Ruckus Wireless™ vSPoT™ Release 3.4.1

Installation Guide

Part Number: 800-71474-001 Rev A
Published: 01 March 2017

www.ruckuswireless.com

Contents

4 Configuring Virtual SPoT Application

5 Managing Virtual SPoT Application

Copyright Notice and Proprietary Information

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, the bark logo, BeamFlex, ChannelFly, Dynamic PSK, FlexMaster, Simply Better Wireless, SmartCell, SmartMesh, SmartZone, Unleashed, ZoneDirector and ZoneFlex 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.

About This Guide

This Installation Guide provides instructions for installing, setup and administration of the Ruckus Wireless™ virtual SmartPositioning Technology (SPoT™) application.

This guide is intended for use by those responsible for managing Ruckus Wireless network equipment. Consequently, it assumes a basic working knowledge of local area networking, wireless networking, and wireless devices.

NOTE Refer to the release notes shipped with your product to be aware of certain challenges when upgrading to this release.

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

Document Conventions

Table 1: Text conventions on page 5 and Table 2: Notice conventions on page 6 list the text and notice conventions that are used throughout this guide.

Table 1: Text conventions

Convention	Description	Example
`message phrase`	Represents messages displayed in response to a command or a status	`[Device Name] >`
`user input`	Represents information that you enter	`[Device Name] > set ipaddr 10.0.0.12`
user interface controls	Keyboard keys, software buttons, and field names	Click **Create New**
Start > **All Programs**	Represents a series of commands, or menus and submenus	Select **Start** > **All Programs**
ctrl+**V**	Represents keyboard keys pressed in combination	Press **ctrl**+**V** to paste the text from the clipboard.
screen or page names		Click **Advanced Settings**. The **Advanced Settings** page appears.
`command name`	Represents CLI commands	
parameter name	Represents a parameter in a CLI command or UI feature	

Convention	Description	Example
variable name	Represents variable data	*{ZoneDirectorID}*
`filepath`	Represents file names or URI strings	`http://ruckuswireless.com`

Table 2: Notice conventions

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

Online Training Resources

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

Related Documentation

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

In addition to this Installation Guide, the SmartPositioning documentation set includes the following:

- **Release Notes**: Provide information about the current software release, including new features, enhancements, and known issues.
- **SPoT User Guide**: Provides information on administration, maintenance and troubleshooting of a SPoT venue. In general, configuration and administration of vSPoT is the same as for cloud-based SPoT. Where differences exist, they are described within this vSPoT Installation Guide. The SPoT User Guide provides additional information not included in the vSPoT Installation Guide.

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

When contacting us, please include the following information:

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

For example:

- vSPoT Release 3.3 Installation Guide
- Part number: 800-71443-001 Revision A
- Page 52

Before You Begin 1

Ruckus Wireless Virtual SmartPositioning Technology (vSPoT) provides an option for deploying a virtual instance of the SPoT server on the users chosen data center. This includes on premise data centers or in AWS (Amazon Web Services)

For more comprehensive information on SPoT administration, maintenance and troubleshooting, refer to the SPoT User Guide, available from support.ruckuswireless.com.

This chapter is a prerequisite for Installing Virtual SPoT on VMware or Installing Virtual SPoT in AWS.

Differences Between SPoT and vSPoT

This section explains the differences between SPoT and vSPoT.

- Installation on the user's chosen data center including on premise data center or on AWS
- Administration pages include additional Diagnostics and Network Settings pages, on which you can view hardware utilization and traffic statistics, as well as configure NTP servers.
- A single vSPoT instance can support multiple venues. Ruckus Wireless recommend up to 500 Access Points (APs) in a single virtual machine even though a maximum of 1,000 APs is possible. This is to optimize the management of vSPoT and as a safeguard to minimize disruption of location services in multiple venues when technical issues arise.

System Specifications

This section explains the system specifications required for a vSPoT installation.

Please ensure that your vSPoT installation platform meets the following minimum hardware and software specifications.

Server Requirements

vSPoT server requirements are affected by the number of tracked devices, and to a certain extent, the number of Access Points (APs).

There is a positive correlation between the number of APs and the number of tracked devices, although there may not always be a direct relation.

Ruckus Wireless recommends up to 500 APs in a single virtual machine though a maximum of 1,000 APs is possible. This is to optimize the management of vSPoT and as a safeguard to minimize disruption of location services in multiple venues if and when technical issues arise.

The actual usage depends heavily on the number of clients detected within the venue. For historical data storage, provision of at least 250kB per 1,000 clients per day is required.

The table lists the server requirements. Intel® Xeon® Processor E5-2690 v2 (25M Cache, 3.00 GHz) is the base for establishing this dimensioning table. A single socket of this processor equals 10 cores.

Table 3: Minimum Server Requirements

Daily unique visitors	Expected maximum real time WiFi unique client load on the system (per minute)	Expected maximum real time location calculations (per minute)	SPoT point CPU and RAM (minimum requirement of 3 APs)	SPoT presence vCPU and RAM (minimum requirement of 1 AP)
1000	100	1000	2 vCPU , 4 GB	1 vCPU, 2 GB
5000	500	5000	4 vCPU , 8 GB	2 vCPU, 4 GB
10000	1000	10000	8 vCPU , 12 GB	4 vCPU, 6 GB
20000	2000	20000	8 vCPU , 16 GB	8 vCPU, 8 GB
30000	3000	30000	12 vCPU , 24 GB	8 vCPU, 16 GB
40000	4000	40000	16 vCPU , 32 GB	12 vCPU, 24 GB
50000	5000	50000	20 vCPU , 40 GB	16 vCPU, 32 GB

NOTE The thumb rule for the number of APs, is one (1) AP per 100 daily unique visitors. In terms of data aggregation, the resource requirements for the SPoT dashboard shown in the above table is based on 1 year's data..

NOTE Ruckus Wireless does not recommend using a 2 vCPU, 4GB RAM setup (or lower) for a production system. Minimum server requirement recommended for production is 4 vCPU with 8 GB RAM..

NOTE Ruckus Wireless recommends CPU family of Intel® Xeon® Processor E5-2690 v2 (25M Cache, 3.00 GHz) for optimum performance.

Virtualization Software

- VMware based installation using VMware ESXi 5.5 and later
- AWS based installation using Amazon Cloud account

NOTE Refer to Installing Virtual SPoT on VMware and Installing Virtual SPoT in AWS for installation procedures.

Network Considerations

This section describes the network considerations required for a vSPoT installation.

The following network topology factors should be taken into consideration when deploying vSPoT in your network along with your ZoneDirector or SmartZone controllers and access points.

Firewall Ports

All traffic flows are initiated from IN (behind firewall) to OUT (Internet) direction.

Typically, such flows do not require rules to be added to the firewall explicitly. However, it is always a good idea to have these firewall rules handy in case of any network connectivity issues. If you must input a “destination” name in a firewall rule instead of “any,” use the same FQDN (Fully Qualified Domain Name) name that you configured on the controller’s Location Services configuration page. The table below lists the firewall ports that must be open for AP/Controller/SPoT communication.

Table 4: Firewall ports

From	To	Port #
Controller	SPoT cloud engine	TCP 8883
AP	SPoT cloud engine	TCP 8883
AP	Controller	TCP 1883

Tips for Remote Controller Deployment

The following are tips for remote controller deployment.

In a typical remote deployment, the APs are deployed at a remote site and managed by a controller (SmartZone or ZoneDirector) back in the data center, and vSPoT is installed within the same data center (or VLAN).

One issue arises because both APs and SZ/ZD need to connect to the vSPoT instance, and not the other way around.

So when you need to specify the IP address of the vSPoT VM on the SmartZone or ZoneDirector Location Services configuration page you can only specify a single IP that needs to be addressable by both SZ/ZD and the APs.

For example, you configure the SZ/ZD location services settings with the vSPoT private IP address, thus SZ/ZD and vSPoT will be able to communicate directly on the local

LAN with their private IP address. However, as APs have to communicate through the public internet they will not be able to connect to vSPoT as the private address will not be routable.

On the other hand, if you set up a NAT server on your data center gateway (to let APs reach vSPoT) and specify its public IP in the SZ/ZD Location Services page, the SZ/ZD must be able to connect to the vSPoT via this public address even though they could have communicated directly.

Solutions

Solution 1

- Specify the vSPoT address with a FQDN on the SZ/ZD Location Services configuration page.
- Set up the DNS server to resolve the FQDN with the private IP address for the SZ/ZD, and with the public IP address for the APs. You may need to have two DNS addresses, once for each network.

Solution 2

- Assign a public IP to vSPoT.
- Key in the public IP of vSPoT on the SZ/ZD Location Services configuration page.
- For the SZ/ZD-vSPoT communications, the firewall can be set to redirect the public IP of vSPoT back to a private IP. And this will settle the SZ – vSPoT link.
- From AP – vSPoT, it will just use the public IP as usual.
- If there are not enough static public IP addresses, assign a port number to vSPoT on an existing public IP. Then the NAT in the firewall should be able to direct traffic to the vSPoT via the assigned port number.

Installing Virtual SPoT on VMware 2

This section describes how you can install virtual SPoT on VMware.

Virtual Machine Installation

The following instructions are on installing the virtual SPoT application as a virtual machine using VMWare ESXi 5.5 and above.

Virtual Machine Download

The Ruckus Wireless support site, https://support.ruckuswireless.com hosts the latest vSPoT software for download. The software has a free trial of 90 days with a temporary AP Capacity licenses. Users who purchase vSPoT will be able to activate their licenses by following the instructions in the section for Licensing Information.

VMware ESXi Installation

To configure the virtual server on VMware ESXi, use the following procedure:

1. Ensure VMware ESXi is running on a suitable host with proper network configuration.
2. Download the vSPoT image. Configure the VM as required for the specific setup on site (e.g., Memory and CPU settings). Refer to the Server Requirements on page 8 table for details.
3. From the VMware interface click the **Start** button to startup the Guest OS that you have just imported to kickstart vSPoT.
4. Allow vSPoT approximately 5 to 10 minutes to complete boot-up and initialization.

Accessing vSPoT Using CLI

Certain technical operations require you to log into the vSPoT through the shell console using the VMware client. Follow the steps to login using CLI.

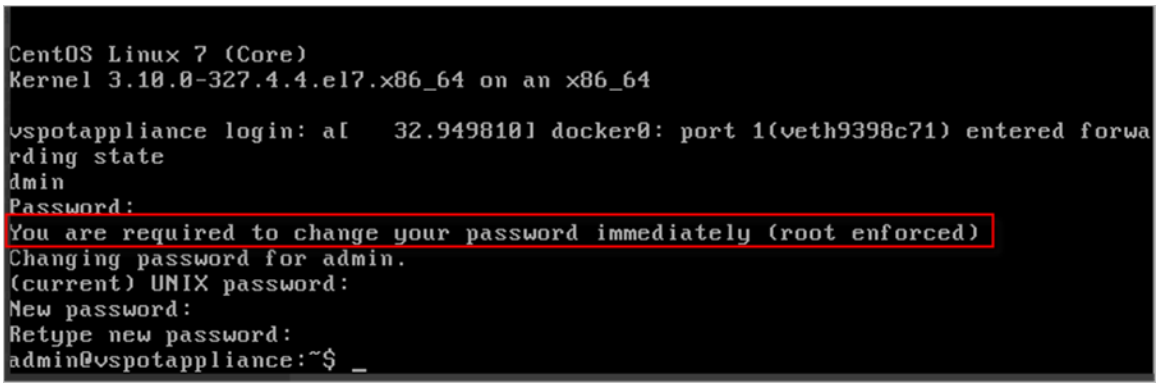
1. Login using the default credentials:

   user name: admin

   password: admin

2. Change the password as the system enforces a change on the first login. See the figure below.

   Figure 1: Login Screen



Setup Static IP Address

This section describes how you set up a static IP address.

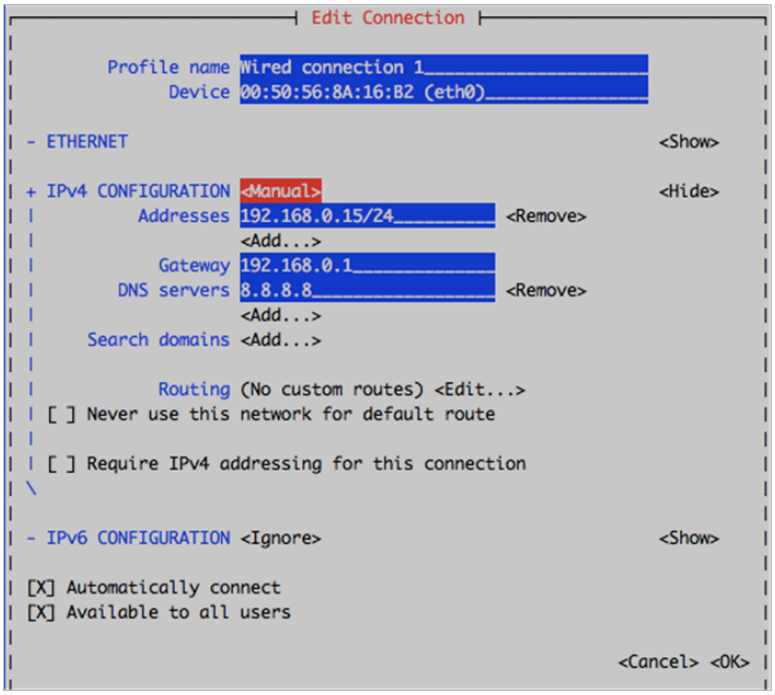
By default vSPoT is configured to use DHCP based dynamic network configuration. In case you do not have a DHCP server on your network segment or you prefer setting a static IP configuration follow these steps.

1. Login to the server through the system console as described in the above section Accessing vSPoT Using CLI on page 13.
2. Run the following command with the specified IP address.

```
admin@vspotappliance:~$ sudo nmtui edit 'Wired connection
1'
```

a. Specify the IPv4 address required as seen in the figure below.

Figure 2: Specifying IP address



b. Save the configuration settings by clicking **OK**.

3. Run the command

```
admin@vspotappliance:~$ sudo ifdown eth0;sudo ifup eth0
```

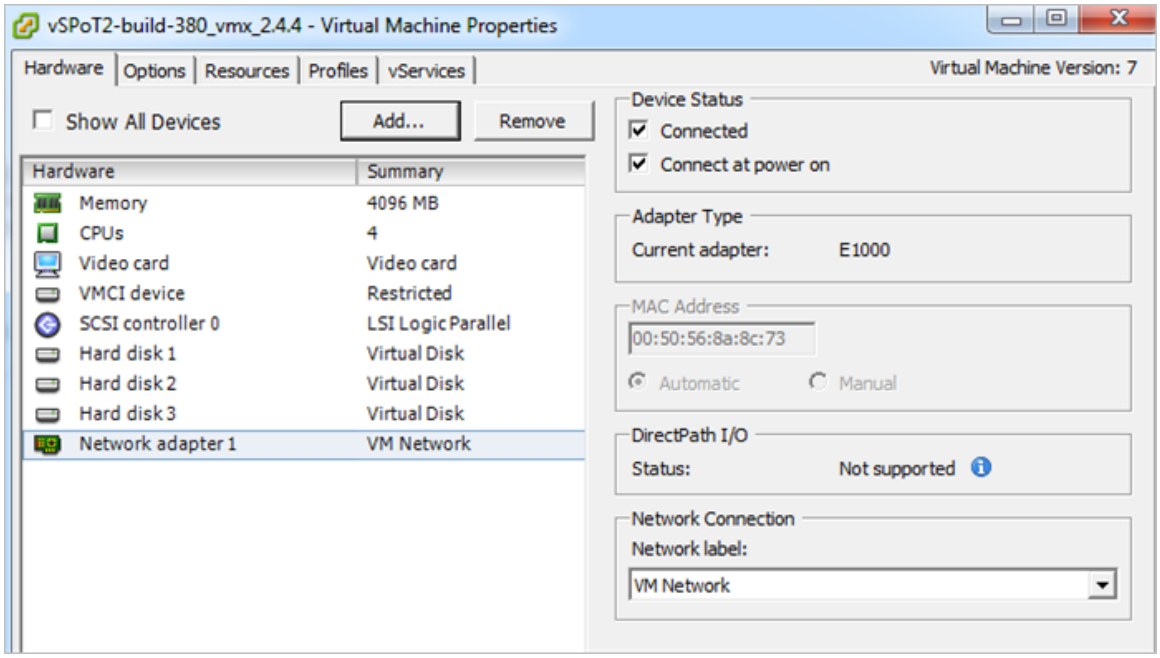
Adding a Second Interface

This section explains how you can add a second interface using VMware ESXi client.

Follow the steps below to add a second interface using VMware ESXi client.

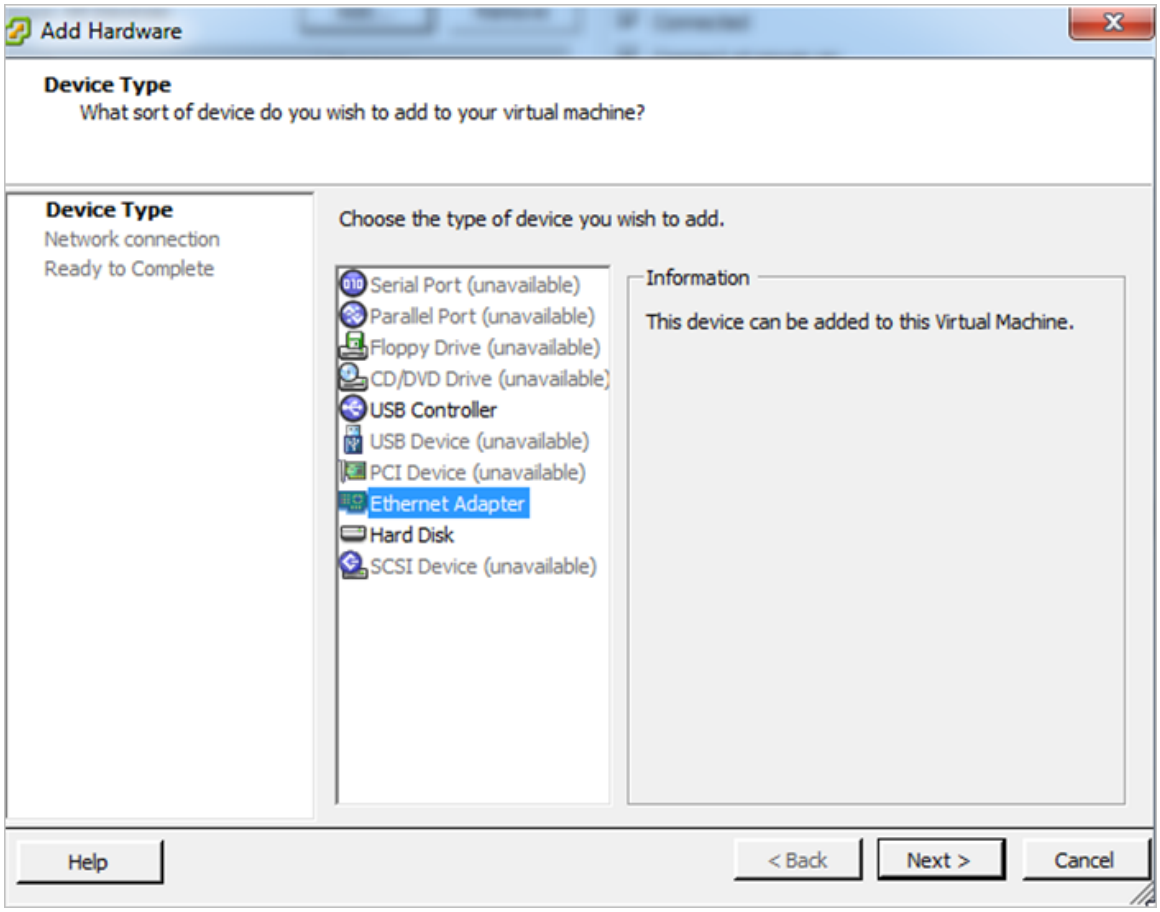
1. Add the network interface to the vSPoT VM in the VMware ESXi client. Locate the VM and edit the VM settings as seen in the figure below.

Figure 3: VMware Edit Page



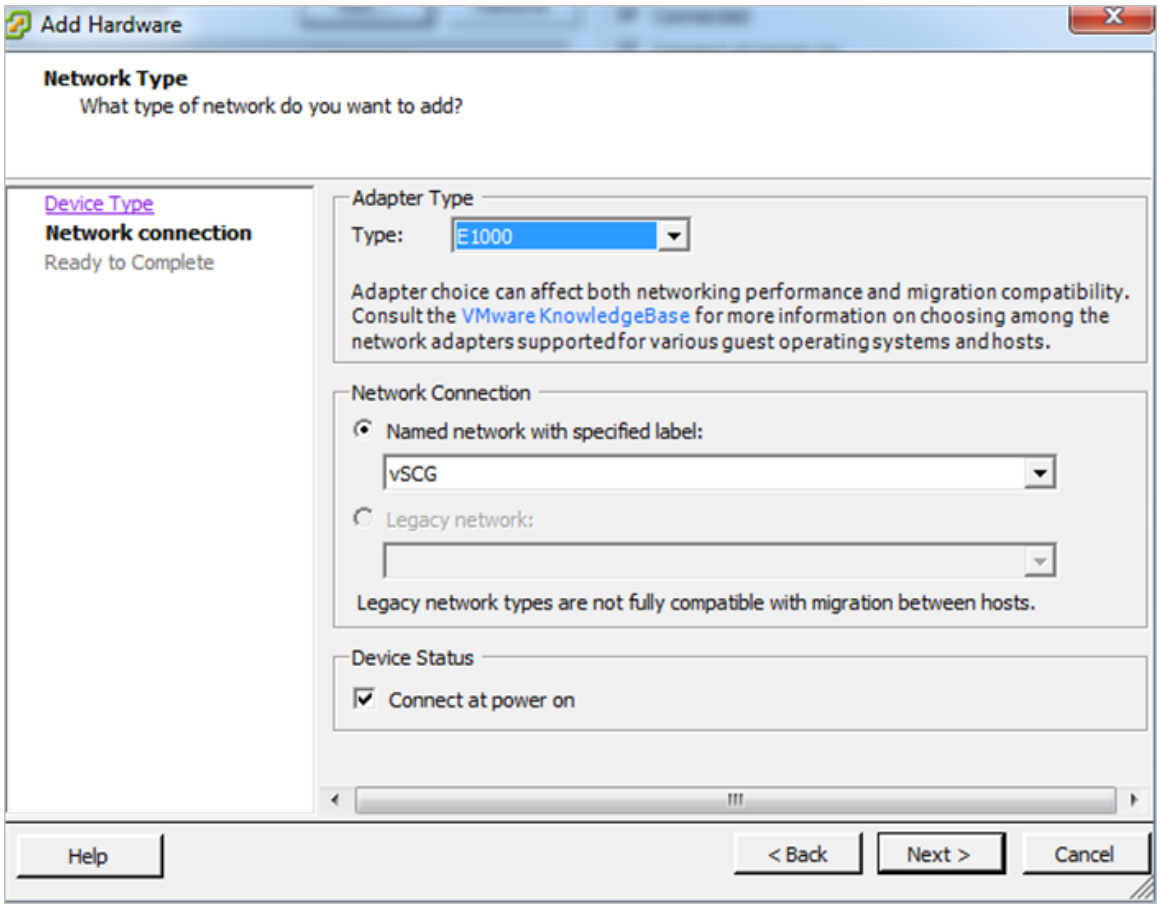
2. Click **Add**.
3. Add the device type as Ethernet adapter as seen in the figure below.

Figure 4: Select the Ethernet adapter



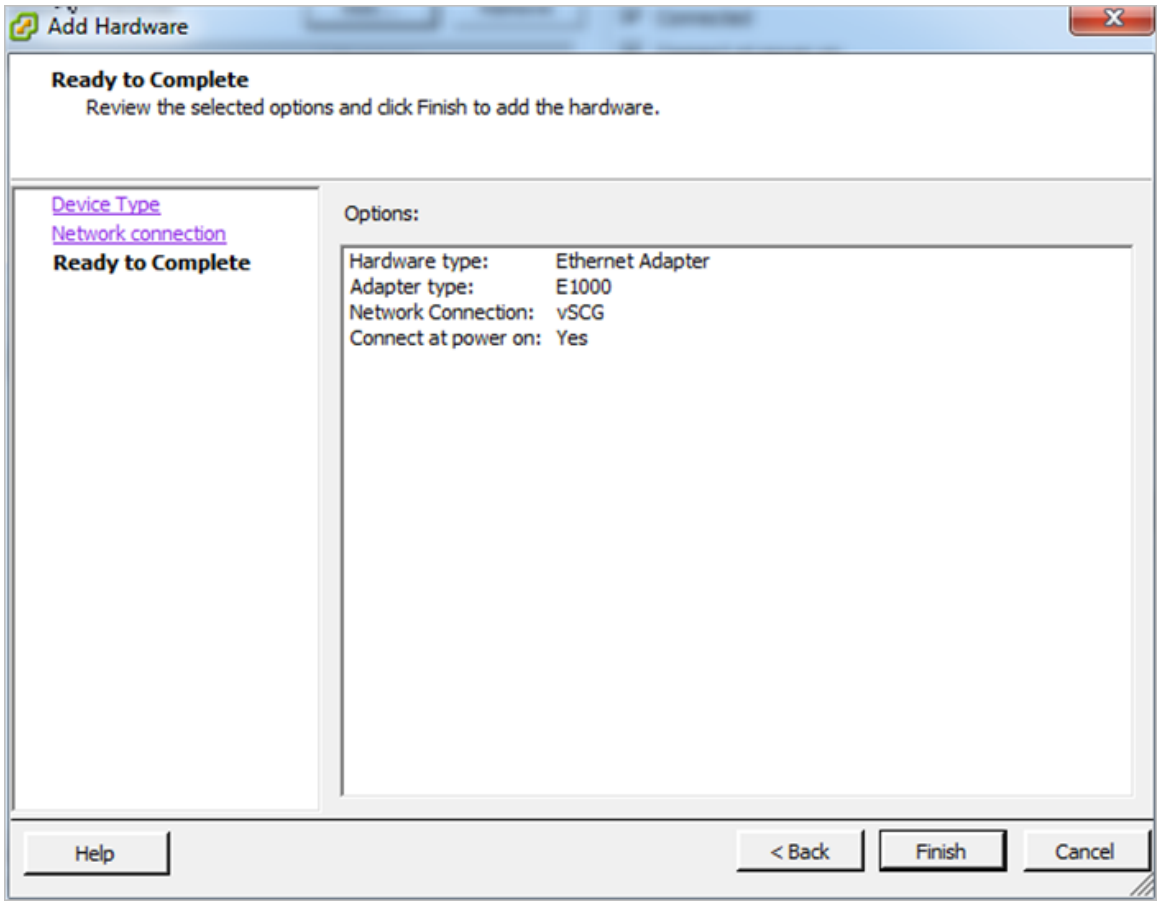
4. Click **Next**.
5. Select the network for the second interface as seen in the figure below.

