

Deployment

Modified on 26 SEP 2017

VMware Validated Design 4.0

VMware Validated Design for Remote Office Branch
Office 4.0



vmware®

You can find the most up-to-date technical documentation on the VMware website at:

<https://docs.vmware.com/>

If you have comments about this documentation, submit your feedback to

docfeedback@vmware.com

VMware, Inc.
3401 Hillview Ave.
Palo Alto, CA 94304
www.vmware.com

Copyright © 2016, 2017 VMware, Inc. All rights reserved. [Copyright and trademark information.](#)

Contents

- 1 About VMware Validated Design Deployment for Remote Office and Branch Office 4**
 - Updated Information 5
- 2 Virtual Infrastructure Implementation in ROBO 6**
 - Install and Configure ESXi Hosts in ROBO 6
 - Deploy and Configure the Virtual Center Components in ROBO 16
 - Deploy and Configure the NSX Instance in ROBO 43
 - Deploy vSphere Data Protection in ROBO 89
- 3 Cloud Management Platform Implementation in ROBO 102**
 - Prerequisites for Cloud Management Platform Implementation in ROBO 102
 - Configure Service Account Privileges in ROBO 103
 - vRealize Automation Installation in ROBO 106
 - vRealize Orchestrator Configuration in ROBO 118
 - vRealize Business Installation in ROBO 119
 - Create Anti-Affinity Rules for vRealize Automation Proxy Agent Virtual Machines in ROBO 127
 - Content Library Configuration in ROBO 127
 - Tenant Content Creation in ROBO 129
- 4 Operations Implementation in ROBO 175**
 - vRealize Operations Manager Implementation in ROBO 175
 - vRealize Log Insight Implementation in ROBO 199
 - vSphere Update Manager Download Service Implementation in ROBO 242

About VMware Validated Design Deployment for Remote Office and Branch Office

1

VMware Validated Design Deployment for VMware Validated Design™ Remote Office and Branch Office provides step-by-step instructions for installing, configuring, and operating a software-defined data center (SDDC) based on the VMware Validated Design for Software-Defined Data Center for use with a remote office and branch office (ROBO).

VMware Validated Design Deployment does not contain step-by-step instructions for performing all of the required post-configuration tasks because they often depend on customer requirements.

Intended Audience

VMware Validated Design Deployment is intended for cloud architects, infrastructure administrators and cloud administrators who are familiar with and want to use VMware software to deploy in a short time and manage an SDDC that meets the requirements for capacity, scalability, backup and restore, and extensibility for disaster recovery support.

Required VMware Software

VMware Validated Design Deployment is compliant and validated with certain product versions. See *VMware Validated Design Release Notes* for more information about supported product versions.

Updated Information

This *Deployment for Remote Office and Branch Office* document is updated with each release of the product or when necessary..

This table provides the update history of the *Deployment for Remote Office and Branch Office* document.

Revision	Description
26 SEPT 2017	■ Added missing number in filename for the command to configure symbolic link between the UMDS and the PostgreSQL. See Configure PostgreSQL Database on Your Linux-Based Host Operating System for UMDS in ROBO .
EN-002520-00	Initial release.

Virtual Infrastructure Implementation in ROBO

2

The virtual infrastructure is the foundation of an operational SDDC, and consists primarily of the physical host's hypervisor and the control of these hypervisors. The management workloads consist of elements in the virtual management layer itself, along with elements in the cloud management layer, service management, business continuity, and security areas.

The following procedures describe the validated flow of installation and configuration for the Virtual Infrastructure for remote office and branch office (ROBO) deployments.

Procedure

1 [Install and Configure ESXi Hosts in ROBO](#)

Start the deployment of the virtual infrastructure in your ROBO location by installing and configuring all the ESXi hosts.

2 [Deploy and Configure the Virtual Center Components in ROBO](#)

Deploy and configure the Virtual Center and cluster components for your remote office and branch office.

3 [Deploy and Configure the NSX Instance in ROBO](#)

Deploy and configure the NSX instance for the consolidated cluster in your ROBO deployment.

4 [Deploy vSphere Data Protection in ROBO](#)

Deploy vSphere Data Protection for backup and restore of SDDC management components in your remote office and branch office (ROBO) deployment.

Install and Configure ESXi Hosts in ROBO

Start the deployment of the virtual infrastructure in your ROBO location by installing and configuring all the ESXi hosts.

Procedure

1 [Prerequisites for Installation of ESXi Hosts in ROBO](#)

Install and configure the ESXi hosts for your ROBO location.

2 [Install ESXi Interactively on All Hosts in ROBO](#)

Install all ESXi hosts for all of the clusters in your ROBO deployment interactively.

3 Configure the Network on All Hosts in ROBO

After the initial boot-up, use the ESXi Direct Console User Interface (DCUI) for initial host network configuration and administrative access for all hosts in the ROBO consolidated pod.

4 Configure a vSphere Standard Switch on a Host in ROBO

You must perform network configuration from the VMware Host Client for one host. You perform all other hosts networking configuration after the deployment of the vCenter Server system that manages the hosts.

5 Configure SSH and NTP on the First Host in ROBO

Time synchronization issues can result in serious problems with your environment. Configure NTP for each of your ROBO hosts.

6 Set Up Virtual SAN Datastore in ROBO

You must set up vSAN storage for use with your ROBO environment.

Prerequisites for Installation of ESXi Hosts in ROBO

Install and configure the ESXi hosts for your ROBO location.

Before you start:

- Make sure that you have a Windows host that has access to your data center. You use this host to connect to your hosts and perform configuration steps.
- Ensure that routing is in place between the home office and the remote office networks, 172.16.11.0/24 and 172.18.11.0/24.

You must also prepare the installation files.

- Download the ESXi ISO installer.
- Create a bootable USB drive that contains the ESXi Installation. See "Format a USB Flash Drive to Boot the ESXi Installation or Upgrade" in *vSphere Installation and Setup*.

IP Addresses, Hostnames, and Network Configuration

The following tables contain all the values needed to configure your ESXi hosts.

Table 2-1. Remote Office Hosts

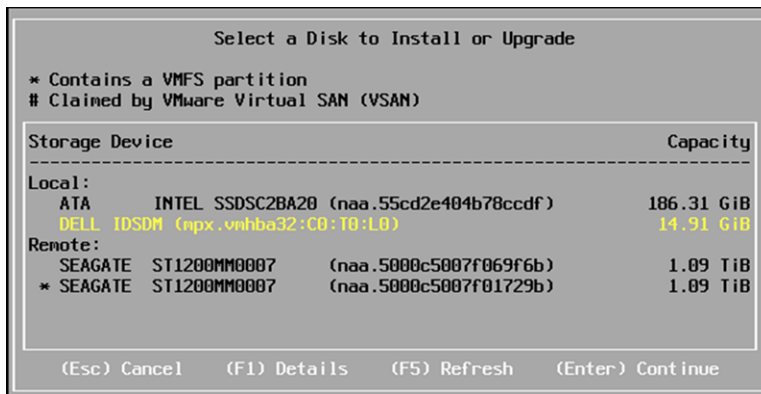
FQDN	IP	Management VLAN	Default Gateway	NTP Server
nyc01esx01.rainpole.local	172.18.11.101	1811	172.18.11.253	■ ntp.rainpole.local
nyc01esx02.rainpole.local	172.18.11.102	1811	172.18.11.253	■ ntp.rainpole.local
nyc01esx03.rainpole.local	172.18.11.103	1811	172.18.11.253	■ ntp.rainpole.local
nyc01esx04.rainpole.local	172.18.11.104	1811	172.18.11.253	■ ntp.rainpole.local

Install ESXi Interactively on All Hosts in ROBO

Install all ESXi hosts for all of the clusters in your ROBO deployment interactively.

Procedure

- 1 Power on the nyc01esx01 host.
- 2 Mount the USB drive containing the ESXi ISO file, and boot from that USB drive.
- 3 On the **Welcome to the VMware 6.5.0 Installation** screen, press Enter to start the installation.
- 4 On the **End User License Agreement (EULA)** screen, press F11 to accept the EULA.
- 5 On the **Select a Disk to Install or Upgrade** screen, select the USB drive or SD card under local storage to install ESXi, and press Enter to continue.



- 6 Select the keyboard layout, and press Enter.
- 7 Enter the *esxi_root_user_password*, enter the password a second time to confirm you are typing the correct password, and press Enter.
- 8 On the **Confirm Install** screen, press F11 to start the installation.
- 9 After the installation has completed unmount the USB drive, and press Enter to reboot the host.
- 10 Repeat this procedure for all hosts in the remote office, using the respective values for each host you configure.

Configure the Network on All Hosts in ROBO

After the initial boot-up, use the ESXi Direct Console User Interface (DCUI) for initial host network configuration and administrative access for all hosts in the ROBO consolidated pod.

Perform the following tasks to configure the host network settings:

- Configure the network adapter (vmk0) and VLAN ID for the Management Network.
- Configure the IP address, subnet mask, gateway, DNS server and host FQDN for the ESXi host.

Repeat this procedure for all hosts in the ROBO consolidated pod. Enter the respective values from the prerequisites section for each host that you configure. See [Prerequisites for Installation of ESXi Hosts in ROBO](#).

Procedure

- 1 Open the DCUI on the physical ESXi host nyc01esx01.
 - a Open a console window to the host.
 - b Press F2 to enter the DCUI.
 - c Enter **root** as login name, and **esxi_root_user_password**, and press Enter.

- 2 Configure the network.
 - a Select **Configure Management Network** and press Enter.
 - b Select **VLAN (Optional)** and press Enter.
 - c Enter **1811** as the VLAN ID for the Management Network, and press Enter.
 - d Select **IPv4 Configuration** and press Enter.
 - e Configure the IPv4 network using the following settings, and press **Enter**.

Setting	Value
Set static IPv4 address and network configuration	Selected
IPv4 Address	172.18.11.101
Subnet Mask	255.255.255.0
Default Gateway	172.18.11.253

- f Select **DNS Configuration** and press **Enter**.
 - g Configure the DNS using the following settings, and press **Enter**.

Setting	Value
Use the following DNS Server address and hostname	Selected
Primary DNS Server	172.18.11.4
Alternate DNS Server	172.16.11.4
Hostname	nyc01esx01.rainpole.local

- h Select **Custom DNS Suffixes** and press Enter.
 - i Ensure there are no suffixes listed, and press Enter.
- 3 After completing all host network settings press Escape to exit, and press Y to confirm the changes.
- 4 Repeat this procedure for all hosts in the ROBO consolidated pod.

Configure a vSphere Standard Switch on a Host in ROBO

You must perform network configuration from the VMware Host Client for one host. You perform all other hosts networking configuration after the deployment of the vCenter Server system that manages the hosts.

You configure a vSphere Standard Switch with two port groups:

- The existing virtual machine port group.
- VMkernel port group.

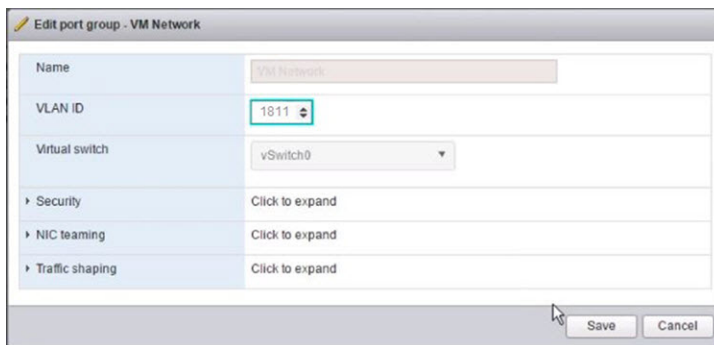
This configuration provides connectivity and common network configuration for virtual machines that reside on each host.

Procedure

- 1 Log in to the vSphere host using the VMware Host Client
 - a Open a Web browser and go to **https://nyc01esx01.rainpole.local**.
 - b Log in using the following credentials.

Setting	Value
User name	root
Password	esxi_root_user_password

- 2 Click **OK** to Join the Customer Experience Improvement Program.
- 3 Configure a VLAN for the VM Network Portgroup.
 - a In the **Navigator**, click **Networking**, click the **Port Groups** tab, choose the VM Network port group, and click **Edit Settings**.
 - b On the **Edit port group - VM Network** window, input **1811** for **VLAN ID**, and click **OK**.



Configure SSH and NTP on the First Host in ROBO

Time synchronization issues can result in serious problems with your environment. Configure NTP for each of your ROBO hosts.

Procedure

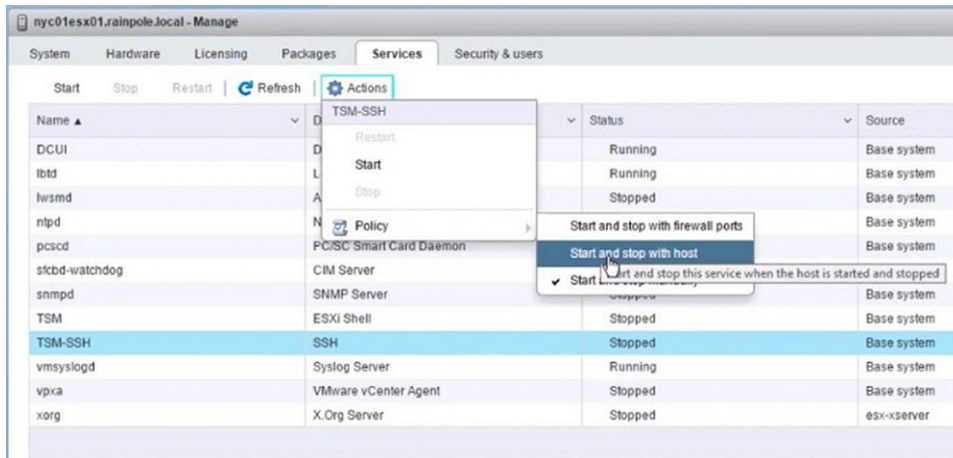
- 1 Log in to the `nyc01esx01.rainpole.local` host by using the VMware Host Client.

- a Open a Web browser and go to `nyc01esx01.rainpole.local`.

Setting	Value
User name	root
Password	<i>esxi_root_user_password</i>

- 2 Configure SSH options.

- a In the Navigator, click **Manage**, click the **Services** tab, select the **TSM-SSH** service, and click the **Actions** menu. Choose **Policy** and click **Start and stop with host**.

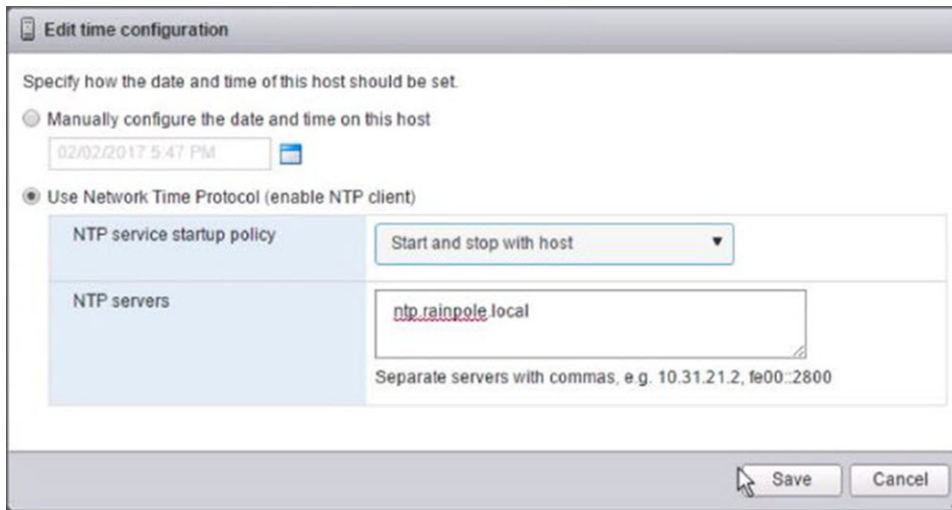


- b Click **Start** to start the service.

- 3 Configure the NTP Daemon (`ntpd`) options.

- a In the Navigator, click **Manage**, click the **System** tab, click **Time & date**, and click **Edit Settings**.
 - b In the **Edit Time configuration** dialog box, select the **Use Network Time Protocol (enable NTP client)** radio button, change the NTP service startup policy to **Start and stop with host**, and enter `ntp.rainpole.local` as the NTP server.

- c Click **Save** to save these changes.



- d Start the service by clicking **Actions**, hover over **NTP service**, and choose **Start**.

Set Up Virtual SAN Datastore in ROBO

You must set up vSAN storage for use with your ROBO environment.

This process is divided into two main tasks.

- Bootstrap the first ESXi host from the command line and create the vSAN datastore.
- After vCenter Server installation, perform vSAN configuration for all other hosts from the vSphere Web Client.

Procedure

- 1 Using an SSH client, connect to the ESXi Shell on **nyc01esx01.rainpole.local**.
 - a Open a console window to the host.
 - b Log in using the following credentials.

Setting	Value
login as:	root
Password	esxi_root_user_password

- 2 Run the following command to determine the current vSAN storage policy.

```
esxcli vsan policy getdefault
```



```
[root@esx01 ~]# esxcli vsan policy getdefault
Policy Class Policy Value
-----
cluster      (('hostFailuresToTolerate' i1))
vdisk        (('hostFailuresToTolerate' i1))
vmnamespace  (('hostFailuresToTolerate' i1))
vmswap       (('hostFailuresToTolerate' i1) ('forceProvisioning' i1))
vmem         (('hostFailuresToTolerate' i1) ('forceProvisioning' i1))
```

- 3 Modify the default vSAN storage policy to force provisioning of the vSAN datastore without generating errors.

```
esxcli vsan policy setdefault -c vdisk -p "((\"hostFailuresToTolerate\" i1) (\"forceProvisioning\" i1))"
esxcli vsan policy setdefault -c vmnamespace -p "((\"hostFailuresToTolerate\" i1) (\"forceProvisioning\" i1))"
esxcli vsan policy getdefault
```

```
[root@esx01 ~]# esxcli vsan policy setdefault -c vdisk -p "((\"hostFailuresToTolerate\" i1) (\"forceProvisioning\" i1))"
[root@esx01 ~]# esxcli vsan policy setdefault -c vmnamespace -p "((\"hostFailuresToTolerate\" i1) (\"forceProvisioning\" i1))"
[root@esx01 ~]# esxcli vsan policy getdefault
Policy Class Policy Value
-----
cluster      (('hostFailuresToTolerate' i1))
vdisk        (('hostFailuresToTolerate' i1) ('forceProvisioning' i1))
vmnamespace  (('hostFailuresToTolerate' i1) ('forceProvisioning' i1))
vmswap       (('hostFailuresToTolerate' i1) ('forceProvisioning' i1))
vmem         (('hostFailuresToTolerate' i1) ('forceProvisioning' i1))
```

- 4 Generate the vSAN cluster UUID and create the vSAN cluster.

Record the \$UUID_GENERATED from the system output to use in the the next step.

```
python -c 'import uuid; print (uuid.uuid4());'
```

```
esxcli vsan cluster join -u <UUID_GENERATED>
esxcli vsan cluster get
```

```
[root@esx01 ~]# python -c 'import uuid; print str(uuid.uuid4());'
914a3564-8aab-4c7c-b430-9381935980ef
[root@esx01 ~]# esxcli vsan cluster join -u 914a3564-8aab-4c7c-b430-9381935980ef
[root@esx01 ~]# esxcli vsan cluster get
Cluster Information
  Enabled: true
  Current Local Time: 2016-01-04T22:58:05Z
  Local Node UUID: 5628701b-f916-1140-77a4-ecf4bbd89a48
  Local Node Type: NORMAL
  Local Node State: MASTER
  Local Node Health State: HEALTHY
  Sub-Cluster Master UUID: 5628701b-f916-1140-77a4-ecf4bbd89a48
  Sub-Cluster Backup UUID:
  Sub-Cluster UUID: 914a3564-8aab-4c7c-b430-9381935980ef
  Sub-Cluster Membership Entry Revision: 0
  Sub-Cluster Member Count: 1
  Sub-Cluster Member UUIDs: 5628701b-f916-1140-77a4-ecf4bbd89a48
  Sub-Cluster Membership UUID: ecf88a56-d723-4593-59d7-ecf4bbd89a48
```

5 List the devices and determine the device name for the SSD and HDD.

You will use these disks to provision the vSAN datastore.

```
vdq -q
```

Identify all of the devices that can be used by vSAN.

Property	SDD Value	HDD Value
State	Eligible for use by VSAN	Eligible for use by VSAN
IsSSD	1	0

```

[ root@      :~] vdq -q
[
  {
    "Name"      : "mpx.vmhba36:C0:T0:L1",
    "VSANUUID"  : "",
    "State"     : "Ineligible for use by VSAN",
    "ChecksumSupport": "0",
    "Reason"    : "Has partitions",
    "IsSSD"     : "0",
    "IsCapacityFlash": "0",
    "IsPDL"     : "0",
  },

  {
    "Name"      : "naa.50000396a83a47f5",
    "VSANUUID"  : "",
    "State"     : "Eligible for use by VSAN",
    "ChecksumSupport": "0",
    "Reason"    : "Non-local disk",
    "IsSSD"     : "0",
    "IsCapacityFlash": "0",
    "IsPDL"     : "0",
  },

  {
    "Name"      : "naa.50000396a83a7845",
    "VSANUUID"  : "",
    "State"     : "Eligible for use by VSAN",
    "ChecksumSupport": "0",
    "Reason"    : "Non-local disk",
    "IsSSD"     : "0",
    "IsCapacityFlash": "0",
    "IsPDL"     : "0",
  },

  {
    "Name"      : "mpx.vmhba32:C0:T0:L0",
    "VSANUUID"  : "",
    "State"     : "Ineligible for use by VSAN",
    "ChecksumSupport": "0",
    "Reason"    : "Has partitions",
    "IsSSD"     : "0",
    "IsCapacityFlash": "0",
    "IsPDL"     : "0",
  },

  {
    "Name"      : "naa.5000c5007f0befe7",
    "VSANUUID"  : "",
    "State"     : "Eligible for use by VSAN",
    "ChecksumSupport": "0",
    "Reason"    : "Non-local disk",
    "IsSSD"     : "0",
    "IsCapacityFlash": "0",
    "IsPDL"     : "0",
  },

  {
    "Name"      : "naa.55cd2e404c0479f9",
    "VSANUUID"  : "",
    "State"     : "Eligible for use by VSAN",
    "ChecksumSupport": "0",
    "Reason"    : "None",
    "IsSSD"     : "1",
    "IsCapacityFlash": "0",
    "IsPDL"     : "0",
  },

  {
    "Name"      : "naa.5000c5007f164c03",
    "VSANUUID"  : "",
    "State"     : "Eligible for use by VSAN",
    "ChecksumSupport": "0",
    "Reason"    : "Non-local disk",
    "IsSSD"     : "0",
    "IsCapacityFlash": "0",
    "IsPDL"     : "0",
  },

  {

```

HDD

SSD

- 6 Create the vSAN datastore using the available SSD and HDD disks you identified in the previous step.

```
esxcli vsan storage add -s SSD_Device_name -d HDD_Device_Name
```

```
[root@ ~]# esxcli vsan storage add -s naa.55cd2e404c0479f9 -d naa.5000c5007f0bfe7 -d naa.5000c5007f164c03
```

- 7 Verify that the vSAN datastore has been created successfully.

```
esxcli storage filesystem list
```

Mount Point	Size	Free	Volume Name	UUID	Mounted	Type
/vmfs/volumes/562870a8-60765e1b-2857-ecf4bbd89a48	299712512	81395712		562870a8-60765e1b-2857-ecf4bbd89a48	true	vfat
/vmfs/volumes/2c1b45e8-7f709b26-ff76-8f8520c111b1	261853184	66375688		2c1b45e8-7f709b26-ff76-8f8520c111b1	true	vfat
/vmfs/volumes/c09dfbe6-c829ac8d-a7dc-d793f8776682	261853184	92123136		c09dfbe6-c829ac8d-a7dc-d793f8776682	true	vfat
/vmfs/volumes/vsan:914a35648aab4c7c-b4309381935980ef			vsanDatastore	vsan:914a35648aab4c7c-b4309381935980ef	true	vsan

The vSAN datastore is now ready for the vCenter Server installation.

