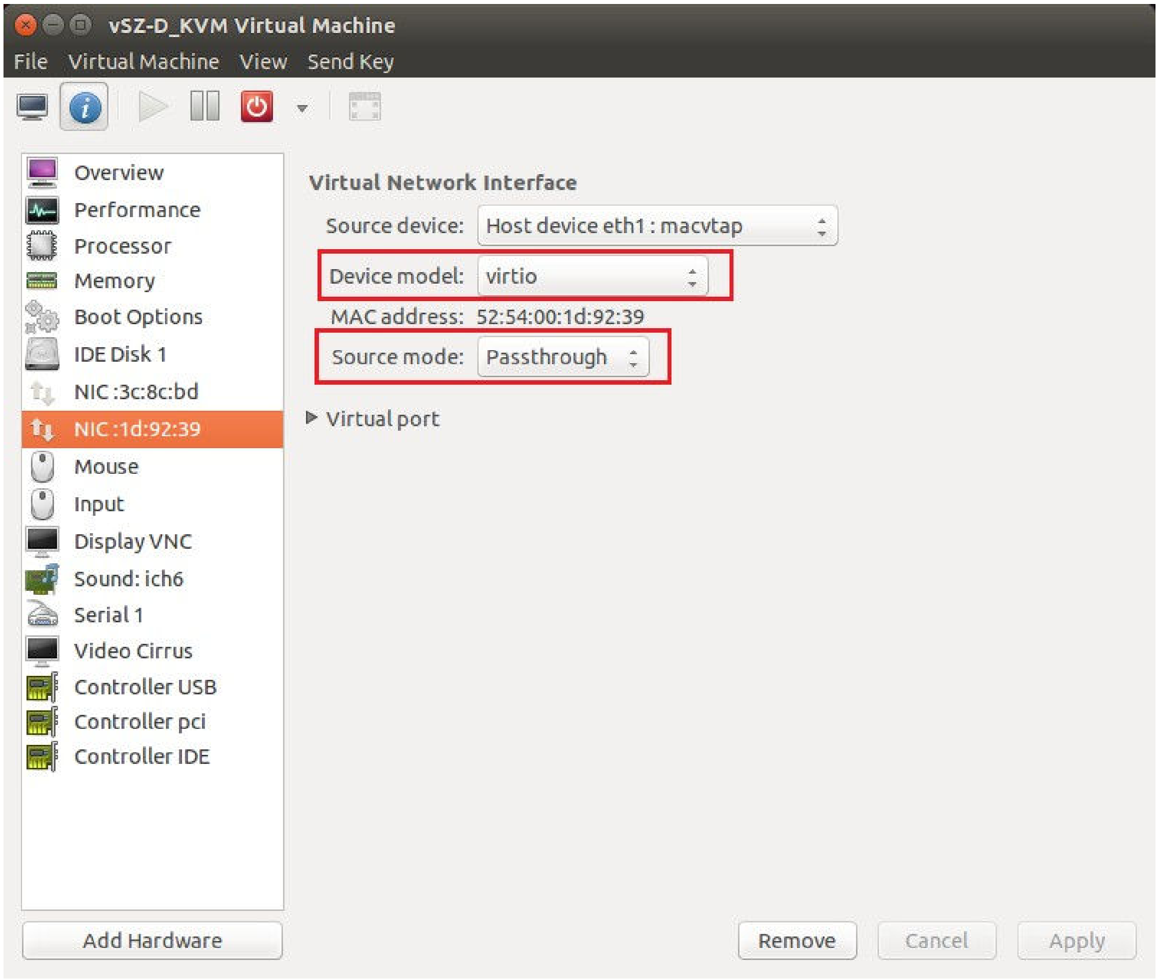
Serial number:

Storage format: qcow2

▶ Performance options

▶ IO Tuning

Tip: 'source' refers to information seen from the host OS, while 'target' refers to information seen from the guest OS



Virtual Network Interface

Source device: Host device eth1 : macvtap

Device model: virtio

MAC address: 52:54:00:1d:92:39

Source mode: Passthrough

▶ Virtual port

NIC Configuration in Direct IO Mode

NOTE
Only the data interface needs to be configured to direct PCI passthrough. The management interface should always be configured to e1000 as the NIC driver.

Before adding a PCI device to the KVM, you need to complete the following steps:

1. Enable VT-d (for Intel processors) in the motherboard BIOS. Intel's VT-d ("Intel Virtualization Technology for Directed I/O") is available on most i7 family processors.
2. Add kernel boot parameters via GRUB to enable IOMMU (see figure below). To enable IOMMU in the kernel of Intel processors, pass **intel_iommu=on** boot parameter on Linux. For more information, read this tutorial.
3. After configuring the boot parameter, reset the computer.

   You can add kernel boot parameters during boot time.

   - For Debian or Ubuntu:
     a. Edit GRUB config template at `/etc/default/grub`.
     b. Add a kernel parameter as "*name=value*" in *GRUB_CMDLINE_LINUX_DEFAULT* variable.

     ```
     $ sudo -e /etc/default/grub
     
     GRUB_CMDLINE_LINUX_DEFAULT="...... intel_iommu=on"
     ```

     c. Then run the following command to generate the GRUB config file.

     ```
     $ sudo update-grub
     ```

     If the command "update-grub" is not found, you can install it as follows:

     ```
     $ sudo apt-get install grub2-common
     ```

   - For Fedora
     a. Edit GRUB config template at `/etc/default/grub`.
     b. Add a kernel parameter as "*name=value*" in *GRUB_CMDLINE_LINUX* variable.

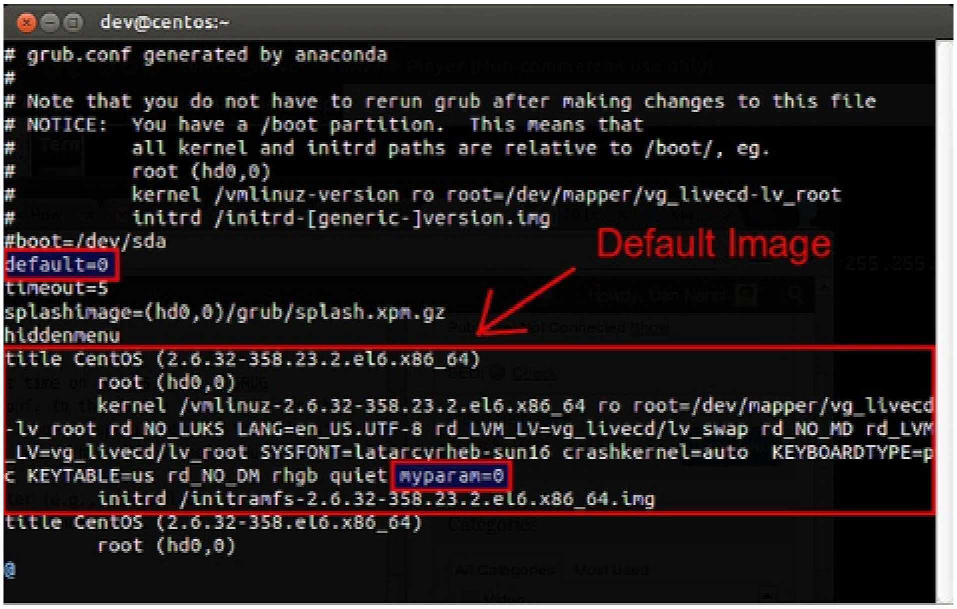
     ```
     $ sudo -e /etc/default/grub
     
     GRUB_CMDLINE_LINUX="...... intel_iommu=on"
     ```

     c. Then run the following command to generate the GRUB config file.

     ```
     $ sudo grub2-mkconfig -o /boot/grub2/grub.cfg
     ```

   - For CentOS
     a. Edit GRUB config template at `/boot/grub/grub.conf`.
     b. In the config file, look for the entry "default=N" at the top of the config file indicates which entry is the default image. On the next line, add a kernel parameter as "*name=value*" in *kernel /vmlinuz-* variable.

     ```
     kernel /vmlinuz-"...... intel_iommu=on"
     ```



```
# grub.conf generated by anaconda
#
# Note that you do not have to rerun grub after making changes to this file
# NOTICE:  You have a /boot partition.  This means that
#          all kernel and initrd paths are relative to /boot/, eg.
#          root (hd0,0)
#          kernel /vmlinuz-version ro root=/dev/mapper/vg_livecd-lv_root
#          initrd /initrd-[generic-]version.img
#boot=/dev/sda
default=0
timeout=5
splashimage=(hd0,0)/grub/splash.xpm.gz
hiddenmenu
title CentOS (2.6.32-358.23.2.el6.x86_64)
        root (hd0,0)
        kernel /vmlinuz-2.6.32-358.23.2.el6.x86_64 ro root=/dev/mapper/vg_livecd
-lv_root rd_NO_LUKS LANG=en_US.UTF-8 rd_LVM_LV=vg_livecd/lv_swap rd_NO_MD rd_LVM
_LV=vg_livecd/lv_root SYSFONT=latarcyrheb-sun16 crashkernel=auto  KEYBOARDTYPE=p
c KEYTABLE=us rd_NO_DM rhgb quiet myparam=0
        initrd /initramfs-2.6.32-358.23.2.el6.x86_64.img
title CentOS (2.6.32-358.el6.x86_64)
        root (hd0,0)
@
```

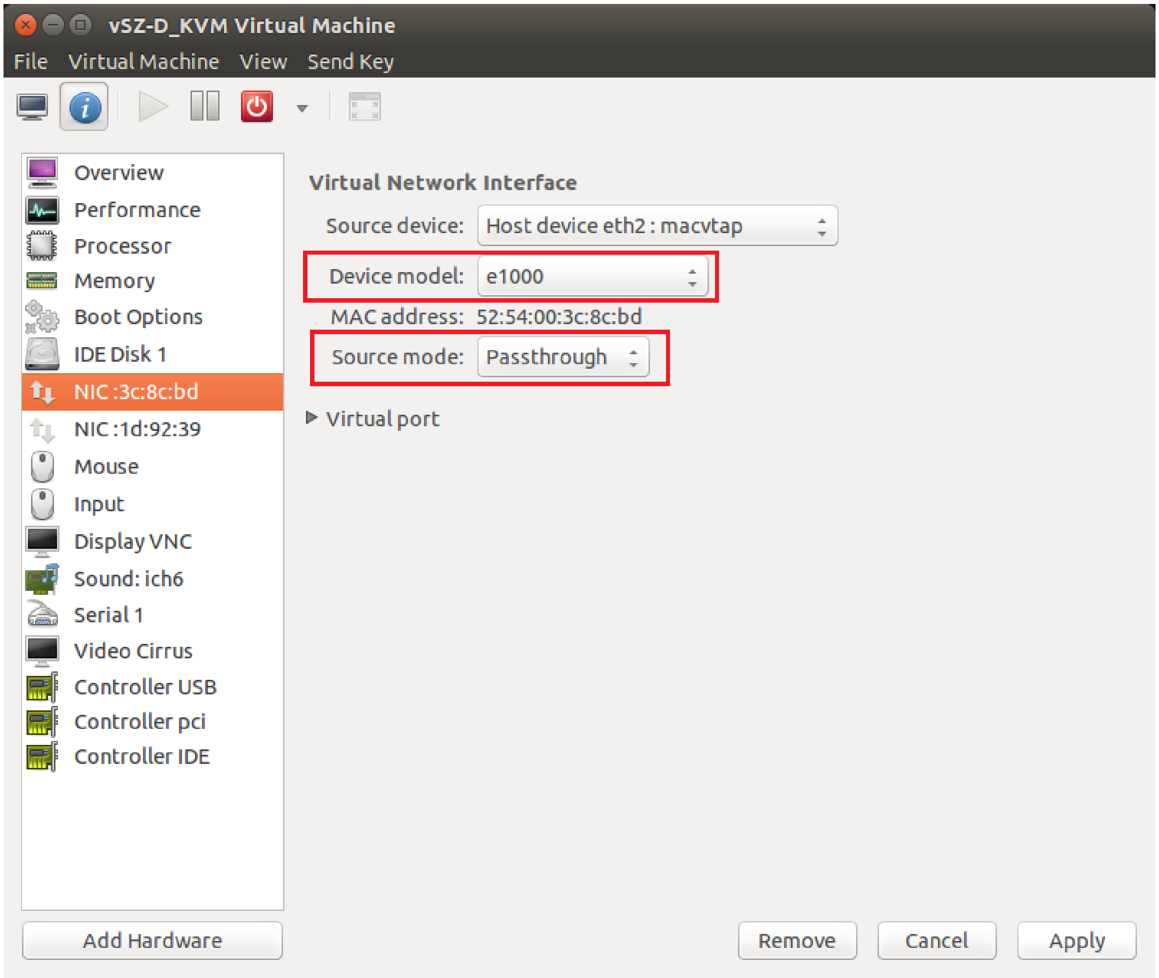
Default Image

NIC Configuration in vSwitch Mode

NOTE
Configure only two ports for vSZ-D/.

For the management interface, use the following settings:

- **Device model**: e1000
- **Source mode**: Either **Bridge** or **Passthrough** if you are using **macvtap** for the device type.



Virtual Network Interface

Source device: Host device eth2 : macvtap

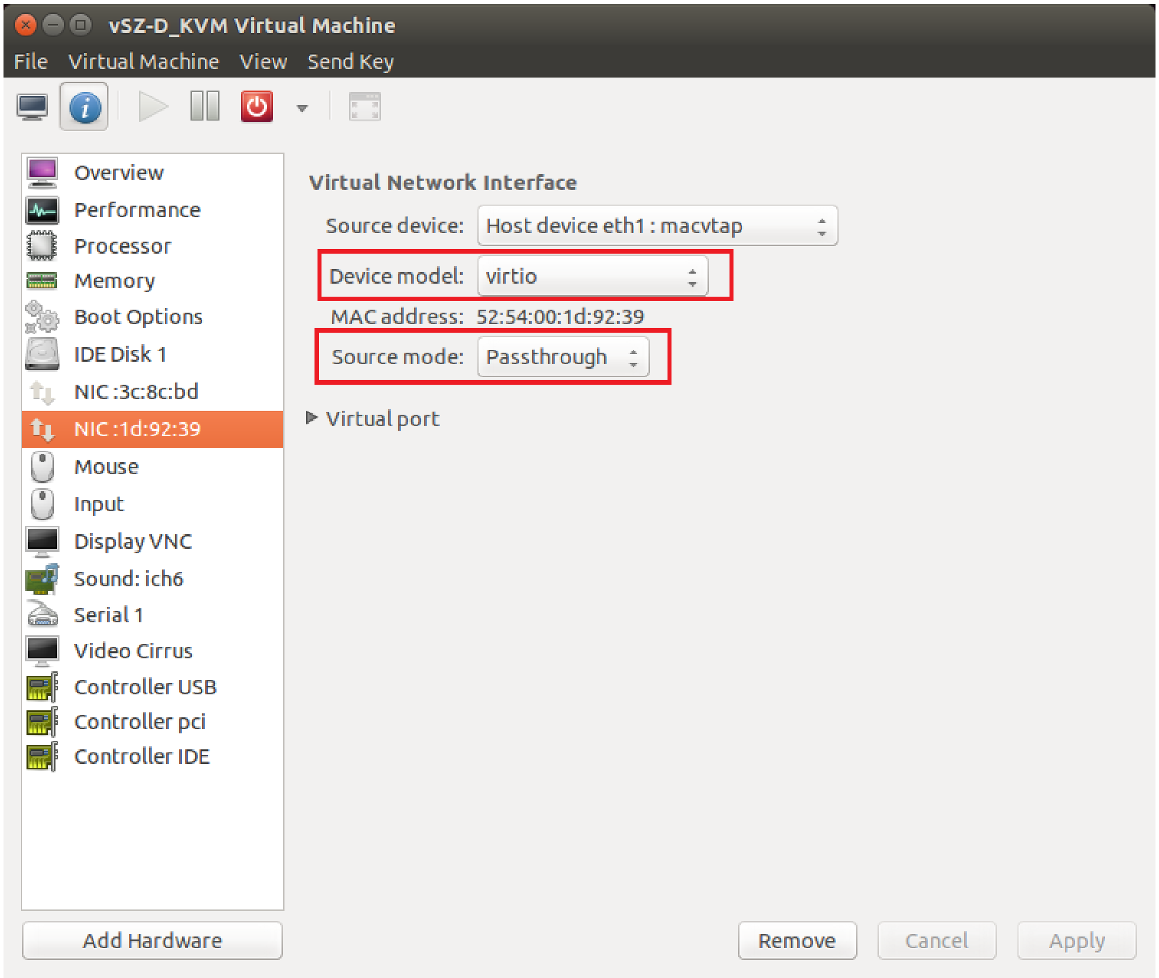
Device model: e1000

MAC address: 52:54:00:3c:8c:bd

Source mode: Passthrough

For the data interface, use the following settings:

- **Device model**: e1000
- **Source mode**: **Passthrough** if you are using macvtap for the device type. Only the passthrough mode can allow UE traffic to pass through the VM NIC.



Virtual Network Interface

Source device: Host device eth1 : macvtap

Device model: virtio

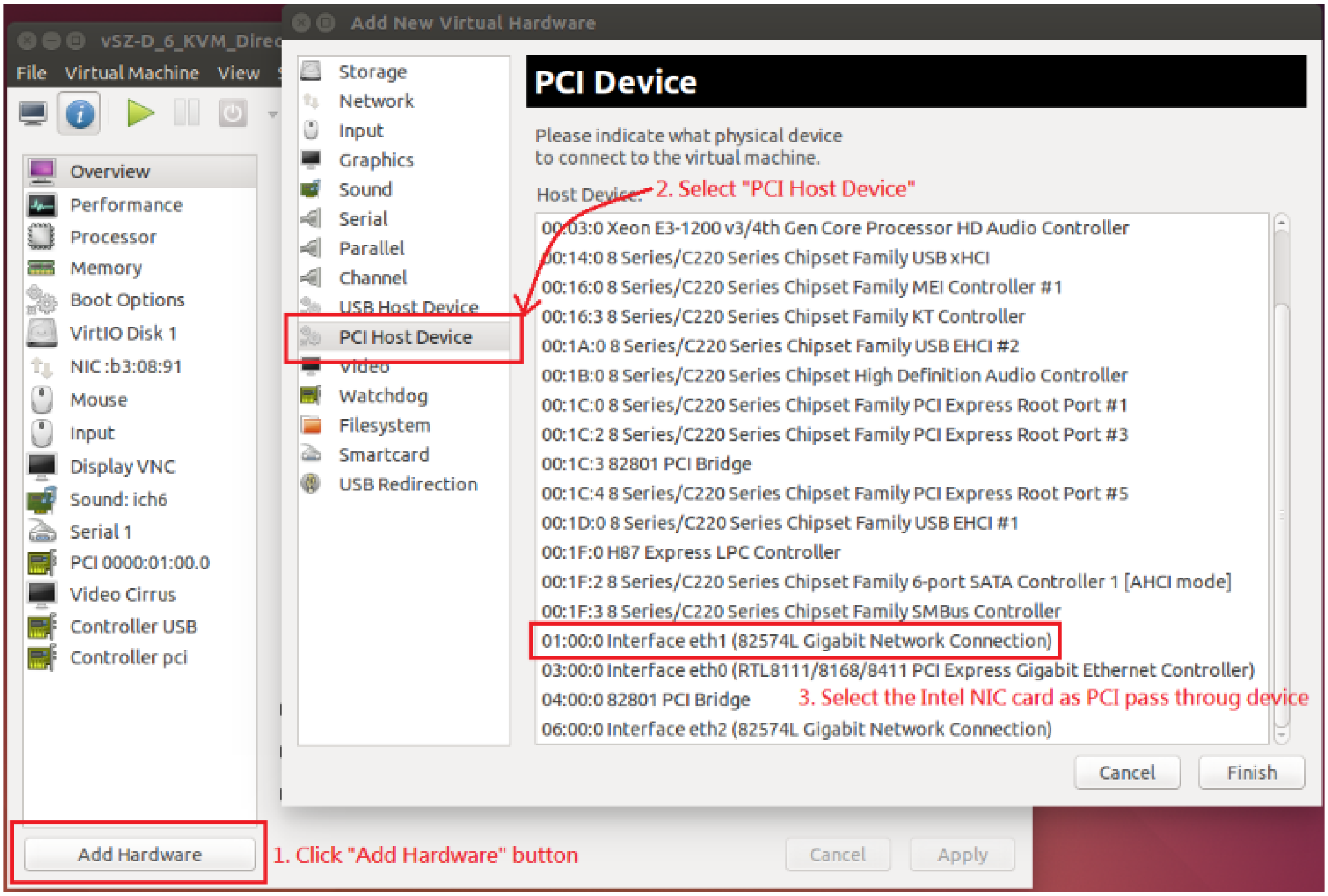
MAC address: 52:54:00:1d:92:39

Source mode: Passthrough

Adding a PCI Device to a VM on Virt-Manager

To assign a PCI device to a guest VM on virt-manager. :

1. From the VNC Viewer and click **Add Hardware** > **PCI Host Device**.
2. Choose a PCI device to assign from the PCI device list, and click **Finish**.



Please indicate what physical device
to connect to the virtual machine.