Figure 5: Adding the network interface



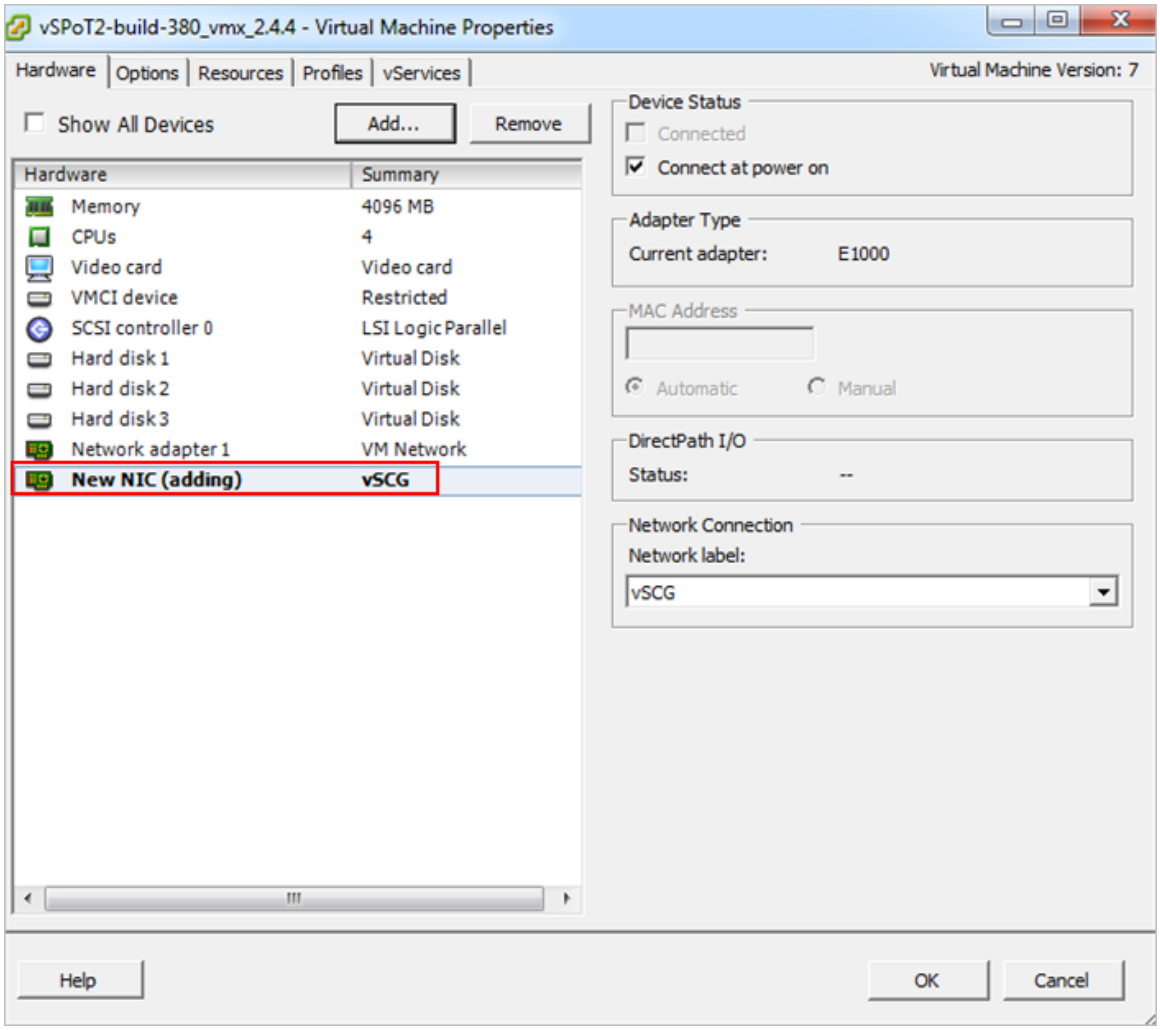
6. Click **Next**.
7. Review the selected options.

Figure 6: Reviewing the configuration settings



8. Click **Finish** to add the second interface.
9. View the second interface as seen in the figure below.

Figure 7: View the second interface



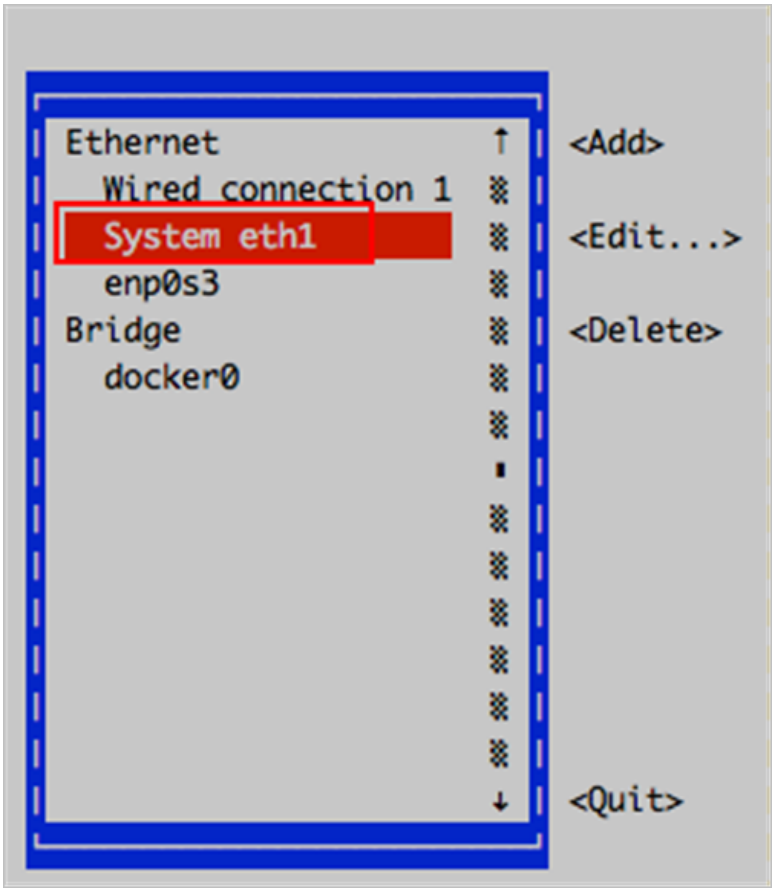
Edit the Second Interface

Follow the below steps to edit the second interface.

1. Boot-up vSPoT VM if it is not running
2. Login to the CLI console (Refer to Accessing vSPoT Using CLI on page 13).
3. Execute the following CLI command to view and edit the second interface. In this example - System eth1 is the second interface as seen in the figure below.

```
admin@vspotappliance:~$ sudo nmtui edit
```

Figure 8: Viewing and editing the second interface



4. Ensure the interface is enabled by executing the following CLI command.

```
admin@vspotappliance:~$ sudo ifup eth1
```

Checklist

Checklist to ensure that the second interface is added successfully.

1. Did you use the shell console to login to the vSPoT instance?
2. Are you able to view the second Ethernet interface? If no, are you able to see the interface by running the CLI command `ifconfig`?

NOTE *Docker0* and *veth** interfaces are used by vSPoT architecture. They are not external interfaces.

---

3. Are you successful in setting the IP address configuration? Are you able to view the setting when using the CLI command `ifconfig`?

Enabling SSH Access

The options in this section help you enable remote SSH access on logging to the vSPoT CLI console.

- SSH key based authentication
- Enabling password based authentication

SSH Key Based Authentication

This is a preferred and secure option. Execute the following CLI commands for enabling SSH access.

1. After logging in to vSPoT CLI, create the SSH directory in the administrator's home directory.

```
admin@vspotappliance:~$ mkdir -p ~/.ssh
```

2. Obtain the SSH public key for your local machine. If you do not have a SSH public key, generate it by following Step 1 of the below reference.

```
https://www.centos.org/docs/5/html/5.2/Deployment_Guide/s3-openssh-rsa-keys-v2.html
```

3. Add your local machine's SSH public key to your vSPoT instance's SSH *authorized_keys* file. This can be done in either of the following two ways:

   Example 1: Copy your local machine's SSH public key into the vSPoT instance

```
admin@vspotappliance:~$ echo 'ssh-rsa
AAAAB3NzaC1yc2EAAAADAQABAAABAQCjfXGGdeNsqTPPWdI6Iext/
DhZ5GrewC6yh6HZAYjlgDamdZebbAvzIwWvWJjxsOGHkhdF5eY9qGlKdZih
WVOTaM1oKrUSshAEEPQnYUBa/nF3J3q4nIX4rOiKsBrT44/
sYKbt+TKgeQ9x5RfwqjqlxCQeq4UbV8K2xfojLCjF6if8jRXYoyUNIf4t0S
mRzGkEtQ8UqnYDmOGlgu4N+kewcT1laz3ty0YfMK1HToN1+
RXL256ZDoLT8w0TAo5h/lpiLthgr8t8+UYHSeejEuoR+
zC2E+37Dr8JVbeTzXAT5zRZhxE7uLkjPCj8HKLekHqyG2225lrdKr
dWeYmrK/Xp joe' >> ~/.ssh/authorized_keys
```

   Example 2: From your vSPoT instance, download your SSH public key from a publicly accessible URL

```
admin@vspotappliance:~$
curl ${SSH_KEY_PUBLIC_URL} >> ~/.ssh/authorized_keys

Example: SSH_KEY_PUBLIC_URL
https://raw.githubusercontent.com/mitchellh/vagrant/master/keys/vagrant.pub
```

Enabling Password Based Authentication

This is a less secure option. Execute the following CLI commands for enabling SSH access.

```
admin@vspotappliance:~$ sudo sed
-i's/^PasswordAuthentication.*/PasswordAuthentication yes/'
/etc/ssh/sshd_config

admin@vspotappliance:~$ sudo service sshd restart

Redirecting to /bin/systemctl restart sshd.service

admin@vspotappliance:~$
```

vSPoT on AWS 3

There are two options to install vSPoT on AWS:

1. Automated Setup using CloudFormation on page 25
2. Automated Setup using AWS CLI on page 33

System Requirements

The following table lists the system requirements recommended for running an instance of vSPoT.

Table 5: System Requirements

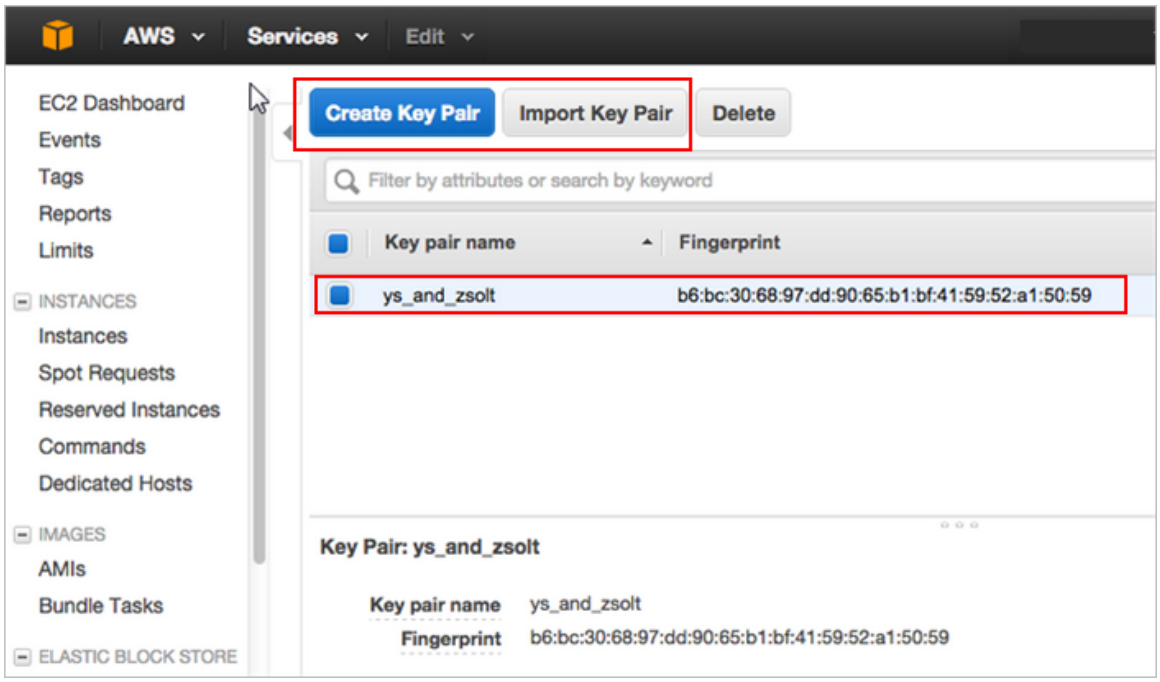
Component	Requirement
System Volume	• System volume comes from the AMI and contains the host operating system and an initial version of the vSPoT application bundle. • The size depends on the maximum number of vSPoT application bundle version you desire to store any given time. The minimum size is 20GB.
Storage Volume	• Specify if you want to use the existing or want to create a new data volume. This needs to automatically mount to / or stored during the instance boot process. • Minimum size is 20Gb, but Ruckus Wireless recommends a size of 100GB. The actual size depends on the AP traffic and the length of the historical data.
EC2 Instance	• The minimum instance size is t2.medium. vSPoT supports only HVM based instances, which has at least 4Gb of system memory.

Preparing to Install vSPoT in AWS

This section contains a general configuration before you install vSPoT in AWS.

1. Ensure you have a SSH public key defined for the region. If the list is empty create a new one or import your desired key. Refer to http://docs.aws.amazon.com/AWSEC2/latest/UserGuide/ec2-key-pairs.html

Figure 9: Inserting a SSH Key

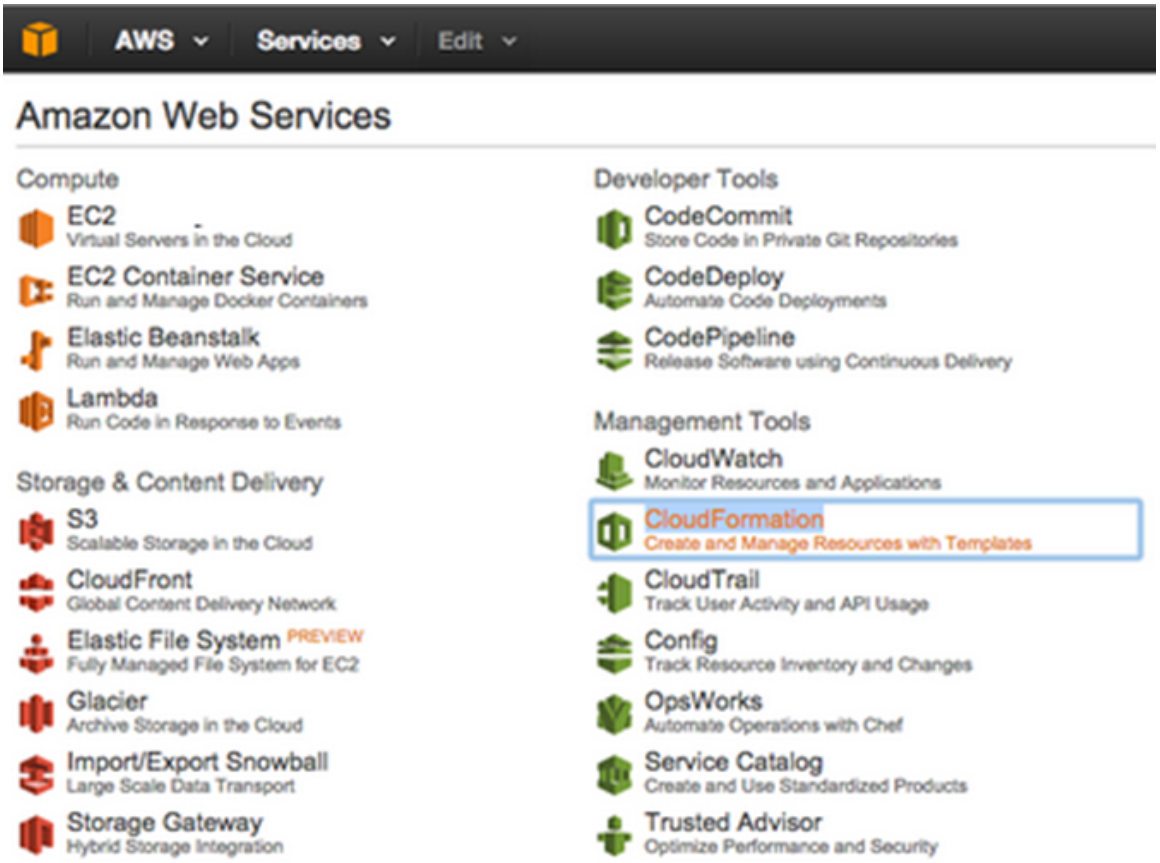


Automated Setup using CloudFormation

Follow the steps to install vSPoT using the AWS web user interface.

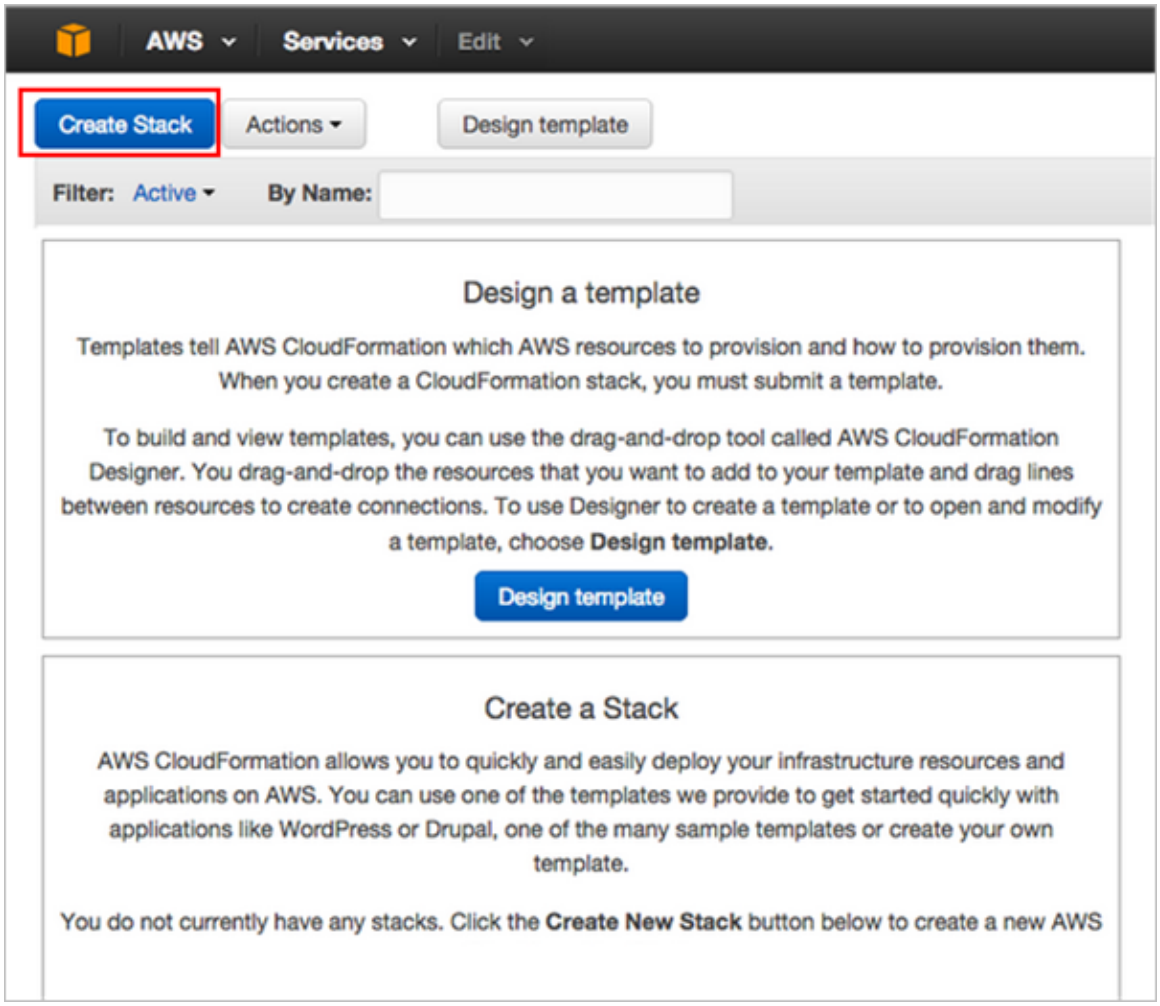
1. Log in to your AWS web console. Navigate to **AWS Services > Management Tools > CloudFormation** to create and manage vSPoT.

   Figure 10: Select Cloud Formation and Region



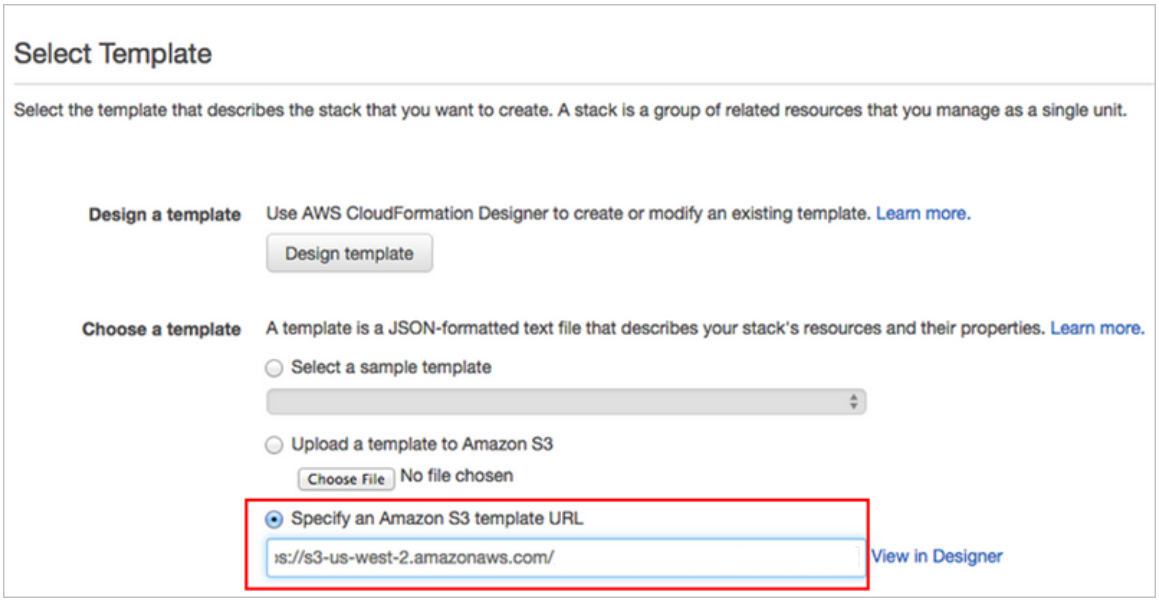
2. Click **Create New Stack**.