Deploy and Configure the Virtual Center Components in ROBO

Deploy and configure the Virtual Center and cluster components for your remote office and branch office.

Procedure

- 1 [Deploy the vCenter Server Instance with an Embedded Platform Services Controller in ROBO](#)

You can now install the vCenter Server appliance for the remote office and configure licensing and security.

- 2 [Replace the vCenter Server Instance with an Embedded Platform Service Controller Certificates in ROBO](#)

After you deploy the vCenter Server instance with an Embedded Platform Service, you replace the self-signed certificate before you deploy to other VMware appliances.

- 3 [Add Custom Advanced Settings for vCenter Server](#)

- 4 [Configure the vSphere Cluster in ROBO](#)

Create and configure the vSphere cluster for use with your ROBO deployment.

- 5 [Create a vSphere Distributed Switch in ROBO](#)

After adding all ESXi hosts to the clusters, you create a vSphere Distributed Switch. You will also create port groups to prepare your environment to migrate the vCenter Server instance to the distributed switch.

6 Set vSAN Storage Policy in ROBO

Set the vSAN storage policy for the vCenter Server appliance for your ROBO deployment.

7 Create vSAN Disk Groups in ROBO

Create vSAN disk groups on each host providing storage to the vSAN datastore for your ROBO deployment.

8 Enable vSphere HA in ROBO

Before creating the host profile for the management cluster, enable vSphere HA for your ROBO deployment.

9 Change Advanced Options on the ESXi Hosts in ROBO

Change the default ESX Admins group to achieve greater levels of security, and enable vSAN to provision the Virtual Machine Swap files as thin to save space in the vSAN datastore.

10 Create and Apply the Host Profile in ROBO

Host Profiles ensure all hosts in the cluster have the same configuration.

11 Set vSAN Policy in ROBO

After you apply the host profile to all the hosts, set the storage policy of the vCenter Server to the vSAN Default Storage Policy.

12 Create the VM and Template Folders in ROBO

Create folders to group objects of the same type for easier management.

Deploy the vCenter Server Instance with an Embedded Platform Services Controller in ROBO

You can now install the vCenter Server appliance for the remote office and configure licensing and security.

Procedure

1 Start the **vCenter Server Appliance 6.5 Installer** wizard.

- a Browse to the vCenter Server Appliance ISO file.
- b Open the <dvd-drive>:\vcsa-ui-installer\win32\Installer application file.

2 Complete the **vCenter Server Appliance 6.5 Installer** wizard.

- a Click **Install** to start the installation.
- b Click **Next** on the **Introduction** page.
- c On the **End User License Agreement** page, select the **I accept the terms of the license agreement** check box and click **Next**.
- d On the **Select deployment type** page, under **External Platform Services Controller**, verify that the **vCenter Server with an Embedded Platform Services Controller** radio button is selected, and click **Next**.

- e On the **Appliance deployment target** page, enter the following settings and click **Next**.

Setting	Value
ESXi host or vCenter Server name	nyc01esx01.rainpole.local
HTTPS port	443
User name	root
Password	<i>esxi_root_user_password</i>

- f In the **Certificate Warning** dialog box, click **Yes** to accept the host certificate.
- g On the **Set up appliance VM** page, enter the following settings and click **Next**.

Setting	Value
VM name	nyc01vc01
Root password	<i>nycvc_root_password</i>
Confirm root password	<i>nycvc_root_password</i>

- h On the **Select deployment size** page, select **Small** Deployment size and click **Next**.
- i On the **Select datastore** page, select the **vsanDatastore** datastore, select the **Enable Thin Disk Mode** check box, and click **Next**.
- j On the **Configure network settings** page, enter the following settings and click **Next**.

Setting	Value
Network	VM Network
IP version	IPv4
IP assignment	static
System name	nyc01vc01.rainpole.local
IP address	172.18.11.61
Subnet mask or prefix length	255.255.255.0
Default gateway	172.18.11.253
DNS servers	172.18.11.4,172.16.11.4

- k On the **Ready to complete stage 1** page, review the configuration and click **Finish** to start the deployment.
- l Once the deployment completes, click **Continue** to proceed to stage 2 of the installation.

3 Install - Stage 2: Complete the **Set Up vCenter Server Appliance with an Embedded PSC** wizard.

- a Click **Next** on the **Introduction** page.
- b On the **Appliance configuration** page, enter the following settings and click **Next**.

Setting	Value
Time Synchronization mode	Synchronize time with NTP servers
NTP servers (comma-separated list)	ntp.rainpole.local
SSH access	Enabled

- c On the **SSO configuration** page, enter the following settings and click **Next**.

SSO domain name	vsphere.local
SSO user name	administrator
SSO password	<i>vsphere_admin_password</i>
Confirm password	<i>vsphere_admin_password</i>
Site name	NYC

- d ON the **Configure CEIP** page, click **Next**.
 - e On the **Ready to complete** page, review the configuration and click **Finish**.
 - f Click **OK** on the **Warning** dialog box.
 - g Once the set up completes, click **Close** to shut down the wizard.
- ### 4 Add the vCenter Server appliance to Active Directory.
- a Open a Web browser and go to **https://nyc01vc01.rainpole.local/vsphere-client**.
 - b Log in using the following credentials.

Setting	Value
User name	administrator@vsphere.local
Password	<i>vsphere_admin_password</i>

- c In the **Navigator**, click **Administration**.
- d In the **Administration** window, click **System Configuration**.
- e In the **System Configuration** window, click **Nodes**, then click the **nyc01vc01.rainpole.local** node that appears below.
- f Click the **Manage** tab, then click **Settings** subtab, then click **Active Directory**.

- g Click **Join**, enter the following settings, and click **OK**.

Setting	Value
Domain:	rainpole.local
Organizational Unit:	N/A
User name:	svc-domain
Password:	svc-domain_password

- h Click on the **Reboot the node** icon, enter a brief message for a reason, and click **OK** to restart the vCenter Server.

- 5 Once the appliance has completed rebooting, log in to vCenter Server and verify the domain membership.

- a Open a Web browser and go to **https://nyc01vc01.rainpole.local/vsphere-client**.
b Log in using the following credentials.

Setting	Value
User name	administrator@vsphere.local
Password	vsphere_admin_password

- c In the **Navigator**, click **Administration**.
d In the **Administration** window, click **System Configuration**.
e In the **System Configuration** window, click **Nodes**, then click the **nyc01vc01.rainpole.local** node that appears below.
f Click the **Manage** tab, then click **Settings** subtab, then click **Active Directory**.
g Verify that **RAINPOLE.LOCAL** is listed as the **Domain**.

- 6 Configure the SSO Identity Source.

- a In the **Navigator**, click **Administration**.
b In the **Administration** window, click **Configuration** and click the **Identity Sources** tab.
c Click the **Add Identity Source** icon to start the wizard.
d On the **Select Identity Source Type** window, click **Next**.
e On the **Configure identity source** window, click **Next**.
f On the **Ready to Complete** window, review the configuration and click **Finish**.
g Click on the **rainpole.local** entry and click the **Set as Default Domain** icon.
h Click **Yes** in the Warning box.

- 7 Add new licenses for this vCenter Server instance and the ESXi hosts, if needed.

- a Click the **Home** icon above the **Navigator** and choose the **Administration** menu item.
b On the **Administration** page, click **Licenses** and click the **Licenses** tab.

- c Click the **Create New Licenses** icon to add license keys.
 - d On the **Enter license keys** page, enter license keys for vCenter Server, ESXi and vSAN, one per line and click **Next**.
 - e On the **Edit license name** page, enter a descriptive name for each license key and click **Next**.
 - f On the **Ready to complete** page, review your entries and click **Finish**.
- 8 Assign the newly added licenses to the respective assets.
- a Click the **Assets** tab.
 - b Select the vCenter Server instance, and click the **Assign License** icon.
 - c Select the vCenter Server license that you entered in the previous step, and click **OK**.
- 9 Assign the vCenterAdmins domain group to the vCenter Server Administrator role.
- a In the **Navigator**, click **Administration**.
 - b In the **Administration** window, click **Global Permissions**.
 - c In the **Global Permissions** box, click the **Manage** tab, then click the **Add permission** button.
 - d In the **Global Permissions Root - Add Permissions** window, click the **Add** button.
 - e Select `rainpole.local` from the **Domain** drop down list.
 - f Enter **vCenterAdmins** in the **Search** field and press **Enter**.
 - g Select the **vCenterAdmins** group, click the **Add** button, and then click **OK**.
 - h Ensure **Administrator** is selected and the **Propagate to Children** check box is selected under **Assigned Role** and click **OK**.

Replace the vCenter Server Instance with an Embedded Platform Service Controller Certificates in ROBO

After you deploy the vCenter Server instance with an Embedded Platform Service, you replace the self-signed certificate before you deploy to other VMware appliances.

Replace the certificates using the build in the Certificate Manager utility.

Table 2-2. Certificate-Related Files on the vCenter Server Instances

vCenter Server FQDN	Files for Certificate Replacement	Replacement Order
nyc01vc01.rainpole.local	<ul style="list-style-type: none"> ■ nyc01vc01.key ■ nyc01vc01.1.cer ■ Root64.cer 	After you deployed vCenter Server Instance with an Embedded Platform Service

Procedure

- 1 Use the `scp` command, FileZilla, or WinSCP to copy the machine and CA certificate files to the `/tmp/ssl` directory on the Management vCenter Server.
Use the `scp` command, FileZilla, or WinSCP to copy the files.

- 2 Log in to the vCenter Server instance by using Secure Shell client.
 - a Open an SSH connection to the FQDN of the vCenter Server appliance.
 - b Log in using the following credentials.

Setting	Value
User name	root
Password	vcenter_server_root_password

- 3 Replace the CA-signed certificate on the vCenter Server instance.
 - a From the SSH client connected to the vCenter Server instance, add the Root certificate to the VMware Endpoint Certificate Store as a Trusted Root Certificate using following command and enter the vCenter Single Sign-On password when prompted.

```
/usr/lib/vmware-vmafd/bin/dir-cli trustedcert publish --chain --cert /tmp/ssl/Root64.cer
```

- b Start the vSphere Certificate Manager utility on the vCenter Server instance.

```
/usr/lib/vmware-vmca/bin/certificate-manager
```

- c Select **Option 1 (Replace Machine SSL certificate with Custom Certificate)**, enter default vCenter Single Sign-On user name **administrator@vsphere.local** and the **vsphere_admin_password** password.
 - d When prompted for the Infrastructure Server IP, provide the IP address of the Platform Services Controller that manages this vCenter Server instance.

vCenter Server	IP Address of Connected Platform Services Controller
nyc01vc01.rainpole.local	172.18.11.61

- e Select **Option 2 (Import custom certificate(s) and key(s) to replace existing Machine SSL certificate)**.
 - f When prompted, provide the full path to the custom certificate, the root certificate file, and the key file that have been generated by vSphere Certificate Manager earlier, and confirm the import with **Yes (Y)**.

vCenter Server	Path to Certificate-Related Files
nyc01vc01.rainpole.local	Provide valid custom certificate for Machine SSL. File: /tmp/ssl/nyc01vc01.1.cer Provide valid custom key for Machine SSL. File: /tmp/ssl/nyc01vc01.key Provide the signing certificate of the Machine SSL certificate. File: /tmp/ssl/Root64.cer

- 4 When the Status indicator reports 100% Completed, wait several minutes until all vCenter Server services are restarted.

```
Updated 21 service(s)  
Status : 100% Completed [All tasks completed successfully]
```

Add Custom Advanced Settings for vCenter Server

Prerequisites

Procedure



Example:

What to do next

Configure the vSphere Cluster in ROBO

Create and configure the vSphere cluster for use with your ROBO deployment.

To create and configure the vSphere cluster:

- Create the Datacenter and Cluster.
- Configure DRS.
- Enable vSAN for the cluster.
- Add the hosts to the cluster.
- Add a host to the active directory domain.
- Reset the vSAN Storage Policy to default for the ESXi host that is used for Bootstrap.
- Create vSAN disk groups.
- Mount the NFS volume for vSphere Data Protection Backups.
- Change the default ESX Admin group.
- Enable and configure vSphere HA
- Create and apply a host profile.
- Set the vCenter Server appliance to the default vSAN storage policy.

Prerequisites

You must replace the self-signed certificate on the vCenter Server prior to creating the vSphere cluster. See [Replace the vCenter Server Instance with an Embedded Platform Service Controller Certificates in ROBO](#).

Procedure

- 1 Log in to the vCenter Server by using the vSphere Web Client.
 - a Open a Web browser and go to **https://nyc01vc01.rainpole.local/vsphere-client**.
 - b Log in using the following credentials.

Setting	Value
User name	administrator@vsphere.local
Password	vsphere_admin_password

- 2 Create a Datacenter object.
 - a In the **Navigator**, click **Hosts and Clusters**.
 - b Right-click **nyc01vc01.rainpole.local** and click **New Datacenter**.
 - c In the **New Datacenter** dialog box, enter **NYC01** as Datacenter name, and click **OK**.

3 Create the cluster.

- a Right-click the **NYC01** datacenter and click **New Cluster**.
- b In the **New Cluster** wizard, enter the following values and click **OK**.

Setting	Value	
Name	NYC01	
DRS	Turn ON	Selected
	Other DRS options	Default values
vSphere HA	Turn ON	Deselected
EVC	Set EVC mode to the lowest available setting supported for the hosts in the cluster	
vSAN	Turn ON	Selected
	Add disks to storage	Manual

New Cluster

Name: NYC01

Location: NYC01

DRS: ☒ Turn ON

Automation Level: Fully automated

Migration Threshold: Conservative — Aggressive

vSphere HA: ☐ Turn ON

EVC: Intel® "Haswell" Generation

Virtual SAN: ☒ Turn ON

Add disks to storage: Manual

Requires manual claiming of any new disks on the included hosts to the shared storage.

Licensing: A license must be assigned to the cluster in order to create disk groups or consume disks automatically.

OK Cancel

4 Add a host to the cluster.

- a Right-click the **NYC01** cluster, and click **Add Host**.
- b On the **Name and location** page, enter **nyc01esx01.rainpole.local** in the **Host name or IP address** text box and click **Next**.
- c On the **Connection settings** page, enter the following credentials and click **Next**.

Setting	Value
User name	root
Password	esxi_root_user_password

- d In the **Security Alert** dialog box, click **Yes**.
- e On the **Host summary** page, review the host information and click **Next**.
- f On the **Assign license** page, select the ESXi license key that you entered during the vCenter Server deployment and click **Next**.
- g On the **Lockdown Mode** page, click **Next**.
- h On the **Resource pool** page, click **Next**.
- i On the **Ready to complete** page, review your entries and click **Finish**.

5 Repeat the previous step for the three remaining hosts to add them to the cluster.

Setting	Value
Host 2	nyc01esx02.rainpole.local
Host 3	nyc01esx03.rainpole.local
Host 4	nyc01esx04.rainpole.local

6 Add an ESXi host to the active directory domain.

- a In the **Navigator**, click **Hosts and Clusters** and expand the entire **nyc01vc01.rainpole.local** tree.
- b Select the **nyc01esx01.rainpole.local** host.
- c Click the **Configure** tab.
- d Under **System**, select **Authentication Services**.
- e In the **Authentication Services** panel, click the **Join Domain** button.
- f In the **Join Domain** dialog box, enter the following settings and click **OK**.

Setting	Value
Domain	rainpole.local
Using credentials	Selected
User name	ad_admin_acct@rainpole.local
Password	ad_admin_password

- 7 Set the Active Directory Service to Start and stop with host.
 - a In the **Navigator**, click **Hosts and Clusters** and expand the entire **nyc01vc01.rainpole.local** tree.
 - b Select the **nyc01esx01.rainpole.local** host.
 - c Click the **Configure** tab.
 - d Under **System**, select **Security Profile**.
 - e Click the **Edit** button next to **Services**.
 - f Select the **Active Directory** service and change the **Startup Policy** to **Start and stop with host** and click **OK**.
- 8 Rename the vSAN datastore.
 - a Select the **NYC01** cluster.
 - b Click the **Datastores** tab.
 - c Select **vsanDatastore**, and select **Actions > Rename..**
 - d In the **Datastore - Rename** dialog box, enter **NYC01-VSAN01** as the datastore name, and click **OK**.
- 9 Configure resource pools for the consolidated cluster.
 - a Right-click the **NYC01** cluster and select **New Resource Pool**.
 - b In the **New Resource Pool** dialog box, enter the following values and click **OK**.
 - c Repeat for each of the resource pools needed.

Setting	Resource Pool 1	Resource Pool 2	Resource Pool 3	Resource Pool 4
Name	NYC01-MGMT	NYC01-Edge	User-Edge	User-VM
CPU-Shares	High	High	Normal	Normal
CPU-Reservation	0	0	0	0
CPU-Reservation Type	Expandable selected	Expandable selected	Expandable selected	Expandable selected
CPU-Limit	Unlimited	Unlimited	Unlimited	Unlimited
Memory-Shares	Normal	Normal	Normal	Normal
Memory-Reservation	102400 MB	15360 MB	0	0
Memory-Reservation Type	Expandable selected	Expandable selected	Expandable selected	Expandable selected
Memory-Limit	Unlimited	Unlimited	Unlimited	Unlimited

Create a vSphere Distributed Switch in ROBO

After adding all ESXi hosts to the clusters, you create a vSphere Distributed Switch. You will also create port groups to prepare your environment to migrate the vCenter Server instance to the distributed switch.

Procedure

- 1 Log in to the vCenter Server by using the vSphere Web Client.

- a Open a Web browser and go to **https://nyc01vc01.rainpole.local/vsphere-client**.
- b Log in using the following credentials.

Setting	Value
User name	administrator@vsphere.local
Password	vsphere_admin_password

- 2 Create vSphere Distributed Virtual Switch.

- a In the **Navigator**, click **Networking** and expand the **nyc01vc01.rainpole.local** tree.
- b Right-click the **NYC01** datacenter, and select **Distributed Switch > New Distributed Switch** to start the **New Distributed Switch** wizard.
- c On the **Name and location** page, enter **vDS-NYC01** as the name and click **Next**.
- d On the **Select version** page, ensure the **Distributed switch: 6.5.0** radio button is selected and click **Next**.
- e On the **Edit settings** page, enter the following values and click **Next**.

Setting	Value
Number of uplinks	2
Network I/O Control	Enabled
Create a default port group	Deselected

- f On the **Ready to complete** page, review your entries and click **Finish**.

- 3 Edit the settings of the vDS-NYC01 distributed switch.

- a Right-click the **vDS-NYC01** distributed switch, and select **Settings > Edit Settings**.
- b Click the **Advanced** tab.
- c Enter **9000** as MTU (Bytes) value, and click **OK**.

4 Create port groups in the vDS-NYC01 distributed switch for the management traffic types.

- a Right-click the **vDS-NYC01** distributed switch, and select **Distributed Port Group > New Distributed Port Group**.
- b Create port groups with the following settings and click **Next**.

Port Group Name	Port Binding	VLAN Type	VLAN ID
vDS-NYC01-Management	Ephemeral - no binding	VLAN	1811
vDS-NYC01-vMotion	Static binding	VLAN	1812
vDS-NYC01-VSAN	Static binding	VLAN	1813
vDS-NYC01-Uplink01	Static binding	VLAN	2814
vDS-NYC01-Uplink02	Static binding	VLAN	2815

Note The port group for VXLAN traffic is automatically created later during the configuration of the NSX Manager.

- c On the **Ready to complete** page, review your entries, and click **Finish**.
 - d Repeat this step for each port group.
- 5 Change the port groups to use the Route Based on Physical NIC Load teaming algorithm.
- a Right-click the **vDS-NYC01** distributed switch and select **Distributed Port Group > Manage Distributed Port Groups**.
 - b On the **Select port group policies** page, select **Teaming and failover** and click **Next**.
 - c Click the **Select distributed port groups** button, add all port groups and click **Next**.
 - d On the **Teaming and failover** page, select **Route based on physical NIC load** from the **Load balancing** drop-down menu and click **Next**.
 - e Click **Finish**.
- 6 Connect the ESXi host, nyc01esx01.rainpole.local, to the vDS-NYC01 distributed switch by migrating their VMkernel and virtual machine network adapters.
- a Right-click the **vDS-NYC01** distributed switch, and click **Add and Manage Hosts**.
 - b On the **Select task** page, select **Add hosts** and click **Next**.
 - c On the **Select hosts** page, click **New hosts**.
 - d In the **Select new hosts** dialog box, select **nyc01esx01.rainpole.local** and click **OK**.
 - e On the **Select hosts** page, click **Next**.
 - f On the **Select network adapter tasks** page, ensure that **Manage physical adapters** and **Manage VMkernel adapters** check boxes are selected, and click **Next**.
 - g On the **Manage physical network adapters** page, click **vmnic1** and click **Assign uplink**.

- h In the **Select an Uplink for vmnic1** dialog box, select **Uplink 2** and click **OK**.
 - i On the **Manage physical network adapters** page, click **Next**.
- 7** Configure the VMkernel network adapters, edit the existing, and add new adapters as needed.
- a On the **Manage VMkernel network adapters** page, click **vmk0** and click **Assign port group**.
 - b Select **vDS-NYC01-Management** and click **OK**.
 - c On the **Manage VMkernel network adapters** page, click **On this switch** and click **New adapter**.
 - d On the **Add Networking** page, select **Select an existing network**, browse to select the **vDS-NYC01-VSAN** port group, click **OK**, and click **Next**.
 - e On the **Port properties** page, select the **vSAN** check box and click **Next**.
 - f On the **IPv4 settings** page, select **Use static IPv4 settings**, enter the IP address **172.18.13.101**, enter the subnet **255.255.255.0**, and click **Next**.
 - g Click **Finish**.
 - h On the **Analyze impact** page, click **Next**.
 - i On the **Ready to complete** page, review your entries and click **Finish**.
- 8** Create the vMotion VMkernel adapter.
- a In the **Navigator**, click **Host and Clusters** and expand the **nyc01vc01.rainpole.local** tree.
 - b Click **nyc01esx01.rainpole.local**.
 - c Click the **Configure** tab then select **VMkernel adapters**.
 - d Click the **Add host networking** icon, select **VMkernel Network Adapter**, and click **Next**.
 - e On the **Add Networking** page, select **Select an existing network**, browse to select the **vDS-NYC01-vMotion** port group, click **OK**, and click **Next**.
 - f On the **Port properties** page, select **vMotion** from the **TCP/IP Stack** drop-down menu and click **Next**.
 - g On the **IPv4 settings** page, select **Use static IPv4 settings**, enter the IP address **172.18.12.101**, enter the subnet **255.255.255.0**, and click **Next**.
 - h Click **Finish**.
- 9** Configure the MTU on the vMotion VMkernel adapter
- a Select the vMotion VMkernel adapter created in step 8 and click **Edit Settings**.
 - b Click the **NIC Settings** page.
 - c Enter **9000** for the **MTU** value and click **OK**.

10 Configure the vMotion TCP/IP stack.

- a Click **TCP/IP configuration**.
- b Select **vMotion** and click the **Edit** icon.
- c Click **Routing** and enter **172.18.12.253** for the **default gateway** and click **OK**.

11 Migrate the vCenter Server instance from the standard switch to the distributed switch.

- a In the **Navigator**, click **Networking** and expand the **nyc01vc01.rainpole.local** tree.
- b Right-click the **vDS-NYC01** distributed switch and click **Migrate VM to Another Network**.
- c On the **Select source and destination networks** page, browse the following networks and click **Next**.

Setting	Value
Source network	VM Network
Destination network	vDS-NYC01-Management

- d On the **Select VMs to migrate** page, select **nyc01vc01.rainpole.local**, and click **Next**.
- e On the **Ready to complete** page, review your entries and click **Finish**.

12 Define Network I/O Control shares for the different traffic types on the vDS-Mgmt distributed switch.

- a Click the **vDS-NYC01** distributed switch, click the **Configure** tab, and click **Resource Allocation > System traffic**.
- b Under **System Traffic**, configure each of the following traffic types with the following values.