Host Device:

00:03:0 Xeon E3-1200 v3/4th Gen Core Processor HD Audio Controller
00:14:0 8 Series/C220 Series Chipset Family USB xHCI
00:16:0 8 Series/C220 Series Chipset Family MEI Controller #1
00:16:3 8 Series/C220 Series Chipset Family KT Controller
00:1A:0 8 Series/C220 Series Chipset Family USB EHCI #2
00:1B:0 8 Series/C220 Series Chipset High Definition Audio Controller
00:1C:0 8 Series/C220 Series Chipset Family PCI Express Root Port #1
00:1C:2 8 Series/C220 Series Chipset Family PCI Express Root Port #3
00:1C:3 82801 PCI Bridge
00:1C:4 8 Series/C220 Series Chipset Family PCI Express Root Port #5
00:1D:0 8 Series/C220 Series Chipset Family USB EHCI #1
00:1F:0 H87 Express LPC Controller
00:1F:2 8 Series/C220 Series Chipset Family 6-port SATA Controller 1 [AHCI mode]
00:1F:3 8 Series/C220 Series Chipset Family SMBus Controller
01:00:0 Interface eth1 (82574L Gigabit Network Connection)
03:00:0 Interface eth0 (RTL8111/8168/8411 PCI Express Gigabit Ethernet Controller)
04:00:0 82801 PCI Bridge
06:00:0 Interface eth2 (82574L Gigabit Network Connection)

1. Click "Add Hardware" button

2. Select "PCI Host Device"

3. Select the Intel NIC card as PCI pass throug device

3. Power on the guest and the host PCI device would be visible in the guest VM.

NIC Card Setting

You must use only two ports.

	Management Interface	Data Interface
KVM w/ vSwitch	e1000	virtio
KVM w/ pci passthrough	e1000	1G: igb 10G:ixgbe
VMware w/ vSwitch	e1000 e1000e	VMXNET3
VMware w/ pci passthrough	e1000 e1000e	1G:igb 10G:ixgbe

Deployment of vSZ

Deploy vSZ-D with 40GB NIC on ESXi Server

Deploy vSZ-D with 40GB NIC on ESXi Server

Hardware Requirement and Prerequisite

The following are the hardware and prerequisite for deploying vSZ-D on ESXi 6.7

Hardware Requirement

1. DELL Inc. PowerEdge R530
2. ESXi Server License 6.7
3. Broadcom NetXtreme BCM5720 Gigabit Ethernet NIC
4. Intel Ethernet XL710 for 40GbE QSFP+
5. CPU minimum 4 cores
6. vSphere ESXi Server 6.7 or later
7. 1 or 2 vNICs
8. 8 GB memory
9. 128 GB Hard disk

Prerequisite

- A hypervisor on ESXi to install vSZ-D. Recommended version is ESXi 6.7 and later.
- Download the vSZ-D package (.OVA file) from Ruckus support .
- The IP addresses, netmask, gateway, DNS, DHCP and NAT support for vSZ-D.
- Before you power on vSZ-D, ensure that the networking is configured on ESXi.
- Recommended to use static network addresses that are assigned to vSZ-D during setup.

  NOTE
  Due to different servers and NIC, the deployment procedure mentioned in this section is for reference.

Topology

The network topologies for vSZ-D deployment on ESXi 6.7 server.

The following are basic topologies for setting up vSZ-D. Based on your requirement you can choose any of the alternatives between one IP domain to three separate domains for deployment.

The below topology shows the different IP addresses for the domains.

FIGURE 22 Three different IP addresses setup

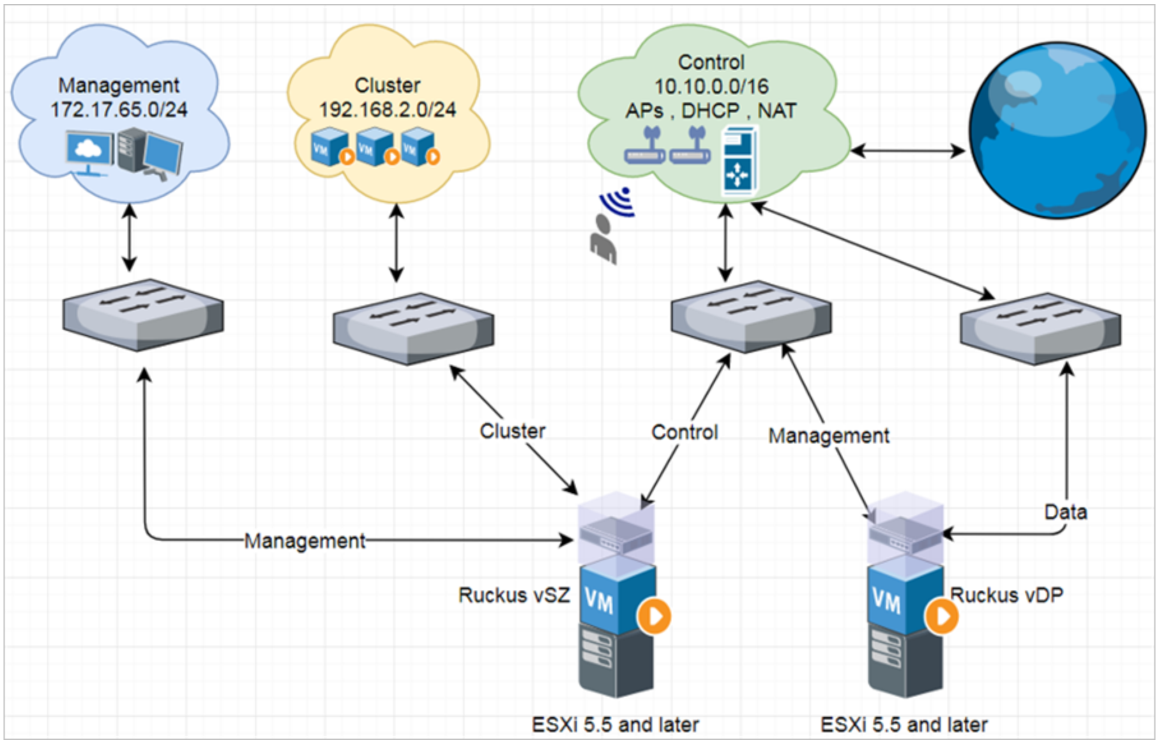
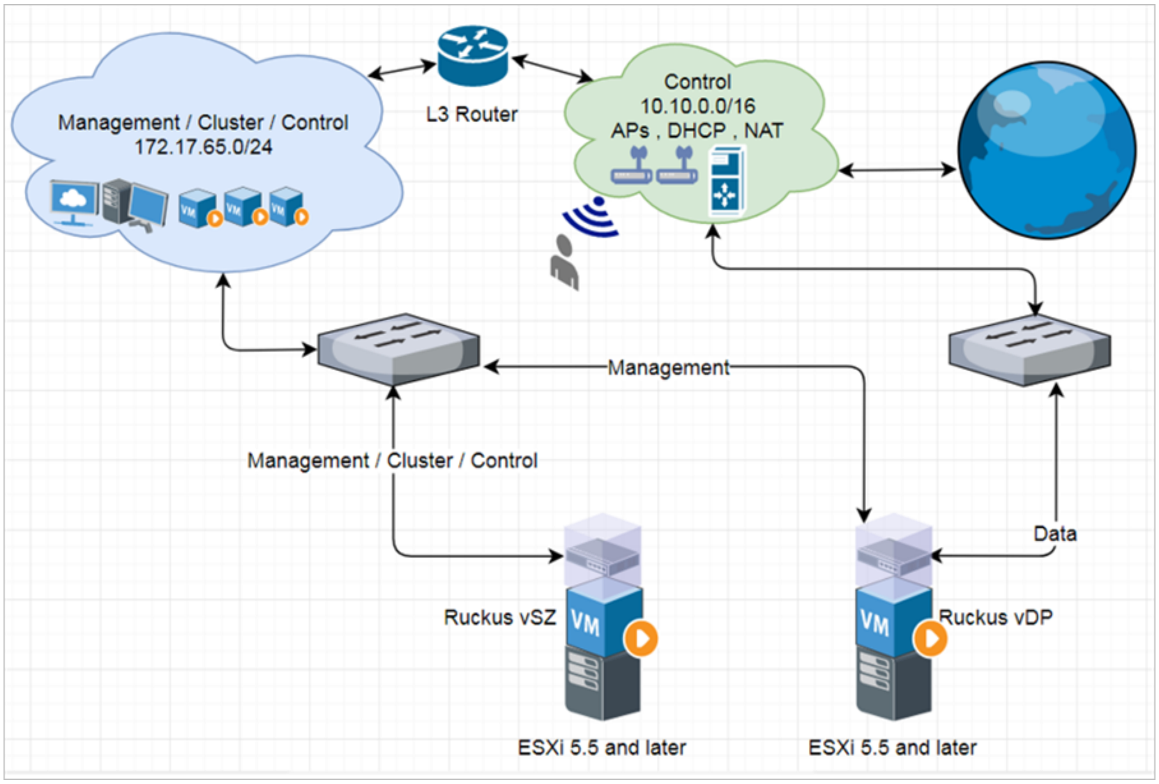
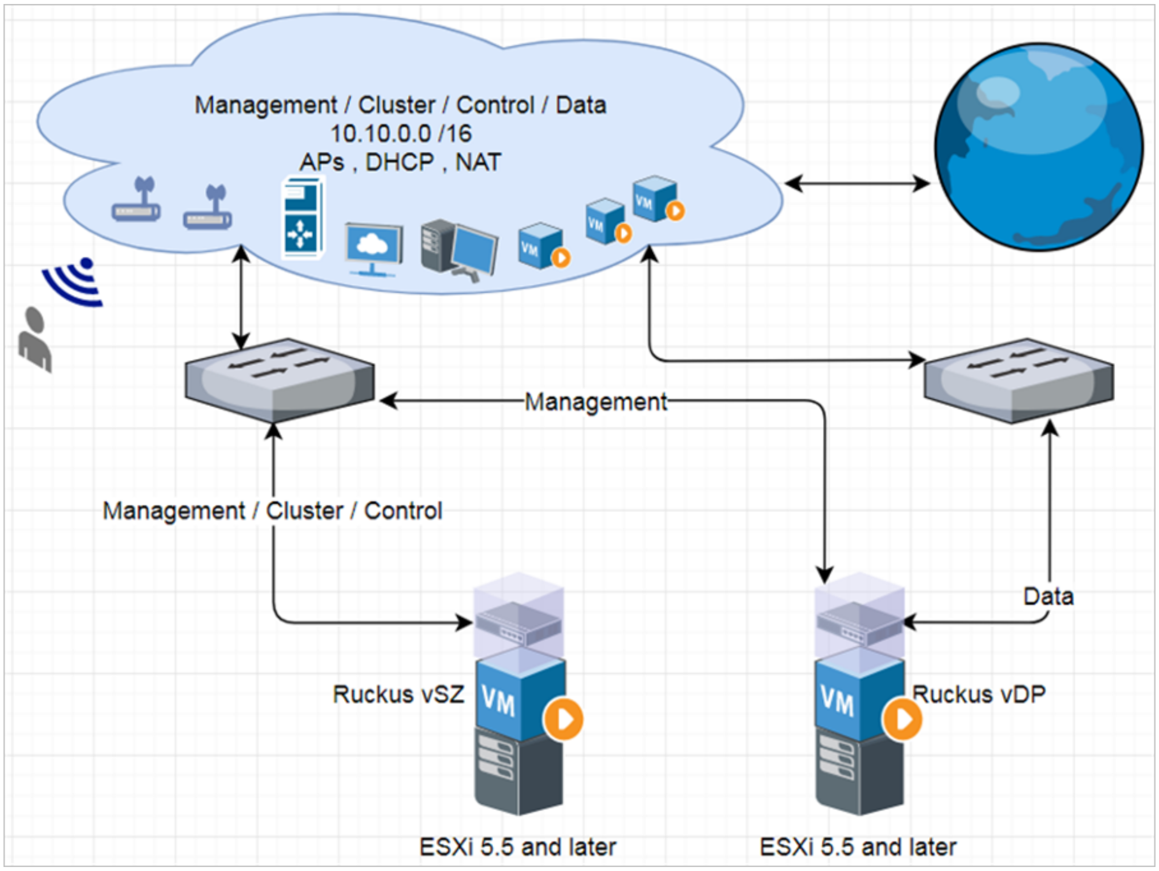


FIGURE 23 Two different domain IP addresses setup



The below topology shows the same IP addresses for the all the interfaces.

FIGURE 24 The same IP addresses setup



Deployment Procedure

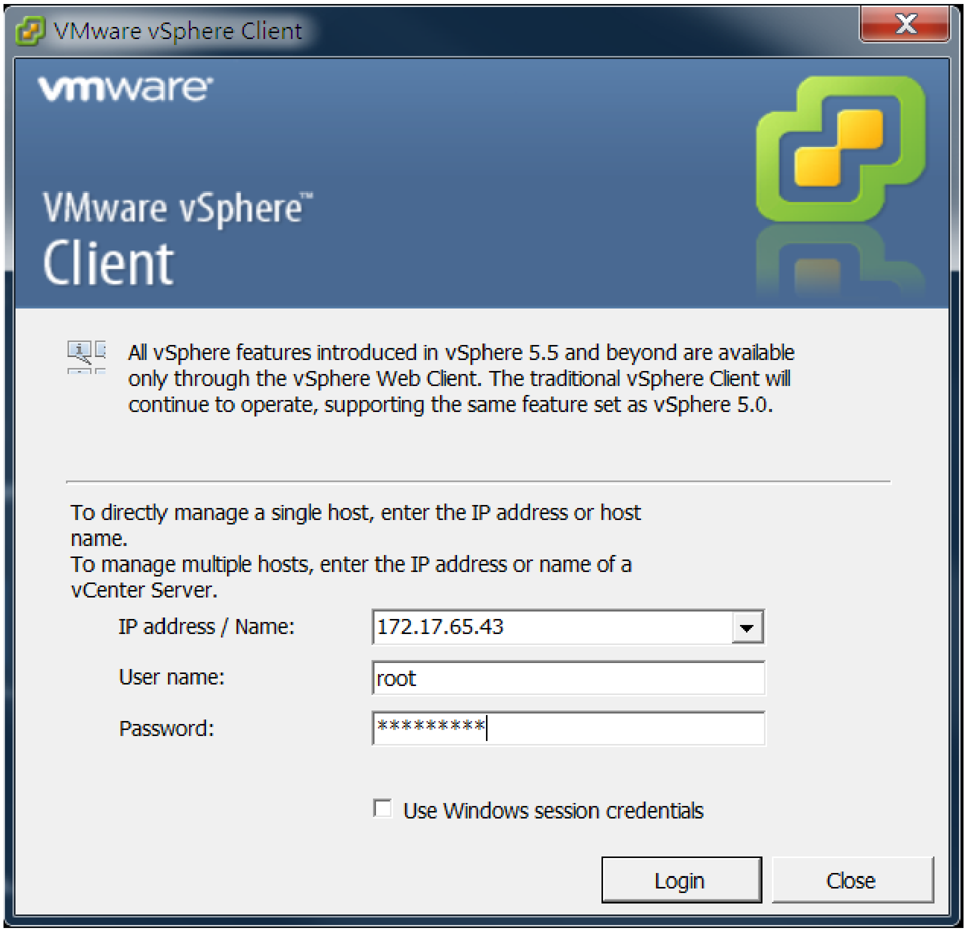
The following are basic instructions for setting up the controller on the ESXi server.

VMware ESXi 6.7 is installed and working.

For this deployment two different IP address domains are considered for controller interfaces. Refer to Topology on page 65

1. Login to the server through vSphere client tool as seen below.

FIGURE 25 Login to vSphere



All vSphere features introduced in vSphere 5.5 and beyond are available only through the vSphere Web Client. The traditional vSphere Client will continue to operate, supporting the same feature set as vSphere 5.0.

To directly manage a single host, enter the IP address or host name.
To manage multiple hosts, enter the IP address or name of a vCenter Server.

IP address / Name: 172.17.65.43

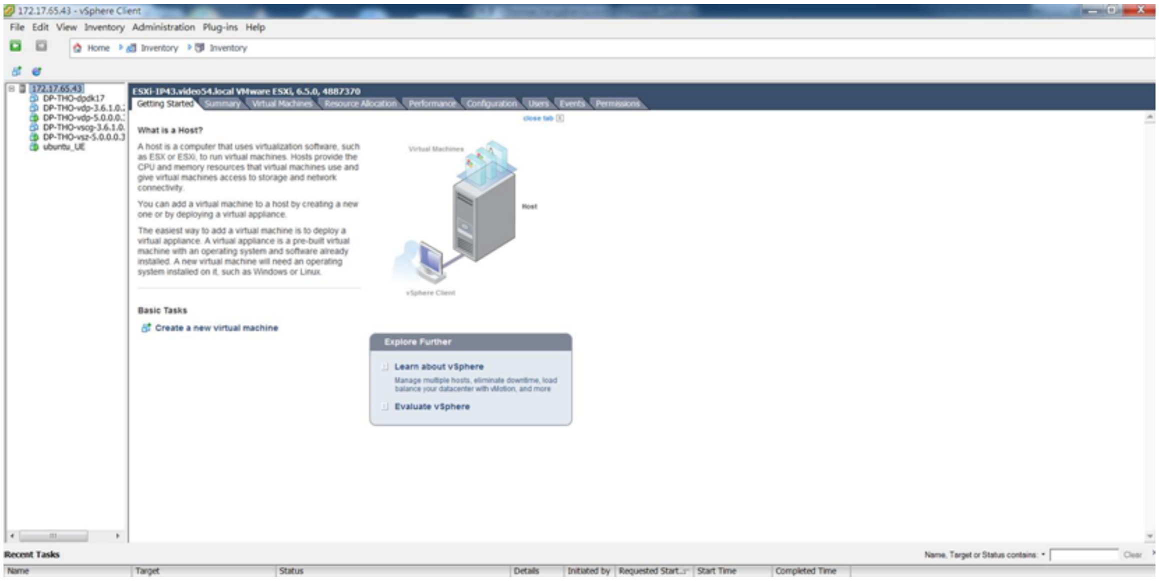
User name: root

Password: *********

□ Use Windows session credentials

The vSphere Client management page appears as shown in the following figure.

FIGURE 26 vSphere Client management page



What is a Host?

A host is a computer that uses virtualization software, such as ESX or ESXi, to run virtual machines. Hosts provide the CPU and memory resources that virtual machines use and give virtual machines access to storage and network connectivity.

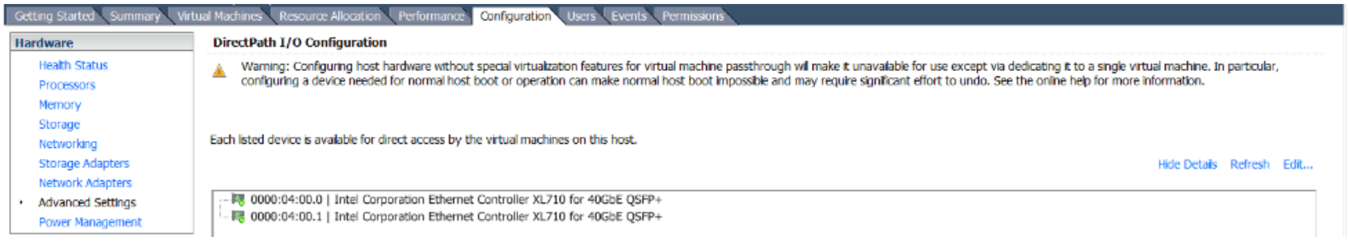
You can add a virtual machine to a host by creating a new one or by deploying a virtual appliance.

The easiest way to add a virtual machine is to deploy a virtual appliance. A virtual appliance is a pre-built virtual machine with an operating system and software already installed. A new virtual machine will need an operating system installed on it, such as Windows or Linux.

Manage multiple hosts, eliminate downtime, load balance your datacenter with vMotion, and more

2. Navigate to **Configuration** > **Advanced Settings** > **Edit**.

   The **DirectPath I/O Configuration** page appears.



DirectPath I/O Configuration

Warning: Configuring host hardware without special virtualization features for virtual machine passthrough will make it unavailable for use except via dedicating it to a single virtual machine. In particular, configuring a device needed for normal host boot or operation can make normal host boot impossible and may require significant effort to undo. See the online help for more information.

Each listed device is available for direct access by the virtual machines on this host.

