



# Ruckus Wireless™ Virtual SmartZone™

## Getting Started Guide for SmartZone 3.2

Part Number 800-71029-001 Rev B  
Published January 2016

[www.ruckuswireless.com](http://www.ruckuswireless.com)

## Copyright Notice and Proprietary Information

Copyright 2015. Ruckus Wireless, Inc. All rights reserved.

No part of this documentation may be used, reproduced, transmitted, or translated, in any form or by any means, electronic, mechanical, manual, optical, or otherwise, without prior written permission of Ruckus Wireless, Inc. ("Ruckus"), or as expressly provided by under license from Ruckus.

### Destination Control Statement

Technical data contained in this publication may be subject to the export control laws of the United States of America. Disclosure to nationals of other countries contrary to United States law is prohibited. It is the reader's responsibility to determine the applicable regulations and to comply with them.

### Disclaimer

THIS DOCUMENTATION AND ALL INFORMATION CONTAINED HEREIN ("MATERIAL") IS PROVIDED FOR GENERAL INFORMATION PURPOSES ONLY. RUCKUS AND ITS LICENSORS MAKE NO WARRANTY OF ANY KIND, EXPRESS OR IMPLIED, WITH REGARD TO THE MATERIAL, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY, NON-INFRINGEMENT AND FITNESS FOR A PARTICULAR PURPOSE, OR THAT THE MATERIAL IS ERROR-FREE, ACCURATE OR RELIABLE. RUCKUS RESERVES THE RIGHT TO MAKE CHANGES OR UPDATES TO THE MATERIAL AT ANY TIME.

### Limitation of Liability

IN NO EVENT SHALL RUCKUS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL OR CONSEQUENTIAL DAMAGES, OR DAMAGES FOR LOSS OF PROFITS, REVENUE, DATA OR USE, INCURRED BY YOU OR ANY THIRD PARTY, WHETHER IN AN ACTION IN CONTRACT OR TORT, ARISING FROM YOUR ACCESS TO, OR USE OF, THE MATERIAL.

### Trademarks

Ruckus Wireless, Ruckus, Bark Logo, BeamFlex, ChannelFly, Ruckus Pervasive Performance, SmartCell, ZoneFlex, Dynamic PSK, FlexMaster, MediaFlex, MetroFlex, Simply Better Wireless, SmartCast, SmartMesh, SmartSec, SpeedFlex, ZoneDirector, ZoneSwitch, and ZonePlanner are trademarks of Ruckus Wireless, Inc. in the United States and other countries. All other product or company names may be trademarks of their respective owners.

# Contents

## About This Guide

Document Conventions . . . . .	7
Related Documentation . . . . .	7
Documentation Feedback . . . . .	7

## 1 Preparing to Install the vSZ

Preparing a Hypervisor . . . . .	9
Obtaining the vSZ Distribution . . . . .	9
Preparing the vSZ Interface Settings to Use . . . . .	10
Determining the System Resources That the Virtual Machine Requires . . . . .	11
Clustering Limitations . . . . .	12

## 2 Installing the vSZ on a Hypervisor

Installing the vSZ on VMWare™ vSphere Hypervisor . . . . .	13
Before You Begin . . . . .	13
Creating a vSZ Instance from the OVA File . . . . .	14
Allocating Resources and Assigning Network Interfaces . . . . .	24
Powering on the vSZ Virtual Machine . . . . .	26
Installing the vSZ on Windows Server Hyper-V . . . . .	27
Installing the vSZ on a Kernel-based Virtual Machine Hypervisor . . . . .	39
Extracting the vSZ Image . . . . .	39
Setting Up the vSZ . . . . .	43

## 3 Installing the vSZ on Microsoft Azure

Logging into Microsoft Azure . . . . .	52
Creating a Storage Account and Container . . . . .	54
Uploading the vSZ Image to Microsoft Azure . . . . .	56
Creating a vSZ Image on Microsoft Azure . . . . .	58
Creating a Network . . . . .	59
Creating a vSZ Virtual Machine . . . . .	62
Configuring Port Numbers for Virtual Machines . . . . .	67
Assigning a Static Internal IP Address to a Virtual Machine . . . . .	70
Assigning a Static Public IP Address to a VM . . . . .	74

<b>4</b>	<b>Installing the vSZ on the Google Computing Engine</b>	
	Before you begin . . . . .	78
	Logging into GCE and Selecting a Project . . . . .	78
	Creating a Storage Bucket . . . . .	79
	Uploading the vSZ image to a Storage . . . . .	81
	Creating a vSZ Image for Virtual Machines . . . . .	83
	Creating Networks and Configuring Firewall Rules . . . . .	84
	Creating Virtual Machine (VM) Instances . . . . .	88
<b>5</b>	<b>Configuring the Virtual Machine Interfaces</b>	
	Setting Up the vSZ with One Interface . . . . .	93
	Setting Up the vSZ with Three Interfaces . . . . .	98
	Important Notes About Selecting the System Default Gateway . . . . .	101
<b>6</b>	<b>Using the Setup Wizard to Install vSZ</b>	
	Before You Begin . . . . .	103
	Step 1: Start the Setup Wizard and Set the Language . . . . .	104
	Step 2: Select the Profile Configuration That Corresponds to Your vSZ License . . . . .	105
	Step 3: Configure the Management IP Address Settings . . . . .	106
	Important Notes About Selecting the Gateway . . . . .	113
	Step 4: Configure the Cluster Settings . . . . .	113
	If This vSZ Is Forming a New Cluster . . . . .	115
	If This vSZ Is Joining an Existing Cluster . . . . .	115
	Step 5: Set the Administrator Password . . . . .	117
	Step 6: Verify the Settings . . . . .	119
	Logging On to the Web Interface . . . . .	121
<b>7</b>	<b>Configuring the vSZ High-Scale for the First Time</b>	
	Creating an AP Zone . . . . .	124
	Configuring AAA Servers and Hotspot Settings . . . . .	128
	Adding an AAA Server . . . . .	128
	Creating a Hotspot Service . . . . .	130
	Creating a Registration Rule . . . . .	133
	Configuring the Rule Priority . . . . .	135
	Defining the WLAN Settings of an AP Zone . . . . .	136
	General Options . . . . .	137
	WLAN Usage . . . . .	137
	Authentication Options . . . . .	138
	Encryption Options . . . . .	138

Authentication & Accounting Service . . . . .	140
Options . . . . .	140
RADIUS Options . . . . .	141
Advanced Options . . . . .	141
Configuring DHCP Option 43 . . . . .	143
Verifying That Wireless Clients Can Associate with a Managed AP . . . . .	146
What to Do Next . . . . .	147

## **8 Ensuring That APs Can Discover the Controller on the Network**

Is LWAPP2SCG Enabled on the Controller? . . . . .	149
Obtaining the LWAPP2SCG Application. . . . .	149
Enabling LWAPP2SCG . . . . .	149
Method 1: Perform Auto Discovery of the Controller Using the SmartLicense Server. . .	150
Method 2: Perform Auto Discovery on Same Subnet, then Transfer the AP to Intended Subnet . . . . .	151
Method 3: Register the Controller with the DNS Server . . . . .	151
Method 4: Configure DHCP Option 43 on the DHCP Server . . . . .	154
Method 5: Manually Configure the Controller Address on the AP's Web Interface. . . . .	157
What to Do Next . . . . .	158

## **Index**

# About This Guide

This *Virtual SmartZone™ (vSZ) Getting Started Guide* provides information on how to set up the vSZ virtual appliance on the network. You can install the vSZ on any of the supported hypervisors.

Topics covered in this guide include preparing your chosen hypervisor, installing the vSZ image on to the hypervisor, and completing the vSZ Setup Wizard.

This guide is intended for use by those responsible for installing and setting up network equipment. Consequently, it assumes a basic working knowledge of local area networking, 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 Wireless Support website at <https://support.ruckuswireless.com/documents>.

# Document Conventions

Table 1 and Table 2 list the text and notice conventions that are used throughout this guide.

Table 1. Text conventions

Convention	Description	Example
monospace	Represents information as it appears on screen	[Device name]>
<b>monospace bold</b>	Represents information that you enter	[Device name]> <b>set ipaddr 10.0.0.12</b>
<b>default font bold</b>	Keyboard keys, software buttons, and field names	On the <b>Start</b> menu, click <b>All Programs</b> .
<i>italics</i>	Screen or page names	Click <b>Advanced Settings</b> . The <i>Advanced Settings</i> page appears.

Table 2. Notice conventions

Notice Type	Description
<b>NOTE</b>	Information that describes important features or instructions
<b>CAUTION!</b>	Information that alerts you to potential loss of data or potential damage to an application, system, or device
<b>WARNING!</b>	Information that alerts you to potential personal injury

## Related Documentation

For a complete list of documents that accompany this release, refer to the Release Notes.

## Documentation Feedback

Ruckus Wireless is interested in improving its documentation and welcomes your comments and suggestions. You can email your comments to Ruckus Wireless at:

[docs@ruckuswireless.com](mailto:docs@ruckuswireless.com)

When contacting us, please include the following information:

- Document title

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

For example:

- Virtual SmartZone (vSZ) Getting Started Guide
- Part number: 800-71029-001
- Page 88



# Preparing to Install the vSZ

# 1

In this chapter:

- [Preparing a Hypervisor](#)
- [Obtaining the vSZ Distribution](#)
- [Preparing the vSZ Interface Settings to Use](#)
- [Determining the System Resources That the Virtual Machine Requires](#)

## Preparing a Hypervisor

[Table 3](#) lists the hypervisors (and their release versions) on which you can install the vSZ.

Table 3. Hypervisors that the vSZ supports

Vendor	Hypervisor	Version
VMWare	ESXi	5.x
Windows	Windows Server Hyper-V	Windows Server Hyper-V
KVM	CentOS	7.0

The vSZ installation procedures for each of these hypervisors vary. For more information, see [Installing the vSZ on a Hypervisor](#).

## Obtaining the vSZ Distribution

From the vSZ download page on the Ruckus Wireless support website, download the .OVA file and documentation for the controller. The vSZ distribution package, which is based on the Open Virtualization Format (OVF) framework, consists of a virtual appliance containing the following files:

- Description file (.ovf)
- Manifest file (.mf)
- Virtual machine state file (.vmdk)

These three files are consolidated into a TAR archive file and distributed as an Open Virtual Appliance (OVA) package. This OVA package can be imported directly into your chosen hypervisor.

## Preparing the vSZ Interface Settings to Use

The vSZ comes with the option to operate with either one (1) network interface or three (3) network interfaces (see [Table 4](#)). Once the network interface configuration has been made and setup executed, the number of network interfaces can no longer be modified.

---

**CAUTION!** If you choose to operate the vSZ with three network interfaces, you must configure the three vSZ interfaces to be on three different subnets when you run the Setup Wizard. Failure to do so may result in loss of access to the web interface or failure of system functions and services.

---

Before installing the vSZ, prepare the following required network settings:

- IP address
- Netmask
- Gateway
- Primary DNS server
- Secondary DNS server

Table 4. vSZ interfaces

Interface	Description
AP	Used for AP configuration and client traffic
Cluster	Used for cluster traffic
Management (Web)	Used for management traffic. The IP address that you assign to this interface will be the IP address at which you can access the vSZ web interface.

# Determining the System Resources That the Virtual Machine Requires

The number of APs and clients that vSZ can support depends on the system resources (CPU and memory) that the virtual machine running vSZ has. vSZ is capable of automatically scaling to and supporting a higher number of APs and clients if it determines, at system bootup, that there is sufficient CPU and memory on the virtual machine to support more APs and clients.

[Table 5](#) (vSZ High-Scale profile configuration) and [Table 6](#) (vSZ Essentials profile configuration) list the maximum recommended number of APs and clients that the vSZ can support based on the available vCPU and memory available on the virtual machine<sup>1</sup>. The first row in [Table 5](#), for example, shows that to support up to 25 APs, the vSZ must have at least 2-core CPU and 8GB of RAM. Whenever the CPU or memory settings are changed, the virtual controller instance must be rebooted for the updated settings to be applied to it.

---

**CAUTION!** When either your AP count or wireless client count reaches the recommended maximum number in the tables below, you must also allocate additional system resources to the virtual machine. For example, if you initially allocated Level 1 resources to the VM to handle 25 APs and your AP count increases to 26, you must update the VM resources to Level 2 to prevent performance-related issues.

---

All resource levels in the following tables are provided based on Intel Xeon CPU E5-2630v2 @2.60 GHz. If the server on which you are hosting the controller software is using a different CPU generation and/or model, it may perform differently. In this case, CPU adjustments can be made to generate the same level of performance.

Table 5. High Scale profile configuration: Recommended system resources

AP Count	Client Count	Resource Level	Max Nodes per Cluster	Disk Size (GB)	vCPU (Core)	RAM (GB)	Physical Free RAM in MB (Threshold)	Max Preserved Events
25	500	1	2	100	2	8	8001 (7900)	15k
50	1000	2	2	100	2	8	8001 (7900)	30k
100	2000	3	2	100	2	8	8001 (7900)	60k
500	10000	4	2	100	4	9	9011(8900)	300k

- 
1. These scalability figures have been observed on the vSZ for vSZ 3.2

Table 5. High Scale profile configuration: Recommended system resources

AP Count	Client Count	Resource Level	Max Nodes per Cluster	Disk Size (GB)	vCPU (Core)	RAM (GB)	Physical Free RAM in MB (Threshold)	Max Preserved Events
1000	20000	5	2	100	4	11	11031 (11000)	600k
2500	50000	6	2	300	6	15	15071(15000)	1500k
10000	100000	7	4	600	24	48	48401 (48000)	3000k

Table 6. Essentials profile configuration: Recommended system resources

AP Count	Client Count	Resource Level	Max Nodes per Cluster	Disk Size (GB)	vCPU (Core)	RAM (GB)	Physical Free RAM in MB (Threshold)	Max Preserved Events
100	2000	1	2	100	2	12	12041 (12000 )	1k
1024	25000	2	4	250	8	20	20121 (20000 )	10k

## Clustering Limitations

If you are deploying the vSZ in clusters, take note of the following limitations:

- vSZ-H supports clustering of up to 4 nodes when using Resource Level 4. At 4 nodes, the maximum number of APs and clients that can be supported are 30,000 and 300,000 respectively.
- vSZ-E supports clustering of up to 4 nodes when using Resource Level 2. Above 2 nodes in a cluster at Resource Level 2, additional 2 CPU cores need to be added to each node to support the added search capabilities and replication. At 4 nodes, the maximum number of APs and clients that can be supported are 3,000 and 60,000 respectively.

In this chapter:

- [Installing the vSZ on VMWare™ vSphere Hypervisor](#)
- [Installing the vSZ on Windows Server Hyper-V](#)
- [Installing the vSZ on a Kernel-based Virtual Machine Hypervisor](#)

## Installing the vSZ on VMWare™ vSphere Hypervisor

Follow these steps to install the vSZ on a VMWare vSphere hypervisor:

- [Before You Begin](#)
- [Creating a vSZ Instance from the OVA File](#)
- [Allocating Resources and Assigning Network Interfaces](#)
- [Powering on the vSZ Virtual Machine](#)

### Before You Begin

Verify that you have the prerequisites before installing the vSZ on VMWare vSphere.

- Verify that vSphere client is installed.
- You can deploy the vSZ only on hosts that are running ESXi version 5.1 or later.
- The vSZ appliance requires at least 100GB of disk space and is limited to a maximum size of 600GB. The vSZ appliance can be deployed with thin-provisioned virtual disks that can grow to the maximum size of 600GB.

## Creating a vSZ Instance from the OVA File

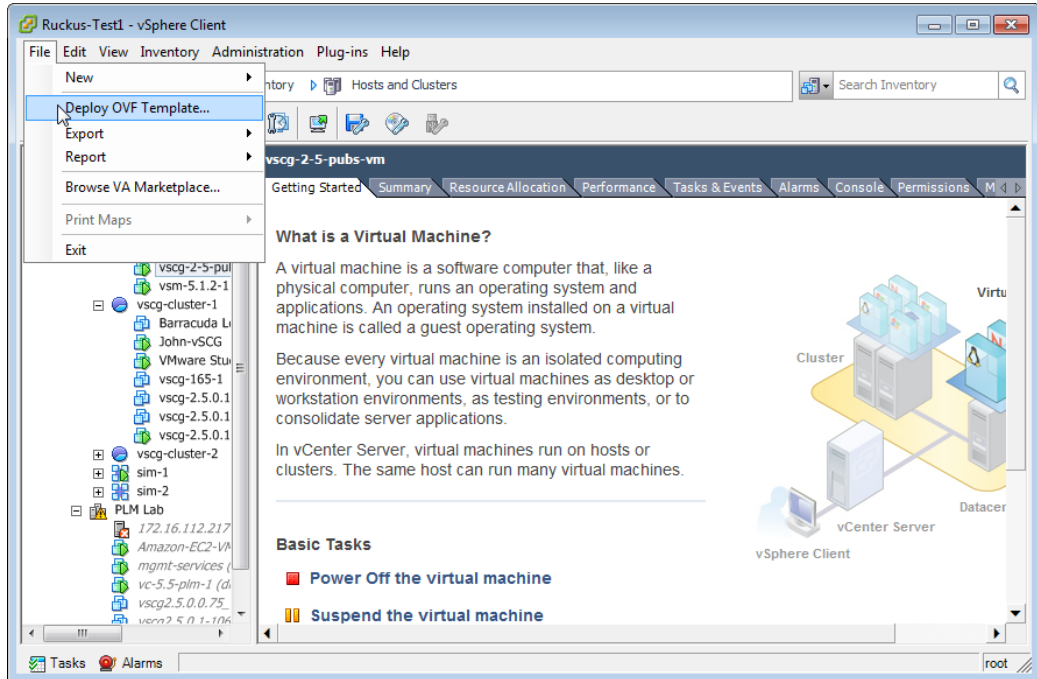
Before continuing, make sure you have already downloaded the vSZ distribution package from the Ruckus Wireless. See [Obtaining the vSZ Distribution](#) for more information.

**NOTE:** The following procedure describes how to create a vSZ instance using the vSphere Web Client.

Follow these steps to create a vSZ instance from the OVA file.

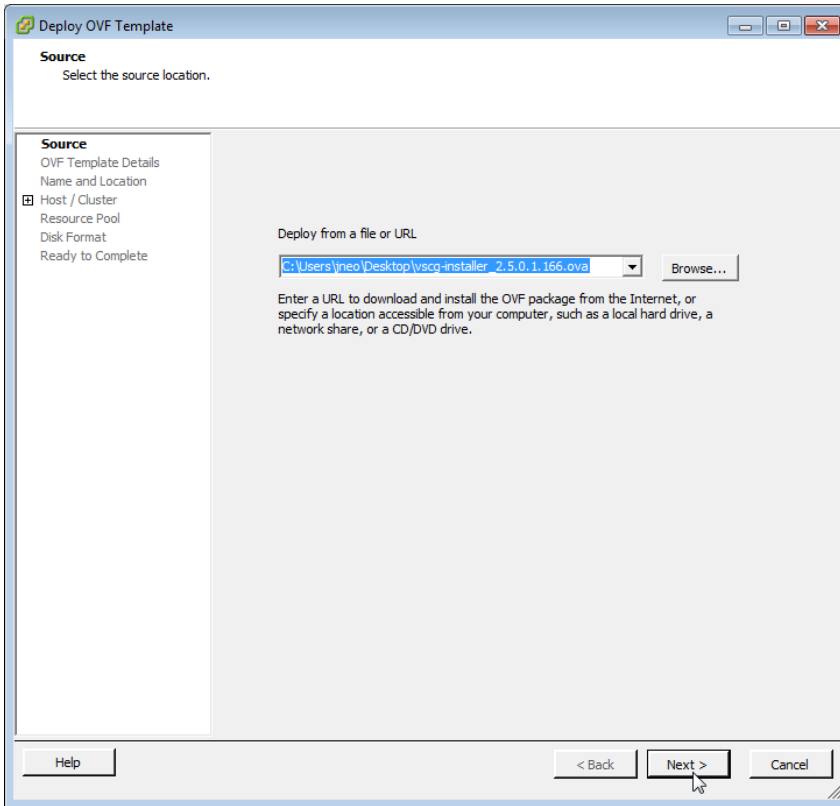
- 1 Use the VMWare vSphere client to log on to the ESXi management interface.
- 2 Click **File > Deploy OVF Template**. The *Source* screen of the *Deploy OVF Template* wizard appears.

Figure 1. Click Deploy OVF Template



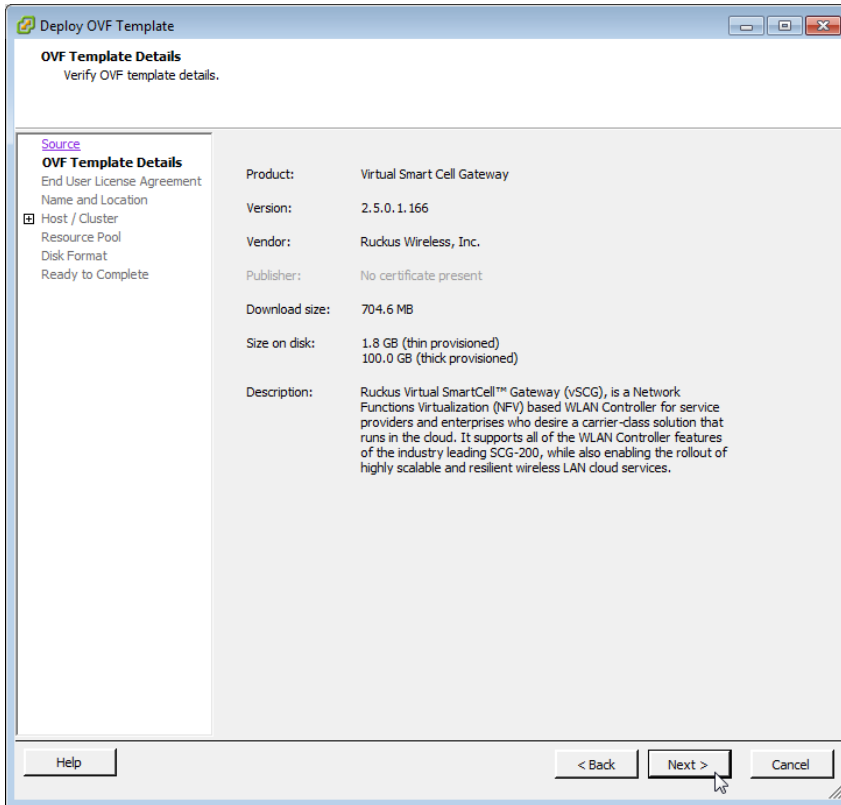
- 3 Click **Browse** to locate the `.ova` file that you downloaded earlier. Select the template.

Figure 2. Click Browse, and then locate and select `.ova` file



4 Click **Next**. The *OVF Template Details* screen appears.

Figure 3. The OVF Template Details screen

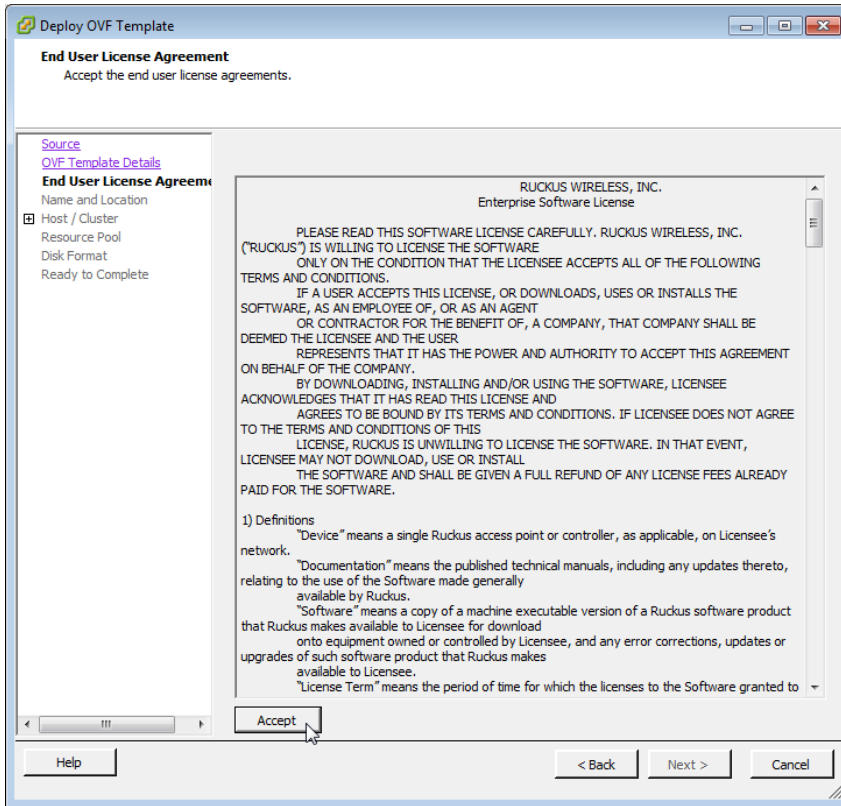


5 Review the OVA virtual appliance details, and then click **Next**. The End User License Agreement (EULA) screen appears.



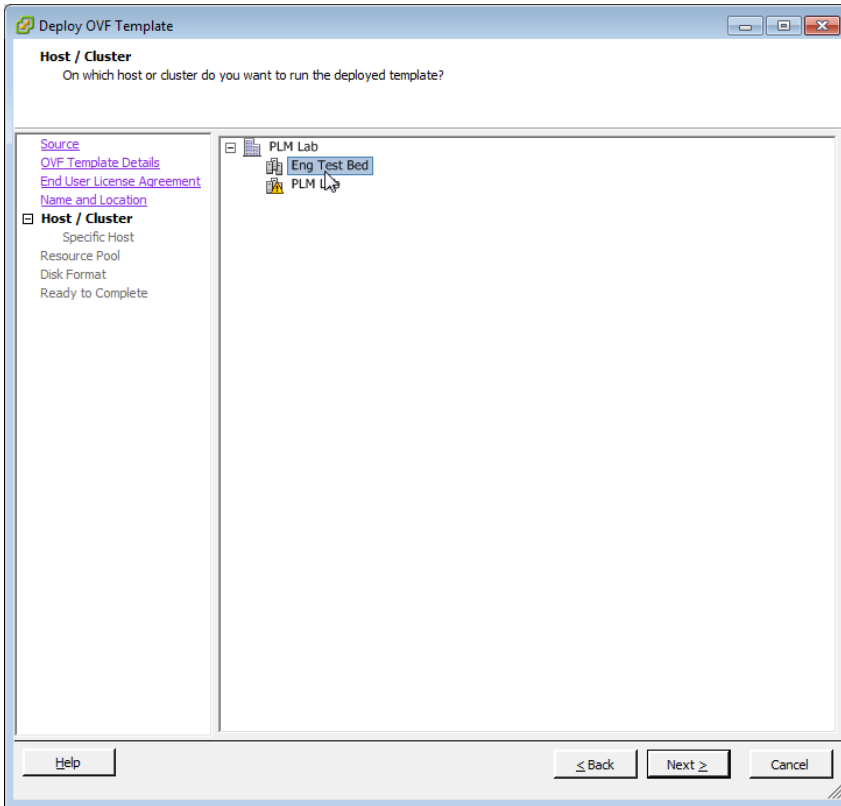
- 6 Click **Accept** to agree to the EULA terms, and then click **Next**. The *Host/Cluster* screen appears.

Figure 4. Accept the EULA for the vSZ OVA



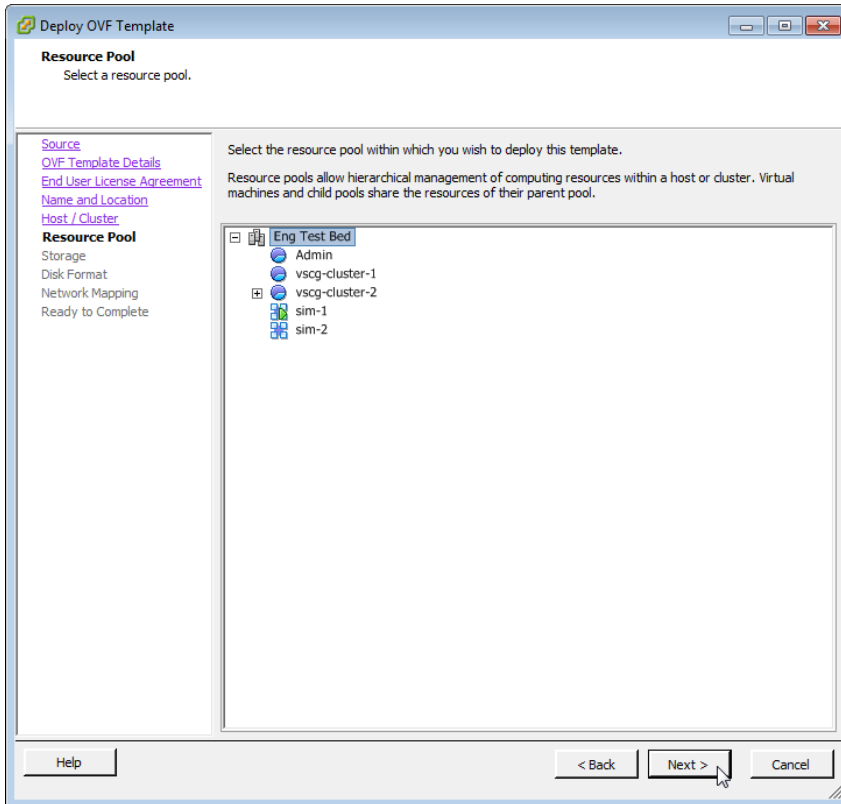
- 7 Select the host or cluster on which you want to run the deployed template, and then click **Next**. The *Resource Pool* screen appears.

Figure 5. Select the destination host or cluster



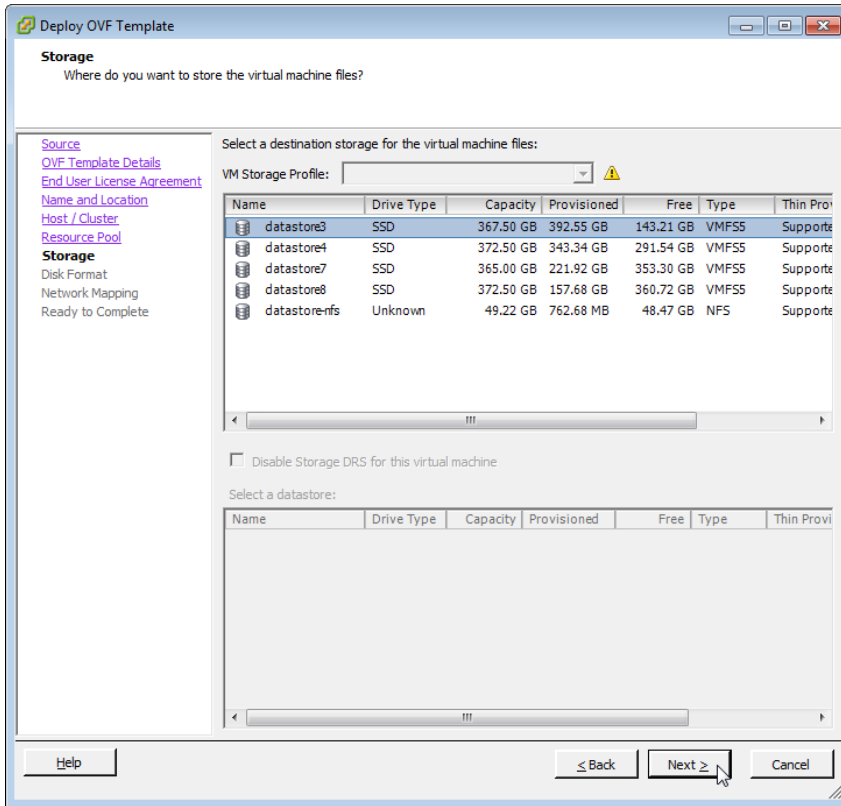
- 8 Select the resource pool within which you want to deploy the template, and then click **Next**. The storage screen appears.

Figure 6. Select the resource pool for the OVA template



- 9 Select the destination storage (data store) for virtual machine files, and then click **Next**. The *Disk Format* screen appears.