Traffic Type	Physical adapter shares
Fault Tolerance (FT) Traffic	Low
Management Traffic	Normal
NFS Traffic	Low
Virtual Machine Traffic	High
Virtual SAN Traffic	High
iSCSI Traffic	Low
vMotion Traffic	Low
vSphere Data Protection Backup Traffic	Low
vSphere Replication (VR) Traffic	Low

13 Migrate the last physical adapter from the standard switch to the vDS-NYC01 distributed switch.

- a In the **Navigator**, click **Networking** and expand the **NYC01** datacenter.
- b Right-click the **vDS-NYC01** distributed switch and select **Add and Manage Hosts**.
- c On the **Select task** page, select **Manage host networking**, and click **Next**.
- d On the **Select hosts** page, click **Attached hosts**.

- e In the **Select member hosts** dialog box, select *nyc01esx01.rainpole.local*, and click **OK**.
 - f On the **Select hosts** page, click **Next**.
 - g On the **Select network adapter tasks** page, select **Manage physical adapters only**, and click **Next**.
 - h On the **Manage physical network adapters** page, select **vmnic0**, and click **Assign uplink**.
 - i In the **Select an Uplink for vmnic1** dialog box, select **Uplink 1**, and click **OK**, and click **Next**.
 - j On the **Analyze Impact** page, click **Next**.
 - k On the **Ready to complete** page, click **Finish**.
- 14** Enable vSphere Distributed Switch Health Check.
- a In the **Navigator**, click **Networking** and expand the **NYC01** datacenter.
 - b Select the **vDS-NYC01** distributed switch and click the **Configure** tab.
 - c In the **Navigator**, select **Health check** and click the **Edit** button.
 - d Select **Enabled** for **VLAN and MTU** and **Teaming and failover** and click **OK**.
- 15** Delete the vSphere Standard Switch.
- a In the **Navigator**, click on **Hosts and Clusters** and expand the *nyc01vc01.rainpole.local* tree.
 - b Click on *nyc01esx01.rainpole.local* and then click the **Configure** tab.
 - c On the **Configure** page, select **Virtual switches**, choose **vSwitch0**, and then click on the **Remove selected switch** icon.
 - d In the **Remove Standard Switch** dialog box, click **Yes** to confirm the removal.

Set vSAN Storage Policy in ROBO

Set the vSAN storage policy for the vCenter Server appliance for your ROBO deployment.

Procedure

- ◆ Reset the vSAN Storage Policy to default for the ESXi host that is used for bootstrap.
 - a Open an SSH connection to the ESXi host *nyc01esx01.rainpole.local*.
 - b Log in using the following credentials.

Setting	Value
User name	root
Password	<i>esxi_root_user_password</i>

- c Run the following command to determine the current vSAN storage policy.

```
esxcli vsan policy getdefault
```

```
[root@      :~] esxcli vsan policy getdefault
Policy Class Policy Value
-----
cluster      ({"hostFailuresToTolerate" i1})
vdisk        ({"hostFailuresToTolerate" i1} {"forceProvisioning" i1})
vmnamespace  ({"hostFailuresToTolerate" i1} {"forceProvisioning" i1})
vmswap       ({"hostFailuresToTolerate" i1} {"forceProvisioning" i1})
vmem         ({"hostFailuresToTolerate" i1} {"forceProvisioning" i1})
[root@      :~]
```

- d Modify the default vSAN storage policy to force provisioning of vSAN datastore without generating errors.

```
esxcli vsan policy setdefault -c vdisk -p "({\"hostFailuresToTolerate\" i1})"
esxcli vsan policy setdefault -c vmnamespace -p "({\"hostFailuresToTolerate\" i1})"
esxcli vsan policy getdefault
```

```
[root@      :~] esxcli vsan policy setdefault -c vdisk -p "({\"hostFailuresToTolerate\" i1})"
[root@      :~] esxcli vsan policy setdefault -c vmnamespace -p "({\"hostFailuresToTolerate\" i1})"
[root@      :~] esxcli vsan policy getdefault
Policy Class Policy Value
-----
cluster      ({"hostFailuresToTolerate" i1})
vdisk        ({"hostFailuresToTolerate" i1})
vmnamespace  ({"hostFailuresToTolerate" i1})
vmswap       ({"hostFailuresToTolerate" i1} {"forceProvisioning" i1})
vmem         ({"hostFailuresToTolerate" i1} {"forceProvisioning" i1})
[root@      :~]
```

Create vSAN Disk Groups in ROBO

Create vSAN disk groups on each host providing storage to the vSAN datastore for your ROBO deployment.

Procedure


- 1 Log in to vCenter Server by using the vSphere Web Client.
 - a Open a Web browser and go to <https://nyc01vc01.rainpole.local/vsphere-client>.
 - b Log in using the following credentials.

Setting	Value
User name	administrator@vsphere.local
Password	vsphere_admin_password

- 2 In the **Navigator**, select **Hosts and Clusters** and expand the **nyc01vc01.rainpole.local** tree.
- 3 Click on the **NYC01** cluster and click the **Configure** tab.
- 4 Under **Virtual SAN**, click **Disk Management**.
- 5 Click **nyc01esx02.rainpole.local** and click the **Create a New Disk Group** button.



- 6 In the **Create Disk Group** window, select a flash disk for the **cache tier**, two hard disk drives for the **capacity tier**, and click **OK**.

First, select a single disk to serve as cache tier.

	Name	Drive Type	Capacity	Transport Type
<input checked="" type="radio"/>	 Local ATA Disk (naa.55cd2e404c047943)	Flash	186.31 GB	vsan.disk....

Then, select one or more disks to serve as capacity tier.

Capacity type: HDD

<input checked="" type="checkbox"/>	Name	Drive Type	Capacity	Transport Type
<input checked="" type="checkbox"/>	 Local TOSHIBA Disk (naa.50000396a83a845d)	HDD	1.09 TB	vsan.disk....
<input checked="" type="checkbox"/>	 Local TOSHIBA Disk (naa.50000396a83a8461)	HDD	1.09 TB	vsan.disk....

- 7 Repeat steps 5 and 6 for **nyc01esx03.rainpole.local** and **nyc01esx04.rainpole.local**.
- 8 Assign a license to vSAN.
- Right click the **NYC01** cluster and select **Assign License**.
 - In the **NYC01 - Assign License** window select the previously added **VSAN License** and click **OK**.

Enable vSphere HA in ROBO

Before creating the host profile for the management cluster, enable vSphere HA for your ROBO deployment.

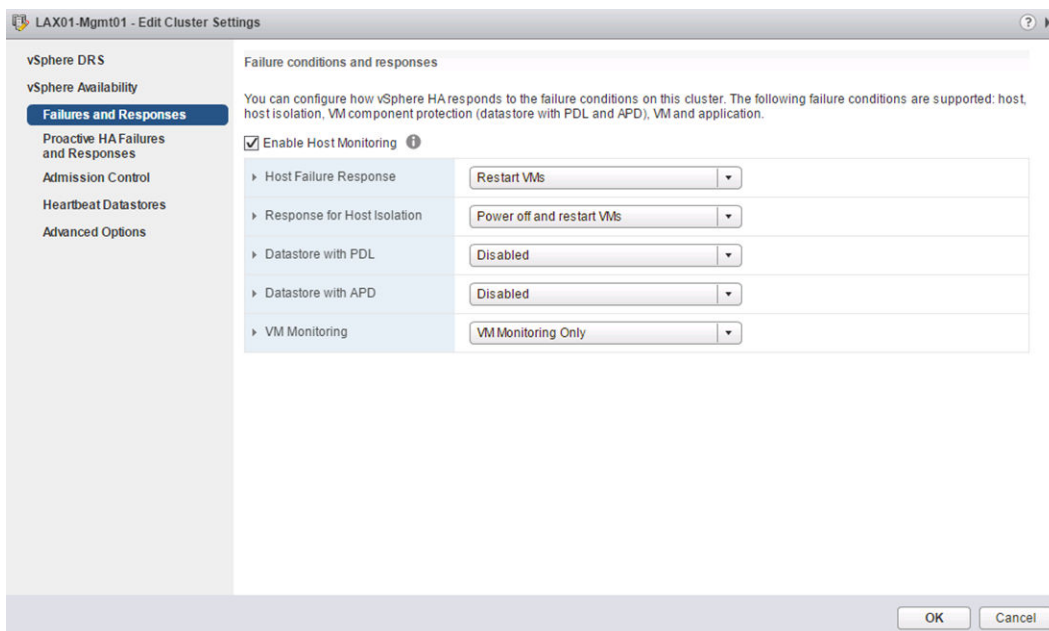
Procedure

- 1 Log in to vCenter Server by using the vSphere Web Client.
 - a Open a Web browser and go to **https://nyc01vc01.rainpole.local/vsphere-client**.
 - b Log in using the following credentials.

Setting	Value
User name	administrator@vsphere.local
Password	vsphere_admin_password

- 2 In the **Navigator**, click **Hosts and Clusters**.
 - a Expand the **nyc01vc01.rainpole.local** inventory.
 - b Select the **NYC01** cluster.
- 3 Click the **Configure** tab, click **vSphere Availability**, and click **Edit**.
- 4 In the **Edit Cluster Settings** dialog box, select the **Turn on vSphere HA** check box.
- 5 Select **Failures and Responses** and select the following values from the drop-down menus.

Setting	Value
Enable Host Monitoring	Selected
Host Failure Response	Restart VMs
Response for Host Isolation	Power off and restart VMs
Datastore with PDL	Disabled
Datastore with APD	Disabled
VM Monitoring	VM Monitoring Only



6 Click **Admission Control**.

7 In the **Admission Control** page enter following settings.

Setting	Value
Host failures cluster tolerates	1
Define host failover capacity by	Cluster resource percentage
Override calculated failover capacity	Deselected
Performance degradation VMs tolerate	100%

8 Click **OK**.

Change Advanced Options on the ESXi Hosts in ROBO

Change the default ESX Admins group to achieve greater levels of security, and enable vSAN to provision the Virtual Machine Swap files as thin to save space in the vSAN datastore.

Procedure

- 1 Log in to vCenter Server by using the vSphere Web Client.
 - a Open a Web browser and go to **<https://nyc01vc01.rainpole.local/vsphere-client>**.
 - b Log in using the following credentials.

Setting	Value
User name	administrator@vsphere.local
Password	vsphere_admin_password

- 2 Change the default ESX Admins group.
 - a In the **Navigator**, click **Hosts and Clusters**.
 - b Expand the entire **nyc01vc01.rainpole.local** vCenter inventory tree, and select the **nyc01esx01.rainpole.local** host.
 - c Click the **Configure** tab, click **System > Advanced System Settings**.
 - d Click the **Edit** button.
 - e In the **filter** box, enter **esxAdmins** and wait for the search results.
 - f Change the value of **Config.HostAgent.plugins.hostsvc.esxAdminsGroup** to **SDDC-Admins** and click **OK**.
- 3 Provision Virtual Machine swap files on vSAN as thin.
 - a In the **Navigator**, click **Hosts and Clusters**.
 - b Expand the entire **nyc01vc01.rainpole.local** vCenter inventory tree, and select the **nyc01esx01.rainpole.local** host.
 - c Click the **Configure** tab, click **System > Advanced System Settings**.
 - d Click the **Edit** button.
 - e In the **filter** box, enter **vsan.swap** and wait for the search results.
 - f Change the value of **VSAN.SwapThickProvisionDisabled** to **1** and click **OK**.
- 4 Disable the SSH warning banner.
 - a In the **Navigator**, click **Hosts and Clusters**.
 - b Expand the entire **nyc01vc01.rainpole.local** vCenter inventory tree, and select the **nyc01esx01.rainpole.local** host.
 - c Click the **Configure** tab, click **System > Advanced System Settings**.
 - d Click the **Edit** button.
 - e In the **Filter** search field, enter **ssh** and wait for the search results.
 - f Change the value of **UserVars.SuppressShellWarning** to **1** and click **OK**.

Create and Apply the Host Profile in ROBO

Host Profiles ensure all hosts in the cluster have the same configuration.

Procedure

- 1 Log in to vCenter Server by using the vSphere Web Client.
 - a Open a Web browser and go to **https://nyc01vc01.rainpole.local/vsphere-client**.
 - b Log in using the following credentials.

Setting	Value
User name	administrator@vsphere.local
Password	vsphere_admin_password

- 2 Create a Host Profile from *nyc01esx01.rainpole.local*
 - a In the **Navigator**, select **Hosts and Clusters** and expand the **nyc01vc01.rainpole.local** tree.
 - b Right-click the ESXi host **nyc01esx01.rainpole.local** and choose **Host Profiles > Extract Host Profile**.
 - c In the **Extract Host Profile** window, enter **NYC01** for the **Name** and click **Next**.
 - d In the **Ready to complete** page, click **Finish**.
- 3 Attach the Host Profile to the management cluster.
 - a In the **Navigator**, select **Hosts and Clusters** and expand the **nyc01vc01.rainpole.local** tree.
 - b Right-click on the **NYC01** cluster and choose **Host Profiles > Attach Host Profile**.
 - c In the **Attach Host Profile** window, click the **NYC01** Host Profile, select the **Skip Host Customization** checkbox and click **Finish**.
- 4 Create a host customization profile for the hosts in the management cluster.
 - a In the **Navigator**, select **Policies and Profiles**.
 - b Click **Host Profiles**, then right click **NYC01** and choose **Export Host Customizations**.
 - c Click **Save**.
 - d Choose a file location to save the *NYC01_host_customizations.csv* file.
 - e Open the *NYC01_host_customizations.csv* in Excel.

- f Edit the Excel file to include the following values.

ESXi Host	Active Directory Configuration Password	Active Directory Configuration Username	NetStack Instance defaultTcpipStack->DNS configuration Name for this host
nyc01esx01.rainpole.local	ad_admin_password	ad_admin_acct@rainpole.local	nyc01esx01
nyc01esx02.rainpole.local	ad_admin_password	ad_admin_acct@rainpole.local	nyc01esx02
nyc01esx03.rainpole.local	ad_admin_password	ad_admin_acct@rainpole.local	nyc01esx03
nyc01esx04.rainpole.local	ad_admin_password	ad_admin_acct@rainpole.local	nyc01esx04

ESXi Host	Host virtual NIC vDS-NYC01:vDS-NYC01-Management:management->IP address settings Host IPv4 address	Host virtual NIC vDS-NYC01:vDS-NYC01-Management:management->IP address settings SubnetMask
nyc01esx01.rainpole.local	172.18.11.101	255.255.255.0
nyc01esx02.rainpole.local	172.18.11.102	255.255.255.0
nyc01esx03.rainpole.local	172.18.11.103	255.255.255.0
nyc01esx04.rainpole.local	172.18.11.104	255.255.255.0

ESXi Host	Host virtual NIC vDS-NYC01:vDS-NYC01-VSAN:vsan->IP address settings Host IPv4 address	Host virtual NIC vDS-NYC01:vDS-NYC01-VSAN:vsan->IP address settings SubnetMask
nyc01esx01.rainpole.local	172.18.13.101	255.255.255.0
nyc01esx02.rainpole.local	172.18.13.102	255.255.255.0
nyc01esx03.rainpole.local	172.18.13.103	255.255.255.0
nyc01esx04.rainpole.local	172.18.13.104	255.255.255.0

ESXi Host	Host virtual NIC vDS-NYC01:vDS-NYC01-vMotion:vmotion->IP address settings Host IPv4 address	Host virtual NIC vDS-NYC01:vDS-NYC01-vMotion:vmotion->IP address settings SubnetMask
nyc01esx01.rainpole.local	172.18.12.101	255.255.255.0
nyc01esx02.rainpole.local	172.18.12.102	255.255.255.0
nyc01esx03.rainpole.local	172.18.12.103	255.255.255.0
nyc01esx04.rainpole.local	172.18.12.104	255.255.255.0

- g When you have updated the Excel file, save it in the CSV file format and close Excel.
- h Click the **Configure** tab.
- i Click the **Edit Host Customizations** button.

- j In the **Edit Host Customizations** window select all hosts and click **Next**.
 - k Click the **Browse** button to use a customization file, locate the *NYC01_host_customizations.csv* file saved earlier and select it and click **Open** then click **Finish**.
- 5 Remediate the hosts in the consolidated cluster .
- a Click the **Monitor** tab and click **Compliance**.
 - b Select **NYC01** and click the **Check Host Profile Compliance** button.
 - c Select **nyc01esx02.rainpole.local**, click the **Remediate host based on its host profile** button, and click **Finish** on the **Ready to complete** window.
 - d Select **nyc01esx03.rainpole.local**, click the **Remediate host based on its host profile** button, and click **Finish** on the **Ready to complete** window.
 - e Select **nyc01esx04.rainpole.local**, click the **Remediate host based on its host profile** button, and click **Finish** on the **Ready to complete** window.
- 6 Add the vMotion IP stack gateway.
- a In the **Navigator**, select **Hosts and Clusters** and expand the **nyc01vc01.rainpole.local** tree.
 - b Select the ESXi host **nyc01esx02.rainpole.local** and click **configure** tab.
 - c In the **configure** tab, under **Networking** click on **TCP/IP configuration**.
 - d Select **vMotion** from the **TCP/IP Stacks** and choose edit.
 - e In the **TCP/IP Stack Configuration window** select **Routing** tab.
 - f Under **VMkernel gateway** enter **172.18.12.253** and click **OK**.
- Repeat this for all the other Esxi hosts in the cluster.
- 7 Verify the Host Compliance.
- a Click the **Monitor** tab and click **Compliance**.
 - b Select **NYC01** and click the **Check Host Profile Compliance** button.
- All hosts should show a **Compliant** status in the **Host Compliance** column.
- 8 Schedule nightly compliance checks.
- a On the **Policies and Profiles** page, click **NYC01**, click the **Monitor** tab, and then click the **Scheduled Tasks** subtab.
 - b Click **Schedule a New Task** then click **Check Host Profile Compliance**.
 - c In the **Check Host Profile Compliance (scheduled)** window click **Scheduling Options**.
 - d Enter **NYC01 compliance Check** in the **Task Name** field.
 - e Click the **Change** button on the **Configured Scheduler** line.

- f In the **Configure Scheduler** window select **Setup a recurring schedule for this action** and change the **Start time** to **10:00 PM** and click **OK**.
- g Click **OK** in the **Check Host Profile Compliance (scheduled)** window.

Set vSAN Policy in ROBO

After you apply the host profile to all the hosts, set the storage policy of the vCenter Server to the vSAN Default Storage Policy.

Set the Platform Services Controller and vCenter Server appliances to the default vSAN storage policy.

Procedure

- 1 Log in to vCenter Server by using the vSphere Web Client.
 - a Open a Web browser and go to **https://nyc01vc01.rainpole.local/vsphere-client**.
 - b Log in using the following credentials.

Setting	Value
User name	administrator@vsphere.local
Password	vsphere_admin_password

- 2 In the **Navigator**, click **Hosts and Clusters**.
- 3 Expand the **nyc01vc01.rainpole.local** tree.
- 4 Select the **nyc01vc01** virtual machine.
- 5 Click the **Configure** tab, click **Policies**, and click **Edit VM Storage Policies**.
- 6 In the **mgmt01psc01:Manage VM Storage Policies** dialog box, from the **VM storage policy** drop down menu, select **Virtual SAN Default Storage Policy**, and click **Apply to all**.
- 7 Click **OK** to apply the changes.
- 8 Verify that the **Compliance Status** column shows a **Compliant** status for all items in the table.

Create the VM and Template Folders in ROBO

Create folders to group objects of the same type for easier management.

Procedure

- 1 Log in to vCenter Server by using the vSphere Web Client.
 - a Open a Web browser and go to **https://nyc01vc01.rainpole.local/vsphere-client**.
 - b Log in using the following credentials.

Setting	Value
User name	administrator@vsphere.local
Password	vsphere_admin_password

- 2 Create a folder for the vRealize Log Insight management application.
 - a In the **Navigator**, click **VMs and Templates**.
 - b Expand the **nyc01vc01.rainpole.local** tree.
 - c Right-click the **NYC01** data center, and select **New Folder > New VM and Template Folder**.
 - d In the **New Folder** dialog box enter **MGMT01** as the name to label the folder, and click **OK**.
 - e Repeat this step to create the remaining folders.

Management Applications	Folder
vCenter Server Appliance + Update Manager Download Service	MGMT01
vRealize Log Insight	vRLI01
vRealize Automation (Proxy Agent) + vRealize Business (Data Collector)	vRA01IAS
vRealize Operations Manager (Remote Collectors)	vROps01RC
NSX Manager + Controllers + Edges	NSX01
vSphere Data Protection	BCDR01

- 3 Move the vCenter Server virtual machine to the MGMT01 folder.
 - a In the **Navigator**, click **VMs and Templates**.
 - b Expand the **nyc01vc01.rainpole.local** tree.
 - c Expand the **Discovered Virtual Machines** folder.
 - d Drag **nyc01vc01** to the **MGMT01** folder.
- 4 Delete the **Discovered Virtual Machines** folder.
 - a In the **Navigator**, click **VMs and Templates**.
 - b Expand the **nyc01vc01.rainpole.local** tree.
 - c Right click the **Discovered Virtual Machines** folder and choose **Remove from Inventory**.

Deploy and Configure the NSX Instance in ROBO

Deploy and configure the NSX instance for the consolidated cluster in your ROBO deployment.

Procedure

1 Deploy the NSX Manager in ROBO

For this ROBO implementation, NSX Manager and vCenter Server have a one-to-one relationship. For every instance of NSX Manager, there is one connected vCenter Server.

2 Replace the NSX Manager Certificate in ROBO

After you replace the certificate on the vCenter Server instance, replace the certificate for the NSX Manager instance.

3 Deploy the NSX Controllers for the NSX Instance in ROBO

After the NSX Manager is successfully connected to the vCenter Server, you must deploy the three NSX Controller nodes that form the NSX Controller cluster. You must deploy every node only after the previous one is successfully deployed.

4 Assign Licensing for NSX Instance in ROBO

Assign licensing for the NSX Instance in your ROBO location.

5 Prepare the ESXi Hosts in the Consolidated Cluster for NSX in ROBO

NSX kernel modules packaged in VIB files run within the hypervisor kernel, and provide services such as distributed routing, distributed firewall, and VXLAN bridging capabilities. To use NSX, you must install the NSX kernel modules on the consolidated cluster ESXi hosts.

6 Configure the NSX Logical Network for the Consolidated Cluster in ROBO

After all the deployment tasks are ready, you can configure the NSX logical network for use with your ROBO deployment.

7 Update the Host Profile for the Consolidated Cluster in ROBO

When an authorized change is made to a host, the host profile must be updated to reflect the changes.

8 Configure NSX Dynamic Routing in ROBO

NSX for vSphere creates a network virtualization layer on top of which all virtual networks are created. This layer is an abstraction between the physical and virtual networks. You configure NSX dynamic routing within the consolidated cluster, deploying two NSX Edge devices and configure a Distributed Logical Router (DLR).

9 Distributed Firewall Configuration in ROBO

You define explicit rules for the distributed firewall which allows access to management applications and workloads in the consolidated cluster for your ROBO deployment.

10 Test the Consolidated Cluster NSX Configuration in ROBO

Test the configuration of the NSX logical network using a ping test. A ping test checks if two hosts in a network can reach each other over the network.

11 Deploy Application Virtual Networks in ROBO

Deploy the application virtual networks for ROBO.

Deploy the NSX Manager in ROBO

For this ROBO implementation, NSX Manager and vCenter Server have a one-to-one relationship. For every instance of NSX Manager, there is one connected vCenter Server.

To deploy the NSX Manager virtual appliance for the consolidated cluster, you first assign a domain service account which NSX uses as the vCenter Server Administrator role. You then deploy the NSX Manager virtual appliance for the consolidated cluster. After you deploy the NSX Manager, you connect it to the vCenter Server instance.