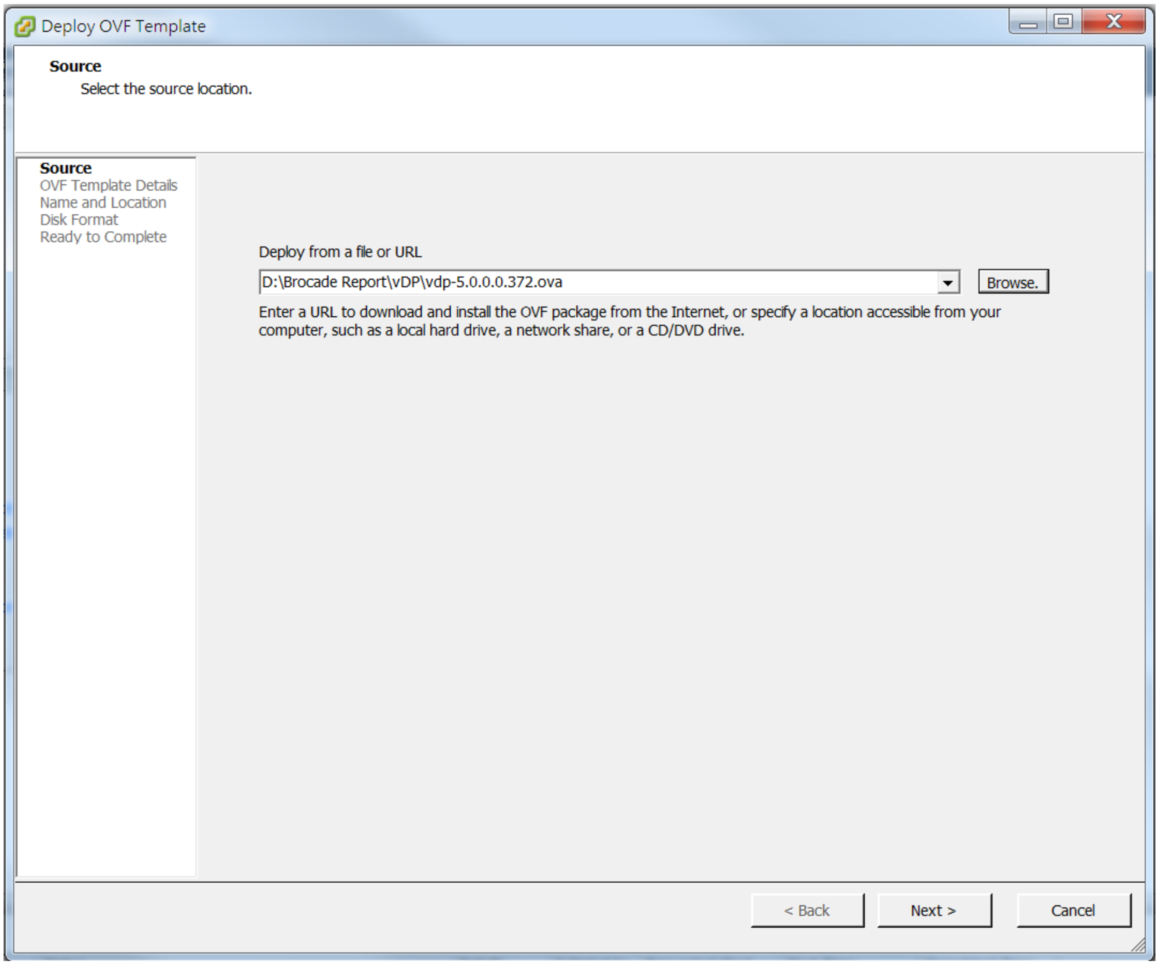
0000:04:00.0 | Intel Corporation Ethernet Controller XL710 for 40GbE QSFP+
0000:04:00.1 | Intel Corporation Ethernet Controller XL710 for 40GbE QSFP+

3. Select **XL710 40GbE QSFP+** ports and reboot vSphere server.

4. Download the controller (.ova file) from Ruckus support .

   NOTE
   You must deploy the controller directly from the .ova file. Copying an instance of the controller from another controller template might not function properly.

FIGURE 27 Deploy the file



Source
Select the source location.

Deploy from a file or URL

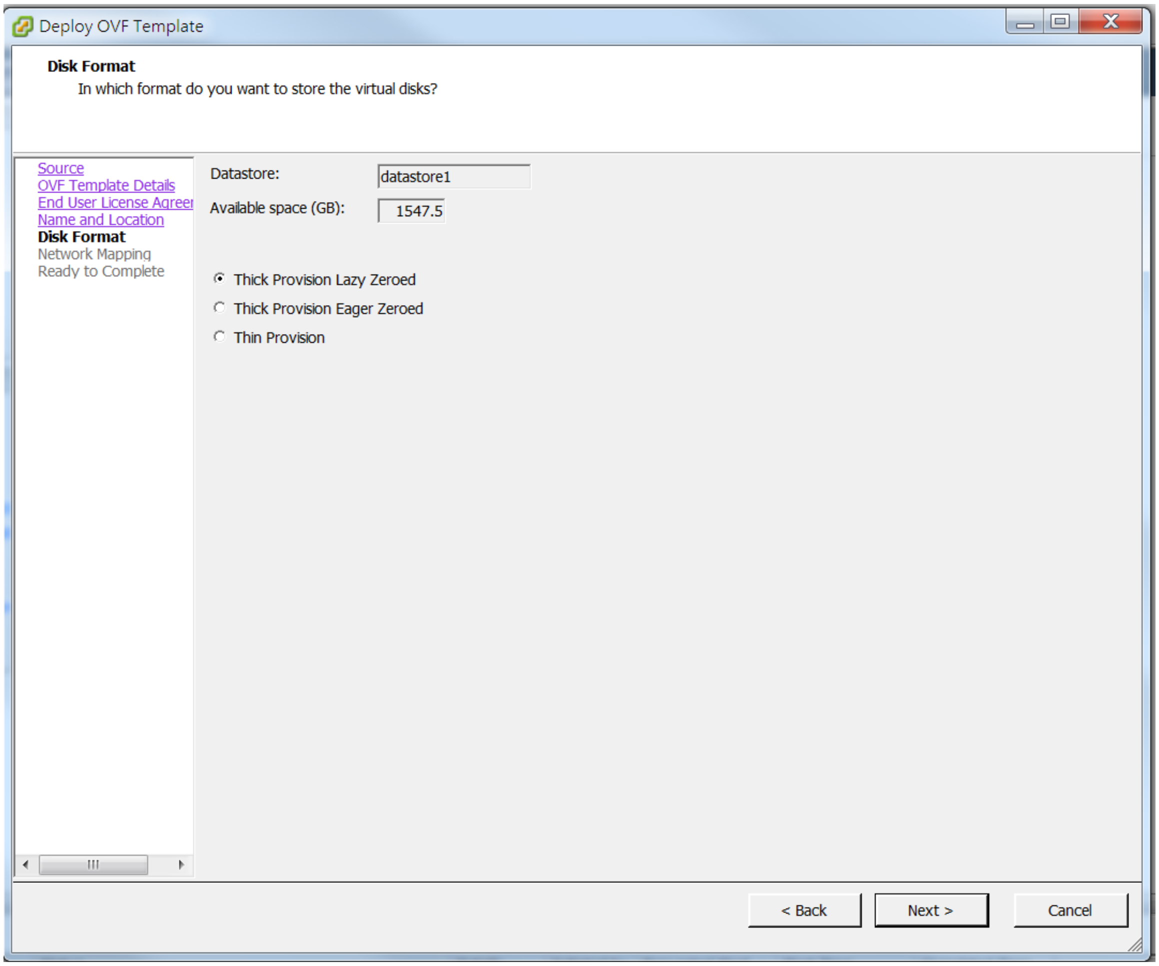
D:\Brocade Report\vDP\vdp-5.0.0.0.372.ova

Enter a URL to download and install the OVF package from the Internet, or specify a location accessible from your computer, such as a local hard drive, a network share, or a CD/DVD drive.

5. Click **Browse**, to select the source location and upload the .ova file.
6. Click **Next.**

7. Enter the vSZ datastore name and choose the disk format as seen below.

FIGURE 28 Choose the disk format



Deploy OVF Template

Disk Format

In which format do you want to store the virtual disks?

Datastore: datastore1

Available space (GB): 1547.5

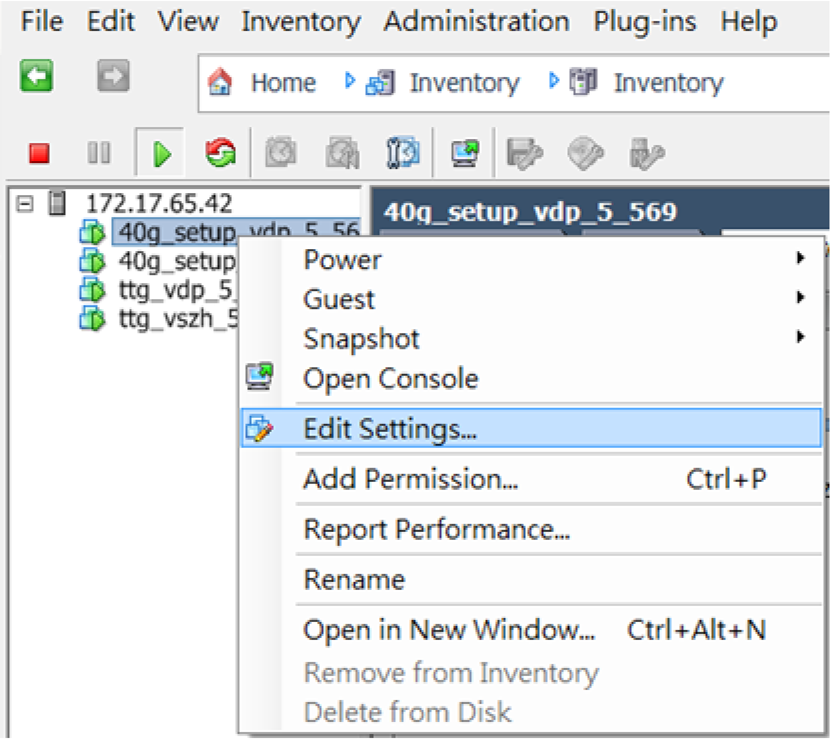
● Thick Provision Lazy Zeroed

○ Thick Provision Eager Zeroed

○ Thin Provision

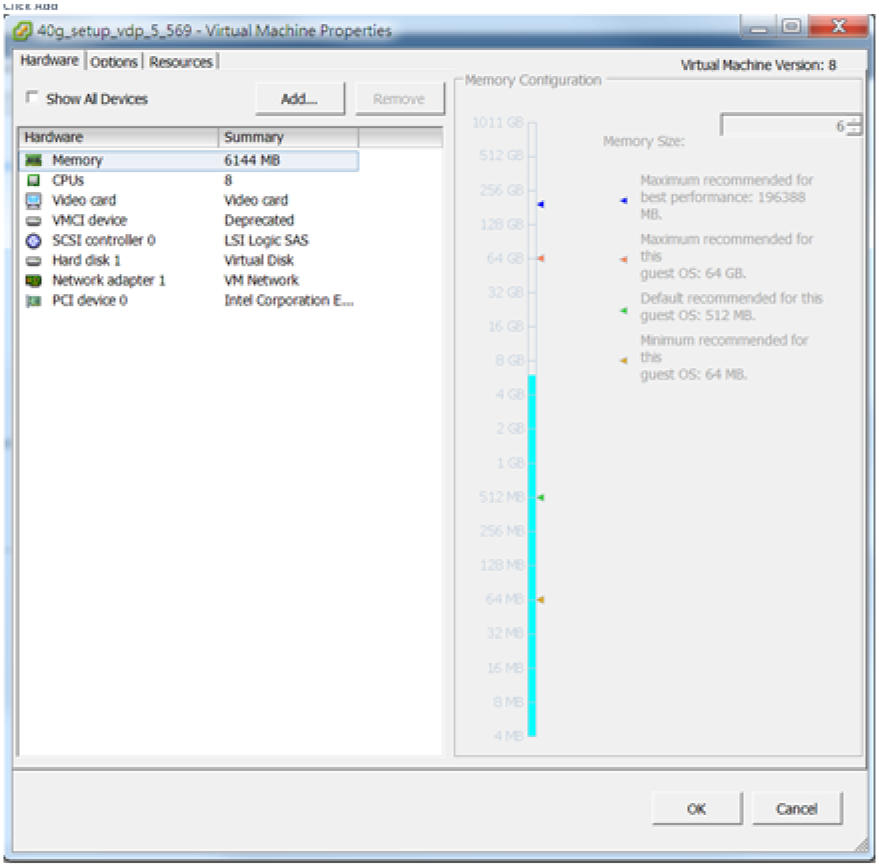
8. Click **Next.**

9. From the controller, right-click the VM and select **Edit Settings**.



The Virtual Machine Properties dialog opens.

10. Select the destination network for each network source and click **Add** as shown in the following image.



40g_setup_vdp_5_569 - Virtual Machine Properties

Hardware | Options | Resources — Virtual Machine Version: 8

□ Show All Devices — Add... — Remove

Hardware	Summary
Memory	6144 MB
CPUs	8
Video card	Video card
VMCI device	Deprecated
SCSI controller 0	LSI Logic SAS
Hard disk 1	Virtual Disk
Network adapter 1	VM Network
PCI device 0	Intel Corporation E...

Memory Configuration

Memory Size: 6

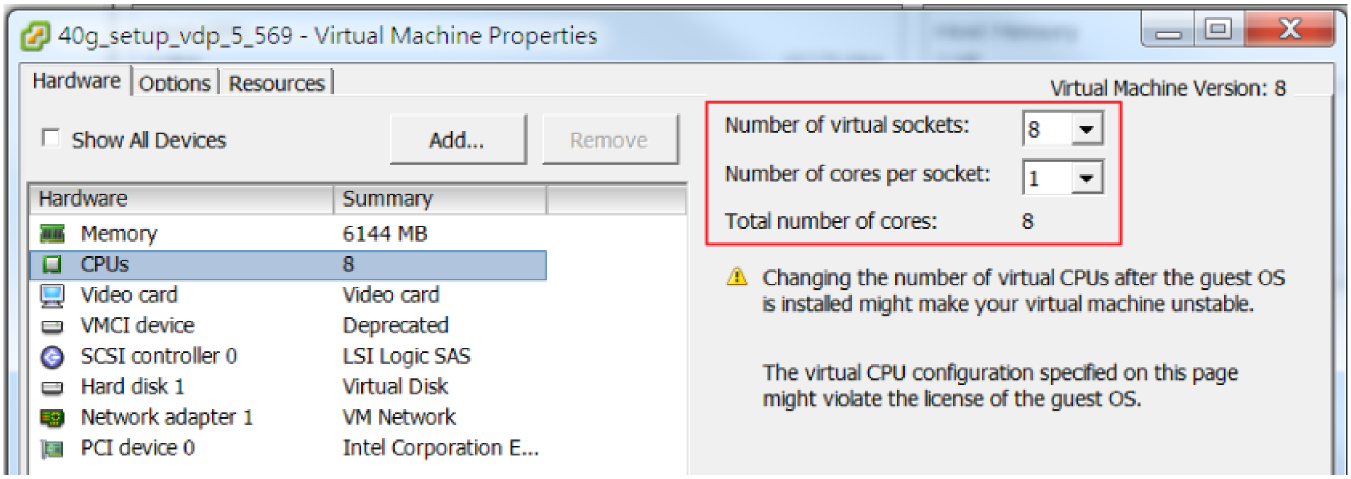
Maximum recommended for best performance: 196388 MB.

Maximum recommended for this guest OS: 64 GB.

Default recommended for this guest OS: 512 MB.

Minimum recommended for this guest OS: 64 MB.

11. For 40Gb throughput performance , select total number of CPU cores to **8**.



40g_setup_vdp_5_569 - Virtual Machine Properties

Hardware | Options | Resources — Virtual Machine Version: 8

□ Show All Devices — Add... — Remove

Hardware	Summary
Memory	6144 MB
CPUs	8
Video card	Video card
VMCI device	Deprecated
SCSI controller 0	LSI Logic SAS
Hard disk 1	Virtual Disk
Network adapter 1	VM Network
PCI device 0	Intel Corporation E...

Number of virtual sockets: 8

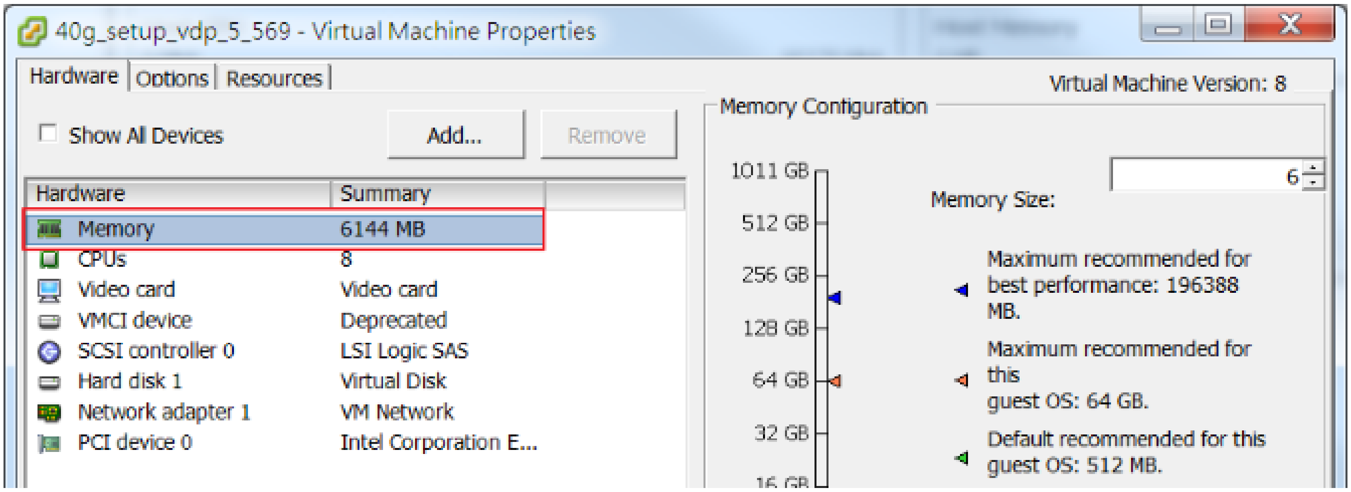
Number of cores per socket: 1

Total number of cores: 8

⚠ Changing the number of virtual CPUs after the guest OS is installed might make your virtual machine unstable.

The virtual CPU configuration specified on this page might violate the license of the guest OS.

12. Select 6GB memory size.



Hardware	Summary
Memory	6144 MB
CPUs	8
Video card	Video card
VMCI device	Deprecated
SCSI controller 0	LSI Logic SAS
Hard disk 1	Virtual Disk
Network adapter 1	VM Network
PCI device 0	Intel Corporation E...

Memory Size: 6

Maximum recommended for best performance: 196388 MB.

Maximum recommended for this guest OS: 64 GB.

Default recommended for this guest OS: 512 MB.

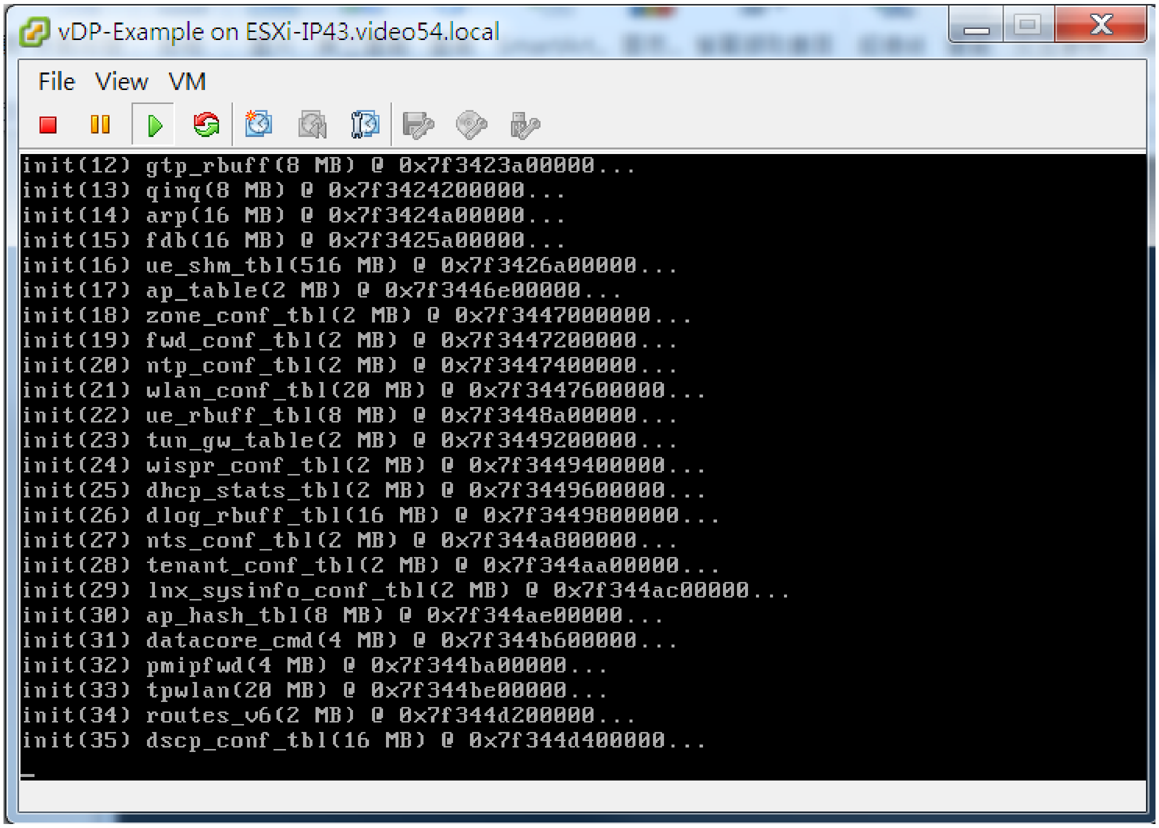
13. Click **OK** to start the deployment.
14. The deployment progress is displayed. On successful deployment, by default the controller now supports two network interfaces for management and data.

vSZ-D/SZ100-D Connect to vSZ Using CLI

Follow the below procedures for vSZ-D/SZ100-D to connect to vSZ.

Open a CLI console window to run the deployed vSZ-D/SZ100-D.