Figure 11: Create New Stack



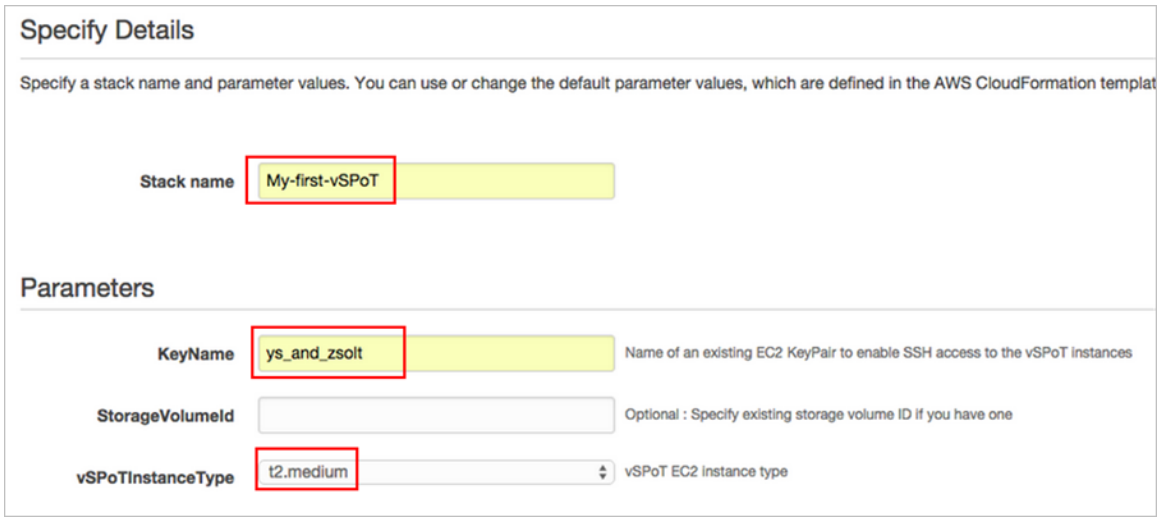
In the Select Template page choose the option Choose a **Template > Specify an Amazon S3 template URL**. Retrieve the URL for the vSPoT template from the Ruckus Wireless Support Web site at (https://support.ruckuswireless.com) and insert the URL as shown in the figure below.

Figure 12: Adding vSPoT template



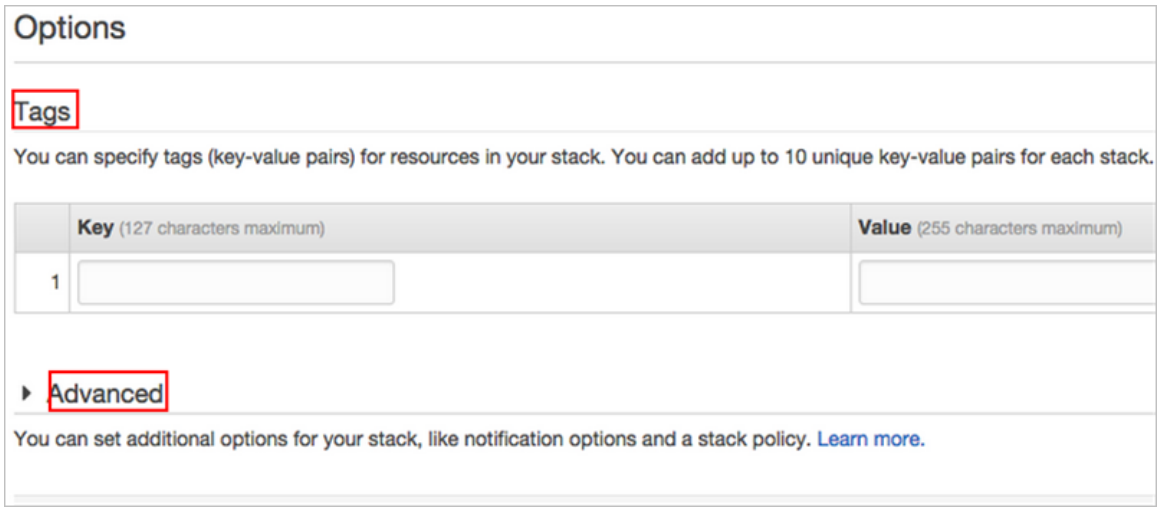
3. Click **Next**.
4. Specify the following in the template.
   a. **Stack Name**: Add a unique template name, which needs to be different from the other vSPoT instances that you would be creating.
   b. **Key Name**: Add a key name required for configuring EC2/keys section
   c. **Storage Volume ID**: Add the volume identifier if you have an existing vSPoT running in AWS to automatically attach and mount to the instance.

Figure 13: Specifying Options in the Template



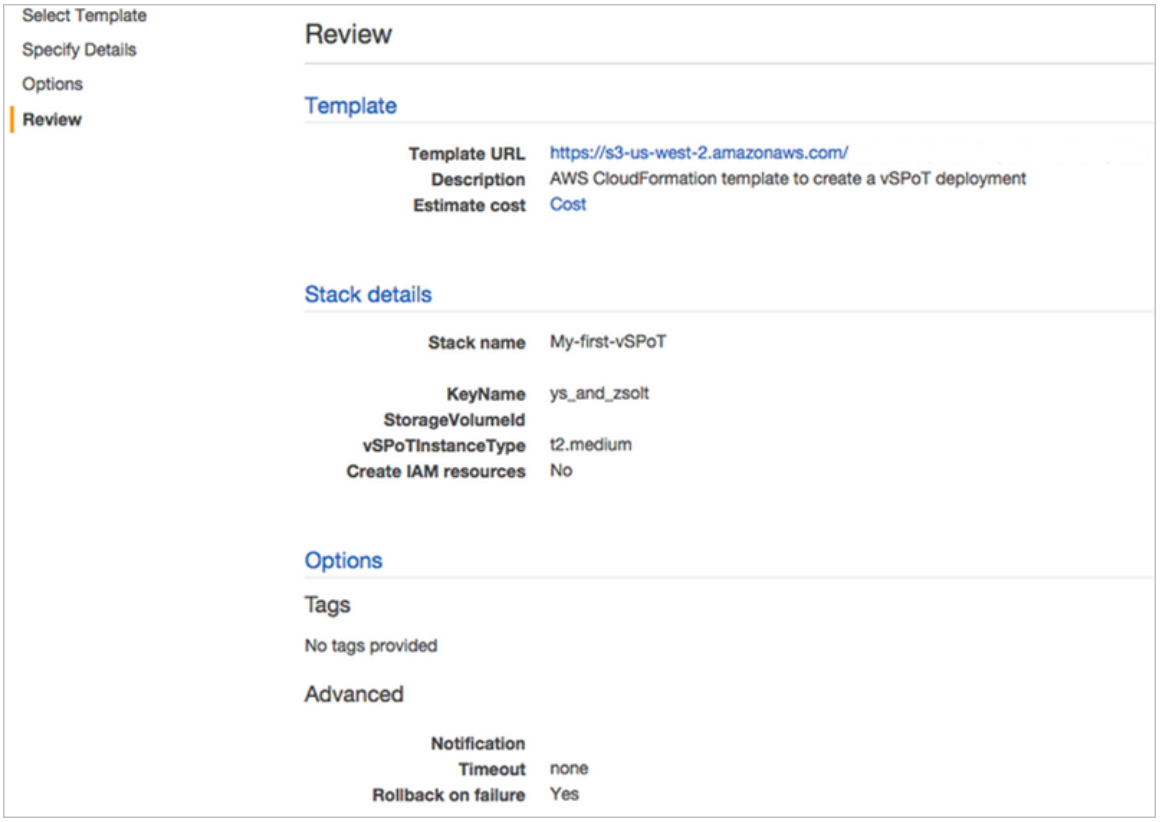
5. Click **Next**.
6. Specify tags or advanced stack configuration options, if any.

Figure 14: Specify Tags and Advanced Options



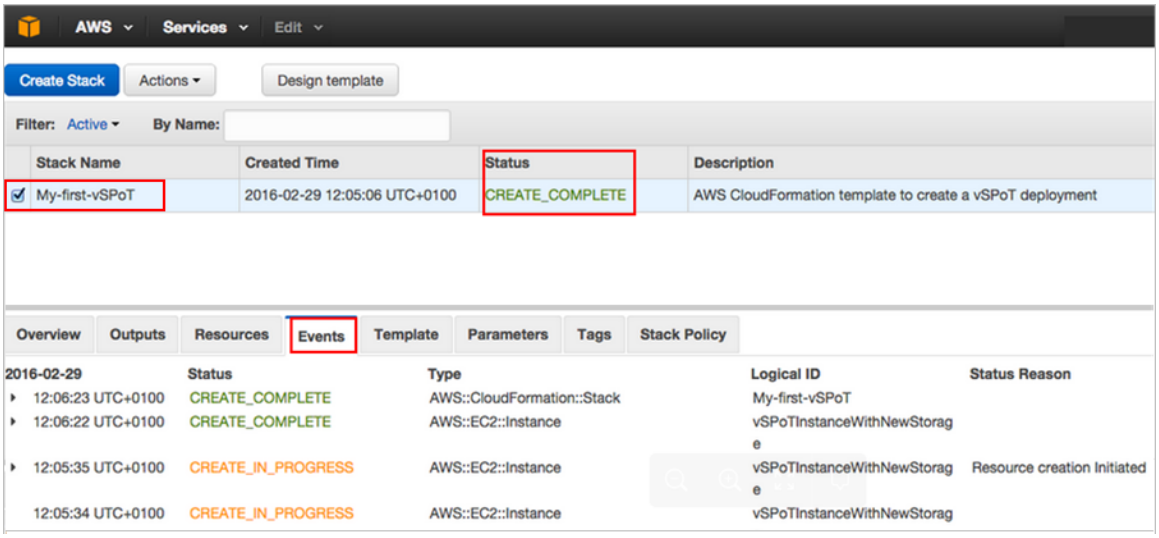
7. Click **Next** to review the configuration settings.

Figure 15: Specifying Tags



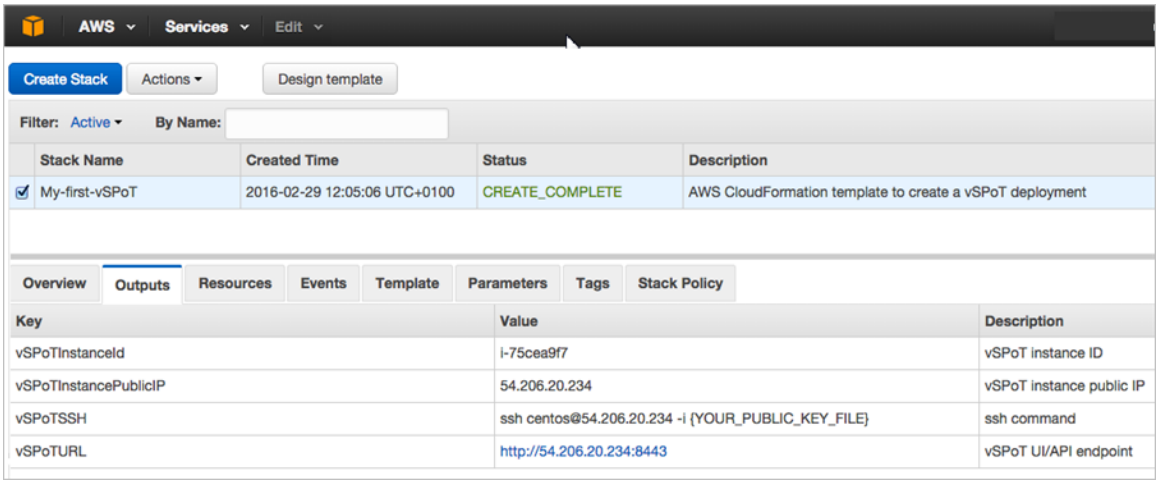
8. Click **Create** to create the resources required to run a vSPoT instance in the AWS cloud. The system displays the progress and successful completion status. Navigate to the **Events** tab on the lower part of the screen to identify and troubleshoot the reason if the installation fails.

Figure 16: Creating a vSPoT instance



9. You now have a running vSPoT instance in your AWS account. You now need to get the IP address of the instance by navigation to the **Outputs** tab. Additional information such as the vSPoT web interface URL and a simple command to SSH into the instance is also displayed.

   Figure 17: IP address of vSPoT instance



10. Open the vSPoT URL (in this example, http://54.206.20.234:8443) in a web browser and login in to vSPoT

    Figure 18: vSPoT login

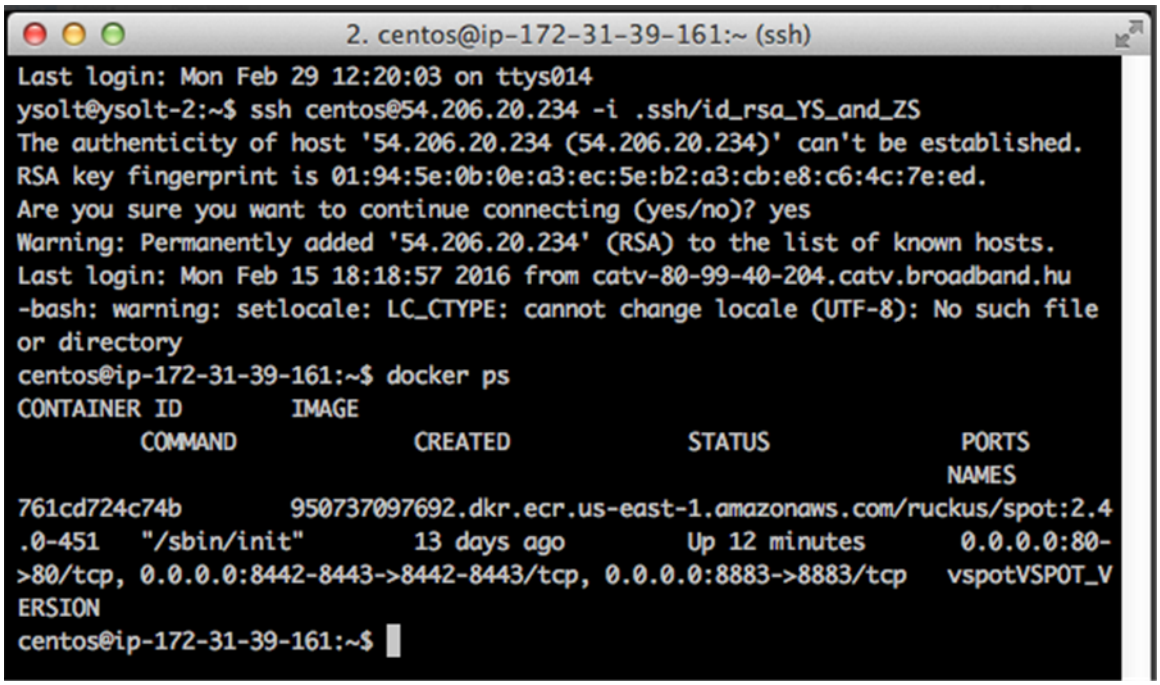
Accessing vSPoT using AWS CLI

This section describes certain technical operations that will require you to log into vSPoT through the shell console using a SSH client.

Follow these steps to login using CLI.

1. Use the SSH command with your private key for the vSPoT instance.
2. The generated or imported SSH key is used as the login to the system as seen in the figure below.

Figure 19: SSH Identifier



Automated Setup using AWS CLI

Follow the steps to install vSPoT using the AWS CLI.

1. Ensure you have AWS CLI installed. In case you do not have it installed download it from AWS website or use **homebrew** if you are running on MacOS.
2. Set up AWS access on your local desktop with the command:

```
$ aws configure
```

3. Create the desired instance, but replace **`ys_and_zsolt`** with your own SSH key name deployed in that AWS region. Refer to step 1 of Accessing vSPoT using AWS CLI on page 32.

```
$ aws cloudformation create-stack --stack-name
vSPoT-evaluation --parameters
'[{"ParameterKey":"KeyName","ParameterValue":"ys_and_zsolt"}]'
 --template-url https://s3-us-west-2.
amazonaws.com/ruckuslbs/public/vspot/vspot.template
```

The response snippet is:

```
{
"StackId":
"arn:aws:cloudformation:us-west-2:950737097692:stack
/vSPoT-evaluation/ef95b9f0-d4be-11e5-b3b1-50d5ca11b8f2"
}
```

4. Use the following command to get the IP address of the instance.

```
$ aws cloudformation describe-stacks --stack-name
vSPoT-evaluation
```

The response snippet is:

```
"Outputs": [
                {
                    "Description": "vSPoT instance ID",
                    "OutputKey": "vSPoTInstanceId",
                    "OutputValue": "i-bb74e063"
                },
                {
                    "Description": "vSPoT instance public
IP",
                    "OutputKey": "vSPoTInstancePublicIP",
                    "OutputValue": "54.191.101.130"
                },
                {
                    "Description": "ssh command",
                    "OutputKey": "vSPoTSSH",
                  "OutputValue": "ssh centos@54.191.101.130
 -i {YOUR_PUBLIC_KEY_FILE}"
                },
                {
                   "Description": "vSPoT UI/API endpoint",

                    "OutputKey": "vSPoTURL",
                    "OutputValue":
"http://54.191.101.130:8443"
                }
            ],
...
```

Access the vSPoT Admin Portal

This section describes how you can access the vSPoT Admin Portal.

1. Launch a web browser and browse to the vSPoT Admin Portal (http://[vSPoT IP address]:8443).

2. Login to the vSPoT Admin Portal:

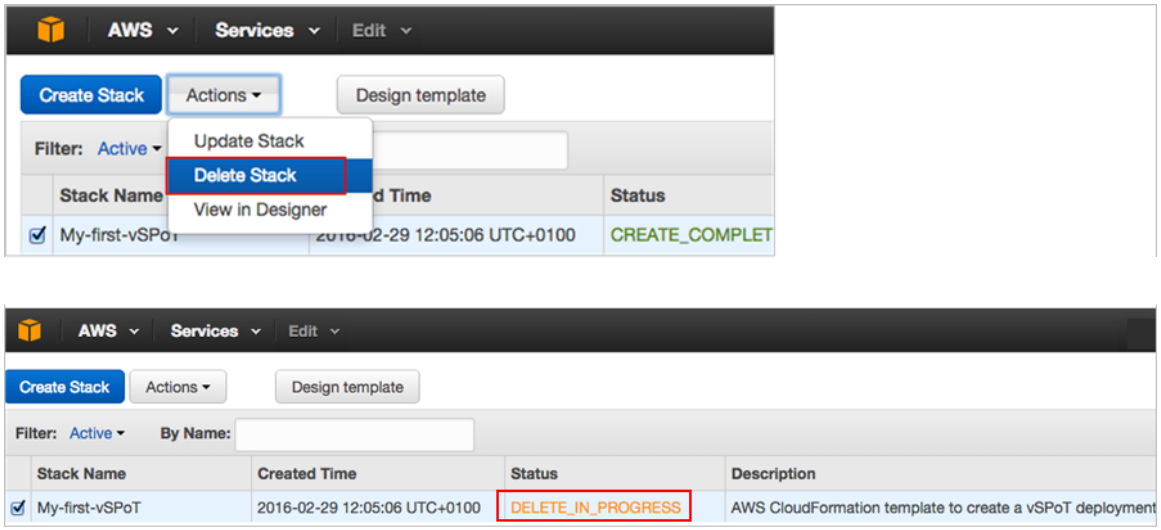
   - **Username**: super_admin@ruckuswireless.com
   - **Password**: 123123123

NOTE At this point, ensure that you change the admin password by clicking **Edit Account** on the top right corner of the screen.

Deleting vSPoT on AWS

To delete a vSPoT instance navigate to **Actions** drop down and click the **Delete Stack** button.

Figure 20: Delete AWS CloudFormation Stack



Delete stack retains data storage volume that has been created. To retain the previous historical data navigate to **Amazon Web Services > Compute > EC2 > Elastic Block Store > Volumes** to store or delete the vSPoT data storage volume.

Figure 21: AWS Data Storage Volume

Configuring Virtual SPoT Application 4

This section describes the system configuration required for a virtual SPoT application.

System Configuration

System configuration steps.

NTP Server

To modify the NTP server configuration for the vSPoT host operating system, login to the server through the system console or by using the SSH remote access. Run the following command and include the NTP server name.

```
admin@vspotappliance:~$ spot config ntp

<your preferred ntp server fqdn or ip>

example: ntp.ruckuswireless.com
```

vSPoT Administration

In general, vSPoT administration procedures are the same as or similar to a typical SPoT deployment (using Ruckus' cloud-based SPoT servers).

For detailed information on SPoT venue administration, see the SPoT User Guide.

Admin Password

NOTE Super Administrators need to keep records of the user name and password. The virtual machine will need to be reinstalled if either user name or password are lost or forgotten.

---

vSPoT Admin Portal

The majority of the Admin Portal feature for vSPoT are the same as those for SPoT. For more information on management options and procedures, refer to the SPoT User Guide, available from support.ruckuswireless.com.

The following sections describe the aspects of vSPoT administration that are different from SPoT.

Access the vSPoT Admin Portal

1. Launch a web browser and browse to the vSPoT Admin Portal (http://[vSPoT IP address]:8443).
2. Login to the vSPoT Admin Portal:

   Username: super_admin@ruckuswireless.com

   Password: 123123123

NOTE At this point, ensure that you change the admin password by clicking **Edit Account** on the top right corner of the Admin Portal screen.

Licensing Information

vSPoT Base software comes pre-shipped with temporary AP Capacity Licenses, valid for a period of 90 days.

Ruckus Wireless recommends a setup up to 500 APs in a single virtual machine. The countdown begins when vSPoT has been configured via the initial setup configuration and the user log in for the first time. For operation beyond 90 days, you can either request for a Trial SKU from Ruckus Sales or Ruckus Support or buy permanent Right to Use Licenses and permanent AP Capacity Licenses. The trial and purchased licenses MUST be activated for them to become valid.

Management of AP Capacity Licenses and activation of permanent Right to Use Licenses is performed using the Ruckus Wireless Support Portal (https://support.ruckuswireless.com). An email will be sent to the user identified on the Purchase Order providing full instructions on activating your Right to Use and AP Capacity Licenses.

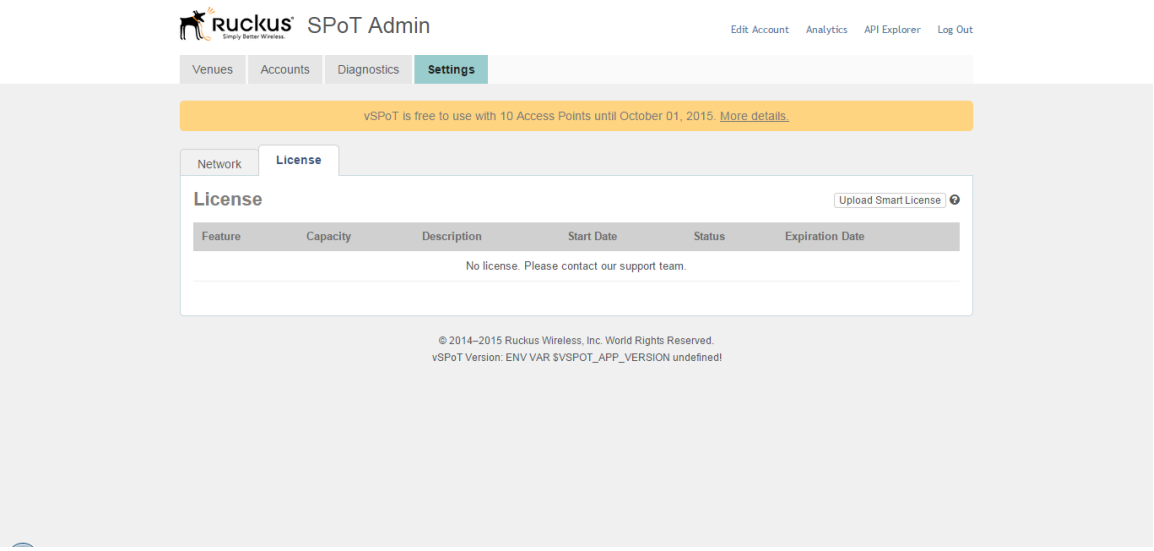
Using the LiMAN (Smart License Management) portal on the Ruckus Wireless Support website, you can assign licenses to or from a vSPoT Virtual Machine (VM) (see the table for a summary of LiMAN features).

It is not necessary for vSPoT to be connected to the Internet to manage licenses.

Table 6: LiMAN features and how to activate them on the vSPoT VM

LiMAN Features	vSPoT
• Register vSPoT software, AP capacity and Support Entitlement licenses. • Add AP capacity licenses to vSPoT. • Remove licenses from one vSPoT Virtual Machine and add to another.	Three steps required: 1. Download the license file from LiMAN. 2. Log on to the vSPoT Virtual Machine. 3. Upload the license file from LiMAN.

Figure 22: License page with free temporary licenses



vSPoT Licenses

This section describes the licenses that you need for vSPot.

You must have a Ruckus Support portal account (including user name and password). You can use this account to access general Support site content including software upgrades, knowledge base articles and technical documents. If you do not have a Support portal account, you will be required to register one before continuing with your product and license activation.

Every capacity and support license that you have purchased will have its own unique activation code and each must be activated for the license to become valid. You will receive the activation code in a separate Support Purchase Acknowledgment (SPA) email for each license/support license.

Depending on the product, you may receive up to three (3) different SPA emails for all of your licenses. The first three characters of the activation code indicate the license type to which the code is applicable.