Assign an NSX Domain Service Account and Deploy the NSX Manager Appliance in ROBO

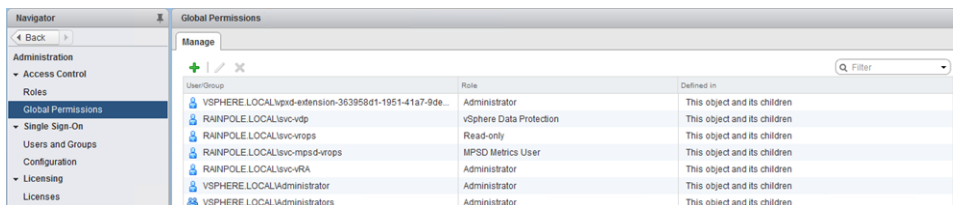
Assign a domain service account for use by NSX to access the vCenter Server Administrator role. Deploy the NSX Manager appliance from the OVF file to the NYC01-MGMT Resource Pool.

Procedure

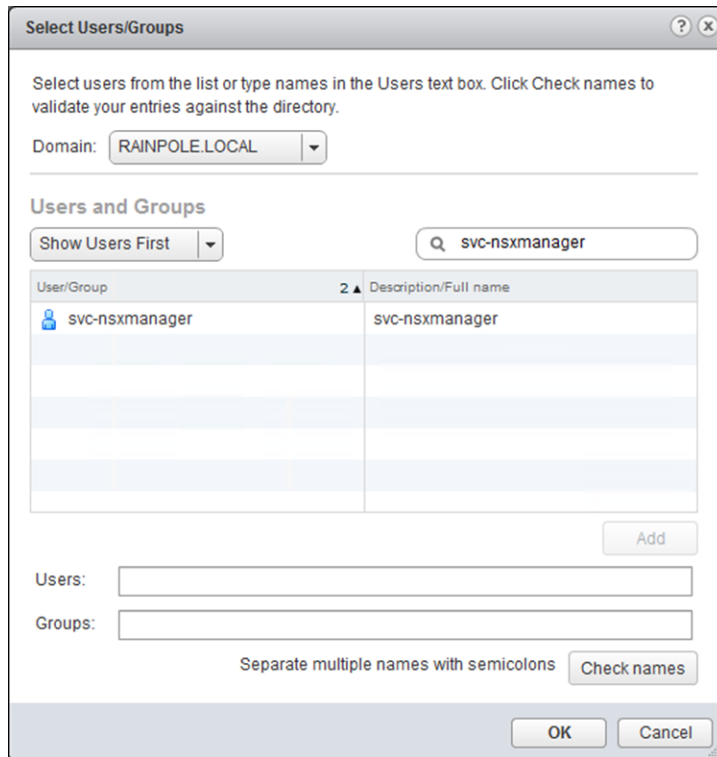
- 1 Log in to the vCenter Server by using the vSphere Web Client.
 - a Open a Web browser and go to **https://nyc01vc01.rainpole.local/vsphere-client**.
 - b Log in using the following credentials.

Setting	Value
User name	administrator@vsphere.local
Password	vsphere_admin_password

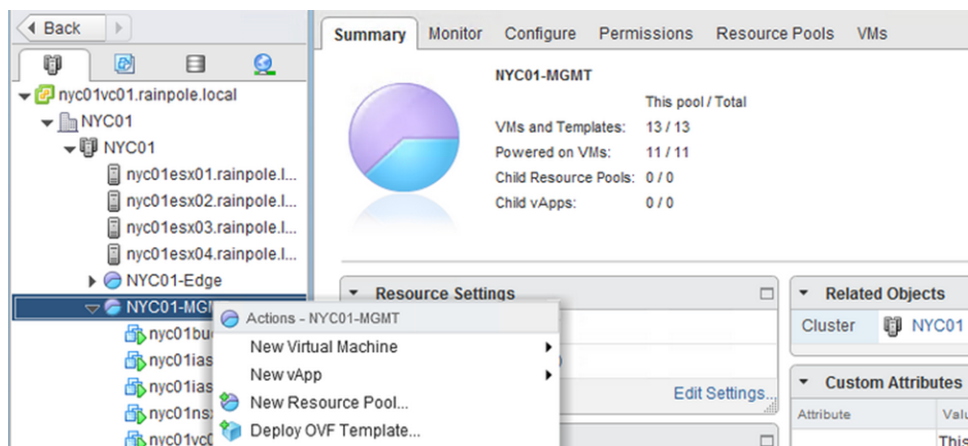
- 2 In the **Navigator**, click the **Home** icon and choose **Administration**. Click **Global Permissions**.
- 3 Click the **Add** icon.



- 4 In the **Global Permission Root - Add Permission** dialog box, click **Add**.
- 5 In the **Select Users/Groups** dialog box, select **rainpole.local** from the **Domain** drop-down menu.
- 6 In the **Search** box, enter **svc-nsxmanager** and press Enter.
- 7 Select **svc-nsxmanager** and click **Add**. Press **OK** to return to the **Global Permission Root - Add Permission** window.



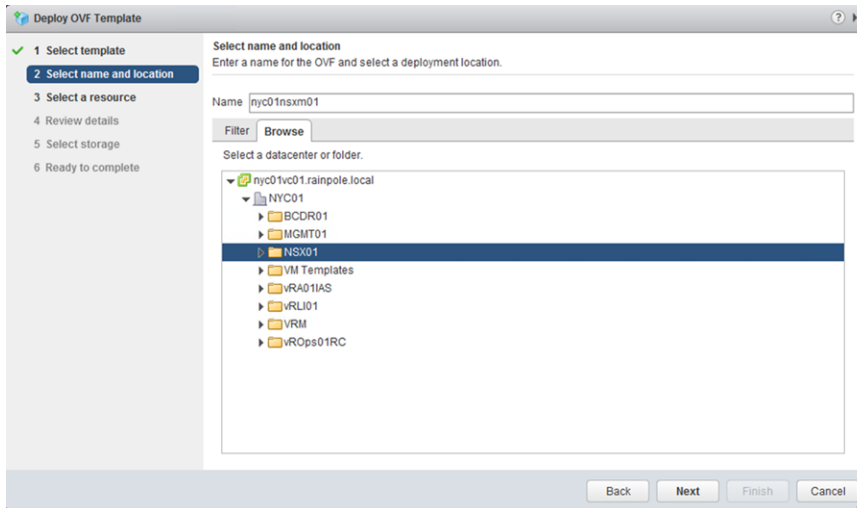
- 8 Click **OK** to give the svc-nsxmanager account vCenter Administrative privileges.
- 9 Click the **Home** icon and choose **Hosts and Clusters** to return to that page in the **Navigator**.
- 10 In the **Navigator** pane, expand the **nyc01vc01.rainpole.local** control tree.
- 11 Expand the **NYC01** cluster.
- 12 Right-click the **NYC01-MGMT** resource pool and click **Deploy OVF Template**.



- 13 On the **Select template** page, click the **Browse** button, select the VMware NSX Manager .ova file, and click **Next**.

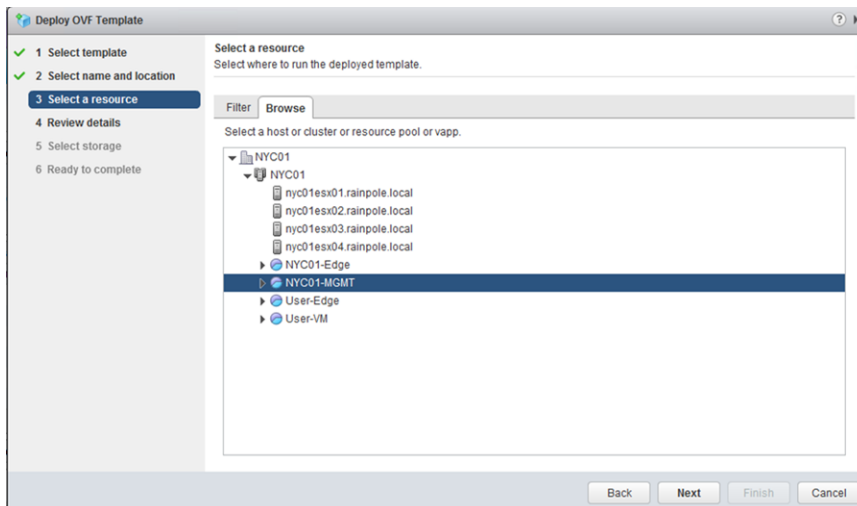
- 14 On the **Select name and location** page, enter the following settings, and click **Next**.

Setting	Value
Name	nyc01nsxm01
Select a datacenter or folder	NSX01



- 15 On the **Select a resource** page, select the following values, and click **Next**.

Setting	Value
Cluster	NYC01
Resource Pool	NYC01-MGMT



- 16 On the **Review details** page, click **Next**.
- 17 On the **Accept license agreements** page, click **Accept** and click **Next**.

- 18 On the **Select storage** page, enter the following settings, and click **Next**.

Setting	Value
Select virtual disk format	Thin provision
VM storage policy	Virtual SAN Default Storage Policy
Datastore	NYC01-VSAN01

- 19 On the **Setup networks** page, under **Destination Network**, select **vDS-NYC01-Management** and click **Next**.

- 20 On the **Customize template** page, expand all options, enter the following settings, and click **Next**.

Setting	Value
DNS Server List	172.18.11.4,172.16.11.4
Domain Search List	rainpole.local
Default IPv4 Gateway	172.18.11.253
Hostname	nyc01nsxm01.rainpole.local
Network 1 IPv4 Address	172.18.11.65
Network 1 Netmask	255.255.255.0
Enable SSH	Selected
NTP Server List	ntp.rainpole.local
CLI "admin" User Password / enter	<i>nyc01nsx_admin_password</i>
CLI "admin" User Password / confirm	<i>nyc01nsx_admin_password</i>
CLI Privilege Mode Password / enter	<i>nyc01nsx_privilege_password</i>
CLI Privilege Mode Password / confirm	<i>nyc01nsx_privilege_password</i>

- 21 On the **Ready to Complete** page, click **Finish**.
- 22 In the **Navigator**, expand the **nyc01vc01.rainpole.local** control tree, select the virtual machine **nyc01nsxm01**, and click the **Power on** button.

Connect NSX Manager to the vCenter Server in ROBO

After you deploy the NSX Manager virtual appliance for the consolidated cluster, connect the NSX Manager to the vCenter Server.

Prerequisites

Before connecting NSX Manager to vCenter Server, replace the NSX certificates. See [Replace the NSX Manager Certificate in ROBO](#).

Procedure

- 1 Connect the NSX Manager to the vCenter Server for ROBO.
 - a Open a Web browser and go to **https://nyc01nsxm01.rainpole.local**.
 - b Log in using the following credentials.

Setting	Value
User name	admin
Password	<i>nsx_manager_admin_password</i>

- 2 Click **Manage vCenter Registration**.
- 3 Under **Lookup Service URL**, click the **Edit** button.
- 4 In the **Lookup Service URL** dialog box, enter the following settings, and click **OK**.

Setting	Value
Lookup Service Host	nyc01vc01.rainpole.local
Lookup Service Port	443
SSO Administrator User Name	administrator@vsphere.local
Password	<i>vsphere_admin_password</i>

- 5 In the **Trust Certificate?** dialog box, click **Yes**.
- 6 Under **vCenter Server**, click the **Edit** button.
- 7 In the **vCenter Server** dialog box, enter the following settings and click **OK**.

Setting	Value
vCenter Server	nyc01vc01.rainpole.local
vCenter User Name	svc-nsxmanager@rainpole.local
Password	<i>svc-nsxmanager_password</i>

- 8 In the **Trust Certificate?** dialog box, click **Yes**.
- 9 Wait for the **Status** indicators for the Lookup Service and vCenter Server to change to a Connected status.

Assign Administrative Access to NSX in ROBO

Assign the `administrator@vsphere.local` account access to NSX for your ROBO deployment.

Procedure

- 1 Log in to vCenter Server by using the vSphere Web Client.
 - a Open a Web browser and go to `https://nyc01vc01.rainpole.local/vsphere-client`.
 - b Log in using the following credentials.

Setting	Value
User name	<code>svc-nsxmanager@rainpole.local</code>
Password	<code>svc-nsxmanager_password</code>

- 2 In the **Navigator**, click **Networking & Security** and click **NSX Managers**.
- 3 Under **NSX Managers**, click the **172.18.11.65** instance.
- 4 Click the **Manage** tab, click **Users** and click the **Add** icon.
- 5 On the **Identify User** page, enter `administrator@vsphere.local` in the **User** text field and click **Next**.
- 6 On the **Select Roles** page, select the **Enterprise Administrator** radio button and click **Finish**.

Replace the NSX Manager Certificate in ROBO

After you replace the certificate on the vCenter Server instance, replace the certificate for the NSX Manager instance.

Table 2-3. Certificate-Related Files on the NSX Manager Instances in Region A

NSX Manager FQDN	Certificate File Name	Replacement Time
<code>nyc01nsxm01.rainpole.local</code>	■ <code>nyc01nsxm01.4.p12</code> from the automation generation	Right after deployment of NSX Manager instance

Procedure

- 1 On the Windows host that has access to the data center, log in to the NSX Manager Web interface.
 - a Open a Web Browser and go to following URL `https://nyc01nsxm01.rainpole.local`
 - b Log in using the following credentials.

Setting	Value
User name	<code>admin</code>
Password	<code>nsx_manager_admin_password</code>

- 2 Click the **Manage Appliance Settings** button.
- 3 On the **Manage** tab, click **SSL Certificates** and click **Upload PKCS#12 Keystore**.

- 4 Browse to the certificate chain file, provide the keystore password or passphrase and click **Import**.
- 5 In the right corner of the NSX Manager user interface, click the **Settings** icon.
- 6 From the drop-down menu, select **Reboot Appliance**.

The NSX Manager restarts, which in turn propagates the CA-signed certificate.

Deploy the NSX Controllers for the NSX Instance in ROBO

After the NSX Manager is successfully connected to the vCenter Server, you must deploy the three NSX Controller nodes that form the NSX Controller cluster. You must deploy every node only after the previous one is successfully deployed.

Procedure

- 1 Log in to vCenter Server by using the vSphere Web Client.
 - a Open a Web browser and go to **`https://nyc01vc01.rainpole.local/vsphere-client`**.
 - b Log in using the following credentials.

Setting	Value
User name	administrator@vsphere.local
Password	vsphere_admin_password

- 2 Configure an IP pool for the NSX Controller cluster
 - a Click the **Home** icon and choose **Networking & Security**.
 - b In the **Navigator**, click **NSX Managers**.
 - c Under **NSX Managers**, click the **172.18.11.65** instance.

- d Click the **Manage** tab, click **Grouping Objects**, click **IP Pools**, and click the **Add New IP Pool** icon.
- e In the **Add Static IP Pool** dialog box, enter the following settings and click **OK**.

Setting	Value
Name	NYC01-NSXC01
Gateway	172.18.11.253
Prefix Length	24
Primary DNS	172.18.11.4
Secondary DNS	172.16.11.4
DNS Suffix	rainpole.local
Static IP Pool	172.18.11.118-172.18.11.120

Add Static IP Pool

Name: * NYC01-NSXC01

Gateway: * 172.18.11.253
A gateway can be any IPv4 or IPv6 address.

Prefix Length: * 24

Primary DNS: 172.18.11.4

Secondary DNS: 172.16.11.4

DNS Suffix: rainpole.local

Static IP Pool: * 172.18.11.118-172.18.11.120
for example 192.168.1.2-192.168.1.100 or
abcd:87:87::10-abcd:87:87::20

OK Cancel

3 Deploy the NSX Controller cluster.

- a In the **Navigator**, click the **Home** icon and choose **Networking & Security** to go back, then click **Installation**.
- b On the **Management** tab, under **NSX Controller nodes**, click the **Add** icon to deploy three NSX Controller nodes with the same configuration.
- c In the **Add Controller page**, enter the following settings and click **OK**. You configure a password only during the deployment of the first controller. The other controllers will use the same password.

Setting	Value
Name	nsx-controller-nyc-01
NSX Manager	172.18.11.65

Setting	Value
Datacenter	NYC01
Cluster/Resource Pool	NYC01-Edge
Datastore	NYC01-VSAN01
Folder	NSX01
Connected To	vDS-NYC01-Management
IP Pool	NYC01-NSXC01
Password	nycnsx_controllers_password
Confirm Password	nycnsx_controllers_password

Add Controller

Name: * nsx-controller-nyc01

NSX Manager: * 172.18.11.65

Datacenter: * NYC01

Cluster/Resource Pool: * NYC01-Edge

Datastore: * NYC01-VSAN01

Host:

Folder: NSX01

Connected To: * vDS-NYC01-Management Change Remove

IP Pool: * NYC01-NSXC01 Select

Password: *

Confirm password: *

OK Cancel

- d When the status of the controller node changes to Connected, repeat the step and deploy the two remaining NSX Controller nodes in the controller cluster using the same configuration.
- 4 Configure DRS affinity rules for the NSX Controller nodes.
 - a Return to the Home page.
 - b In the Navigator, click **Hosts and Clusters** and expand the **nyc01vc01.rainpole.local** tree control.
 - c Select the **NYC01** cluster, and click the **Configure** tab.
 - d Under **Configuration** click **VM/Host Rules**.

- e Click **Add**.
- f In the **NYC01 - Create VM/Host Rule** dialog box, enter the following settings and click **Add**.

Setting	Value
Name	anti-affinity-rule-nsxcontrollers
Enable rule	Selected
Type	Separate Virtual Machine

- g In the **Add Rule Member** dialog box, select the check box next to each of the three NSX Controller virtual machines and click **OK**.
- h In the **NYC01 - Create VM/Host Rule** dialog box, click **OK**.

Assign Licensing for NSX Instance in ROBO

Assign licensing for the NSX Instance in your ROBO location.

Procedure

- 1 Log in to vCenter Server by using the vSphere Web Client.
 - a Open a Web browser and go to **<https://nyc01vc01.rainpole.local/vsphere-client>**.
 - b Log in using the following credentials.

Settings	Value
User name	administrator@vsphere.local
Password	vsphere_admin_password

- 2 Add new licenses for this NSX instance.
 - a Click the **Home** icon above the Navigator and choose the **Administration** menu item.
 - b On the **Administration page**, under **Licensing** and select **Licenses**.
 - c Under **Licenses** , click on **Licenses** tab.
 - d Click the **Create New Licenses** icon to add license keys.
 - e On the **Enter license keys** page, enter license keys for **NSX**, and click **Next**.
 - f On the **Edit license name page**, enter **License name** and click **Next**.
 - g On the **Ready to complete** page, review your entries and click **Finish**.

Prepare the ESXi Hosts in the Consolidated Cluster for NSX in ROBO

NSX kernel modules packaged in VIB files run within the hypervisor kernel, and provide services such as distributed routing, distributed firewall, and VXLAN bridging capabilities. To use NSX, you must install the NSX kernel modules on the consolidated cluster ESXi hosts.

Install the NSX kernel modules on the management cluster ESXi hosts.

Procedure

- 1 Log in to vCenter Server by using the vSphere Web Client.
 - a Open a Web browser and go to **<https://nyc01vc01.rainpole.local/vsphere-client>**.
 - b Log in using the following credentials.

Setting	Value
User name	administrator@vsphere.local
Password	vsphere_admin_password

- 2 In the **Navigator**, click the **Home** icon and choose **Networking & Security**.
- 3 Click **Installation** and click the **Host Preparation** tab.
- 4 Select **172.18.11.65** from the **NSX Manager** drop-down menu.
- 5 Under **Installation Status**, click **Install** for the **NYC01** cluster, and click **Yes** in the confirmation dialog box..
- 6 Verify that the **Installation Status** column displays the NSX version for all hosts in the cluster, confirming that you have successfully installed the NSX kernel modules.

Installation		
Management	Host Preparation	Logical Network Preparation Service Deployments
NSX Manager: 172.18.11.65		
NSX Component Installation on Hosts		
Actions		
Clusters & Hosts	Installation Status	Firewall
▼ NYC01	✓ 6.3.0.5007049	✓ Enabled
nyc01esx01.rainpole.local	✓ 6.3.0.5007049	✓ Enabled
nyc01esx04.rainpole.local	✓ 6.3.0.5007049	✓ Enabled
nyc01esx03.rainpole.local	✓ 6.3.0.5007049	✓ Enabled
nyc01esx02.rainpole.local	✓ 6.3.0.5007049	✓ Enabled

Configure the NSX Logical Network for the Consolidated Cluster in ROBO

After all the deployment tasks are ready, you can configure the NSX logical network for use with your ROBO deployment.

To configure the NSX logical network, perform the following tasks:

- Configure the Segment ID allocation.
- Configure the VXLAN networking.
- Configure the Transport Zone.

Procedure

- 1 Log in to vCenter Server by using the vSphere Web Client.
 - a Open a Web browser and go to **`https://nyc01vc01.rainpole.local/vsphere-client`**.
 - b Log in using the following credentials.

Setting	Value
User name	administrator@vsphere.local
Password	vsphere_admin_password

- 2 Configure the Segment ID allocation.
 - a In the **Navigator**, click the **Home** icon and choose **Networking & Security**.
 - b Click **Installation**, click the **Logical Network Preparation** tab, and click **Segment ID**.

- c Select **172.18.11.65** from the **NSX Manager** drop-down menu.
- d Click **Edit**, enter the following values, and click **OK**.

Setting	Value
Segment ID pool	5000-9000
Enable Multicast addressing	Selected
Multicast addresses	239.18.0.0-239.18.255.255

Edit Segment IDs and Multicast Address Allocation ?

Provide a Segment ID pool and Multicast range unique to this NSX Manager.

Segment ID pool: * 5000-9000
(In the range of 5000-16777215)

☒ Enable Multicast addressing
Multicast addresses are required only for Hybrid and Multicast control plane modes.

Multicast addresses: * 239.18.0.0-239.18.255.255
(Recommended range - 239.0.0.0-239.255.255.255)

OK Cancel

- 3 Configure the VXLAN networking.
 - a Click the **Host Preparation** tab.
 - b Under **VXLAN**, click **Not Configured**, enter the following values, and click **OK**.

Setting	Value
Switch	vDS-NYC01
VLAN	1814
MTU	9000
VMKNic IP Addressing	Use DHCP
VMKNic Teaming Policy	Load Balance - SRCID
VTEP	2

4 Configure the transport zone.

- a On the **Installation** page, click the **Logical Network Preparation** tab and click **Transport Zones**.
- b Click the **Add New Transport zone** icon.
- c In the **New Transport Zone** dialog box, enter the following settings and click **OK**.

Setting	Value
Name	NYC01
Replication mode	Hybrid
Select clusters that will be part of the Transport Zone	NYC01

New Transport Zone

Name:

Description:

Replication mode: ☐ Multicast
Multicast on Physical network used for VXLAN control plane.
☐ Unicast
VXLAN control plane handled by NSX Controller Cluster.
☒ Hybrid
Optimized Unicast mode. Offloads local traffic replication to physical network.

Select clusters that will be part of the Transport Zone

	Name	NSX vSwitch	Status
<input checked="" type="checkbox"/>	NYC01	vDS-NYC01	Normal
<input type="checkbox"/>			
<input type="checkbox"/>			
<input type="checkbox"/>			
<input type="checkbox"/>			
<input type="checkbox"/>			
<input type="checkbox"/>			
<input type="checkbox"/>			

OK Cancel

Update the Host Profile for the Consolidated Cluster in ROBO

When an authorized change is made to a host, the host profile must be updated to reflect the changes.

Procedure

- 1 Log in to vCenter Server by using the vSphere Web Client.
 - a Open a Web browser and go to **https://nyc01vc01.rainpole.local/vsphere-client**.
 - b Log in using the following credentials.

Setting	Value
User name	administrator@vsphere.local
Password	vsphere_admin_password

- 2 Update the host profile for the management cluster.
 - a In the **Navigator**, click the **Home** icon and select **Policies and Profiles**.
 - b Click **Host Profiles**, right click **NYC01**, and select **Copy settings from Host**.
 - c Select **nyc01esx01.rainpole.local** and click **OK**.
- 3 Verify compliance for the hosts in the management cluster.
 - a Click the **Monitor** tab and click **Compliance**.
 - b Select **NYC01** and click the **Check Host Profile Compliance** button.