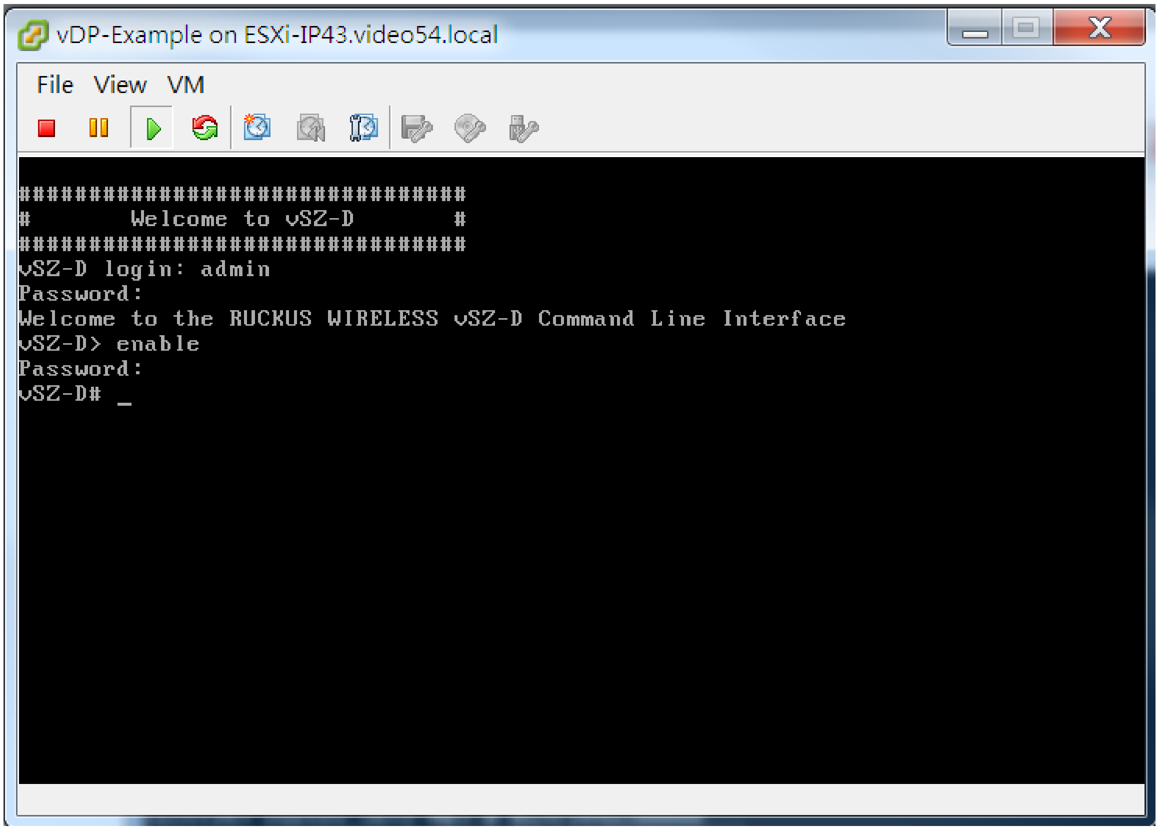
FIGURE 29 Run vSZ-D/SZ100-D on the console



```
init(12) gtp_rbuff(8 MB) @ 0x7f3423a00000...
init(13) qinq(8 MB) @ 0x7f3424200000...
init(14) arp(16 MB) @ 0x7f3424a00000...
init(15) fdb(16 MB) @ 0x7f3425a00000...
init(16) ue_shm_tbl(516 MB) @ 0x7f3426a00000...
init(17) ap_table(2 MB) @ 0x7f3446e00000...
init(18) zone_conf_tbl(2 MB) @ 0x7f3447000000...
init(19) fwd_conf_tbl(2 MB) @ 0x7f3447200000...
init(20) ntp_conf_tbl(2 MB) @ 0x7f3447400000...
init(21) wlan_conf_tbl(20 MB) @ 0x7f3447600000...
init(22) ue_rbuff_tbl(8 MB) @ 0x7f3448a00000...
init(23) tun_gw_table(2 MB) @ 0x7f3449200000...
init(24) wispr_conf_tbl(2 MB) @ 0x7f3449400000...
init(25) dhcp_stats_tbl(2 MB) @ 0x7f3449600000...
init(26) dlog_rbuff_tbl(16 MB) @ 0x7f3449800000...
init(27) nts_conf_tbl(2 MB) @ 0x7f344a800000...
init(28) tenant_conf_tbl(2 MB) @ 0x7f344aa00000...
init(29) lnx_sysinfo_conf_tbl(2 MB) @ 0x7f344ac00000...
init(30) ap_hash_tbl(8 MB) @ 0x7f344ae00000...
init(31) datacore_cmd(4 MB) @ 0x7f344b600000...
init(32) pmipfwd(4 MB) @ 0x7f344ba00000...
init(33) tpwlan(20 MB) @ 0x7f344be00000...
init(34) routes_v6(2 MB) @ 0x7f344d200000...
init(35) dscp_conf_tbl(16 MB) @ 0x7f344d400000...
```

1. At the login prompt, login using **administrator** credentials of username and password. At the **>** prompt, enter the **enable (en)** command and the admin password to change the mode to Privileged-exec mode.

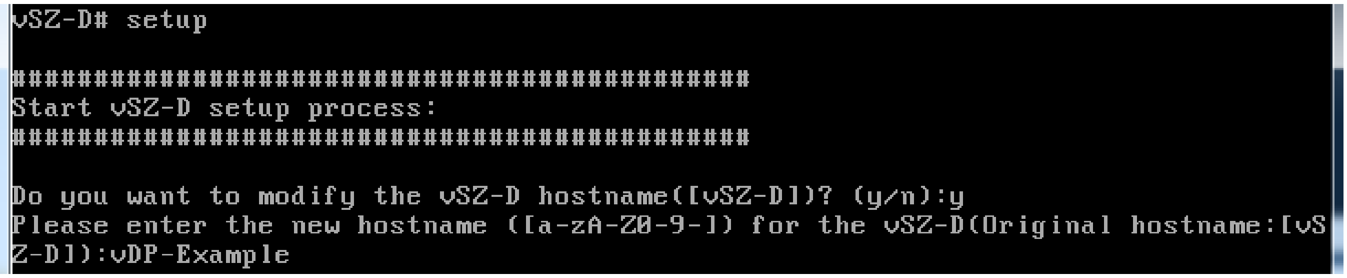
FIGURE 30 Login and Privileged mode



```
################################
#       Welcome to vSZ-D       #
################################
vSZ-D login: admin
Password:
Welcome to the RUCKUS WIRELESS vSZ-D Command Line Interface
vSZ-D> enable
Password:
vSZ-D# _
```

2. Run the **setup** command to configure the IP address for management and data interface. It is recommended to add a new host if you have multiple hosts for various configurations

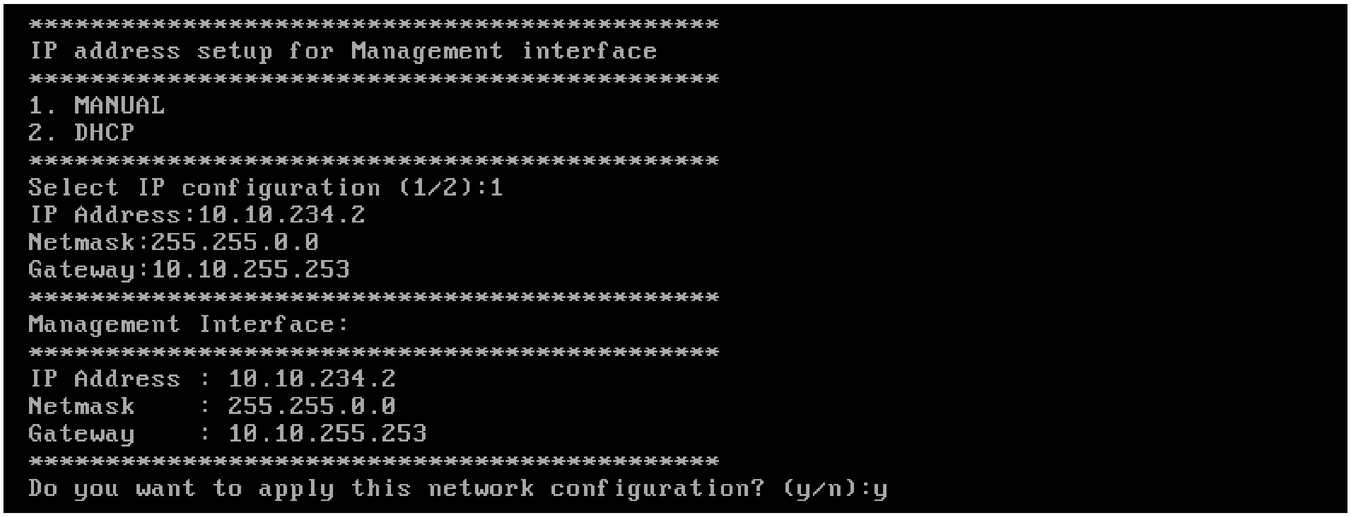
FIGURE 31 Execute the setup command



```
vSZ-D# setup

#############################################
Start vSZ-D setup process:
#############################################

Do you want to modify the vSZ-D hostname([vSZ-D])? (y/n):y
Please enter the new hostname ([a-zA-Z0-9-]) for the vSZ-D(Original hostname:[vS
Z-D]):vDP-Example
```

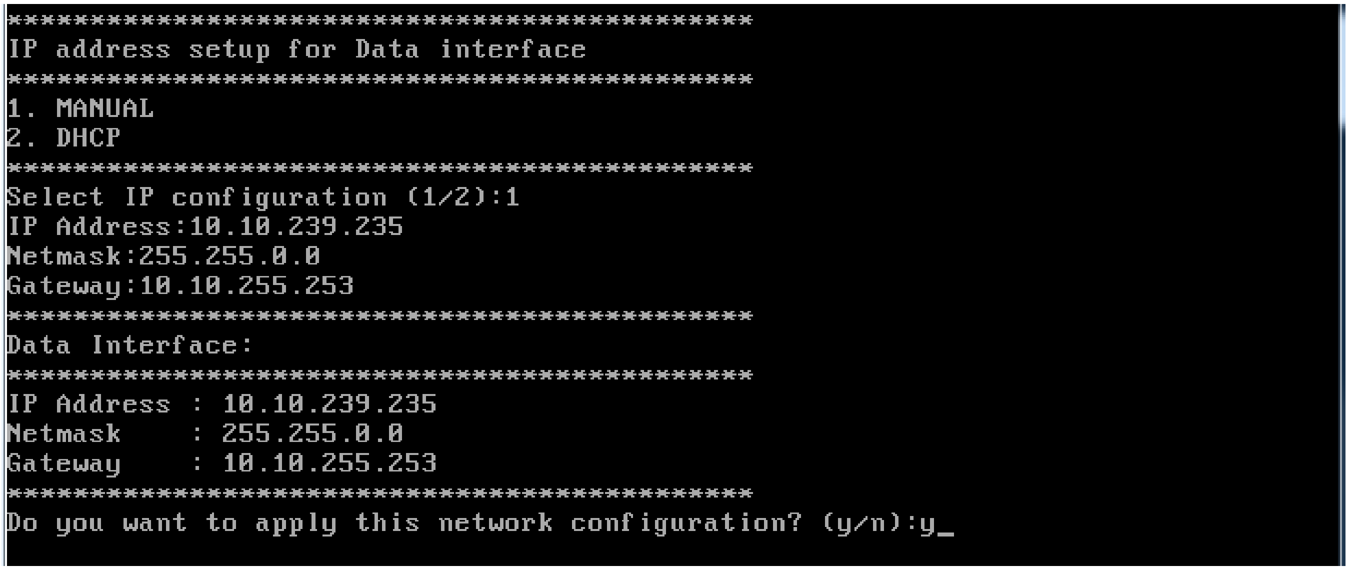
3. Choose the IP address setup (IPv4 only or IPv4 and IPv6) for Management and Data interface by either selecting manual or DHCP. On defining the IP setup the process of vSZ-D/SZ100-D connecting to vSZ controller starts.

FIGURE 32 Management interface



```
**********************************************
IP address setup for Management interface
**********************************************
1. MANUAL
2. DHCP
**********************************************
Select IP configuration (1/2):1
IP Address:10.10.234.2
Netmask:255.255.0.0
Gateway:10.10.255.253
**********************************************
Management Interface:
**********************************************
IP Address : 10.10.234.2
Netmask    : 255.255.0.0
Gateway    : 10.10.255.253
**********************************************
Do you want to apply this network configuration? (y/n):y
```

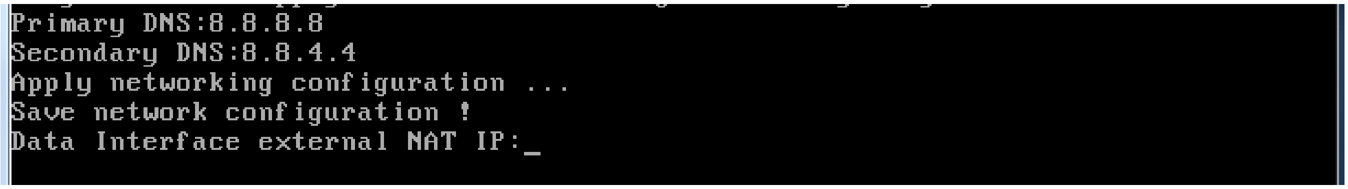
FIGURE 33 Data interface



```
**********************************************
IP address setup for Data interface
**********************************************
1. MANUAL
2. DHCP
**********************************************
Select IP configuration (1/2):1
IP Address:10.10.239.235
Netmask:255.255.0.0
Gateway:10.10.255.253
**********************************************
Data Interface:
**********************************************
IP Address : 10.10.239.235
Netmask    : 255.255.0.0
Gateway    : 10.10.255.253
**********************************************
Do you want to apply this network configuration? (y/n):y_
```

4. Enter the DNS setting and select Enter to skip the NAT IP setting.

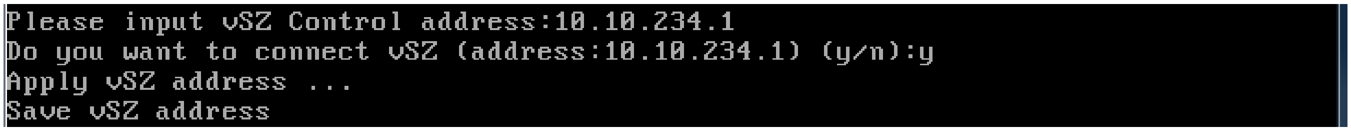
FIGURE 34 DNS setting



```
Primary DNS:8.8.8.8
Secondary DNS:8.8.4.4
Apply networking configuration ...
Save network configuration !
Data Interface external NAT IP:_
```

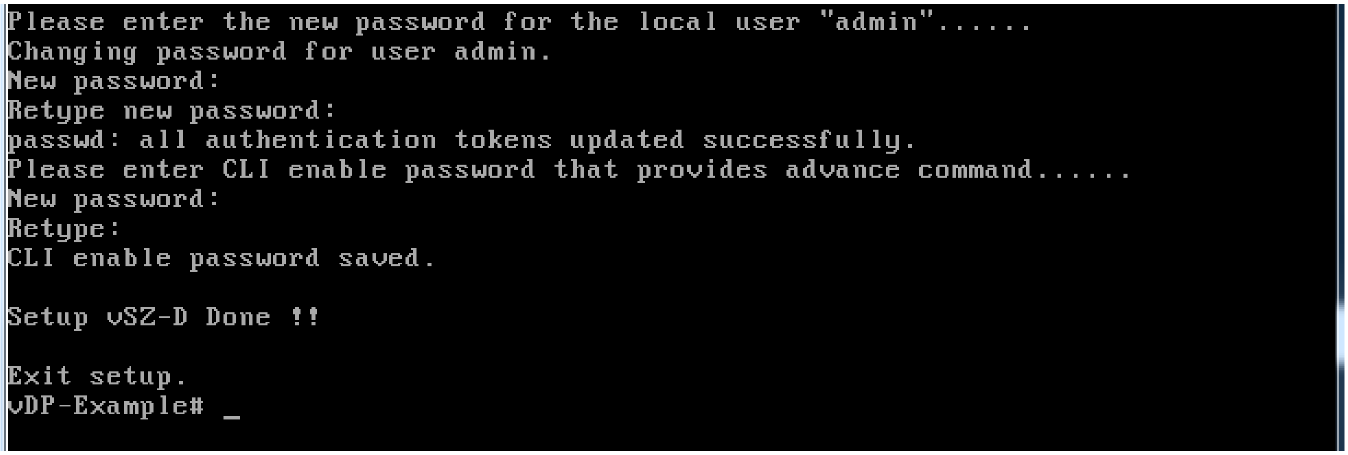
5. Enter vSZ control interface IP address. Follow the set of sequences as seen below for the vSZ-D/SZ100-D to connect to vSZ controller. This changes the mode for vSZ-D/SZ100-D as well as for vSZ.

FIGURE 35 vSZ control IP address



```
Please input vSZ Control address:10.10.234.1
Do you want to connect vSZ (address:10.10.234.1) (y/n):y
Apply vSZ address ...
Save vSZ address
```

FIGURE 36 Connecting to vSZ

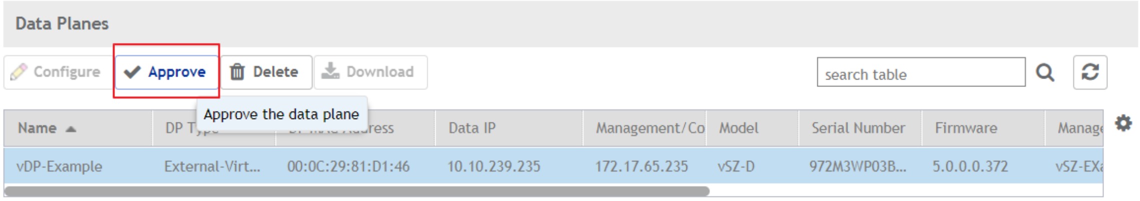


```
Please enter the new password for the local user "admin"......
Changing password for user admin.
New password:
Retype new password:
passwd: all authentication tokens updated successfully.
Please enter CLI enable password that provides advance command......
New password:
Retype:
CLI enable password saved.

Setup vSZ-D Done !!

Exit setup.
vDP-Example# _
```

6. Exit from CLI console.

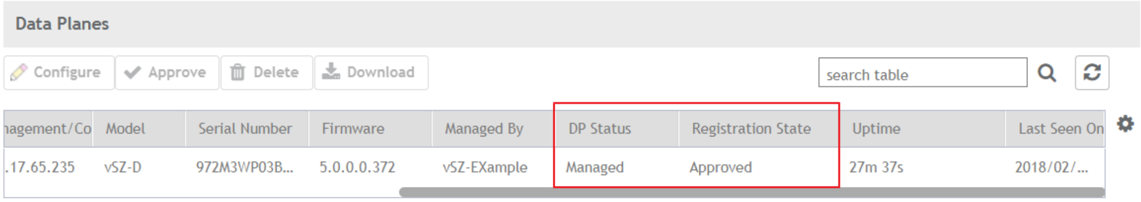
7. To view and approve the vSZ-D/SZ100-D, login to the web interface. Navigate to **Clusters** > **Data planes**. Select the vSZ-D/SZ100-D and click on **Approve.** On approval the status is greyed.

FIGURE 37 Approve the vSZ-D/SZ100-D



Name ▲	DP T	ress	Data IP	Management/Co	Model	Serial Number	Firmware	Manag
vDP-Example	External-Virt...	00:0C:29:81:D1:46	10.10.239.235	172.17.65.235	vSZ-D	972M3WP03B...	5.0.0.0.372	vSZ-EX

FIGURE 38 Approved status



agement/Co	Model	Serial Number	Firmware	Managed By	DP Status	Registration State	Uptime	Last Seen On
.17.65.235	vSZ-D	972M3WP03B...	5.0.0.0.372	vSZ-EXample	Managed	Approved	27m 37s	2018/02/...

You have successfully added the vSZ-D/SZ100-D image to the vSZ controller.

Deploy vSZ-D with 40GB NIC on Linux Server

Deploy vSZ-D with 40GB NIC on Linux Server

Hardware Requirement and Prerequisite

The following are the hardware and prerequisite for deploying vSZ-D on LINUX CentOS 7.

Hardware Requirement

1. DELL Inc. PowerEdge R320
2. Linux CentOS 7
3. Broadcom NetXtreme BCM5720 Gigabit Ethernet 2 Ports
4. Intel Ethernet 10G 2P X520

Prerequisite

- A Linux host enabled KVM which to install vSZ-D VM. Prefer CentOS 7 and later.
- Download the vSZ-D package (.qcow2 file) from Ruckus support .
- The IP addresses, netmask, gateway, DNS, DHCP and NAT support for vSZ-D.
- Two network interfaces to support vSZ-D.
- Before you power on vSZ-D, ensure that the networking is configured on LINUX.
- Recommended to use static network addresses that are assigned to vSZ-D during setup.

- Using CentOS 7, install KVM package with the **yum** command.

  ```
  root@localhost ruckusvnc]# yum -y install qemu-kvm qemu-img virt-manager virt-viewer virt-install
  libvirt libvirt-phthon libvirt-client
  ```

- Ensure KVM is active and running the following command

  ```
  [root@localhost ruckusvnc]# systemctl status libvirtd
  ```

- Edit the following commands and file.

  ```
  sudo yum install grub2-common

  gedit /etc/default/grub
  GRUB_TIMEOUT=5
  GRUB_DISTRIBUTOR="$(sed 's, release .*$,,g' /etc/system-release)"
  GRUB_DEFAULT=saved
  GRUB_DISABLE_SUBMENU=true
  GRUB_TERMINAL_OUTPUT="console"
  GRUB_CMDLINE_LINUX="crashkernel=auto rd.lvm.lv=centos/root rd.lvm.lv=centos/swap rhgb quiet
  intel_iommu=on"
  GRUB_DISABLE_RECOVERY="true"

  sudo grub2-mkconfig -o /boot/grub2/grub.cfg
  ```

- Reboot Linux host.