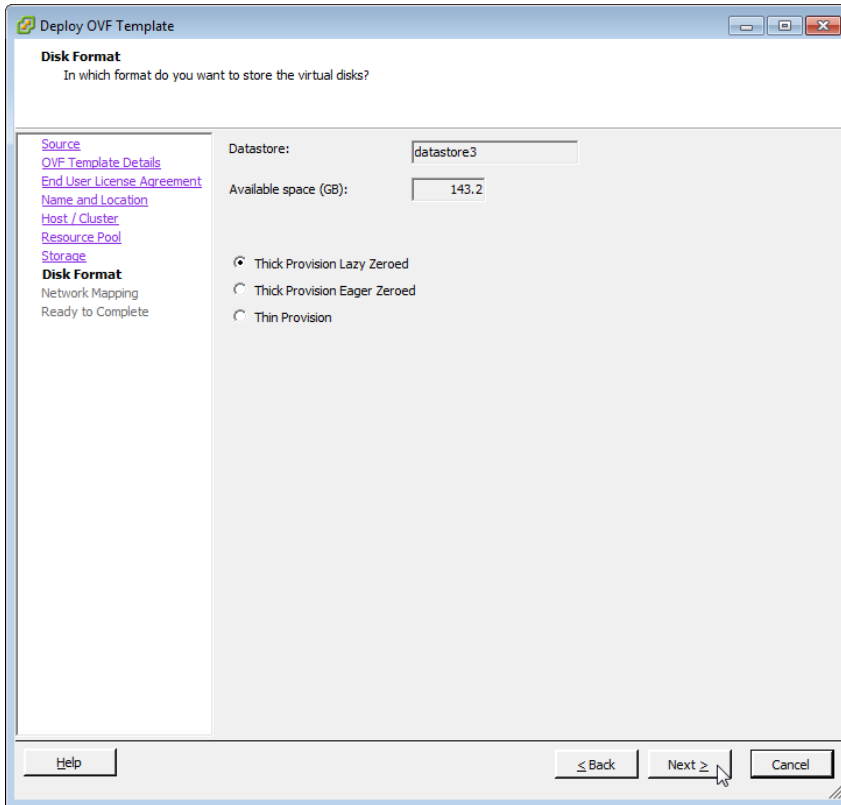
Figure 7. Select the data store for the virtual machine files



10 Select the disk format that is appropriate for your deployment scenario. Options include:

- Thick Provision Lazy Zeroed
- Thick Provision Eager Zeroed
- Thin Provision

Figure 8. Select the disk format for your deployment scenario



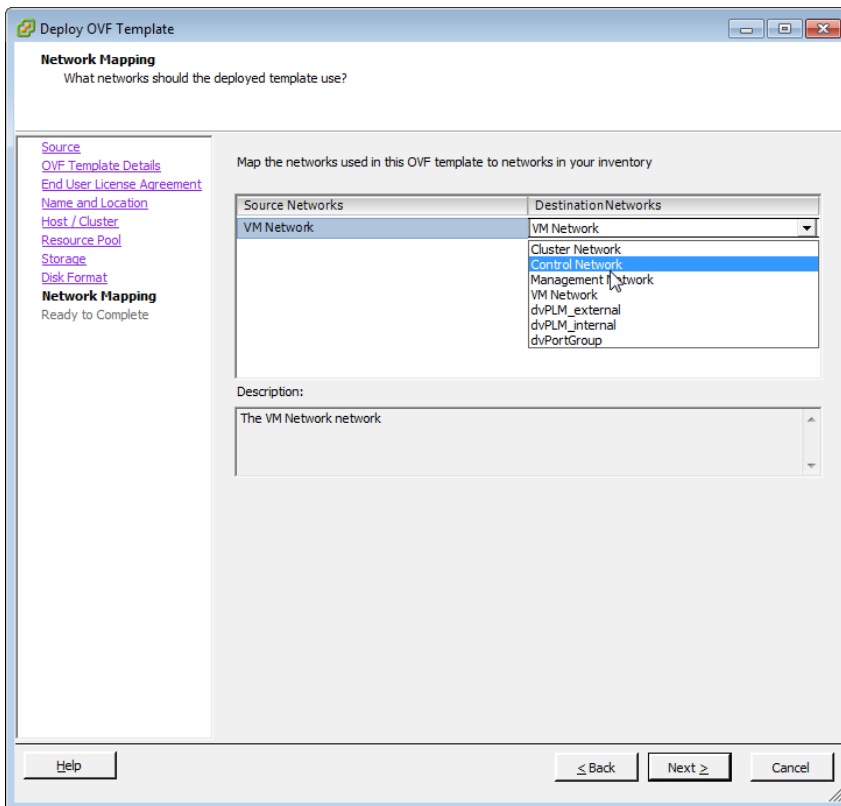
- 11 Click **Next**. The *Network Mapping* screen appears.
- 12 Select the ESXi virtual network interface that you want to use for the control interface, and then click **Next**. The *Ready to Complete* screen appears. For more information see, [Allocating Resources and Assigning Network Interfaces](#).

---

**NOTE:** The installation screen only allows you to select the virtual network interface for the control interface. After you complete the installation (and before you power on and set up the vSZ), you will need to adjust the cluster and management interfaces as appropriate.

---

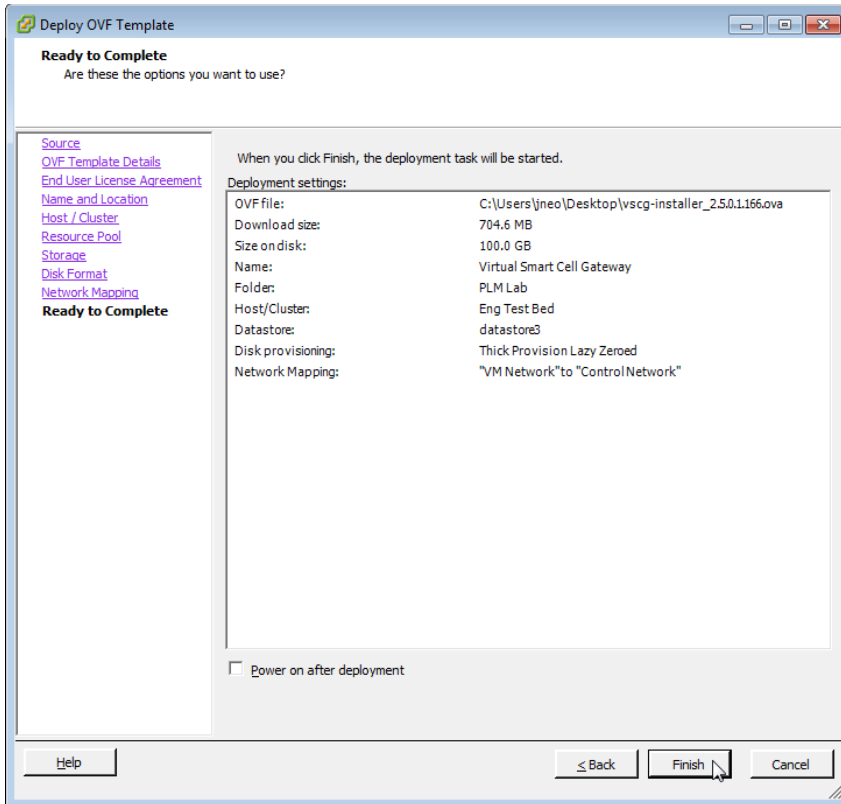
Figure 9. Select the virtual network interface that the template will use



**13** Review the settings that you have configured on the previous screens.

If you find a setting that you want to change, click **Back** until you reach the screen where you can edit the setting. Update the setting, and then click **Next** until you reach the *Ready to Complete* screen again.

Figure 10. Review the settings that you have configured



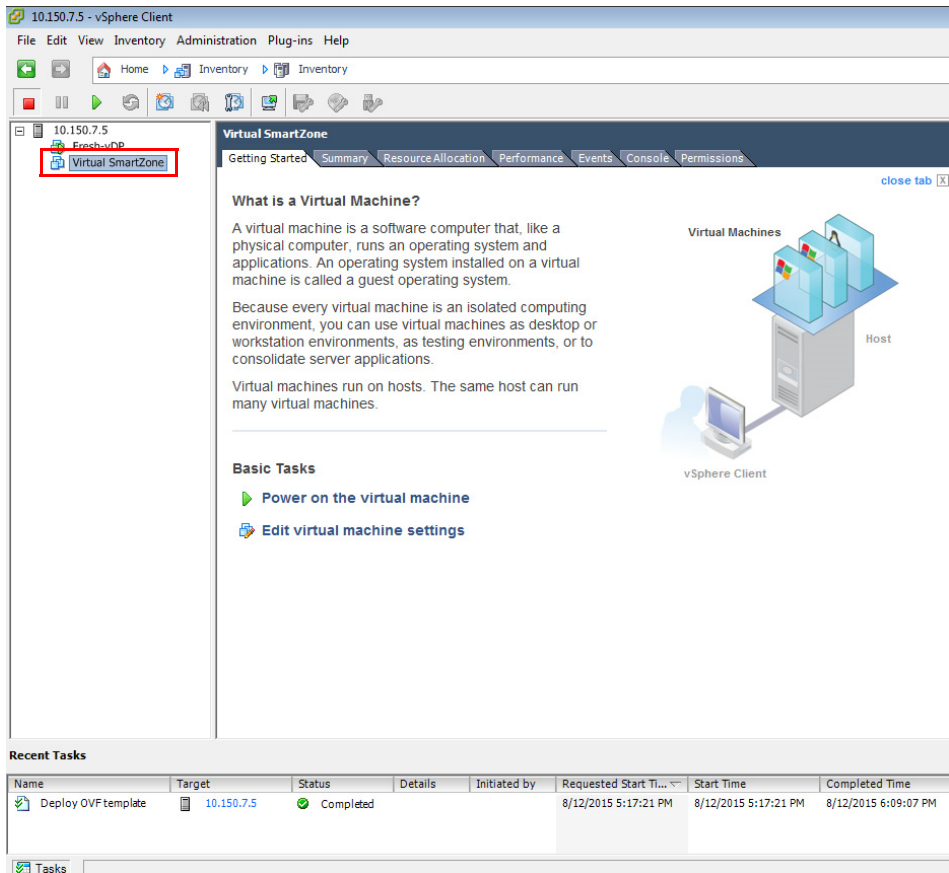
**14** Make sure that the **Power on after deployment** check box is clear so you can adjust the network settings before the vSZ setup.

**CAUTION!** If you power on the vSZ after installation, you will no longer be able to adjust the network settings.

**15** Click **Finish**.

ESXi deploys the new vSZ instance. When ESXi completes the deployment, the new vSZ instance appears on the list of installed virtual machines on the target host.

Figure 11. The vSZ instance appears on the list of installed VMs



You have completed creating a vSZ instance from the OVA file.

## Allocating Resources and Assigning Network Interfaces

Before starting the vSZ instance for the first time, edit the virtual machine settings to allocate CPU and memory resources to the vSZ and to assign the ESXi network interfaces to the remaining vSZ interfaces (cluster and management).

**NOTE:** Before continuing, review [Determining the System Resources That the Virtual Machine Requires](#) and determine the minimum resources that you need to allocate to the vSZ instance. If the setup program detects that the vSZ instance does not have sufficient resources, it will halt the setup process.



Follow these steps to allocate resources and assign network interfaces to the vSZ.

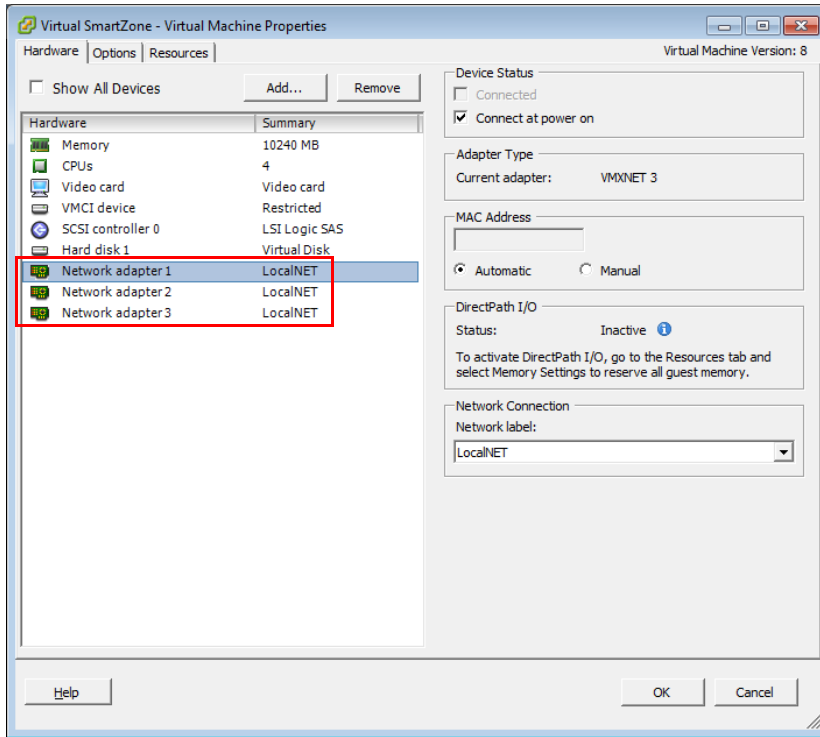
- 1 On the list of virtual machines, click the new vSZ instance.
- 2 Click **Actions** to display the additional options, and then click **Edit Settings**.
- 3 Set the number of CPUs and the amount of RAM to allocate to the vSZ instance. By default, the OVA template is set to 4 CPUs and 8GB of RAM.
- 4 Under *Network adapter 1*, verify that it is the same ESXi network interface that you selected for the control interface during the OVA import process. Ensure that the **Connect at Power On** check box is selected.
- 5 Under *Network adapter 2*, select the ESXi network interface for the cluster interface from the drop-down list. Ensure that the **Connect at Power On** option is selected.
- 6 Under *Network adapter 3*, select the ESXi network interface for the management interface from the drop-down list. Ensure that the **Connect at Power On** option is selected.

---

**NOTE:** While assigning interfaces, ensure that each interface is in a different subnet.

---

Figure 12. Select the interfaces to use



7 Click **OK**.

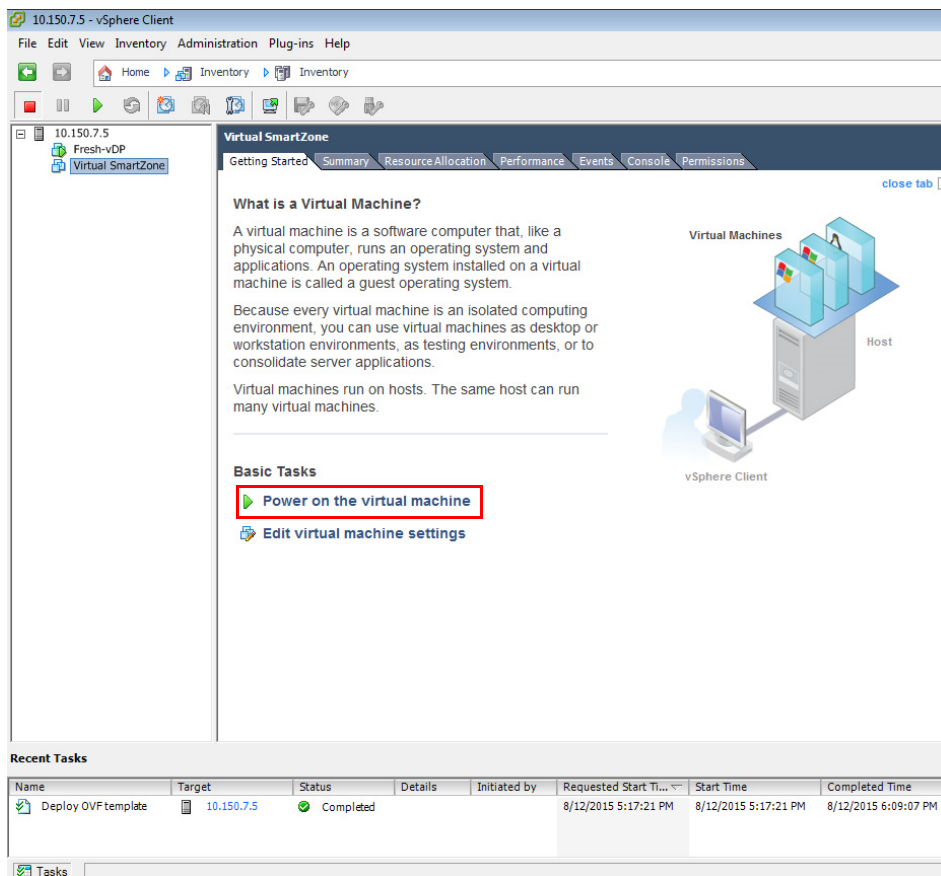
You have completed allocating resources and assigning network interfaces to the vSZ.

## Powering on the vSZ Virtual Machine

The next step is to power on the vSZ virtual appliance.

- 1 From the list of virtual machines on the host, click the vSZ instance.
- 2 Under *Basic Tasks*, click **Power on the virtual machine**.

Figure 13. Click Power on the virtual machine



- 3 Open a console window to monitor the startup process. To do this, click the **Console** tab.

After the vSZ completes its startup process, you are ready to configure its interfaces using a console connection to perform this task.

For information on how to configure the vSZ interface, see [Configuring the Virtual Machine Interfaces](#).

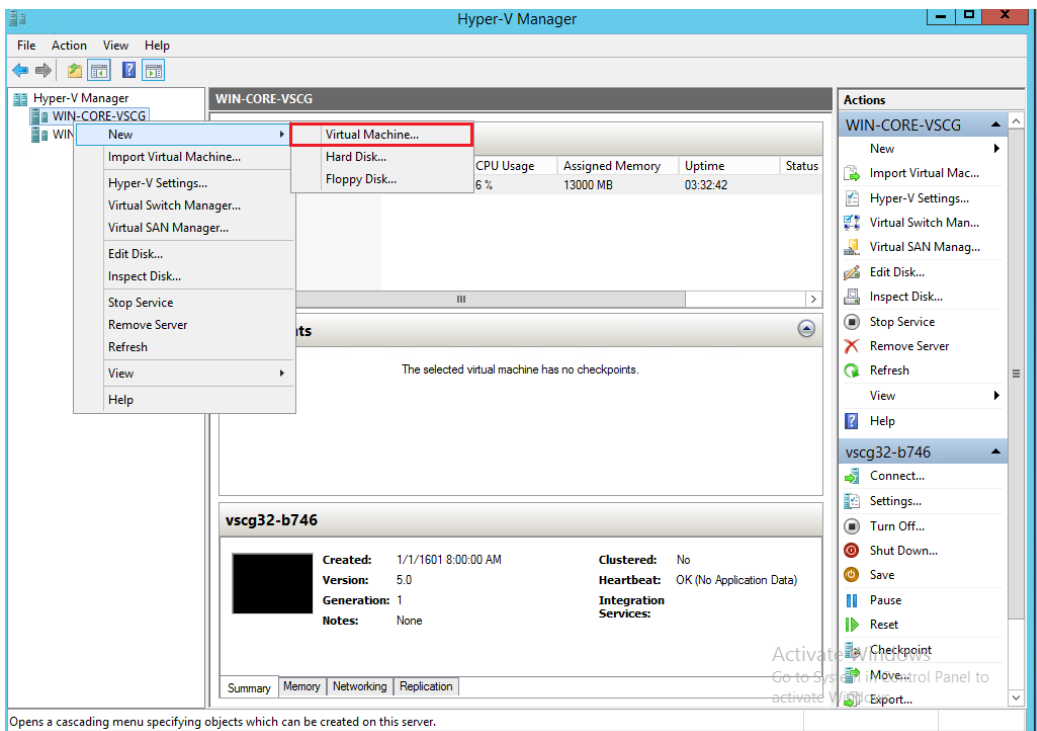
## Installing the vSZ on Windows Server Hyper-V

Before you begin, verify that Hyper-V is enabled on Windows Server.

Follow these steps to install the vSZ on Windows Server Hyper-V.

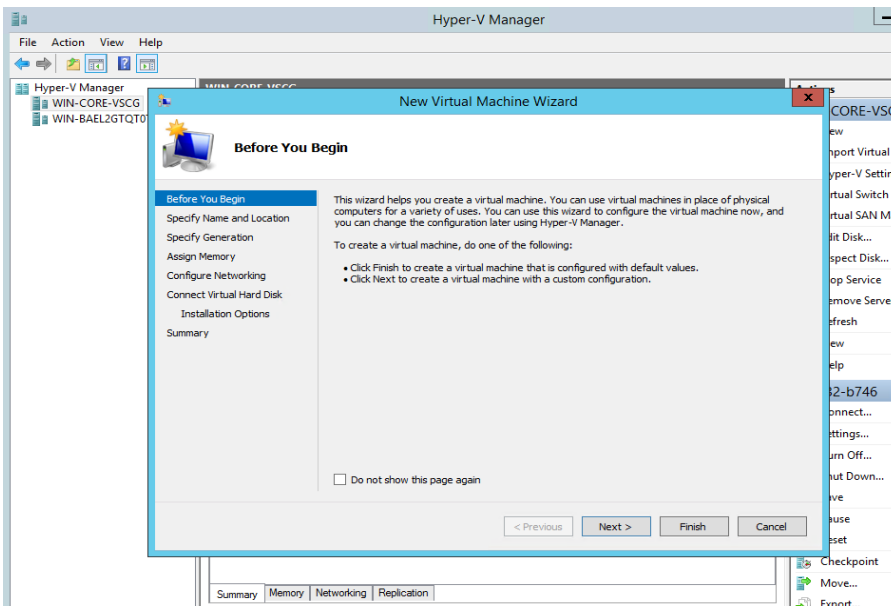
- 1 Obtain a copy of the vSZ image in VHD format.
- 2 Extract the vSZ image to the .vhd disk file.
- 3 Copy the image to the Windows Server on which you are running Hyper-V.
- 4 On the Windows Server, click **Start > Administrative Tools**, and then double-click **Hyper-V Manager**.
- 5 In the *Hyper-V Manager*, select the Hyper-V core for which you want to create a virtual machine and click **Action > New > Virtual Machine**.  
The *New Virtual Machine Wizard* appears and displays the *Before You Begin* screen.

Figure 14. Click Action > New > Virtual Machine



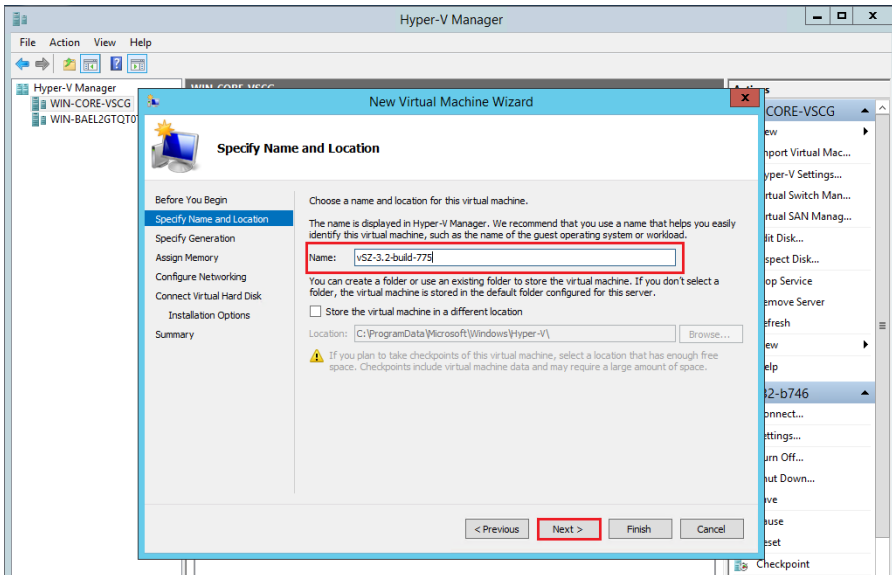
- 6 Click **Next**. The *Specify Name and Location* screen appears.

Figure 15. The New Virtual Machine Wizard screen



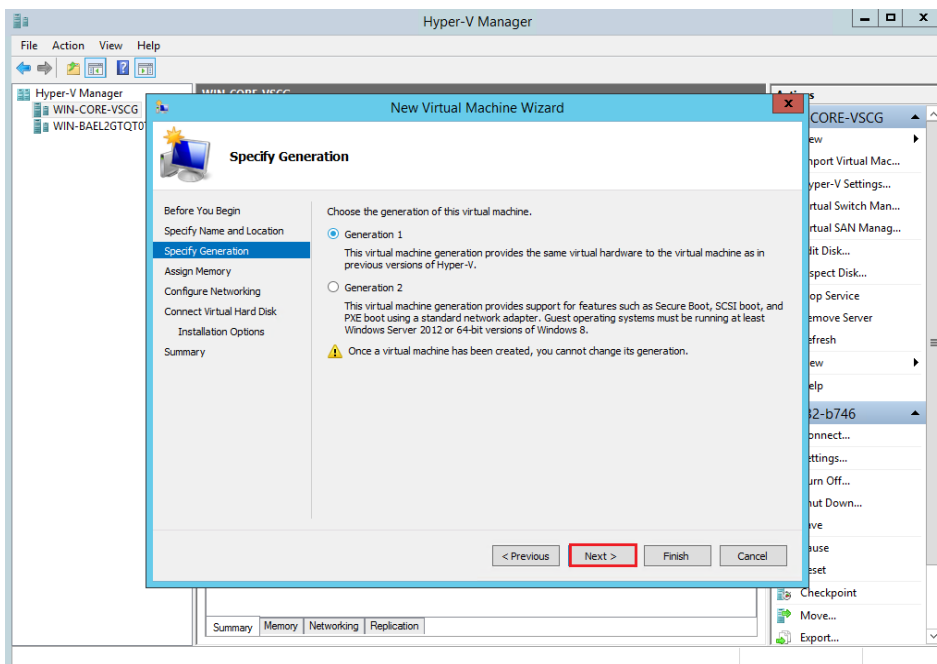
- 7 In *Name*, type a name for the virtual machine that you are installing (for example, Virtual SmartZone).

Figure 16. Specify Name and Location



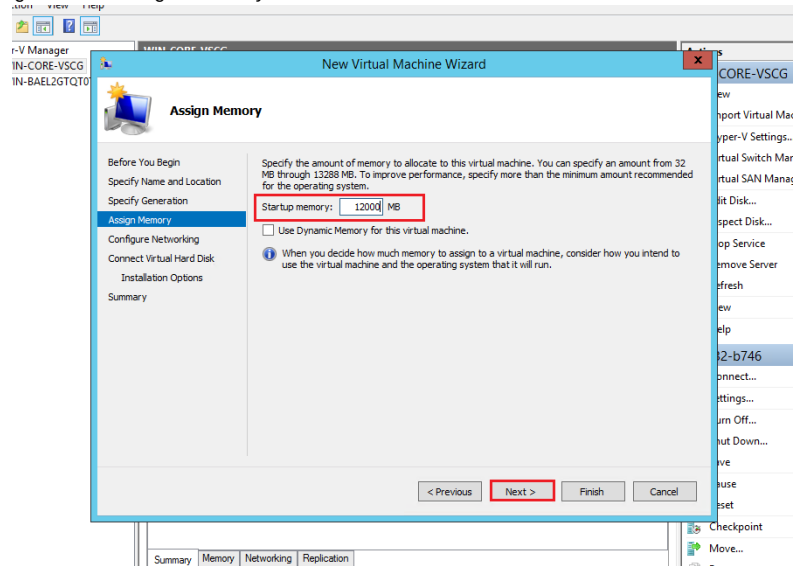
- 8 Specify the folder on the server where you want to install the virtual machine.
  - To install the virtual machine in the default location, make sure that the **Store the virtual machine in a different location** check box is clear.
  - To install the virtual machine in a location other than the default, select the **Store the virtual machine in a different location** check box, and then browse to or type the new location.
- 9 Click **Next**. The *Specify Generation* screen appears.

Figure 17. Specify Generation



- 10 Select Generation 1 for the virtual machine that you are installing. Hyper-V offers Generation 1 and Generation 2. See the Hyper-V documentation for more information about these two generations.
- 11 Click **Next**. The *Assign Memory* screen appears.

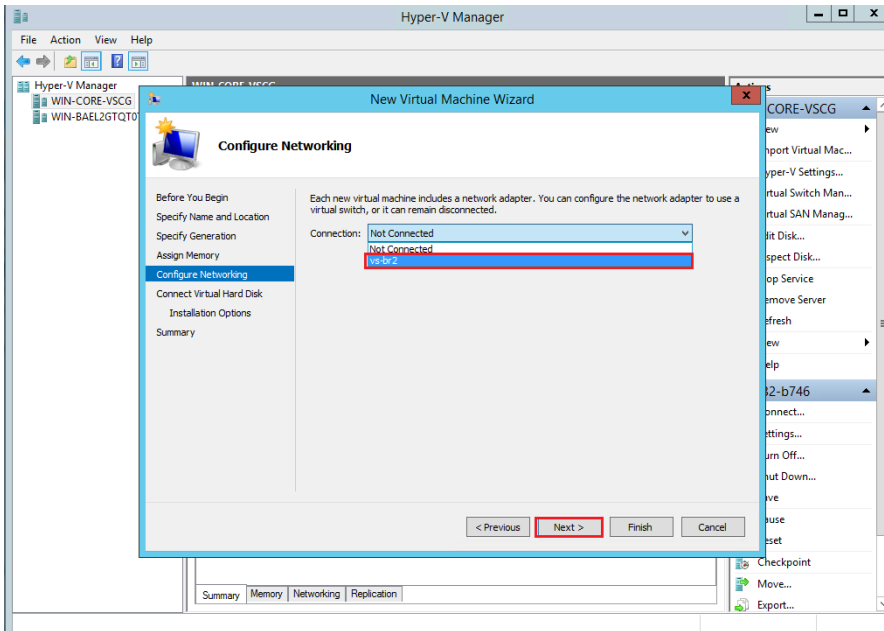
Figure 18. Assign Memory



- 12 In *Startup memory*, type 12000 MB which is the minimum recommended memory that Ruckus Wireless recommends for deploying vSZ. You can type a higher value if more memory is available on the server. For more information, see [Table 5](#).
- 13 Click **Next**. The *Configure Networking* screen appears.



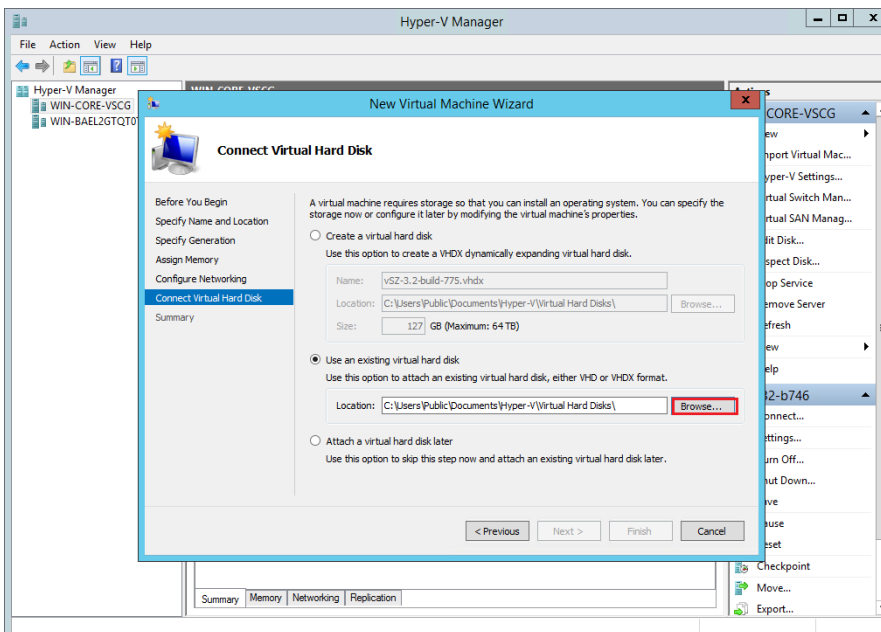
Figure 19. Configuring Network



**14** In *Connection*, select the network adapter that you want the virtual machine to use.

**15** Click **Next**. The *Connect Virtual Hard Disk* screen appears.

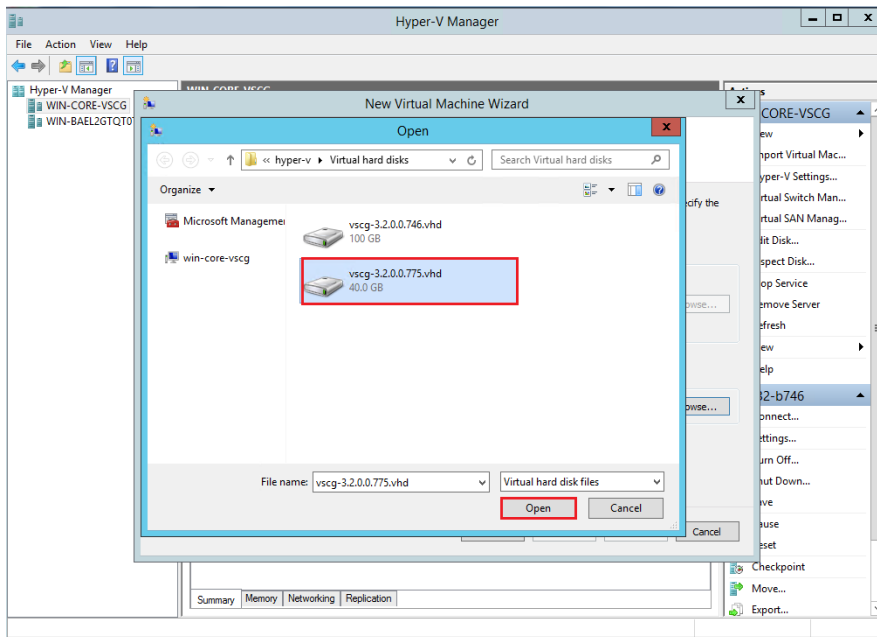
Figure 20. Connect Virtual Hard Disk



16 Select **Use an existing virtual hard disk**.

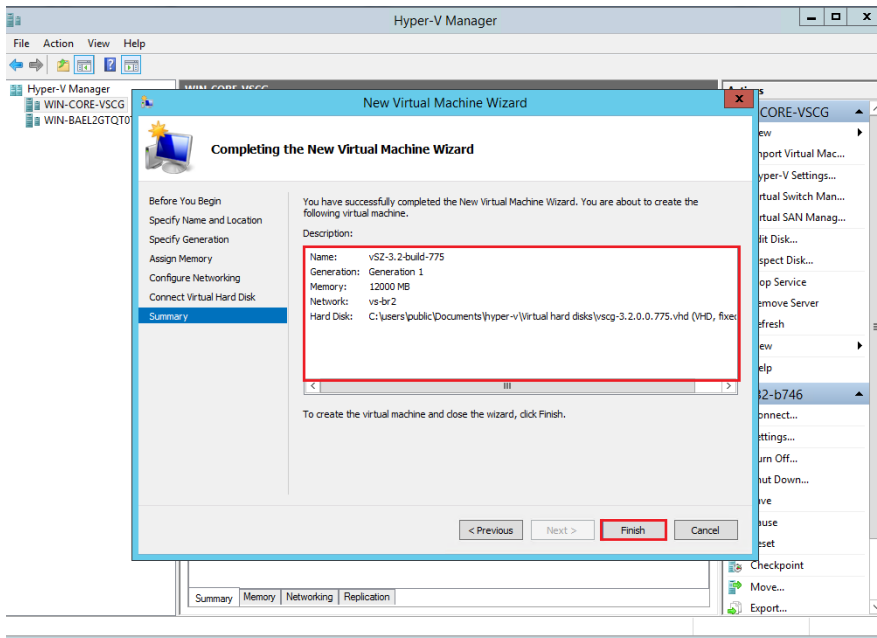
17 Click **Browse** to specify the location of the existing virtual hard disk for the virtual machine to use.