All hosts must display a **Host Compliance** status of **Compliant**.

Host/Cluster	Host Compliance	Last Checked
NYC01	✓ 4	2/3/2017 1:02 PM
nyc01esx01.rainpole.local	✓ Compliant	2/3/2017 1:02 PM
nyc01esx02.rainpole.local	✓ Compliant	2/3/2017 1:02 PM
nyc01esx03.rainpole.local	✓ Compliant	2/3/2017 1:02 PM
nyc01esx04.rainpole.local	✓ Compliant	2/3/2017 1:02 PM

Configure NSX Dynamic Routing in ROBO

NSX for vSphere creates a network virtualization layer on top of which all virtual networks are created. This layer is an abstraction between the physical and virtual networks. You configure NSX dynamic routing within the consolidated cluster, deploying two NSX Edge devices and configure a Distributed Logical Router (DLR).

Procedure

1 Create a Logical Switch for use as the Transit Network in ROBO

Create a Logical Switch for use as the transit network in your ROBO deployment.

2 Deploy NSX Edge Devices for North-South Routing in ROBO

3 Disable the Firewall Service in ECMP Edges in ROBO

Disable the firewall of the NSX Edge devices, this is required for equal-cost multi-path (ECMP) to operate correctly.

4 Enable and Configure BGP Routing in ROBO

The Border Gateway Protocol (BGP) is a protocol for exchanging routing information between gateway hosts (each with its own router) in a network of autonomous systems (AS).

5 Verify Peering of Upstream Switches and Establishment of BGP in ROBO

The NSX Edge devices need to establish a connection to each of the upstream BGP switches before BGP updates can be exchanged. Verify that the NSX Edges devices are successfully peering, and that BGP routing has been established.

6 Deploy the Distributed Logical Router in ROBO

7 Configure Distributed Logical Router for Dynamic Routing in ROBO

Configure the distributed logical router (DLR) to use dynamic routing in ROBO.

8 Verify Establishment of BGP for the Distributed Logical Router in ROBO

Verify that the DLR is successfully peering, and that BGP routing has been established.

Create a Logical Switch for use as the Transit Network in ROBO

Create a Logical Switch for use as the transit network in your ROBO deployment.

Procedure

1 Log in to vCenter Server by using the vSphere Web Client.

- a Open a Web browser and go to **`https://nyc01vc01.rainpole.local/vsphere-client`**.
- b Log in using the following credentials.

Setting	Value
User name	administrator@vsphere.local
Password	vsphere_admin_password

- 2 Click the **Home** icon and choose **Networking & Security**.
- 3 In the **Navigator**, click **Logical Switches**.
- 4 Select the NSX Manager instance labelled **172.18.11.65**.
- 5 Click the **Add** icon.

The **New Logical Switch** dialogue box appears.

- 6 In the **New Logical Switch** dialogue box, enter the following settings and click **OK**.

Setting	Value
Name	Transit Network
Transport Zone	NYC01
Replication Mode	Hybrid
Enable IP Discovery	Checked
Enable MAC Learning	Unchecked

Deploy NSX Edge Devices for North-South Routing in ROBO

Perform this procedure twice to deploy two identical NSX Edge devices. Enter the name and IP addresses for the respective device using the values shown in the tables.

NSX Edge Device	Device Name
NSX Edge Device 1	NYC01-ESG01
NSX Edge Device 2	NYC01-ESG02

Interface	Primary IP Address NYC01-ESG01	Primary IP Address NYC01-ESG02
Uplink01	172.18.16.2	172.18.16.3
Uplink02	172.18.17.3	172.18.17.2
NYC01-DLR01	172.18.18.1	172.18.18.2

Procedure

- 1 Log in to vCenter Server by using the vSphere Web Client.
 - a Open a Web browser and go to **<https://nyc01vc01.rainpole.local/vsphere-client>**.
 - b Log in using the following credentials.

Settings	Value
User name	administrator@vsphere.local
Password	vsphere_admin_password

- 2 Under **Inventories**, click **Networking & Security**.
- 3 In the **Navigator**, click **NSX Edges**.

- 4 Select **172.18.11.65** from the **NSX Manager** drop-down menu.
- 5 Click the **Add** icon to deploy a new NSX Edge.

The **New NSX Edge** wizard appears.

- a On the **Name and description** page, enter the following settings and click **Next**.

Settings	Value
Install Type	Edge Service Gateway
Name	NYC01-ESG01
Deploy NSX Edge	Selected
Enable High Availability	Deselected

- b On the **Settings** page, enter the following settings and click **Next**.

Settings	Value
User Name	admin
Password	<i>edge_admin_password</i>
Enable SSH access	Selected
Enable FIPS mode	Deselected
Enable auto rule generation	Selected
Edge Control Level logging	INFO

- c On the **Configure deployment** page, select the **Large** radio button to specify the Appliance Size and click the **Add** icon.

The **Add NSX Edge Appliance** dialog box appears.

- d In the **Add NSX Edge Appliance** dialog box, enter the following settings, click **OK**, and click **Next**.

Setting	Value
Cluster/Resource Pool	NYC01-Edge
Datastore	NYC01-VSAN01
Folder	NSX01

- e On the **Configure Interfaces** page, click the **Add** icon to configure the Uplink01 interface, enter the following settings, and click **OK**.

Setting	Value
Name	Uplink01
Type	Uplink
Connected To	vDS-NYC01-Uplink01
Connectivity Status	Connected
Primary IP Address	172.18.16.2
Subnet Prefix Length	24
MTU	9000
Send ICMP Redirect	Selected

- f Click the **Add** icon once again to configure the Uplink02 interface, enter the following settings, and click **OK**.

Setting	Value
Name	Uplink02
Type	Uplink
Connected To	vDS-NYC01-Uplink02
Connectivity Status	Connected
Primary IP Address	172.18.17.3
Subnet Prefix Length	24
MTU	9000
Send ICMP Redirect	Selected

- g Click the **Add** icon a third time to configure the DLR interface, enter the following settings, click **OK**, and click **Next**.

Setting	Value
Name	NYC01-DLR01
Type	Internal
Connected To	Transit Network
Connectivity Status	Connected
Primary IP Address	172.18.18.1
Subnet Prefix Length	24
MTU	9000
Send ICMP Redirect	Selected

- h On the **Default Gateway Settings** page, deselect the **Configure Default Gateway** check box and click **Next**.

- i On the **Firewall and HA** page, click **Next**.
 - j On the **Ready to Complete** page, review the configuration settings you entered and click **Finish**.
- 6 Repeat this procedure to configure another NSX edge using the settings for the second NSX Edge device.

Upon repeating the procedure to configure NYC01-ESG02, the **Ready to Complete** page in the **New NSX Edge** wizard must display the following values.

New NSX Edge

Ready to complete

Name and description

Name: NYC01-ESG02
 Install Type: Edge Services Gateway
 Tenant:
 Size: Large
 HA: Disabled
 Automatic Rule Generation: Enabled

NSX Edge Appliances

Resource Pool	Host
NYC01-Edge	

Interfaces

vNIC#	Name	IP Address	Subnet Prefix Length	Connected To
0	Uplink01	172.18.16.3*	24	vDS-NYC01-...
1	Uplink02	172.18.17.2*	24	vDS-NYC01-...
2	NYC01-DL...	172.18.18.2*	24	Transit Network

Back Next **Finish** Cancel

- 7 Configure DRS affinity rules for the Edge Services Gateways.
- a Go back to the **Home** page.
 - b In the **Navigator**, click **Hosts and Clusters**, and expand the **nyc01vc01.rainpole.local** tree control.
 - c Select the **NYC01** cluster, and click the **Configure** tab.
 - d Under **Configuration**, click **VM/Host Rules**.
 - e Click **Add**.

- f In the **NYC01 - Create VM/Host Rule** dialog box, enter the following settings and click **Add**.

Setting	Value
Name	anti-affinity-rule-ecmpedges
Enable rule	Selected
Type	Separate Virtual Machine

- g In the **Add Rule Member** dialog box, select the check box next to each of the two, newly deployed NSX ESGs, and click **OK**.
- h In the **NYC01 - Create VM/Host Rule** dialog box, click **OK**.

Disable the Firewall Service in ECMP Edges in ROBO

Disable the firewall of the NSX Edge devices, this is required for equal-cost multi-path (ECMP) to operate correctly.

Perform this procedure twice for each of the NSX Edge devices NYC01-ESG01 and NYC01-ESG02.

Procedure

- 1 Log in to vCenter Server by using the vSphere Web Client.
 - a Open a Web browser and go to **https://nyc01vc01.rainpole.local/vsphere-client**.
 - b Lo in using the following credentials.

Setting	Value
User name	administrator@vsphere.local
Password	vsphere_admin_password

- 2 Under **Inventories**, click **Networking & Security**.
- 3 In the **Navigator**, click **NSX Edges**.
- 4 Select **172.18.11.65** from the **NSX Manager** drop-down menu.
- 5 Double-click the **NYC01-ESG01** NSX Edge device.
- 6 Click the **Manage** tab and click **Firewall**.
- 7 On the Firewall page, click the **Disable** button.
- 8 Click the **Publish Changes** button.
- 9 Repeat this procedure for the NSX Edge device **NYC01-ESG02**.

Enable and Configure BGP Routing in ROBO

The Border Gateway Protocol (BGP) is a protocol for exchanging routing information between gateway hosts (each with its own router) in a network of autonomous systems (AS).

Repeat this procedure two times to enable BGP for both NSX Edge devices: NYC01-ESG01 and NYC01-ESG02.

Procedure

- 1 Log in to vCenter Server by using the vSphere Web Client.
 - a Open a Web browser and go to **https://nyc01vc01.rainpole.local/vsphere-client**.
 - b Log in using the following credentials.

Setting	Value
User name	administrator@vsphere.local
Password	vsphere_admin_password

- 2 Under **Inventories**, click **Networking & Security**.
- 3 In the **Navigator**, click **NSX Edges**.
- 4 Select **172.18.11.65** from the **NSX Manager** drop-down menu.
- 5 Double-click the **NYC01-ESG01** NSX Edge device.
- 6 Click the **Manage** tab, and click **Routing**.
- 7 On the **Global Configuration** page, enter the following settings.
 - a Click the **Enable** button for **ECMP**.
 - b Click the **Edit** button for **Dynamic Routing Configuration**.
 - c Choose **Uplink01** as the **Router ID**.
 - d Click **Publish Changes**.
- 8 On the **Routing** tab, select **Static Routes** to configure it.
 - a Click the **Add** icon, enter the following settings, and click **OK**.

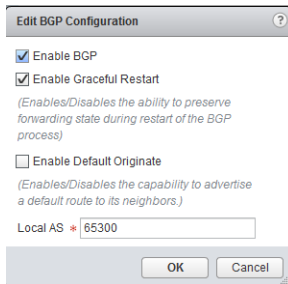
Setting	Value
Network	172.18.19.0/24
Next Hop	172.18.18.3
Interface	NYC01-DLR01
MTU	9000
Admin Distance	210

Note You must add all subnets that are behind the DLR.

- b Click **Publish Changes**.

- 9 On the **Routing** tab, select **BGP** to configure it.
- a Click the **Edit** button, enter the following settings, and click **OK**.

Setting	Value
Enable BGP	Selected
Enable Graceful Restart	Selected
Enable Default Originate	Deselected
Local AS	65300



- b Click the **Add** icon to add a neighbor.

The **New Neighbor** dialog box appears. You add two neighbors: the first Top of Rack Switch and the second Top of Rack Switch.

- c In the **New Neighbor** dialog box, enter the following values for the first Top of Rack Switch, and click **OK**.

Setting	Value
IP Address	172.18.16.1
Remote AS	65200
Weight	60
Keep Alive Time	4
Hold Down Time	12
Password	<i>BGP_password</i>

New Neighbour

IP Address : * 172.18.16.1

Remote AS : * 65200

Weight : 60

Keep Alive Time : 4 (Seconds)

Hold Down Time : 12 (Seconds)

(BGP Keep alive timer value needs to be one third of hold down timer)

Password : *****

BGP Filters :

Direction	Action	Network	IP Prefix GE	IP Prefix LE

0 items Copy

OK Cancel

- d Click the **Add** icon to add another neighbor.

The **New Neighbor** dialog box appears. Add the second Top of Rack switch, whose IP address is 172.18.17.1.

- e In the **New Neighbor** dialog box, enter the following values for the second Top of Rack Switch, and click **OK**.

Setting	Value
IP Address	172.18.17.1
Remote AS	65200
Weight	60
Keep Alive Time	4
Hold Down Time	12
Password	<i>BGP_password</i>

New Neighbour

IP Address : * 172.18.17.1

Remote AS : * 65200

Weight : 60

Keep Alive Time : 4 (Seconds)

Hold Down Time : 12 (Seconds)

(BGP Keep alive timer value needs to be one third of hold down timer)

Password : *****

BGP Filters :

Direction	Action	Network	IP Prefix GE	IP Prefix LE

0 items Copy

OK Cancel

- f Click the **Add** icon to add another Neighbor.

The **New Neighbor dialog** box appears. Configure the distributed logical router (DLR) as a neighbor.

- g In the **New Neighbor** dialog box, enter the following values, and click **OK**.

Setting	Value
IP Address	172.18.18.4
Remote AS	65300
Weight	60
Keep Alive Time	1
Hold Down Time	3
Password	<i>BGP_password</i>

- h Click **Publish Changes**.

The three neighbors you added are now visible in the **Neighbors** table.

- 10 On the **Routing** tab, select **Route Redistribution** to configure it.

- On the **Route Redistribution** page, click the **Edit** button.
- In the **Change Redistribution Settings** dialog box, select the **BGP** check box and click **OK**.
- Under **Route Redistribution** table, click the **Add** icon.
- In the **New Redistribution Criteria** dialog box, enter the following settings and click **OK**.

Setting	Value
Prefix	Any
Learner Protocol	BGP
OSPF	Deselected
Static routes	Selected
Connected	Selected
Action	Permit

- e Click **Publish Changes**.

The route redistribution configuration is now visible in the **Route Redistribution** table.

- 11 Repeat this procedure for the NYC01-ESG02 NSX Edge.

Verify Peering of Upstream Switches and Establishment of BGP in ROBO

The NSX Edge devices need to establish a connection to each of the upstream BGP switches before BGP updates can be exchanged. Verify that the NSX Edges devices are successfully peering, and that BGP routing has been established.

You repeat this procedure two times for each of the NSX Edge devices: NYC01-ESG01 and NYC01-ESG02.

Procedure

- 1 Log in to the NSX Edge device using a Secure Shell (SSH) client.
 - a Open an SSH connection to the **NYC01-ESG01** NSX Edge device.
 - b Log in using the following credentials.

Setting	Value
User name	admin
Password	edge_admin_password

- 2 Run the `show ip bgp neighbors` command to display information about the BGP connections to neighbors.

The BGP State will display `Established`, `UP` if you have peered with the upstream switches.

Note You have not yet created the distributed logical router (DLR), so it will not display the `Established`, `UP` status message.

```

nyc01-esg01.rainpole.local - PuTTY

BGP neighbor is 172.18.16.1, remote AS 65200,
BGP state = Established, up
Hold time is 12, Keep alive interval is 4 seconds
Neighbor capabilities:
  Route refresh: advertised and received
  Address family IPv4 Unicast:advertised and received
  Graceful restart Capability:advertised and received
  Restart remain time: 0
Received 736 messages, Sent 765 messages
Default minimum time between advertisement runs is 30 seconds
For Address family IPv4 Unicast:advertised and received
  Index 1 Identifier 0x2c18da3c
  Route refresh request:received 0 sent 0
  Prefixes received 24 sent 7 advertised 7
Connections established 1, dropped 32
Local host: 172.18.16.2, Local port: 179
Remote host: 172.18.16.1, Remote port: 12063

BGP neighbor is 172.18.17.1, remote AS 65200,
BGP state = Established, up
Hold time is 12, Keep alive interval is 4 seconds
Neighbor capabilities:
  Route refresh: advertised and received
  Address family IPv4 Unicast:advertised and received
  Graceful restart Capability:advertised and received
  Restart remain time: 0
Received 705 messages, Sent 696 messages
Default minimum time between advertisement runs is 30 seconds
For Address family IPv4 Unicast:advertised and received
  Index 2 Identifier 0x2c18da3c
  Route refresh request:received 0 sent 0
  Prefixes received 24 sent 7 advertised 7
Connections established 1, dropped 5
Local host: 172.18.17.3, Local port: 179
Remote host: 172.18.17.1, Remote port: 10886

BGP neighbor is 172.18.18.4, remote AS 65300,
BGP state = Established, up
Hold time is 3, Keep alive interval is 1 seconds
Neighbor capabilities:
  Route refresh: advertised and received
Byte 1646

```

- 3 Run the `show ip route` command to verify that you are receiving routes using BGP, and that there are multiple routes to BGP learned networks.

You verify multiple routes to BGP learned networks by locating the same route using a different IP address. The IP addresses are listed after the word *via* in the right-side column of the routing table output. In the image below there are two different routes to the following BGP networks: `0.0.0.0/0`, `172.18.11.0`. You can identify BGP networks by the letter B in the left-side column. Lines beginning with C (connected) have only a single route.

```

Codes: O - OSPF derived, I - IS-IS derived, B - BGP derived,
C - connected, S - static, L1 - IS-IS level-1, L2 - IS-IS level-2,
IA - OSPF inter area, E1 - OSPF external type 1, E2 - OSPF external type 2,
N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2

Total number of routes: 31

B      0.0.0.0/0      [20/0]      via 172.18.16.1
B      0.0.0.0/0      [20/0]      via 172.18.17.1
B      10.159.4.0/23   [20/0]      via 172.18.16.1
B      10.159.4.0/23   [20/0]      via 172.18.17.1
B      172.11.10.0/24   [20/0]      via 172.18.16.1
B      172.11.10.0/24   [20/0]      via 172.18.17.1
B      172.11.11.0/24   [20/0]      via 172.18.16.1
B      172.11.11.0/24   [20/0]      via 172.18.17.1
B      172.11.12.0/24   [20/0]      via 172.18.16.1
B      172.11.12.0/24   [20/0]      via 172.18.17.1
B      172.13.10.0/24   [200/0]     via 172.18.18.3
B      172.13.11.0/24   [200/0]     via 172.18.18.3
B      172.13.12.0/24   [200/0]     via 172.18.18.3
B      172.18.11.0/24   [20/0]      via 172.18.16.1
B      172.18.11.0/24   [20/0]      via 172.18.17.1
B      172.18.12.0/24   [20/0]      via 172.18.16.1
B      172.18.12.0/24   [20/0]      via 172.18.17.1
C      172.18.16.0/24   [0/0]       via 172.18.16.2
C      172.18.17.0/24   [0/0]       via 172.18.17.3
C      172.18.18.0/24   [0/0]       via 172.18.18.1
B      172.18.19.0/24   [200/0]     via 172.18.18.3
B      172.20.11.0/24   [20/0]      via 172.18.16.1
B      172.20.11.0/24   [20/0]      via 172.18.17.1
B      172.20.31.0/24   [20/0]      via 172.18.16.1
B      172.20.31.0/24   [20/0]      via 172.18.17.1
B      172.20.35.0/24   [20/0]      via 172.18.16.1
B      172.20.35.0/24   [20/0]      via 172.18.17.1
B      172.21.11.0/24   [20/0]      via 172.18.16.1
B      172.21.11.0/24   [20/0]      via 172.18.17.1
B      172.21.31.0/24   [20/0]      via 172.18.16.1
B      172.21.31.0/24   [20/0]      via 172.18.17.1
B      172.27.24.0/24   [20/0]      via 172.18.16.1
B      172.27.24.0/24   [20/0]      via 172.18.17.1
B      172.27.25.0/24   [20/0]      via 172.18.16.1
B      172.27.25.0/24   [20/0]      via 172.18.17.1
B      172.27.31.0/24   [20/0]      via 172.18.16.1
byte 2601

```

- 4 Repeat this procedure for the NSX Edge device **NYC01-ESG02**.

Deploy the Distributed Logical Router in ROBO

Deploy the distributed logical router (DLR).

Procedure

- 1 Log in to the vCenter Server by using the vSphere Web Client.
 - a Open a Web browser and go to **<https://nyc01vc01.rainpole.local/vsphere-client>**
 - b Log i.n using the following credentials.

Setting	Value
User name	administrator@vsphere.local
Password	vsphere_admin_password

- 2 Under **Inventories**, click **Networking & Security**.
- 3 In the **Navigator**, click **NSX Edges**.
- 4 Select **172.18.11.65** from the **NSX Manager** drop-down menu.
- 5 Click the **Add** icon to create a new DLR,
The New NSX Edge wizard appears.

- 6 On the **Name and description** page, enter the following settings, and click **Next**.

Setting	Value
Logical (Distributed) Router	Selected
Name	NYC01-DLR01
Deploy Edge Appliance	Selected
Enable High Availability	Selected

- 7 On the **Settings** page, enter the following settings, and click **Next**.

Setting	Value
User Name	admin
Password	<i>dlr_admin_password</i>
Enable SSH access	Selected
Enable FIPS mode	Deselected
Edge Control Level logging	INFO

- 8 On the **Configure deployment** page, and click the **Add** icon.

The **Add NSX Edge Appliance** dialog box appears.

- 9 In the **Add NSX Edge Appliance** dialog box, enter the following settings and click **Next**.

Setting	Value
Cluster/Resource Pool	NYC01-Edge01
Datastore	NYC01-VSAN01
Folder	NSX01

- 10 On the **Configure deployment** page, and click the **Add** icon a second time to add a second NSX Edge device.

The **Add NSX Edge Appliance** dialog box appears.

- 11 In the **Add NSX Edge Appliance** dialog box, enter the following settings and click **Next**.

Setting	Value
Resource Pool	NYC01-Edge01
Datastore	NYC01-VSAN01
Folder	NSX01

- 12 On the **Configure interfaces** page, under **HA Interface Configuration**, click **Select** and connect to **vDS-NYC01-Management**.

- 13 On the **Configure interfaces** page enter the following configuration settings and click **Next**.

Setting	Value
Primary IP Address	1.1.1.1

Setting	Value
Subnet Prefix Length	29

- a Click the **Add** icon. The **Add Interface** dialog box appears.
- b Enter the following settings in the **Add Interface** dialog box, and click **OK**.

Setting	Value
Name	Transit Network
Type	Uplink
Connected To	Transit Network
Connectivity Status	Connected
Primary IP Address	172.18.18.3
Subnet Prefix Length	24
MTU	9000

- 14 In the **Default gateway settings** page, deselect **Configure Default Gateway** and click **Next**.
- 15 In the **Ready to complete** page, click **Finish**.

Configure Distributed Logical Router for Dynamic Routing in ROBO

Configure the distributed logical router (DLR) to use dynamic routing in ROBO.

Procedure

- 1 Log in to vCenter Server by using the vSphere Web Client.
 - a Open a Web browser and go to **<https://nyc01vc01.rainpole.local/vsphere-client>**.
 - b Log in using the following credentials.

Setting	Value
User name	administrator@vsphere.local
Password	vsphere_admin_password

- 2 Under **Inventories**, click **Networking & Security**.
- 3 In the **Navigator**, click **NSX Edges**.
- 4 Select **172.18.11.65** from the **NSX Manager** drop-down menu.
- 5 Configure the Distributed Logical Router.
 - a Double-click **NYC01-DLR01**.
 - b Click the **Manage** tab, click **Routing**.
 - c On the **Global Configuration** page, under Routing Configuration **Enable ECMP**.
 - d Under Dynamic Routing Configuration, select **Transit Network** as the Router ID.

- e Select **Enable Logging**.
- f Click **Publish Changes**.

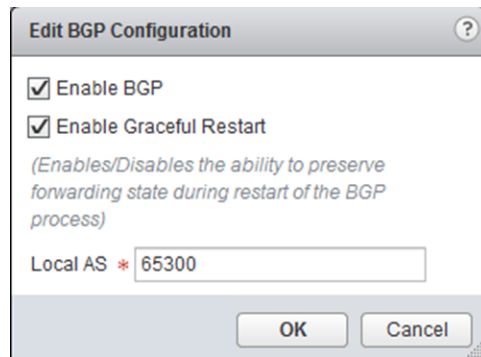
6 On the left, select **BGP** to configure it.