  NOTE
  Due to different servers and NIC, the deployment procedure mentioned in this section is for reference.

Topology

The network topologies for vSZ-D deployment on LINUX CentOS 7.

The following are basic topologies for setting up vSZ-D. Based on your requirement you can choose any of the alternatives between one IP domain to three separate domains for deployment.

The below topology shows the different IP addresses for the domains.

FIGURE 39 Three different IP addresses setup

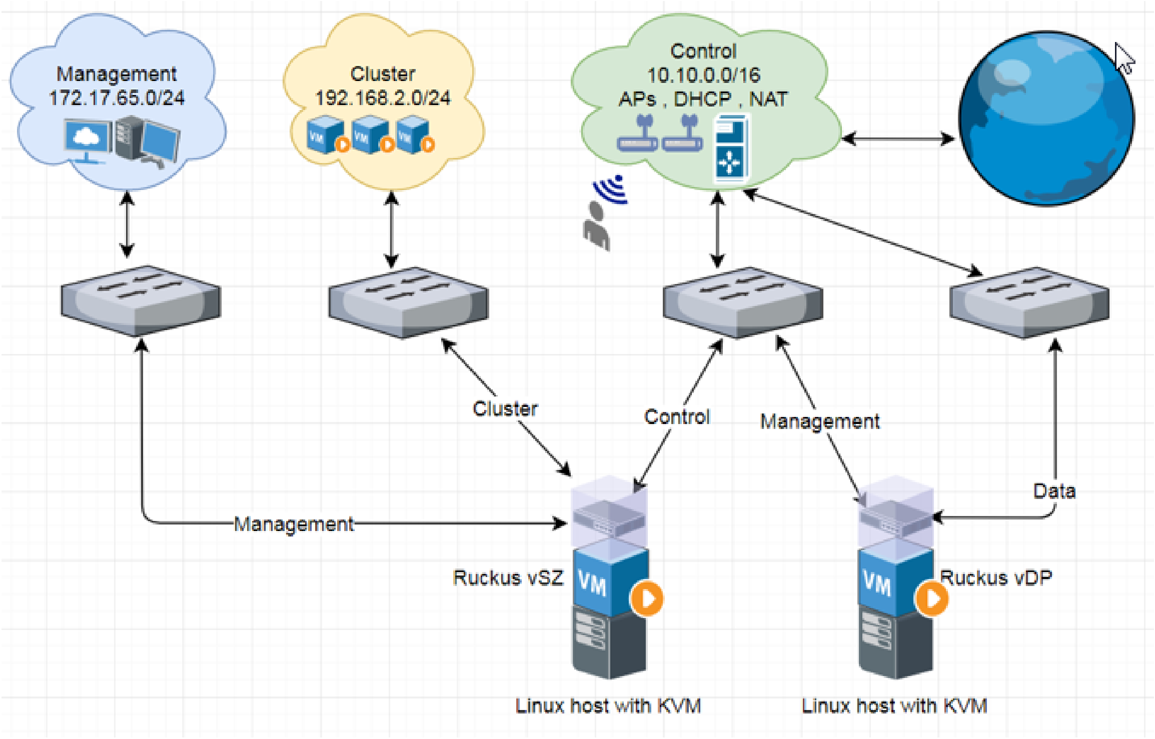
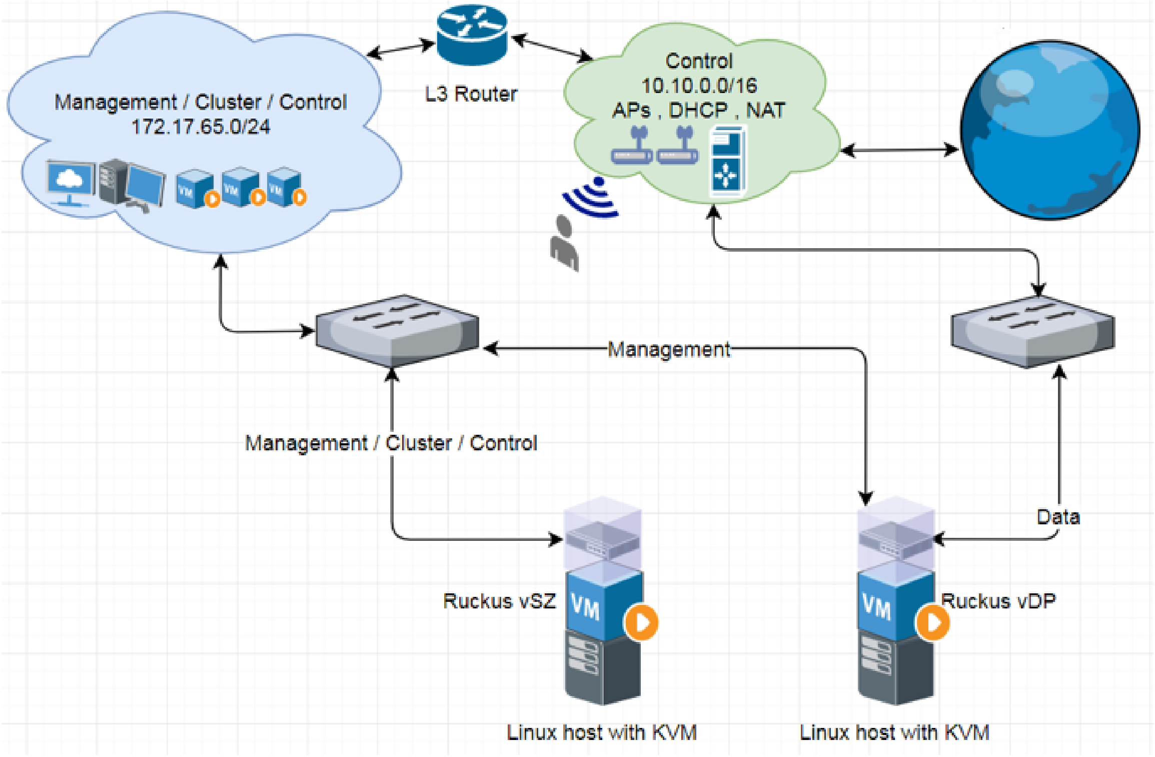
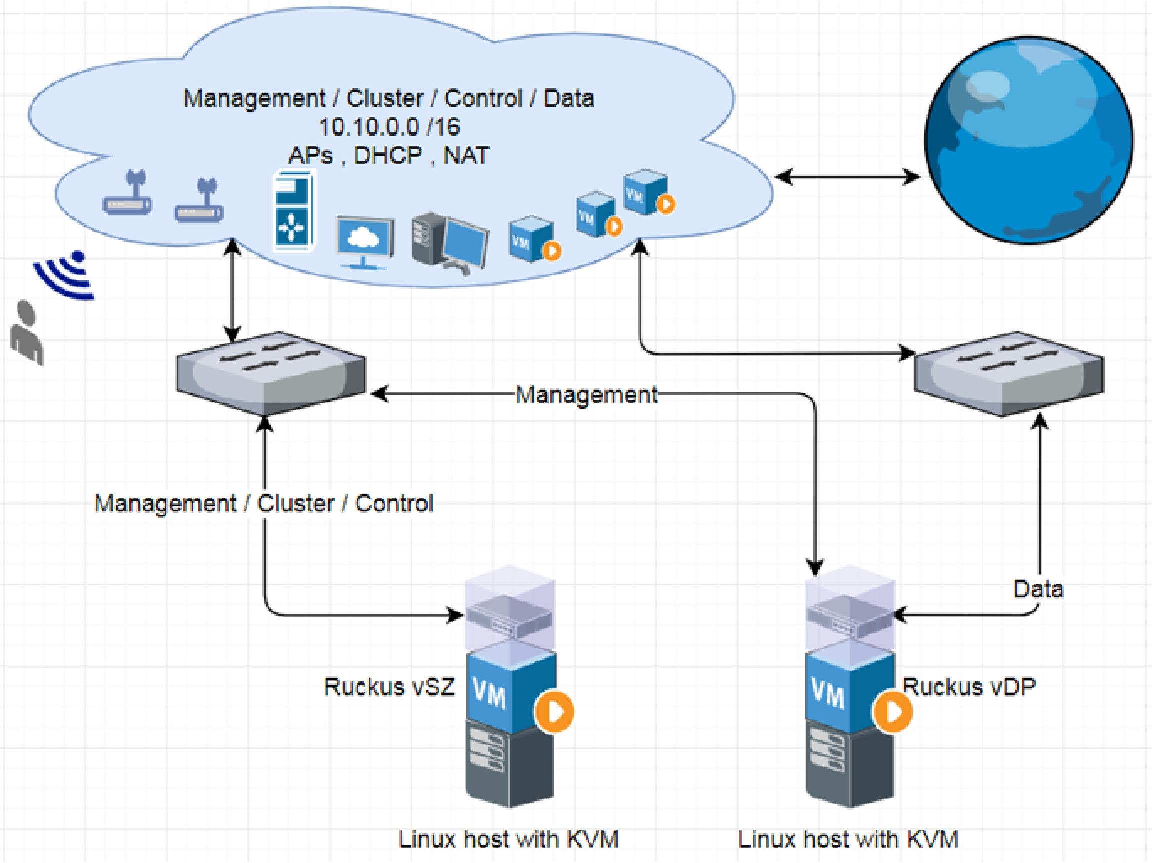


FIGURE 40 Two different domain IP addresses setup



The below topology shows the same IP addresses for the all the interfaces.

FIGURE 41 The same IP addresses setup



Deployment Procedure

The following are basic instructions for setting up vSZ-D on LINUX KVM.

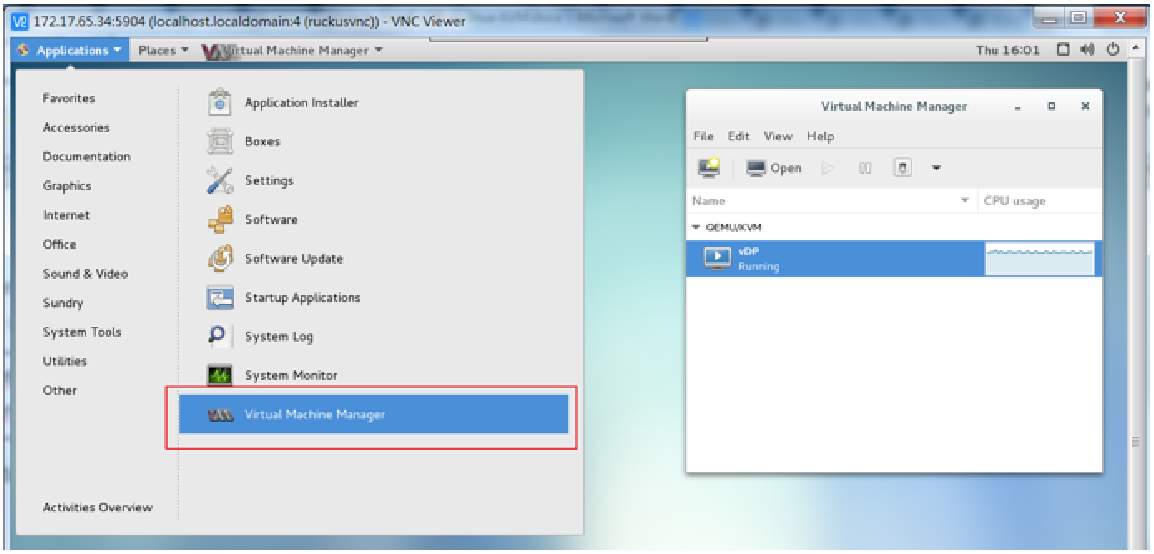
LINUX CentOS 7 KVM Package is installed and working.

For this deployment two different IP address domains are considered for Data Plane interfaces. Refer to Topology on page 81.

1. Download the Data Plane package (.qcow2 file) from Ruckus support .

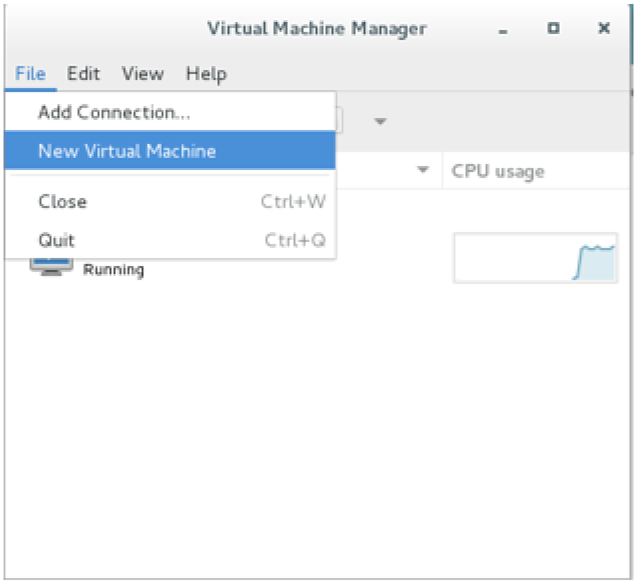
2. From the VNC Viewer, click **System Tools** > **Virtual Machine Manager** to open the Virtual Machine Manager tool. The Data Plane status must appear Running as shown in the following figure.

FIGURE 42 Virtual Machine Manager



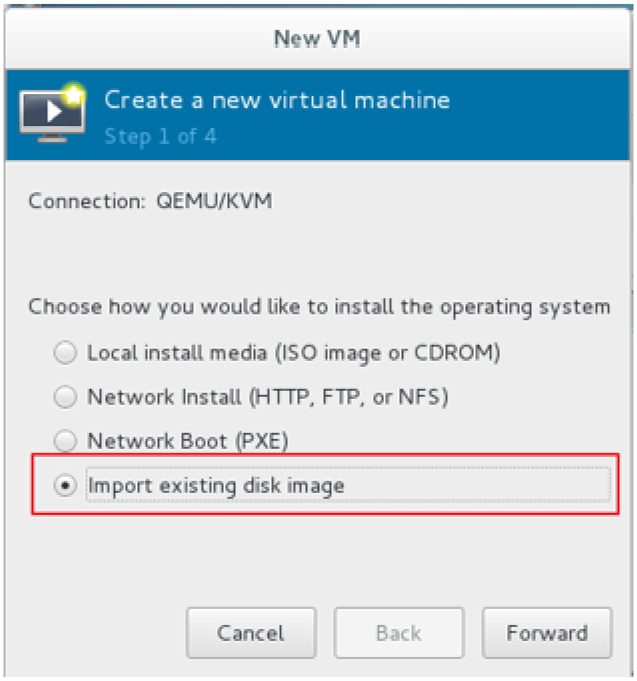
3. Create a new VM.
   a) Click **File** and select **New Virtual Machine** as shown in the following figure.

FIGURE 43 Creating a Virtual Machine



   b) In the New VM dialog box, choose the disk format option as shown in the following figure.

FIGURE 44 Disk Format


New VM

Create a new virtual machine
Step 1 of 4

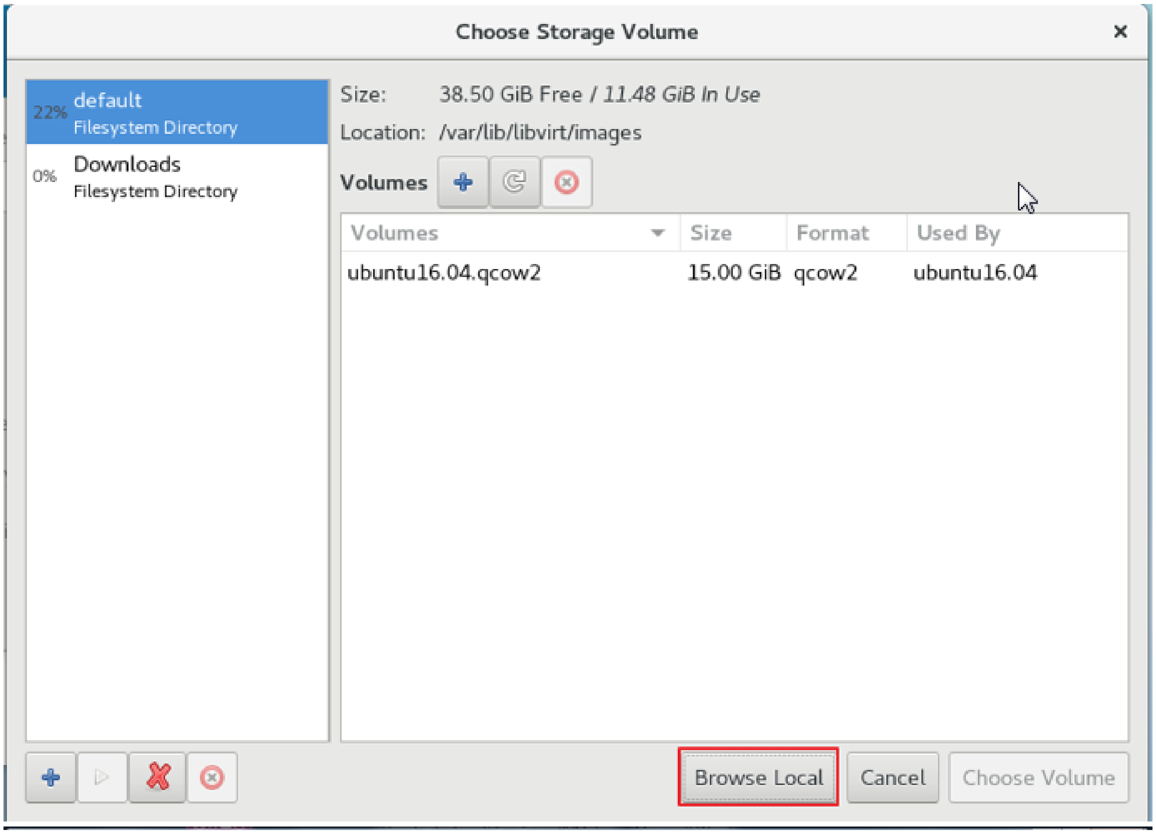
Connection: QEMU/KVM

Choose how you would like to install the operating system
○ Local install media (ISO image or CDROM)
○ Network Install (HTTP, FTP, or NFS)
○ Network Boot (PXE)
● Import existing disk image

c) Click **Forward**.

d) Choose destination storage path and storage volume. Click **Browse Local** as show in the following figure.

FIGURE 45 Storage Volume



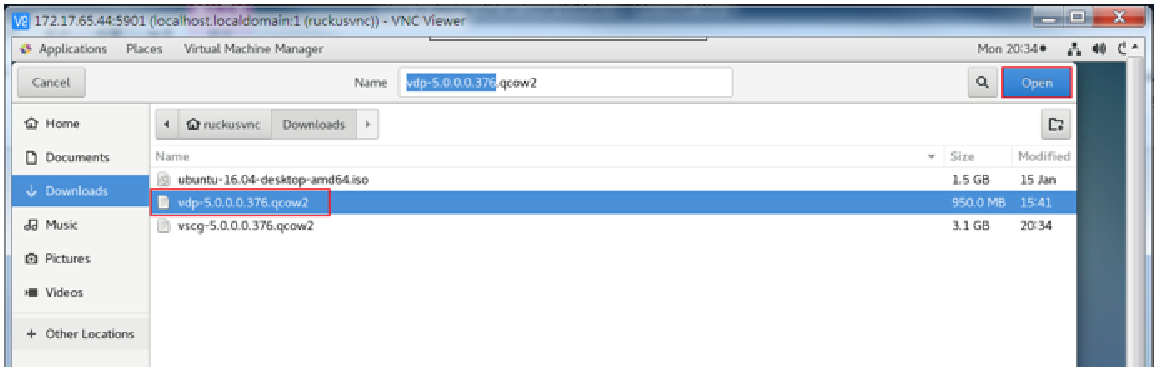
Size: 38.50 GiB Free / *11.48 GiB In Use*

Location: /var/lib/libvirt/images

Volumes	Size	Format	Used By
ubuntu16.04.qcow2	15.00 GiB	qcow2	ubuntu16.04

e) Select the Data Plane file and click **Open** as shown in the following figure.