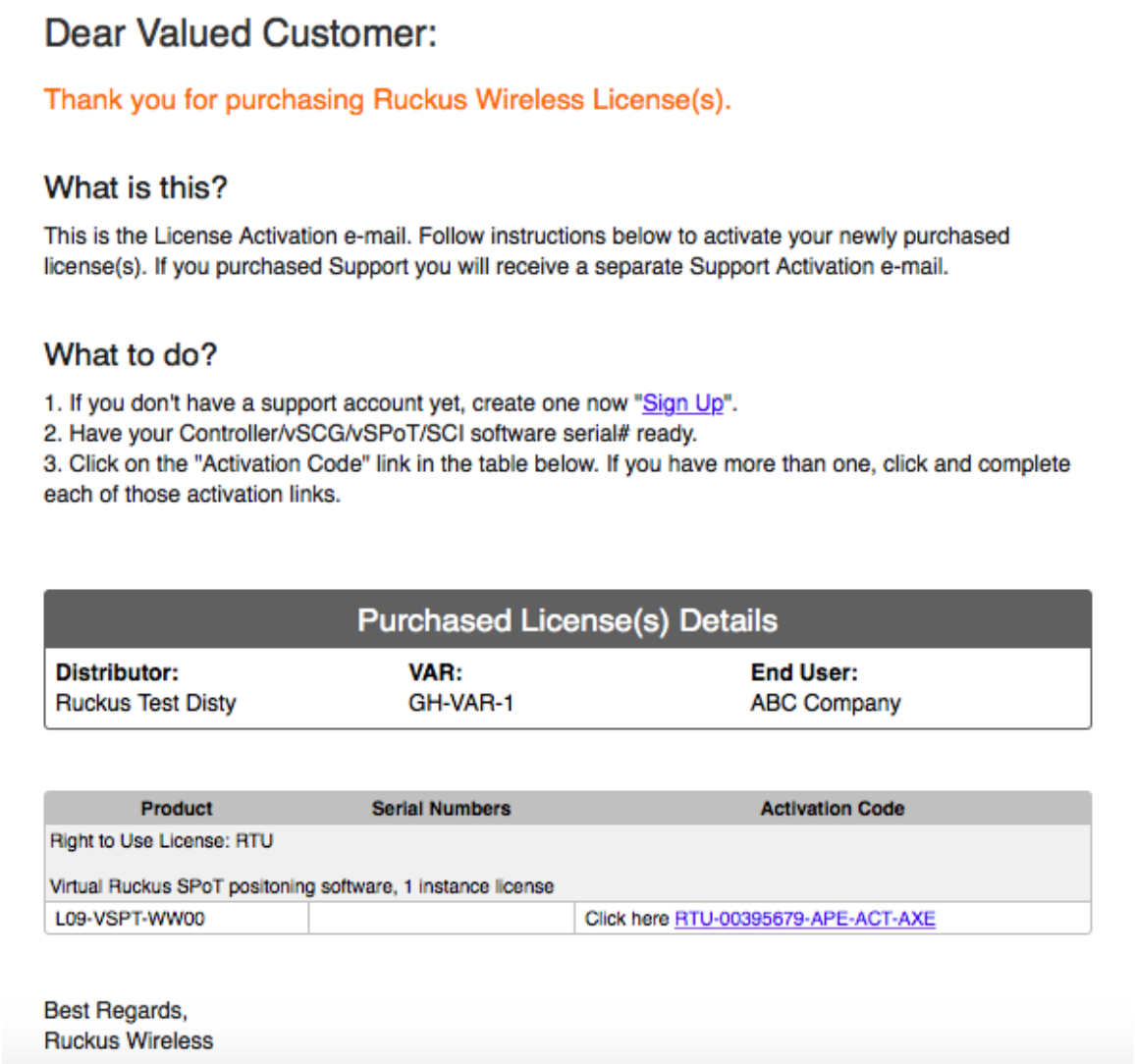
- RTU: Base Software License
- LIC: AP Tunnel License
- SUP: Support License

Activating vSPoT Licenses and Support Licenses

This section explains the procedure to activate your licenses for your vSPoT deployment.

1. Open the SPA email that you received from Ruckus Wireless.

   Figure 23: SPA email



Dear Valued Customer:

Thank you for purchasing Ruckus Wireless License(s).

What is this?

This is the License Activation e-mail. Follow instructions below to activate your newly purchased license(s). If you purchased Support you will receive a separate Support Activation e-mail.

What to do?

1. If you don't have a support account yet, create one now "Sign Up".
2. Have your Controller/vSCG/vSPoT/SCI software serial# ready.
3. Click on the "Activation Code" link in the table below. If you have more than one, click and complete each of those activation links.

Purchased License(s) Details

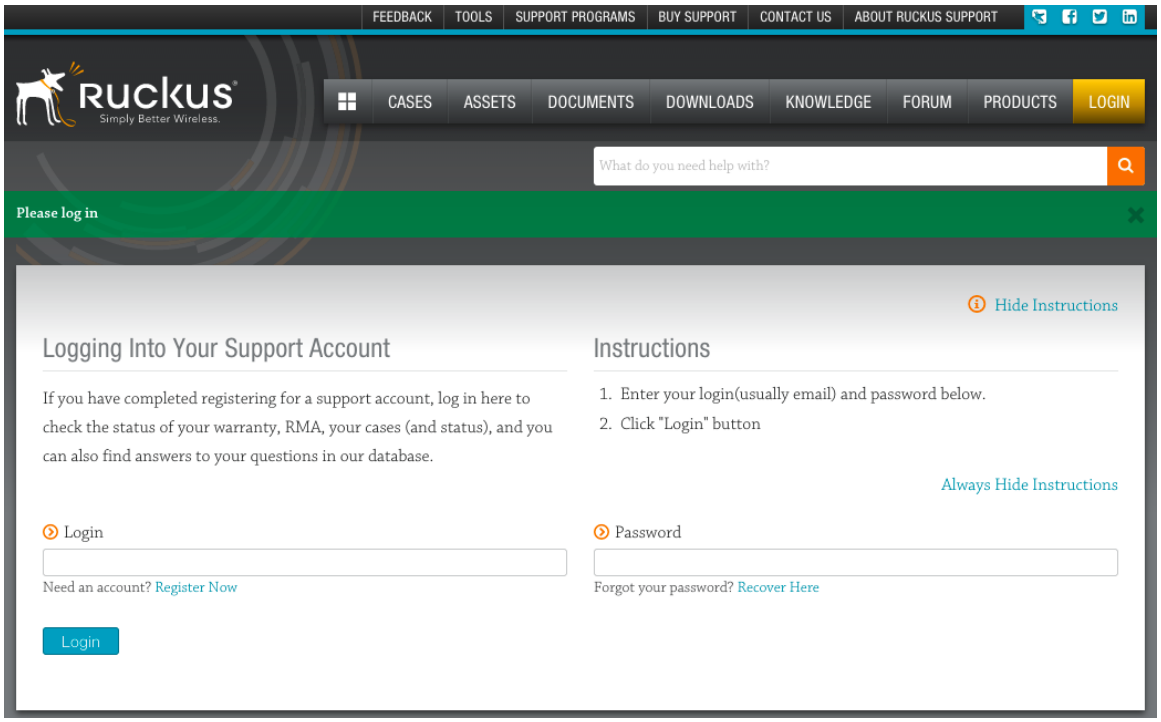
Distributor:	VAR:	End User:
Ruckus Test Disty	GH-VAR-1	ABC Company

Product	Serial Numbers	Activation Code
Right to Use License: RTU Virtual Ruckus SPoT positoning software, 1 instance license		
L09-VSPT-WW00		Click here RTU-00395679-APE-ACT-AXE

Best Regards,
Ruckus Wireless

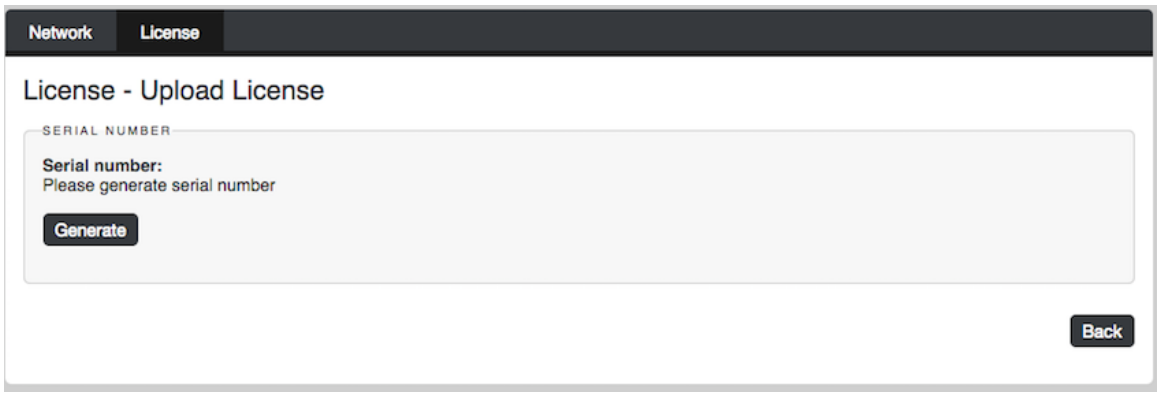
2. Log into the Ruckus Support portal at https://support.ruckuswireless.com.

Figure 24: Logging into the Support portal



3. In the vSPoT Admin Portal, go to **Settings > License > Upload License**, click **Generate** to obtain a Serial Number for the virtual machine. Have the Serial Number of your vSPoT VM device ready.

   Figure 25: Generate Serial Number



4. Click the link in the SPA email.
5. Follow the on-screen instructions to activate the licenses purchased. When required, you will be prompted for your vSPoT serial number.

6. It is important that you repeat steps #1 to #5 above for all licenses that you have purchased as this will simplify the "+License" workflow in step 7 below.
7. After you finish activating all of your licenses, you need to assign them to your Support portal account. Click the **LiMAN** button, which appears after a license has been successfully activated. If your device is listed, click its serial number and proceed to step 8. If your device is NOT listed, click the **Register Smart Device** button enter your device's serial number, and then click the **Register Smart Device** button.
8. Click the **+ License** button enter the number of licenses to add in **Qty to add**, and then click the **Add License** button.
9. Repeat for all licenses.

Figure 26: Click + License to add licenses to this device

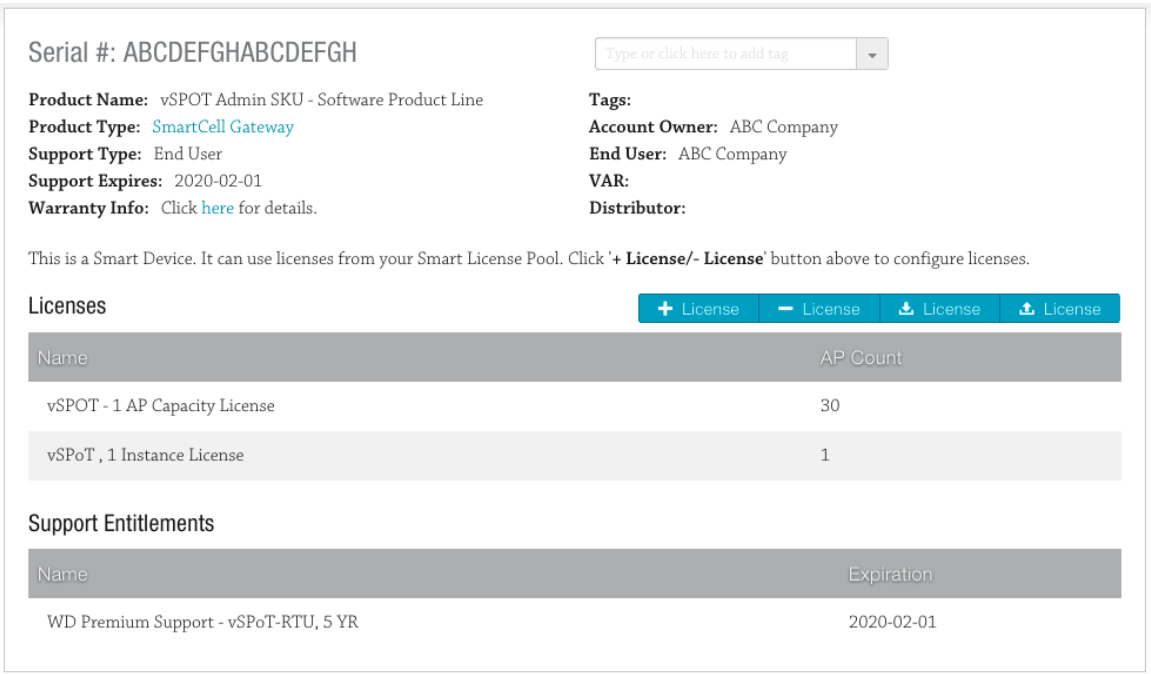
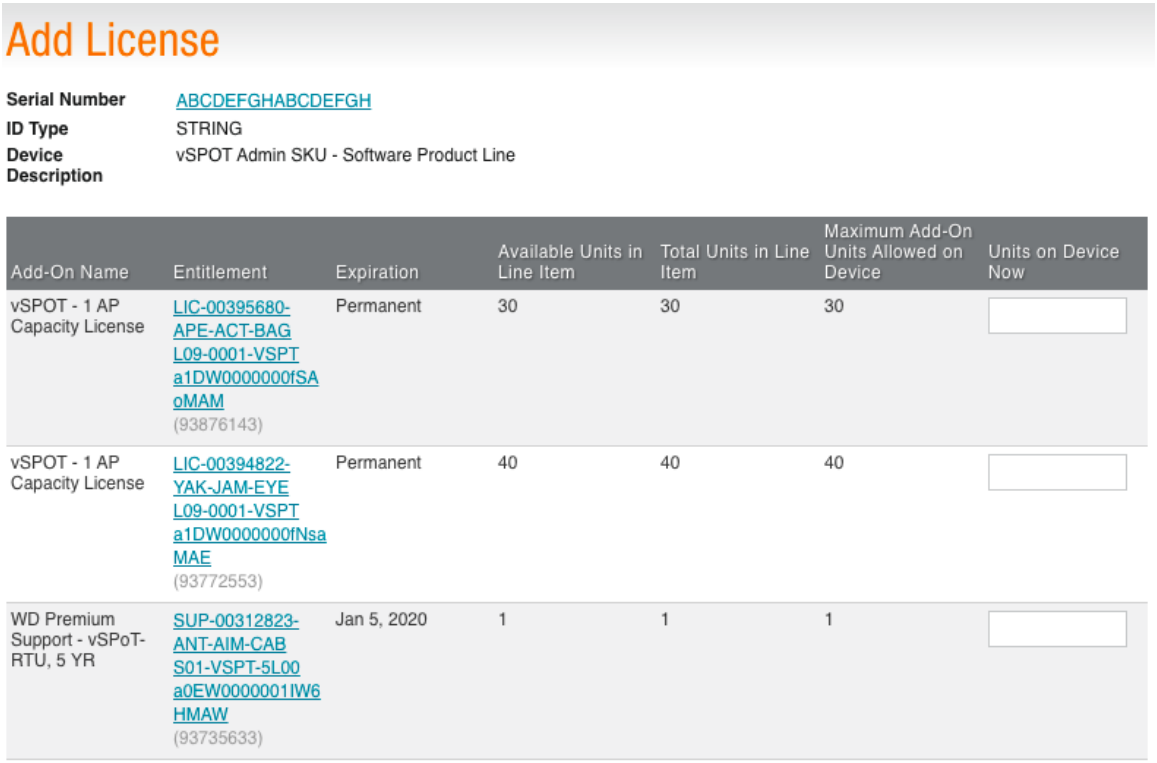


Figure 27: Enter quantity of licenses to add



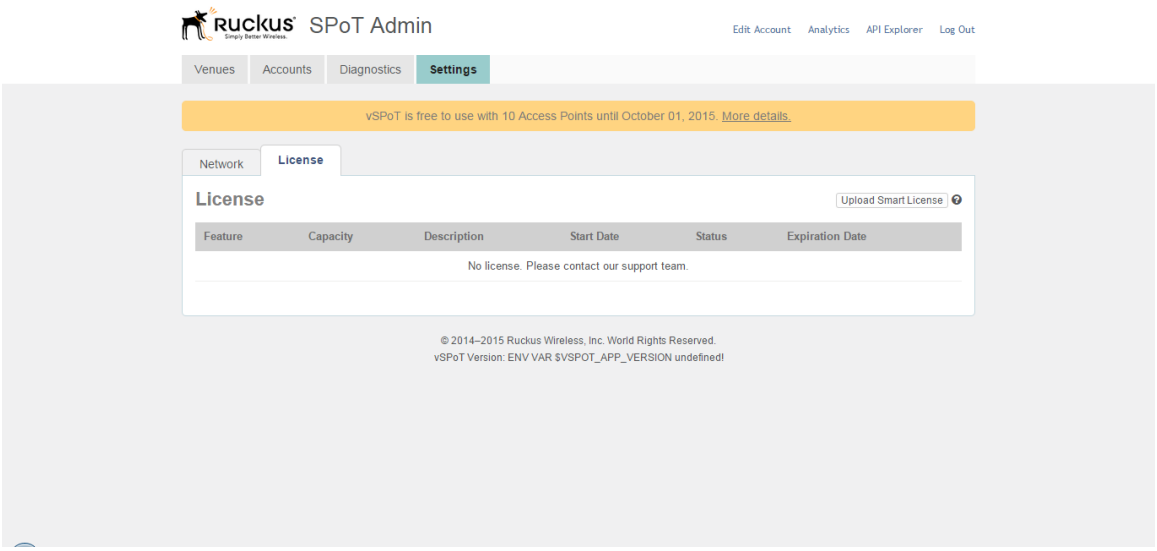
Syncing Licenses on a vSPoT VM

After your licenses have been allocated to your vSPoT instance using LiMAN, you must sync the vSPoT instance with the license information on LiMAN.

Use the following procedure to do so:

1. On the Add License page of LiMAN, click the vSPoT's serial number. The View Device page appears.
2. Click **Download License File**. The license file is saved to the client.
3. On the vSPoT Admin Portal, go to **Settings > License**, and click the **Upload Smart License** button

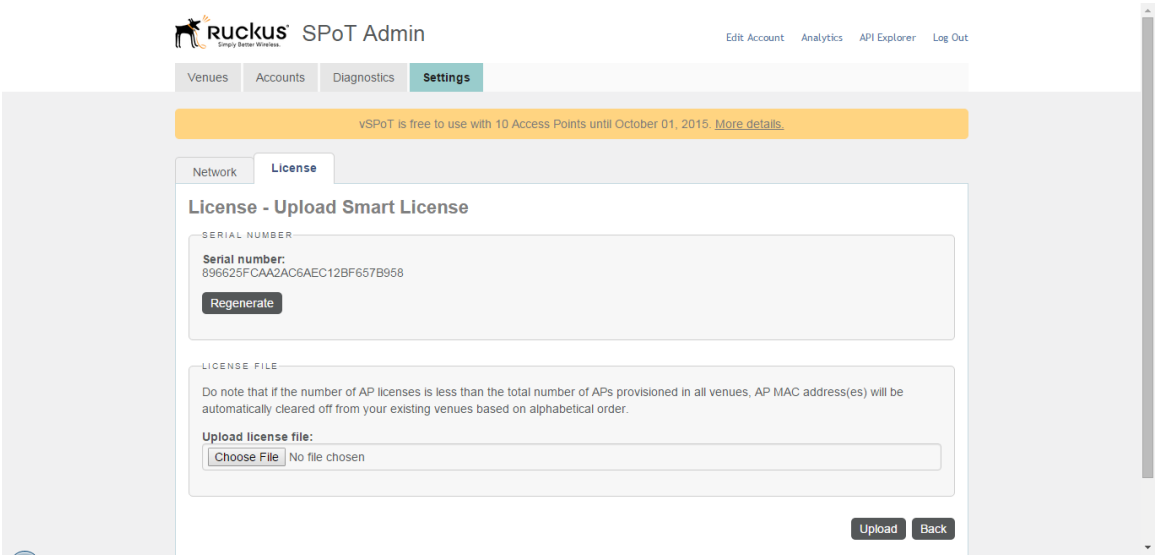
Figure 28: Click Upload Smart License



.

4. In the Upload License section, click the **Choose File** button, and then select the license file from your client to upload it to the vSPoT VM.

Figure 29: Click Upload Smart License



5. Once your license is successfully uploaded, you will see the license displayed on the License page of the vSPoT Admin Portal.

Figure 30: License successfully uploaded

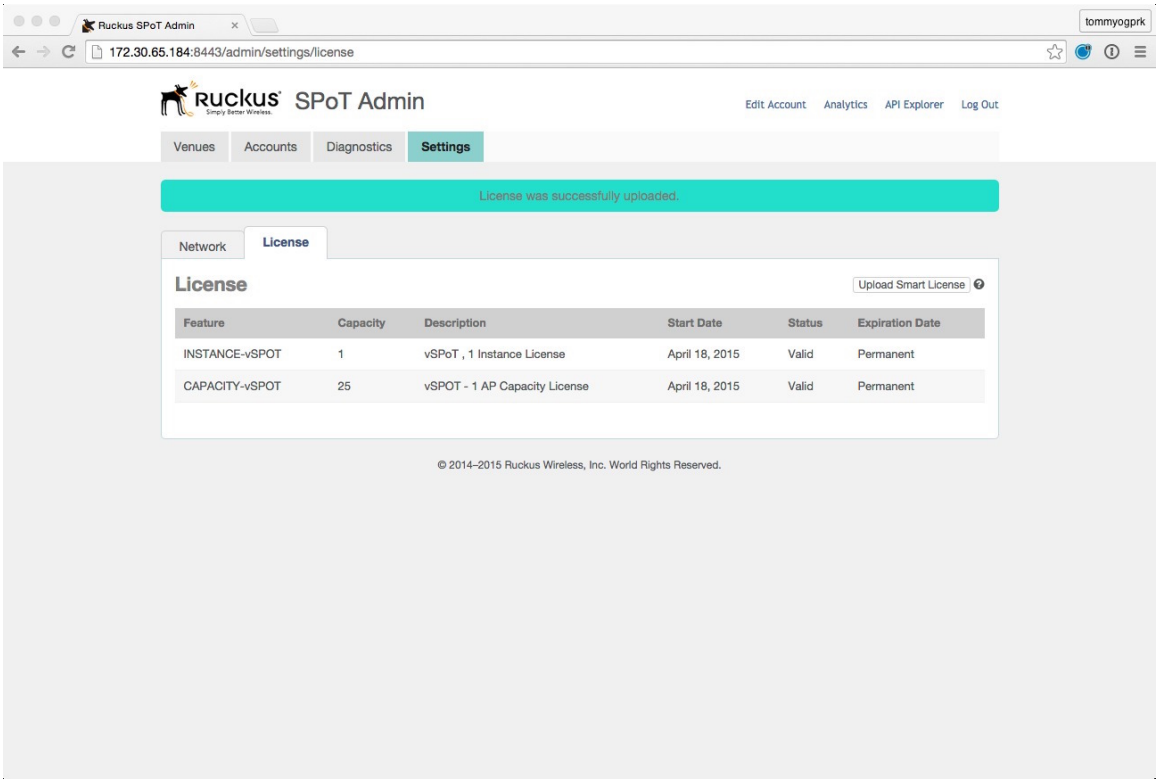
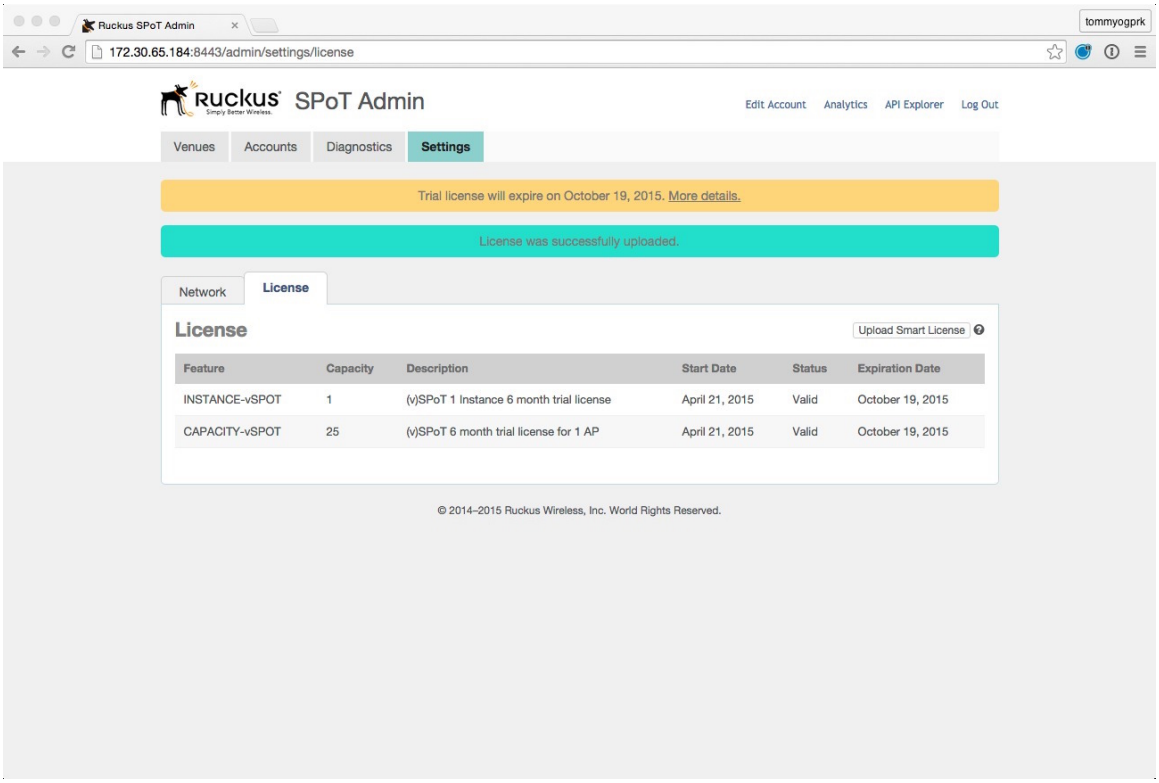


Figure 31: Trial License successfully uploaded



You have completed activating licenses on a vSPoT VM.