- a On the **BGP** page, click the **Edit** button.

The **Edit BGP Configuration** dialog box appears.

- b In the **Edit BGP Configuration** dialog box, enter the following settings and click **OK**.

Setting	Value
Enable BGP	Selected
Enable Graceful Restart	Selected
Local AS	65300



- c Click the **Add** icon to add a Neighbor.

The **New Neighbor** dialog box appears.

- d In the **New Neighbor** dialog box, enter the following values for both NSX Edge devices, and click **OK**.

Repeat this step two times to configure the DLR for both NSX Edge devices: **NYC01-ESG01** and **NYC01-ESG02**.

Setting	NYC01-ESG01 Value	NYC01-ESG02 Value
IP Address	172.18.18.1	172.18.18.2
Forwarding Address	172.18.18.3	172.18.18.3
Protocol Address	172.18.18.4	172.18.18.4
Remote AS	65300	65300
Weight	60	60
Keep Alive Time	1	1
Hold Down Time	3	3
Password	<i>BGP_password</i>	<i>BGP_password</i>

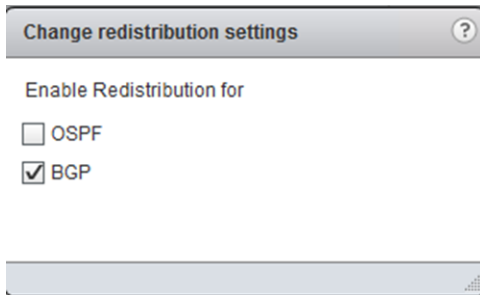
The screenshot shows the NSX Manager interface for the configuration of NYC01-DLR01. The 'Neighbors' table is as follows:

Forwarding A...	Protocol Addr...	IP Address	Remote AS	Weight	Keep Alive Time (Seconds)	Hold Down Time (Seconds)
172.18.18.3	172.18.18.4	172.18.18.1	65300	60	1	3
172.18.18.3	172.18.18.4	172.18.18.2	65300	60	1	3

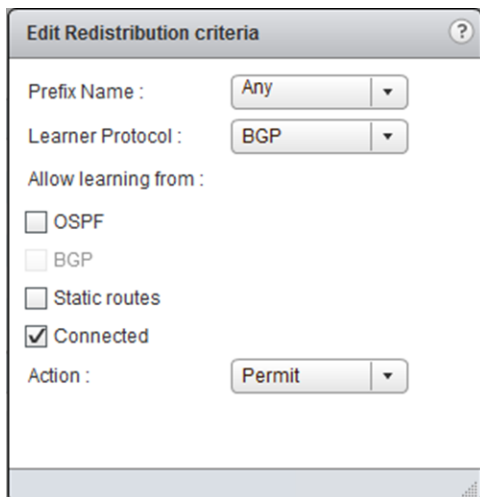
- e Click **Publish Changes**.

- 7 On the left, select **Route Redistribution** to configure it.
- a Click the **Edit** button. In the **Change redistribution settings** dialog box, enter the following settings, and click **OK**.

Setting	Value
OSPF	Deselected
BGP	Selected



- b On the **Route Redistribution table**, select the default **OSPF** entry and click the **Edit** button.
- c Select **BGP** from the **Learner Protocol** drop-down menu, and click **OK**.



- d Click **Publish Changes**.

Verify Establishment of BGP for the Distributed Logical Router in ROBO

Verify that the DLR is successfully peering, and that BGP routing has been established.

Procedure

- 1 Log in to the NYC01-DLR01 by using a Secure Shell (SSH) client.
 - a Open an SSH connection to NYC01-DLR01, the DLR whose peering and BGP configuration you want to verify.
 - b Log in using the following credentials.

Setting	Value
User name	admin
Password	<i>dlr_admin_password</i>

- 2 Run the `show ip bgp neighbors` command to display information about the BGP and TCP connections to neighbors.

The BGP State will display `Established`, `UP` if you have successfully peered with the Edge Service Gateway.

```

nyc01-dlr01.rainpole.local - PuTTY
NSX-edge-3-0> show ip bgp neighbors

BGP neighbor is 172.18.18.1, remote AS 65300,
BGP state = Established, up
Hold time is 3, Keep alive interval is 1 seconds
Neighbor capabilities:
  Route refresh: advertised and received
  Address family IPv4 Unicast:advertised and received
  Graceful restart Capability:advertised and received
  Restart remain time: 0
Received 4959 messages, Sent 4951 messages
Default minimum time between advertisement runs is 30 seconds
For Address family IPv4 Unicast:advertised and received
  Index 1 Identifier 0xe26f963c
  Route refresh request:received 0 sent 0
  Prefixes received 28 sent 5 advertised 5
Connections established 1, dropped 1
Local host: 172.18.18.4, Local port: 51773
Remote host: 172.18.18.1, Remote port: 179

BGP neighbor is 172.18.18.2, remote AS 65300,
BGP state = Established, up
Hold time is 3, Keep alive interval is 1 seconds
Neighbor capabilities:
  Route refresh: advertised and received
  Address family IPv4 Unicast:advertised and received
  Graceful restart Capability:advertised and received
  Restart remain time: 0
Received 4959 messages, Sent 4951 messages
Default minimum time between advertisement runs is 30 seconds
For Address family IPv4 Unicast:advertised and received
  Index 2 Identifier 0xe26f963c
  Route refresh request:received 0 sent 0
  Prefixes received 28 sent 5 advertised 5
Connections established 1, dropped 1
Local host: 172.18.18.4, Local port: 55041
Remote host: 172.18.18.2, Remote port: 179

NSX-edge-3-0>
  
```

- 3 Run the `show ip route` command to verify that you are receiving routes using BGP, and that there are multiple routes to BGP learned networks.

The letter `B` before the route indicates that BGP is used.

```

Codes: O - OSPF derived, I - IS-IS derived, B - BGP derived,
C - connected, S - static, L1 - IS-IS level-1, L2 - IS-IS level-2,
IA - OSPF inter area, E1 - OSPF external type 1, E2 - OSPF external type 2,
N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2

Total number of routes: 33

B      0.0.0.0/0      [200/0]      via 172.18.18.1
B      0.0.0.0/0      [200/0]      via 172.18.18.2
C      1.1.1.0/24     [0/0]        via 1.1.1.1
B      10.159.4.0/23  [200/0]      via 172.18.18.1
B      10.159.4.0/23  [200/0]      via 172.18.18.2
C      169.254.1.0/30 [0/0]        via 169.254.1.1
B      172.11.10.0/24 [200/0]      via 172.18.18.1
B      172.11.10.0/24 [200/0]      via 172.18.18.2
B      172.11.11.0/24 [200/0]      via 172.18.18.1
B      172.11.11.0/24 [200/0]      via 172.18.18.2
B      172.11.12.0/24 [200/0]      via 172.18.18.1
B      172.11.12.0/24 [200/0]      via 172.18.18.2
C      172.13.10.0/24 [0/0]        via 172.13.10.1
C      172.13.11.0/24 [0/0]        via 172.13.11.1
C      172.13.12.0/24 [0/0]        via 172.13.12.1
B      172.18.11.0/24 [200/0]      via 172.18.18.1
B      172.18.11.0/24 [200/0]      via 172.18.18.2
B      172.18.12.0/24 [200/0]      via 172.18.18.1
B      172.18.12.0/24 [200/0]      via 172.18.18.2
B      172.18.16.0/24 [200/0]      via 172.18.18.1
B      172.18.16.0/24 [200/0]      via 172.18.18.2
B      172.18.17.0/24 [200/0]      via 172.18.18.1
B      172.18.17.0/24 [200/0]      via 172.18.18.2
C      172.18.18.0/24 [0/0]        via 172.18.18.4
C      172.18.19.0/24 [0/0]        via 172.18.19.1
B      172.20.11.0/24 [200/0]      via 172.18.18.1
B      172.20.11.0/24 [200/0]      via 172.18.18.2
B      172.20.31.0/24 [200/0]      via 172.18.18.1
B      172.20.31.0/24 [200/0]      via 172.18.18.2
B      172.20.35.0/24 [200/0]      via 172.18.18.1
B      172.20.35.0/24 [200/0]      via 172.18.18.2
B      172.21.11.0/24 [200/0]      via 172.18.18.1
B      172.21.11.0/24 [200/0]      via 172.18.18.2
B      172.21.31.0/24 [200/0]      via 172.18.18.1
B      172.21.31.0/24 [200/0]      via 172.18.18.2
byte 253

```

Distributed Firewall Configuration in ROBO

You define explicit rules for the distributed firewall which allows access to management applications and workloads in the consolidated cluster for your ROBO deployment.

Add vCenter Server Instance to the NSX Distributed Firewall Exclusion List in ROBO

Exclude vCenter Server from all of your distributed firewall rules. This ensures that network access between vCenter Server and NSX is not blocked.

You configure NSX Distributed Firewall using vCenter Server. If a rule prevents access between NSX Manager and vCenter Server, you will not be able to manage the distributed firewall. For this reason, you must exclude vCenter Server from all of your distributed firewall rules, ensuring that access between the two products is not blocked.

Procedure

- 1 Log in to vCenter Server by using the vSphere Web Client.
 - a Open a Web browser and go to **https://nyc01vc01.rainpole.local/vsphere-client**.
 - b Log in using the following credentials.

Setting	Value
User name	administrator@vsphere.local
Password	vsphere_admin_password

- 2 In the **Navigator**, click **Networking & Security**.
- 3 Click **NSX Managers** and select the **172.18.11.65** instance.
- 4 Click **Manage** and then click **Exclusion List**.
- 5 Click the **Add** button.
- 6 Add **nyc01vc01** to the **Selected Objects list**, and click **OK**.

Create IP Sets for Management Components in the Consolidated Cluster in ROBO

Create IP sets for all ROBO management applications in the consolidated cluster. You use the IP sets later to create security groups for use with the distributed firewall rules.

You perform this procedure multiple times to configure all of the necessary IP sets. You allocate one IP set per group of applications.

Table 2-4. IP Sets for the Management Components in the Consolidated Cluster

Name	IP Addresses
vRealize Automation Proxy Agents	<i>vRealize-Automation-Proxy-Agents-IP's</i>
vRealize Business Data Collector	<i>vRealize-Business-Data-Collector_IP's</i>
vSphere Data Protection	<i>vSphere-Data-Protection_IP's</i>
vRealize Operations Manager Remote Collectors	<i>vRealize-Operations-Manager-Remote-Collectors_IP's</i>
vRealize Log Insight	<i>vRealize-Log-Insight_IP's</i>
Update Manager Download Service	<i>UMDS_IP's</i>
ROBO SDDC	<i>Management-VLAN_Subnets, Management-VXLAN_Subnets</i>
Administrators	<i>Ext-Management_Subnet</i>

Note *Management-VLAN_Subnets* and *Management-VXLAN_Subnets* includes the subnets in the ROBO site as well as the subnets in the SDDC hub sites.

You must also add the ROBO *Management-VLAN_Subnets* and *Management-VXLAN_Subnets* to the SDDC IP Set in the Hub.

Procedure

- 1 Log in to vCenter Server by using the vSphere Web Client.
 - a Open a Web browser and go to **https://nyc01vc01.rainpole.local/vsphere-client**.
 - b Log in using the following credentials.

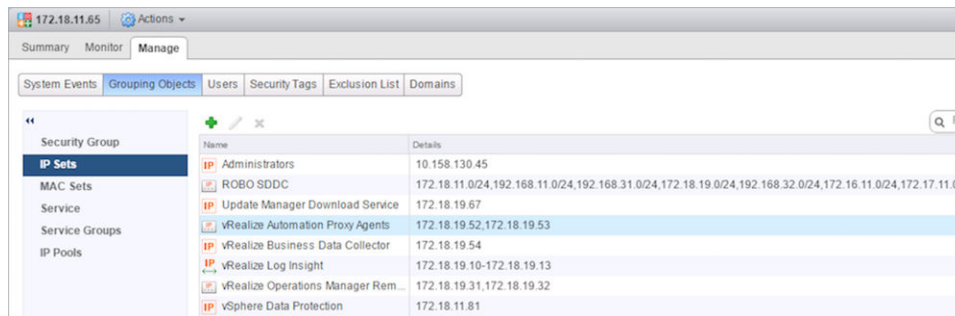
Setting	Value
User name	administrator@vsphere.local
Password	vsphere_admin_password

- 2 In the **Navigator**, click **Networking & Security**.
- 3 Click **NSX Managers** and select the **172.18.11.65** instance.
- 4 Click **Manage**, click **Grouping Objects**, and click **IP Sets**.
- 5 Click the **Add** icon.
- 6 In the **New IP Set** dialog box, configure the values for the IP set that you are adding, and click **OK**.

Setting	Value
Name	vRealize Automation Proxy Agents
IP Addresses	172.18.19.52,172.18.19.53

- 7 Repeat this procedure to create IP sets for all of the remaining components.

Figure 2-1. IP Sets



Create Security Groups in ROBO

Create security groups for use in configuring firewall rules for the groups of applications in the SDDC.

A security group is a collection of assets (or objects) from your vSphere inventory that you group together.

You perform this procedure multiple times to configure all of the necessary security groups. In addition, you create the VMware Appliances and Windows Servers groups from the security groups you add in the previous repetitions of this procedure.

Table 2-5. Security Groups for the Management Clusters Components in the Consolidated Cluster

Name	Object Type	Selected Object
vRealize Automation Proxy Agents	IP Sets	vRealize Automation Proxy Agents
vRealize Business Data Collector	IP Sets	vRealize Business Data Collector
vSphere Data Protection	IP Sets	vSphere Data Protection
vRealize Operations Manager Remote Collectors	IP Sets	vRealize Operations Manager Remote Collectors
vRealize Log Insight	IP Sets	vRealize Log Insight
Update Manager Download Service	IP Sets	Update Manager Download Service
ROBO SDDC	IP Sets	ROBO SDDC
Administrators	IP Sets	Administrators
Windows Servers	Security Groups	<ul style="list-style-type: none"> ■ vRealize Automation Proxy Agents
VMware Appliances	Security Groups	<ul style="list-style-type: none"> ■ vRealize Business Data Collector ■ vSphere Data Protection ■ vRealize Operations Manager Remote Collectors ■ vRealize Log Insight

Procedure

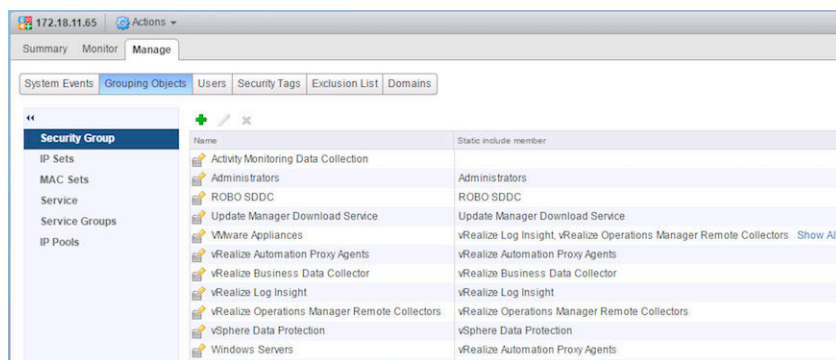
- 1 Log in to vCenter Server by using the vSphere Web Client.
 - a Open a Web browser and go to **https://nyc01vc01.rainpole.local/vsphere-client**.
 - b Log in using the following credentials.

Setting	Value
User name	administrator@vsphere.local
Password	vsphere_admin_password

- 2 In the **Navigator**, click **Networking & Security** and click **NSX Managers**.
- 3 Select the **172.18.11.65** NSX Manager instance, and click the **Manage** tab.
- 4 Click **Grouping Objects**, select **Security Group**, and click the **Add new Security Group** icon.
The **Add Security Group** wizard appears.
- 5 On the **Name and description** page, enter **vRealize Automation Proxy Agents** in the **Name** text box, and click **Next**.
- 6 On the **Define dynamic membership** page, click **Next**.
- 7 On the **Select objects to include** page, select **IP Sets** from the **Object Type** drop-down menu, select **vRealize Automation Proxy Agents** from the list of available objects, click the **Add** button, and click **Next**.
- 8 On the **Select Objects to exclude** page, leave the defaults , click **Next**.

- 9 On the **Ready to Complete** page, verify the configuration values that you entered and click **Finish**.
- 10 Repeat this procedure to create all of the necessary security groups.

Figure 2-2. Security Groups



Create Distributed Firewall Rules in ROBO

Create firewall rules that allow administrators to connect to the different VMware solutions.

Also create rules to allow user access to the vRealize Automation portal and to provide external connectivity to the SDDC.

A firewall rule consists of a section to segregate the firewall rules and the rule itself, which defines what network traffic is, or is not, blocked.

Procedure

- 1 Log in to vCenter Server by using the vSphere Web Client.
 - a Open a Web browser and go to **`https://nyc01vc01.rainpole.local/vsphere-client`**.
 - b Log in using the following credentials.

Setting	Value
User name	administrator@vsphere.local
Password	vsphere_admin_password

- 2 Add a section for the rules for the management applications.
 - a In the **Navigator**, click **Networking & Security** and click **Firewall**.
 - b From the **NSX Manager** drop-down menu, select **172.18.11.65**.
 - c Click the **Add Section** icon.
 - d In the **Add New Section** dialog box, enter **VMware Management Services** in the **Section Name** text box, select the **Add above** check box, and click **Save**.

- 3 Create a distributed firewall rule to allow SSH access to administrators for the different VMware appliances.
 - a Click **Add rule** in the VMware Management Services section.
 - b In the **Name** cell of the new rule, click the **Edit** icon to change the rule name to **Allow SSH to admins**.
 - c Click the **Edit** icon in the **Source** column, change the **Object Type** to **Security Groups**, add **Administrators** to the **Selected Objects** list, and click **OK**.
 - d Click the **Edit** icon in the **Destination** column, change the **Object Type** to **Security Groups**, add **VMware Appliances** and **Update Manager Download Service** to the **Selected Objects** list, and click **OK**.
 - e Click the **Edit** icon in the **Service** column, enter **SSH** in the filter, add **SSH** to the **Selected Objects** list, and click **OK**.
 - f Click **Publish Changes**.
- 4 Repeat the previous step to create the following distributed firewall rules.

Name	Source	Destination	Service / Port
Allow ROBO SDDC to any	ROBO SDDC	* any	* any
Allow RDP to admins	Administrators	Windows Servers	RDP
Allow VAMI to admins	Administrators	VMware Appliances	TCP:5480
Allow VDP to admins	Administrators	VMware Appliances	TCP:8543
Allow vRLI to admins	Administrators	vRealize Log Insight	HTTP HTTPS

- 5 Create a distributed firewall rule to deny all other traffic to the management subnets.
 - a Click **Add rule** in the VMware Management Services section.
 - b In the **Name** cell of the new rule, click the **Edit** icon to change the rule name to **Deny Management subnets**.
 - c Click the **IP** icon in the **Destination** column, enter **172.18.11.0/24,172.18.19.0/24** and click **OK**.
 - d Click the **Edit** icon in the **Action** column and change the action to **Block** and click **Save**.
 - e Click **Publish Changes**.

Figure 2-3. Distributed Firewall Rules

Firewall

Configuration | Saved Configurations | Settings

NSX Manager: 172.18.11.65

Last publish operation succeeded 3/23/2017 7:28:03 AM

General | Ethernet | Partner security services

No.

Name

Rule ID

Source

Destination

Service

Action

▼ VMware Management Services (Rule 1 - 7)

1

Allow SSH to admins

1010

Administrators

Update Manager Download Service
VMware Appliances

SSH

Allow

2

Allow ROBO SDDC to any

1009

ROBO SDDC

any

any

Allow

3

Allow RDP to admins

1008

Administrators

Windows Servers

RDP

Allow

4

Allow VMM to admins

1007

Administrators

VMware Appliances

TCP:5480

Allow

5

Allow VDP to admins

1006

Administrators

vSphere Data Protection

TCP:8543

Allow

6

Allow VRLI to admins

1011

Administrators

vRealize Log Insight

HTTP
HTTPS

Allow

7

Deny Management subnets

1005

any

172.18.11.0/24, 172.18.19.0/24

any

Block

Test the Consolidated Cluster NSX Configuration in ROBO

Test the configuration of the NSX logical network using a ping test. A ping test checks if two hosts in a network can reach each other over the network.

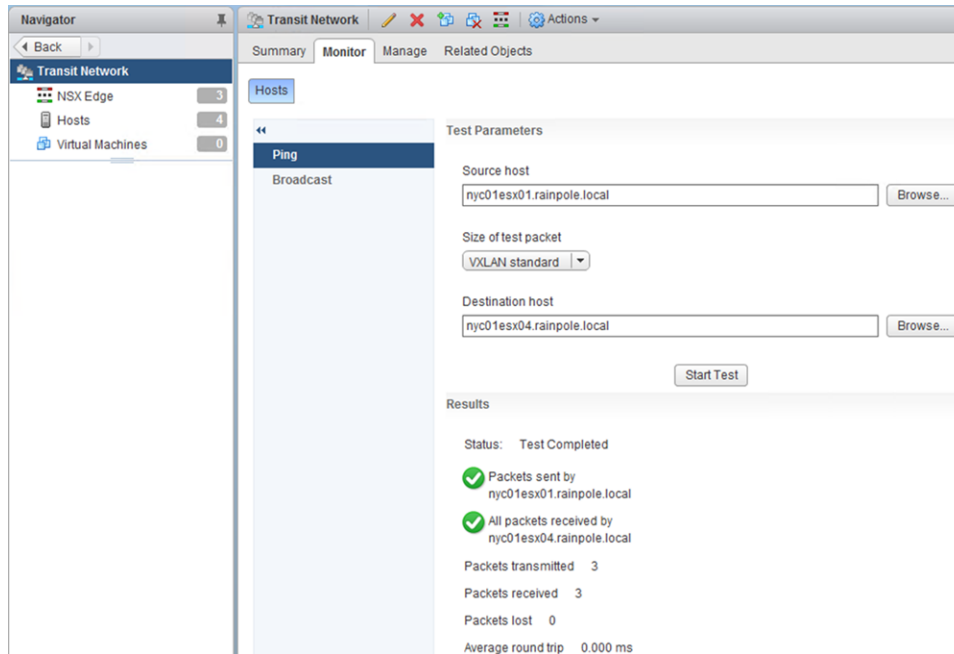
Procedure

- 1 Log in to vCenter Server by using the vSphere Web Client.
 - a Open a Web browser and go to **https://nyc01vc01.rainpole.local/vsphere-client**.
 - b Log in using the following credentials.

Settings	Value
User name	administrator@vsphere.local
Password	vsphere_admin_password

- 2 Use the Ping Monitor to test connectivity.
 - a Under **Logical Switches**, double-click **Transit Network**.
 - b Click the **Monitor** tab.
 - c From the **Source host** drop-down menu select **nyc01esx01.rainpole.local**.

- d From the **Destination host** drop-down menu select **nyc01esx04.rainpole.local**.
- e Click **Start Test**.



The host-to-host ping test results are displayed in the **Results** text box. Verify that there are no error messages.

Deploy Application Virtual Networks in ROBO

Deploy the application virtual networks for ROBO.

Procedure

- 1 Log in to vCenter Server by using the vSphere Web Client.
 - a Open a Web browser and go to **<https://nyc01vc01.rainpole.local/vsphere-client>**.
 - b Log in using the following credentials.

Settings	Value
User name	administrator@vsphere.local
Password	vsphere_admin_password

- 2 Create a Logical Switch for workloads specific to ROBO.
 - a Under **Inventories**, click **Networking & Security**.
 - b In the **Navigator**, click **Logical Switches**.
 - c Select **172.18.11.65** from the **NSX Manager** drop-down menu.

- d Click the **Add** icon to create a new Logical Switch.
- e In the **New Logical Switch** dialog box, enter the following settings, and click **OK**.