FIGURE 46 Data Plane File

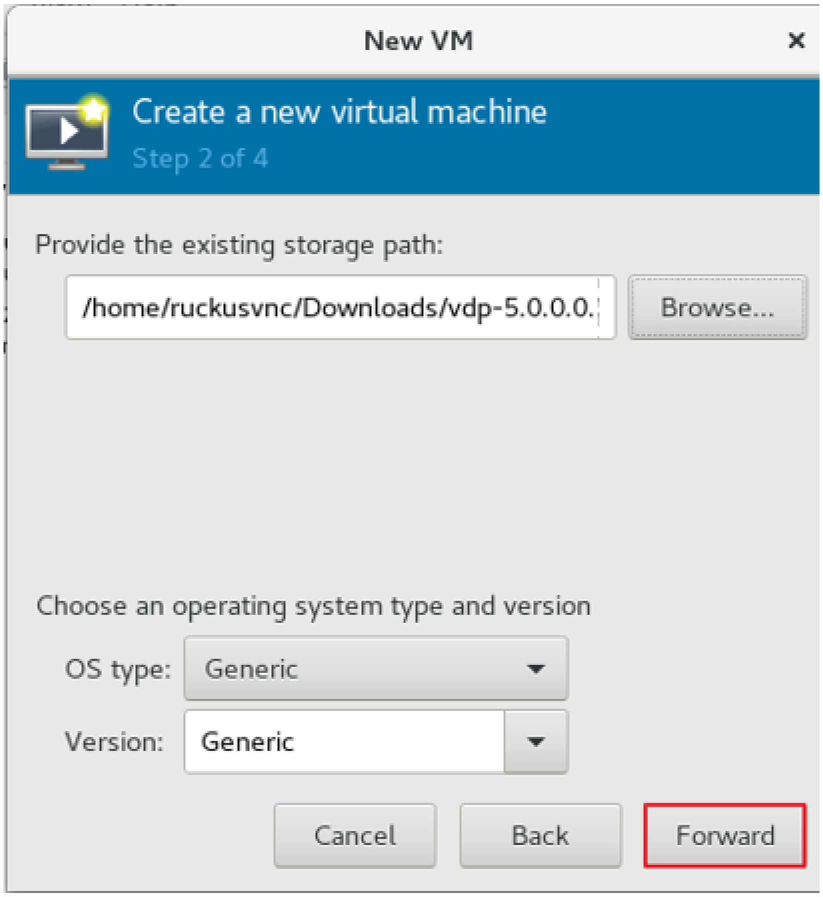


Name vdp-5.0.0.0.376.qcow2

Name	Size	Modified
ubuntu-16.04-desktop-amd64.iso	1.5 GB	15 Jan
vdp-5.0.0.0.376.qcow2	950.0 MB	15:41
vscg-5.0.0.0.376.qcow2	3.1 GB	20:34

f) To select the storage path, click **Browse** as shown in the following figure.

FIGURE 47 Storage Path



New VM

Create a new virtual machine

Step 2 of 4

Provide the existing storage path:

/home/ruckusvnc/Downloads/vdp-5.0.0.0.

Choose an operating system type and version

OS type: Generic

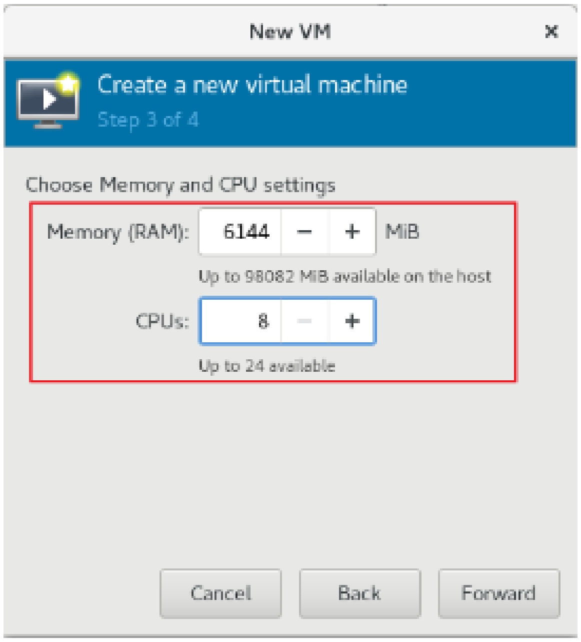
Version: Generic

g) Click **Forward**.

h) Enter the **Memory (RAM)** and **CPUs** setting as shown in the following figure.

NOTE
Memory (RAM) must be 6GB and CPUs must be 8 cores.

FIGURE 48 Memory and CPU Settings



Choose Memory and CPU settings

Memory (RAM): 6144 MiB

Up to 98082 MiB available on the host

CPUs: 8

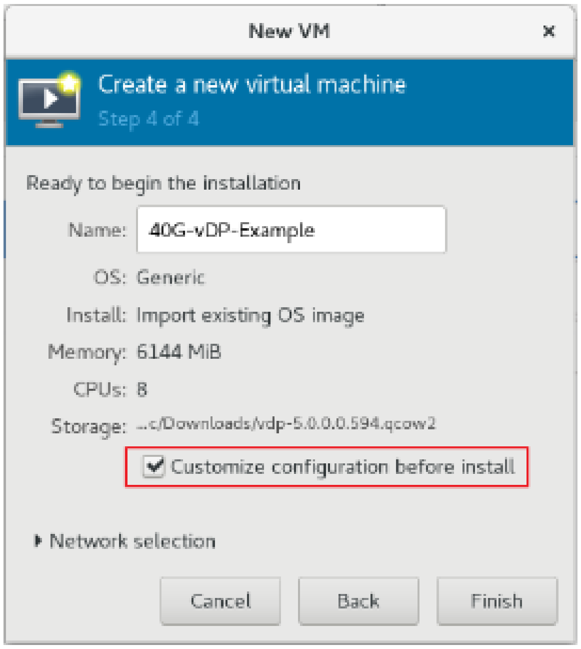
Up to 24 available

i) Click **Forward**.

j) To confirm the installation process, click **Finish** as shown in the following figure.

NOTE
The sequence for Network interfaces must first be Management and the Data.

FIGURE 49 Installation Confirmation



Ready to begin the installation

Name: 40G-vDP-Example

OS: Generic

Install: Import existing OS image

Memory: 6144 MiB

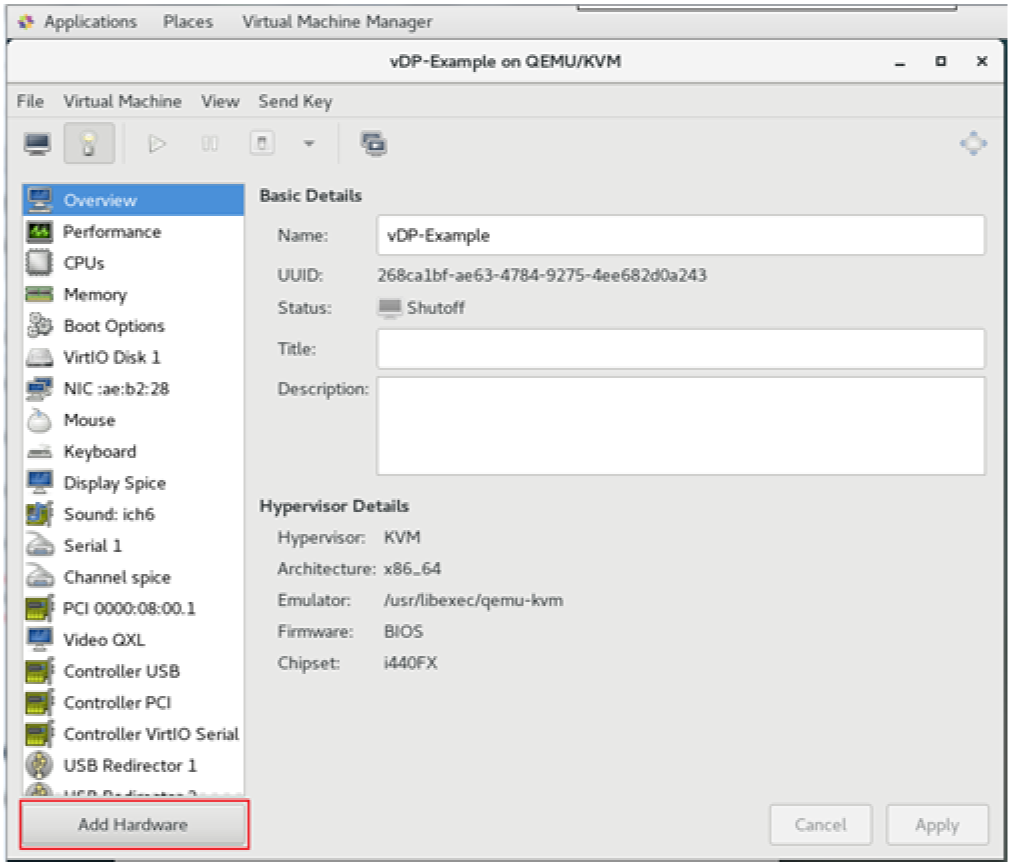
CPUs: 8

Storage: ...c/Downloads/vdp-5.0.0.0.594.qcow2

☑ Customize configuration before install

4. 4. Add another NIC as Data Plane needs two interfaces; Management and Data. From the VNC Viewer and click **Add Hardware** > **PCI Host Device** > **PCI Device** to add another NIC as shown in the following figure.

FIGURE 50 Adding NIC



Basic Details

Name: vDP-Example

UUID: 268ca1bf-ae63-4784-9275-4ee682d0a243

Status: Shutoff

Title:

Description:

Hypervisor Details

Hypervisor: KVM

Architecture: x86_64

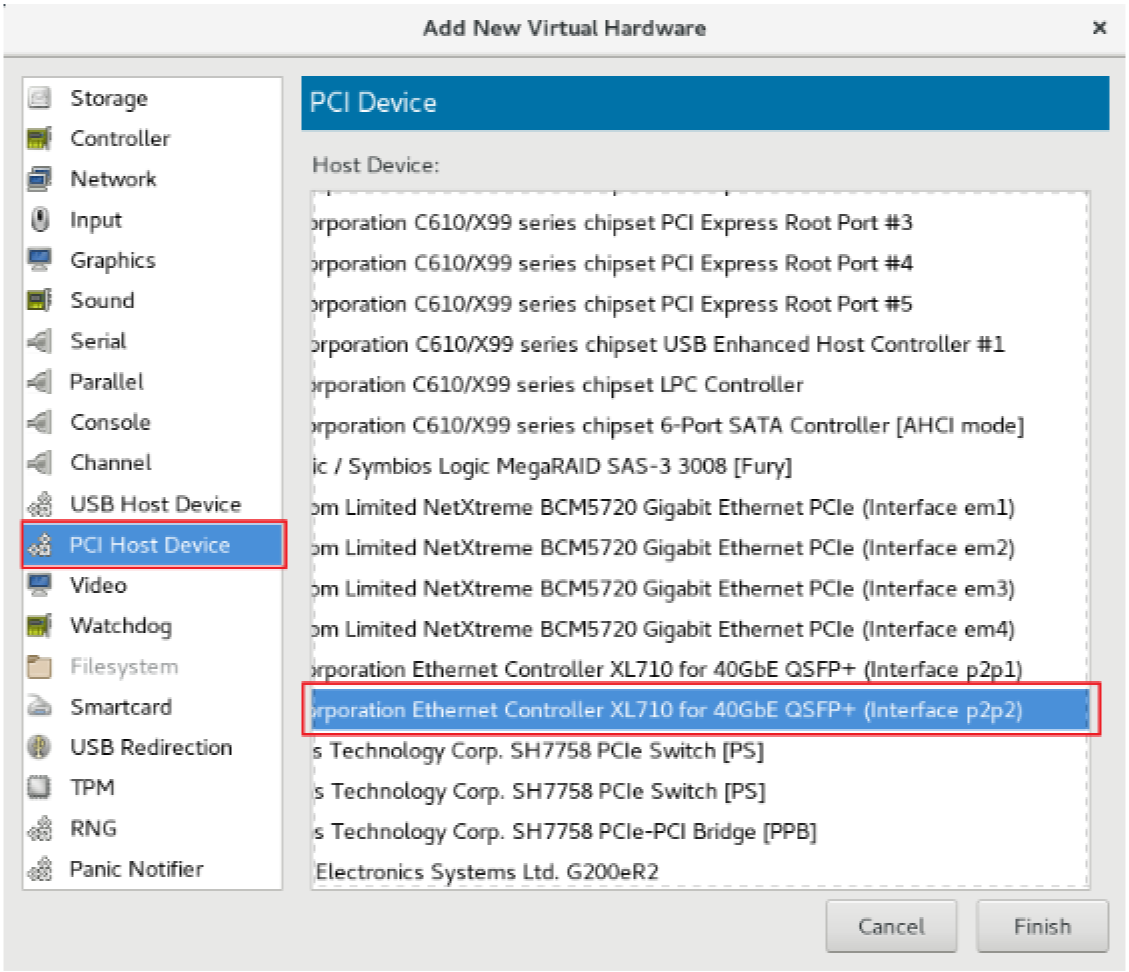
Emulator: /usr/libexec/qemu-kvm

Firmware: BIOS

Chipset: i440FX

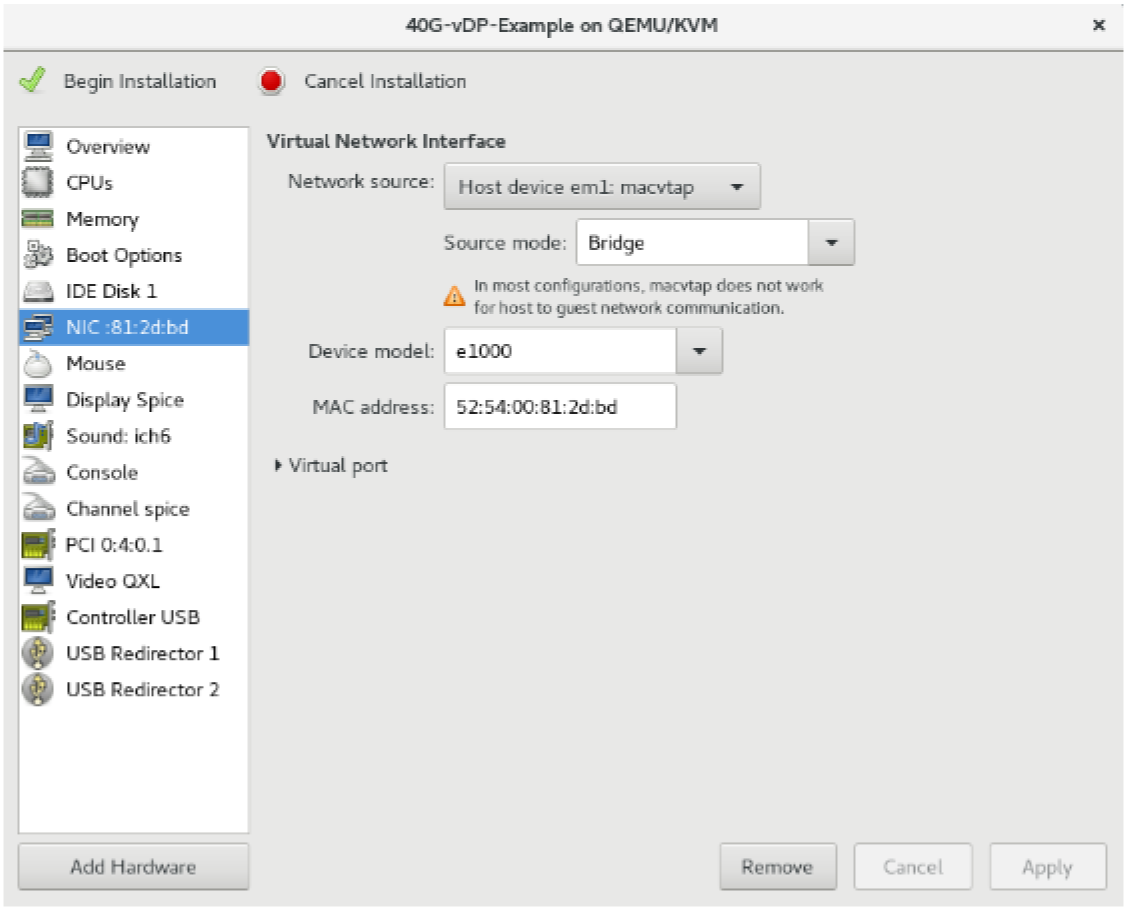
5. Select **PCI Host Device** > **PCI Device** and click **Finish** to add another NIC as shown in the following figure.

FIGURE 51 PCI Host Device


Add New Virtual Hardware
×
Storage
Controller
Network
Input
Graphics
Sound
Serial
Parallel
Console
Channel
USB Host Device
PCI Host Device
Video
Watchdog
Filesystem
Smartcard
USB Redirection
TPM
RNG
Panic Notifier
PCI Device
Host Device:
›rporation C610/X99 series chipset PCI Express Root Port #3
›rporation C610/X99 series chipset PCI Express Root Port #4
›rporation C610/X99 series chipset PCI Express Root Port #5
›rporation C610/X99 series chipset USB Enhanced Host Controller #1
›rporation C610/X99 series chipset LPC Controller
›rporation C610/X99 series chipset 6-Port SATA Controller [AHCI mode]
ic / Symbios Logic MegaRAID SAS-3 3008 [Fury]
›m Limited NetXtreme BCM5720 Gigabit Ethernet PCIe (Interface em1)
›m Limited NetXtreme BCM5720 Gigabit Ethernet PCIe (Interface em2)
›m Limited NetXtreme BCM5720 Gigabit Ethernet PCIe (Interface em3)
›m Limited NetXtreme BCM5720 Gigabit Ethernet PCIe (Interface em4)
›rporation Ethernet Controller XL710 for 40GbE QSFP+ (Interface p2p1)
›rporation Ethernet Controller XL710 for 40GbE QSFP+ (Interface p2p2)
s Technology Corp. SH7758 PCIe Switch [PS]
s Technology Corp. SH7758 PCIe Switch [PS]
s Technology Corp. SH7758 PCIe-PCI Bridge [PPB]
Electronics Systems Ltd. G200eR2
Cancel
Finish

6. Select the NIC and choose the **Device model** to update the management interface associate as shown in the following figure.

FIGURE 52 Management Interface



Virtual Network Interface

Network source: Host device em1: macvtap

Source mode: Bridge

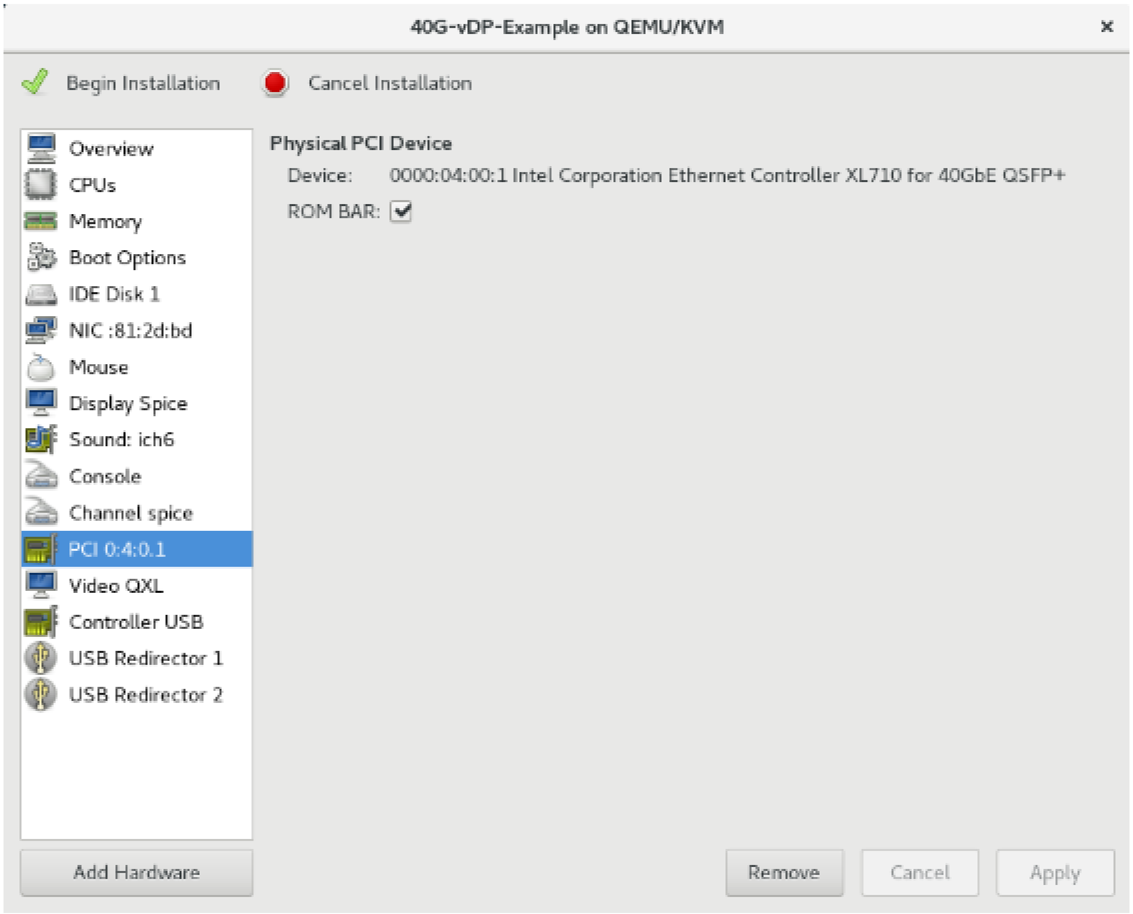
In most configurations, macvtap does not work for host to guest network communication.