NOTE When Upgrading from a Trial license to a Purchased License, regenerate the Serial Number of the VM and repeat the steps in Activating vSPoT Licenses and Support Licenses and Syncing Licenses on a vSPoT VM.

CAUTION! When updating vSPoT within the trial period, do not regenerate the Serial Number of the VM. You will need to access LiMan to download the existing Trial license file and upload it to the updated vSPoT VM.

Venue Setup

The default venue provided out of the box is 'vspot' with an initial 'production active' radio map named 'demo', with 23 AP slots with randomly generated AP MAC addresses.

1. To upload and use your own venue map from the Admin Portal, go to **Radio Maps > Create Radio Maps**. Specify the radio map **Name**, then click **Create Own Map** and follow the directions. When the map is completed, click **Save**.

2. Wait approximately 3 to 10 minutes for the created map to be batch processed.
3. Go to **Radio Map > Details**. Set the new radio map created as 'Production', with the **Start timestamp** being the current date time.
4. Leave the **End timestamp** empty as this is your first production radio map.
5. From the Radio Maps tab, click on the Files link, click and choose the 'floor_1_annotated.png' file link and review the map.
6. With the above map, go to the Access Points tab, and update the MAC addresses of the APs that will be connected to vSPoT (use the AP location and ID overlay from the map as a guide).
7. Go to **Venue Details > Locality** and update **Address** and **Timezone** to the correct timezone for your venue.
8. To Add a new venue to vSPoT, go to Venues, click on **New** and repeat steps 1 to 7.

Additional Information

For additional information on vSPoT administration, see the SPoT User Guide, available from https://support.ruckuswireless.com.

Controller Configuration

To configure your venue, you must perform several steps on the ZoneDirector or SmartZone controller that is deployed at your venue.

See the following section depending on which controller your venue is using:

- To Configure ZoneDirector
- To Configure SmartZone

To Configure ZoneDirector

This section describes how to configure ZoneDirector as your controller for your venue.

NOTE To manage multiple vSPoT venues on a single Zone Director controller, use firmware 9.12.2 and above. This will allow the controller to manage multiple vSPoT Venue IDs using a single IP.

---

1. Log into ZoneDirector to point your ZoneDirector and APs to the vSPoT virtual machine.
2. On the ZD web interface, go to **Configure > Location Services**. On the **Create New** venue form, enter the following information:
   - **Server FQDN or IP Address**: Enter the IP address of the machine on which you are running the vSPoT VM.
   - **Server Port**: Enter the Port number as displayed on the vSPoT Admin portal Config page.

- **Password**: Enter the password as displayed on the vSPoT Admin portal Config page.

NOTE This information is available on http://[vSPoT IP Address]:8443/admin/venues/vspot/edit_config.

3. On the ZD web interface, go to **Access Point Groups > Editing (System Default) > Location Services**, and configure the following settings:
   - **Enable/Disable**: Enable.
   - **Venue Name**: Select the venue you created on the Location Services page from the drop-down list.
4. Go to **Monitor > Location Services** in ZD to check that AP-LS Status and ZD-LS Status is connected.
5. Go to **Monitor > Access Points** to view status lights of the AP. If Green, vSPoT is now running successfully in your venue. You may proceed to calibration (if using SPoT Point with Calibration). If Red, contact Customer Service for assistance.
6. You can configure the vSPoT Locator parameters via the Config page on the vSPoT Admin Portal (http://[vSPoT IP address]:8443/admin/venues/vspot/edit_config).
7. Detailed vSPoT VM diagnostics are also available at http://[vSPoT IP address]:8442 in case you would like to investigate your hardware resource consumption. A summary is provided on the Diagnostics page.
8. Proceed to perform the calibration using the SPoT Calibrator app.
9. Analytics functionality will be available by clicking **SPoT Analytics**.

To Configure SmartZone

This section describes how to configure SmartZone as your controller for your venue.

NOTE To manage multiple vSPoT venues on a single SmartZone controller, use firmware 3.1.1 patch 1 and above. This will allow the controller to manage multiple vSPoT Venue IDs using a single IP.

1. On the controller web interface, go to **Configuration > Services & Profiles > Services > Location Services**.
2. Click **Create New**. The Create New LBS Server form appears.
3. Configure with the cloud LBS parameters that you obtain from the **SPoT Admin Portal -> Config** page. And Click **OK** to Save Changes.
4. Next, configure the controller to use the LBS server. There are 2 methods:
   - Set an entire AP zone to use an LBS server: When you create or edit an AP zone, you can enable the LBS service for the entire zone by selecting the Enable LBS Service check box, and then selecting an LBS server to use.
   - Set an AP group to override the LBS settings of a zone: If you want APs that belong to an AP group to use a different LBS server, you can override the LBS settings at the AP group level. Follow these steps.

5. Go to **Configuration > AP Zones**. In the AP Zone List, click the zone name to which the AP group you want to configure belongs.
6. On the sidebar, click **AP Group**. Click **Create New** to create a new AP group, or click the AP group name to edit it.
7. In the form that appears, scroll down to the Advanced Options section. Click the plus (**+**) sign to display all options. In Location Based Service, select the **Override zone config** check box.
8. Configure the LBS settings as required.
    - To disable the LBS service for this AP group, clear the **Enable LBS service** check box.
    - To use a different LBS server for this AP group, select the **Enable LBS service** check box, and then select the LBS server that you want to use from the drop-down list.
9. Configure the other AP group settings as required. Click **OK**. You have completed setting an AP group to override the LBS settings of its zone.

NOTE For more information on ZoneDirector or SmartZone configuration, refer to their respective User Guides available on the Ruckus support site.

Managing Virtual SPoT Application 5

This chapter explains how you can manage the vSPoT application and has the following sections.

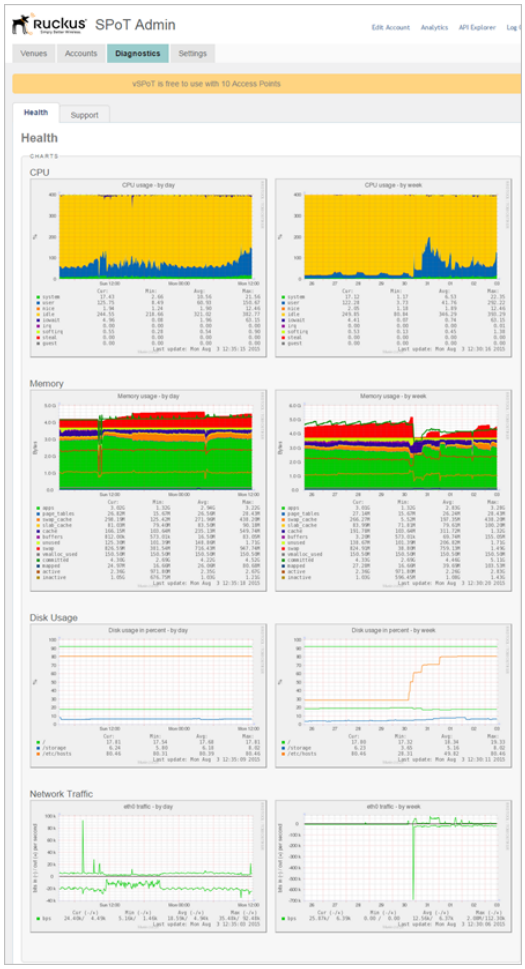
Diagnostics

The Diagnostics tab in the vSPoT Administrator user interface provides charts to enable users to track the health of the resource utilization by vSPoT, in terms of:

- CPU
- Memory
- Storage
- Network

You can view daily and weekly charts.

Figure 32: Diagnostics page



Insufficient Server Resources

If there is a drastic and sustained increase in the resource utilization (as viewed from the Diagnostics tab) or a drastic and sustained decrease in location analytics numbers (as viewed from the Analytics dashboard), there could be insufficient server resources for vSPoT to handle the incoming data load. Users are recommended to increase the server resources allocated to vSPoT.

Configuring the Number of vSPoT Processing Workers

CAUTION! This section is only applicable to vSPoT version 3.2 and above.

The collators processes receive raw data streams from the APs, and transforms the data accordingly for the location engine. The pas_workers processes run in the location engine and generates the location coordinates for the WiFi clients detected. As you scale

up the server with hardware resources, to ensure that vSPoT is able to efficiently utilize the server resources, you would also need to configure the number of collators and pas_workers processes. Follow the below procedure

1. Login to the vSPoT CLI using the console access or through SSH using the 'admin' user. Refer to if you have not yet configured SSH access.

```
ssh admin@<vspot_host_os_public_ip>
```

   For example:

```
ssh admin@192.168.0.5
```

2. Ensure NTP server synchronization between Controller, APs and vSPoT Host OS.
3. Enter the vSPoT docker container

```
admin@vspotappliance:~$ spot enter
```

4. Stop the rk-venue server processes

```
root@vspot:~# systemctl stop rk-venue.target
```

5. Run the CLI command to change the number of workers. For example, 10 collators and 16 pas_workers.

```
root@vspot:~# cd $RK_VENUE_ROOT
```

```
root@vspot:~# bundle exec rake
bootstrap:generate_init_scripts[,collator=10,pas_worker=16]
```

6. Start the rk-venue server processes

```
root@vspot:~# systemctl start rk-venue.target
```

   The following table provides a guideline for specifying the number of collators and pas_workers processes, based on the number of vCPUs available from your server.

   Table 7: Number of Worker Processes

vCPU	Number of collators	Number of pas_workers
40	36	60
20	15	25
16	10	10
8	3	5
4	2	5

vCPU	Number of collators	Number of pas_workers
2	2	3

Remote Support

For troubleshooting purposes, you can establish a reverse SSH connection to the Ruckus vSPoT support server, so that a Ruckus Customer Support representative can access your vSPoT VM remotely and assist with troubleshooting.

There are two methods to access vSPoT remotely.

- Using the vSPot User Interface
- Using the CLI Console on page 56

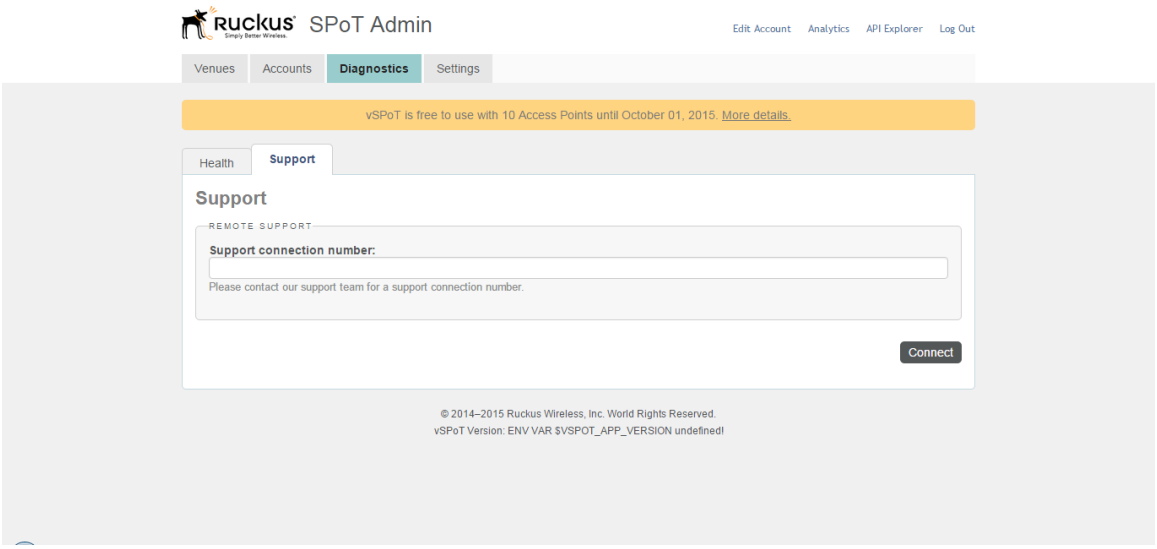
Using the vSPoT User Interface

This section explains how you can access vSPoT remotely using the vSPoT User Interface.

Follow the steps for allowing remote access through the user interface.

1. Go to **Settings > Support**.

Figure 33: Remote Support page



2. Contact Ruckus Customer Support at https://support.ruckuswireless.com.
3. The support representative will give you a 4-digit support connection number. Enter this number in **Support Connection Number** and click **Connect**.

4. Click **Disconnect** after the support session has ended to end the SSH connection.

NOTE In order for the remote support functionality to work properly, please ensure the following:

1. The vSPoT VM has access to a DNS server that is able to resolve public URLs.
2. The firewall, if any, allows outbound traffic on port 50000.

Using the CLI Console

This section explains how you can access vSPoT using the CLI console.

Follow the steps for allowing remote access using the vSPoT console.

1. Login to the vSPoT CLI using the console access or through SSH using the 'admin' user
2. Enable remote SSH support connection by executing the CLI command. By default this option is disabled.

```
admin@vspotappliance:~$ spot support on
```

3. Set up a NAT rule or open port to enable inbound network communication on TCP/22 port.
4. To disable remote SSH support connection execute the CLI command:

```
admin@vspotappliance:~$ spot support off
```

Backup and Restore

Backup is performed through VMware vSphere by copying the database volume to a separate server. When a new VM is provisioned, data can be restored by pointing the new VM to the desired database volume. Again, this is done through VMware.

Upgrading to a New Version

This chapter lists important information that you must be aware of when upgrading vSPoT.

NOTE A full HOST OS upgrade is required for vSPoT 3.2 since it includes changes related to CentOS7 based docker container with systemd support. System commands to start and stop application data services is different for systemd in comparison to previous vSPoT versions.

Key Features

The following is the distinction between the two upgrade procedures.

Full Upgrade

NOTE Full upgrade refers to vSPoT on VMware Upgrade from Version 3.x to Latest on page 59, vSPoT on VMware Upgrade Version 2.4.x to 3.x (Latest) on page 62 or vSPoT on AWS Upgrade on page 76

- Provides better security since it contains host operating system improvements and security updates
- Provides a more atomic upgrade since the host operating system and application containers are built and tested together as part of the release process
- Easier for VMware administrators

Rolling Upgrade

NOTE If you are upgrading to vSPoT 3.x from vSPoT 2.4.0 or earlier versions, Ruckus Wireless highly recommends that you do a full upgrade to take advantage of the security and performance improvements to the Host OS.

NOTE vSPoT upgrades from version 3.x onwards can be performed via rolling upgrades.

- Decreased downtime during the upgrade procedure since there is no switch to virtual disks or having to restart the VM. This saves an enormous amount of downtime
- Easier upgrade procedure since access and storage configuration of VMware is not required
- Decreased manual configuration since networking and NTP server configuration is persisted within the VM, therefore this does not require reconfiguration
- Easier for Linux administrators

Full Upgrade

The following is the upgrade procedure based on the installation type.

CAUTION! In order to upgrade to vSPoT version 3.x, you need to first ensure that the existing vSPoT is on version 2.4.0 and above. If your vSPoT version is below 2.4.0, you **cannot directly upgrade** to vSPoT 3.x. Do refer to *vSPoT 2.4.4 Installation Guide* on the support website (https://support.ruckuswireless.com) to **first** upgrade to vSPoT 2.4.4 before upgrading to 3.x.

---

1. vSPoT on VMware Upgrade from Version 3.x to Latest on page 59
2. vSPoT on VMware Upgrade Version 2.4.x to 3.x (Latest) on page 62
3. vSPoT on AWS Upgrade on page 76

vSPoT on VMware Upgrade from Version 3.x to Latest

The following is the procedure for a full upgrade of vSPoT from version 3.x to the latest version.

1. Log in to the vSphere Client:
   a. Launch an instance of VMWare vSphere Client (e.g. Windows VMWare vSphere Client).
   b. In the VMWare vSphere Client, enter the IP Address (or Hostname) and administrative credentials to login to your instance of ESXi server running the source and target vSPoT instances where you want to migrate the data storage volume.
2. Copy the AP MAC addresses seen on the Access Points page (navigate to **SPoT Admin Portal** > **Access Points**), in order to retain a backup of all the AP MAC addresses.
3. Power Off Source and Target vSPoT instances:

   NOTE As an example, the source instance is vSPoT 3.0.0 and the target instance is vSPoT 3.2.

   a. On the left panel, expand the list of installed VM instances, and locate the source and target vSPoT instances that will be swapping data storage volumes.
   b. Right click on each and **Power-Off** each instance successively (shortcut: **Ctrl-E**).
4. Detach source vSPoT instance data storage volume:
   a. Once both source and target instances have been Powered Off, navigate to the source VM instance (note the name of the source vSPoT instance - this will be used to relocate and mount the storage from the source to the target vSPoT instance in later steps). Right-click and choose the '**Edit Settings...**' menu item.
   b. On the child window that appears, on the left panel, locate and identify the item under the 'Hardware' column, named '**Hard disk 3**', and click to select it.
   c. From the same child window, with the 'Hard disk 3' item selected, locate the '**Remove**' button at the top of the left panel of the child window.

      CAUTION! On **Removal Options** displayed on the right panel, select '**Remove from virtual machine' ONLY.** (**Do Not** use the other option, as this would wipe out the data and therefore make it impossible to migrate the data volume to the new target instance.)

   d. Notice that the 'Hard disk 3' item is struck out and the 'Summary' column indicates it as 'Removed'; Click '**OK**' at the bottom right hand corner of the child window to proceed.
5. Remove target vSPoT instance data storage volume:

a. From the list of VM instances on the parent window left panel, locate the target vSPoT instance item, and select and right click on the '**Edit Settings...**' menu item.
b. Repeat Steps (3b) to (3d) above but for the target vSPoT instance, and click '**OK**' to end the disk removal process, so that the data storage volume to be attached may take its place.

6. Attach source vSPoT instance data storage volume to target vSPoT instance:

a. From the list of VM instances on the parent window left panel, again locate the target vSPoT instance item, right-click and select the '**Edit Settings...**' menu item.
b. On the 'Virtual Machine Properties' child window, now locate and click the '**Add...**' button at the top of the left panel of the child window.
c. On the new 'Add Hardware' child window, select the '**Hard Disk**' item in the middle panel of this child window and click on the '**Next**' button located at the bottom of this child window.
d. In the 'Select a Disk' option under the 'Add Hardware' child window, select the option '**Use an existing virtual disk - Reuse a previously configured virtual disk**' in the 'Disk' option, then click on the '**Next**' button located at the bottom of this child window.
e. On the 'Select Existing Disk' option under the 'Add Hardware' child window, click on the '**Browse...**' button next to the 'Disk File Path' text entry field.
f. From the new Windows file explorer dialog, locate and select the '**Datastores**' file type that was created for your ESXi server, (e.g. esxi-local-storage-1), select the item, then click '**Open**'.
g. From the expanded list in the 'Browse Datastores' dialog, scroll to and locate the 'Name' identical to your source vSPoT instance that you recorded in Step (3a) above (e.g. *vSPoT2-3.0.0-build-543_vmx*), and select the item, then click '**Open**'.
h. From the refreshed 'Browse Datastores' dialog, locate and select the item ending with '**_vmx_2.vmdk**', and click '**OK**'.
i. Back in the parent '**Add Hardware' -> 'Select Existing Disk**' child window, notice the filled out 'Disk File Path' file based on your selections from the above steps, then click the '**Next**' button.
j. On the '**Add Hardware' -> 'Advanced Options**' child window, right side panel, locate the '**Virtual Device Node**' section, and select the item directly beneath the 'SCSI (0:1) Hard disk 2' item (e.g. '**SCSI (0:2)**'), then click the '**Next**' button.
k. Review the '**Add Hardware' -> 'Ready to Complete' -> 'Options**' summary information, and click the '**Finish**' button to complete the data storage volume transfer action, OR, click '**Back**' to alter/edit any previously entered values/choices, OR, click '**Cancel**' to ABORT the operation.
l. Finally, click the '**OK**' button at the bottom right-hand corner of the '**Virtual Machine Properties**' window to finish the VM settings changes applied/changed/aborted.

Power On your target vSPoT instance VM and verify the data volume migration action has successfully completed.

7. Verify successful upgrade.
   a. Verify that the web service is running.
   b. View and validate application state from *http://<vSPoT VM IP>:8443*.
   c. Check the application version (example, latest version), and login to the vSPoT administration dashboard using a valid user account and admin account.
8. Verify admin and analytics dashboards.
   a. From the Admin pages, validate the data presence of radio maps, access points, venues, etc.
   b. From the analytics page, verify real-time and historical data (heat maps and daily visit counts)

NOTE Refer to Upload and Rollback of Self Signed SSL Certificate on page 90 to upload or revert the pre-bundled self-signed SSL certificate.

---

vSPoT on VMware Upgrade Version 2.4.x to 3.x (Latest)

The following is the procedure to upgrade a vSPoT deployment from version 2.4.x to vSPoT 3.x (latest).

NOTE This upgrade process will result in application downtime due to the need for migrating data across different and incompatible storage engines. During the migration process, vSPoT should not be running, otherwise data could be lost during migration.

CAUTION! In order to upgrade to vSPoT version 3.x, you need to first ensure that the existing vSPoT is on version 2.4.0 and above. If your vSPoT version is below 2.4.x, you **cannot directly upgrade** to vSPoT 3.x. Do refer to *vSPoT 2.4.4 Installation Guide* on the support website (https://support.ruckuswireless.com) to **first** upgrade to vSPoT 2.4.4 before upgrading to 3.x.

Prerequisites

- You are required to open port 22 of your vSPoT host operating system (Host OS) on a public facing IP address.

Upgrade Procedure

The upgrade procedure has the following list of instructions.

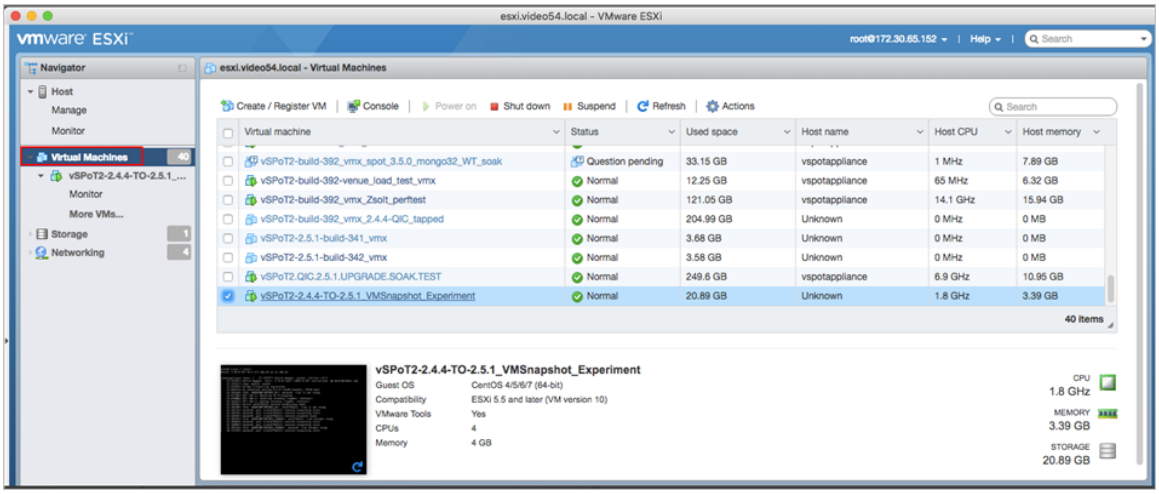
NOTE Ruckus Wireless recommends that you follow the procedure for a successful upgrade.

Backup the Current vSPoT

This section describes the procedure to backup the current vSPoT.

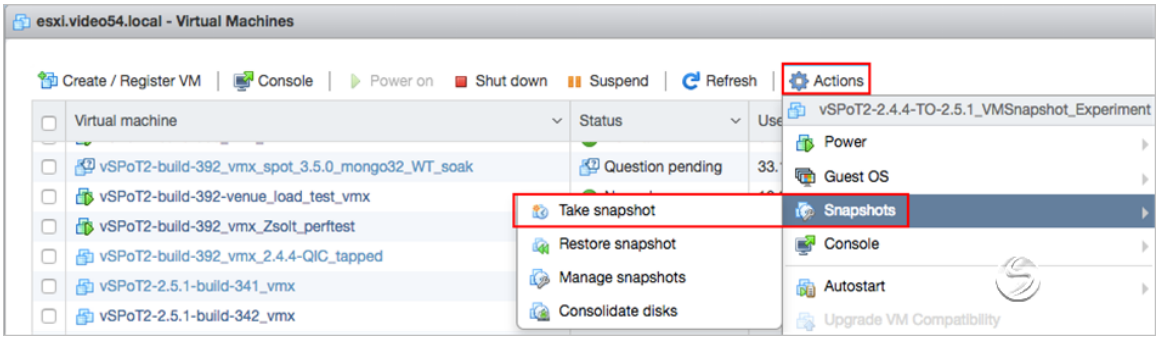
1. Login to the vSPoT vCenter
2. Using the VMWare ESXi web interface navigate to select **Virtual Machines > VMware** instance for a backup.