Setting	Value
Name	Mgmt-NYC01-VXLAN
Transport Zone	NYC01
Replication Mode	Hybrid

New Logical Switch

Name: * Mgmt-NYC01-VXLAN

Description:

Transport Zone: * NYC01 [Change](#) [Remove](#)

Replication mode:

☐ Multicast
Multicast on Physical network used for VXLAN control plane.

☐ Unicast
VXLAN control plane handled by NSX Controller Cluster.

☒ Hybrid
Optimized Unicast mode. Offloads local traffic replication to physical network.

☒ Enable IP Discovery

☐ Enable MAC Learning

OK **Cancel**

- 3 Connect the **Mgmt-NYC01-VXLAN** to the **DLR01** Distributed Logical Router.
 - a On the **Logical Switches** page, select the **Mgmt-NYC01-VXLAN** logical switch.
 - b Click the **Connect Edge** icon.
 - c On the **Connect an Edge** page, select **NYC01-DLR01** and click **Next**.

- d On the **Edit NSX Edge Interface** page, enter the following settings and click **Next**.

Setting	Value
Name	Mgmt-NYC01-VXLAN
Type	Internal
Connected To	Mgmt-NYC01-VXLAN
Connectivity Status	Connected
Primary IP Address	172.18.19.1
Subnet Prefix Length	24

- e On the **Ready to Complete** page click **Finish**.
- 4 Configure the MTU for the Logical Switches.
- On the **NSX Edges** page, double-click **NYC01-DLR01**.
 - Click the **Manage** tab, and click **Settings**.
 - On the **Settings** page, click **Interfaces**.

- d Under **Interfaces**, select **Mgmt-NYC01-VXLAN**, and click **Edit**.
- e On the **Edit Logical Router Interface** dialog box, specify a value of **9000** for the **MTU** value, and click **OK**.

Edit Logical Router Interface

Name: * Mgmt-NYC01-VXLAN

Type: ☒ Internal ☐ Uplink

Connected To: * Mgmt-NYC01-VXLAN Change Remove

Connectivity Status: ☒ Connected ☐ Disconnected

Configure Subnets:

+ ✎ ✕ Filter

Primary IP Address	Subnet Prefix Length
172.18.19.1	24

1 items Copy

MTU: 9000

OK Cancel

Deploy vSphere Data Protection in ROBO

Deploy vSphere Data Protection for backup and restore of SDDC management components in your remote office and branch office (ROBO) deployment.

vSphere Data Protection enables the backup and restore of virtual machines associated with the following components:

- vCenter Server and embedded Platform Services Controller for ROBO
- NSX Manager for the ROBO cluster
- vRealize Automation
- vRealize Operations Manager
- vRealize Log Insight

Procedure

1 [Prerequisites for Deploying vSphere Data Protection in ROBO](#)

Before you deploy vSphere Data Protection in the ROBO, verify that your environment satisfies the requirements for this deployment.

2 [Deploy the Virtual Appliance of vSphere Data Protection in ROBO](#)

Deploy vSphere Data Protection as a virtual appliance on the cluster in the ROBO.

3 [Install a CertGenVVD-Generated Certificate on vSphere Data Protection in ROBO](#)

After you use the VMware Validated Design Certificate Generation Utility (CertGenVVD) to generate certificates for the SDDC management components, replace the default VMware-signed certificate on vSphere Data Protection in the ROBO with the certificate that is generated by CertGenVVD.

4 [Configure Service Account Access in vSphere for Integration with vSphere Data Protection in ROBO](#)

Configure an operations service account with permissions that are required to enable vSphere Data Protection access to provide backup operations on the ROBO vCenter Server.

5 [Register vSphere Data Protection with Management vCenter Server in ROBO](#)

After you deploy the virtual appliance for vSphere Data Protection on the management cluster in the ROBO, complete the initial configuration of vSphere Data Protection.

Prerequisites for Deploying vSphere Data Protection in ROBO

Before you deploy vSphere Data Protection in the ROBO, verify that your environment satisfies the requirements for this deployment.

IP Addresses and Host Names

Verify that static IP address and FQDN for vSphere Data Protection are available for the ROBO SDDC deployment.

Table 2-6. IP Addresses and Host Names for vSphere Data Protection in ROBO

Network Setting	Value
IP address	172.18.11.81
FQDN	nyc01vdp01.rainpole.local
DNS servers	172.18.11.5
Default gateway	172.18.11.253
Subnet mask	255.255.255.0

Deployment Prerequisites

Verify that you have fulfilled the following prerequisites in addition to the networking settings.

Prerequisite	Value
Initial Storage	<ul style="list-style-type: none"> Virtual disk provisioning <ul style="list-style-type: none"> Thin Required storage <ul style="list-style-type: none"> Secondary Storage
Software Features	<ul style="list-style-type: none"> vSphere <ul style="list-style-type: none"> ROBO vCenter Server ROBO cluster with enabled vSphere DRS and HA ROBO cluster configured with resource pools for the management components, edge components and compute components. vSphere Distributed Switch configured for the vSphere management network
Installation Package	Download the .ova file of the vSphere Data Protection virtual appliance on the machine where you use the vSphere Web Client.

Deploy the Virtual Appliance of vSphere Data Protection in ROBO

Deploy vSphere Data Protection as a virtual appliance on the cluster in the ROBO.

vSphere Data Protection does not support deployment to resource pools within a cluster. The use of resource pools ensures that all management components within the ROBO SDDC receive adequate resources at runtime. After you deploy vSphere Data Protection appliance and configure it, you move the appliance under the NYC01-MGMT resource pool.

Procedure

- 1 Log in to vCenter Server by using the vSphere Web Client.
 - a Open a Web browser and go to **`https://nyc01vc01.rainpole.local/vsphere-client`**.
 - b Log in using the following credentials.

Setting	Value
User name	administrator@vsphere.local
Password	vsphere_admin_password

- 2 In the vSphere Web Client, navigate to the NYC01 cluster object.

Inventory Object	Value
vCenter Server	nyc01vc01.rainpole.local
Data center	NYC01
Cluster	NYC01

- 3 Right-click the **NYC01** cluster object and select **Deploy OVF Template**.
- 4 On the **Select template** page, select **Local file**, browse to the location of the vSphere Data Protection OVA file on your file system, and click **Next**.

- 5 On the **Select name and location** page, enter a node name, select the inventory folder for the virtual appliance, and click **Next**.

Setting	Value
Name	nyc01vdp01
vCenter Server	nyc01vc01.rainpole.local
Data center	NYC01
Folder	BCDR01

- 6 On the **Select a resource** page, click the **Browse** tab, select the **NYC01** cluster, and click **Next**.
- 7 On the **Review details** page, examine the virtual appliance details, such as product, version, download size, and size on disk, and click **Next**.
- 8 On the **Accept license agreements** page, accept the end user license agreement and click **Next**.
- 9 On the **Select storage** page, select the NFS datastore that is provisioned for vSphere Data Protection, configure storage settings, and click **Next**.

Setting	Value
Datastore	Secondary Storage
Select virtual disk format	Thin provision
VM storage policy	None

- 10 On the **Select networks** page, select the **vDS-NYC01-Management** distributed port group from the **Isolated Network** drop-down menu, select **IPv4** from the **IP protocol** drop-down menu and click **Next**.

Deploy OVF Template

1 Select template
2 Select name and location
3 Select a resource
4 Review details
5 Accept license agreements
6 Select storage
7 Select networks
8 Customize template
9 Ready to complete

Select networks
Select a destination network for each source network.

Source Network	Destination Network
Isolated Network	vDS-NYC01-Management

Description - Isolated Network
The Isolated Network network

IP Allocation Settings
IP protocol: IPv4
IP allocation: Static - Manual

Back Next Finish Cancel

- 11 On the **Customize template** page, enter the networking settings for the virtual appliance, and click **Next**.

IPv4 Setting	Value
DNS	172.18.11.4
Default Gateway	172.18.11.253
Network 1 IP Address	172.18.11.81
Network 1 Netmask	255.255.255.0

- 12 On the **Ready to complete** page, verify that the settings are correct and click **Finish**.
- 13 After the virtual appliance is deployed, right-click the virtual appliance object in the vSphere Web Client and select **Power > Power On**.

Install a CertGenVVD-Generated Certificate on vSphere Data Protection in ROBO

After you use the VMware Validated Design Certificate Generation Utility (CertGenVVD) to generate certificates for the SDDC management components, replace the default VMware-signed certificate on vSphere Data Protection in the ROBO with the certificate that is generated by CertGenVVD.

Procedure

- 1 Copy the .keystore file that CertGenVVD tool generated to the /root folder on the vSphere Data Protection virtual appliance.

You can use scp, FileZilla or WinSCP.

- 2 Log in to the vSphere Data Protection appliance.
- Open a SSH connection to the virtual machine nyc01vdp01.rainpole.local.
 - Log in using the following credentials.

Setting	Value
User name	root
Password	vdp_root_password

- 3 Restart all vSphere Data Protection services by running the following commands.

```
dpnctl stop all
dpnctl start all
```

- 4 Run the addFingerprint.sh script to update the vSphere Data Protection server thumbprint displayed in the VM console welcome screen.

```
/usr/local/avamar/bin/addFingerprint.sh
```

Configure Service Account Access in vSphere for Integration with vSphere Data Protection in ROBO

Configure an operations service account with permissions that are required to enable vSphere Data Protection access to provide backup operations on the ROBO vCenter Server.

You associate the svc-vdp service account in the Active Directory with a user role that has certain privileges. You assign the user to the ROBO vCenter Server.

Define a User Role in vSphere for Integration with vSphere Data Protection in ROBO

In vSphere, create a user role with privileges that are required for performing backup operations against for the management virtual machines in vSphere Data Protection in the ROBO.

Procedure

- 1 Log in to vCenter Server by using the vSphere Web Client.
 - a Open a Web browser and go to **`https://mgmt01vc01.sfo01.rainpole.local/vsphere-client`**.
 - b Log in using the following credentials.

Setting	Value
User name	administrator@vsphere.local
Password	vsphere_admin_password

- 2 On the **Home** page of the vSphere Web Client, select **Roles** under **Administration**.

3 Create a new role for managing backups.

- a On the **Roles** page, click the **Create role action** icon.
- b In the **Create Role** dialog box, configure the role using the following configuration settings, and click **OK**.

Setting	Value
Role name	vSphere Data Protection User
Privilege	<ul style="list-style-type: none"> ■ Alarms.Create alarm ■ Alarms.Modify alarm ■ Datastore.Allocate space ■ Datastore.Browse datastore ■ Datastore.Configure datastore ■ Datastore.Low level file operations ■ Datastore.Move datastore ■ Datastore.Remove datastore ■ Datastore.Remove file ■ Datastore.Rename datastore ■ Extension.Register extension ■ Extension.Update extension ■ Folder.Create folder ■ Global.Cancel task ■ Global.Disable methods ■ Global.Enable methods ■ Global.Licenses ■ Global.Log event ■ Global.Manage custom attributes ■ Global.Settings ■ Network.Assign network ■ Network.Configure ■ Resource.Assign virtual machine to resource pool ■ Sessions.Validate session ■ Tasks.Create task ■ Tasks.Update task ■ Virtual Machine.Configuration.Add existing disk ■ Virtual Machine.Configuration.Add new disk ■ Virtual Machine.Configuration.Add or remove device ■ Virtual Machine.Configuration.Advanced ■ Virtual Machine.Configuration.Change CPU count ■ Virtual Machine.Configuration.Change resource ■ Virtual Machine.Configuration.Disk change tracking ■ Virtual Machine.Configuration.Disk lease ■ Virtual Machine.Configuration.Extend virtual disk ■ Virtual Machine.Configuration.Host USB device ■ Virtual Machine.Configuration.Memory ■ Virtual Machine.Configuration.Modify device settings ■ Virtual Machine.Configuration.Raw device

Setting	Value
	<ul style="list-style-type: none"> ■ Virtual Machine.Configuration.Reload from path ■ Virtual Machine.Configuration.Remove disk ■ Virtual Machine.Configuration.Rename ■ Virtual Machine.Configuration.Reset guest information ■ Virtual Machine.Configuration.Set annotation ■ Virtual Machine.Configuration.Settings ■ Virtual Machine.Configuration.Swapfile placement ■ Virtual Machine.Configuration.Upgrade virtual machine compatibility ■ Virtual Machine.Guest Operations.Guest operation modifications ■ Virtual Machine.Guest Operations.Guest operation program execution ■ Virtual Machine.Guest Operations.Guest operation queries ■ Virtual Machine.Interaction.Console interaction ■ Virtual Machine.Interaction.Device connection ■ Virtual Machine.Interaction.Guest operating system management by VIX API ■ Virtual Machine.Interaction.Power off ■ Virtual Machine.Interaction.Power on ■ Virtual Machine.Interaction.Reset ■ Virtual Machine.Interaction.VMware Tools install ■ Virtual Machine.Inventory.Create new ■ Virtual Machine.Inventory.Register ■ Virtual Machine.Inventory.Remove ■ Virtual Machine.Inventory.Unregister ■ Virtual Machine.Provisioning.Allow disk access ■ Virtual Machine.Provisioning.Allow read-only disk access ■ Virtual Machine.Provisioning.Allow virtual machine download ■ Virtual Machine.Provisioning.Mark as template ■ Virtual Machine.Snapshot management.Create snapshot ■ Virtual Machine.Snapshot management.Remove snapshot ■ Virtual Machine.Snapshot management.Revert to snapshot ■ vApp.Export ■ vApp.Import ■ vApp.vApp application configuration

This role inherits the **System.Anonymous System.View**, and **System.Read** permissions.

Configure User Privileges in vSphere for Integration with vSphere Data Protection in ROBO

Assign global permissions in the ROBO to the operations service account svc-vdp so that you can manage and perform backups by using vSphere Data Protection.

The svc-vdp user has access rights that are specifically required for performing backups of vCenter Server inventory.

Prerequisites

- Verify that the ROBO vCenter Server is connected to the Active Directory domain.

- Verify that the users and groups from the `rainpole.local` domain are available on the ROBO vCenter Server.

Procedure

- 1 Log in to vCenter Server by using the vSphere Web Client.
 - a Open a Web browser and go to **`https://nyc01vc01.rainpole.local/vsphere-client`**.
 - b Log in using the following credentials.

Setting	Value
User name	administrator@vsphere.local
Password	vsphere_admin_password

- 2 From the **Home** menu, select **Administration**.
- 3 Assign global permissions to the `svc-vdp@rainpole.local` service account.
 - a In the vSphere Web Client Navigator, click **Global Permissions** under **Access Control**.
 - b On the **Manage** tab, click **Add Permission**.
 - c In the **Global Permissions Root - Add Permission** dialog box, click **Add** button to associate a user or a group with a role.
 - d In the **Select Users/Groups** dialog box, from the **Domain** drop-down menu, select **rainpole.local**, in the filter box type **svc**, and press Enter.

- e From the list of users and groups, select the **svc-vdp** user, click **Add**, and click **OK**.

Select Users/Groups

Select users from the list or type names in the Users text box. Click Check names to validate your entries against the directory.

Domain: rainpole.local

Users and Groups

Show Users First

Q svc

User/Group	Description/Full name
svc-srm	svc-srm-vcenter
svc-vdp	svc-vdp
svc-vr	svc-vr
svc-vRA	svc-vRA svc-vRA
svc-vra-vrops	svc-vra-vrops
svc-vrli-vrops	svc-vrli-vrops
svc-vRO	svc-vRO svc-vRO

Add

Users: rainpole.local/svc-vdp

Groups:

Separate multiple names with semicolons

Check names

OK Cancel

- f In the **Global Permissions Root - Add Permission** dialog box, from the **Assigned Role** drop-down menu, select **vSphere Data Protection User**, select **Propagate to children** checkbox, and click **OK**.

Register vSphere Data Protection with Management vCenter Server in ROBO

After you deploy the virtual appliance for vSphere Data Protection on the management cluster in the ROBO, complete the initial configuration of vSphere Data Protection.

Procedure

- 1 Log in to the vSphere Data Protection Configuration Utility.
 - a Open a Web browser and go to
`https://nyc01vdp01.rainpole.local:8543/vdp-configure`.
 - b Log in using the following credentials.

Setting	Value
Username	root
Password	changeme

The configuration wizard of vSphere Data Protection appears.

- 2 On the **Welcome** page, click **Next**.
- 3 On the **Network Settings** page, verify that the network settings are populated correctly and click **Next**.
- 4 On the **Time Zone** page, select the **UTC** time zone and click **Next**.
- 5 On the **VDP Credentials** page, enter and confirm a new password for the root Linux appliance user, and click **Next**.

The password must satisfy the following requirements:

- If all four character classes are used, the password must be at least 6 characters.
- If three character classes are used, the password must be at least 7 characters.
- If one or two character classes are used, the password must be at least 8 characters.
- The four-character classes are as follows:
 - Upper case letters A-Z
 - Lower case letters a-z
 - Numbers 0-9
 - Special characters (for example: ~!@#,.)

- 6 On the **vCenter Registration** page, configure the settings for registration with the Management vCenter Server.

- a Enter the settings for connection to the Management vCenter Server.

vCenter Server Setting	Value
vCenter username	rainpole.local\svc-vdp
vCenter password	svc-vdp_password
vCenter FQDN or IP	nyc01vc01.rainpole.local
vCenter HTTP port	80
vCenter HTTPS port	443
Verify vCenter certificate	Deselected
Use vCenter for SSO authentication	Selected

- b Click **Test Connection** and in the **Connection success** message box, click **OK**.
- c On the *vCenter Registration* page, click **Next**.
- 7 On the **Create Storage** page, select **Create new storage**, in the **Capacity** text box select 2 TiB, and click **Next**.
- 8 On the **Device Allocation** page, from the **Provision** drop-down menu select **Thin** and click **Next**.
- 9 On the **CPU and Memory** page, leave the default settings and click **Next**.
- 10 On the **Product Improvement** page, select **Enable Customer Experience Improvement Program** and click **Next**.
- 11 On the **Ready to Complete** page, select **Run performance analysis on storage configuration** and **Restart the appliance if successful**, and click **Next**.
- 12 In the warning message box about storage configuration, click **Yes**.
vSphere Data Protection setup starts configuring data disks.
- 13 After disk configuration is complete, click **OK** in the success box.
- 14 Relocate the vSphere Data Protection appliance to the management resource pool for resource segmentation of the different types of components in the ROBO cluster.
- a Open a Web browser and go to **https://nyc01vc01.rainpole.local/vsphere-client**.
- b Log in using the following credentials.

Setting	Value
User name	administrator@vsphere.local
Password	vsphere_admin_password

- c Navigate to the **nyc01vc01.rainpole.local** vCenter Server object.
- d Locate the **nyc01vdp01** virtual appliance.
- e Right-click on the virtual appliance, select **Power > Shut Down Guest OS**.

- f After the appliance is powered off, drag and drop it to the **NYC01-MGMT** resource pool.
 - g Right-click on the virtual appliance, select **Power > Power On..**
- 15** Verify that vSphere Data Protection is accessible in the vSphere Web Client after you complete the initial configuration and relocate the appliance to the management resource pool.
- a Open a Web browser and go to **`https://nyc01vc01.rainpole.local/vsphere-client`**.
 - b Log in using the following credentials.

Setting	Value
User name	administrator@vsphere.local
Password	vsphere_admin_password

- c On the vSphere Web Client **Home** page, verify that the **VDP** icon is available and you can connect to the appliance.

Cloud Management Platform Implementation in ROBO

3

The Cloud Management Platform (CMP) consists of integrated products that provide for the management of public, private and hybrid cloud environments. VMware's CMP consists of vRealize Automation, vRealize Orchestrator, and vRealize Business. vRealize Automation incorporates virtual machine provisioning and a self-service portal. vRealize Business enables billing and chargeback functions. vRealize Orchestrator provides workflow optimization.

The following procedures describe the validated flow of installation and configuration for the remote office and branch office (ROBO) deployment.

This section includes the following topics:

- [Prerequisites for Cloud Management Platform Implementation in ROBO](#)
- [Configure Service Account Privileges in ROBO](#)
- [vRealize Automation Installation in ROBO](#)
- [vRealize Orchestrator Configuration in ROBO](#)
- [vRealize Business Installation in ROBO](#)
- [Create Anti-Affinity Rules for vRealize Automation Proxy Agent Virtual Machines in ROBO](#)
- [Content Library Configuration in ROBO](#)
- [Tenant Content Creation in ROBO](#)

Prerequisites for Cloud Management Platform Implementation in ROBO

Verify that the following configurations are established prior to beginning the Cloud Management Platform deployment procedures for ROBO.

DNS Entries and IP Address Mappings for ROBO

Verify that the static IP address and FQDNs, listed in the table below, are available for use by the vRealize Automation application virtual network for the ROBO deployment.

Table 3-1. IP Addresses and Host Name for the vRA Proxy Agents and vRB Data Collector for ROBO

Role	IP Address	FQDN
vRealize Automation Proxy Agents	172.18.19.52	nyc01ias01.rainpole.local
	172.18.19.53	nyc01ias02.rainpole.local
vRealize Business Data Collector	172.18.19.54	nyc01buc01.rainpole.local
Default gateway	172.18.19.1	
DNS server	172.18.11.4	
Subnet mask	255.255.255.0	
NTP	172.18.11.251 172.18.11.252	ntp.rainpole.local

Configure Service Account Privileges in ROBO

In order for you to provision virtual machines and logical networks, you must configure privileges for vRealize Automation for the service account `svc-vra@rainpole.local` on both the vCenter Server and the NSX Instance in the consolidated cluster.

Procedure

1 [Configure Service Account Privileges on the vCenter Server in ROBO](#)

Configure Administrator privileges for the `svc-vra` and `svc-vro` users on the vCenter Server for ROBO

2 [Configure the Service Account Privilege on the NSX Instance in ROBO](#)

Configure Enterprise Administrator privileges in NSX manager for the `svc-vra@rainpole.local` service account.

Configure Service Account Privileges on the vCenter Server in ROBO

Configure Administrator privileges for the `svc-vra` and `svc-vro` users on the vCenter Server for ROBO

Procedure

1 Log in to vCenter Server by using the vSphere Web Client.

- Open a Web browser and go to **`https://nyc01vc01.rainpole.local/vsphere-client`**.
- Log in using the following credentials.

Setting	Value
User name	<code>administrator@vsphere.local</code>
Password	<code>vsphere_admin_password</code>

2 In the Navigator pane, select **Hosts and Cluster**.

- 3 Right-click the **nyc01vc01.rainpole.local** instance and select **Add Permissions**.
- 4 In the **Add Permission** dialog box, click the **Add** button.

The **Select Users/Groups** dialog box appears.

- 5 Select **RAINPOLE** from the **Domain** drop-down menu, and in the **Show Users First** text box enter **svc-vr** to filter user and group names.

Select Users/Groups

Select users from the list or type names in the Users text box. Click Check names to validate your entries against the directory.

Domain: RAINPOLE.LOCAL

Users and Groups

Show Users First

Q svc-vr

User/Group	Description/Full name
svc-vRA	svc-vRA svc-vRA
svc-vRO	svc-vRO svc-vRO
svc-vrops	svc-vrops svc-vrops

Add

Users: RAINPOLE.LOCAL\svc-vRA;RAINPOLE.LOCAL\svc-vRO

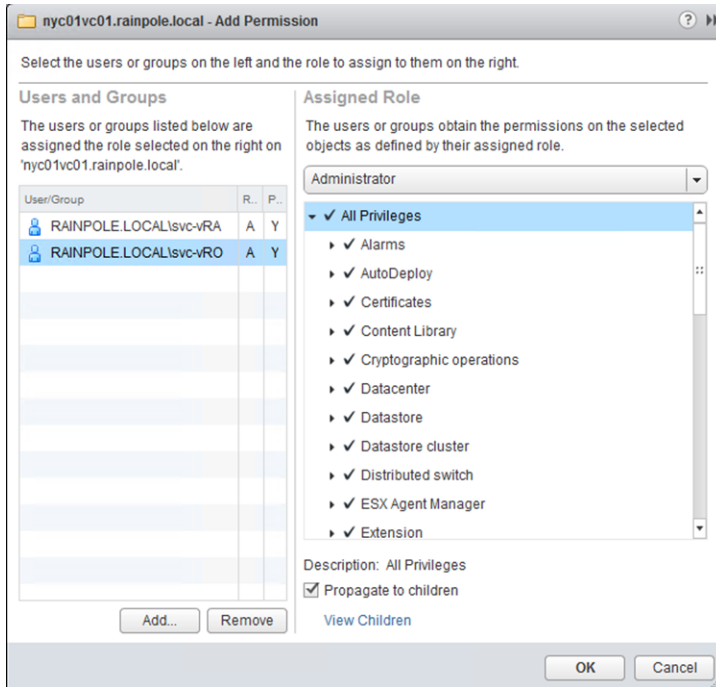
Groups:

Separate multiple names with semicolons

Check names

OK Cancel

- 6 Select **svc-vra** and **svc-vro** from the **User/Group** list, click the **Add** button and click **OK**.