Device model: e1000

MAC address: 52:54:00:81:2d:bd

7. From PCI, select the **ROM BAR** check box to define the Data IP domain as shown in the following figure.

FIGURE 53 Data IP Domain



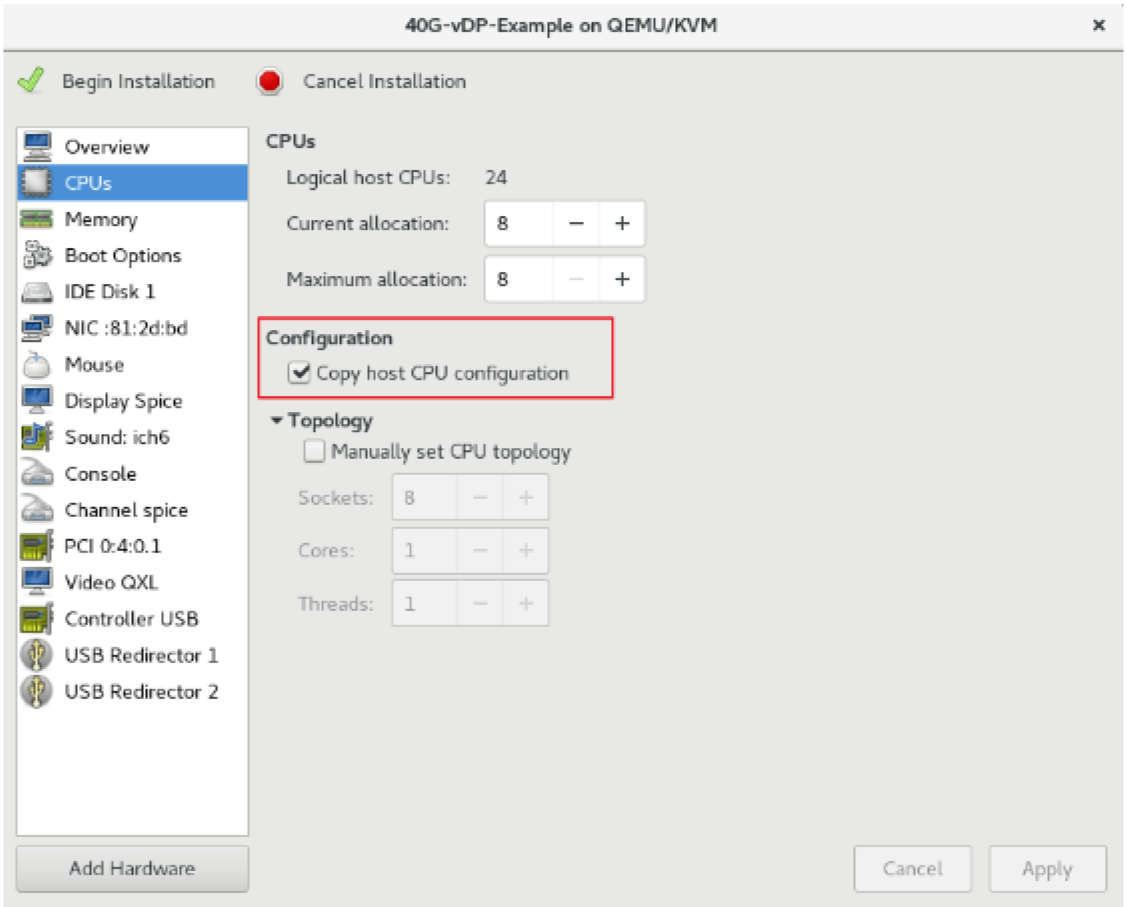
Physical PCI Device

Device: 0000:04:00:1 Intel Corporation Ethernet Controller XL710 for 40GbE QSFP+

ROM BAR: ☑

8. Define the CPU Configuration. Select the **Copy host CPU configuration** check box as shown in the following figure.

FIGURE 54 CPU Configuration



CPUs

Logical host CPUs: 24

Current allocation: 8 − +

Maximum allocation: 8 − +

Configuration

☑ Copy host CPU configuration

▾ Topology

☐ Manually set CPU topology

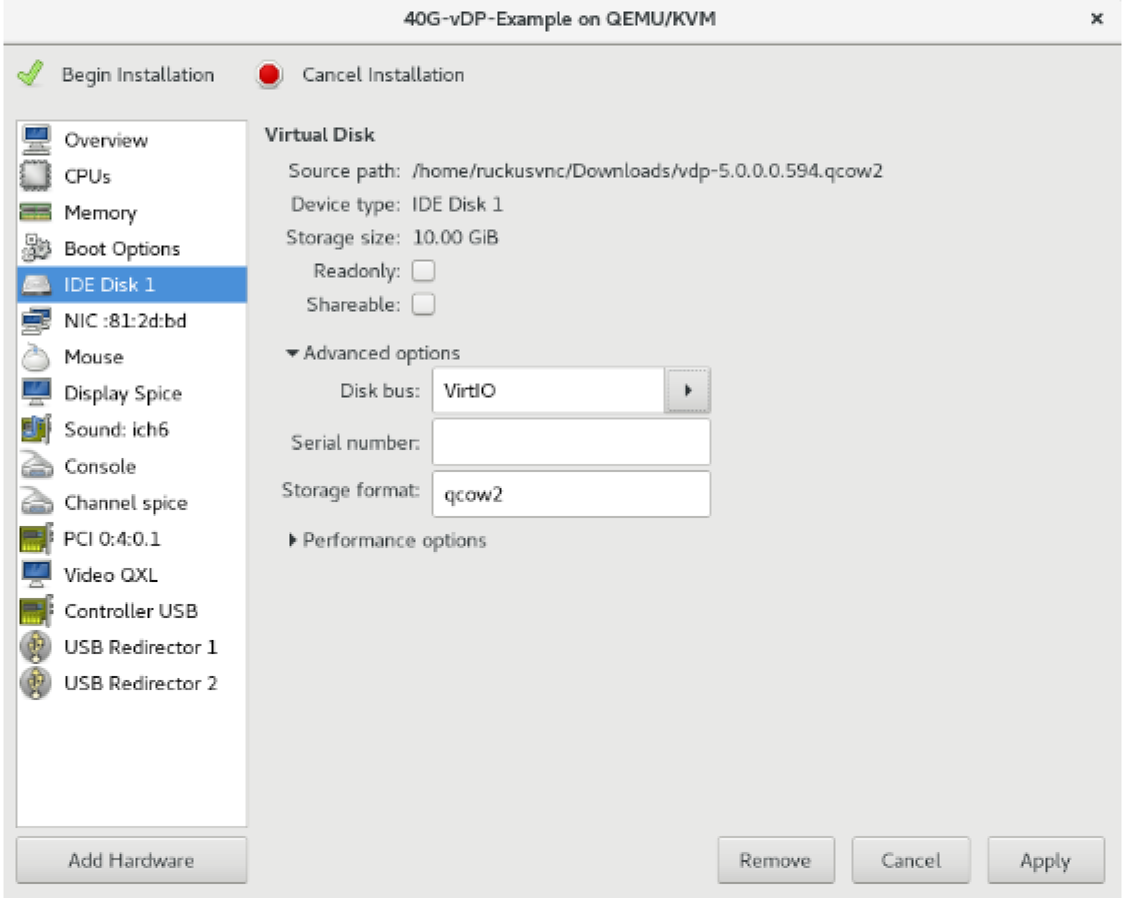
Sockets: 8 − +

Cores: 1 − +

Threads: 1 − +

9. Define the IDE Disk Configuration. Choose the **Disk bus** option as shown in the following figure.

FIGURE 55 IDE Disk Configuration



40G-vDP-Example on QEMU/KVM

Virtual Disk

Source path: /home/ruckusvnc/Downloads/vdp-5.0.0.0.594.qcow2

Device type: IDE Disk 1

Storage size: 10.00 GiB

Readonly: □

Shareable: □

Advanced options

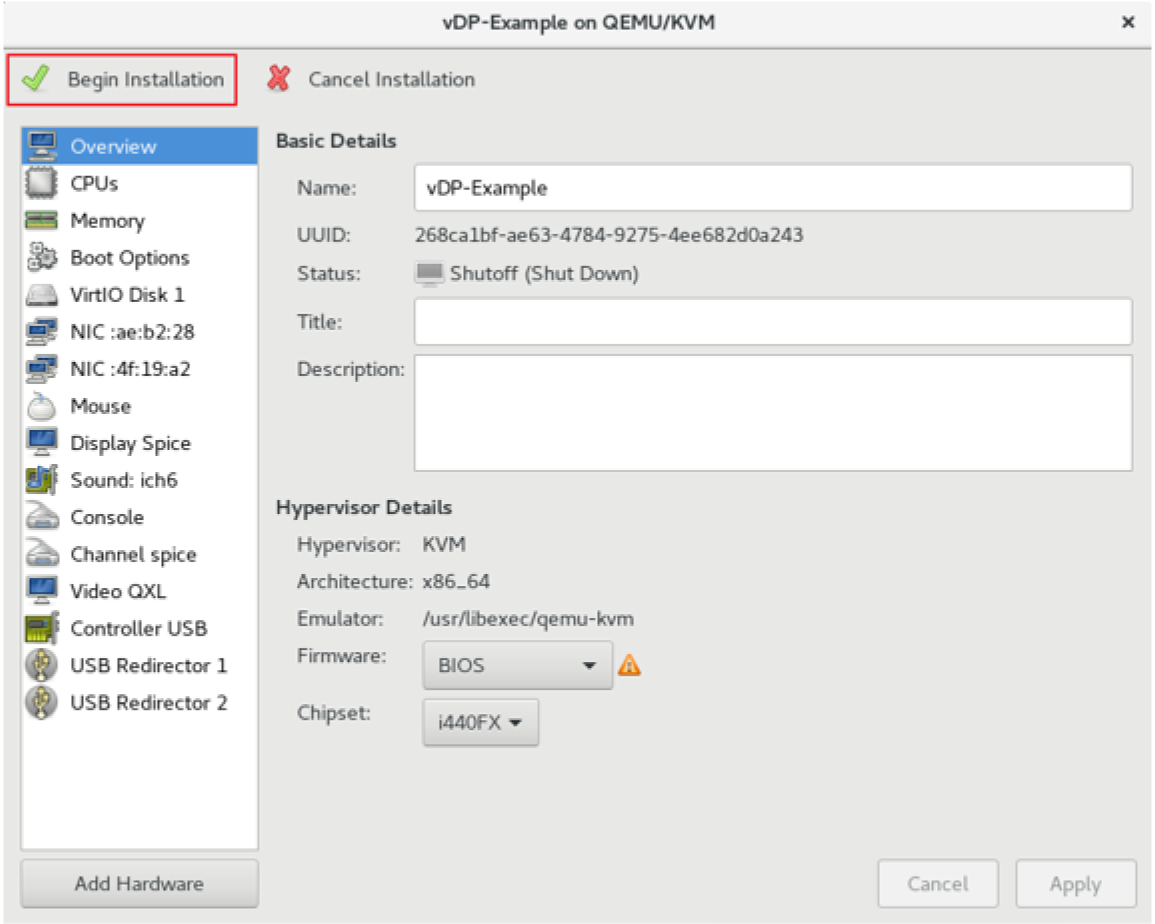
Disk bus: VirtIO

Serial number:

Storage format: qcow2

10. Select **Begin Installation** as shown in the following figure.

FIGURE 56 Begin Installation



Basic Details

Name: vDP-Example

UUID: 268ca1bf-ae63-4784-9275-4ee682d0a243

Status: Shutoff (Shut Down)

Title:

Description:

Hypervisor Details

Hypervisor: KVM

Architecture: x86_64

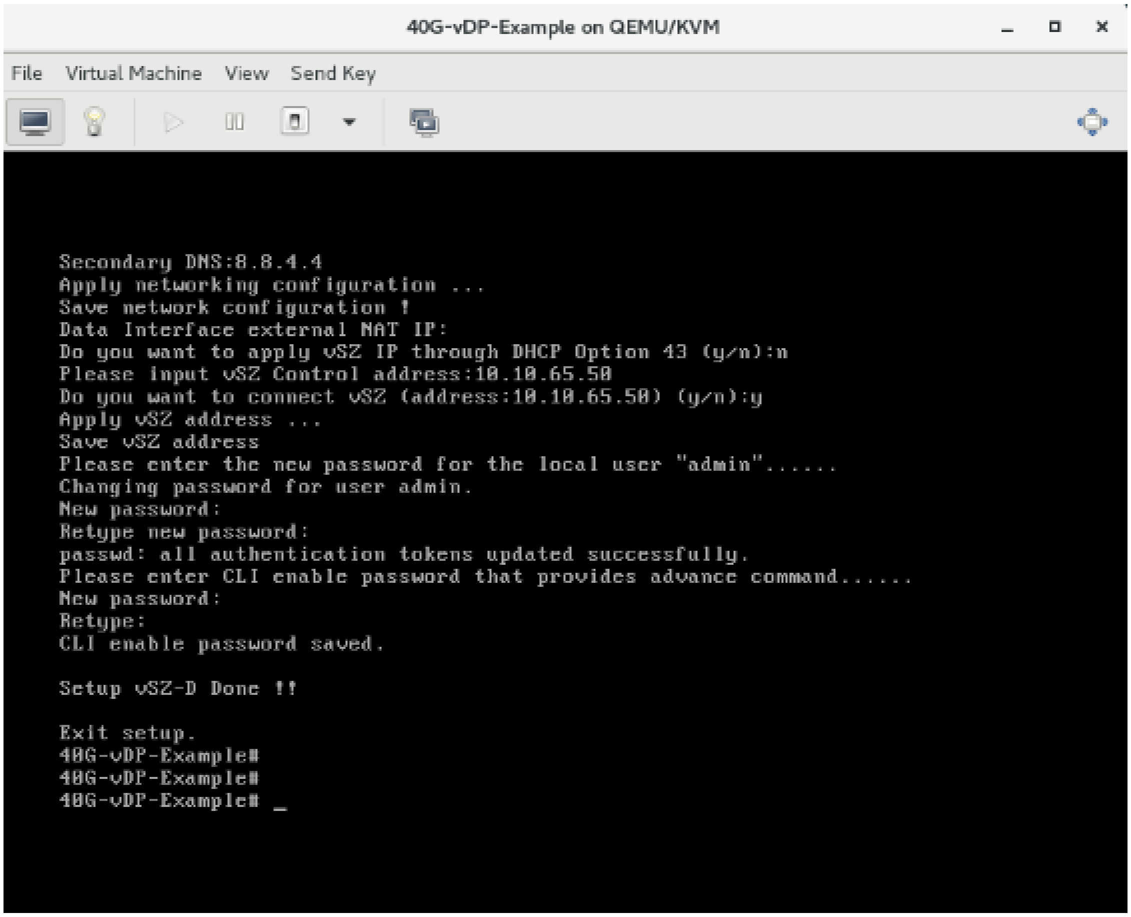
Emulator: /usr/libexec/qemu-kvm

Firmware: BIOS

Chipset: i440FX

11. The Data Plane setup is complete as shown in the following image.

FIGURE 57 Installation Complete



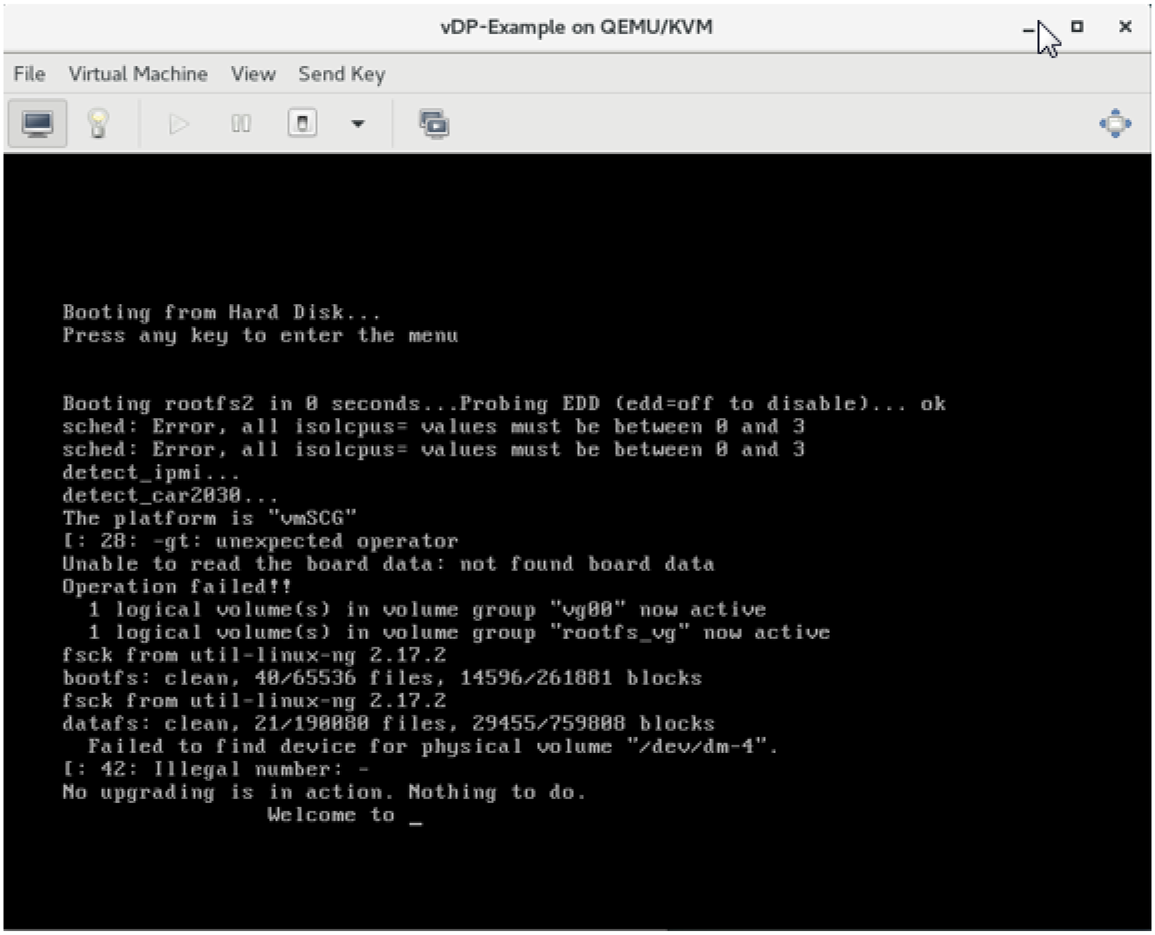
```
Secondary DNS:8.8.4.4
Apply networking configuration ...
Save network configuration !
Data Interface external NAT IP:
Do you want to apply vSZ IP through DHCP Option 43 (y/n):n
Please input vSZ Control address:10.10.65.50
Do you want to connect vSZ (address:10.10.65.50) (y/n):y
Apply vSZ address ...
Save vSZ address
Please enter the new password for the local user "admin"......
Changing password for user admin.
New password:
Retype new password:
passwd: all authentication tokens updated successfully.
Please enter CLI enable password that provides advance command......
New password:
Retype:
CLI enable password saved.

Setup vSZ-D Done !!

Exit setup.
40G-vDP-Example#
40G-vDP-Example#
40G-vDP-Example# _
```

vSZ-D/SZ100-D Connect to vSZ Using CLI

Follow the below procedures for vSZ-D/SZ100-D to connect to vSZ.

Open a CLI console window to run the deployed vSZ-D/SZ100-D.

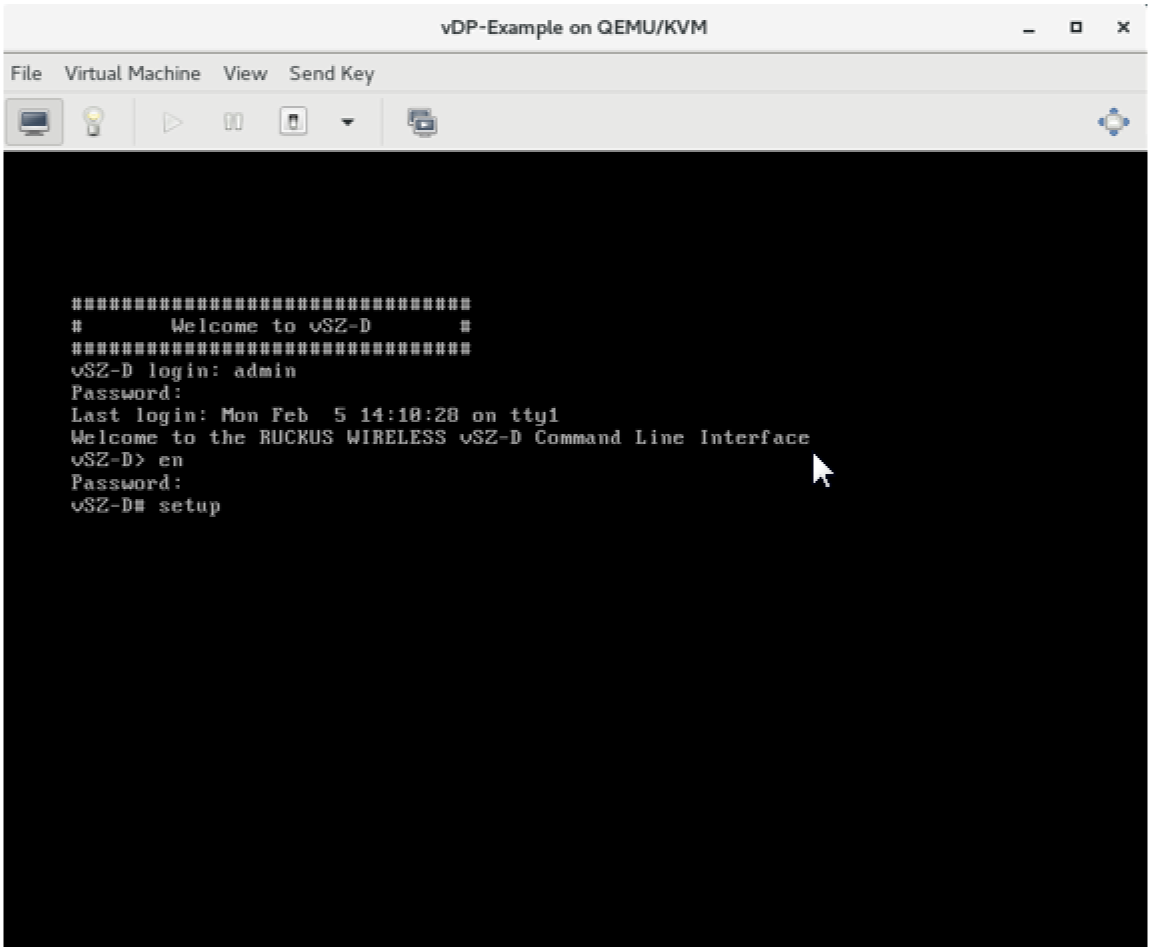
FIGURE 58 Run vSZ-D/SZ100-D on the console



```
Booting from Hard Disk...
Press any key to enter the menu


Booting rootfs2 in 0 seconds...Probing EDD (edd=off to disable)... ok
sched: Error, all isolcpus= values must be between 0 and 3
sched: Error, all isolcpus= values must be between 0 and 3
detect_ipmi...
detect_car2030...
The platform is "vmSCG"
[: 28: -gt: unexpected operator
Unable to read the board data: not found board data
Operation failed!!
  1 logical volume(s) in volume group "vg00" now active
  1 logical volume(s) in volume group "rootfs_vg" now active
fsck from util-linux-ng 2.17.2
bootfs: clean, 40/65536 files, 14596/261881 blocks
fsck from util-linux-ng 2.17.2
datafs: clean, 21/190080 files, 29455/759808 blocks
  Failed to find device for physical volume "/dev/dm-4".
[: 42: Illegal number: -
No upgrading is in action. Nothing to do.
                Welcome to _
```

1. At the login prompt, login using **administrator** credentials of username and password. At the **>** prompt, enter the **enable (en)** command and the admin password to change the mode to Privileged-exec mode.