Figure 21. Selecting Virtual Hard Disk



**18** Click **Next**. The *Completing New Virtual Machine Wizard* screen appears.

Figure 22. Completing New Virtual Machine Wizard

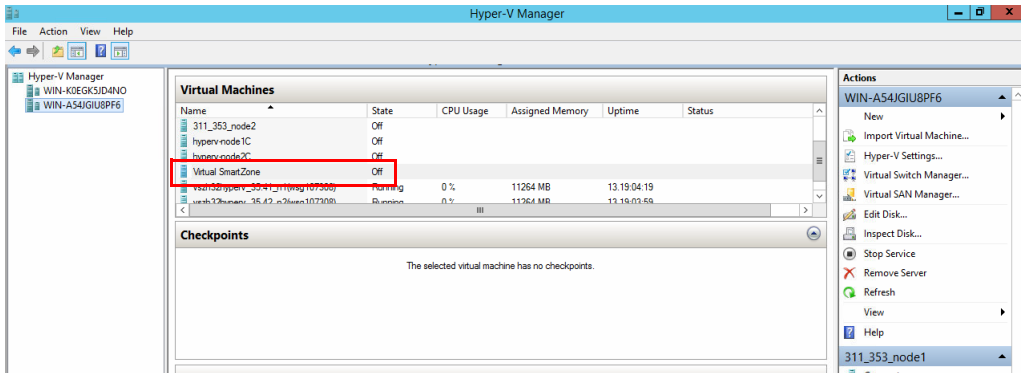


**19** Review the settings that you can configure for the virtual machine.

If you find any setting that need to be changed, click **Previous** until you reach the screen where you can update the setting. Update the setting, and then click **Next** until the *Completing New Virtual Machine Wizard* screen appears again.

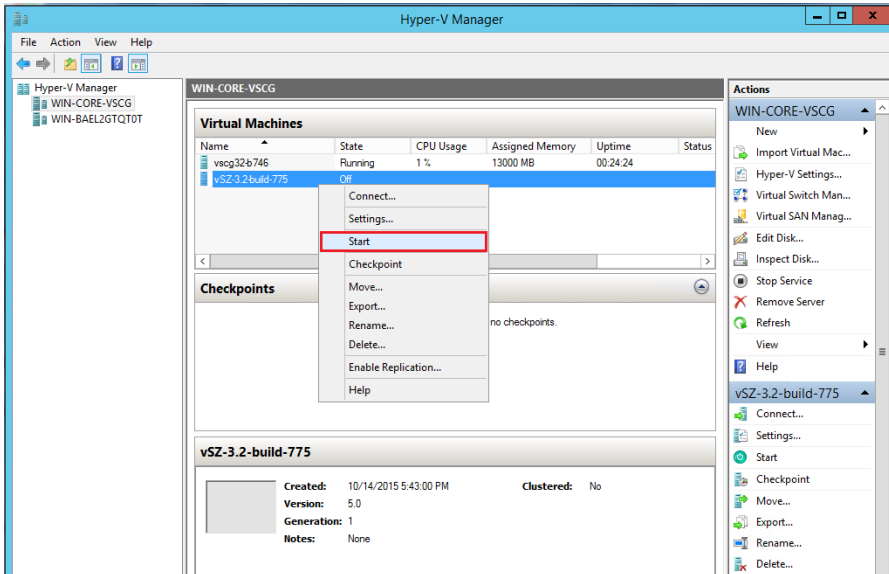
**20** Click **Finish** to install the virtual machine. When Windows Server completes installing the virtual machine, the *New Virtual Machine Wizard* disappears and the virtual machine you installed appears on the list of virtual machines on Hyper-V Manager.

Figure 23. The virtual machine you installed appears on the list of virtual machines on Hyper-V Manager



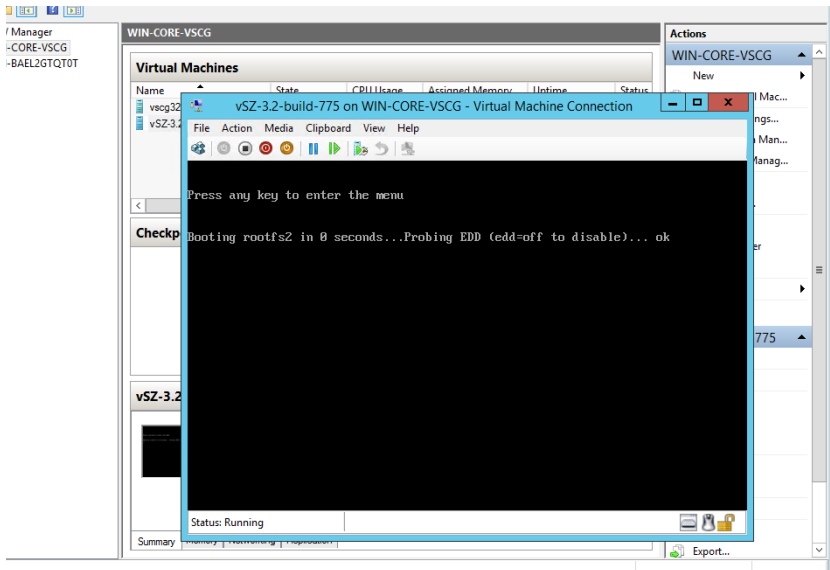
21 Right-click the virtual machine you installed, and then click **Start** to power on the virtual machine.

Figure 24. Right-click the virtual machine, and then click Start



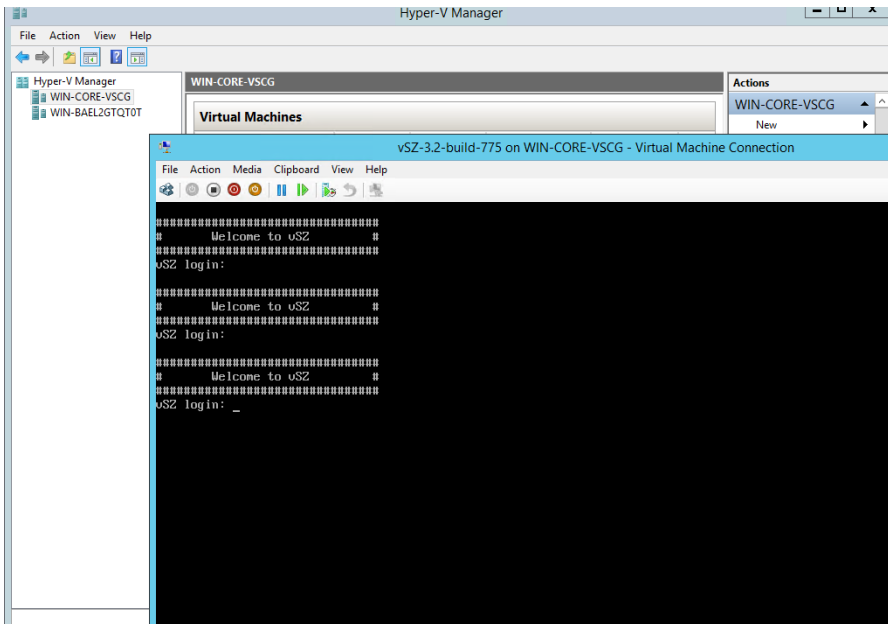
The Virtual Machine Connection screen appears.

Figure 25. Virtual Machine Connection



22 Login to the virtual machine with your credentials.

Figure 26. Login to the Virtual Machine



You have now completed installing the vSZ on Windows Server Hyper-V.

## Installing the vSZ on a Kernel-based Virtual Machine Hypervisor

This section describes how to install the vSZ on a KVM hypervisor.

- [Extracting the vSZ Image](#)
- [Setting Up the vSZ](#)

### Extracting the vSZ Image

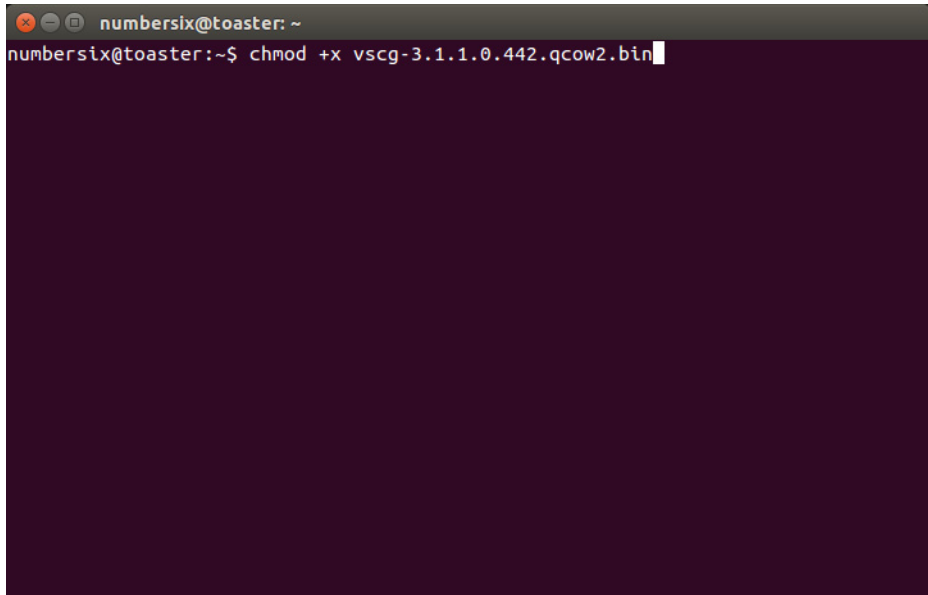
The vSZ image for a kernel-based virtual machine (KVM) is distributed in QCOW2 format.

- 1 Obtain the vSZ image in QCOW2 format.
- 2 Copy the image to the KVM.
- 3 Open the terminal window.
- 4 Make the image bin file executable by entering the following command:

```
chmod +x {file name of the controller QCOW bin}
```

See [Figure 27](#) for an example.

Figure 27. Make the bin file executable

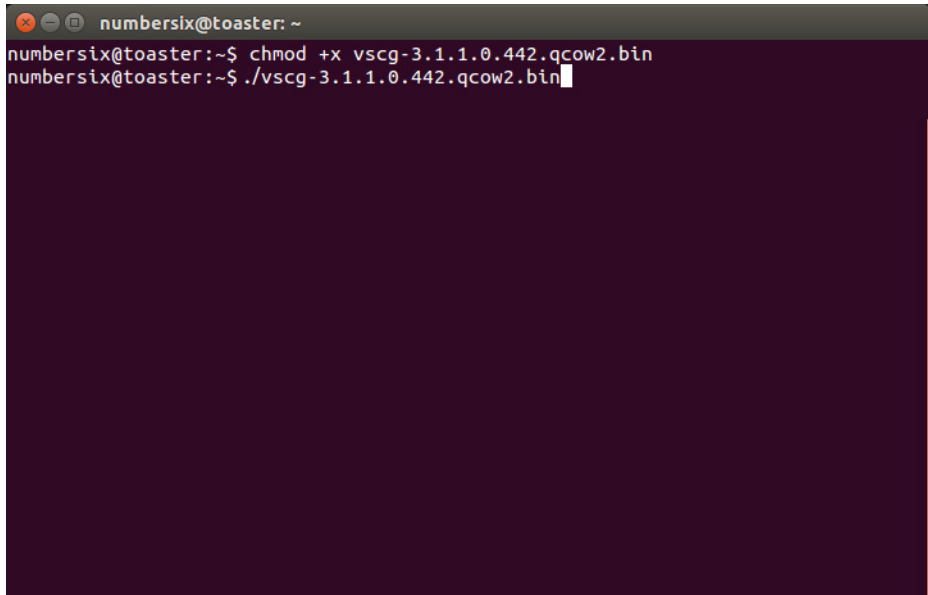
A terminal window with a dark background and light text. The window title is "numbersix@toaster: ~". The prompt is "numbersix@toaster:~\$". The command entered is "chmod +x vscg-3.1.1.0.442.qcow2.bin". The cursor is at the end of the command.

```
numbersix@toaster: ~
numbersix@toaster:~$ chmod +x vscg-3.1.1.0.442.qcow2.bin
```

- 5 Extract the contents of the QCOW2 bin file. See [Figure 28](#).



Figure 28. Extract the contents of the QCOW2 image

A terminal window with a dark background and light text. The window title is "numbersix@toaster: ~". The prompt is "numbersix@toaster:~\$". The first command entered is "chmod +x vscg-3.1.1.0.442.qcow2.bin". The second command entered is "./vscg-3.1.1.0.442.qcow2.bin". The rest of the terminal is obscured by a large black rectangle.

```
numbersix@toaster: ~
numbersix@toaster:~$ chmod +x vscg-3.1.1.0.442.qcow2.bin
numbersix@toaster:~$ ./vscg-3.1.1.0.442.qcow2.bin
```

The end user license agreement appears on screen.

- 6 At the `Accept this agreement? [yes/no]` prompt, enter **yes**.

Figure 29. Accept the EULA terms

```

numbersix@toaster: ~
withheld. This agreement may be executed simultaneously in any number of
counterparts, each of which will be deemed an original, but all of
which together constitute one and the same agreement. The parties agree
that electronic signatures are valid signatures for enforcement of
this agreement. This agreement constitutes the entire agreement between
Ruckus and Licensee with respect to the subject matter hereof.
This agreement supersedes all prior negotiations, agreements and underta
kings between the parties with respect to such subject matter. As a
matter of clarity, the preceding two sentences do not affect either part
y's obligations regarding confidential information under any other
agreement between the parties. No modification of this agreement will be
effective unless contained in writing and signed by an authorized
representative of each party. Notwithstanding applicable law, electronic
communications will not be deemed signed writings. Any additional
orders for licenses hereunder shall be governed by the terms of this Agr
eement. No term or condition contained in Licensee's purchase order
or similar document will apply unless specifically agreed to by Ruckus i
n writing, even if Ruckus has accepted the order set forth in such
purchase order, and all such terms or conditions are otherwise hereby ex
pressly rejected by Ruckus. In the event of a conflict between this
agreement and any other applicable agreement, this agreement shall gover
n.
Accept this agreement? [yes/no]:

```

The KVM continues to extract the contents of the image. When the extraction process is complete, the QCOW2 file appears in the same directory as the .bin file.

Figure 30. The QCOW2 file appears in the same directory as the .bin file

Places	Name	Size	Modified
Search	Desktop		13:13
Recently Used	Documents		13:13
numbersix	Downloads		13:21
Desktop	Music		13:13
File System	Pictures		13:47
285 GB Volume	Public		13:13
Documents	Templates		13:13
Music	Videos		13:13
Pictures	examples.desktop	9.0 kB	12:55
Videos	vscg-3.1.1.0.442.qcow2	2.3 GB	15-06-25
Downloads	vscg-3.1.1.0.442.qcow2.bin	876.8 MB	13:21

---

**NOTE:** If the “uudecode: command not found” error appears during the extraction process, install the “sharutils” package on the KVM, and then try extracting the image again.

---

- 7 Resize the vSZ disk image, if necessary. By default, the vSZ disk size is 50GB. If you want to allocate more disk space to the vSZ, run the `qemu-img` command. The complete syntax is as follows:

```
qemu-img resize {file name of the controller QCOW bin}  
+size
```

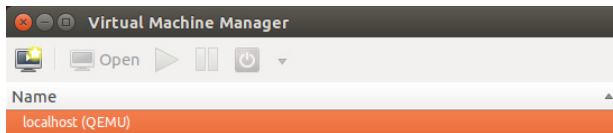
## Setting Up the vSZ

This section describes how to set up the vSZ using the Red Hat Virtual Machine Manager (also known as “virt-manager”). If you are installing the vSZ on a different hypervisor or virtual machine monitor, the procedure may be slightly different. Refer to the hypervisor documentation for more information.

Follow these steps to set up the vSZ on the Virtual Machine Manager.

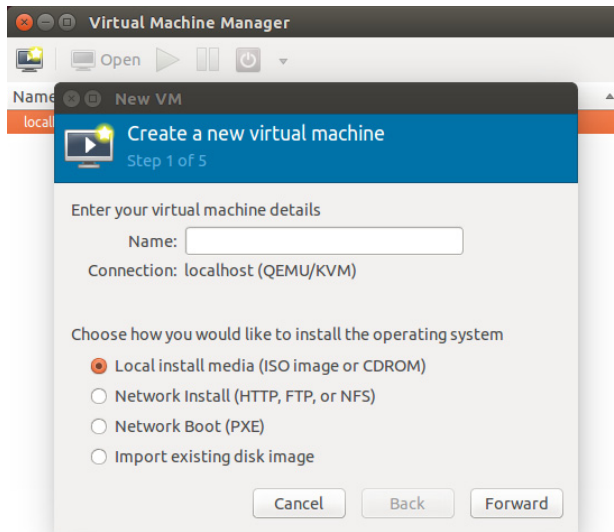
- 1 Start the Virtual Machine Manager by clicking **Applications > System Tools > Virtual Machine Manager**. Or double-click the Virtual Machine Manager icon if it appears on the desktop. The Virtual Machine Manager interface appears.

Figure 31. The Virtual Machine Manager interface



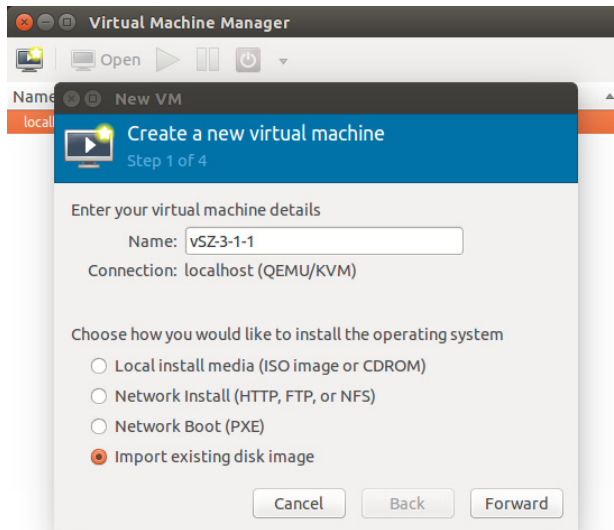
- 2 In *File*, click **Create New VM**. Or click the *New VM* icon. The *New VM* screen appears.

Figure 32. After you click Create New VM, the New VM screen appears



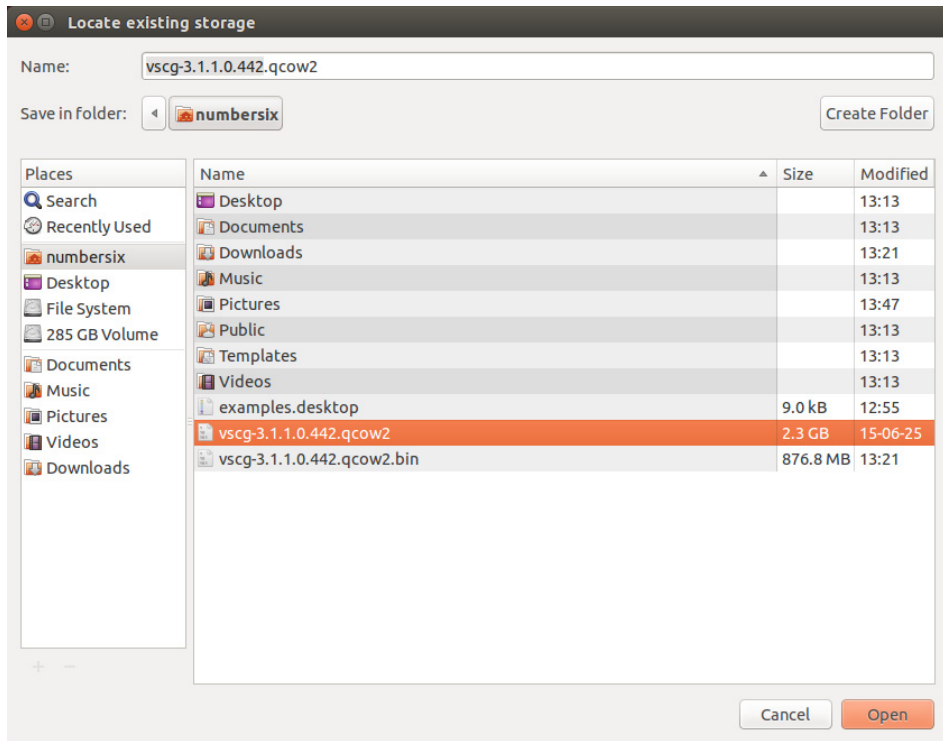
- 3 Configure the options on the *New VM (Step 1 of 4)* screen.
  - In *Name*, type a name that you want to assign to the virtual machine.
  - In *Choose how you would like to install the operating system*, click **Import existing disk image**.

Figure 33. Type a name and select how you want to install the operating system



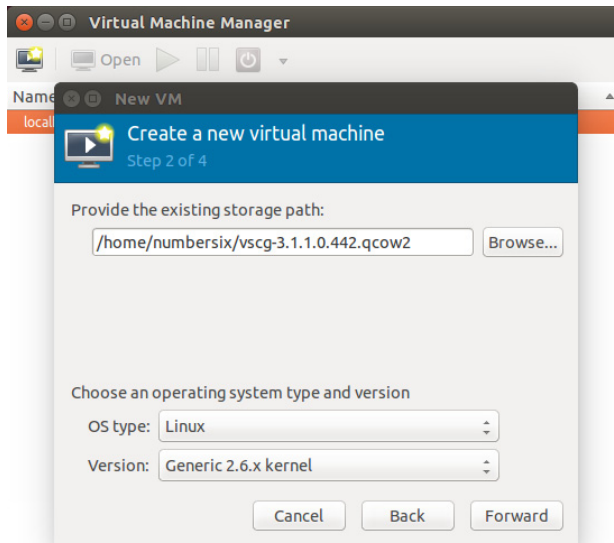
- 4 Click **Forward**. The *Locate Existing Storage* dialog box appears.
- 5 Browse to the location of the vSZ QCOW2 image, select the image file, and then click **Open**. The *New VM (Step 2 of 4)* screen reappears and displays the storage path to the QCOW2 image file that you selected.

Figure 34. Browse to the vSZ QCOW2 image



- 6 In the lower portion of the *New VM (Step 2 of 4)* screen, select the operating system type and version.
  - In *OS type*, select **Linux**.
  - In *Version*, select **Generic 2.6.x kernel**.

Figure 35. Select the operating system and version

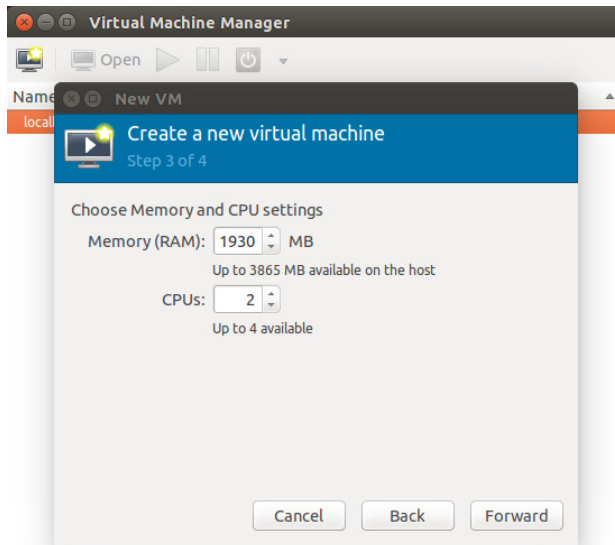


- 7 Click **Forward**. The *New VM (Step 3 of 4)* screen appears.
- 8 Configure the memory and CPU settings of the virtual machine.
  - In *Memory (RAM)*, set to memory (in MB) that you want to allocate to the vSZ.
  - In *CPU*, set the number of CPUs that you want to allocate to the vSZ.

For more information see, [Table 5](#)

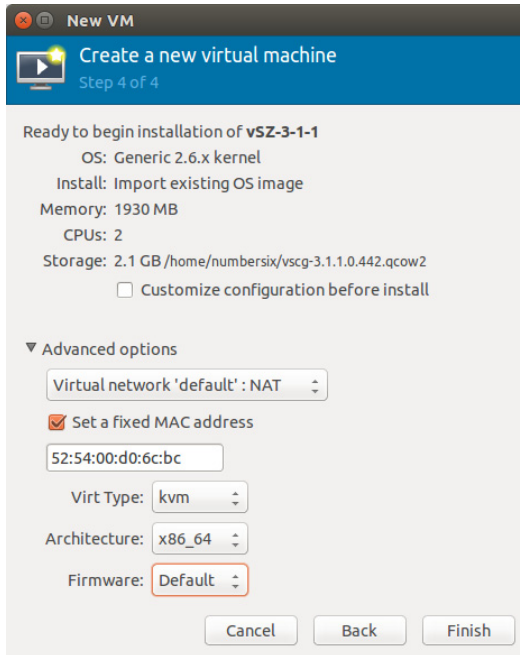


Figure 36. Configure the memory and CPU settings



- 9 Click **Forward**. The *New VM (Step 4 of 4)* screen appears and displays a summary of the settings you configured.

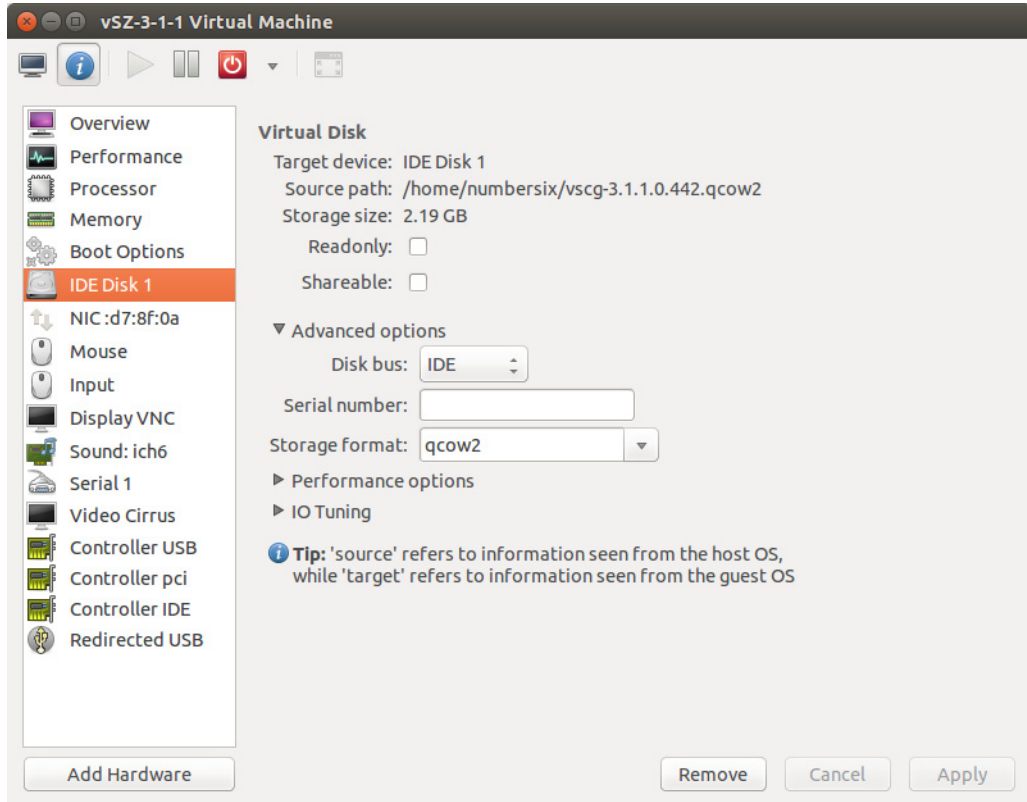
Figure 37. A summary of the settings you configured appears



- 10 Verify that the settings you configured on the previous screens are correct. If you need to make changes to any of the settings, click **Back** until you reach the screen on which the setting appears, make the change, and then click **Forward** until you reach the *New VM (Step 4 of 4)* screen again.
- 11 Click **Finish** to install the vSZ on the virtual machine.
- 12 After you complete installing the vSZ on the virtual machine, decide how many interfaces you want the vSZ to use. The vSZ supports either a single interface or three interfaces. By default, a single interface exists after installation.
- If you want the vSZ to use a single interface, you do not need to take action in this step. Continue to the next step.
  - If you want the vSZ to use three interfaces, you must create the two additional interfaces before the initial bootup of the vSZ. Once the vSZ has completed its initial bootup, you will no longer be able to change the number of interfaces.

**CAUTION!** If you want to add interfaces, you must do so before the initial bootup of the vSZ. After the initial bootup, you will no longer be able to change the number of interfaces.

Figure 38. By default, a single interface exists



**13** Power on the virtual machine. The vSZ performs its initial bootup.

**14** When the vSZ `login` prompt appears, enter **admin**.

You have completed setting up the vSZ on a KVM hypervisor. You are now ready to start the vSZ Setup Wizard. See [Using the Setup Wizard to Install vSZ](#) for more information.

# Installing the vSZ on Microsoft Azure

# 3

In this chapter:

- [Logging into Microsoft Azure](#)
- [Creating a Storage Account and Container](#)
- [Uploading the vSZ Image to Microsoft Azure](#)
- [Creating a vSZ Image on Microsoft Azure](#)
- [Creating a Network](#)
- [Creating a vSZ Virtual Machine](#)
- [Configuring Port Numbers for Virtual Machines](#)
- [Assigning a Static Internal IP Address to a Virtual Machine](#)
- [Assigning a Static Public IP Address to a VM](#)

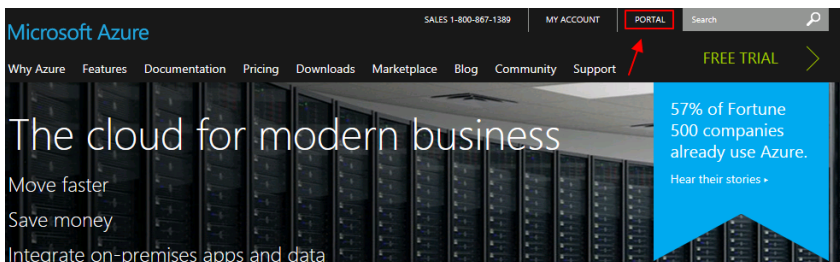
This section describes how to install the vSZ on Microsoft Azure.

## Logging into Microsoft Azure

Follow these steps to login to Microsoft Azure:

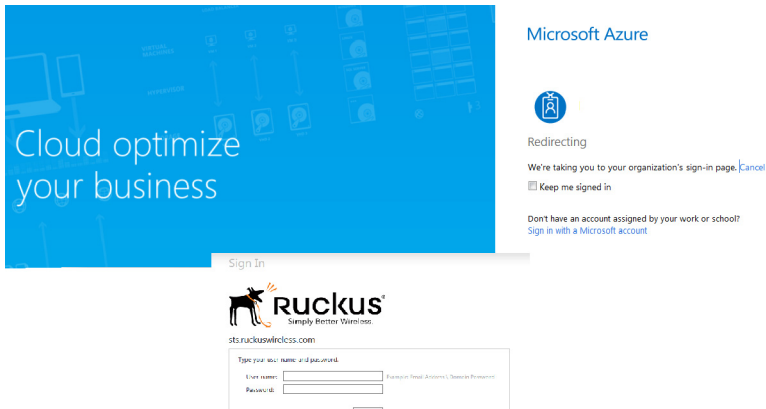
- 1 Click <http://azure.microsoft.com/en-us/> to access the *Microsoft Azure* site.
- 2 Click the **Portal** tab as show in the figure.

Figure 39. Portal tab

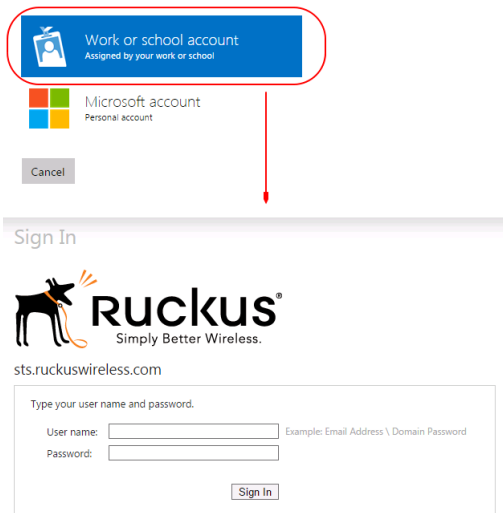


- 3 The *Microsoft Azure* login page appears and redirects you to the *Ruckus Wireless login* page as shown in the figure.

Figure 40. Microsoft Azure login page



If the page does not redirected to the *Ruckus Wireless login* page and asks to you choose a user account, select the **Work or school account** as shown in the figure.



The *Ruckus Wireless login* page appears.

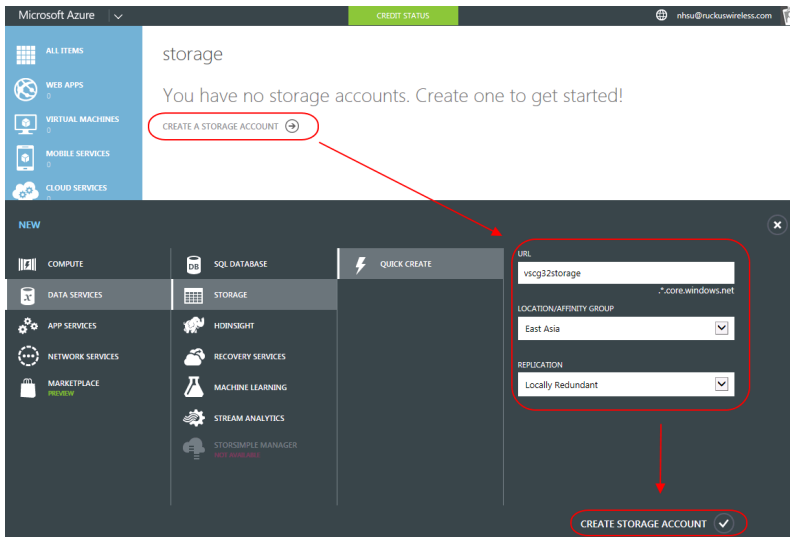
4 Enter your *User name* and *Password* to login.

## Creating a Storage Account and Container

To create a Microsoft Azure storage account, perform the following steps:

- 1 From the *Microsoft Azure* page, click **Create a storage account**. The *Create a storage* screen appears.

Figure 41. Creating a storage account



- 2 In *URL*, type the URL.
- 3 In *Location/Affinity Group*, type the location of the storage.
- 4 In *Replication*, select an option from the drop-down list.
- 5 Click **Create Storage Account**. The *Storage* screen appears listing the new storage account.

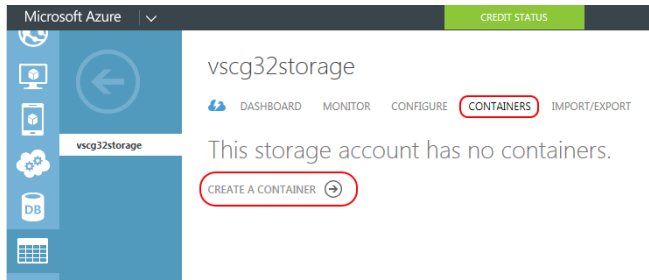
Figure 42. New storage account listed

storage

NAME	STATUS	LOCATION	SUBSCRIPTION
vscg32storage	→ ✓ Online	East Asia	Free Trial

- 6 Select the storage account and click **Containers > Create a Container**.