Figure 34: Selecting Virtual Machine Instance



3. Ensure that your shared storage mounted for vCenter or ESXi has sufficient disk space for the snapshot backup. If vSPoT is using around 1TB, ensure you have at least 1TB additional free storage space for the snapshot backup.
4. In the tab menu navigate to select **Actions > Snapshots > Take snapshot**

Figure 35: Selecting the Snapshot Option

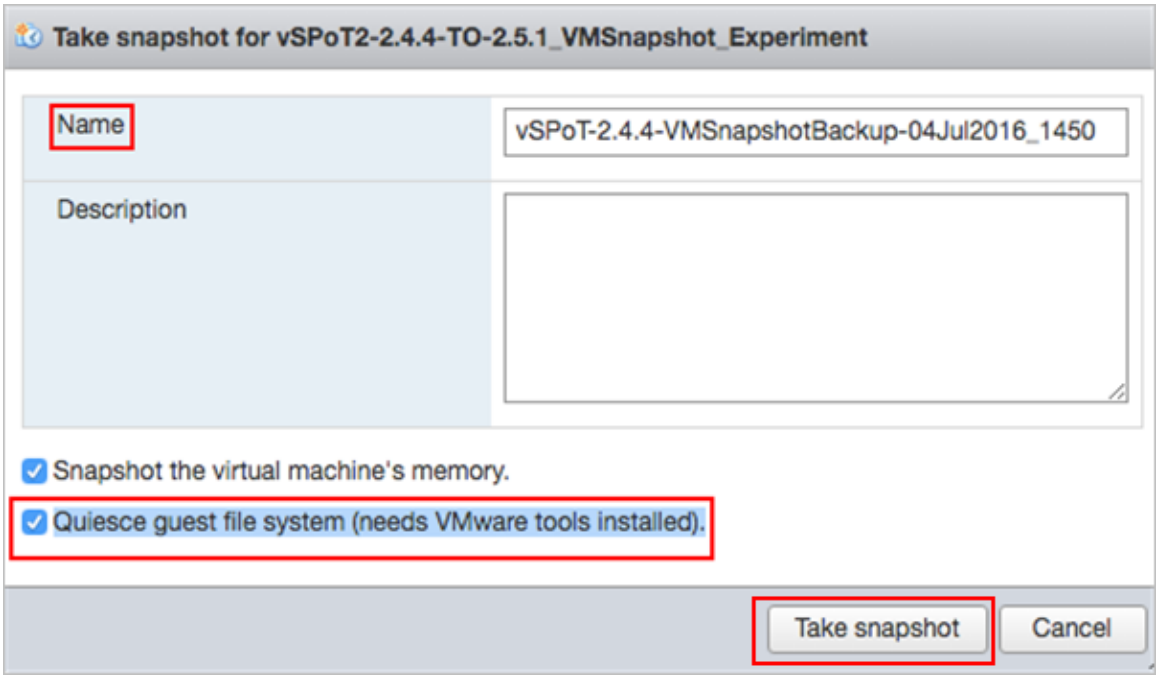


5. Enter a name for snapshot backup.

```
For example, vSPoT-2.4.4-VMSnapshotBackup-04Jul2016_1450.
```

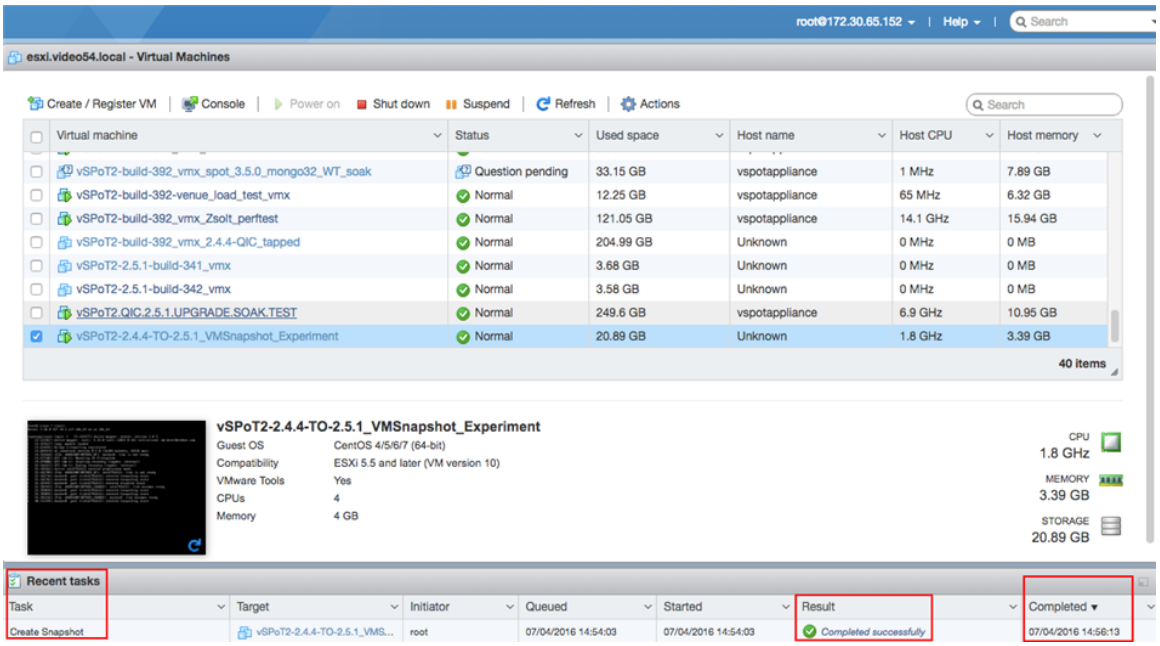
Also, select the option, *Quiesce guest file system (needs VMware tools installed)*.

Figure 36: Snapshot Name



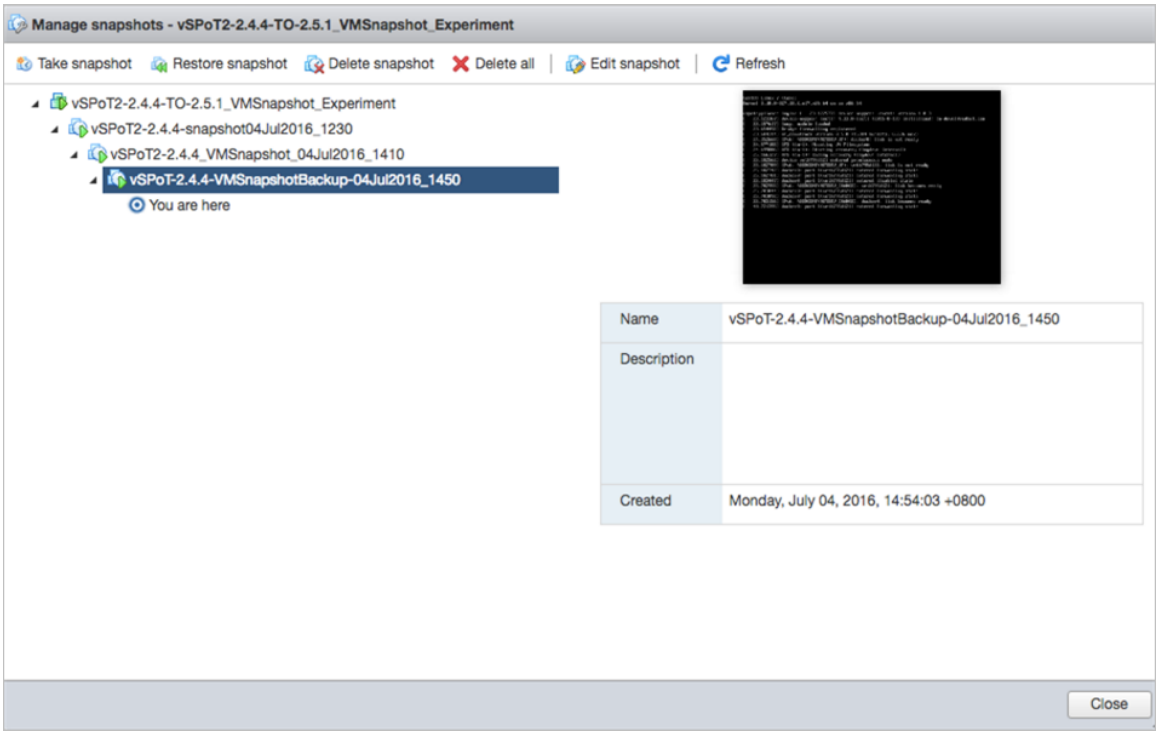
6. Click on the **Take snapshot** button to complete the snapshot.
7. Check the **Recent tasks** tab at the bottom panel to ensure that the snapshot is complete. This could potentially be a long running task from 5 minutes to around 30 minutes depending on the size of your Vmdk, mounted storage, storage type and performance.

Figure 37: Check Status of Snapshot



8. Check that your created snapshot is visible in the list of snapshots by navigating to Actions > Snapshots > Manage snapshots. You should be able to see your created snapshot in the list pop-up window.

Figure 38: Created Snapshot



In the event that you need to restore a previous snapshot, follow the Procedure to Restore VMWare Snapshots (Optional) on page 75

Venue Identifiers

After a successful backup of the vSPoT instance, ensure you have an updated list of Venue identifiers. This is required during migration.

Download vSPoT 3.x

Download the latest vSPoT build version 3.x (example -vSPoT-3.2.0-build-985.tar) from the support site (https://support.ruckuswireless.com)

Stop VM Server Running vSPoT

Stop the existing VM server running vSPoT version 2.4.4 by running the following CLI commands.

1. SSH to the vSPoT host operating system and to the vSPoT docker container.

NOTE Refer to SSH Key Based Authentication if you have not yet configured SSH access.

```
ssh admin@<vspot_host_os_public_ip>
admin@vspotappliance:~$ spot enter
```

2. Shut down all the running services other than Mongod server.

NOTE Keep the Mongod server process up and running.

```
root@vspot:~# stop rk-venue
root@vspot:~# stop resque
root@vspot:~# service nginx stop
```

3. Exit from the docker container and return to the vSPoT host operating system (Host OS).

Backup the MongoDB

Backup the MongoDB data directory and clean the existing MongoDB data directory contents with the following steps.

1. From vSPoT Host OS, enter the container and download the scripts *vspot_venue_dump.sh* and *vspot_venue_restore.sh* from Ruckus vSPoT AWS S3 migration_scripts, and give the scripts execution rights.

```
admin@vspotappliance:~$ spot enter
root@vspot:~# wget -O /storage/vspot_venue_dump.sh
https://s3-us-west-2.amazonaws.com/ruckuslbs/public/vspot/vspot_venue_dump.sh
root@vspot:~# wget -O /storage/vspot_venue_restore.sh
https://s3-us-west-2.amazonaws.com/ruckuslbs/public/vspot/vspot_venue_restore.sh
root@vspot:~# wget -O /usr/bin/mongodump32
https://s3-us-west-2.amazonaws.com/ruckuslbs/public/vspot/mongodump32
root@vspot:~# chmod +x
/storage/{vspot_venue_dump.sh,vspot_venue_restore.sh}
/usr/bin/mongodump32
```

2. Backup the MongoDB data for a specified venue (example *rksg-dev*) by using the below procedure.

NOTE If you have more than one venue to migrate, repeat this step for each venue as per your list of Venue Identifiers on page 66.

```
root@vspot:~# bash /storage/vspot_venue_dump.sh rksg-dev
--full-dump
```

```
Response:
THIS SCRIPT MUST BE RUN IN vSPoT docker container!
IT IS MEANT TO DO A vSPoT MongoDB and radio maps dump for
a vSPoT data migration purpose!
+ '[' '!' -f /etc/envvars ']'
+ source /etc/envvars

Creating /storage/venue_dump/dump_mongo and
/storage/venue_dump/dump_radio_maps directories ...
```

```
DONE.

Proceed to dump groups ...
+ /usr/bin/mongodump32 --gzip --port 27017 --db
rk-system_production --query '{'\''_id'\'':
ObjectId("562677639180054fd7000002")}' --collection groups
 --out /storage/venue_dump/dump_mongo
2016-07-26T14:52:43.841+0800    writing
rk-system_production.groups to
2016-07-26T14:52:43.843+0800    done dumping
rk-system_production.groups (1 document)

DONE.

Proceed to dump venue rksg-dev ...
+ /usr/bin/mongodump32 --gzip --port 27017 --db
rk-system_production --query '{'\''_id'\'':
'\''rksg-dev'\''}' --collection venues --out
/storage/venue_dump/dump_mongo
2016-07-26T14:52:43.862+0800    writing
rk-system_production.venues to
2016-07-26T14:52:43.863+0800    done dumping
rk-system_production.venues (1 document)

DONE.

Proceed to dump venue rksg-dev access_points ...
2016-07-26T15:09:20.821+0800
rk-system_production.impressions  28173377
2016-07-26T15:09:21.962+0800
rk-system_production.impressions  28285371
2016-07-26T15:09:21.963+0800    done dumping
rk-system_production.impressions (28285371 documents)

DONE.

Analytics data dump completed DONE.

Copying radio maps for rksg-dev into
/storage/venue_dump/dump_radio_maps ...
+ cp -rpfv /opt/spot/system/private/venues/rksg-dev
/storage/venue_dump/dump_radio_maps
`/opt/spot/system/private/venues/rksg-dev' ->
`/storage/venue_dump/dump_radio_maps/rksg-dev'
`/opt/spot/system/private/venues/rksg-dev/foreground_maps'
 -
`/storage/venue_dump/dump_radio_maps/rksg-dev/foreground_maps'

DONE.
+ cd /storage/venue_dump

Creating gzip tarball at /storage/rksg-dev_dump.tar.gz of
above mongodumps and radio maps ...
```

```
+ tar -zcvf /storage/rksg-dev_dump.tar.gz dump_mongo
dump_radio_maps
dump_mongo/
dump_mongo/rk-system_production/
dump_mongo/rk-system_production/groups.metadata.json.gz

dump_radio_maps/rksg-dev/radio_maps/56383dbb3d6ae907d7000012/floor_6.png
dump_radio_maps/rksg-dev/radio_maps/56383dbb3d6ae907d7000012/floor_3.png
dump_radio_maps/rksg-dev/radio_maps/56383dbb3d6ae907d7000012/floor_6_annotated.png

DONE.
Deleting mongodumps and radio maps dump temp dir
/storage/venue_dump ...
+ rm -rf /storage/venue_dump
+ ls -alrth /storage/rksg-dev_dump.tar.gz
-rw-r--r-- 1 root root 919M Jul 26 15:10
/storage/rksg-dev_dump.tar.gz

ALL DONE.
```

3. Verify the existence of non-empty archive file.

```
root@vspot:~#ls -lah /storage/rksg-dev_dump.tar.gz
```

Remove Redis Append Only File (AOF)

Upgraded version of vSPoT does not use Redis AOF.

1. This must be removed to prevent data corruption during Redis server startup by executing the following command:

```
admin@vspotappliance:~$ sudo rm -f
/storage/redis/data/rk_venue.aof
```

2. Exit and return to the vSPoT Host OS.

Prepare the Existing MongoDB Data Directories

Prepare existing MongoDB data directories by executing the following commands.

1. From vSPoT Host OS, enter vSPoT docker container and stop the MongoDB server process.

```
admin@vspotappliance:~$ spot enter
root@vspot:~# service mongod stop
```

2. Prepare a new MongoDB data directory from the vSPoT docker container and a new working directory.

```
root@vspot:~# mv /storage/mongo /storage/mongo24
root@vspot:~# mkdir -p /storage/mongo/{data,log}
root@vspot:~# chown mongod:mongod -R /storage/mongo
```

3. Exit back to vSPoT Host OS and shut down vSPoT docker container.

```
admin@vspotappliance:~$ spot stop 244
```

Detach Storage from vSPoT

From vSphere user interface, detach the storage volume for the current VM running vSPoT version 2.4.4.

CAUTION! Do not delete the detached storage volume.

Install and Import the vSPoT 3.x VM Image

Install and import the VMDK image into your existing vSphere.

The procedure is similar to that described in vSPoT on VMware Upgrade from Version 3.x to Latest on page 59 but keep in mind that this installation is for vSPoT 3.x.

Attach Storage to vSPoT

From vSphere user interface, attach the storage volume to the current VM running the installed vSPoT 3.x.

Start vSPoT 3.x

Start the vSPoT 3.x VM after the storage volume has been successfully attached.

Migrate Data to New Storage Engine Format

Migrate MongoDB data to be compatible with the new storage engine used in vSPoT 3.x by following the below procedure.

1. Check vSPoT 3.x docker container is running by running the command:

```
admin@vspotappliance:~$ spot list
```

2. Shut down all the running services other than Mongod server.

```
root@vspot:~# systemctl stop rk-venue.target
root@vspot:~# systemctl stop resque.target
root@vspot:~# service nginx stop
root@vspot:~# service redis-rk_venue stop
root@vspot:~# service redis-rk_system stop
root@vspot:~# service mosquitto stop
```

3. Check that all processes that was stopped in the above step have been terminated

```
#The following should not return any lines
```

```
root@vspot:~# ps -ef | grep  -E 'ruby|redis|mosquitto|nginx'
 | grep -v grep

# If any process is returned, repeat the commands to shutdown
 the respective process.
```

Restore the Data

Restore the MongoDB data with the following steps.

1. Enter the Docker container

```
admin@vspotappliance:~$ spot enter
```

2. Run the data restore script to first restore the MongoDB data, then subsequently create database indexes.

NOTE This may take a long time to complete, based on the migration data set.

```
root@vspot:~# bash /storage/vspot_venue_restore.sh
/storage/rksg-dev_dump.tar.gz
```

NOTE If you had previously exported more than one venue, you will need to repeat this data restore step for each venues as per your list of venue identifiers.

Response

```
> THIS SCRIPT MUST BE RUN IN vSPoT docker container!
> .
> ONLY A MongoDB and radio maps restore from a valid vSPoT
 venue dump will be performed from
/storage/rksg-dev_dump.tar.gz file.
> .
> ADDITIONAL MONGODB DATA CHANGES MUST BE PERFORMED FOR AN
 AWS SPoT to vSPoT data restoration!
> .
> .
> Deleting any previous /storage/venue_dump dir and
contents...
> + rm -rf /storage/venue_dump
> .
> DONE.
> + cd /storage
> + '[' -f /storage/rksg-dev_dump.tar.gz ']'
> + mkdir -p /storage/venue_dump
> .
> Exploding /storage/rksg-dev_dump.tar.gz into
/storage/venue_dump ...
> + tar -zxvf /storage/rksg-dev_dump.tar.gz -C
/storage/venue_dump
> dump_mongo/
```

```
> dump_mongo/rk-system_production/
> dump_mongo/rk-system_production/groups.metadata.json.gz
> dump_mongo/rk-system_production/visits.metadata.json.gz
> dump_mongo/rk-system_production/locations.bson.gz
> .
> .
> dump_mongo/rk-system_production/groups.bson.gz
>
dump_mongo/rk-system_production/access_points.metadata.json.gz
> dump_radio_maps/
> dump_radio_maps/rksg-dev/
> dump_radio_maps/rksg-dev/foreground_maps/
>
dump_radio_maps/rksg-dev/foreground_maps/pPEVNY51Jtutq2vW8Yxq2w.png
>
dump_radio_maps/rksg-dev/foreground_maps/hjiaM6CtqdqMBLb96YkxqA.jpg
> .
> .
>
dump_radio_maps/rksg-dev/radio_maps/56383dbb3d6ae907d7000012/floor_6_annotated.png
> .
> DONE.
> .
> Restoring DB data dump ...
> + mongorestore --gzip --port 27017 --noIndexRestore
/storage/venue_dump/dump_mongo
> 2016-07-26T16:11:54.938+0800    building a list of dbs
and collections to restore from
/storage/venue_dump/dump_mongo dir
> 2016-07-26T16:11:54.940+0800    reading metadata for
rk-system_production.visits from
/storage/venue_dump/dump_mongo/rk-system_production/visits.metadata.json.gz
> .
> .
> 2016-07-26T16:26:54.940+0800    [########################]
       rk-system_production.visits  4.2 GB/393.5 MB
(1100.9%)
> 2016-07-26T16:26:54.940+0800    [########################]
  rk-system_production.impressions  7.4 GB/267.1 MB
(2848.0%)
> 2016-07-26T16:26:54.940+0800
> 2016-07-26T16:26:57.356+0800    [########################]
  rk-system_production.impressions  7.4 GB/267.1 MB
(2853.7%)
> 2016-07-26T16:26:57.356+0800    no indexes to restore
> 2016-07-26T16:26:57.356+0800    finished restoring
rk-system_production.impressions (28285371 documents)
> 2016-07-26T16:26:57.939+0800    [########################]
  rk-system_production.visits  4.2 GB/393.5 MB  (1104.0%)
> .
> .
> 2016-07-26T16:48:15.702+0800    [########################]
  rk-system_production.visits  7.9 GB/393.5 MB  (2062.0%)
```

```
> 2016-07-26T16:48:15.702+0800    no indexes to restore
> 2016-07-26T16:48:15.702+0800    finished restoring
rk-system_production.visits (28138897 documents)
> 2016-07-26T16:48:15.702+0800    done
> .
> DONE.
> + cd /opt/spot/system
> .
> Create indexes for Analytics DB ...
> + bundle exec rake mi:create_indexes
> Run options: --seed 10490
> # Running:
> .
> Finished in 0.002529s, 0.0000 runs/s, 0.0000 assertions/s.
> 0 runs, 0 assertions, 0 failures, 0 errors, 0 skips
> .
> DONE.
> .
> Restoring radio maps dump ...
> + cp -rpfv /storage/venue_dump/dump_radio_maps/rksg-dev
/opt/spot/system/private/venues/
>
`/storage/venue_dump/dump_radio_maps/rksg-dev/foreground_maps/xIhaFqAniklXPImRY1dewg.png'
 ->
`/opt/spot/system/private/venues/rksg-dev/foreground_maps/xIhaFqAniklXPImRY1dewg.png'
> .
> .
>
`/storage/venue_dump/dump_radio_maps/rksg-dev/radio_maps/56383dbb3d6ae907d7000012/venue.svg'
 ->
`/opt/spot/system/private/venues/rksg-dev/radio_maps/56383dbb3d6ae907d7000012/venue.svg'
>
`/storage/venue_dump/dump_radio_maps/rksg-dev/radio_maps/56383dbb3d6ae907d7000012/floor_3_inside.png'
 ->
`/opt/spot/system/private/venues/rksg-dev/radio_maps/56383dbb3d6ae907d7000012/floor_3_insid
e.png'
> .
> DONE.
> .
> ALL DONE.
root@vspot:~#
```

Verify Successful Migration

Start the required services for verification.

```
root@vspot:~# service mosquitto start
root@vspot:~# service redis-rk_venue start
root@vspot:~# service redis-rk_system start
root@vspot:~# service nginx start
```

View and validate application state from http://<vSPoT VM IP>:8443. Check the application version, and its ability to login to vSPoT version 3.x administration dashboard using a valid user account and admin account.

Start Data Services

Start the data services and background services.

```
root@vspot:~# systemctl start rk-venue.target
root@vspot:~# systemctl start resque.target
```

NOTE This will begin to receive live data from the access points.

From the Admin pages, validate the data presence of radio maps, access points, venues, etc. From the analytics page, verify real-time and historical data (heat maps and daily visit counts).

Clean Directories and Backup Snapshots

After successfully migrating to vSPoT version 3.x follow the below procedure

1. Clean the earlier database directory by running the below command.

```
admin@vspotappliance:~$ sudo rm -fr /storage/mongo24
```

2. Exit to vSPoT Host OS and from VMWare vCenter web interface.
3. You may want to delete or cleanup your VMWare snapshots after you have ascertained that the upgrade is successful. You may no longer need to revert to the previous version of vSPoT VM.

Re-Import vSPoT License File

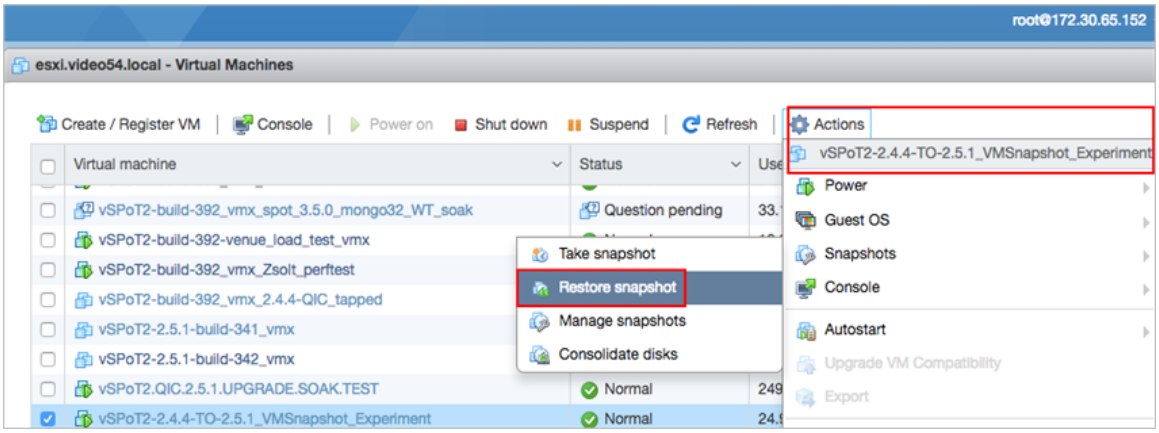
Re-import the vSPoT license to get the full working license purchased for your vSPoT instance.