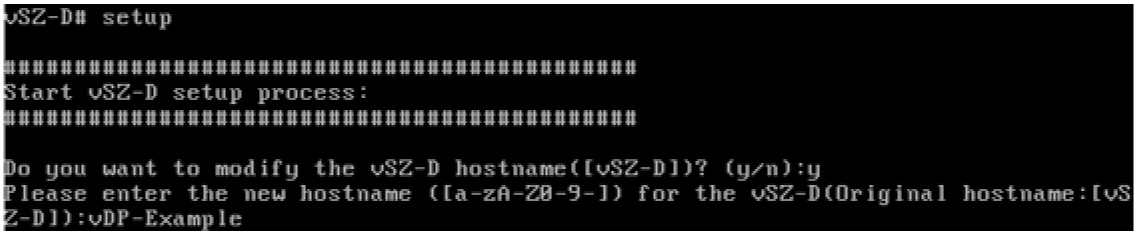
FIGURE 59 Login and Privileged mode



```
################################
#       Welcome to vSZ-D       #
################################
vSZ-D login: admin
Password:
Last login: Mon Feb  5 14:10:28 on tty1
Welcome to the RUCKUS WIRELESS vSZ-D Command Line Interface
vSZ-D> en
Password:
vSZ-D# setup
```

2. Run the **setup** command to configure the IP address for management and data interface. It is recommended to add a new host if you have multiple hosts for various configurations

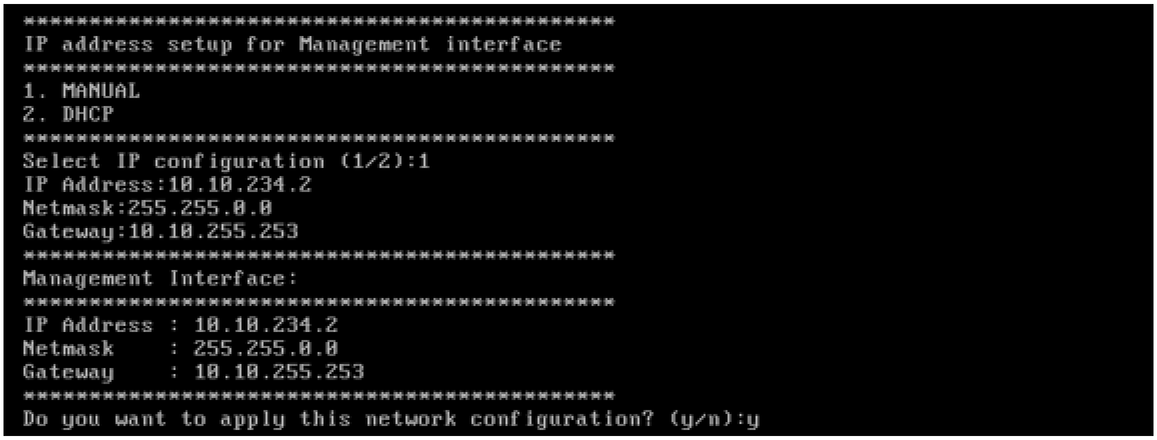
FIGURE 60 Execute the setup command



```
vSZ-D# setup

##################################################
Start vSZ-D setup process:
##################################################

Do you want to modify the vSZ-D hostname([vSZ-D])? (y/n):y
Please enter the new hostname ([a-zA-Z0-9-]) for the vSZ-D(Original hostname:[vS
Z-D]):vDP-Example
```

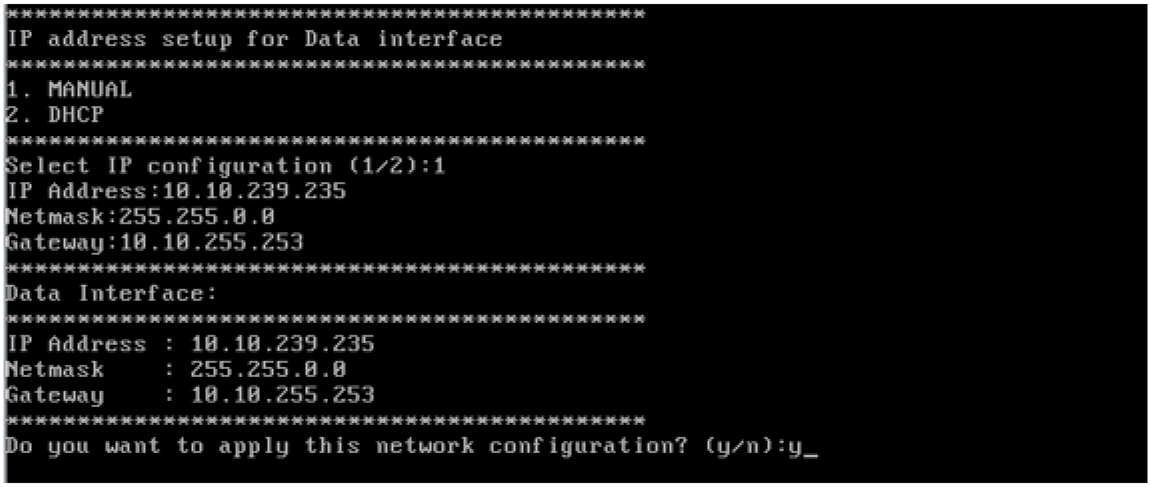
3. Choose the IP address setup (IPv4 only or IPv4 and IPv6) for Management and Data interface by either selecting manual or DHCP. On defining the IP setup the process of vSZ-D/SZ100-D connecting to vSZ controller starts.

FIGURE 61 Management interface



```
*********************************************
IP address setup for Management interface
*********************************************
1. MANUAL
2. DHCP
*********************************************
Select IP configuration (1/2):1
IP Address:10.10.234.2
Netmask:255.255.0.0
Gateway:10.10.255.253
*********************************************
Management Interface:
*********************************************
IP Address : 10.10.234.2
Netmask    : 255.255.0.0
Gateway    : 10.10.255.253
*********************************************
Do you want to apply this network configuration? (y/n):y
```

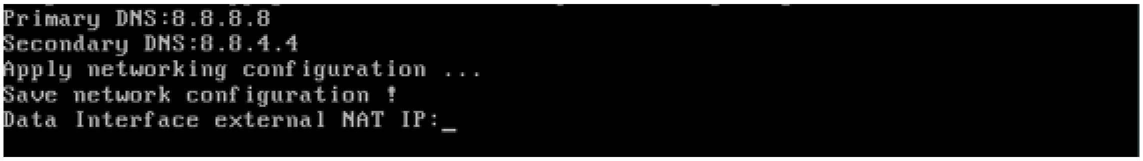
FIGURE 62 Data interface



```
*********************************************
IP address setup for Data interface
*********************************************
1. MANUAL
2. DHCP
*********************************************
Select IP configuration (1/2):1
IP Address:10.10.239.235
Netmask:255.255.0.0
Gateway:10.10.255.253
*********************************************
Data Interface:
*********************************************
IP Address : 10.10.239.235
Netmask    : 255.255.0.0
Gateway    : 10.10.255.253
*********************************************
Do you want to apply this network configuration? (y/n):y_
```

4. Enter the DNS setting and select Enter to skip the NAT IP setting.

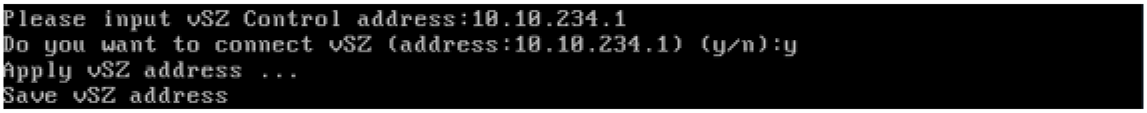
FIGURE 63 DNS setting



```
Primary DNS:8.8.8.8
Secondary DNS:8.8.4.4
Apply networking configuration ...
Save network configuration !
Data Interface external NAT IP:_
```

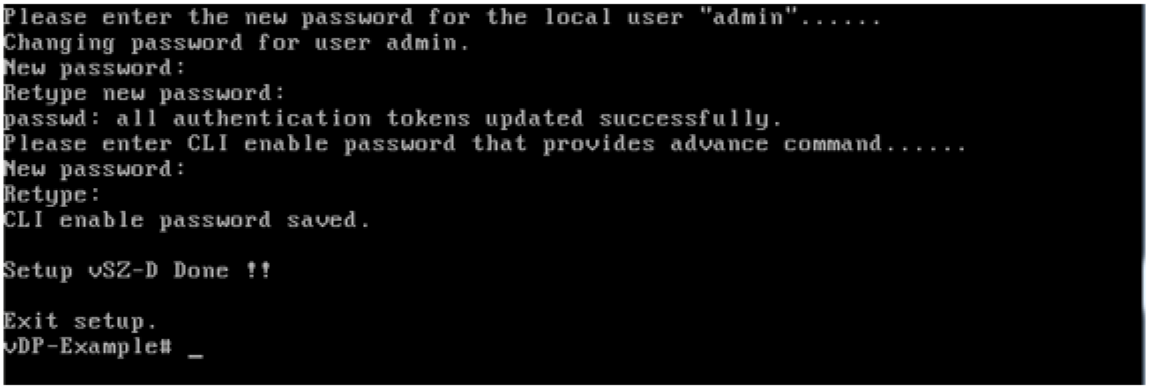
5. Enter vSZ control interface IP address. Follow the set of sequences as seen below for the vSZ-D/SZ100-D to connect to vSZ controller. This changes the mode for vSZ-D/SZ100-D as well as for vSZ.

FIGURE 64 vSZ control IP address



```
Please input vSZ Control address:10.10.234.1
Do you want to connect vSZ (address:10.10.234.1) (y/n):y
Apply vSZ address ...
Save vSZ address
```

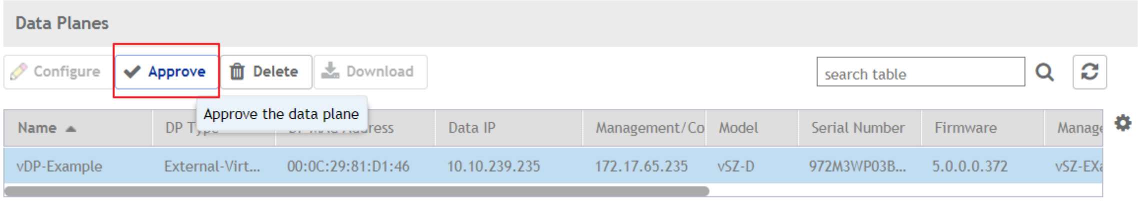
FIGURE 65 Connecting to vSZ



```
Please enter the new password for the local user "admin"......
Changing password for user admin.
New password:
Retype new password:
passwd: all authentication tokens updated successfully.
Please enter CLI enable password that provides advance command......
New password:
Retype:
CLI enable password saved.

Setup vSZ-D Done !!

Exit setup.
vDP-Example# _
```

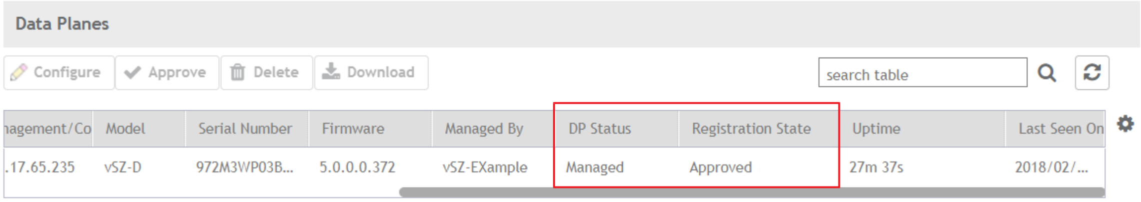
6. Exit from CLI console.
7. To view and approve the vSZ-D/SZ100-D, login to the web interface. Navigate to **Clusters** > **Data planes**. Select the vSZ-D/SZ100-D and click on **Approve.** On approval the status is greyed.

FIGURE 66 Approve the vSZ-D/SZ100-D



Name ▲	DP Ty	ress	Data IP	Management/Co	Model	Serial Number	Firmware	Manag
vDP-Example	External-Virt...	00:0C:29:81:D1:46	10.10.239.235	172.17.65.235	vSZ-D	972M3WP03B...	5.0.0.0.372	vSZ-EXa

FIGURE 67 Approved status



nagement/Co	Model	Serial Number	Firmware	Managed By	DP Status	Registration State	Uptime	Last Seen On
.17.65.235	vSZ-D	972M3WP03B...	5.0.0.0.372	vSZ-EXample	Managed	Approved	27m 37s	2018/02/...

You have successfully added the vSZ-D/SZ100-D image to the vSZ controller.

Upgrade Procedure

Upgrade Procedure

Procedure for upgrading to a new vSZ-D version.

Controller and vSZ-D/SZ100-D Firmware Compatibility Matrix

The below table indicates the compatibility matrix. In general, Ruckus supports N-2 vSZ-D releases with vSZ.

NOTE
vSZ-D version 3.2 needs to be upgraded to 3.4 or 3.5 prior to upgrading to 3.6 and onwards. vSZ support APs starting version 3.4.

TABLE 9 Controller and vSZ-D/SZ100-D Firmware Compatibility Matrix

vSZ Release	SZ100-D Release	vSZ-D Release				
	5.1.x	**5.1.x**	**5.0.x**	**3.6.x**	**3.5.x**	**3.4.x**
5.1.x	Yes	Yes	Yes	Yes	No	No
5.0.x	No	No	Yes	Yes	No	No
3.6.x	No	No	No	Yes	Yes	Yes
3.5 .x	No	No	No	No	Yes	Yes
3.4 .x	No	No	No	No	No	Yes

NOTE
Before starting this procedure, you should have already obtained a valid software upgrade file from Ruckus® Support or an authorized reseller.

NOTE
If you are upgrading both vSZ and vSZ-D/SZ100-D, Ruckus® recommends upgrading vSZ first before vSZ-D/SZ100-D.

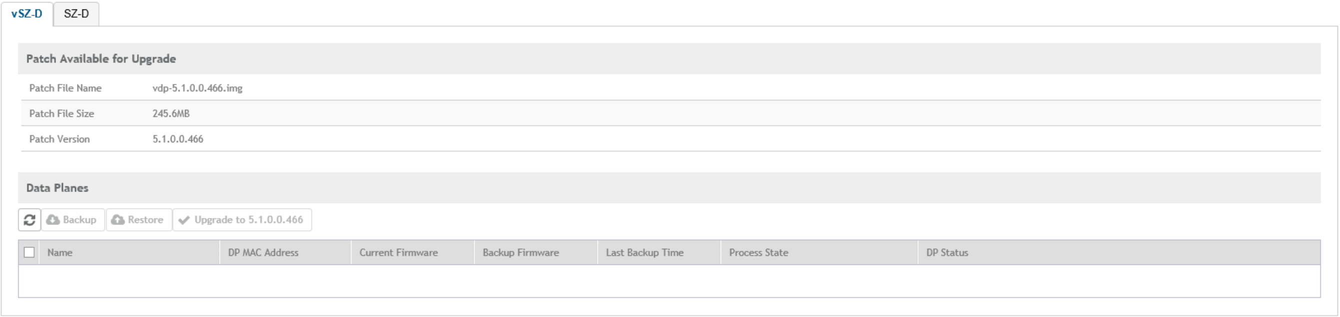
There is no order in upgrading the AP zone or vSZ-D/SZ100-D. During the vSZ upgrade, all tunnels stay up except the main tunnel which moves to the vSZ. Once the upgrade procedure is completed, allow ten minutes for the vSZ-D/SZ100-D to settle.

Upgrade to R5.0 does not support data migration (statistics, events, administrator logs). Existing system and network configuration is preserved. For further clarification, Contact Ruckus support.

Follow these steps to upgrade the vSZ-D/SZ100-D version.

1. Copy the software upgrade file that you received from Ruckus® to the computer where you are accessing the controller web interface or to any location on the network that is accessible from the web interface.
2. Go to **Controller web interface** > **Administration** > **Upgrade**.

FIGURE 68 Upgrade Section



Patch Available for Upgrade

Patch File Name	vdp-5.1.0.0.466.img
Patch File Size	245.6MB
Patch Version	5.1.0.0.466

Data Planes

□	Name	DP MAC Address	Current Firmware	Backup Firmware	Last Backup Time	Process State	DP Status

3. Select the **DP Patch** tab. The **DP Patch** page appears.
4. In the **Patch File Upload** section, click the **Browse** button, and then browse to the location of the software upgrade file.

   The file name of the software upgrade file is `vSZ-D-installer_{version}.ximg.`

5. Click **Upload** to upload the software upgrade file.

   The controller automatically identifies the Type of DP (vSZ-D or SZ-D) and switches to the specific Tab page. Uploads the file to its database, and then performs file verification. After the file is verified, the **Patch Available for Upgrade** section is populated with information about the upgrade file.

   The following details are displayed:

   - **Patch File Name**: Displays the name of the patch file.
   - **Patch File Size**: Displays the size of the patch file.
   - **Patch Version**: Displays the version of the patch file.

6. In Data Planes, identify the data plane you want to upgrade, and then choose a patch file version **Upgrade to**.
7. Click Apply to apply the patch file version to the virtual data plane.

   The following information about the virtual data plane is displayed after the patch file upgrade is completed.

   - **Name**: Displays the name of the virtual data plane.
   - **DP MAC Address**: Displays the MAC IP address of the data plane.
   - **Current Firmware**: Displays the current version of the data plane that has been upgraded.
   - **Backup Firmware**: Displays the backup version of the data plane.
   - **Last Backup Time**: Displays the date and time of last backup.
   - **Process State**: Displays the completion state of the patch file upgrade for the virtual data plane.
   - **DP Status**: Displays the DP status.

   You have successfully upgraded the data plane.

8. To verify if the upgrade is successful after a reboot:

   - Go to **Controller web interface** > **Administration** > **Upgrade** to view a confirmation message that the data plane firmware upgrade is complete.
   - Go to **Controller web interface** > **Configuration** > **System** > **Cluster Planes** to view a confirmation message that the data plane is managed with an upgrade firmware version.

NOTE
To have a copy of the data plane firmware or move back to the older version, you can select the data plane from the list and click **Backup** or **Restore** respectively.

vSZ-D Performance Recommendations

vSZ-D/SZ100-D has been designed to induce minimal latency in user data aggregation and forwarding. The unique design of the vSZ-D/SZ100-D software enables consistent packet performance with minimal throughput degradation as the number of tunnels or the number of clients' increase.

The fast path processing of the vSZ-D/SZ100-D is engineered to scale to the underlying NIC capacity profiles whether be it 1G or 10G speeds. vSZ-D/SZ100-D is designed to scale and handle data tunnels and data forwarding capabilities at high scale.

The following are some important observations and recommendations related to the vSZ-D/SZ100-D performance:

- To obtain the best throughput, Ruckus recommends operating vSZ-D/SZ100-D in directIO mode. This recommended mode of operation applies whether the hypervisor used is VMware or KVM.
- vSZ-D/SZ100-D supports vSwitch mode of operation for added flexibility in deployments where vSZ-D/SZ100-D may be co-located with other VMs for service chaining on the same underlying hardware. Note that the current observations are that in the vSwitch mode of operation, there is an induced performance impact in comparison with the directIO mode of operation. This may be due to the latency or performance bottleneck in virtIO and vSwitch sharing. This is still being researched at the Ruckus R&D Labs.
- There is an expected performance impact when enabling encryption (AES 128 bit and AES 256 bit) on the Ruckus GRE Tunnels. This is due to the overhead induced by the crypto processing on Ruckus AP and vSZ-D/SZ100-D due to the associated overheads of encryption and decryption on a per packet basis. The vSZ-D/SZ100-D software is designed to introduce minimal latency and overheads associated in packet processing. vSZ-D/SZ100-D takes advantage of the underlying Intel chip's crypto module for packet encryption and decryption and the associated impact is primarily bounded at the hardware level.

For specific recommendations and calibrations that may be needed for your deployment, contact Ruckus.

Ruckus Wireless, Inc., a wholly owned subsidiary of ARRIS International plc.
350 West Java Dr., Sunnyvale, CA 94089 USA
www.ruckuswireless.com