Figure 43. Creating a storage container



The *New Container* screen appears.

Figure 44. New container


- 7 In *Name*, type the name of the storage container.
- 8 In *Access*, select an option from the drop-down list.
- 9 Click the  icon. The new container is listed in the *Containers* tab.

Figure 45. New container listed

vscg32storage

DASHBOARD MONITOR CONFIGURE CONTAINERS IMPORT/EXPORT

NAME	URL	LAST MODIFIED
vscg	<a href="https://vscg32storage.blob.core.windows.net/vscg">https://vscg32storage.blob.core.windows.net/vscg</a>	6/23/2015 2:11:34 PM

## Uploading the vSZ Image to Microsoft Azure

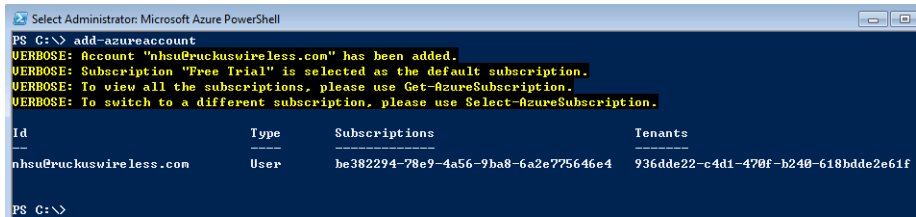
### Before you Begin

Ensure that you have installed Windows Azure Power Shell (web platform installer) from <http://go.microsoft.com/fwlink/p/?linkid=320376&clid=0x409>.

Follow these steps to upload the vSZ image to Microsoft Azure:

- 1 Open Microsoft Azure PowerShell and type the **add-azureaccount** command. The *Microsoft Azure Login* screen appears.
- 2 Type the *User name* and *Password*.
- 3 Click **Sign in**. A success message appears confirming your Microsoft Azure account is added.

Figure 46. Account creation success message



```

Select Administrator: Microsoft Azure PowerShell
PS C:\> add-azureaccount
VERBOSE: Account "nhsu@ruckuswireless.com" has been added.
VERBOSE: Subscription "Free Trial" is selected as the default subscription.
VERBOSE: To view all the subscriptions, please use Get-AzureSubscription.
VERBOSE: To switch to a different subscription, please use Select-AzureSubscription.

Id                               Type             Subscriptions    Tenants
--                               -
nhsu@ruckuswireless.com         User             be382294-78e9-4a56-9ba8-6a2e775646e4  936dde22-c4d1-470f-b240-618bde2e61f
PS C:\>

```

- 4 Type command **add-azurevhd** to initiate uploading the image.

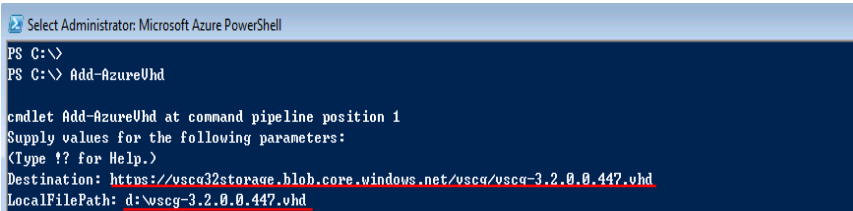
---

**NOTE:** Ensure that the URL in *Destination* and *Microsoft Azure storage* are the same.

---



Figure 47. Verifying URLs match



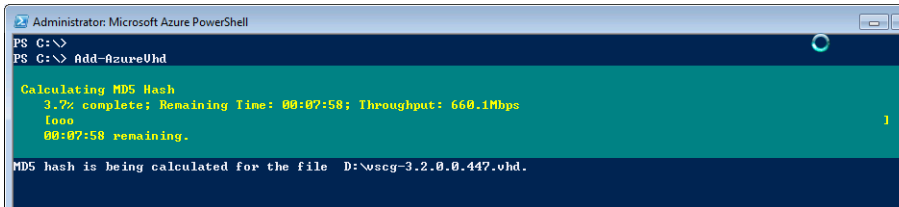
```

Select Administrator: Microsoft Azure PowerShell
PS C:\>
PS C:\> Add-AzureUhd

cmdlet Add-AzureUhd at command pipeline position 1
Supply values for the following parameters:
(Type ?? for Help.)
Destination: https://vscg32storage.blob.core.windows.net/vscg/vscg-3.2.0.0.447.vhd
LocalFilePath: d:\vscg-3.2.0.0.447.vhd

```

Figure 48. Uploading the vSZ image



```

Administrator: Microsoft Azure PowerShell
PS C:\>
PS C:\> Add-AzureUhd

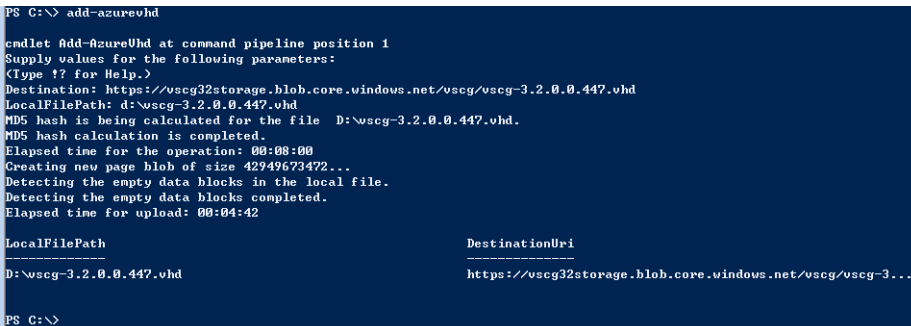
Calculating MD5 Hash
 3.7% complete; Remaining Time: 00:07:58; Throughput: 660.1Mbps
Time
00:07:58 remaining.

MD5 hash is being calculated for the file D:\vscg-3.2.0.0.447.vhd.

```

After the vSZ image is uploaded, a confirmation message appears.

Figure 49. vSZ message indicating image upload is complete



```

PS C:\> add-azurevhd

cmdlet Add-AzureUhd at command pipeline position 1
Supply values for the following parameters:
(Type ?? for Help.)
Destination: https://vscg32storage.blob.core.windows.net/vscg/vscg-3.2.0.0.447.vhd
LocalFilePath: d:\vscg-3.2.0.0.447.vhd
MD5 hash is being calculated for the file D:\vscg-3.2.0.0.447.vhd.
MD5 hash calculation is completed.
Elapsed time for the operation: 00:08:00
Creating new page blob of size 42949673472...
Detecting the empty data blocks in the local file.
Detecting the empty data blocks completed.
Elapsed time for upload: 00:04:42

LocalFilePath                                     DestinationUri
-----
D:\vscg-3.2.0.0.447.vhd                           https://vscg32storage.blob.core.windows.net/vscg/vscg-3...

PS C:\>

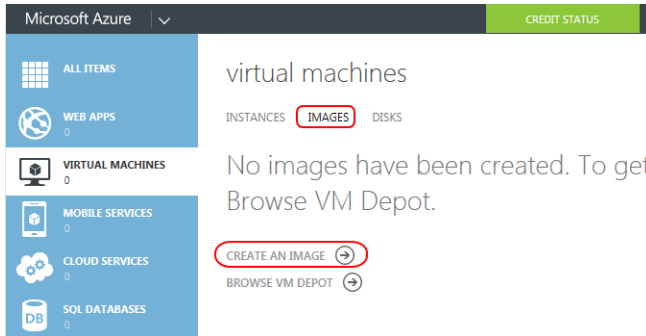
```

## Creating a vSZ Image on Microsoft Azure

Follow these steps to create a vSZ image on Microsoft Azure:

- 1 From the *Microsoft Azure* page, click **Virtual Machines > Images**.

Figure 50. Creating an image



- 2 Click **Create an Image**. The *Create an Image from VHD* screen appears.

Figure 51. Creating an image from VHD


- 3 In *Name*, type the name of the image.
- 4 In *Description*, provide a brief description about the image.
- 5 Click **VHD URL** and browse to the cloud storage to select the VHD file.
- 6 In *Operating System Family*, select an option from the drop-down list.
- 7 Click the  icon. The new image is listed in the *Images* tab.

Figure 52. A new vSZ image is created

virtual machines

INSTANCES IMAGES DISKS

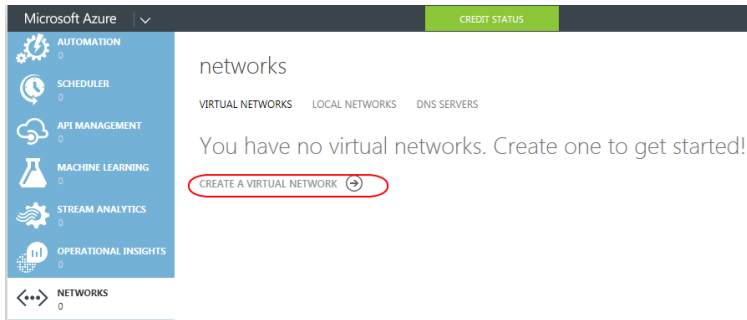
NAME	STATUS	SOURCE	LAST UPDATE	SUBSCRIPTION	LOCATION
vscj-3.2.0.0.447	Available	-	-	Free Trial	East Asia

## Creating a Network

Follow these steps to create a virtual network:

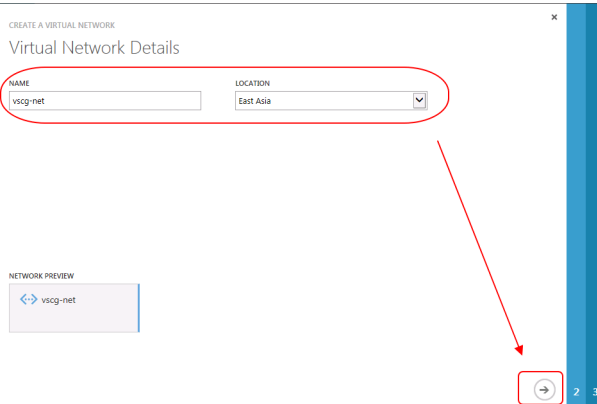
- 1 From the *Microsoft Azure* page, click **Networks > Virtual Networks**.

Figure 53. Creating a virtual network



- 2 Click **Create a Virtual Network**. The *Virtual Network Details* screen appears.

Figure 54. Virtual Network Details screen




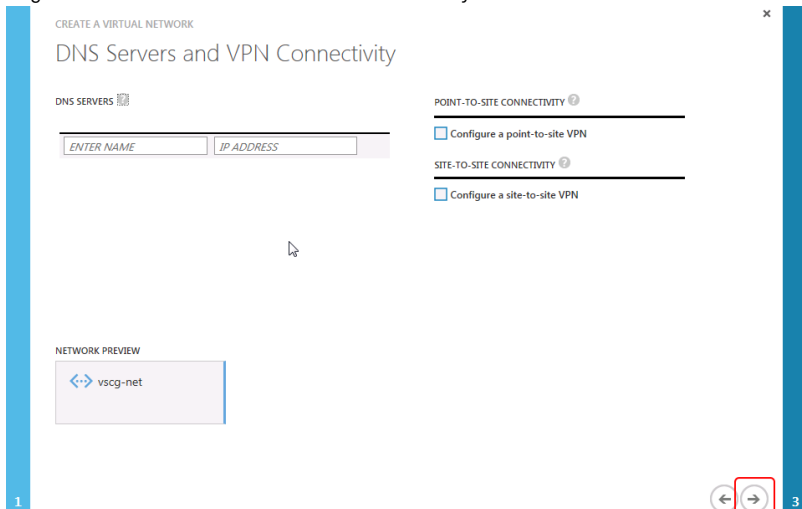
- 3 In *Name*, type the name of the virtual network.
- 4 In *Location*, select a location from the drop-down list.
- 5 Click the  icon. The *DNS Servers and VPN Connectivity* screen appears.

Figure 55. DNS Servers and VPN Connectivity screen




- 6 In *DNS Server*, type the name of the server and IP address.
- 7 Configure the VPN connectivity. You can choose between a point-to-site or site-to-site connectivity.
- 8 Click the  icon. The *Virtual Network Address Spaces* screen appears.

Figure 56. Virtual Network Address Spaces screen

CREATE A VIRTUAL NETWORK

### Virtual Network Address Spaces

ADDRESS SPACE	STARTING IP	CIDR (ADDRESS COUNT)	USABLE ADDRESS RANGE
10.250.0.0/16	10.250.0.0	/16 (65536)	10.250.0.0 - 10.250.255.255
<b>SUBNETS</b>			
Subnet-1	10.250.1.0	/24 (256)	10.250.1.0 - 10.250.1.255
Subnet-2	10.250.2.0	/24 (256)	10.250.2.0 - 10.250.2.255

add address space

add subnet

NETWORK PREVIEW

↔ vscg-net

1 2

⏪ ⏩ ✓

9 Type the address space and subnet information as appropriate.

10 Click the ✓ icon. The virtual network is created and listed in the *networks* page.

Figure 57. The new virtual network is added and listed in the Networks page

networks

VIRTUAL NETWORKS LOCAL NETWORKS DNS SERVERS

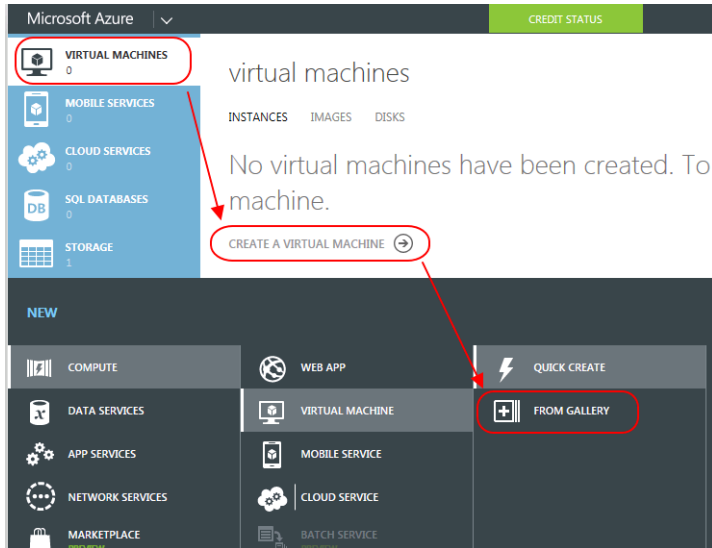
NAME	STATUS	SUBSCRIPTION	LOCATION	
vscg-net	→ ✓ Created	Free Trial	East Asia	

## Creating a vSZ Virtual Machine

Follow these steps to create a vSZ virtual machine:

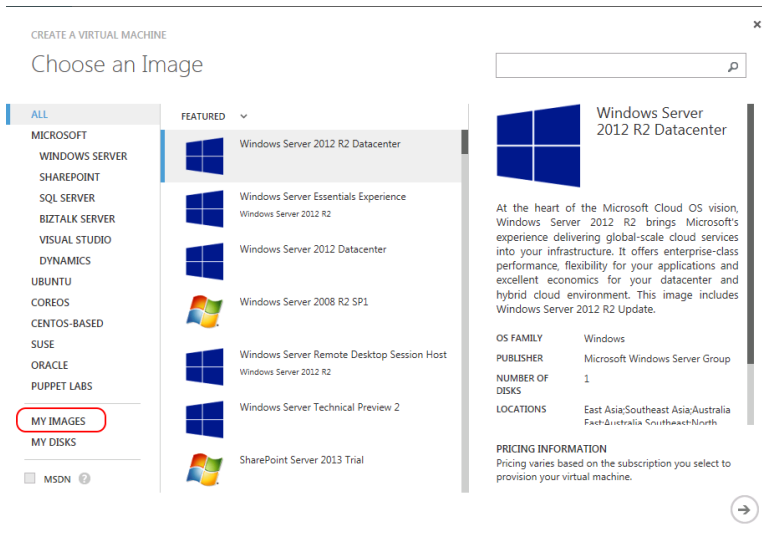
- 1 From the *Microsoft Azure* page, click **Virtual Machines > Instances**. The *New* screen appears.

Figure 58. New screen



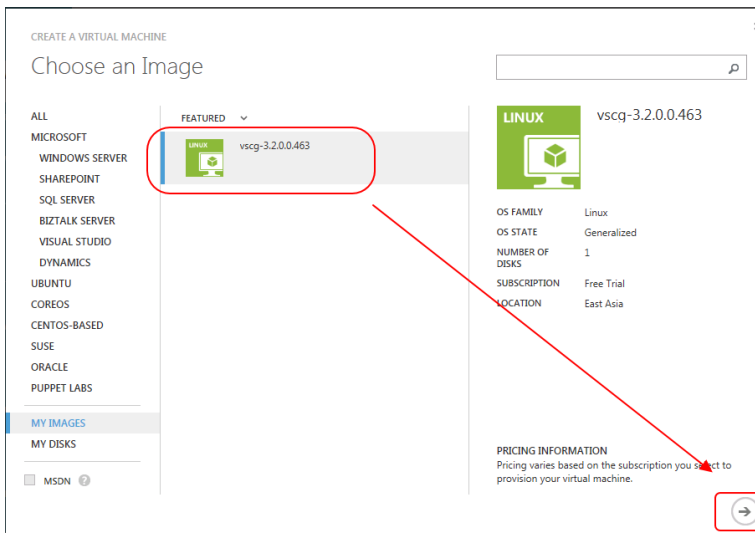
- 2 Click **Compute > Virtual Machine > Quick Create > From Gallery**. The *Choose an Image* screen appears.

Figure 59. Choosing an image



3 Click **My Images**. A list of images you created appears.

Figure 60. A list of images



4 Select an image.

5 Click the  icon. The *Virtual Machine Configuration* screen appears.

Figure 61. Virtual machine configuration - screen 1

CREATE A VIRTUAL MACHINE

## Virtual machine configuration

VIRTUAL MACHINE NAME ?

TIER

SIZE ?

A5 (2 cores, 14 GB memory) ▼

NEW USER NAME

AUTHENTICATION ?

UPLOAD COMPATIBLE SSH KEY FOR AUTHENTICATION

PROVIDE A PASSWORD

NEW PASSWORD CONFIRM

•••••••• ✓ ••••••••

LINUX vscq-3.2.0.0.463

OS FAMILY  
Linux

OS STATE  
Generalized

NUMBER OF DISKS  
1

SUBSCRIPTION  
Free Trial

LOCATION  
East Asia

PRICING INFORMATION  
Pricing varies based on the subscription you select to provision your virtual machine.

1 ← → 3 4


- 6 In *Virtual Machine Name*, type the name of the VM.
- 7 In *Tier*, select *Standard*.
- 8 In *Size*, select an option from the drop-down list.
- 9 In *New User Name*, type the user name.
- 10 In *Authentication*, select the *Provide a Password* option. Type the new password and confirm.
- 11 Click the  icon. The next configuration screen appears.



Figure 62. Virtual machine configuration - screen 2

CREATE A VIRTUAL MACHINE

### Virtual machine configuration

**CLOUD SERVICE**

Create a new cloud service

**CLOUD SERVICE DNS NAME**

vsz01 .cloudapp.net

**REGION/AFFINITY GROUP/VIRTUAL NETWORK**

vscg-net

**VIRTUAL NETWORK SUBNETS**

Subnet-1(10.250.1.0/24)

**AVAILABILITY SET**

(None)

**ENDPOINTS**

NAME	PROTOCOL	PUBLIC PORT	PRIVATE PORT
SSH	TCP	22	22

ENTER OR SELECT A VALUE

**OS FAMILY**  
Linux

**OS STATE**  
Generalized

**NUMBER OF DISKS**  
1

**SUBSCRIPTION**  
Free Trial

**LOCATION**  
East Asia

**PRICING INFORMATION**  
Pricing varies based on the subscription you select to provision your virtual machine.

1 2 4

12 In *Cloud Service*, select a service from the drop-down list.

13 In *Cloud Service DNS Name*, type the DNS name.

14 In *Region/Affinity Group/Virtual Network*, select an option from the drop-down list.

15 In *Virtual Network Subnets*, select an option from the drop-down list.

16 In *Availability Set*, select an option from the drop-down list.

17 In *End Points*, type the values as appropriate.

Additionally, you can configure the following ports:

Table 7. Port numbers to configure virtual machines

Feature	Port Number
vscg_ftp	21
vscg_ap-fw	91
vscg_ap-key	443
vscg_gui	8443
vscg_wispr01	8090
vscg_wispr02	8099
vscg_wispr03	8100

Table 7. Port numbers to configure virtual machines

Feature	Port Number
vscg_wispr04	8111
vscg_wispr05	9998
vscg_nbi01	9080
vscg_nbi02	9443
vscg_lwapp	12223


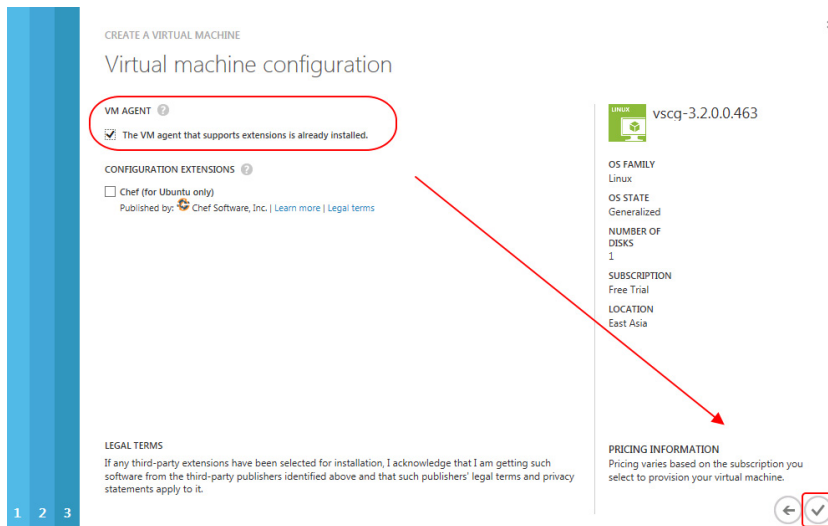
18 Click the  icon. The next configuration screen appears.

Figure 63. Virtual machine configuration - screen 3



19 In *VM Agent*, select the check-box to enable VM agent.


20 Click the  icon. The new VM is listed in the *Virtual Machines* page.

Figure 64. The new VM is created and listed

## virtual machines

INSTANCES IMAGES DISKS

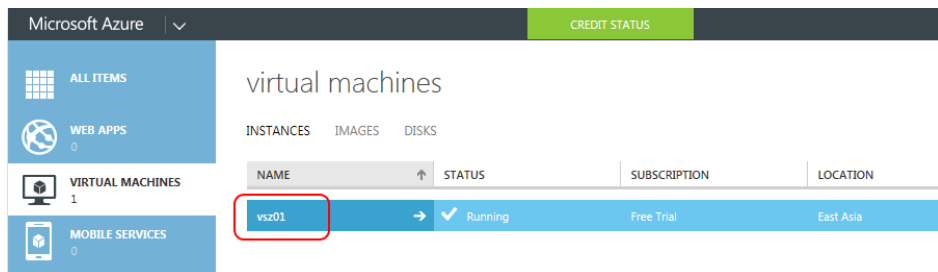
NAME	STATUS	SUBSCRIPTION	LOCATION	DNS NAME
vsz01	Running	Free Trial	East Asia	vsz01.cloudapp.

## Configuring Port Numbers for Virtual Machines

Follow these steps to configure port numbers for your VM using Microsoft Azure:

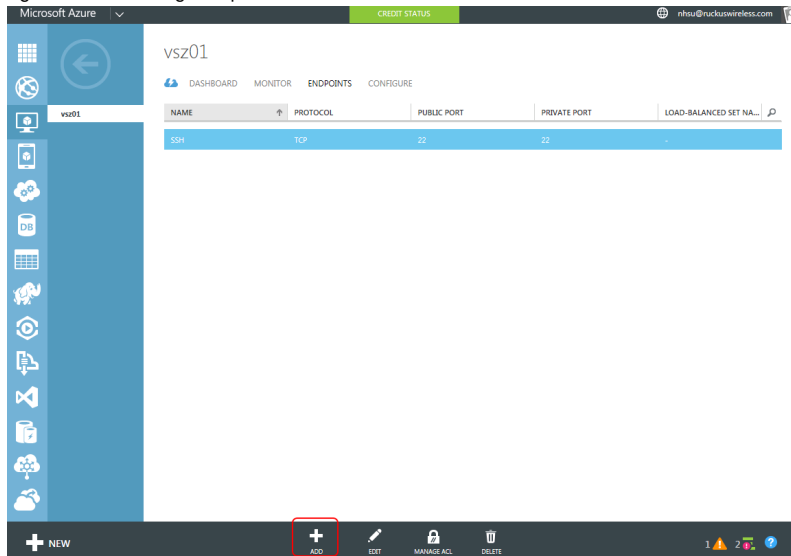
- 1 From the *Microsoft Azure* page, click **Virtual Machines > Instances**.

Figure 65. Selecting a VM



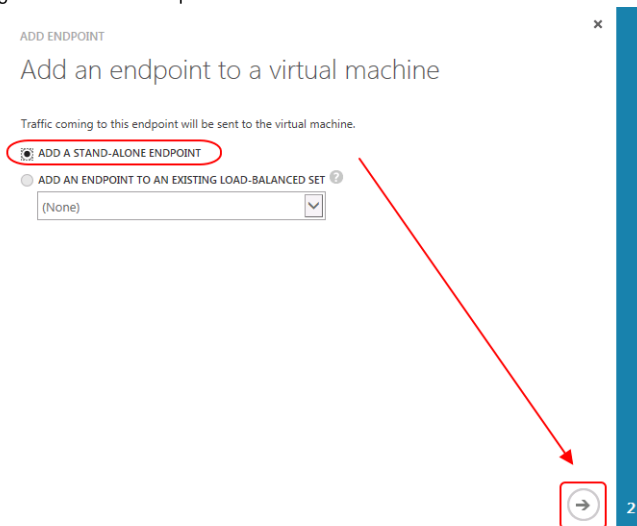
- 2 Select the virtual machine to configure the ports.
- 3 Click *Endpoints*.
- 4 Select **Add Endpoint**.

Figure 66. Adding endpoints



The *Add Endpoint* screen appears.

Figure 67. Add Endpoint - screen 1




- 5 Select *Add a stand-alone end point*.
- 6 Click the  icon. The next configuration screen appears.

Figure 68. Adding Endpoint - screen 2

ADD ENDPOINT

Specify the details of the endpoint

NAME  
vscg-webs

PROTOCOL  
TCP

PUBLIC PORT  
8443

PRIVATE PORT  
8443

CREATE A LOAD-BALANCED SET

ENABLE DIRECT SERVER RETURN

1


- 7 In *Name*, type the name of the endpoint.
- 8 In *Protocol*, select the protocol from the drop-down list.
- 9 In *Public Report*, type 8443.
- 10 In *Private Report*, type 8443.
- 11 Click the  icon. The endpoint is created and listed in the *Endpoints* tab for the VM.

Figure 69. A new endpoint for the VM is created and listed

vsz01

DASHBOARD MONITOR ENDPOINTS CONFIGURE

**UPDATE IN PROGRESS** An update is in progress. You can change the configuration settings after it finishes.

NAME	PROTOCOL	PUBLIC PORT	PRIVATE PORT	LOAD-BALANCED SET NA...
SSH	TCP	22	22	-
vscg-webs	TCP	8443	8443	-

## Assigning a Static Internal IP Address to a Virtual Machine

A Virtual machine in a network is assigned an internal IP address. These addresses change when the VM is restarted. Some scenarios such as the following might require VMs to have a static internal IP address that does not change:

- If the VM is an internal DNS server.
- If the VM is a node within a cluster.
- If the VM is part of a site-to-site VPN connection.

### Before You Begin

Ensure that a vSZ virtual machine is created using Microsoft Azure.

Also, ensure that you assign an internal IP for the VM before configuring the virtual network.

Follow these steps to assign a static internal IP to a VM:

- 1 From the *Microsoft Azure* page, click **Virtual Machines > Instances**.
- 2 From the *Virtual Machines* page, select the VM.

---

**NOTE:** An internal IP is assigned to the VM by default when it is created.

---

Figure 70. Default IP assigned to the VM

The screenshot displays the Azure portal interface for a virtual machine. The left sidebar shows a list of VMs: sim01, vsz-cp01, vsz-server01, vsz02, and vsz03. The main area shows the 'usage overview' for vsz03, including a bar chart for '2 CORE(S)' and a table for 'disks'. The right-hand pane shows configuration details, with the 'INTERNAL IP ADDRESS' field circled in red, indicating the value 10.250.1.5.

DISK	TYPE	HOST CACHE	VHD
vsz03-vs203-2015-06-30	OS disk	Read/Write	https://vscg32storage.blob.o

- 3 Click **Shutdown**.

Figure 71. Shutting down the VM

virtual machines

INSTANCES IMAGES DISKS

NAME	STATUS	SUBSCRIPTION	LOCATION
sim01	Running	Free Trial	East Asia
vsz-cp01	Running	Free Trial	East Asia
vsz-server01	Running	Free Trial	East Asia
vsz02	Running	Free Trial	East Asia
vsz03	Running	Free Trial	East Asia

CONNECT RESTART SHUT DOWN ATTACH REPAIR DISK CAPTURE DELETE

- 4 Verify that the VM has stopped running.

Figure 72. Verifying VM has stopped running

virtual machines

INSTANCES IMAGES DISKS

NAME	STATUS	SUBSCRIPTION	LOCATION	DNS NAME
sim01	Running	Free Trial	East Asia	sim01.cloudapp.net
vsz-cp01	Running	Free Trial	East Asia	vsz-cp01.cloudapp.net
vsz-server01	Running	Free Trial	East Asia	vsz-server01.cloudapp.net
vsz02	Running	Free Trial	East Asia	vsz02.cloudapp.net
vsz03	Stopped (Deallocated)	Free Trial	East Asia	vsz03.cloudapp.net

- 5 Open command prompt.
- 6 Enter the **Test-AzureStaticVnetIP -VnetName <name> -IPAddress <test IP address>** command to verify that the IP address is available to assign to the VM.

Figure 73. Verifying IP address availability

```

PS C:\> Test-AzureStaticVNetIP -VNetName vszg-net -IPAddress 10.250.1.10
VERBOSE: 下午 01:42:27 - Begin Operation: Test-AzureStaticVNetIP
VERBOSE: 下午 01:42:36 - Completed Operation: Test-AzureStaticVNetIP

IsAvailable           : True
AvailableAddresses   : {}
OperationDescription : Test-AzureStaticVNetIP
OperationId          : 66517887-bc97-b994-9fbi-a2b8d806a8a
OperationStatus      : Succeeded

PS C:\>
PS C:\> Test-AzureStaticVNetIP -VNetName vszg-net -IPAddress 10.250.1.50
VERBOSE: 下午 01:42:49 - Begin Operation: Test-AzureStaticVNetIP
VERBOSE: 下午 01:42:56 - Completed Operation: Test-AzureStaticVNetIP

IsAvailable           : False
AvailableAddresses   : {10.250.1.6, 10.250.1.7, 10.250.1.8, 10.250.1.9...}
OperationDescription : Test-AzureStaticVNetIP
OperationId          : fdb23add-140b-b59b-bd48-55435202a110
OperationStatus      : Succeeded

```

- Assign the available IP (10.250.1.10 in this example) to the VM using the **Get-AzureVM -ServiceName vsz03 -Name vsz03 | Set-AzureStaticVNetIP -IPAddress 10.250.1.10 | Update-AzureVM** commands.

Figure 74. Assigning the static IP to the VM

```

PS C:\>
PS C:\> Get-AzureVM -ServiceName vsz03 -Name vsz03 `
>> | Set-AzureStaticVNetIP -IPAddress 10.250.1.10 `
>> | Update-AzureVM
>>

VERBOSE: 下午 01:49:07 - Completed Operation: Get Deployment
VERBOSE: 下午 01:49:10 - Completed Operation: Get Deployment
VERBOSE: 下午 01:49:10 - Begin Operation: Update-AzureVM
VERBOSE: 下午 01:50:12 - Completed Operation: Update-AzureVM

OperationDescription      OperationId              OperationStatus
-----
Update-AzureVM            8856febb-ac82-bf09-bf2f-d9d8b0472400  Succeeded

PS C:\>

```

- From the *Virtual Machines* page, select the VM.
- Click **Start**.



Figure 75. Starting the VM  
virtual machines

INSTANCES IMAGES DISKS

NAME	STATUS	SUBSCRIPTION	LOCATION
sim01	Running	Free Trial	East Asia
vsz-cp01	Running	Free Trial	East Asia
vsz-server01	Running	Free Trial	East Asia
vsz02	Running	Free Trial	East Asia
vsz03	Stopped (Deallocated)	Free Trial	East Asia

CONNECT START SHUT DOWN ATTACH DETACH DISK CAPTURE DELETE

10 Click the VM properties and verify that the IP address has changed.

Figure 76. Verifying static IP address is assigned to the VM

Microsoft Azure CREDIT STATUS nhsu@ruckuswireless

usage overview

VSZ03 2 CORE(S) 10 of 20 CORE(S)

disks

DISK	TYPE	HOST CACHE	VHD
vsz03-vsz03-2015-06-30	OS disk	Read/Write	https://vscg32storage.blob.c

STATUS: Running

DNS NAME: vsz03.cloudapp.net

HOST NAME: -

PUBLIC VIRTUAL IP (VIP) ADDRESS: 23.99.114.42

INTERNAL IP ADDRESS: 10.250.1.10

SSH DETAILS: vsz03.cloudapp.net : 22

## Assigning a Static Public IP Address to a VM

Microsoft Azure assigns a dynamic IP address to a VM when it is created. In addition, a static public IP address must be assigned to a VM as DNS names cannot be configured in a vSZ; resulting in changes to the public IP address.

**NOTE:** Microsoft Azure currently only supports assigning static public IP addresses to VMs through the command line interface (CLI).

Follow these steps to assign a static public IP address to a VM:

- 1 Open the command prompt and create a static IP by typing the **New-AzureReservedIP-ReservedIPName <name>-Label <label name>-Location <location name>** command.

Figure 77. Creating a static IP address

```
PS C:\> New-AzureReservedIP -ReservedIPName "vsz-IP_01" -Label "Nick_for_vsz01" -Location "East Asia"
VERBOSE: 上午 11:13:45 - Begin Operation: New-AzureReservedIP
VERBOSE: 上午 11:14:17 - Completed Operation: New-AzureReservedIP

OperationDescription      OperationId                OperationStatus
-----
New-AzureReservedIP      bbad788d-3f79-b0c3-8826-d85b4795029f  Succeeded

PS C:\>
```

- 2 Verify that the static IP address is created by typing the **Get-AzureReservedIP** command.