Procedure to Restore VMWare Snapshots (Optional)

Follow the below procedure to restore the vSPoT backup.

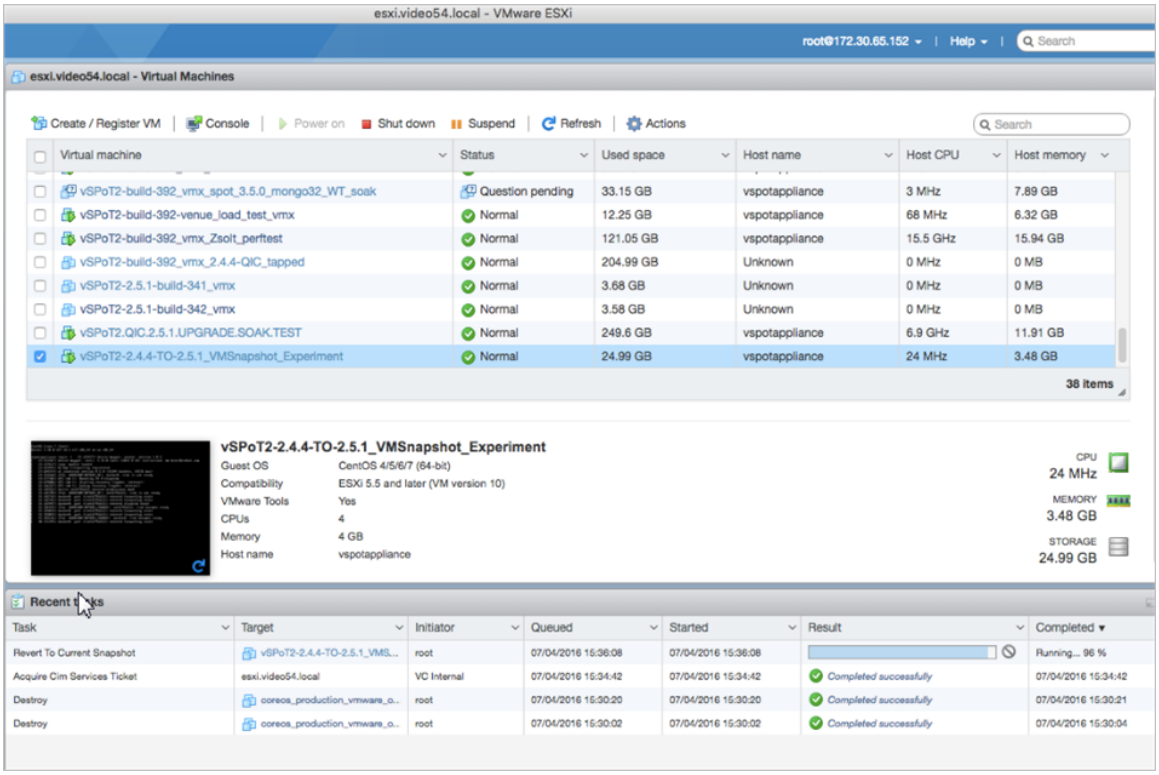
1. Login to the vSPoT vCenter.
2. Using the VMWare ESXi web interface navigate to select **Virtual Machines > VMware** backup instance for restoration. Ensure that the backup is a good valid working snapshot.
3. In the tab menu navigate to select **Actions > Snapshots > Restore snapshot.**

Figure 39: Selecting Restore Snapshot Option



4. To start the restore click the **Restore** button in the pop-up confirmation window.
5. Check the state of the snapshot restoration from the **Recent tasks** panel at the bottom panel. Your vSPoT restored instance should be up and running on successful completion.

Figure 40: View the Restored Snapshot


esxi.video54.local - VMware ESXi
root@172.30.65.152
Help
Search
esxi.video54.local - Virtual Machines
Create / Register VM
Console
Power on
Shut down
Suspend
Refresh
Actions
Search
Virtual machine
Status
Used space
Host name
Host CPU
Host memory
vSPoT2-build-392_vmx_spot_3.5.0_mongo32_WT_soak
Question pending
33.15 GB
vspotappliance
3 MHz
7.89 GB
vSPoT2-build-392-venue_load_test_vmx
Normal
12.25 GB
vspotappliance
68 MHz
6.32 GB
vSPoT2-build-392_vmx_Zsolt_perftest
Normal
121.05 GB
vspotappliance
15.5 GHz
15.94 GB
vSPoT2-build-392_vmx_2.4.4-QIC_tapped
Normal
204.99 GB
Unknown
0 MHz
0 MB
vSPoT2-2.5.1-build-341_vmx
Normal
3.68 GB
Unknown
0 MHz
0 MB
vSPoT2-2.5.1-build-342_vmx
Normal
3.58 GB
Unknown
0 MHz
0 MB
vSPoT2.QIC.2.5.1.UPGRADE.SOAK.TEST
Normal
249.6 GB
vspotappliance
6.9 GHz
11.91 GB
vSPoT2-2.4.4-TO-2.5.1_VMSnapshot_Experiment
Normal
24.99 GB
vspotappliance
24 MHz
3.48 GB
38 items
vSPoT2-2.4.4-TO-2.5.1_VMSnapshot_Experiment
Guest OS
CentOS 4/5/6/7 (64-bit)
Compatibility
ESXi 5.5 and later (VM version 10)
VMware Tools
Yes
CPUs
4
Memory
4 GB
Host name
vspotappliance
CPU
24 MHz
MEMORY
3.48 GB
STORAGE
24.99 GB
Recent tasks
Task
Target
Initiator
Queued
Started
Result
Completed
Revert To Current Snapshot
root
07/04/2016 15:36:08
07/04/2016 15:36:08
Running... 96 %
Acquire Cim Services Ticket
esxi.video54.local
VC Internal
07/04/2016 15:34:42
07/04/2016 15:34:42
Completed successfully
07/04/2016 15:34:42
Destroy
root
07/04/2016 15:30:20
07/04/2016 15:30:20
Completed successfully
07/04/2016 15:30:21
Destroy
root
07/04/2016 15:30:02
07/04/2016 15:30:02
Completed successfully
07/04/2016 15:30:04

vSPoT on AWS Upgrade

Virtual SPoT in AWS can be upgraded with the following steps for version 2.4.4 to 3.x latest.

CAUTION! This upgrade process will result in application downtime due to the need for data migration across different and incompatible storage engines. During the migration process, vSPoT should not be running, otherwise data could be lost during migration.

Prerequisite

You are required to get full administration access to AWS billing account and management console.

Upgrade Procedure

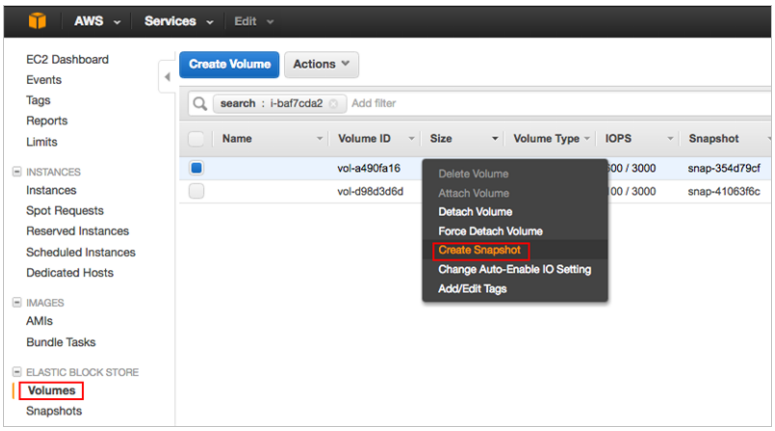
The following are the steps for upgrading vSPoT in AWS for version 2.4.4 to 3.x.

Backup the Current vSPoT

This section describes the procedure to backup the current vSPoT.

1. Login to the AWS EC2 management console and obtain the identifier **INSTANCE ID** of your vSPoT instance, which is in the format *i-ffffffff*.
2. Navigate to **Elastic Block Store** > **Volumes** to search for volumes using the identifier **INSTANCE ID** obtained in Step 1. In this example, the identifier is *i-baf7cda2*.

Figure 41: Create Snapshot



3. Select the vSPoT instance and right-click to select **Create Snapshot**.
4. After snapshot creation is triggered, the process will run in the background. You can proceed to the next step.

Venue Identifiers

After a successful backup of the vSPoT instance, ensure you have an updated list of Venue identifiers. This is required during migration.

Download vSPoT 3.x Template

Download the latest **Ruckus vSPoT Software Release** template for AWS from (https://support.ruckuswireless.com)

Figure 42: Download Details

Stop vSPoT Server

Stop the existing server running vSPoT version 2.4.4 by using the following CLI commands.

NOTE Ensure you have the IP address and SSH private key file for accessing your AWS EC2 instance.

---

1. Refer to Accessing vSPoT using AWS CLI on page 32 to login using SSH to the vSPoT AWS EC2 instance host operating system (Host OS). Enter the vSPoT docker container.

```
ssh centos@IP_ADDR -i $SSH_PRIVATE_KEY_FILE
centos@ip-addr:~$ spot enter
```

2. Shut down all the running services other than Mongod server.

```
root@vspot:~# stop rk-venue
root@vspot:~# stop resque
root@vspot:~# service nginx stop
```

Backup the MongoDB

Backup the MongoDB data directory and clean the existing MongoDB data directory contents with the following steps.

1. From the vSPoT docker container, download the Ruckus vSPoT AWS S3 migration scripts, and give it execution rights..

```
admin@vspotappliance:~$ spot enter
root@vspot:~# wget -O /storage/vspot_venue_dump.sh
https://s3-us-west-2.amazonaws.com/ruckuslbs/public/vspot/vspot_venue_dump.sh
root@vspot:~# wget -O /storage/vspot_venue_restore.sh
https://s3-us-west-2.amazonaws.com/ruckuslbs/public/vspot/vspot_venue_restore.sh
root@vspot:~# wget -O /usr/bin/mongodump32
https://s3-us-west-2.amazonaws.com/ruckuslbs/public/vspot/mongodump32
root@vspot:~# chmod +x
/storage/{vspot_venue_dump.sh,vspot_venue_restore.sh}
/usr/bin/mongodump32
```

2. Backup the MongoDB data for a specified venue (example *rksg-dev*) by using the below procedure.

NOTE If you have more than one venue to migrate, repeat this step for each venue as per your list of Venue Identifiers on page 66.

```
root@vspot:~# bash /storage/vspot_venue_dump.sh rksg-dev
--full-dump
```

3. Verify the existence of non-empty archive file.

```
root@vspot:~#ls -lah /storage/rksg-dev_dump.tar.gz
```

Remove Redis Append Only File (AOF)

Upgraded version of vSPoT does not use Redis AOF.

1. This must be removed to prevent data corruption during Redis server startup by executing the following command:

```
root@vspot:~# rm -f /storage/redis/data/rk_venue.aof
```

Prepare the Existing MongoDB Data Directories

Prepare existing MongoDB data directories by executing the following commands.

1. From vSPoT Host OS, enter vSPoT docker container and stop the MongoDB server process.

```
admin@vspotappliance:~$ spot enter
root@vspot:~# service mongod stop
```

2. Prepare a new MongoDB data directory from the vSPoT docker container and a new working directory.

```
root@vspot:~# mv /storage/mongo /storage/mongo24
root@vspot:~# mkdir -p /storage/mongo/{data,log}
root@vspot:~# chown mongod:mongod -R /storage/mongo
```

3. Exit back to vSPoT Host OS and shut down vSPoT docker container.

```
admin@vspotappliance:~$ spot stop 244
```

Remove vSPoT 2.4.4. Stack Template

CAUTION! Do not delete the detached storage volume from AWS EC2 management console.

1. Refer to Deleting vSPoT on AWS on page 35 to remove the vSPoT 2.4.4 stack. This will also detach the storage volume. Do make a note of the storage volume identifier for later use.

Create a new EC2 Instance with vSPoT 3.x Stack Template

To create a new EC2 instance:

1. Refer to Automated Setup using CloudFormation on page 25 to install vSPoT 3.x using the vSPoT 3.x stack template downloaded . You will also need to specify the StorageVolumeId field as seen in the figure below. The identifier is in the format of *vol-ffffffff* or *vol-ffffffffffffffff*.

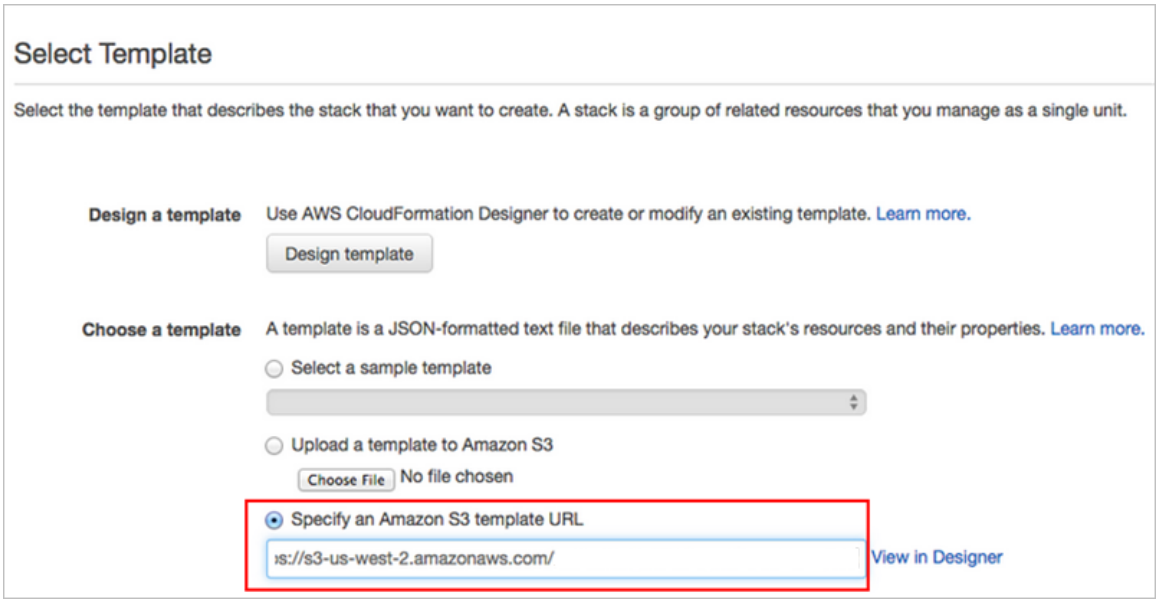


Figure 43: Specifying Options in the Template

Migrate Data to New Storage Engine Format

Migrate MongoDB data to be compatible with the new storage engine used in vSPoT 3.x by following the below procedure.

1. Check vSPoT 3.x docker container is running by running the command:

```
centos@ip-addr:~$ spot list
```

2. Shut down all the running services other than Mongod server.

```
centos@ip-addr:~# spot enter
root@vspot:~# systemctl stop rk-venue.target
root@vspot:~# systemctl stop resque.target
root@vspot:~# service nginx stop
root@vspot:~# service redis-rk_venue stop
root@vspot:~# service redis-rk_system stop
root@vspot:~# service mosquitto stop
```

3. Check that all processes that was stopped in the above step have been terminated.

```
root@vspot:~# ps -ef | grep -E 'ruby|redis|mosquitto|nginx'
 | grep -v grep
```

NOTE If any process is returned, repeat the commands to shutdown the processes.

Restore the Data

Restore the MongoDB data with the following steps.

1. Run the data restore script to first restore the MongoDB data, then subsequently create database indexes.

NOTE This may take a long time to complete, based on the migration data set.

```
root@vspot:~# bash /storage/vspot_venue_restore.sh
/storage/rksg-dev_dump.tar.gz
```

NOTE If you had previously exported more than one venue, you will need to repeat this data restore step for each venues as per your list of venue identifiers.

Verify Successful Migration

Start the required services for verification.

```
root@vspot:~# service mosquitto start
root@vspot:~# service redis-rk_venue start
```

```
root@vspot:~# service redis-rk_system start
root@vspot:~# service nginx start
```

View and validate application state from http://<vSPoT VM IP>:8443. Check the application version, and its ability to login to vSPoT version 3.x administration dashboard using a valid user account and admin account.

Start Data Services

Start the data services and background services.

```
root@vspot:~# systemctl start rk-venue.target
root@vspot:~# systemctl start resque.target
```

NOTE This will begin to receive live data from the access points.

From the Admin pages, validate the data presence of radio maps, access points, venues, etc. From the analytics page, verify real-time and historical data (heat maps and daily visit counts).

Clean Directories and Backup Snapshots

After successfully migrating to vSPoT version 3.x follow the below procedure.

1. Clean the earlier database directory by running the below command.

```
admin@vspotappliance:~$ sudo rm -fr /storage/mongo24
```

2. Exit from the SSH terminal session.
3. You may want to delete or cleanup your EC2 EBS snapshots after you have ascertained that the upgrade is successful and you may no longer need to revert to the previous version of vSPoT VM.

Re-Import vSPoT License File

Re-import the vSPoT license to get the full working license purchased for your vSPoT instance.

Rolling Upgrade for vSPoT 3.x to latest

The rolling upgrade functionality provides a simplified and faster application upgrade procedure for an existing vSPoT deployment.

This feature removes the need for any post-configuration steps. For example, IP address or NTP server configuration for a vSPoT upgrade. For example, IP address or NTP server configuration for a vSPoT upgrade.

NOTE Rolling upgrades was introduced from 2.4.0 release and continues to 3.x. and later releases.

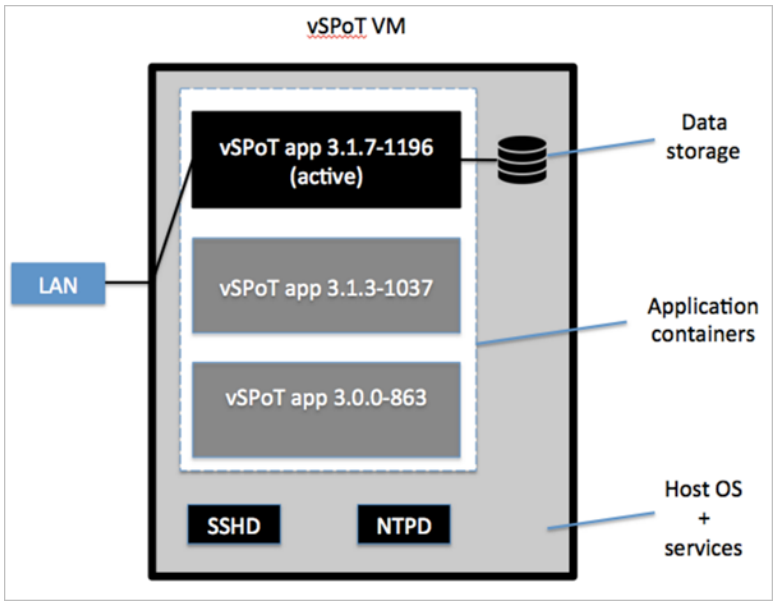
This procedure can be used to upgrade vSPoT 3.x to the latest version of vSPoT. However, if you are upgrading from vSPoT 2.4.0 to vSPoT 3.x, Ruckus Wireless highly recommends that you perform a Full Upgrade on page 58 to take advantage of the security and performance improvements to the Host OS.

NOTE To upgrade to vSPoT 3.2, perform a full upgrade.

vSPoT Architecture

From 2.4.x releases, the new vSPoT internal architecture (as seen in the figure below) relies on docker container technology, which provides a means to decouple the virtual machine (VM) runtime environment from the vSPoT application. Each vSPoT application version is distributed as a separate container image and additional CLI tools are provided to enable switching between different vSPoT application versions. Due to network and storage configurations, at any given time only one application version can be active or running within a single vSPoT VM.

Figure 44: vSPoT VM Architecture



Prerequisites

The following are the prerequisites for using rolling upgrade.

- This upgrade procedure works with vSPoT version 2.4.0 and higher.
- This procedure is a CLI based solution, which requires a console or SSH access to the vSPoT VM.
- The license file needs to be uploaded after every upgrade.

Upgrade Procedure

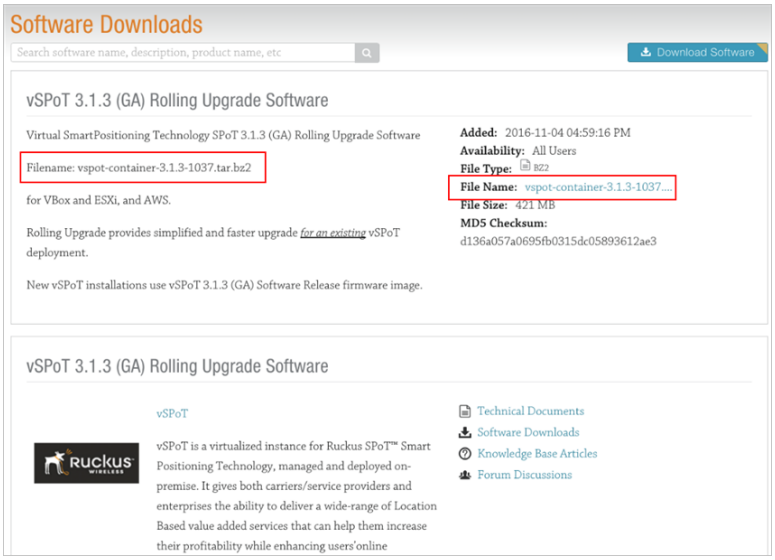
Ensure you have a running vSPoT instance and follow these steps to upgrade vSPoT.

1. Login to the vSPoT console (see: Using the CLI Console on page 56). SSH to the vSPoT host operating system (Host OS) using the below command.

```
ssh admin@<vspot_host_os_public_ip>
```

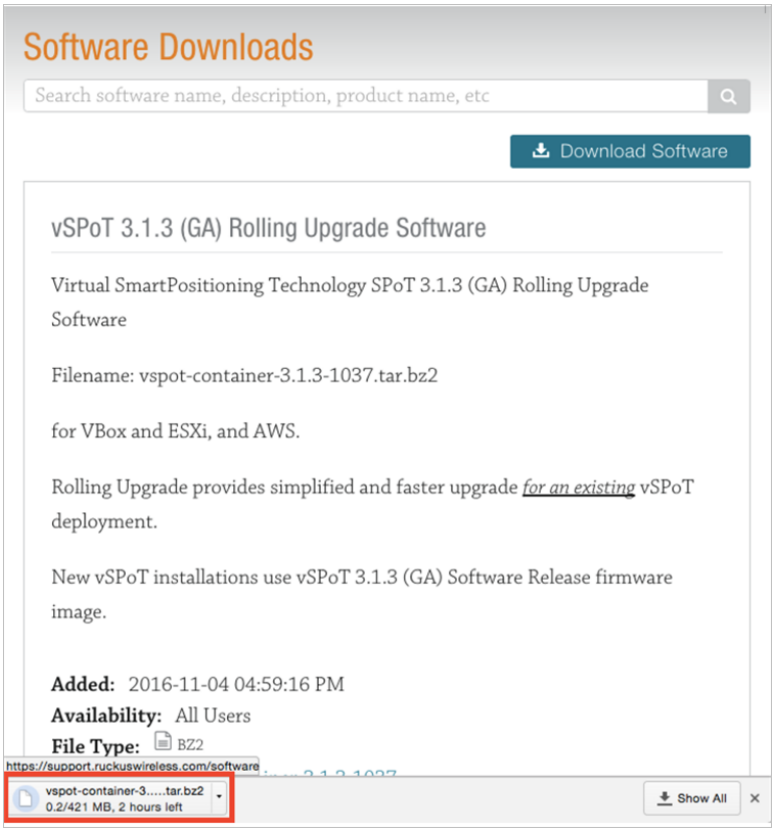
2. Logout from the vSPoT web application.
3. Navigate to the Ruckus support website https://support.ruckuswireless.com/ to obtain the download URL for the vSPoT application bundle
   a. Login in with your user credentials (login name and password)
   b. Navigate to vSPoT download section to locate the download URL for the application bundle image. For example, rolling upgrade for vSPoT 3.1.3 requires *${APPLICATION_BUNDLE_FILE} 'vspot-container-3.1.3-1037.tar.bz2* as seen in the figure below.

Figure 45: File Location



4. Click on the file name or the **Download Software** button to begin the application bundle download. Depending on your web browser, the download progress indicator will show up in the lower left corner, or appear as a pop-up window.

Figure 46: Software Download

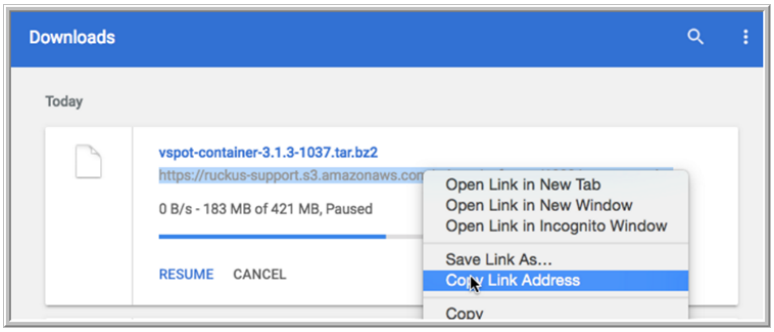


5. Transfer the application bundle to your vSPoT instance. There are two possible approaches:

   a. **Option A**, If your vSPoT instance has Internet access

      a. Open your web browser's download manager. You will see the download in progress.