Figure 78. Verifying static IP address is created

```
PS C:\> Get-AzureReservedIP
VERBOSE: 下午 01:35:57 - Begin Operation: Get-AzureReservedIP
VERBOSE: 下午 01:36:00 - Completed Operation: Get-AzureReservedIP

ReservedIPName           : MyReservedIP
Address                   : 23.99.118.9
Id                        : a7f1f41a-0427-4b9b-a410-b632ea06d907
Label                     : ReservedIPLabel
Location                  : East Asia
State                     : Created
InUse                     : True
ServiceName               : vsz-server01
DeploymentName            : vsz-server01
OperationDescription      : Get-AzureReservedIP
OperationId               : 1228af4d-8db9-b472-aaf5-0e7cfa3d5203
OperationStatus           : Succeeded

ReservedIPName           : vsz-IP_01
Address                   : 23.99.122.87
Id                        : 9d876fb4-0bc6-4177-8427-e27f60fc863f
Label                     : Nick_for_vsz01
Location                  : East Asia
State                     : Created
InUse                     : False
ServiceName               : Null before assignment
DeploymentName            :
OperationDescription      : Get-AzureReservedIP
OperationId               : 1228af4d-8db9-b472-aaf5-0e7cfa3d5203
OperationStatus           : Succeeded
```

- 3 Select a VM to assign the static public IP by typing the **get-azurevm** command.

Figure 79. Selecting the VM to assign a static IP address

```
PS C:\> get-azurevm
```

ServiceName	Name	Status
sim01	sim01	ReadyRo le
vsz-cp01	vsz-cp01	Provisionin
vsz-server01	vsz-server01	ReadyRo le

- 4 Set the IP address to the VM by typing the **Set-AzureReservedIPAssociation-ReservedIPName <name>-ServiceName <name>** command.

Figure 80. Setting the IP address

```
PS C:\> Set-AzureReservedIPAssociation -ReservedIPName vsz-IP_01 -ServiceName vsz-cp01
VERBOSE: 下午 01:42:19 - Begin Operation: Set-AzureReservedIPAssociation
VERBOSE: 下午 01:44:17 - Completed Operation: Set-AzureReservedIPAssociation
```

OperationDescription	OperationId	OperationStatus
Set-AzureReservedIPAssociation	503e8b53-3c0d-b4c5-ac3c-68d06bb6f231	Succeeded

```
PS C:\>
```

- 5 Verify that the static public IP address to assigned to the VM by typing the **Get-AzureReservedIP** command.

Figure 81. Verifying that the IP address is assigned

```

PS C:\> Get-AzureReservedIP
VERBOSE: 01:49:33 - Begin Operation: Get-AzureReservedIP
VERBOSE: 01:49:36 - Completed Operation: Get-AzureReservedIP

ReservedIPName      : MyReservedIP
Address              : 23.99.118.9
Id                   : a7f1f41a-0427-4b9b-a410-b632ea06d907
Label                : ReservedIPLabel
Location             : East Asia
State                : Created
InUse                : True
ServiceName          : vsz-server01
DeploymentName       : vsz-server01
OperationDescription : Get-AzureReservedIP
OperationId          : 8409bdf-fd02-bfe9-afd6-e3ea05262d83
OperationStatus      : Succeeded

ReservedIPName      : vsz-IP_01
Address              : 23.99.122.87
Id                   : 9d876fb4-0bc6-4177-8427-e27f60fc863f
Label                : Nick_for-vsz01
Location             : East Asia
State                : Created
InUse                : True
ServiceName          : vsz-cp01
DeploymentName       : vsz-cp01
OperationDescription : Get-AzureReservedIP
OperationId          : 8409bdf-fd02-bfe9-afd6-e3ea05262d83
OperationStatus      : Succeeded

```

- 6 From the *Microsoft Azure* page, click **Virtual Machines > Instances** and verify that DNS Name.
- 7 Select the VM.
- 8 Click the **Dashboard** tab. Verify that you are able to see the updated Public IP address.

Figure 82. Verifying the DNS name and static public IP address changes virtual machines

The screenshot displays the Azure portal interface. At the top, there are tabs for INSTANCES, IMAGES, and DISKS. Below this is a table listing virtual machines:

NAME	STATUS	SUBSCRIPTION	LOCATION	DNS NAME
vm01	Running	Free Trial	East Asia	vm01.cloudapp.net
vsz-cp01	Running	Free Trial	East Asia	vsz-cp01.cloudapp.net
vsz-server01	Running	Free Trial	East Asia	vsz-server01.cloudapp.net

Below the table, the dashboard for the selected VM 'vsz-cp01' is shown. It includes a 'DASHBOARD' tab (highlighted with a red circle), 'MONITOR', 'ENDPOINTS', and 'CONFIGURE' options. A performance graph displays metrics like CPU PERCENTAGE, DISK READ BYTES/SEC, DISK WRITE BYTES/SEC, NETWORK IN, and NETWORK OUT over a 1-hour period. Specific data points are labeled: 187.8 KB/s for Disk Read, 358.32 KB/s for Disk Write, 218.39 B/s for Network In, and 11.03% for CPU Percentage. The 'quick glance' section on the right provides a summary of the VM's status and configuration:

- STATUS: Running
- DNS NAME: vsz-cp01.cloudapp.net
- HOST NAME: vsz-cp01
- PUBLIC VIRTUAL IP (VIP) ADDRESS: 23.99.125.119
- INTERNAL IP ADDRESS: 10.250.1.4

The 'PUBLIC VIRTUAL IP (VIP) ADDRESS' and 'INTERNAL IP ADDRESS' fields are circled in red. The 'usage overview' section shows that the VM is using 2 cores out of 20 available. The 'disks' section is partially visible at the bottom.

# Installing the vSZ on the Google Computing Engine

# 4

In this chapter:

- [Logging into GCE and Selecting a Project](#)
- [Creating a Storage Bucket](#)
- [Uploading the vSZ image to a Storage](#)
- [Creating a vSZ Image for Virtual Machines](#)
- [Creating Networks and Configuring Firewall Rules](#)
- [Creating Virtual Machine \(VM\) Instances](#)

This section describes how to install the vSZ on a GCE.

## Before you begin

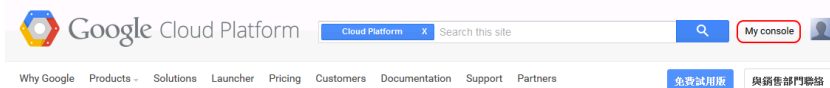
Ensure that you have created an account with GCE and have the login details for the same.

## Logging into GCE and Selecting a Project

Follow these steps to login to the GCE site:

- 1 Click <http://cloud.google.com> to access the *Google Cloud Platform* website.
- 2 Select **My console** as shown.

Figure 83. GCE Page - My console



- 3 Login to the account with your user name and password.
- 4 Click **Sign in**. A list of projects you created is displayed.

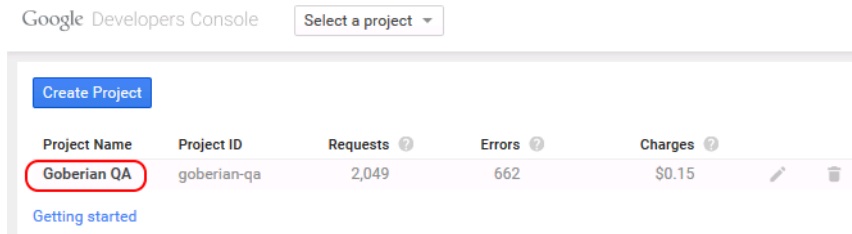
---

**NOTE:** You can create projects by clicking **Create a project** in the drop-down.

---

5 Click **Select a project** to choose a project as shown.

Figure 84. Selecting a Project

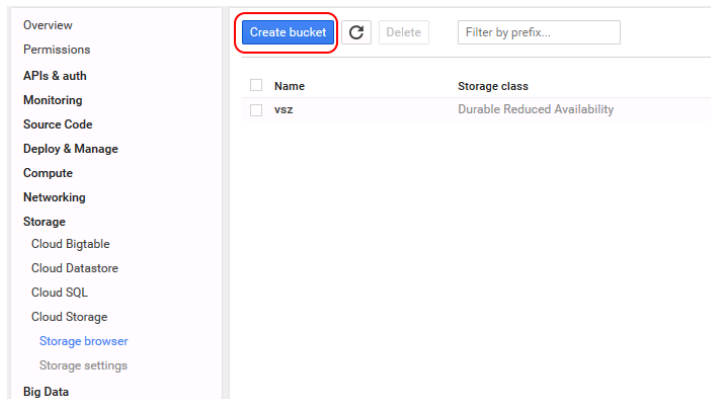


## Creating a Storage Bucket

You can create storage for the objects you create. Follow these steps to create storage:

- 1 From *Google Developers Console*, click **Storage > Cloud Storage > Browser**. The *Cloud Storage Buckets* screen appears.
- 2 Click **Create bucket**. The *New bucket* screen appears.

Figure 85. Creating a Storage Bucket



- 3 In *Name*, type the name of the storage bucket
- 4 In *Storage class*, select the storage class you want. You can choose from *Standard*, *DRA*, and *Nearline* in the drop-down list.
- 5 In *Location*, select the location from the drop-down list.

Figure 86. New Bucket Information

**New bucket**

**Name**  
Bucket names must be unique across all projects in Cloud Storage.  
vsz

**Storage class**  
Standard buckets provide higher availability. DRA buckets cost less and can be located in specific regions. [Learn more](#)  
Durable Reduced Availability

**Location** ? **Region** ?  
Asia ASIA-EAST1

**Create** **Cancel**

- 6 Click **Create**. The storage bucket you created is listed in the browser.
- 7 To create another storage, click **Create bucket** as shown.

Figure 87. Creating Another Storage Bucket

Overview  
Permissions  
APIs & auth  
Monitoring  
Source Code  
Deploy & Manage  
Compute  
Networking  
Storage  
Cloud Bigtable  
Cloud Datastore  
Cloud SQL  
Cloud Storage  
Storage browser  
Storage settings

**Create bucket** **Delete**

<input type="checkbox"/>	Name	Storage class
<input type="checkbox"/>	vsz	Durable Reduced Availability

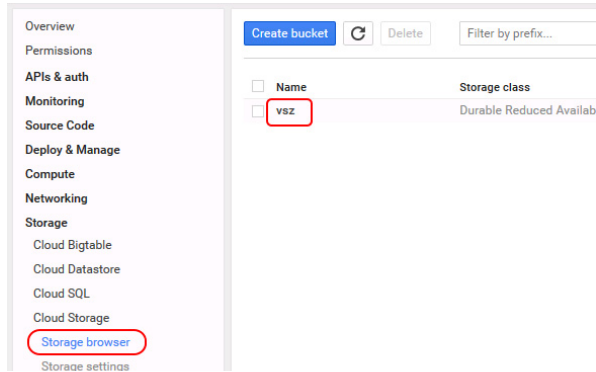


## Uploading the vSZ image to a Storage

Follow these steps to upload a vSZ image to the storage bucket you created:

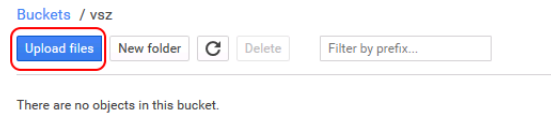
- 1 Select the storage bucket to upload the vSZ image as shown.

Figure 88. Selecting the Storage



- 2 Click **Upload files**.

Figure 89. Uploading the vSZ Image



- 3 Browse to the location of the vSZ image and select it.

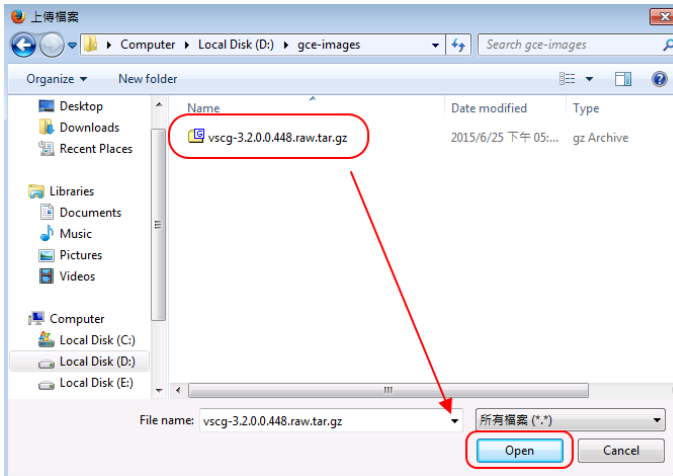
---

**NOTE:** Only images with file-type \*.raw.tar.gz can be selected.

---

- 4 Click **Open**.

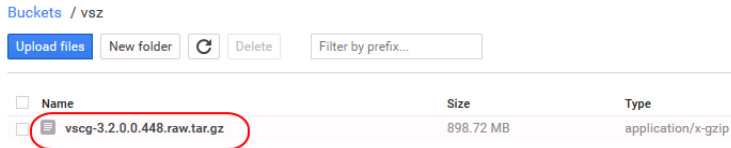
Figure 90. Selecting the vSZ Image



The status of the upload process is displayed.

5 The image is listed in the storage bucket after the image is uploaded.

Figure 91. vSZ Image Uploaded to Storage Bucket

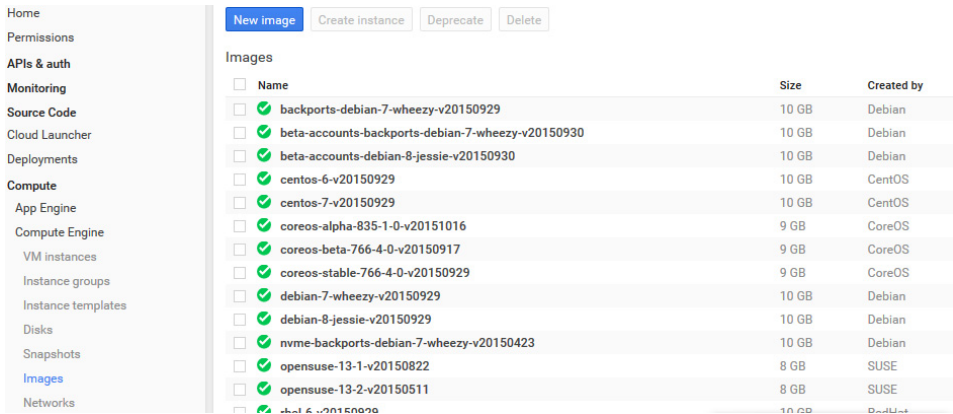


## Creating a vSZ Image for Virtual Machines

Follow these steps to create a vSZ image for virtual machines:

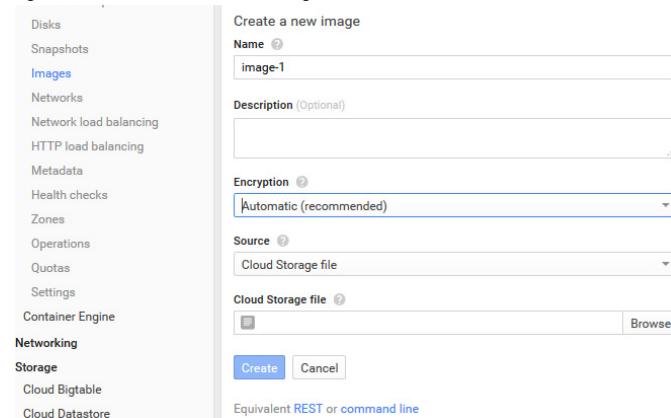
- 1 From *Google Developers Console*, click **Compute > Compute Engine > Images**. A page displaying a list of images appears.

Figure 92. Creating a New Image



- 2 Click **New Image**. The *Create a new image* screen appears.

Figure 93. Create a New Image Screen



- 3 In *Name*, type the name of the image.
- 4 In *Description*, provide a brief description about the image.

- 5 In *Encryption*, select an option from the drop-down list containing Automatic (recommended) and Customer supplied.
- 6 In *Source*, select *Cloud storage file*.
- 7 In *Cloud Storage file*, click *Browse* to select the file.
- 8 Click *Create*. The new image is listed.

Figure 94. The New Image is Listed



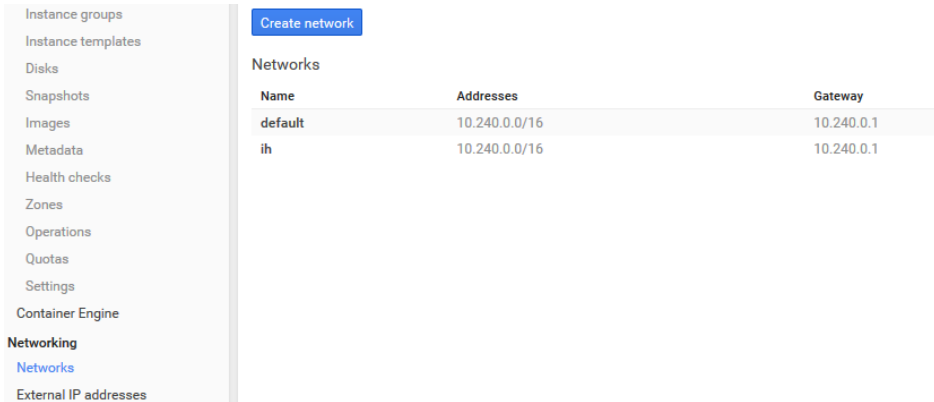
<input type="checkbox"/>	Name	Created by	Crei
<input checked="" type="checkbox"/>	vsz3-2-0-0-448	Goberian QA	Jun
<input type="checkbox"/>	backports-debian-7-wheezy-v20150603	Debian	Jun

## Creating Networks and Configuring Firewall Rules

Follow these steps to create a network and configure firewall rules for your network:

- 1 From *Google Developers Console*, click **Networking > Networks**. A page displaying a list of networks appears.

Figure 95. List of Networks



Name	Addresses	Gateway
default	10.240.0.0/16	10.240.0.1
ih	10.240.0.0/16	10.240.0.1

- 2 Click **Create network**. The *Create a network* screen appears.

Figure 96. Creating a Network

←

Create a network

**Name**

**Description** (Optional)

**Address range**

**Gateway** (Optional)

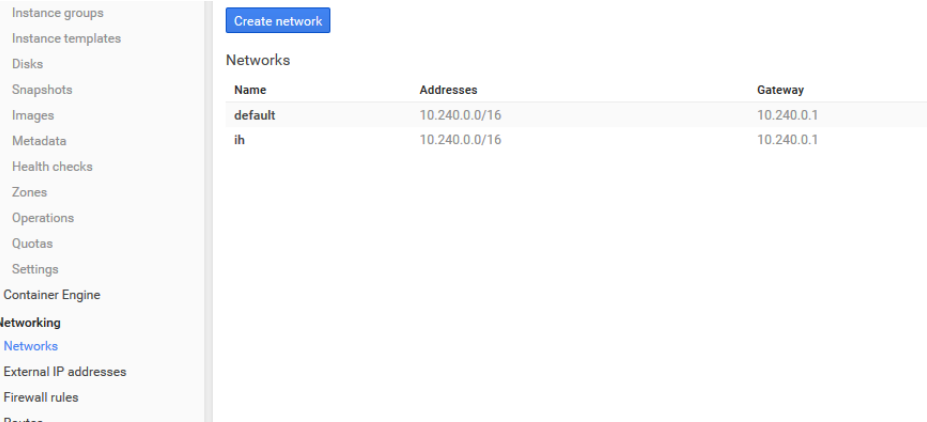
**Firewall rules**  Select any of the firewall rules below that you would like to apply to this network. Once the network is created, you can manage all firewall rules on the Firewall rules page.

<input type="checkbox"/> Name	Source tag / IP range	Allowed protocols / ports
<input checked="" type="checkbox"/> vsz-allow-icmp	0.0.0.0/0	icmp
<input type="checkbox"/> vsz-allow-internal	10.240.0.0/16	tcp:1-65535, 2 more
<input type="checkbox"/> vsz-allow-rdp	0.0.0.0/0	tcp:3389
<input type="checkbox"/> vsz-allow-ssh	0.0.0.0/0	tcp:22

[Equivalent REST](#) or [command line](#)

- 3 In *Name*, type the name of the network.
- 4 In *Description*, provide a brief description about the network.
- 5 In *Address range*, specify the address range for the network.
- 6 In *Gateway*, type the gateway address.
- 7 Under *Firewall rules*, select the rule you want to apply to the network.
- 8 Click **Create**. A page including the new network appears.

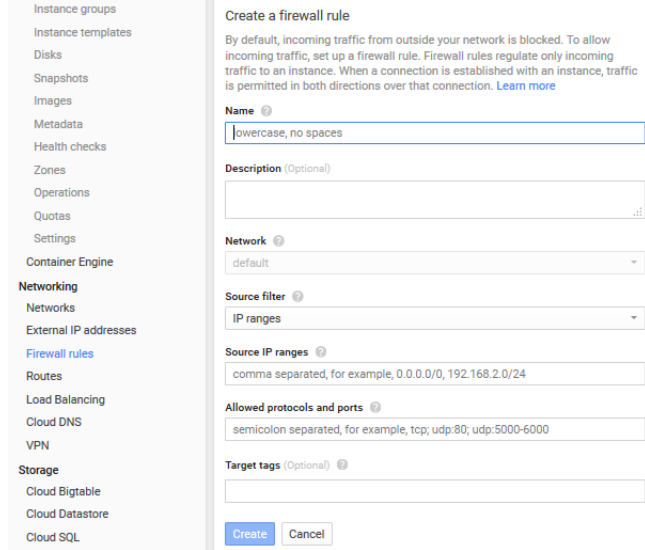
Figure 97. The New Network is Created



9 From the network list, select a network for which you want to add or configure firewall rules.

10 To add a firewall rule, click **Add firewall rule**. The *Create a firewall rule* screen appears.

Figure 98. Creating a Firewall Rule



- 11 In *Name*, type the name of the rule.
- 12 In *Description*, provide a brief description about the rule.
- 13 In *Network*, type the network address.
- 14 In *Source filter*, select *Allow from any source*.
- 15 In *Source IP ranges*, type the range.
- 16 In *Allowed protocols and ports*, type the protocols and ports that will be allowed.
- 17 In *Target tags*, specify a tag name. It is recommended that you provide a tag as all network instances with this tag will adhere to the firewall rule.
- 18 Click **Create**. A page displaying the new firewall rule appears.

Figure 99. Adding Firewall Rules

The screenshot shows the Google Cloud Platform console interface for managing firewall rules. The left sidebar contains a navigation menu with categories like Compute Engine, Networking, and Storage. The main content area is titled 'Firewall rules' and includes a table of existing rules. The 'rule1' rule is highlighted with a red border. Below the table, there is a 'Routes' section with a table of routes and an 'Equivalent REST' link.

Name	Source tag / IP range	Allowed protocols / ports
default-allow-icmp	0.0.0.0/0	icmp
default-allow-internal	10.240.0.0/16	tcp:1-65535; udp:1-65535; icmp
default-allow-rdp	0.0.0.0/0	tcp:3389
default-allow-ssh	0.0.0.0/0	tcp:22
rule1	0.0.0.0/0	tcp

Name	Destination IP ranges	Priority
default-route-27648ffb30780a7	10.240.0.0/16	1000
default-route-d303b6c33adc729e	0.0.0.0/0	1000

## Creating Virtual Machine (VM) Instances

Follow these steps to create new VM instances:

- 1 From Google Developers Console, click **Compute > Compute Engine > VM instances**. The *Compute Engine VM instances* screen appears.
- 2 Click **Create instance**. The *Create a new instance* screen appears.

Figure 100. Creating a new VM Instance

The screenshot shows the 'Create a new instance' form in the Google Cloud Platform console. On the left is a navigation sidebar with categories like Home, Permissions, APIs & auth, Monitoring, Source Code, Cloud Launcher, Deployments, Compute, App Engine, Compute Engine, VM instances (highlighted), Instance groups, Instance templates, Disks, Snapshot, Images, Metadata, Health checks, Zones, Operations, Quotas, Settings, Container Engine, Networking, Storage, Cloud Bigtable, and Cloud Datastore.

The main form area is titled 'Create a new instance' and contains the following sections:

- Name:** A text input field containing 'instance-1'.
- Zone:** A dropdown menu showing 'us-central1-b'.
- Machine type:** A section showing a stack of blue disks icon, 'n1-standard-1', 'vCPUs: 1', and 'Memory: 3.75 GB'. A 'Change' button is to the right.
- Boot disk:** A section showing a disk icon, 'New 10 GB standard persistent disk', 'Image: Debian GNU/Linux 7.9 (wheezy)', and a 'Change' button.
- Firewall:** A section with the heading 'Add tags and firewall rules to allow specific network traffic from the Internet'. It contains two unchecked checkboxes: 'Allow HTTP traffic' and 'Allow HTTPS traffic'.
- Project access:** A section with an unchecked checkbox 'Allow API access to all Google Cloud services in the same project. [Learn more](#)'. Below it is a link 'Management, disk, networking, access & security options'.


At the bottom of the form, there is a note: 'Your Free Trial credits, if available, will be used for this instance.' Below this note are two buttons: 'Create' (in blue) and 'Cancel' (in grey).


- 3 In *Name*, type the name of the VM instance.
- 4 In *Zone*, select a zone from the drop-down list.
- 5 In *Machine type*, *CPU* and *Memory* are selected by default. To modify, click **Change**. The *Select a machine type* screen appears.




Figure 101. Select a Machine Type

Create a new instance


Name  vsz01

Zone  asia-east1-a

Machine type 


Machine type	vCPU	Memory
n1-standard-1	1	3.75 GB

[Change](#)

Boot disk 

New 10 GB standard persistent disk  
Image  
Debian GNU/Linux 7.8 (wheezy)

[Change](#)

Firewall 

Add tags and firewall rules to allow specific network traffic

Allow HTTP traffic

Allow HTTPS traffic

[Management, disk, networking, access & security options](#)

High memory machines

- n1-highmem-2  
2 vCPU, 13 GB Memory
- n1-highmem-4  
4 vCPU, 26 GB Memory
- n1-highmem-8  
8 vCPU, 52 GB Memory
- n1-highmem-16  
16 vCPU, 104 GB Memory
- n1-highmem-32  
32 vCPU, 208 GB Memory

[Select](#) [Cancel](#)

- 6 Click **Select**.
- 7 In *Boot disk*, a standard image is selected by default. To modify, click **Change**. The *Boot disk* screen appears.
- 8 From *Your image*, select the image you want to include.
- 9 Click **Select**.
- 10 In *Firewall*, select the options as appropriate.
- 11 In *Project access*, allow API access as appropriate.
- 12 In *Management*, type the values as appropriate.

Figure 102. VM Management

Management Disks Networking Access & security

Description (Optional)

Tags (Optional)

Automation

Startup script (Optional)

You can choose to specify a startup script that will run when your instance boots up or restarts. Start up scripts can be used to install software and updates, and to ensure that services are running within the virtual machine. [Learn more](#)

Metadata (Optional)

You can set custom metadata for an instance or project outside of the server-defined metadata. This is useful for passing in arbitrary values to your project or instance that can be queried by your code on the instance. [Learn more](#)

Key	Value

+ Add item

---

**NOTE:** Ensure that the tag provided is the same as the one provided while creating a firewall rule. This ensures port mapping happens correctly.

---

**13** In *Disk*, select the options as appropriate.

Figure 103. VM Disk Configuration

Management Disks Networking Access & security

Deletion rule

Delete boot disk when instance is deleted

Encryption ?

Automatic (recommended)

Additional disks ? (Optional)

+ Add item

⤴ Less

---

Your Free Trial credits, if available, will be used for this instance.

Create Cancel

Equivalent REST or [command line](#)

14 In *Networking*, select the options as appropriate.

Management   Disks   **Networking**   Access & security

**Network** ?

default

**External IP** ?

Ephemeral

**IP forwarding** ?

On

[Less](#)

---

Your Free Trial credits, if available, will be used for this instance.

[Create](#) [Cancel](#)

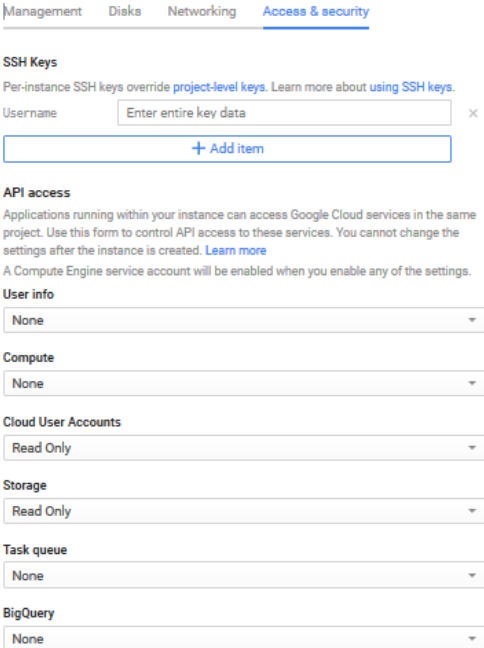
[Equivalent REST or command line](#)

Table 8. External IP Address Options for VM Network Configuration

External IP Options	Description
Ephemeral	The VM is assigned a dynamic public IP address
None	The VM instance is not assigned an external IP address
New static IP address	The VM is assigned a static public IP address

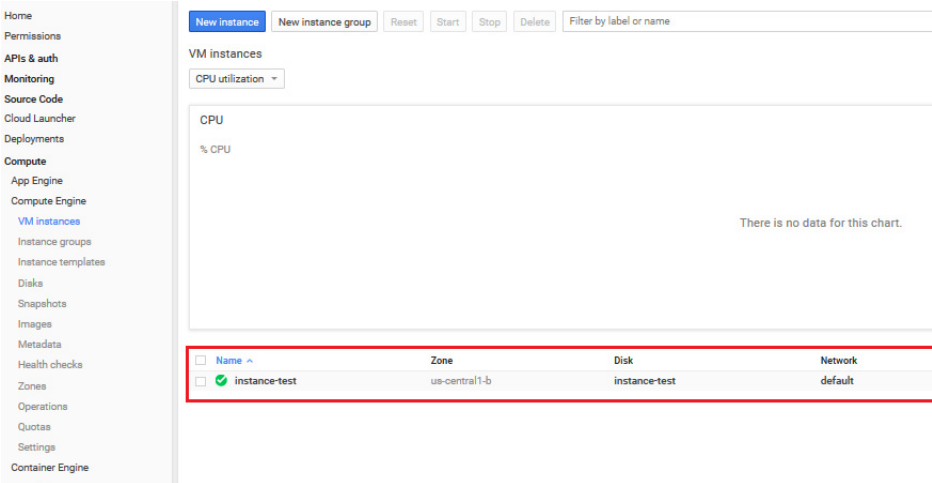
15 In *Access and security*, select the options as appropriate.

Figure 104. VM Access and Security Configuration



16 Click **Create**. The *VM instances* page appears listing the new VM that is created.

Figure 105. New VM is Created



# Configuring the Virtual Machine Interfaces

# 5

The vSZ comes with the option to operate with either one (1) network interface or three (3) network interfaces. Therefore the procedure for setting up the vSZ interface depends on the number of interfaces that it has.

Follow the procedure below that corresponds to the number of interfaces that the vSZ you are installing has.

- [Setting Up the vSZ with One Interface](#)
- [Setting Up the vSZ with Three Interfaces](#)

---

**NOTE:** By default, the VMWare ESXi package comes with three network interfaces. If you want to deploy the vSZ with only one interface, you can edit the virtual machine settings to remove the extra interfaces. The KVM package, on the other hand, comes with a single interface. If you want to deploy the vSZ with three interfaces, edit the virtual machine settings to create two additional interfaces.

---

## Setting Up the vSZ with One Interface

Follow these steps to set up the vSZ with a single network interface.

- 1 Log on to the console using the following credentials:
  - User name: admin
  - Password: admin
- 2 At the `vSZ>` prompt, enter **en** to enable privileged mode.
- 3 At the `Password` prompt, enter **admin**. The `vSZ#` prompt appears.
- 4 Enter **setup**. The console displays the current network settings (if any), and then displays the following prompt:  
Do you want to setup network? [YES/no]

Figure 106. At the vSZ&gt; prompt, enter setup

```
#####
vSZ login: admin
Password:
Last login: Thu Aug 13 03:28:02 on tty1
Please wait. CLI initializing...

Welcome to the Ruckus Virtual SmartZone Command Line Interface
Version: 3.2.0.0.632

vSZ> en
Password: *****

vSZ# setup
```

- 5 Enter **YES**. The next screen prompts you to select the profile configuration that you want to use for this instance of vSZ. The options include:
  - (1) High-Scale
  - (2) Essentials
- 6 Enter the number that corresponds to the profile configuration that you want to deploy.

---

**NOTE:** If you selected *Essentials* and the virtual machine has insufficient memory resources available (for example, the VM has only 8GB of RAM when the minimum RAM requirement is 12GB), you will be unable to continue with the setup process.

---

Figure 107. Enter the number that corresponds to the profile that you want to deploy

```
#####
vSZ login: admin
Password:
Last login: Thu Aug 13 03:28:02 on tty1
Please wait. CLI initializing...

Welcome to the Ruckus Virtual SmartZone Command Line Interface
Version: 3.2.0.0.632

vSZ> en
Password: *****

vSZ# setup

#####
Start vSZ setup process:
#####

*****
vSZ Profile
*****
1. Essentials
2. High Scale
*****
Select vSZ Profile (1/2): 2_
```

- 7 At the `Select IP Version Support` prompt, enter one of the following options:
  - 1: IPv4 Only
  - 2: IPv4 and IPv6
- 8 At the `Select IP configuration` prompt, enter **1** to set up the single vSZ interface (for Control [AP], Cluster, and Management [Web]) manually.
- 9 Configure the IP address, netmask, and gateway of the *control interface*, and then press **<Enter>**. The IP address configuration that you entered appears.
- 10 When the prompt `Are these correct? (y/n)` appears, enter **y** to confirm the IP address configuration.

Figure 108. Configure the IP address settings of the single interface

```

*****
IP Version Support
*****
1. IPv4 only
2. IPv4 and IPv6
*****
Select address type: (1/2) 1
Disabling IPv6...

*****
IPv4 address setup for Control,Cluster,Management
*****
1. MANUAL
2. DHCP
*****
Select IP configuration (1/2): 2

*****
Control,Cluster,Management:
*****
IP Address       : 10.150.5.78
Netmask          : 255.255.252.0
Gateway          : 10.150.4.1
*****
Are these correct (y/n): y_

```

- 11 When the prompt `Select system default gateway (Control, Cluster, Management)?` appears, enter **Control**.

---

**NOTE:** This entry is case-sensitive. Make sure you enter the system default gateway exactly as shown at the prompt.

---

Figure 109. When prompted for the system default gateway, enter Control

```
2. DHCP
*****
Select IP configuration (1/2): 1
IP Address: 172.17.32.124
Netmask: 255.255.255.0
Gateway: 172.17.32.1

*****
Control (AP), Cluster, Management (Web):
*****
IP Address      : 172.17.32.124
Netmask        : 255.255.255.0
Gateway        : 172.17.32.1
*****
Are these correct (y/n): y
Execute networking configuration of Control (AP), Cluster, Management (Web)!
Save networking configuration of Control (AP), Cluster, Management (Web)!

*****
Available Gateway:
*****
Control        : 172.17.32.1
*****
Select system default gateway (Control): Control
```

- 12 At the Primary DNS Server prompt, enter the primary DNS server on the network.
- 13 At the Secondary DNS Server prompt, enter the secondary DNS server (if any) on the network.



- At the `Control NAT IP` prompt, enter the public IP address of the NAT server on the network. If you are not deploying the vSZ behind a NAT server, press `<Enter>` without typing an IP address.

---

**NOTE:** Ensure that each vSZ is associated with a dedicated NAT device.

---

Figure 110. Enter the public IP address of the NAT server (if any)

```
IP Address: 172.17.32.124
Netmask: 255.255.255.0
Gateway: 172.17.32.1

*****
Control (AP), Cluster, Management (Web) :
*****
IP Address      : 172.17.32.124
Netmask        : 255.255.255.0
Gateway        : 172.17.32.1
*****
Are these correct (y/n): y
Execute networking configuration of Control (AP), Cluster, Management (Web) !
Save networking configuration of Control (AP), Cluster, Management (Web) !

*****
Available Gateway:
*****
Control        : 172.17.32.1
*****
Select system default gateway (Control): Control
Primary DNS Server: 208.67.222.222
Secondary DNS Server: 208.67.222.220
Control NAT IP: 216.115.79.136
```

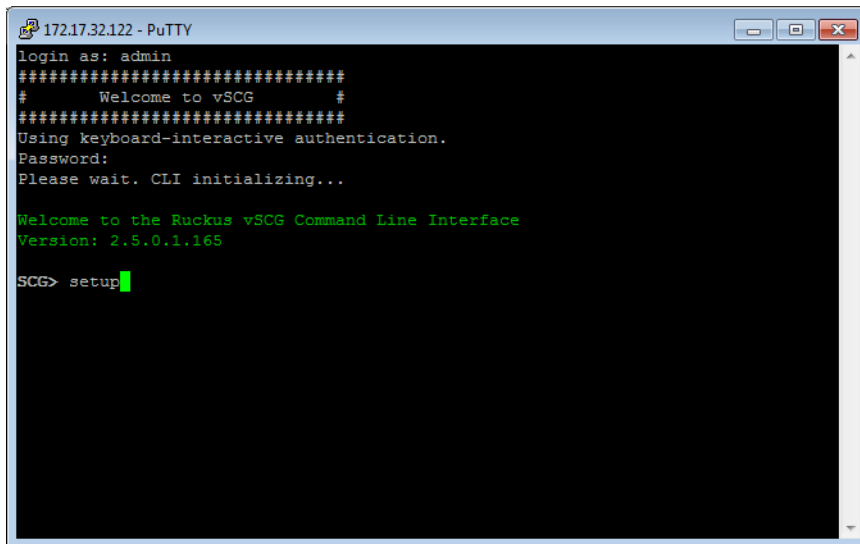
- Enter `restart network`.

You have completed configuring the vSZ interfaces. You are now ready to run the vSZ Setup Wizard. See [Using the Setup Wizard to Install vSZ](#).

## Setting Up the vSZ with Three Interfaces

- 1 Log on to the console using the following credentials:
  - User name: admin
  - Password: admin
- 2 At the vSZ> prompt, enter **en** to enable privileged mode.
- 3 At the Password prompt, enter **admin**. The vSZ# prompt appears.
- 4 Enter **setup**. The console displays the current network settings (if any), and then displays the following prompt:  
Do you want to setup network? [YES/no]

Figure 111. At the vSZ> prompt, enter setup



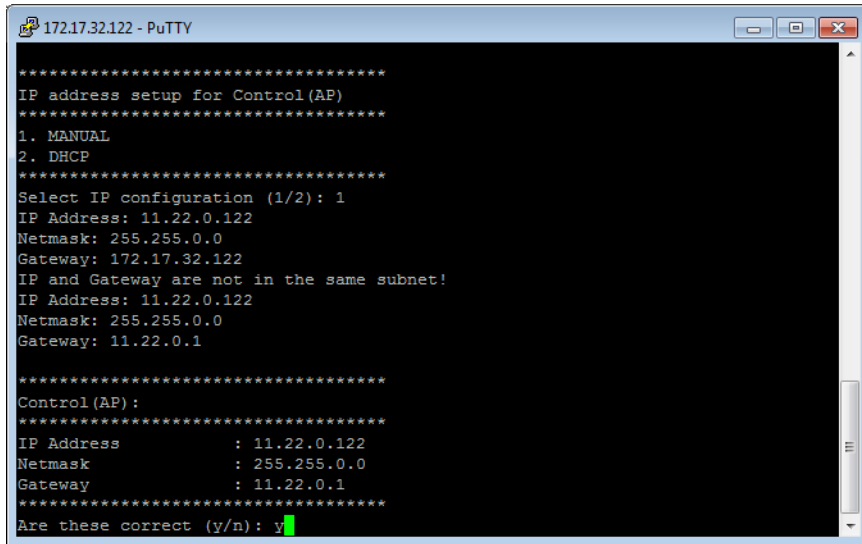
```
172.17.32.122 - PuTTY
login as: admin
#####
#           Welcome to vSCG           #
#####
Using keyboard-interactive authentication.
Password:
Please wait. CLI initializing...

Welcome to the Ruckus vSCG Command Line Interface
Version: 2.5.0.1.165

vSZ> setup
```

- 5 At the Select IP configuration appears prompt, enter **1** to set up the *control interface* manually.
  - a Configure the IP address, netmask, and gateway of the *control interface*, and then press <Enter>. The IP address configuration that you entered appears.
  - b When the message *Are these correct?* appears, enter **y** to confirm the IP address configuration.

Figure 112. Configure the IP address settings of the control interface



- 6 At the `Select IP configuration` prompt, enter **1** to set up the *cluster interface* manually.
  - a Configure the IP address, netmask, and gateway of the *cluster interface*, and then press <Enter>. The IP address configuration that you entered appears.
  - b When the message *Are these correct?* appears, enter **y** to confirm the IP address configuration.
- 7 At the `Select IP configuration` prompt, enter **1** to set up the *management interface* manually.
  - a Configure the IP address, netmask, and gateway of the *management interface*, and the press <Enter>. The IP address configuration that you entered appears.

---

**NOTE:** Take note of the IP address that you assign to the management interface – you will use this IP address to log on to the vSZ web interface.

---

- b When the message *Are these correct?* appears, enter **y** to confirm the IP address configuration.

- 8 When the message `Select system default gateway (Control, Cluster, Management) ?`, enter **Control** or **Management**, depending on your network topology (see [Important Notes About Selecting the System Default Gateway](#)).

---

**NOTE:** This entry is case-sensitive. Make sure you enter the system default gateway exactly as shown at the prompt.

---

Figure 113. When prompted for the system default gateway, enter either Management or Control (depending on your network design)

```

172.17.32.122 - PuTTY
Select IP configuration (1/2): 1
IP Address: 172.17.32.122
Netmask: 255.255.255.0
Gateway: 172.17.32.1

*****
Management (Web) :
*****
IP Address      : 172.17.32.122
Netmask        : 255.255.255.0
Gateway        : 172.17.32.1
*****
Are these correct (y/n): y
Execute networking configuration of Management(Web)!
Save networking configuration of Management(Web)!

*****
Available Gateway:
*****
Control        : 11.22.0.1
Cluster       : 10.27.0.1
Management    : 172.17.32.1
*****
Select system default gateway (Control, Cluster, Management): Management
  
```

- 9 When prompted, enter the primary and secondary DNS server IP addresses.

10 Enter **restart network**.

You have completed configuring the vSZ interfaces. You are now ready to run the vSZ Setup Wizard. See [Using the Setup Wizard to Install vSZ](#).

## Important Notes About Selecting the System Default Gateway

Depending on your network topology, you may select either the **Management** or **Control** interface as the system default gateway.

- If all of the managed APs are located in different locations on the Internet, the vSZ may not know all of the IP subnets of these APs. In this case, the control interface should be set as the default gateway for the vSZ and you will need to add a static route to reach the management network.
- If all of the managed APs belong to a single subnet or to multiple subnets on which you can set the route statically, then you can set the management interface as the default gateway users can set default gateway for the vSZ and set static routes for the vSZ to reach all of its managed APs.

# Using the Setup Wizard to Install vSZ

# 6

In this chapter:

- [Before You Begin](#)
- [Step 1: Start the Setup Wizard and Set the Language](#)
- [Step 2: Select the Profile Configuration That Corresponds to Your vSZ License](#)
- [Step 3: Configure the Management IP Address Settings](#)
- [Step 4: Configure the Cluster Settings](#)
- [Step 5: Set the Administrator Password](#)
- [Step 6: Verify the Settings](#)
- [Logging On to the Web Interface](#)

## Before You Begin

The Setup Wizard helps you perform the initial configuration of the vSZ by presenting the vSZ configuration options in a set of easy-to-complete screens.

The Setup Wizard will prompt you to select one of the two available profile configurations (High-Scale profile and Essentials profile). You must select the profile configuration that corresponds to the vSZ license that you purchased.

Before you start the Setup Wizard, make sure you know the profile configuration that you need to select. If you are unsure which profile configuration you need to select, contact Ruckus Wireless Support.

Follow these steps to run and complete the vSZ Setup Wizard:

[Step 1: Start the Setup Wizard and Set the Language](#)

[Step 2: Select the Profile Configuration That Corresponds to Your vSZ License](#)

[Step 3: Configure the Management IP Address Settings](#)

[Step 4: Configure the Cluster Settings](#)

[Step 5: Set the Administrator Password](#)

[Step 6: Verify the Settings](#)

---

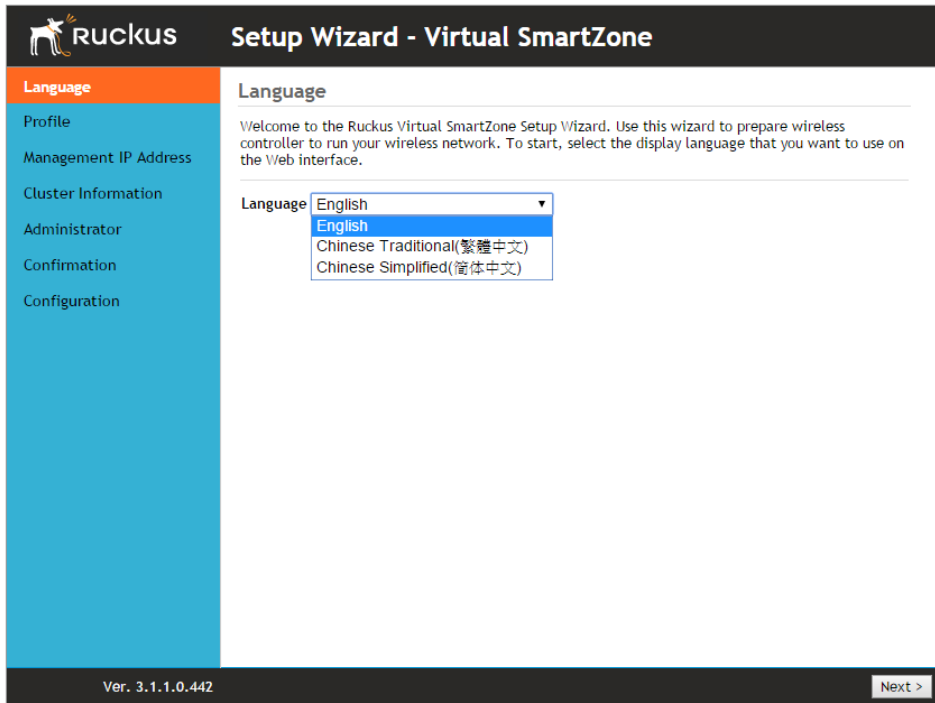
**NOTE:** This guide describes the Setup Wizard screens that appear when you select the High-Scale profile configuration. If you select the Essentials profile configuration, the screens that appear may be slightly different.

---

# Step 1: Start the Setup Wizard and Set the Language

- 1 Start your web browser, and then enter the following in the address bar:  
`https://{management-IP-address}:8443`  
Where management-IP-address is the address you assigned to the management interface.  
The vSZ Setup Wizard appears, displaying the *Language* page.

Figure 114. The Language page



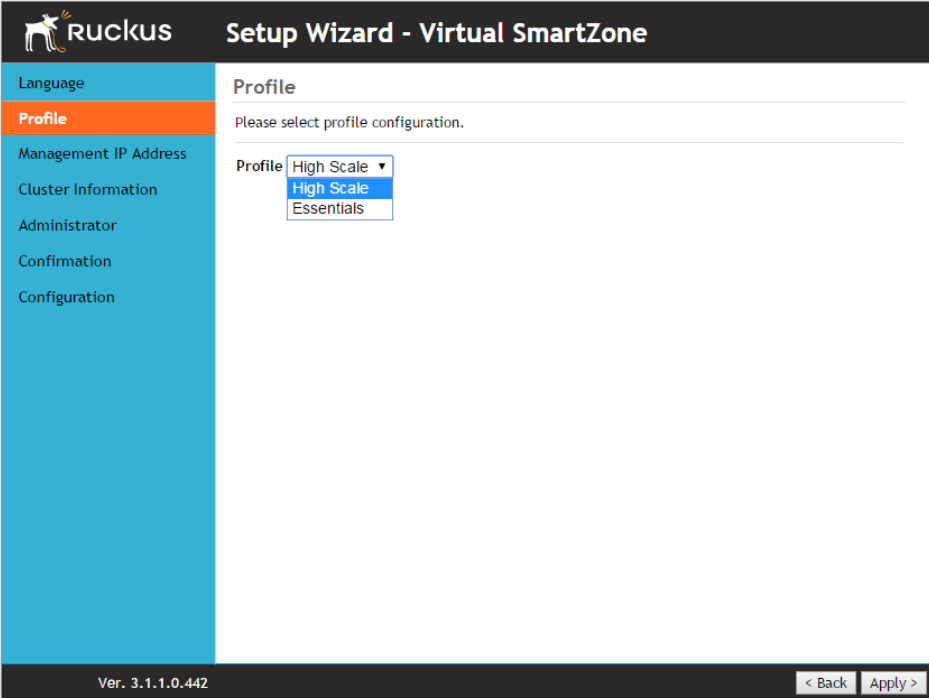
- 2 Select your preferred language for the vSZ web interface. Available options include:
  - English
  - Traditional Chinese
  - Simplified Chinese
- 3 Click **Next**. The *Profile* page appears.



## Step 2: Select the Profile Configuration That Corresponds to Your vSZ License

- 1 Select the profile configuration that corresponds to the vSZ license that you purchased. Available profile configurations include:
  - High Scale
  - Essentials
- 2 Click **Apply**. The message `Applying profile` appears, and then the *Management IP* page appears.

Figure 115. The Profile page



**RUCKUS** Setup Wizard - Virtual SmartZone

Language

**Profile**

Management IP Address

Cluster Information

Administrator

Confirmation

Configuration

Profile

Please select profile configuration.

Profile High Scale ▾  
High Scale  
Essentials

Ver. 3.1.1.0.442

< Back Apply >

## Step 3: Configure the Management IP Address Settings

---

**NOTE:** The vSZ comes in either a single network interface or three network interfaces (one interface each for Control (AP), Cluster, and Management (Web) traffic). The following procedure assumes that the vSZ you are installing uses a single network interface.

---

**WARNING!** If the vSZ that you are installing comes with three network interfaces, you must configure each of the three interfaces to be on three different subnets. Failure to do so may result in loss of access to the web interface or failure of system functions and services.

---

1 In *IP Version Support*, select one of the following options:

- **IPv4 Only:** Click this option if you want the controller to obtain an IPv4 address from a DHCP server on the network.
- **IPv4 and IPv6:** Click this option if you want the controller to obtain both IPv4 and IPv6 addresses from DHCP and DHCPv6 servers on the network.

Figure 116. Select the IP version support

**RUCKUS** Setup Wizard - Virtual SmartZone

Language  
Profile  
**Management IP Address**  
Cluster Information  
Administrator  
Confirmation  
Configuration

### Management IP

Select how you want the Virtual SmartZone to obtain its IPv4 (and IPv6, if supported on your network) IP address settings. To obtain an IP address automatically using DHCP, click "DHCP" for IPv4 or "Auto Configuration" for IPv6. To specify an IP address, click "Static" and then type the IP address settings in "IP Address," "Netmask," and "Gateway." An asterisk (\*) indicates required information.

IP Version Support  IPv4 only  IPv4 and IPv6

Control(AP) Cluster Management(Web)

**IPv4**

Static  DHCP

IP Address \*

Netmask \*

Gateway

Default Gateway\*

Primary DNS Server

Secondary DNS Server

Control NAT IP

Ver. 3.1.1.0.442 Apply >

2 Configure the IP address settings of the *Control (AP/DataPlane)* interface.

- a Under the *IPv4* section, click **Static**, and then enter the network settings that you want to assign to the AP/DataPlane interface, through which client traffic and configuration data are sent and received.

**NOTE:** Although it is possible to use DHCP to assign IP address settings to the Control interface automatically, Ruckus Wireless strongly recommends assigning a static IP address to this interface.

The following network settings are required (others are optional):

- IP address
- Netmask
- Default gateway

- b** If you clicked **IPv4 and IPv6** at the beginning of this procedure, under the *IPv6* section, click **Auto Configuration** if you want the controller to obtain its IP address from Router Advertisements (RAs) or from a DHCPv6 server on the network. If you want to manually assign the IPv6 network address, click **Static**, and then set the values for the following:
- *IP address* (IPv6): Enter an IPv6 address (global only) with a prefix length (for example, 1234::5678:0:c12/123). Link-local addresses are unsupported.
  - *Gateway*: Enter an IPv6 address (global or link-local) without a prefix length. Here are examples:
    - Global address without a prefix length: 1234::5678:0:c12
    - Link-local address without a prefix length: fe80::5678:0:c12
- c** Click the *Cluster* tab when done.

Figure 117. The Cluster tab

**RUCKUS** Setup Wizard - Virtual SmartZone

Language  
Profile  
**Management IP Address**  
Cluster Information  
Administrator  
Confirmation  
Configuration

### Management IP

Select how you want the Virtual SmartZone to obtain its IPv4 (and IPv6, if supported on your network) IP address settings. To obtain an IP address automatically using DHCP, click "DHCP" for IPv4 or "Auto Configuration" for IPv6. To specify an IP address, click "Static" and then type the IP address settings in "IP Address," "Netmask," and "Gateway." An asterisk (\*) indicates required information.

IP Version Support  IPv4 only  IPv4 and IPv6

Control(AP) **Cluster** Management(Web)

**IPv4**

Static  DHCP

IP Address \*

Netmask \*

Gateway

Default Gateway\*

Primary DNS Server

Secondary DNS Server

Control NAT IP

Ver. 3.1.1.0.442 Apply >

- On the *Cluster* tab, click **Static** under the *IPv4* section, and then enter the network settings that you want to assign to the cluster interface, through which cluster data will be sent and received.

**NOTE:** Although it is possible to use DHCP to assign IP address settings to the Cluster interface automatically, Ruckus Wireless strongly recommends assigning a static IP address to this interface.

The following network settings are required (others are optional):

- IP address
- Netmask
- Default gateway

Click the *Management (Web)* tab when done.

Figure 118. The Management (Web) tab

**Ruckus Setup Wizard - Virtual SmartZone**

Language  
Profile  
**Management IP Address**  
Cluster Information  
Administrator  
Confirmation  
Configuration

### Management IP

Select how you want the Virtual SmartZone to obtain its IPv4 (and IPv6, if supported on your network) IP address settings. To obtain an IP address automatically using DHCP, click "DHCP" for IPv4 or "Auto Configuration" for IPv6. To specify an IP address, click "Static" and then type the IP address settings in "IP Address," "Netmask," and "Gateway." An asterisk (\*) indicates required information.

IP Version Support  IPv4 only  IPv4 and IPv6

Control(AP) Cluster Management(Web)

**IPv4**

Static  DHCP

IP Address \*

Netmask \*

Gateway

Default Gateway\*

Primary DNS Server  IPv4 Primary DNS

Secondary DNS Server  IPv4 Secondary DNS

Control NAT IP

Ver. 3.1.1.0.442 Apply >

- On the *Management (Web)* tab, configure the IP address settings of the management interface.

- a Under the *IPv4* section, click **Static**, and then enter the network settings that you want to assign to the AP/DataPlane interface, through which client traffic and configuration data are sent and received.

---

**NOTE:** Although it is possible to use DHCP to assign IP address settings to the Control interface automatically, Ruckus Wireless strongly recommends assigning a static IP address to this interface.

---

The following network settings are required (others are optional):

- IP address
  - Netmask
  - Default gateway
- b If you clicked **IPv4 and IPv6** at the beginning of this procedure, under the *IPv6* section, click **Auto Configuration** if you want the management (web) interface to obtain its IP address from Router Advertisements (RAs) or from a DHCPv6 server on the network. If you want to manually assign the IPv6 network address, click **Static**, and then set the values for the following:
    - *IP address* (IPv6): Enter an IPv6 address (global only) with a prefix length (for example, 1234::5678:0:c12/123). Link-local addresses are unsupported.
    - *Gateway*: Enter an IPv6 address (global or link-local) without a prefix length. Here are examples:
      - Global address without a prefix length: 1234::5678:0:c12
      - Link-local address without a prefix length: fe80::5678:0:c12
- 5 At the bottom of the screen (see [Figure 119](#)), select the interface that you want to set as the default system gateways for IPv4 and IPv6 (if enabled), and then type the primary and secondary DNS server addresses.

---

**NOTE:** The appropriate interface to use as the default system gateway depends on the topology of your network. See [Important Notes About Selecting the Gateway](#) for more information.

---

Figure 119. Select the IPv4 and IPv6 (if enabled) default system gateways

**RUCKUS** Setup Wizard - Virtual SmartZone

Language  
Profile  
**Management IP Address**  
Cluster Information  
Administrator  
Confirmation  
Configuration

### Management IP

Select how you want the Virtual SmartZone to obtain its IPv4 (and IPv6, if supported on your network) IP address settings. To obtain an IP address automatically using DHCP, click "DHCP" for IPv4 or "Auto Configuration" for IPv6. To specify an IP address, click "Static" and then type the IP address settings in "IP Address," "Netmask," and "Gateway." An asterisk (\*) indicates required information.

IP Version Support  IPv4 only  IPv4 and IPv6

Control(AP) Cluster Management(Web)

**IPv4**

Static  DHCP

IP Address \* 1.1.1.100

Netmask \* 255.255.255.0

Gateway

Default Gateway\* Management ▼

Primary DNS Server 10.10.10.10

Secondary DNS Server IPv4 Secondary DNS

Control NAT IP

Ver. 3.1.1.0.442 Apply >

- 6 Check the network settings that you have configured on the *Control*, *Cluster*, and *Management* tabs and the default gateway that you have selected. Verify that they are all correct.
- 7 Click the **Apply** to continue. The controller validates and applies the network settings that you have configured.

Figure 120. The controller validates and applies the network settings you have configured

**CAUTION!** It may take the controller up to 15 minutes to activate its interfaces. If an error message appears after you apply the network interface settings, wait at least 15 minutes, and then try again.

**NOTE:** If the controller is unable to validate the network settings that you configured, an error message appears. If this happens, check the network settings that you configured and verify that you are able to connect to the IP address that you assigned to the *Management (Web)* interface.

- 8 Update the IP address settings of the administrative computer with the same subnet settings that you assigned to the *Management (Web)* interface (see [Step 4](#)).

Continue to [Step 4: Configure the Cluster Settings](#).



## Important Notes About Selecting the Gateway

Depending on your network topology, you may select either the *Management* or *Control* interface as the gateway.

- If all of the managed APs are located in different locations on the Internet, the controller may not know all of the IP subnets of these APs. In this case, the control interface should be set as the default system gateway of the controller and you will need to add a static route to reach the management network.
- If all of the managed APs belong to a single subnet or to multiple subnets on which you can set the route statically, then you can set the management interface as the default gateway users can set default system gateway of the controller and set static routes for the controller to reach all of its managed APs.

## Step 4: Configure the Cluster Settings

The next step is to configure the vSZ cluster settings. The actions that you need to perform in this step depend on whether you are creating a new cluster (with this vSZ as the first node) or you are setting up this vSZ to join an existing cluster.

- [If This vSZ Is Forming a New Cluster](#)
- [If This vSZ Is Joining an Existing Cluster](#)

Figure 121. The Cluster Information page, showing the New Cluster option

**RUCKUS** Setup Wizard - Virtual SmartZone

Language  
Profile  
Management IP Address  
**Cluster Information**  
Administrator  
Confirmation  
Configuration

**Cluster Information**

vSZ Cluster Setting:

Cluster Name:

Controller Name:

Controller Description:

NTP Server:

AP Conversion  Convert ZoneDirector APs in factory settings to Virtual SmartZone APs automatically

Ver. 3.1.1.0.442

## If This vSZ Is Forming a New Cluster

Follow these steps if you want to use this vSZ to create a new cluster.

- 1 On the *Cluster Information* page, configure the following settings:
  - In *vSZ Cluster Setting*, select **New Cluster**.
  - In *Cluster Name*, type a name that you want to assign to this new cluster.

---

**NOTE:** The *Cluster Name* and *Controller Name* boxes only accept alphanumeric characters, hyphens (-), and underscores (\_). They do not accept the space character or other special characters (for example, \$, \*, #, !).

---

- In *Controller Name*, type a name for the vSZ controller in this new cluster.
- In *Controller Description*, type a description for the vSZ controller.
- In *NTP Server*, type the address of the NTP server from which members of the cluster will obtain and synchronize time. The default NTP server is `pool.ntp.org`.

---

**CAUTION!** Before continuing, verify that the cluster settings are correct. Once the cluster is created, you will be unable to edit its settings without rebuilding the cluster from scratch.

---

- 2 Click **Next** to continue to the *Administrator* page (see [Step 5: Set the Administrator Password](#)).

## If This vSZ Is Joining an Existing Cluster

If this is not the first vSZ cluster on the network, you can set up this vSZ virtual appliance to join an existing cluster.

---

**CAUTION!** To add this vSZ to an existing cluster, the entire target cluster must be in a healthy state (no node must be in “out of service” state). If any member node is out of service, the join request will fail. You will need to remove any out-of-service node from the cluster before you can add a new node successfully.

---

**CAUTION!** A vSZ cluster supports a maximum of four nodes. If you are building a vSZ-E cluster with more than two nodes, two (2) additional cores must be added to each node to support the added search and replication capabilities.

---

Follow these steps to configure this vSZ to join an existing cluster.

- 1 In *vSZ Cluster Setting*, select **Join Existing Cluster**.
- 2 In *Cluster Name*, type the name of the cluster that this vSZ is joining.

**NOTE:** The *Cluster Name* and *Controller Name* boxes only accept alphanumeric characters, hyphens (-), and underscores (\_). They do not accept the space character or other special characters (for example, \$, \*, #, !).

- 3 In *Controller Name (optional)*, type a name that you want to assign to this new controller.
- 4 In *Controller Description*, type a description for this new controller.
- 5 In *Join Exist vSZ Cluster IP*, type the IP address of the leader in the existing cluster.
- 6 In *Admin Password*, type the administrator password to the web interface of the leader node.
- 7 Click **Next** to continue to the *Administrator* page. See [Step 5: Set the Administrator Password](#).

Figure 122. The Cluster Information page, showing the Join Existing Cluster option

**RUCKUS** Setup Wizard - Virtual SmartZone

Language  
Profile  
Management IP Address  
**Cluster Information**  
Administrator  
Confirmation  
Configuration

**Cluster Information**

vSZ Cluster Setting: Join Existing Cluster ▾  
Cluster Name:   
Controller Name:   
Controller Description:

Join Exist vSZ Cluster IP:   
Admin Password:\*

Ver. 3.1.1.0.442

**NOTE:** If the firmware version on this vSZ (shown in the lower left area of the *Cluster Information* page) does not match the firmware version of the cluster, a message appears and prompts you to upgrade the vSZ firmware. Click **Upgrade**, and then follow the prompts to perform the upgrade.

---

## Step 5: Set the Administrator Password

- 1 On the *Administrator* page, configure the web interface and CLI passwords. All fields are required.
    - *Admin Password:* Type a password that you want to use to access the web interface.
    - *Confirm Password:* Retype the password above to confirm.
    - *Enable Password:* Type a password that you want to use to enable CLI access to the vSZ.
    - *Confirmation Password:* Retype the password above to confirm.
- 

**NOTE:** The web interface and CLI passwords must be at least eight (8) characters and must include one number, one letter, and one special character (for example, \$, \*, #, !).

---

- 2 Click **Next** to continue. The *Confirmation* page appears and displays all the vSZ settings that you have configured using the Setup Wizard.

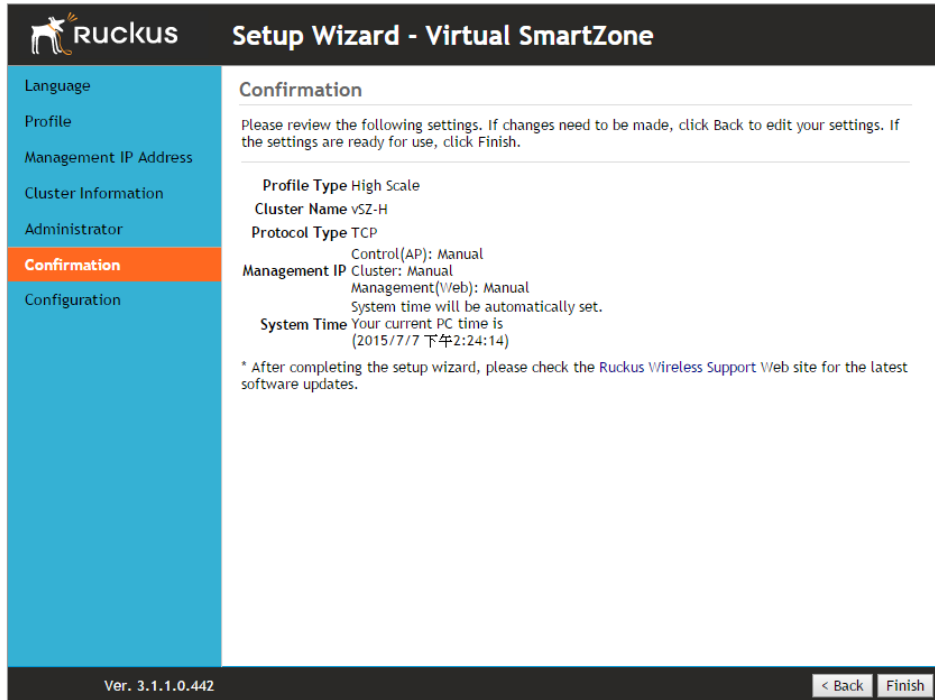
Figure 123. Set the web interface and CLI passwords

The screenshot shows the Ruckus Setup Wizard interface for configuring the Administrator password. The left sidebar contains a list of steps: Language, Profile, Management IP Address, Cluster Information, Administrator (highlighted in orange), Confirmation, and Configuration. The main content area is titled "Administrator" and includes the following text: "Enter Admin's password and password that permits administrative access to the Web interface. (Use this information to log into the Web interface after this setup is complete, to further configure your new wireless network.)". Below this text are two password input fields: "Admin Password \*" and "Confirm Password \*", both containing masked characters. A horizontal line separates this section from the next, which is titled "Confirmation" and includes the text: "Enter CLI enable password and password that provides advance command". Below this text are two more password input fields: "Enable Password \*" and "Confirm Password \*", both containing masked characters. At the bottom of the screen, the version number "Ver. 3.1.1.0.442" is displayed on the left, and navigation buttons "< Back" and "Next >" are on the right.

## Step 6: Verify the Settings

Verify that all the settings displayed on the *Confirmation* page are correct. If they are all correct, click **Finish** to apply the settings and activate the vSZ on the network.

Figure 124. The Confirmation page

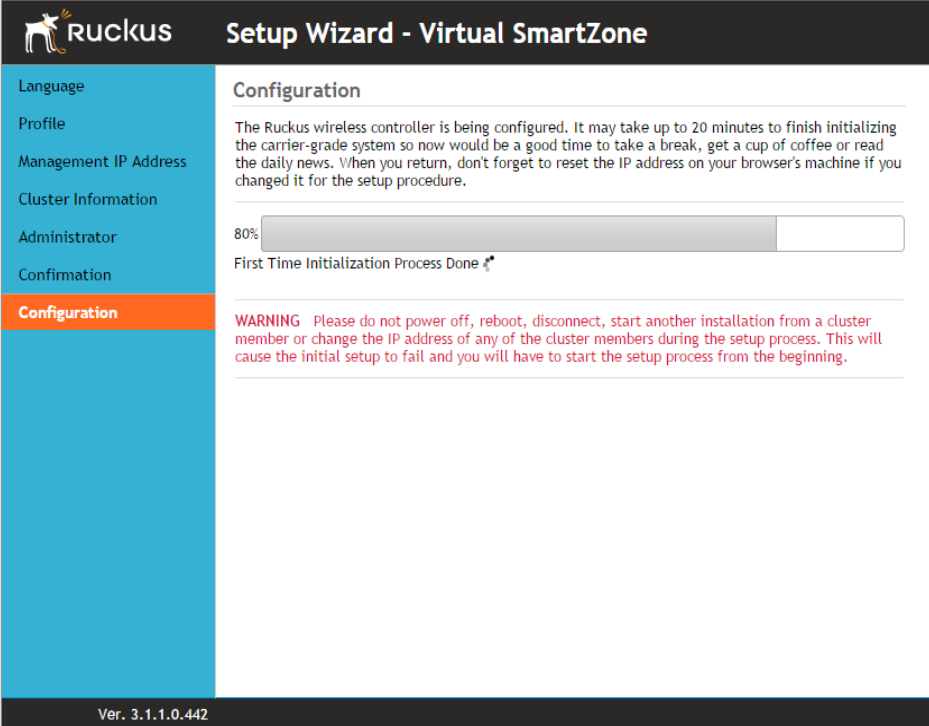


**NOTE:** If you find an incorrect setting, click the **Back** button until you reach the related page, and then edit the settings. When you finish editing the settings, click the **Next** button until you reach the *Confirmation* page again.