      Figure 47: Download Progress



b. Right-click on the download URL and select **Copy Link Address** from the pop-up menu.
c. In a terminal console within the vSPoT Host OS, use the *wget* command and paste the download URL (using *Ctrl+V* or *Cmd+V*) within single-quotes. This will download the application bundle from within vSPoT Host OS.

```
admin@vspotappliance:~$ wget '${FILE_DOWNLOAD_URL}'
```

```
The FILE_DOWNLOAD_URL should look similar to:
'https://ruckus-support.s3.amazonaws.com/private/software/931/
vspot-container-3.1.3-1037.tar.bz2?AWSAccessKeyId=AKIAJM3QLNNK-
LOV235TQ&Expires=1464965029&Signature=k9LS0cENQ5ooDa9HWW-
mPEdgGSr0%3D'
```

NOTE The download URL needs to be placed within single quotes in the command line. An incorrect download URL will result in a '403 Forbidden' error.

NOTE As a security feature, the download URL is only valid for the next 15 minutes from the time of starting the download. You should download the application bundle immediately.

If you encounter an expiry notification, you will need to restart the download process from Step 4, which is to press the *Download Software* button again to generate a new download URL.

---

b. Option B, If your vSPoT instance does not have Internet access, but your local machine has Internet access

a. Wait for the file download (initiated in Step 4) to complete.
b. Use a file transfer client (SCP or SFTP) to copy the application bundle to your vSPoT instance home directory. If you are using Windows, you can use WinSCP (https://winscp.net)

```
$ scp ${APPLICATION_BUNDLE_FILE} admin@VSPOT_IP_ADDR
```

6. Verify vSPoT application bundle by navigating to the home directory of your vSPoT Host OS. The application bundle file should be present in this directory.
7. Load the vSPoT application image from the new application bundle. This will take quite a few minutes.

```
admin@vspotappliance:~$ spot load ${APPLICATION_BUNDLE_FILE}
```

Figure 48: SPoT Application Image

```
e192ed93fce9: Loading layer [==================================================>] 1.532 GB/1.532 GB
Loaded image: registry.internal.ruckuslbs.com/ruckus/vspot:3.1.3-1037
```

8. Verify vSPoT images by executing the command:

```
admin@vspotappliance:~$ spot images
```

Figure 49: SPoT Images

```
REPOSITORY                                          TAG         IMAGE ID      CREATED       SIZE
registry.internal.ruckuslbs.com/ruckus/vspot   3.1.3-1037   9076f4c70a63  7 days ago    1.463 GB
registry.internal.ruckuslbs.com/ruckus/vspot   3.0.0-863    9cf108e16fd7  5 weeks ago   1.483 GB
```

9. Verify the current running vSPoT application version. This should be lower than the new vSPoT application version that you have just loaded.

```
admin@vspotappliance:~$ spot list
```

Figure 50: SPoT List

```
CONTAINER ID        IMAGE                                                    COMMAND                  CREATED             STATUS
        PORTS                                                                                 NAMES
826e797fda1d        registry.internal.ruckuslbs.com/ruckus/vspot:3.0.0-863   "/bin/sh -c /sbin/ini"   6 minutes ago       Up 6 minutes
        0.0.0.0:80->80/tcp, 0.0.0.0:8442-8443->8442-8443/tcp, 0.0.0.0:8883->8883/tcp   vspot300
```

In this example, the current running vSPoT application version number is 3.0.0-863, and the most recent application version is 3.1.3-1037.

10. Stop the current running vSPoT application by using the application version number.

```
admin@vspotappliance:~$ spot stop 3.0.0-863
```

11. Start the new vSPoT application.

```
admin@vspotappliance:~$ spot start 3.1.3-1037
```

12. Verify the currently running application version.

```
admin@vspotappliance:~$ spot list
```

Figure 51: SPoT List

```
CONTAINER ID        IMAGE                                                    COMMAND                  CREATED             STATUS
        PORTS                                                                                 NAMES
e130d7133493        registry.internal.ruckuslbs.com/ruckus/vspot:3.1.3-1037   "/bin/sh -c /sbin/ini"   7 seconds ago       Up 5 seconds
        0.0.0.0:80->80/tcp, 0.0.0.0:8442-8443->8442-8443/tcp, 0.0.0.0:8883->8883/tcp   vspot313
```

13. Login to the vSPoT web application Administration user interface and upload the licenses.
14. Verify that the new vSPoT application works correctly by ensuring that the:
    a. Access Points on the Administration user interface indicate a green status
    b. Analytics user interface shows real-time heat maps and historical charts such as unique visitors.
15. Delete any outdated vSPoT application images based on the image identifier. In this example, the outdated application image tag is 3.0.0-863 and the image identifier to remove it is 9cf108e16fd7.

```
admin@vspotappliance:~$ docker rmi ${IMAGE_ID}
```

16. Verify the current available application images by executing the command:

```
admin@vspotappliance:~$ spot images
```

Upload and Rollback of Self Signed SSL Certificate

From vSPoT version 3.3 onwards, vSPoT ships with a default temporary unverified SSL certificate for HTTPS support. This section gives you the procedure for replacing the default certificate with a valid CA (Certificate Authority) signed SSL certificate.

For vSPoT installations accessed with FQDN (Fully Qualified Domain Name) or DNS hostname (for example, https://www.vspot.ruckuslbs.com), it is mandatory to update with a C.A. signed SSL certificate corresponding to their domain or sub-domain name. Without a valid SSL certificate for the domain name, it may not be possible to access the vSPoT login page using the FQDN URL. However, you can still access vSPoT using its IP address (for example, https://54.206.20.234).

CAUTION! This upgrade process will restart the *nginx* process, which could cause a system server failure during startup if the certificate related files are invalid or corrupt. Do ensure necessary arrangements are made for required downtime of vSPoT admin dashboard.

Prerequisites

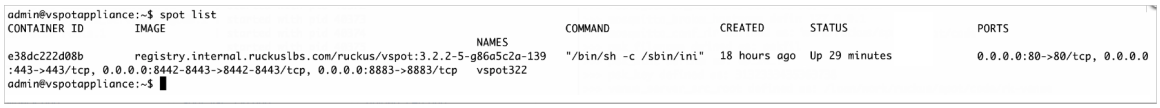
1. Network port 443 needs to be open on the corporate firewall.
2. Valid SSL certificate files (*.key, *.crt) are required.
3. Valid intermediate CA certificates (*.crt) if any.

Update the SSL Certificate

Follow the below steps to update the SSL certificate.

1. Check vSPoT 3.3.x docker container is running by using the below command.

```
admin@vspotappliance:~$ spot list
```



2. If you have a domain SSL certificate with intermediate CA certificates, you would need to merge them as one certificate file using your local machine.

```
 bash:~$ cat vspot.client.com.crt intermediate_ca.crt >
my.crt
```

This merged certificate file (in this example, *my.crt*) should be used as the *.crt file in the next step.

NOTE If the intermediate certificates are not merged with the issued SSL certificate, the trusted-chain certificate might not be established. This means that when users attempt to access the site, errors such as *Security Alert* or *Not Secure* can been seen in the site's certificate chain.

---

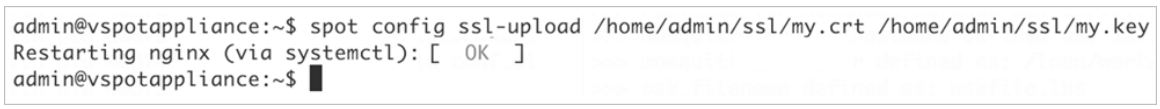
3. From your local machine, copy the SSL certificate files *.key and *.crt file (merged certificate file in case of intermediate CA's) to the vSPoT host machine's home directory. For example, */home/admin/ssl/*.

```
bash:~$ scp my.crt admin@VSPOT_IP_ADDR:/home/admin/ssl

bash:~$ scp my.key admin@VSPOT_IP_ADDR:/home/admin/ssl
```

4. SSH into your vSPoT host machine to run the following command to update the SSL certificate. Ensure the order of the files as per the below example.

```
admin@vspotappliance:~$ spot config ssl-upload
/home/admin/ssl/my.crt /home/admin/ssl/my.key
```

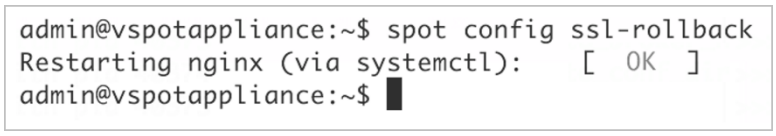


5. Open the vSPoT URL (in this example, https://54.206.20.234) in a web browser to verify whether the *nginx server* is working with the updated certificate.
6. For vSPoT installations accessed with FQDN or DNS hostname (for example, https://www.vspot.ruckuslbs.com), access the domain name in a web browser to verify if the browser accepts the updated SSL certificate as a valid certificate. For example, on Google Chrome it is seen as a green lock icon. Other browser exhibit it differently.
7. You should be able to view the vSPoT login page to login using the user credentials.

Rollback the Updated SSL Certificate

This step is useful in case the updated SSL certificate fails to bring up the vSPoT login page. Run the following command to rollback to the default SSL certificate.

```
admin@vspotappliance:~$ spot config ssl-rollback
```



How to Increase vSPoT Historical Data Collection Capacity

If you need to increase the capacity of vSPoT to store historical data for a longer period of time, you can use the procedure in this section.

If you need to increase the capacity of vSPoT to store historical data for a longer period of time, you can use the following procedure.

Change the Volume Size on the vSPoT Instance

- On VMware Installation
- On AWS Installation

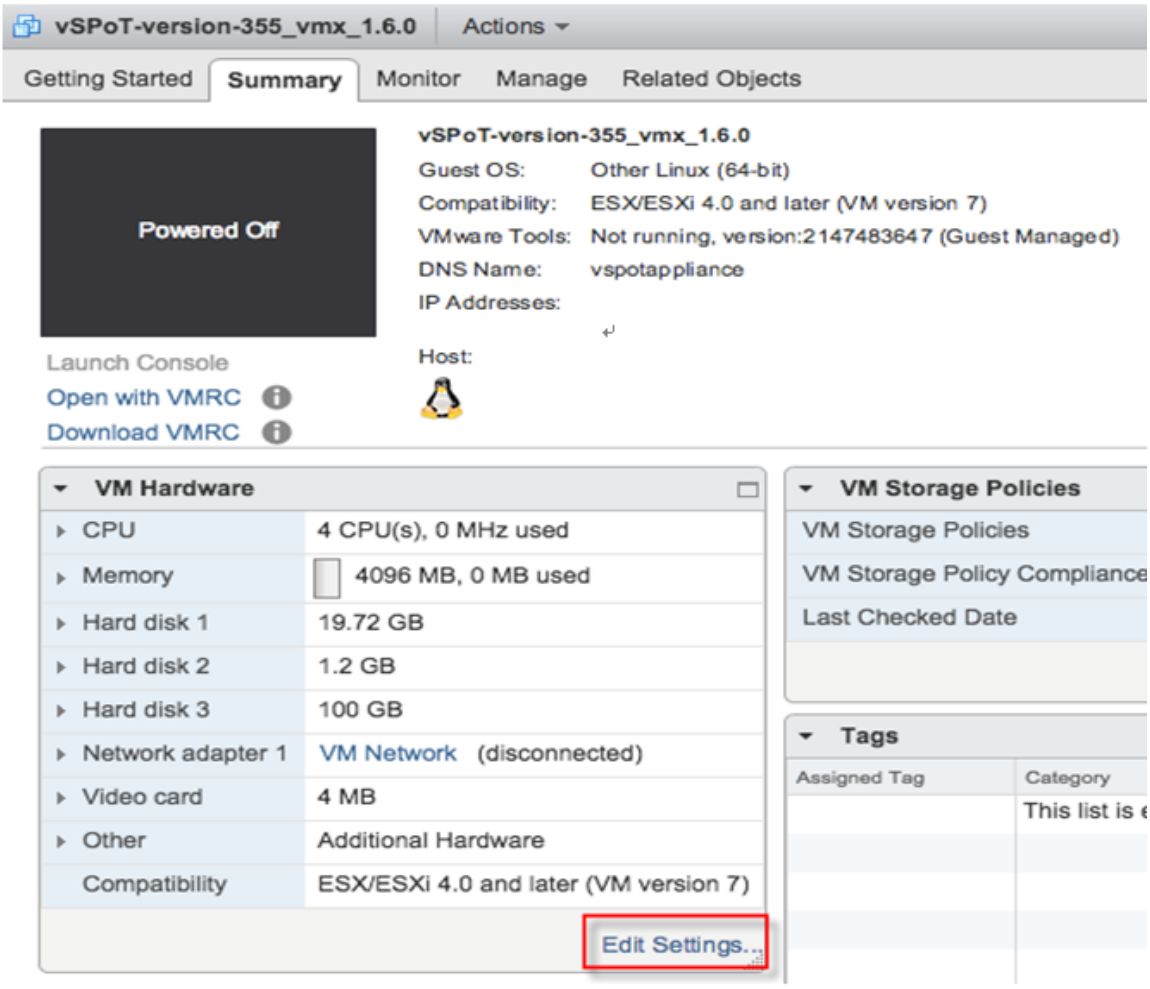
On VMware Installation

1. First, make sure your vSPoT instance is in the power off state (see Initialize shutdown command in case the vSPoT virtual machine is still running).

   Figure 52: Make sure vSPoT is powered off

2. Click the **Edit settings** link.

   Figure 53: Click Edit Settings



3. Select Hard disk 3 and increase the storage size to the desired new size, e.g., 500GB. Please keep in mind that only “grow” operation is available on the storage resize.

Figure 54: Select Hard Disk 3 and choose new storage size

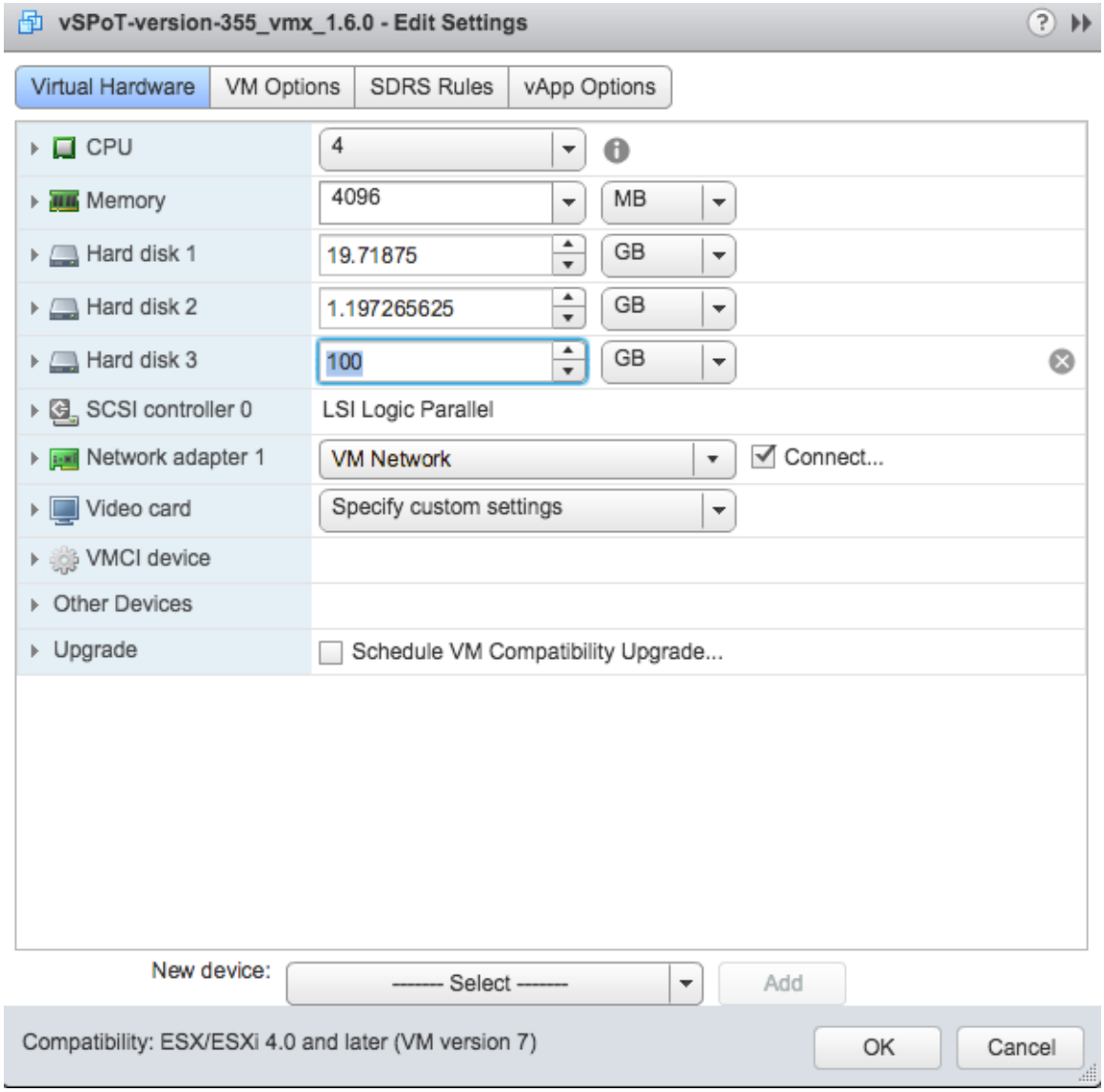
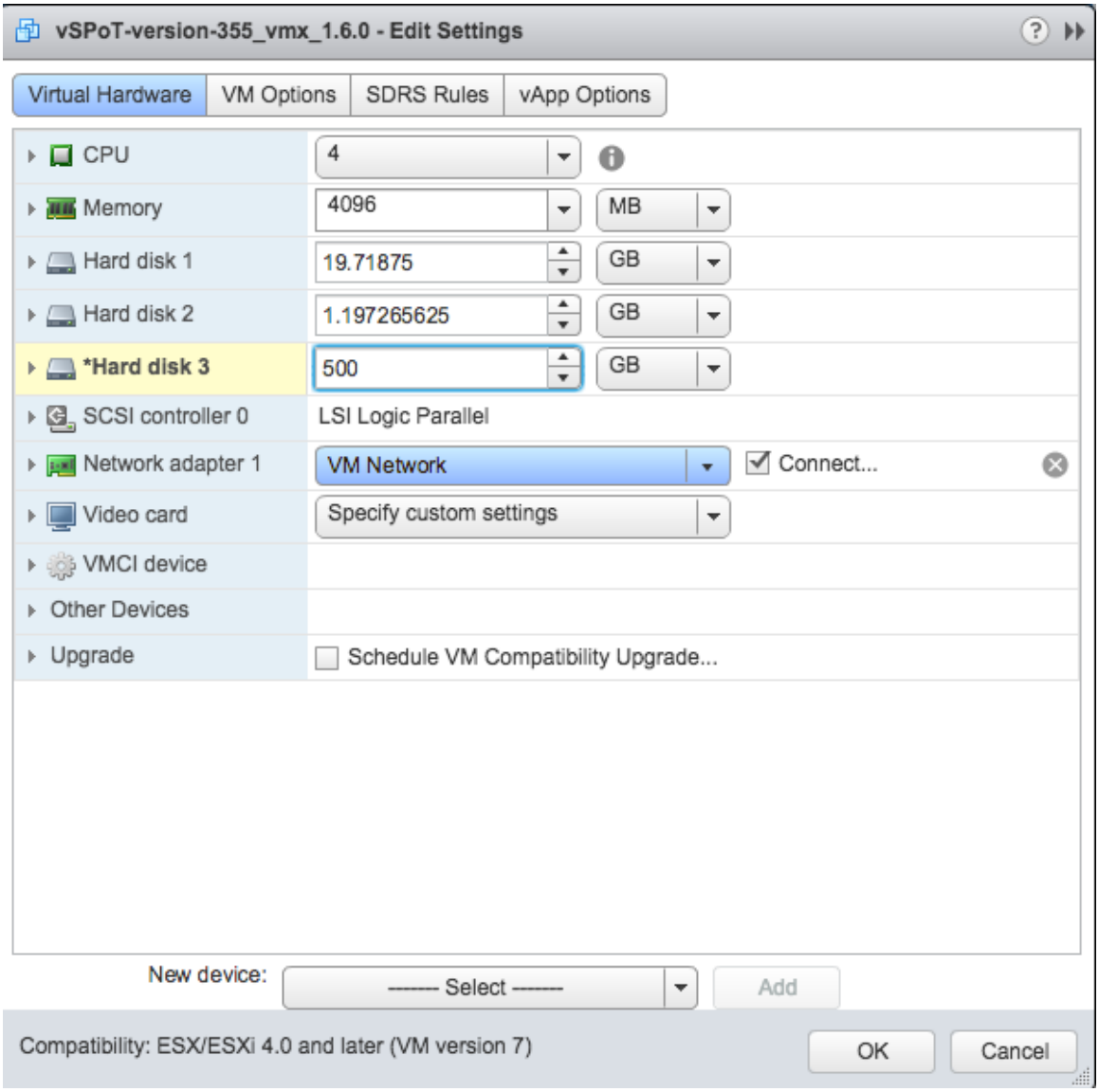
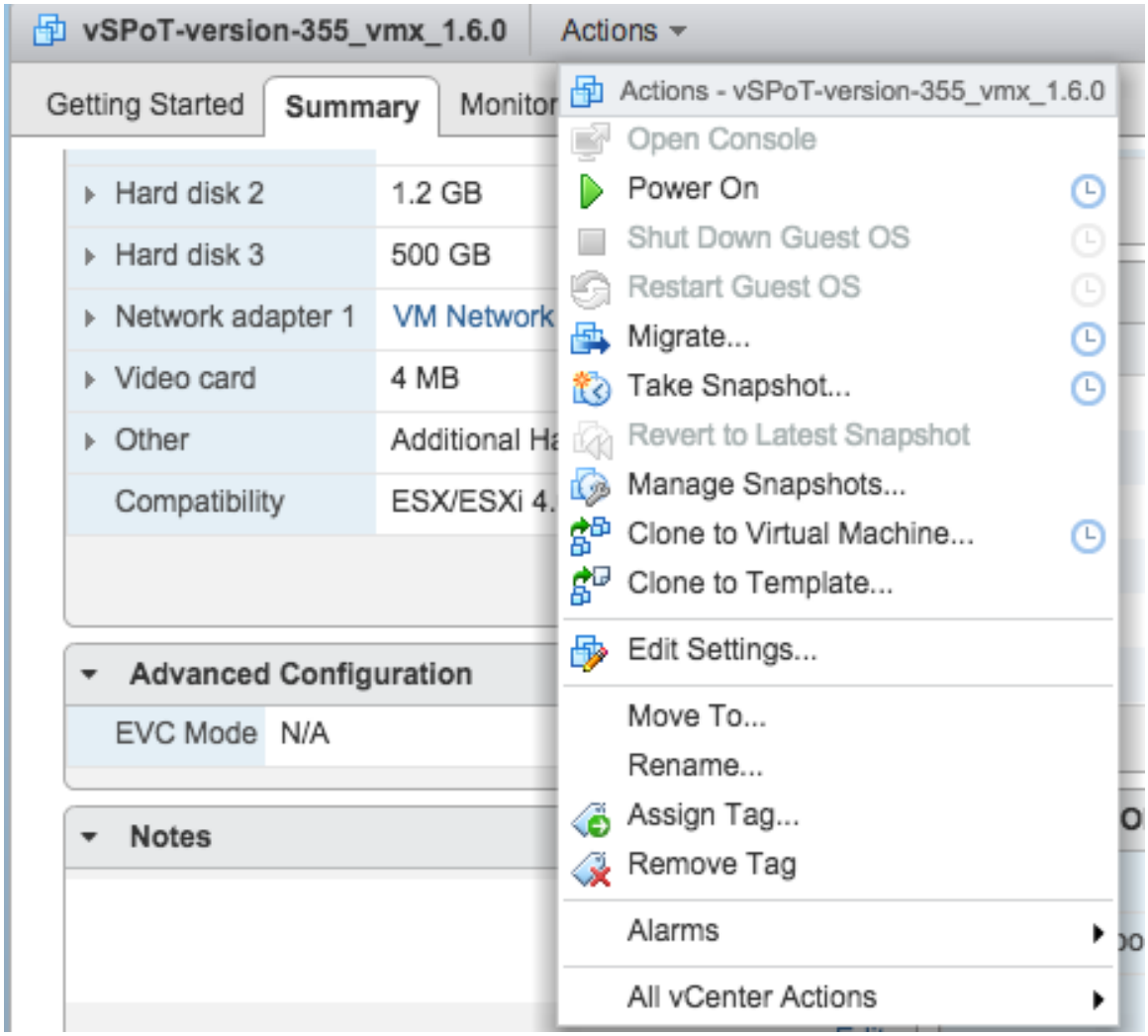


Figure 55: Choose, for example, 500 GB



4. Click **OK**.
5. Power on the virtual machine using the Actions drop-down menu.

Figure 56: Power on the virtual machine



6. Login to the vSPoT CLI. Refer to Accessing vSPoT using CLI
7. Execute the following CLI command

```
admin@vspotappliance:~$ sudo resize2fs /dev/sdc
```

Index

350 West Java Drive, Sunnyvale, CA

www.ruckuswireless.com