A progress bar appears and displays the progress of applying the settings, starting the vSZ services, and activating the vSZ on the network.

When the process is complete, the progress bar shows the message 100% Done. The page also shows the IP address through which you can access the vSZ web interface to manage the appliance.

Figure 125. Setup is complete when the progress bar shows “100% Done”



**RUCKUS** Setup Wizard - Virtual SmartZone

Language  
Profile  
Management IP Address  
Cluster Information  
Administrator  
Confirmation  
**Configuration**

**Configuration**

The Ruckus wireless controller is being configured. It may take up to 20 minutes to finish initializing the carrier-grade system so now would be a good time to take a break, get a cup of coffee or read the daily news. When you return, don't forget to reset the IP address on your browser's machine if you changed it for the setup procedure.

80%

First Time Initialization Process Done 🎉

**WARNING** Please do not power off, reboot, disconnect, start another installation from a cluster member or change the IP address of any of the cluster members during the setup process. This will cause the initial setup to fail and you will have to start the setup process from the beginning.

Ver. 3.1.1.0.442

Congratulations! You have completed the Setup Wizard. You are now ready to log on to the web interface. Go to `https:// {management-IP-address} : 8443`, and then log on with the user name and password that you assigned to the web interface.



# Logging On to the Web Interface

You can access the vSZ web interface from any computer that is on the same subnet as the management (web) interface.

Follow these steps to log on to the vSZ web interface.

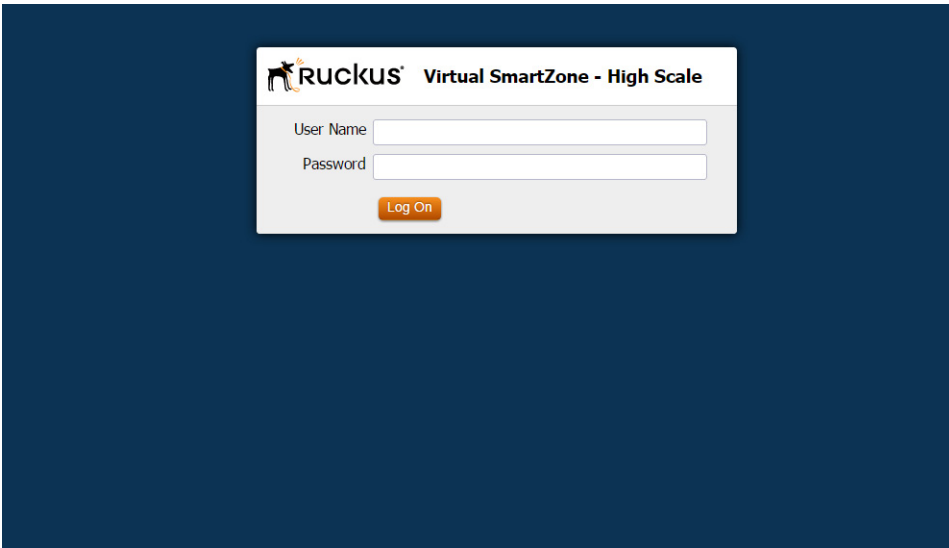
- 1 On a computer that is on the same subnet as the Management (Web) interface, start a web browser.
- 2 In the address bar, enter the IP address that you assigned to the Management (Web) interface and append a colon and 8443 (vSZ management port number) at the end of the address.

For example, if the IP address that you assigned to the Management (Web) interface is 10.10.101.1, then you should enter:

https://10.10.101.1:8443

The vSZ web interface logon page appears.

Figure 126. vSZ web interface logon page



- 3 Log on to the vSZ web interface using the following logon details:
  - User Name: **admin**
  - Password: **{the password that you set when you ran the vSZ Setup Wizard}**
- 4 Click **Log On**.

The web interface refreshes, and then displays the vSZ dashboard page, which indicates that you have logged on successfully.

You are now ready to configure the vSZ.

# Configuring the vSZ High-Scale for the First Time

# 7

---

**NOTE:** This chapter describes the initial configuration tasks that Ruckus Wireless recommends you perform for the vSZ *High-Scale*. The initial configuration of the vSZ *Essentials* is more straightforward and, therefore, is not described here. For information on configuring the vSZ Essentials, refer to the vSZ *Essentials Administrator Guide*.

---

In this chapter:

- [Creating an AP Zone](#)
- [Configuring AAA Servers and Hotspot Settings](#)
- [Creating a Registration Rule](#)
- [Defining the WLAN Settings of an AP Zone](#)
- [Configuring DHCP Option 43](#)
- [Verifying That Wireless Clients Can Associate with a Managed AP](#)
- [What to Do Next](#)

# Creating an AP Zone

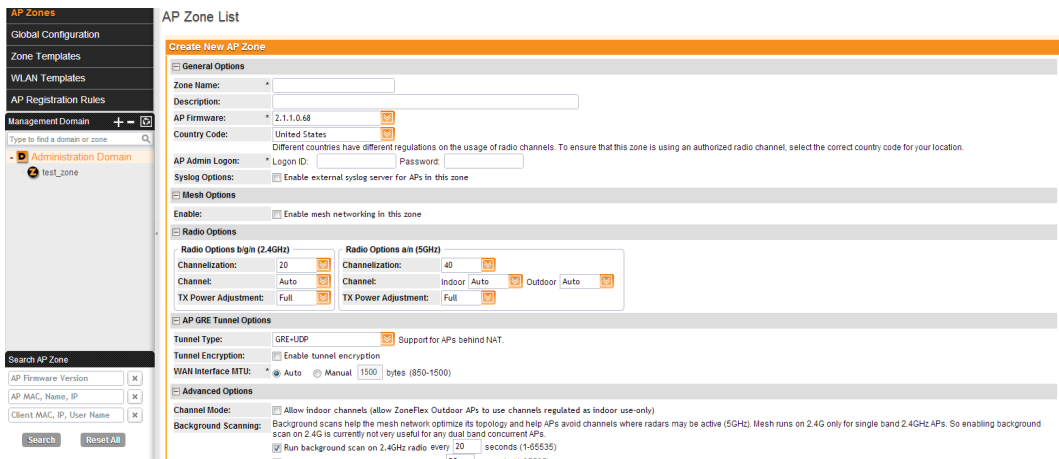
The first step in configuring the vSZ is to create an AP zone. An AP zone functions as a way of grouping APs and applying a particular set of settings (including WLANs and their settings) to these groups of APs. Each AP zone can include up to six WLAN services.

A zone called `staging zone` exists by default. Any AP that registers with the vSZ that is not assigned a specific zone is automatically assigned to the `staging zone`.

Follow these steps to create a new AP zone.

- 1 Click **Configuration > AP Zones**.
- 2 Click **Create New**.

Figure 127. Creating a new AP zone



- 3 Configure the options listed in [Table 9](#).

Table 9. Configuration options in the Create New Zone form

Option	Description
<i>General Options</i>	
Zone Name	Type a name that you want to assign to this new zone.
Description	Type a description for this new zone.
AP Firmware	Displays the latest AP firmware available on the vSZ. If you want this zone to use a different firmware, click <b>Change</b> , and then select a firmware from the list.

Table 9. Configuration options in the Create New Zone form (Continued)

Option	Description
Country Code	<p>Different countries and regions maintain different rules that govern which channels can be used for wireless communications.</p> <p>Set the country code to the proper regulatory region ensures that your vSZ network does not violate local and national regulatory restrictions.</p>
AP Admin Logon	<p>Specify the user name and password that administrators can use to log on directly to the managed access point's native web interface.</p> <p>The following boxes are provided:</p> <ul style="list-style-type: none"> <li>• <i>Logon ID</i>: Type the admin user name.</li> <li>• <i>Password</i>: Type the admin password.</li> </ul>
Syslog Options	<p>If you have a syslog server on the network and you want the vSZ to send syslog data to it, select the <b>Enable external syslog server for APs in this zone</b> check box.</p> <p>The following boxes are provided:</p> <ul style="list-style-type: none"> <li>• <i>IP Address</i>: Type the IP address of the syslog server.</li> <li>• <i>Port</i>: Type the port number that has been opened on the server for syslog data. The default port number is 514.</li> </ul>
<i>Mesh Options</i>	
Enable	<p>Select the <b>Enable mesh networking in this zone</b> check box if you want managed devices that belong to this zone to be able to form a mesh network automatically.</p>
<i>Radio Options</i>	
Radio Options b/g/n (2.4GHz)	<p>Configure the following 2.4GHz radio options:</p> <ul style="list-style-type: none"> <li>• <i>Channelization</i>: Select either 20MHz or 40MHz channel width.</li> <li>• <i>Channel</i>: Select Auto or manually assign a channel for the 2.4GHz radio.</li> <li>• <i>TX Power Adjustment</i>: Manually set the transmit power on all 2.4GHz radios (default is Full).</li> </ul>

Table 9. Configuration options in the Create New Zone form (Continued)

Option	Description
Radio Options a/n (5GHz)	Configure the following 5GHZ radio options: <ul style="list-style-type: none"> <li>• <i>Channelization</i>: Select either 20MHz or 40MHz channel width.</li> <li>• <i>Channel (Indoor and Outdoor)</i>: Select Auto or manually assign channels to the indoor and outdoor 5GHz radios.</li> <li>• <i>TX Power Adjustment</i>: Manually set the transmit power on all 5GHz radios (default is <b>Full</b>).</li> </ul>
AP GRE Tunnel Options	
Tunnel Type	Select a protocol to use for tunneling WLAN traffic back to the vSZ. Options include <b>Ruckus GRE</b> and <b>SoftGRE</b> .
Tunnel Profile	Select the tunnel profile that you want to use. If you want to use Ruckus GRE tunneling for this AP zone, you can use the default tunnel profile or you can select a profile that you created. If you want to use Soft GRE tunneling, you must first create a Soft GRE tunnel profile. NOTE: Instructions for creating Ruckus GRE and Soft GRE tunnel profiles are provided in the <i>Administrator Guide</i> for this release.
Advanced Options	
Channel Mode	If you want to allow outdoor APs that belong to this zone to use wireless channels that are regulated as indoor use only, select the <b>Allow indoor channels</b> check box.
Background Scanning	If you want APs to automatically evaluate radio channel usage, enable and configure the background scanning settings on both the 2.4GHz and 5GHz radios.  By default, background scanning is enabled on both radios and set to run every 20 seconds.

Table 9. Configuration options in the Create New Zone form (Continued)

Option	Description
Client Load Balancing	<p>Improve WLAN performance by enabling load balancing. Load balancing spreads the wireless client load between nearby access points, so that one AP does not get overloaded while another site idles. Load balancing must be enabled on a per-radio basis. To enable load balancing, select the <b>Enable load balancing on [2.4GHz or 5GHz]</b> check box, and then set or accept the default <i>Adjacent Radio Threshold</i> (50dB for the 2.4GHz radio and 43dB for the 5GHz radio).</p>
Smart Monitor	<p>To disable the WLANs of an AP (that belongs to this zone) whenever the AP uplink or Internet connection becomes unavailable, select the <b>Enable</b> check box. And then, configure the following options:</p> <ul style="list-style-type: none"> <li>• <i>Health Check Interval</i>: Set the interval (between 5 and 60 seconds) at which the vSZ will check the AP's uplink connection. The default value is 10 seconds.</li> <li>• <i>Health Check Retry Threshold</i>: Set the number of times (between 1 and 10 times) that the vSZ will check the AP's uplink connection. If the vSZ is unable to detect the uplink after the configured number of retries, the vSZ will disable the AP's WLANs. The default value is 3 retries.</li> </ul> <p>NOTE: When the vSZ disables the AP's WLANs, the AP creates a log for the event. When the AP's uplink is restored, the AP sends the event log (which contains the timestamp when the WLANs were disabled, and then enabled) to the vSZ.</p>

- 4 Click **Create New** to finish creating your first AP Zone. When the vSZ completes creating the AP zone, the following confirmation message appears:

AP zone created successfully. Do you want to view the zone information?

- 5 Click **Yes** to view the zone details, or click **No** to close the confirmation message and return to the zone list.

You have completed creating your first AP zone. You can create additional AP zones, if needed.

## Configuring AAA Servers and Hotspot Settings

---

**NOTE:** If you do not have an AAA server on the network, skip this step.

---

If you have an existing RADIUS (AAA) server on the network, you can set up hotspot services across the network using the Ruckus Wireless access points that the vSZ is managing. To provide hotspot services, you need to add at least one AAA server to the vSZ and create a hotspot service.

AAA servers and hotspot settings must be configured on a per-AP zone basis.

### Adding an AAA Server

Follow these steps to add an AAA server to an AP zone.

- 1 Go to **Configuration > AP Zones**.
- 2 Click the AP zone for which you want to add an AAA server. Alternatively, click the AP zone from the *Management Domains* tree.
- 3 Under the *AP Zones* menu on the sidebar, click **AAA**.
- 4 Click **Create New**. The *Create New RADIUS Server* form appears.
- 5 In the *General Options* section, configure the following settings:
  - *Name*: Type a name for the AAA server that you are adding.
  - *Description*: Type a description for the AAA server that you are adding.
  - *Type*: Click either **RADIUS** or **RADIUS Accounting**, depending on the type of RADIUS server that you are using.
  - *Backup RADIUS*: If a backup RADIUS server exists on the network, you may enable RADIUS backup support by selecting the **Enable backup RADIUS support** check box.
- 6 Configure the options in the Health Check Policy section. These options define the health monitoring settings of the primary RADIUS server by the secondary RADIUS server. The secondary RADIUS is responsible for monitoring the health of the primary RADIUS and for periodically synchronizing its settings to match those of the primary RADIUS.



- *Response Window*: Set the time (in seconds) during which the secondary RADIUS must wait for a response from the primary RADIUS. If the secondary RADIUS does not receive a response during the defined Response Window, the Zombie Period (see below) is started for the primary RADIUS. The default Response Window is 20 seconds.
  - *Zombie Period*: Set the time (in seconds) during which the secondary RADIUS must wait for a response from the primary RADIUS before marking it as “down”. If the secondary RADIUS does not receive a response during the defined Zombie Period, the Revive Interval (see below) is started for the primary server. The default Zombie Period is 40 seconds. If the primary RADIUS still does not respond when the Zombie Period expires, it will be marked as down and the secondary RADIUS will start receiving new requests from the Network Access Server (NAS).
  - *Revive Interval*: Set the time (in seconds) during which the secondary RADIUS must wait for the primary RADIUS to start responding to requests again. If the primary RADIUS starts responding before the Revive Interval expires, new requests will be forwarded to the primary RADIUS again. The default Revive Interval is 120 seconds.
  - *No Response Fail*: Click **Yes** to respond with a reject message to the NAS if no response is received from the RADIUS server. Click **No** to skip sending a response.
- 7 In the *Primary Server* section, configure the following settings:
- *IP Address*: Type the IP address of the AAA server.
  - *Port*: Type the AAA port number. The default AAA port number is 1812.
  - *Shared Secret*: Type the AAA shared secret.
  - *Confirm Secret*: Retype the AAA shared secret that you typed above.
- 8 If you selected the **Enable backup RADIUS support** check box, the *Secondary Server* section is visible. Configure the following *Secondary Server* settings:
- *IP Address*: Type the IP address of the secondary AAA server.
  - *Port*: Type the AAA port number. The default AAA port number is 1812.
  - *Shared Secret*: Type the AAA shared secret.
  - *Confirm Secret*: Retype the AAA shared secret that you typed above.
- 9 Click **Create New**. The following message appears to confirm that you have successfully added the AAA server to the vSZ:
- ```
Authentication server created successfully.
```

The page refreshes, and then the AAA server that you created appears under the *AAA Servers Configuration* section.

Figure 128. The Create New RADIUS Server form

AP Zone: test\_zone >> AAA Servers

AAA Servers

Create New RADIUS Server

General Options

Name: \*

Type:  RADIUS  RADIUS Accounting

Backup RADIUS:  Enable backup RADIUS support

Health Check Policy

Response Window: \* 20 Seconds

Zombie Period: \* 40 Seconds

Revoke Interval: \* 120 Seconds

No Response Fail:  Yes  No

Primary Server

IP Address: \*

Port: \* 1812

Shared Secret: \*

Confirm Secret: \*

Create New Cancel

Show 20 << 1 >> No data

## Creating a Hotspot Service

**NOTE:** If you do not want to provide a hotspot service to users, skip this step.

**NOTE:** Before creating a hotspot, you need to create a user defined interface. For information on how to create a user defined interface, see the *Administrator Guide* for release 2.5.

A hotspot service requires an AAA server. Before creating a hotspot service, make sure you have already added an AAA server to the vSZ. For more information, refer to [Adding an AAA Server](#).

Follow these steps to create a hotspot service for an AP zone.

- 1 Go to **Configuration > AP Zones**.
- 2 Click the AP zone for which you want to create a hotspot service. Alternatively, click the AP zone from the *Management Domains* tree.
- 3 Under the *AP Zones* menu on the sidebar, click **WISPr (Hotspot)**.
- 4 Click **Create New**. The *Create New Hotspot Service* form appears.

## 5 Configure the hotspot service settings listed in [Table 10](#).

Table 10. Hotspot service settings

| Setting              | Description                                                                                                                                                                                                                                                                            |
|----------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| General Options      |                                                                                                                                                                                                                                                                                        |
| Name                 | Type a name for this new hotspot service that you are creating.                                                                                                                                                                                                                        |
| Description          | Type a description for this new hotspot service (for example, <code>Main Office Lobby</code> ).                                                                                                                                                                                        |
| Type                 | Click <b>Registered Users</b> if you want only users with existing profiles on the vSZ to be able to connect to this hotspot. Click <b>Guest-Access</b> if you want guest users to be able to connect to this hotspot.                                                                 |
| Redirection          |                                                                                                                                                                                                                                                                                        |
| Smart Client Support | <ul style="list-style-type: none"> <li>• <b>None:</b> Click to disable Smart Client support.</li> <li>• <b>Enable:</b> Click to enable Smart Client support.</li> <li>• <b>Only Smart Client allowed:</b> Click to allow only Smart Clients to access this hotspot service.</li> </ul> |
| Logon URL            | Type the URL of the subscriber portal (the page where hotspot users can log in to access the service). For more information, see the section “Configuring the Logon URL” in the <i>Administrator Guide</i> for release 2.5.                                                            |
| Start Page           | Set where users will be redirected after logging in successfully. You could redirect them to the page that they want to visit, or you could set a different page where users will be redirected (for example, your company website).                                                   |
| User Session         |                                                                                                                                                                                                                                                                                        |
| Session Timeout      | Set a time limit after which users will be disconnected from the hotspot service and required to log on again. Allowed session timeout range is between 2 and 14400 minutes. The default value is 1440 minutes.                                                                        |
| Grace Period         | Allow disconnected users a grace period after disconnection, during which clients will not need to re-authenticate. Allowed grace period range is between 1 and 14399 minutes. The default value is 60 minutes.                                                                        |

Table 10. Hotspot service settings (Continued)

| Setting              | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
|----------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Location Information |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
| Location ID          | Type a location ID for the hotspot, for example:<br><code>isocc=us,cc=1,ac=408,network=ACMEWISP<br/>_NewarkAirport</code>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
| Location Name        | Type a location name for the hotspot, for example:<br><code>ACMEWISP,Gate_14_Terminal_C_of_Newark<br/>_Airport</code>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
| Walled Garden        | <p>Click <b>Create New</b> to add a walled garden, which is a limited environment to which an unauthenticated user is given access for the purpose of setting up an account. In the box provided, type a URL or IP address to which you want to grant unauthenticated user access. You can add up to 128 network destinations to the walled garden. Network destinations can be any of the following:</p> <ul style="list-style-type: none"> <li>• IP address (for example, <code>10.11.12.13</code>)</li> <li>• Exact website address (for example, <code>www.ruckuswireless.com</code>)</li> <li>• Website address with regular expression (for example, <code>*.ruckuswireless.com, *.com, *</code>)</li> </ul> <p>After the account is established, the user is allowed out of the walled garden. URLs will be resolved to IP addresses. Users will not be able to click through to other URLs that may be presented on a page if that page is hosted on a server with a different IP address.</p> <p>Avoid using common URLs that are translated into many IP addresses (such as <code>www.yahoo.com</code>), as users may be redirected to re-authenticate when they navigate through the page.</p> |

## 6 Click **Create New**.

The page refreshes, and then the hotspot that you created appears under the *WISPr (Hotspot) Configuration* section.

Figure 129. The Create New Hotspot Service form

AP Zones

Zone Configuration

AP Group

AAA

WISPr (Hotspot)

Hotspot 2.0

WLAN

Global Configuration

Zone Templates

WLAN Templates

AP Registration Rules

Management Domain + -

Type to find a domain or zone

Administration Domain

test\_zone

AP Zone: test\_zone >> WISPr (Hotspot) Services

WISPr (Hotspot) Services

Search

Name Description M/VNO Account Actions

Create New Hotspot Service

General Options

Name: \*

Description: \*

Type:  Registered Users  Guest Access

Redirection

Smart Client Support:  None  Enable  Only Smart Client Allowed

Logon URL:  Internal  External  Redirect unauthenticated user to the URL for authentication:

Start Page: After user is authenticated.  Redirect to the URL that user intends to visit.  Redirect to the following URL: \*

User Session

Session Timeout: \* 1440 Minutes (1 - 14400)

Grace Period: \* 60 Minutes (1 - 14400)

## Creating a Registration Rule

Registration rules enable the vSZ to assign an AP to an AP zone automatically based on the rule that the AP matches.

Follow these steps to create a registration rule.

- 1 Go to **Configuration > AP Zones**.
- 2 On the sidebar on the left, click **AP Registration Rules**. The *AP Registration Rules* page appears.
- 3 Click **Create New**. A form appears.
- 4 In *Rule Description*, type a name that you want to assign to this rule.
- 5 In *Rule Type*, click the basis upon which you want to create the rule. Options include:
  - *IP Address*: If you select this option, type the *From* (starting) and *To* (ending) IP address that you want to use.
  - *Subnet Mask*: If you select this option, type the IP address and subnet mask pair to use for matching.
  - *GPS Coordinates*: If you select this option, type the GPS coordinates to use for matching. Access points that have been assigned the same GPS coordinates will be automatically assigned to the AP zone that you will choose in the next step.

- **Provision Tag:** If the access points that are joining the vSZ have been configured with provision tags, click the **Provision Tag** option, and then type a tag name in the *Provision Tag* box. Access points with matching tags will be automatically assigned to the AP zone that you will choose in the next step.

**NOTE:** Provision tags can be configured on a per-AP basis from the access point's command line interface.

6 In *Zone Name*, click the drop-down list to display available AP zones, and then click an AP zone to which APs that match this rule will be assigned.

7 Click **OK**.

You have completed creating an AP registration rule.

Figure 130. Creating an AP registration rule

| ID | Rule Type        | Rule Description | Rule Parameters                            | Zone Name   | Created By | Created On          | Actions |
|----|------------------|------------------|--------------------------------------------|-------------|------------|---------------------|---------|
| 1  | IP Address Range | rule-1           | IP From: 5.35.0.2, IP To: 5.35.3.239       | sim-zone-1  | admin      | 2012/10/16 03:49:57 |         |
| 2  | IP Address Range | rule-2           | IP From: 5.35.3.240, IP To: 5.35.7.223     | sim-zone-2  | admin      | 2012/10/16 03:57:35 |         |
| 3  | IP Address Range | rule-3           | IP From: 5.35.7.224, IP To: 5.35.11.207    | sim-zone-3  | admin      | 2012/10/16 04:00:43 |         |
| 4  | IP Address Range | rule-4           | IP From: 5.150.47.64, IP To: 5.150.51.47   | sim-zone-4  | admin      | 2012/10/19 05:03:21 |         |
| 5  | IP Address Range | rule-5           | IP From: 5.23.15.192, IP To: 5.23.19.175   | sim-zone-5  | admin      | 2012/10/16 05:36:19 |         |
| 6  | IP Address Range | rule-6           | IP From: 3.221.21.168, IP To: 3.221.25.151 | sim-zone-6  | admin      | 2012/10/16 06:06:34 |         |
| 7  | IP Address Range | rule-7           | IP From: 3.221.25.152, IP To: 3.221.29.135 | sim-zone-7  | admin      | 2012/10/16 06:06:56 |         |
| 8  | IP Address Range | rule-8           | IP From: 5.25.59.16, IP To: 5.25.62.253    | sim-zone-8  | admin      | 2012/10/25 04:23:45 |         |
| 10 | IP Address Range | rule-10          | IP From: 4.112.39.96, IP To: 4.112.43.79   | sim-zone-10 | admin      | 2012/10/16 09:26:37 |         |

To create another registration rule, repeat the preceding steps. You can create as many registration rules as you need to manage access points on the network.

## Configuring the Rule Priority

The vSZ applies registration rules in the same order as they appear in the AP Registration Rules table (highest to lowest priority). If you want a particular registration rule to have higher priority, you must move it up the table. Once an AP matches a registration rule, the vSZ assigns the AP to the zone specified in the rule and stops processing the remaining rules.

Follow these steps to configure the rule priority.



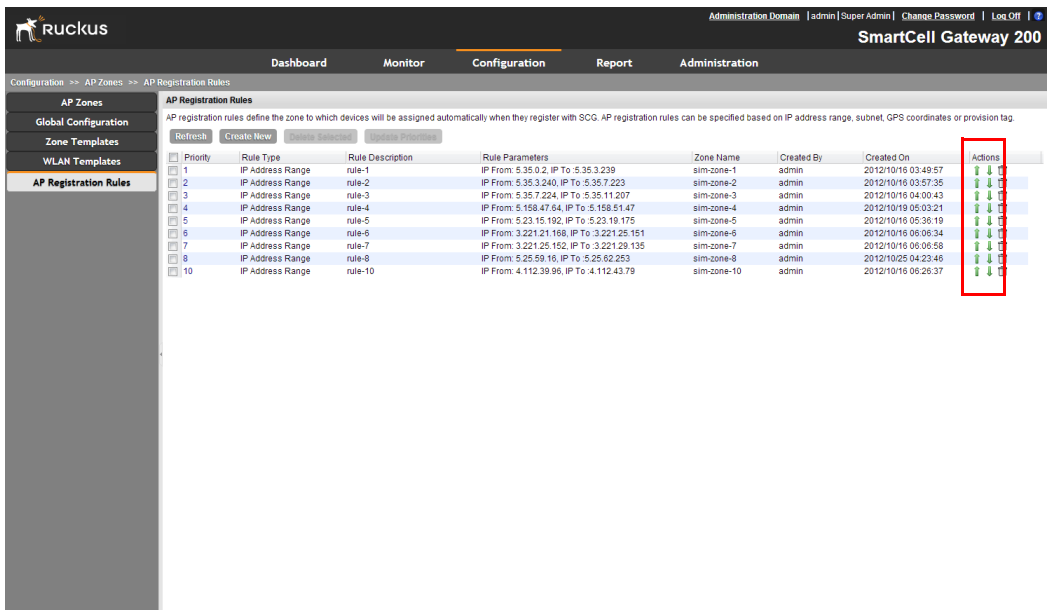
- 1 Go to **Configuration > AP Zones**.
- 2 On the sidebar on the left, click **AP Registration Rules**. The AP Registration Rules page appears and displays the rules that you have created.
- 3 Change the priority of each registration rule as required.
  - To give a rule higher priority, move it up the table by clicking the  (up-arrow) icon that is in the same row as the rule name.
  - To give a rule lower priority, move it down the table by clicking the  (down-arrow) icon that is in the same row as the rule name.
- 4 When you finish configuring the rule priority, click **Update Priorities** to save your changes.

Figure 131. Change the rule priority by clicking the up-arrow or down-arrow



## Defining the WLAN Settings of an AP Zone

Follow these steps to configure the WLAN settings of an AP zone.

- 1 Go to **Configuration > AP Zones**.
- 2 Click the AP zone for which you want to add the WLAN settings. Alternatively, click the AP zone from the *Management Domains* tree.
- 3 Under the *AP Zones* menu on the sidebar, click **WLAN**.
- 4 Click **Create New**. The *Create New WLAN Configuration* form appears.
- 5 Configure the WLAN settings listed in [Table 11](#). You can find a detailed description of each setting in the succeeding sections.

Table 11. Overview of WLAN settings

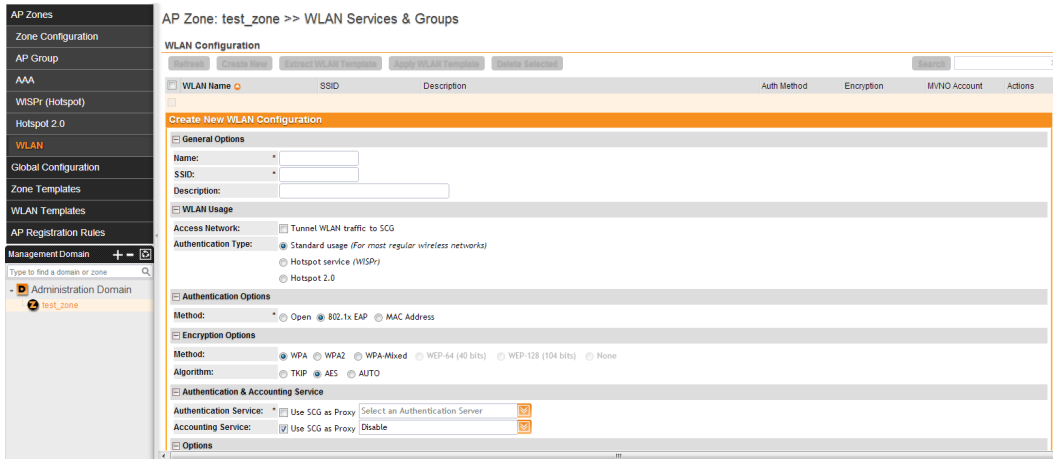
| WLAN Setting                        | Description                                                                                                                                                                                                                                                                                                                                    |
|-------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| General Options                     | Enter the WLAN name and description. See <a href="#">General Options</a> .                                                                                                                                                                                                                                                                     |
| WLAN Usage                          | Select the usage type (standard WLAN or hotspot). See <a href="#">WLAN Usage</a> .                                                                                                                                                                                                                                                             |
| Authentication Options              | Select an authentication method for this WLAN (open or 802.1X EAP). See <a href="#">Authentication Options</a> .                                                                                                                                                                                                                               |
| Encryption Options                  | Select an encryption method (WPA, WPA2, WPA Mixed, and WEP), encryption algorithm (AES or TKIP) and enter a WPA passphrase/WEP key. See <a href="#">Encryption Options</a> .                                                                                                                                                                   |
| Authentication & Accounting Service | This section only appears when certain authentication options are selected. See <a href="#">Authentication &amp; Accounting Service</a> .                                                                                                                                                                                                      |
| Options                             | Select whether web-based authentication (captive portal) will be used, and which type of authentication server will be used to host credentials (local database, Active Directory, RADIUS, LDAP). Also, enable or disable Wireless Client Isolation, Zero-IT Activation, Dynamic PSK and Priority for this WLAN. See <a href="#">Options</a> . |
| Advanced Options                    | Select an accounting server and configure ACLs, rate limiting, VLAN/dynamic VLAN settings, tunneling, background scanning, maximum client threshold, and service schedule. See <a href="#">Advanced Options</a> .                                                                                                                              |



6 Click **OK** to finish creating the WLAN service.

You have completed creating your first WLAN. To create another WLAN, repeat [Step 4](#) to [Step 6](#). You can create up to six WLANs per AP zone.

Figure 132. Configuring the WLAN settings of an AP zone



## General Options

- *Name/ESSID*: Type a short name (2-31 characters) for this WLAN. In general, the WLAN name is the same as the advertised SSID (the name of the wireless network as displayed in the client's wireless configuration program). However, you can also separate the ESSID from the WLAN name by entering a name for the WLAN in the first field, and a broadcast SSID in the second field. In this way, you can advertise the same SSID in multiple locations (controlled by the same vSZ) while still being able to manage the different WLANs independently. Each WLAN "name" must be unique within the vSZ, while the broadcast SSID can be the same for multiple WLANs.
- *Description*: Enter a brief description of the qualifications or purpose of this WLAN (for example, *Engineering* or *Voice*).

## WLAN Usage

- In *Access Network*, select the Tunnel WLAN traffic to vSZ check box if you want to tunnel the traffic from this WLAN back to the vSZ. Tunnel mode enables wireless clients to roam across different APs on different subnets. If the WLAN has clients that require uninterrupted wireless connection (for example, VoIP

devices), Ruckus Wireless recommends enabling tunnel mode. When you enable this option, you need to select core network for tunneling WLAN traffic back to the vSZ.

- In *Authentication Type*, click one of the following options:
  - **Standard usage (For most regular wireless networks):** This is a regular WLAN suitable for most wireless networks.
  - **Hotspot service (WISPr):** Click this option if want to use a hotspot (WISPr) service that you previously created.
  - **Hotspot 2.0:** Click this option if you want to use a Hotspot 2.0 profile that you previously created.
  - **Guest Access:** Click this option if you want to use this WLAN for guest access.

## Authentication Options

Authentication defines the method by which users are authenticated prior to gaining access to the WLAN. The level of security should be determined by the purpose of the WLAN you are creating.

- *Open [Default]:* No authentication mechanism is applied to connections. If WPA or WPA2 encryption is used, this implies WPA-PSK authentication.
- *802.1X/EAP:* Uses 802.1X authentication against a user database.
- *MAC Address:* Uses the MAC address of a client for authentication. MAC address authentication requires a RADIUS server and uses the MAC address as the user logon name and password. You have two options for the MAC address format to use for authenticating clients:
  - Use user defined text as authentication password (default is device MAC address)
  - Set device MAC address in 802.1x format 00-10-A4-23-19-C0. The default is 0010a42319c0.

## Encryption Options

Encryption choices include WPA, WPA2, WPA-Mixed, WEP and none. WPA and WPA2 are both encryption methods certified by the Wi-Fi Alliance and are the recommended encryption methods. The Wi-Fi Alliance will be mandating the removal of WEP due to its security vulnerabilities, and Ruckus Wireless recommends against using WEP if possible.

## Method

- *WPA*: Standard Wi-Fi Protected Access with either TKIP or AES encryption.
- *WPA2*: Enhanced WPA encryption using the stronger AES encryption algorithm.
- *WPA-Mixed*: Allows mixed networks of WPA and WPA2 compliant devices. Use this setting if your network has a mixture of older clients that only support WPA and TKIP, and newer client devices that support WPA2 and AES.
- *WEP-64*: Provides a lower level of encryption, and is less secure, using 40-bit WEP encryption.
- *WEP-128*: Provides a higher level of encryption than WEP-64, using a 104-bit key for WEP encryption. However, WEP is inherently less secure than WPA.
- *None*: No encryption; communications are sent in clear text.

---

**CAUTION!** If you set the encryption method to WEP-64 (40 bit) or WEP-128 (104 bit) and you are using an 802.11n AP for the WLAN, the AP will operate in 802.11g mode.

---

## Algorithm (For WPA or WPA2 Encryption Only)

- *TKIP*: This algorithm provides greater compatibility with older client devices, but retains many of the security weaknesses of WEP. Therefore, if you select TKIP encryption, 11n devices will be limited to 11g transfer rates. Furthermore, the Wi-Fi Alliance will be mandating the removal of TKIP, so it should not be used.
- *AES*: This algorithm provides enhanced security over TKIP, and is the only encryption algorithm supported by the 802.11i standard. Choose AES encryption if you are confident that all of your clients will be using 802.11i-compliant NICs.
- *Auto*: Automatically selects TKIP or AES encryption based on the client's capabilities. Note that since it is possible to have clients using both TKIP and AES on the same WLAN, only unicast traffic is affected (broadcast traffic must fall back to TKIP; therefore, transmit rates of broadcast packets from 11n APs will be at lower 11g rates).

---

**CAUTION!** If you set the encryption algorithm to TKIP and you are using an 802.11n AP for the WLAN, the AP will operate in 802.11g mode.

---

**CAUTION!** If you set the encryption algorithm to TKIP, the AP will only be able to support up to 26 clients. When this limit is reached, additional clients will be unable to associate with the AP. On the other hand, if you select AES or none, the AP will be able to support up to 256 clients (less if wireless mesh is also enabled on the same radio).

---

## WEP Key/Passphrase

- *WEP Key:* WEP methods only. Click the *Hex* field, and then type the required key text. If the key is for WEP 64 encryption, enter ten hexadecimal characters (any combination of 0-9, A-F). If it is for WEP 128 encryption, enter 26 hexadecimal characters (any combination of 0-9, A-F).
- *Passphrase:* WPA-PSK methods only. Click in this field and type the text of the passphrase used for authentication. The passphrase must contain between eight and 63 characters (or 64 hexadecimal characters).

## Authentication & Accounting Service

- *Authentication Service:* This option appears only when 802.1x EAP is selected as the authentication method. Select the authentication server that you want to use for this WLAN. Only AAA servers that you previously added appear here.
- *Accounting Service:* This option appears only when 802.1x EAP is selected in Authentication method. Additionally, you must have added a RADIUS Accounting server previously. Select the RADIUS Accounting server from the drop-down list, as a proxy for vSZ.

## Options

- *Wireless Client Isolation:* This option appears only when Standard Usage is selected as the WLAN usage type. Wireless client isolation enables subnet restrictions for connected clients. Click Enable if you want to prevent wireless clients associated with the same AP from communicating with each other locally. The default value is Disable.
- *Priority:* Set the priority of this WLAN to Low if you would prefer that other WLAN traffic takes priority. For example, if you want to prioritize internal traffic over guest WLAN traffic, you can set the priority in the guest WLAN configuration settings to “Low.” By default, all WLANs are set to high priority.

## RADIUS Options

---

**NOTE:** The *RADIUS Options* section only appears when *Authentication Type* (under *WLAN Usage*) is set to **Standard usage (For most regular wireless networks)**.

---

- *RADIUS NAS ID:* Select how the RADIUS server will identify the AP:
  - WLAN BSSID
  - AP MAC
  - User-defined
- *RADIUS NAS Request Timeout:* Type the timeout period (in seconds) after, which an expected RADIUS response message is considered to have failed.
- *RADIUS NAS Max Number of Retries:* Type the number of failed connection attempts after which the vSZ will fail over to the backup RADIUS server.
- *RADIUS NAS Reconnect Primary:* If the vSZ fails over to the backup RADIUS server, this is the interval (in minutes) at which the vSZ will recheck the primary RADIUS server if it is available. The default interval is 5 minutes.
- *Call STA ID:* Use either WLAN BSSID or AP MAC as the station calling ID. Select one.

## Advanced Options

- *Rate Limiting:* Rate limiting controls fair access to the network. When enabled, the network traffic throughput of each network device (client) is limited to the rate specified in the traffic policy, and that policy can be applied on either the uplink or downlink.

Toggle the Uplink and/or Downlink drop-down lists to limit the rate at which WLAN clients upload/download data. The “Disabled” state means rate limiting is disabled; thus, traffic flows without prescribed limits.
- *Access VLAN:* By default, all wireless clients associated with APs that the vSZ is managing are segmented into a single VLAN (with VLAN ID 1). If you want to tag this WLAN traffic with a different VLAN ID, enter a valid VLAN ID (2-4094) in the box. Select the **Enable Dynamic VLAN** check box to allow the vSZ to assign VLAN IDs on a per-user basis. Before enabling dynamic VLAN, you need to define on the RADIUS server the VLAN IDs that you want to assign to users.
- *Hide SSID:* Click this option if you do not want the ID of this WLAN advertised at any time. This will not affect performance or force the WLAN user to perform any unnecessary tasks.

- *Proxy ARP*: When enabled on a WLAN, the AP provides proxy service for stations when receiving neighbor discovery packets (for example, ARP requests and ICMPv6 Neighbor Solicit messages), and acts on behalf of the station in delivering ARP replies. When the AP receives a broadcast ARP/Neighbor Solicit request for a known host, the AP replies on behalf of the host. If the AP receives a request for an unknown host, it forwards the request at the rate limit specified.
- *Max Clients*: Limit the number of clients that can associate with this WLAN per AP (default is 100). You can also limit the total number of clients that a specific AP (or radio, on dual radio APs) will manage.
- *802.11d*: The 802.11d standard provides specifications for compliance with additional regulatory domains (countries or regions) that were not defined in the original 802.11 standard. Enable this option if you are operating in one of these additional regulatory domains.
- *DHCP Option 82*: When this option is enabled and an AP receives a DHCP request from a wireless client, the AP will encapsulate additional information (such as VLAN ID, AP name, SSID and MAC address) into the DHCP request packets before forwarding them to the DHCP server. The DHCP server can then use this information to allocate an IP address to the client from a particular DHCP pool based on these parameters.
- *Client TX/RX Statistics*: Select the **Ignore statistics from unauthorized clients** check box if you do not want the vSZ to monitor traffic statistics for unauthorized clients.
- *Inactivity Timeout*: Select the check box and enter a value in minutes (6 to 600 minutes) after which idle clients will be disconnected.
- *Client Fingerprinting*: If you select this check box, the vSZ will attempt to identify client devices by their operating system, device type, and host name, if available. This makes identifying client devices easier on the Dashboard, Monitor and Client Details pages.
- *Disable WLAN*: Select this option to disable this WLAN service.

## Configuring DHCP Option 43

To enable the vSZ to manage an AP, the AP must be able to locate the vSZ on the network successfully and register with it. The easiest way to ensure that APs can successfully locate the vSZ on the network is by configuring DHCP Option 43 on your DHCP server.

DHCP Option 43 enables the DHCP server on your network to provide the vSZ server address – either IP address or FQDN– (specifically, the IP address assigned to the vSZ’s control plane or cluster plane interface) to DHCP clients, including APs that are connected to the network.

The procedure for configuring DHCP option 43 varies, depending on the DHCP server that you are using. Refer to the documentation provided with your DHCP server software for information on how to configure DHCP option 43.

---

**NOTE:** The following procedure describes how to configure DHCP option 43 on a Linux server (Fedora). If your DHCP server is running on a different platform, refer to the DHCP server documentation for the relevant instructions.

---

Follow these steps to configure DHCP option 43 on a Linux server.

- 1 Log on to your DHCP server via a console terminal (for example, PuTTY).
- 2 Go to `/etc` directory.
- 3 Run `vi dhcpd.conf`. This command opens the DHCP configuration file for editing.
- 4 At the beginning of the DHCP configuration file, insert the following lines:

```
option space VendorInfo;  
option VendorInfo.WSG code 6 = text;
```

OR

```
option space VendorInfo;  
option VendorInfo.SCG code 6 = text;
```

---

**CAUTION!** Make sure that space characters exist in “6 = text”. Omitting these space characters could result in AP connectivity issues.

---

- 5 Under the subnet section, insert the following lines:

```
Vendor-option-space VendorInfo;
```

```
option VendorInfo.WSG "{control-ip-address-or-fqdn}"
OR
Vendor-option-space VendorInfo;
option VendorInfo.SCG "{control-ip-address-or-fqdn}"
```

---

**NOTE:** {control-ip-address-or-fqdn} must be the IP address or FQDN of the control plane (br0).

---

Remember to remove the curly brackets ({} ) that enclose the IP addresses or FQDNs. If the control plane IP addresses are mapped to proper names on the DNS server, you could also use FQDN host names instead of IP addresses.

The vSZ supports two formats for vendor information:

- Plain IP address or FQDN (for example, 10.2.0.87 or server.company.com)
- URL-based IP address or FQDN (for example, https://10.2.0.87/wsg/ap or https://server.company.com/wsg/ap) where 10.2.0.87 or server.company.com is the IP address or FQDN of the control plane interface, respectively.

### Inserting Multiple IP Addresses or URLs

If you want to insert multiple IP addresses or URLs, use any of the following formats:

- URL format
  - option VendorInfo.WSG "https://10.2.0.87/wsg/ap,https://10.2.0.88/wsg/ap", or
  - option VendorInfo.SCG "https://10.2.0.87/wsg/ap,https://10.2.0.88/wsg/ap"
- IP address format
  - option VendorInfo.WSG "10.2.0.87,10.2.0.88", or
  - option VendorInfo.SCG "10.2.0.87,10.2.0.88"

---

**CAUTION!** Take care not to insert any space characters before or after the comma (,) character that separates the multiple IP addresses or URLs.

---

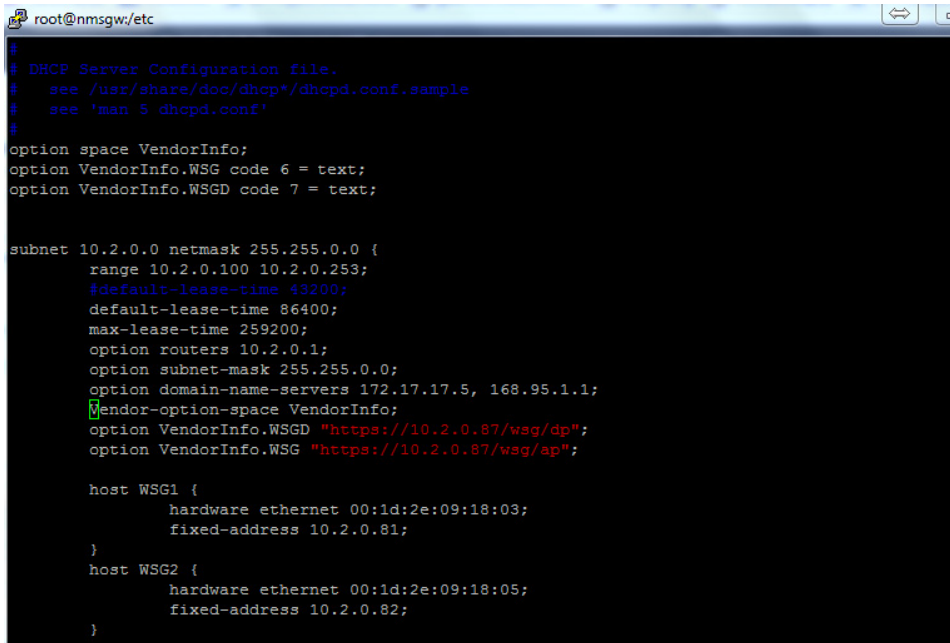
**6** Save the changes.

**7** Restart the DHCP server to apply the new settings.

You have completed configuring DHCP option 43 on a Linux server.



Figure 133. Editing dhcpd.conf



```
root@nmsgw:/etc
#
# DHCP Server Configuration file.
#   see /usr/share/doc/dhcp*/dhcpd.conf.sample
#   see 'man 5 dhcpd.conf'
#
option space VendorInfo;
option VendorInfo.WSG code 6 = text;
option VendorInfo.WSGD code 7 = text;


subnet 10.2.0.0 netmask 255.255.0.0 {
    range 10.2.0.100 10.2.0.253;
    #default-lease-time 43200;
    default-lease-time 86400;
    max-lease-time 259200;
    option routers 10.2.0.1;
    option subnet-mask 255.255.0.0;
    option domain-name-servers 172.17.17.5, 168.95.1.1;
    Vendor-option-space VendorInfo;
    option VendorInfo.WSGD "https://10.2.0.87/wsg/dp";
    option VendorInfo.WSG "https://10.2.0.87/wsg/ap";


    host WSG1 {
        hardware ethernet 00:1d:2e:09:18:03;
        fixed-address 10.2.0.81;
    }
    host WSG2 {
        hardware ethernet 00:1d:2e:09:18:05;
        fixed-address 10.2.0.82;
    }
}
```

## Verifying That Wireless Clients Can Associate with a Managed AP

The last step in the vSZ setup process is to verify that APs can register with the vSZ and that wireless clients can associate with the APs successfully.

Follow these steps to verify that wireless clients can connect to the network.

- 1 Verify that the vSZ is connected to the backbone network.
- 2 Physically connect an AP to the same network as the vSZ. If DHCP option 43 was configured correctly, this AP should be able to locate the vSZ on the network and to register with it successfully.
- 3 Check the vSZ Dashboard. The AP zone that you created earlier should have at least one member AP (the AP that you connected to the network in [Step 2](#)). The AP count appears green, which indicates that it is online.
- 4 Associate a wireless client with the AP. The following describes the procedure if you are using a Windows-based wireless client.
  - a In the system tray, right-click the  (Wireless Network Connection) icon, and then click **View Available Wireless Networks**.
  - b In the list of available wireless network, click the wireless network name (SSID) that you configured on the AP.
  - c Click **Connect**.

Your wireless client connects to the wireless network. After the wireless client connects to the wireless network successfully, the wireless client icon in the system tray changes to .

- 5 Start your web browser, and then enter `www.ruckuswireless.com` in the address bar.

If you are able to connect to the Ruckus Wireless website, you have completed setting up the vSZ on the network. Congratulations!

## What to Do Next

For more information on configuring and managing the vSZ, refer to the *Administrator Guide* for your vSZ platform, which is available for download on the Ruckus Wireless Support website at

<https://support.ruckuswireless.com/documents>

---

**NOTE:** For a complete list of documentation that is available for your vSZ profile configuration, refer to the *Release Notes*.

---

# Ensuring That APs Can Discover the Controller on the Network

## 8

Before the controller can start managing an AP, the AP must first be able to discover the controller on the network when it boots up. This chapter describes procedures that you can perform to ensure that APs can discover and register with the controller on the network.

In this chapter:

- [Is LWAPP2SCG Enabled on the Controller?](#)
- [Method 1: Perform Auto Discovery of the Controller Using the SmartLicense Server](#)
- [Method 2: Perform Auto Discovery on Same Subnet, then Transfer the AP to Intended Subnet](#)
- [Method 3: Register the Controller with the DNS Server](#)
- [Method 4: Configure DHCP Option 43 on the DHCP Server](#)
- [Method 5: Manually Configure the Controller Address on the AP's Web Interface](#)

## Is LWAPP2SCG Enabled on the Controller?

All of the controller discovery methods described in this chapter require LWAPP2SCG (the application that enables APs to discover and be managed by a controller) to be installed and enabled on the controller. See [Table 12](#) to check if your controller release includes the LWAPP2SCG application and whether it is enabled or disabled by default.

Table 12. LWAPP2SCG availability on each controller release

| Controller Release      | LWAPP Discovery                                                                                   | Default Setting | AP Compatibility                                                                                                    |
|-------------------------|---------------------------------------------------------------------------------------------------|-----------------|---------------------------------------------------------------------------------------------------------------------|
| SCG 1.1.2, 2.1.2        | Application installed by administrator. See <a href="#">Obtaining the LWAPP2SCG Application</a> . | Disabled        | <ul style="list-style-type: none"> <li>ZF-AP Release 9.6.x – 9.8.x</li> <li>AP Release 100.0.x and later</li> </ul> |
| SCG 2.5.x               | Enabled by administrator. See <a href="#">Enabling LWAPP2SCG</a> .                                | Disabled        |                                                                                                                     |
| SCG 2.6.x               | Enabled by administrator. See <a href="#">Enabling LWAPP2SCG</a> .                                | Disabled        | <ul style="list-style-type: none"> <li>ZF-AP Release 9.7.x – 9.8.x</li> </ul>                                       |
| Release 3.0.x and later | Enabled by default                                                                                | Enabled         | <ul style="list-style-type: none"> <li>AP Release 100.0.x and later</li> </ul>                                      |

### Obtaining the LWAPP2SCG Application

If your controller release does not have the LWAPP2SCG application pre-installed, contact Ruckus Wireless Support to obtain a copy of the LWAPP2SCG application files and installation instructions.

### Enabling LWAPP2SCG

If the LWAPP2SCG application is pre-installed but disabled in your controller release, do the following to enable it:

- 1 Log on to the controller's console.
- 2 Enter **en** to enable privileged mode.
- 3 Enter **config**.
- 4 Enter **lwapp2scg**.
- 5 Enter **policy accept-all**.

You have completed enabling the LWAPP2SCG application on the controller.

# Method 1: Perform Auto Discovery of the Controller Using the SmartLicense Server

---

**NOTE:** This guide assumes that you have already activated the controller's licenses on the SmartLicense server. If you have not activated the controller's licenses, see the *Virtual SmartZone Quick Setup Guide* for this release for more information.

---

The Ruckus Wireless SmartLicense registration server is a cloud-based, HTTPS-enabled web server that allows an access point to query information about its parent controller by sending its serial number and base MAC address.

After you ensure that the controller's licenses have been activated on the SmartLicense server, you only need to connect the AP to the network, ensure that it has Internet connectivity, and then reboot the AP. Upon reboot, the AP will automatically attempt to discover its parent controller by sending the following HTTPS query to `ap-registrar.ruckuswireless.com` (the SmartLicense server URL):

```
https://ap-registrar.ruckuswireless.com/  
controller?ap_mac=APMAC&ap_serial=APSERIAL
```

Where APMAC is the AP's MAC address (for example, APMAC: 74:91:1A:20:59:90) and APSERIAL (for example, APSERIAL: 311003001685) is the AP's serial number, both of which are printed on the AP's product label.

If the AP is unable to discover its parent controller after the first attempt, it will continue to do so:

- Once every 5 minutes for up to 60 minutes (12 queries)
- Once every hour for the remaining day (23 queries)
- Once every 24-hour for the remaining two weeks (12 queries)

If the AP is still unable to discover its parent controller after two weeks of uptime, this cloud-based controller discovery method will be disabled permanently. You will need to reset the AP to factory default settings to re-enable this controller discovery method.

## Method 2: Perform Auto Discovery on Same Subnet, then Transfer the AP to Intended Subnet

If you are deploying the AP and the controller on different subnets, let the AP perform auto discovery on the same subnet as the controller before moving the AP to another subnet. To do this, connect the AP to the same network as the controller. When the AP starts up, it will discover and attempt to register with the controller. Approve the registration request if auto approval is disabled. After the AP registers with the controller successfully, transfer it to its intended subnet. It will be able to find and communicate with the controller once you reconnect it to the other subnet.

---

**NOTE:** If you use this method, make sure that you do not change the IP address of the controller after the AP discovers and registers with it. If you change the controller's IP address, the AP will no longer be able to communicate with it and will be unable to rediscover it.

---

## Method 3: Register the Controller with the DNS Server

If you register the controller with your DNS server, supported APs that request IP addresses from your DHCP server will also obtain DNS related information that will enable them to discover controllers on the network. Using the DNS information they obtained during the DHCP request, APs will attempt to resolve the controller IP address using `RuckusController.{DNS domain name}` and `zonedirector.{DNS domain name}`.

To register the controller with the DNS server, do the following.

- 1 Open the DNS zone file, and then add two records with the following information:
  - Record Key#1: RuckusController  
Type: A (IPv4 Domain Name Translation)  
Value: (IP address of the controller)
  - Record Key#2: zonedirector  
Type: A (IPv4 Domain Name Translation)  
Value: (IP address of the controller)

Figure 134. Add records for “RuckusController” and “zonedirector” to the DNS zone file

Zone Editor – YaST

## Zone Editor

In this dialog, edit the resource records of the zone. [more](#)

Settings for Zone

Basics NS Records MX Records SOA **Records**

**Record Settings**

Record Key:  Type:  Value:

Configured Resource Records

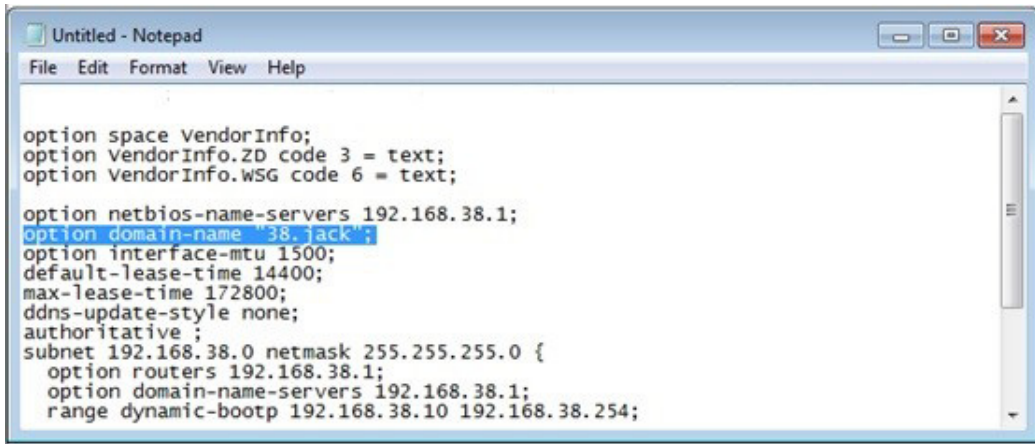
| Record Key       | Type | Value                  |
|------------------|------|------------------------|
| router4          | A    | 172.17.22.90           |
| router2          | A    | 172.17.36.124          |
| router4          | AAAA | 2002:3b7c:e439:9138::1 |
| router2          | AAAA | 2002:3b7c:e439:9132::1 |
| router3          | A    | 172.17.21.37           |
| router3          | AAAA | 2002:3b7c:e439:9135::1 |
| RuckusController | A    | 172.17.36.61           |
| zonedirector     | A    | 172.17.36.61           |

- 2 Save the zone file.
- 3 Open the DHCP configuration file, and then insert the DNS domain name in the DHCP configuration file. For example, if the DNS domain name is “38.jack”, insert the following line into the DHCP configuration file:

**option domain-name “38.jack”**



Figure 135. Insert option domain-name “38.jack”



```
Untitled - Notepad
File Edit Format View Help

option space VendorInfo;
option VendorInfo.ZD code 3 = text;
option VendorInfo.WSG code 6 = text;
option netbios-name-servers 192.168.38.1;
option domain-name 38.jack;
option interface-mtu 1500;
default-lease-time 14400;
max-lease-time 172800;
ddns-update-style none;
authoritative ;
subnet 192.168.38.0 netmask 255.255.255.0 {
  option routers 192.168.38.1;
  option domain-name-servers 192.168.38.1;
  range dynamic-bootp 192.168.38.10 192.168.38.254;
```

#### 4 Save the DHCP configuration file.

When the AP obtains the DNS domain name from the DHCP server (using “Domain Name option 15” in the DHCP-offer packet), it will resolve “RuckusController.{domain-name}” and “zonedirector.{domain-name}” through the DNS server, and then it will obtain the controller’s IP address from the DNS server’s response.

---

**NOTE:** If the AP uses a static IP address or it cannot obtain the DNS domain name from the DHCP server, the AP will attempt to resolve “RuckusController” and “zonedirector” without a domain name from the DNS server as the FQDN of controller’s control interface.

---

You have completed registering the controller with the DNS server.

## Method 4: Configure DHCP Option 43 on the DHCP Server

Another method for the AP to discover the controller on the network automatically is to configure the DHCP server on the network. To do this, you will need to configure DHCP Option 43 (043 Vendor Specific Info) with the IP address of the controller on the network. When an AP requests an IP address from the DHCP server, the DHCP server will send a list of controller IP addresses to the AP. If there are multiple controller devices on the network, the AP will automatically select a controller to register with from this list of IP addresses.

DHCP Option 43 enables the DHCP server on your network to provide the controller's server address – either IP address or FQDN– (specifically, the IP address assigned to the controller's control plane or cluster plane interface) to DHCP clients, including APs that are connected to the network.

The procedure for configuring DHCP option 43 varies, depending on the DHCP server that you are using. Refer to the documentation provided with your DHCP server software for information on how to configure DHCP option 43.

---

**NOTE:** The following procedure describes how to configure DHCP option 43 on a Linux server (Fedora). If your DHCP server is running on a different platform, refer to the DHCP server documentation for the relevant instructions.

---

**CAUTION!** If you have a ZoneDirector controller on the network and you do not want APs to be managed by this ZoneDirector controller, you must disable auto approval on the ZoneDirector web interface. Log on to the ZoneDirector web interface, and then go to *Configure > Access Points > Access Points Policies* page, and then clear the **Approval** check box.

---

Follow these steps to configure DHCP option 43 on a Linux server.

- 1 Log on to your DHCP server via a console terminal (for example, PuTTY).
- 2 Go to `/etc` directory.
- 3 Run `vi dhcpd.conf`. This command opens the DHCP configuration file for editing.

- 4 At the beginning of the DHCP configuration file, insert the following lines:

```
option VendorInfo.WSG_sub6 code 6=text;
option VendorInfo.WSG_sub3 code 3=text;

option VendorInfo.WSG_sub6 "<Controller IP>";
option VendorInfo.WSG_sub3 "<Controller IP>";
```

For example, if you only have one controller on the network and its IP address is 120.0.0.3, then these lines in the DHCP configuration file should look like in [Figure 136 Sample DHCP Option 43 configuration](#).

Figure 136. Sample DHCP Option 43 configuration

```
option space VendorInfo;
option VendorInfo.WSG code 6 = text;
option VendorInfo.ZD code 3 = text;

Vendor-option-space VendorInfo;
option VendorInfo.WSG "120.0.0.3";
```

If you have a two-node controller cluster on the network, use a comma to separate the control interface IP addresses in option VendorInfo.WSG, for example:

```
option VendorInfo.WSG "120.0.0.3,120.0.0.4"
```

where 120.0.0.3 is the control interface IP address of the first controller and 120.0.0.4 is the control interface IP address of the second controller.

- 5 Save the DHCP configuration file.
- 6 Restart the DHCP server to apply the new settings.
- 7 Verify that the LWAPP2SCG application is enabled on the controller. To verify, log on to the controller's CLI, and then enter the following command:

```
show running-config lwapp2scg
```

If LWAPP2SCG is enabled, the value for ACL Policy should show as Accept all.

Figure 137. “Accept all” indicates that LWAPP2SCG is enabled

```
sz30# show running-config lwapp2scg
LWAPP2SCG Configuration
-----
ACL Policy                               : Accept all
Dynamic Data Transmission Port Range    : Not specified
ACL APs                                  :
```

If LWAPP2SCG is disabled, do the following to enable it:

- a Enter **config**.
- b Enter **lwapp2scg**.
- c Enter **policy**.
- d Enter one of the following commands:
  - **accept {MAC**
  - **address}**: Enter this command if you only want specific APs to be managed by the controller. See [Figure 139](#).
  - **accept-all**: Enter this command if you want all APs that discover the controller to be managed by it.

Figure 138. Options that appear after you enter the “policy” command

```
Sol-SZ1 (config) # lwapp2scg
<cr>

Sol-SZ1 (config) # lwapp2scg

Sol-SZ1 (config-lwapp2scg) # policy
accept          Accept by ACL AP List
accept-all     Accept All
deny            Deny by ACL AP List
deny-all       Deny All

Sol-SZ1 (config-lwapp2scg) # █
```

Figure 139. Enter accept {MAC address} if you only want specific APs to be managed by the controller

```
Sol-SZ1(config-lwapp2scg)# policy accept
Sol-SZ1(config-lwapp2scg)# acl-ap
  mac      AP MAC Address
  serial   AP Serial Number
Sol-SZ1(config-lwapp2scg)# acl-ap mac 6C:AA:B3:3D:66:90
Sol-SZ1(config-lwapp2scg)# acl-ap serial
<SerialNumber>   AP Serial Number(s). Please separate with comma e.g 123456789012,987654321021
Sol-SZ1(config-lwapp2scg)# acl-ap serial █
```

- 8 Reset the AP to factory default settings, and then connect it to a network subnet where it can communicate with the controller.
- 9 Reboot the AP.

After the AP reboots, it will obtain an IP address and the IP address of its parent controller from the DHCP server. Once the AP registers with the controller, it will download and install the latest SmartZone AP firmware.

You have completed

## Method 5: Manually Configure the Controller Address on the AP's Web Interface

- 1 Log on to the AP's web interface.
- 2 Go to the Administration > Management page.
- 3 In *Primary Controller Address*, type the IP address of the controller that you want to manage the AP.
- 4 In *Secondary Controller Address*, type the IP address of a backup controller that you want to manage the AP if the primary controller is unavailable.
- 5 Click **Apply**.

You have completed manually configuring the controller's IP address on the AP's web interface.

Figure 140. Set the IP addresses of the primary and secondary controllers that you want to manage the AP

**Ruckus T300E Multimedia Hotzone Wireless AP**

**Administration :: Management**

**Status**  
 Device  
 Internet  
 Local Subnets  
 Radio 2.4G  
 Radio 5G

**Configuration**  
 Device  
 Internet  
 Local Subnets  
 Radio 2.4G  
 Radio 5G  
 Ethernet Ports  
 Hotspot

**Maintenance**  
 Upgrade  
 Reboot / Reset  
 Support Info

**Administration**  
 Management  
 Diagnostics  
 Log

**Network Profile:** 4bss

**Telnet Access?**  Enabled  Disabled

**Telnet Port:** 23

**SSH Access?**  Enabled  Disabled

**SSH Port:** 22

**HTTP Access?**  Enabled  Disabled

**HTTP Port:** 80

**HTTPS Access?**  Enabled  Disabled

**HTTPS Port:** 443

**Certificate Verification:** PASSED

**Controller Discovery Agent (LWAPP)?**  Enabled  Disabled

**Cloud Discovery Agent (FQDN)**  Enabled  Disabled

**Set Controller Address**  Enabled  Disabled

**Primary Controller Addr:**

**Secondary Controller Addr:**

**TR069 / SNMP Management Choice**

Auto (SNMP and TR069 will work together.)

SNMP only

FlexMaster only

None

**DHCP Discovery:**

**Ruckus WIRELESS** **Ruckus T300E Multimedia Hotzone Wireless AP**

## What to Do Next

For more information on configuring and managing the controller, refer to the *Virtual SmartZone Administrator Guide* for this release, which is available for download on the Ruckus Wireless Support website at <http://support.ruckuswireless.com>.

**NOTE:** For a complete list of documentation that is available for this vSZ release, refer to the *Release Notes*.

# Index

## Numerics

802.11d 142

## A

AAA server 128  
ACLs 136  
AES 139  
AP zone 124, 136  
authentication options 138

## B

background scanning 126  
backup RADIUS 128

## C

client fingerprinting 142  
cluster name 115  
cluster setting 115  
controller name 115, 116  
country code 125  
creating a new cluster 115

## D

description file 9  
DHCP Option 43 143  
DHCP Option 82 142  
DHCP server 143  
disable WLAN 142  
Dynamic VLAN 141

## E

encryption algorithm 139  
encryption options 138  
ESSID 137  
ESXi 9

## F

firmware version 117

## G

gateway 10  
GCE  
    configuring firewalls 84  
    configuring networks 84  
    creating vSZ image 83  
    storage bucket 79  
    uploading vSZ image 81  
    virtual machines 83, 88

## H

hide SSID 141  
hotspot 128  
hotspot service 130  
Hyper-V 9  
hypervisors 9

## I

inactivity timeout 142  
interface settings 10  
IP address 10

## J

joining a cluster 115

## K

KVM 9

## L

logging on 121

## M

management interface 121  
manifest file 9  
max clients 142  
mesh settings 125  
Microsoft Azure 52  
    configuring ports 67  
    creating vSZ image 58

- endpoint 67
- static IP address 70
- static public IP address 74
- storage account 54
- storage container 55
- uploading vSZ image 56
- virtual machines 62
- virtual network 59

## N

- netmask 10
- NTP server 115

## O

- OVA 10

## P

- passphrase 140
- primary DNS server 10
- proxy ARP 142

## R

- RADIUS 128
- RADIUS Accounting 128
- rate limiting 141
- recommended system resources 11
- registration rule 133
  - priority 135
- rule priority 135

## S

- setup wizard 103
- software version 117
- SSID
  - hiding 141
- staging zone 124

## T

- TKIP 139

## V

- virtual machine
  - recommended system resources 11
- virtual machine state file 9



- VLAN 141
- VMWare 9
- vSphere client 13
- vSZ
  - required disk space 13

## W

- Web interface 121
- WEP key 140
- WEP-128 139
- WEP-64 139
- WLAN
  - disabling 142
- WLAN name 137
- WLAN settings 136
- WLAN usage 137
- WPA 139
- WPA2 139
- WPA-Mixed 139



Copyright © 2006-2015. Ruckus Wireless, Inc.  
350 West Java Dr. Sunnyvale, CA 94089. USA  
[www.ruckuswireless.com](http://www.ruckuswireless.com)