- 7 In the **Add Permission** dialog box, select **Administrator** from the **Assigned Role** drop-down menu and click **OK** for both **svc-vra** and **svc-vro**.

The svc-vra and svc-vro users now have **Administrator** privilege on the vCenter Server in ROBO.

Configure the Service Account Privilege on the NSX Instance in ROBO

Configure Enterprise Administrator privileges in NSX manager for the svc-vra@rainpole.local service account.

Procedure

- 1 Log in to vCenter Server by using the vSphere Web Client.
 - a Open a Web browser and go to **https://nyc01vc01.rainpole.local/vsphere-client**.
 - b Log in using the following credentials.

Setting	Value
User name	administrator@vsphere.local
Password	vsphere_admin_password

- 2 In the **Navigator**, click **Networking & Security** and click **NSX Managers**.
- 3 Under **NSX Managers**, click the **172.18.11.65** instance.
- 4 Click **Manage**, click **Users**, and click the **Add** icon.

The **Assign Role** wizard appears.

- 5 On the **Identify User** page, select the **Specify a vCenter User** radio button, enter **svc-vra@rainpole.local** in the **User** text box, and click **Next**.

The screenshot shows a window titled "Assign Role" with a sidebar on the left containing two steps: "1 Identify User" (marked with a green checkmark) and "2 Select Roles". The main area is titled "Identify User" with the instruction "Select a vCenter user or group to assign role." There are two radio buttons: "Specify a vCenter user" (which is selected) and "Specify a vCenter group". Below the first radio button is a text field labeled "User:" containing the text "svc-vra@rainpole.local". Below the text field is a note: "User can log on with the credentials maintained at vCenter. (ex: test@vsphere.local or test@domain.com)". At the bottom of the window are four buttons: "Back", "Next", "Finish", and "Cancel".

- 6 On the **Select Roles** page, select the **Enterprise Administrator** radio button, and click **Finish**.

The svc-vra@rainpole.local user is now configured as an **Enterprise Administrator** for the NSX instance, and appears in the lists of users and roles.

vRealize Automation Installation in ROBO

A vRealize Automation installation includes installing and configuring single sign-on (SSO) capabilities, the user interface portal, and Infrastructure as a Service (IaaS) components.

After installation you can customize the installation environment and configure one or more tenants, which sets up access to self-service provisioning and life-cycle management of cloud services. By using the secure portal Web interface, administrators, developers, or business users can request IT services and manage specific cloud and IT resources based on their roles and privileges. Users can request infrastructure, applications, desktops, and IT service through a common service catalog.

- [Deploy Windows Virtual Machines for vRealize Automation in ROBO](#)

vRealize Automation requires several Windows virtual machines to act as IaaS components in a distributed configuration. These redundant components provide high availability for the vRealize Automation infrastructure features.

- [Install vRealize Automation Proxy Agents in ROBO](#)

Proxy agents are required so vRealize Automation can communicate with vCenter Server instances. For every vCenter Server instance that will be a target for vRealize Automation, deploy at least two proxy agents.

Deploy Windows Virtual Machines for vRealize Automation in ROBO

vRealize Automation requires several Windows virtual machines to act as IaaS components in a distributed configuration. These redundant components provide high availability for the vRealize Automation infrastructure features.

Procedure

1 Create a Customization Specification for the IaaS Proxy Agent Servers in ROBO

Create a vSphere Image Customization template to use with your vRealize Automation IaaS Proxy Agent deployment.

2 Deploy Windows Virtual Machines for vRealize Automation in ROBO

vRealize Automation requires several Windows virtual machines to act as IaaS components in a distributed configuration. These redundant components provide high availability for the vRealize Automation infrastructure features.

3 Install vRealize Automation Management Agent on Windows IaaS Virtual Machines in ROBO

For each Windows virtual machine deployed as part of the vRealize Automation installation, a management agent must be deployed to facilitate the installation of the Windows dependencies and vRealize Automation components.

Create a Customization Specification for the IaaS Proxy Agent Servers in ROBO

Create a vSphere Image Customization template to use with your vRealize Automation IaaS Proxy Agent deployment.

Procedure

1 Log in to vCenter Server by using the vSphere Web Client.

- a Open a Web browser and go to **<https://nyc01vc01.rainpole.local/vsphere-client>**.
- b Log in using the following credentials.

Setting	Value
User name	administrator@vsphere.local
Password	vsphere_admin_password

2 From the **Home** page, click **Customization Specification Manager**.

3 Select **nyc01vc01.rainpole.local** from the **vCenter Server** drop-down menu.

4 Click the **Create a new specification** icon.

The **New VM Guest Customization Spec** wizard opens.

- 5 On the **Specify Properties** page, configure the following settings, and click **Next**.

Setting	Value
Target VM Operating System	Windows
Use custom SysPrep answer file	Deselected
Customization Spec Name	vra7-proxy-agent-template

- 6 On the **Set Registration Information** page, configure the following settings, and click **Next**.

Setting	Value
Name	Rainpole
Organization	Rainpole IT

- 7 On the **Set Computer Name** page, select the **Enter a name in the Clone/Deploy wizard** radio button, and click **Next**.

- 8 On the **Enter Windows License** page, enter the following settings, and click **Next**.

If you are using **Microsoft License Server**, or have multiple single license keys, leave the **Product Key** text box blank.

Setting	Value
Product Key	<i>volume_license_key</i>
Include Server License Information	Selected
Server License Mode	Per seat

- 9 On the **Set Administrator Password** page, configure the following settings, and click **Next**.

Setting	Value
Password	<i>local_administrator_pwd</i>
Automatically logon as Administrator	Selected
Number of times to logon automatically	1

- 10 On the **Time Zone** page, select **(GMT) Coordinated Universal Time** from the **Time Zone** drop down menu, and click **Next**.
- 11 On the **Run Once** page, type **net localgroup administrators rainpole\svc-vra /add** in the text box and click **Add**. This command will add service account rainpole\svc-vra into virtual machine's local administrators group. Click **Next**.
- 12 On the **Configure Network** page, select the **Manually select custom settings** radio button, select **NIC1** from the list of network interfaces in the virtual machine, and click **Edit**.

The **Network Properties** dialog box displays.

- 13** In the **Edit Network** dialog box, on the **IPv4** page, configure the following settings and click **DNS**.

Setting	Value
Prompt the user for an address when the specification is used	Selected
Subnet Mask	255.255.255.0
Default Gateway	172.18.19.1

- 14** On the **DNS** page, provide DNS servers and search suffixes.

- a Configure the following DNS server settings.

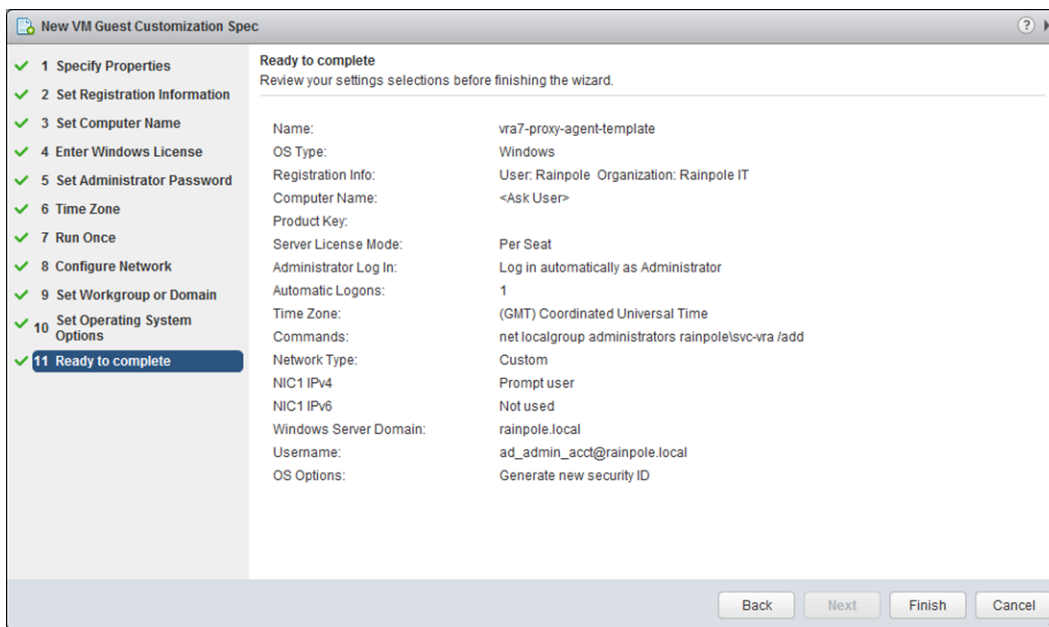
Setting	Value
Use the following DNS server address	Selected
Preferred DNS Server	172.18.11.4
Alternate DNS Server	172.16.11.4

- b Enter **rainpole.local** in the **For all connections with TCP/IP enabled** text box and click the **Add** button.
- c Click **OK** to save settings and close the **Edit Network** dialog box, and click **Next**.

- 15** On the **Set Workgroup or Domain** page, enter credentials that have administrative privileges in the domain, and click **Next**.

Setting	Value
Windows Server Domain	rainpole.local
Username	ad_admin_acct@rainpole.local
Password	ad_admin_password

- 16** On the **Set Operating System** options page, select the **Generate New Security ID (SID)** check box, and click **Next**.
- 17** On the **Ready to Complete** page, review the settings that you entered, and click **Finish**.



The customization specification you created is listed in the **Customization Specification Manager**, and can be used to customize virtual machine guest operating systems.

Deploy Windows Virtual Machines for vRealize Automation in ROBO

vRealize Automation requires several Windows virtual machines to act as IaaS components in a distributed configuration. These redundant components provide high availability for the vRealize Automation infrastructure features.

To facilitate cloning, this design uses the vra7-proxy-agent-template image customization specification template and the windows-2012r2-64 VM template. Two virtual machines that run on Windows will be required to install vRealize Automation Proxy Agents in ROBO. Repeat this procedure twice by using the information in the following table to create two VMs.

Name for Virtual Machines	NetBIOS name	vCenter Folder	IP	vCPU number	Memory Size	Image Customization Specification Template	Network
nyc01ias01.rainpole.local	nyc01ias01	vRA01IAS	172.18.19.52	2	4 GB	vra7-proxy-agent-template	vxw-dvs-xxxx-Mgmt-NYC01-VXLAN
nyc01ias02.rainpole.local	nyc01ias02	vRA01IAS	172.18.19.53	2	4 GB	vra7-proxy-agent-template	vxw-dvs-xxxx-Mgmt-NYC01-VXLAN

Prerequisites

Verify that you have created the Windows 2012 R2 template VM `windows2012r2-template`. See *Virtual Machine Template Specifications in the VMware Validated Design for SDDC*.

Procedure

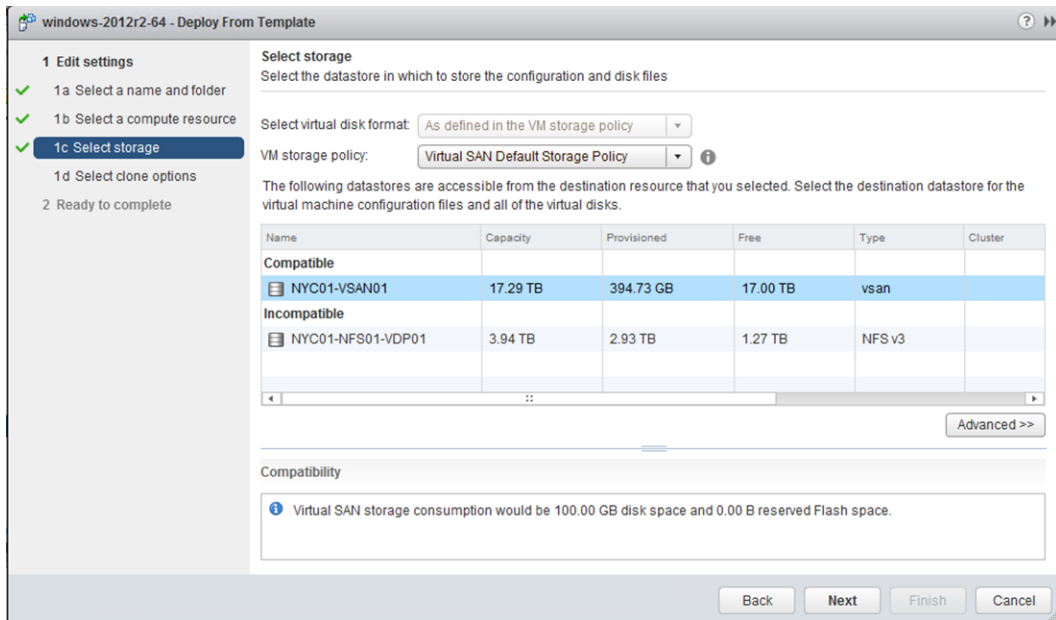
- 1 Log in to vCenter Server by using the vSphere Web Client.

- a Open a Web browser and go to **`https://nyc01vc01.rainpole.local/vsphere-client`**.
- b Log in using the following credentials.

Setting	Value
User name	<code>administrator@vsphere.local</code>
Password	<code>vsphere_admin_password</code>

- 2 In the Navigator pane, select **Global Inventory Lists > vCenter Servers**. Click the **`nyc01vc01.rainpole.local`** instance.
- 3 Select **VM Templates in Folders**, and from the VM Templates in Folders pane, right-click the IaaS windows template **`win2012r2-template`** and select **New VM from this Template**.
- 4 On the **Select a name and folder** page of the **Deploy From Template** wizard, specify a name and location for the virtual machine.
 - a Enter **`nyc01ias01.rainpole.local`** in the **Enter a name for the virtual machine** text box.
 - b In the **Select a location for the virtual machine** pane, select the **`vRA01IAS`** folder in the **`NYC01`** datacenter under **`nyc01vc01.rainpole.local`**, and click **Next**.
- 5 On the **Select a compute resource** page, select the resource pool **`NYC01-MGMT`**, and click **Next**.

- 6 On the **Select storage** page, select the datastore on which to create the virtual machine's disks.
 - a Select **Virtual SAN Default Storage Policy** from the **VM Storage Policy** drop-down menu.
 - b Select the **NYC01-VSAN01** vSAN datastore from the datastore table and click **Next**.



- 7 On the **Select Clone options** page, select the **Customize the operating system** check box, and click **Next**.
- 8 On the **Customize guest OS** page, select the **vra7-proxy-agent-template**, and click **Next**.
- 9 On the **User Settings** page, enter the following values, and click **Next**.

Setting	Value
NetBIOS name	nyc01ias01
IPv4 address	172.18.19.52
IPv4 subnet mask	255.255.255.0

- 10 On the **Ready to Complete** page, review your settings and click **Finish**.

windows-2012r2-64 - Deploy From Template	
1 Edit settings	Provisioning type: Deploy from template
✓ 1a Select a name and folder	Source template: windows-2012r2-64
✓ 1b Select a compute resource	Virtual machine name: nyc01ias01.rainpole.local
✓ 1c Select storage	Folder: vRA01IAS
✓ 1d Select clone options	Resource pool: NYC01-MGMT
✓ 1e Customize guest OS	Datastore: NYC01-VSAN01
✓ 1f User Settings	Disk storage: As defined in the VM storage policy
✓ 2 Ready to complete	VM storage policy: Virtual SAN Default Storage Policy
	Guest OS customization specification: vra7-proxy-agent-template

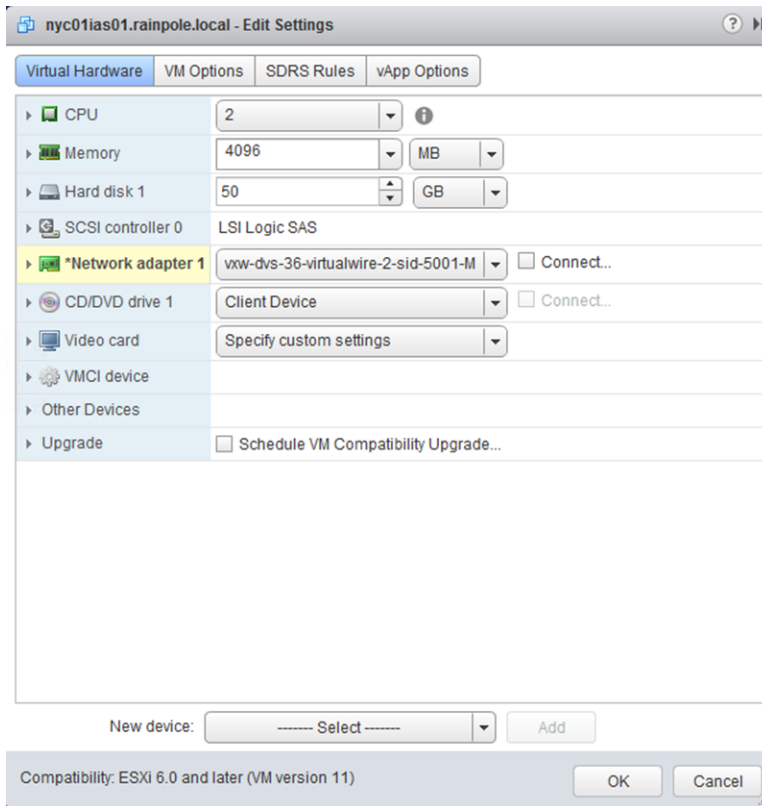
Back Next Finish Cancel

When the deployment of the virtual machine completes, you can customize the virtual machine.

11 In the **Navigator**, select **VMs and Templates**.

12 Right-click the **nyc01ias01.rainpole.local** virtual machine and select **Edit Settings**.

- 13 Click **Virtual Hardware** and configure the settings for **CPU**, **Memory**, and the **Network adapter 1**.
- Select **2** from the **CPU** drop-down menu.
 - Set the **Memory** settings to **4096 MB**.
 - Expand **Network adapter 1** and select **vxw-dvs-xxxx-Mgmt-NYC01-VXLAN** from the drop-down menu and click **OK**.



- 14 Right-click the virtual machine **nyc01ias01.rainpole.local**, and select **Power > Power on**.
- 15 From the Virtual Machine Console, verify that **nyc01ias01.rainpole.local** reboots, and uses the configuration settings that you specified.
- After the Windows customization process completes, a clean desktop appears.
- 16 Log in to the Windows operating system and perform final verification and customization.
- Verify that the IP address, computer name, and domain are correct.
 - Verify vRealize Automation service account `svc-vra@rainpole.local` to the Local Administrators Group.
- 17 Repeat this procedure to deploy and configure the remaining virtual machine.

Install vRealize Automation Management Agent on Windows IaaS Virtual Machines in ROBO

For each Windows virtual machine deployed as part of the vRealize Automation installation, a management agent must be deployed to facilitate the installation of the Windows dependencies and vRealize Automation components.

Repeat this procedure twice to install the Management Agent on both of the Windows IaaS virtual machines. The host names of the Windows IaaS virtual machines are `nyc01ias01.rainpole.local` and `nyc01ias02.rainpole.local`.

Procedure

- 1 Log in to the Windows IaaS Proxy Agent virtual machine.
 - a Connect to **`nyc01ias01.rainpole.local`** over RDP.
 - b Log in using the local administrator credentials that you specified during the creation of the customization specification process.
- 2 Download the vRealize Management Agent.
 - a Open a Web browser and go to **`https://vra01svr01a.rainpole.local:5480/installer`**.
 - b Download the Management Agent Installer .msi package.
- 3 Install the vRealize Management Agent.
 - a Start the `vCAC-IaaSManagementAgent-Setup.msi` installer.
 - b On the **Welcome** page, click **Next** to start the install process.
 - c On the **EULA** page, select the **I accept the terms of this agreement** check box and click **Next**.
 - d On the **Destination Folder** page, click **Next** to install in the default path.
 - e On the **Management Site Service** page, enter the following settings and click **Load**.

Setting	Value
vRA Appliance Address	<code>https://vra01svr01a.rainpole.local:5480</code>
Root username	<code>root</code>
Password	<code>vra_appA_root_password</code>

- f Select the **I confirm the fingerprint matches the Management Site Service SSL certificate** check box, and click **Next**.
- 4 On the **Management Agent Account Configuration** page, configure the following credentials and click **Next**.

Setting	Value
Username	<code>rainpole\svc-vra</code>
Password	<code>svc-vra_password</code>

- 5 On the **Ready to install** page, click **Install**.
- 6 Repeat the procedure to install the Management Agent in virtual machine `nyc01ias02.rainpole.local`.

Install vRealize Automation Proxy Agents in ROBO

Proxy agents are required so vRealize Automation can communicate with vCenter Server instances. For every vCenter Server instance that will be a target for vRealize Automation, deploy at least two proxy agents.

Repeat this procedure twice to install the IaaS proxy Agent on the Windows virtual machines `nyc01ias01.rainpole.local` and `nyc01ias02.rainpole.local`.

Procedure

- 1 Log in to the `nyc01ias01.rainpole.local` virtual machine console using the vRealize Automation service account.

Setting	Value
Username	Rainpole\svc-vra
Password	<i>svc-vra_password</i>

- 2 Open a Web browser and go to `https://vra01svr01a.rainpole.local:5480/installer`.
- 3 Click the **IaaS Installer** link and save the installer with its default file name.
- 4 Right-click the installer file and select **Run as administrator**.
- 5 On the **Log In** page, configure the following settings, and click **Next**.

Setting	Value
Appliance host name	vra01svr01a.rainpole.local:5480
User name	root
Password	<i>root_password</i>
Accept Certificate	Selected

- 6 On the **Installation Type** page, select **Custom Install**, select **Proxy Agents**, and click **Next**.
- 7 On the **Server and Account Settings** page, configure the following settings and click **Next**.

Setting	Value
Local server	Use the default host name
User name	RAINPOLE\svc-vra
Password	<i>svc-vra_password</i>

- 8 On the **Install Proxy Agent** page, configure the following values, and click **Add**.

Setting	Value
Agent Type	vSphere
Agent Name	NYC01-AGENT-01
Manager Service Host name	vra01ims01.rainpole.local
Model Manager Web Service Host name	vra01iws01.rainpole.local
vSphere Endpoint	nyc01vc01.rainpole.local

vRealize Automation Configuration

Install Proxy Agent
Install and configure Proxy Agent

Agent type: vSphere

Proxy Agent Details

Agent name: NYC01-AGENT-01

Manager Service Host: vra01ims01.rainpole.local [Test](#) Passed

Model Manager Web Service Host: vra01iws01.rainpole.local [Test](#) Passed

vSphere

Endpoint name: nyc01vc01.rainpole.local
This value must match the name of the vSphere endpoint in the vRealize Automation UI.

[Add](#) [Save](#)

Type	Name	Manager Service Host	Model Manager Web Service Host	Service User
vSphere	NYC01-AGENT...	vra01ims01.rainpole.local	vra01iws01.rainpole.local	RAINPOLE\svc-vra

[Remove](#) [Edit](#)

[< Back](#) [Next >](#) [Cancel](#)

- 9 Click **Next**.
- 10 Verify the configuration, and click **Install** to install the proxy agent.
- 11 Repeat the procedure for virtual machine nyc01ias02.rainpole.local to install another proxy agent for redundancy, using the following values.

Setting	Value
Agent Type	vSphere
Agent Name	NYC01-AGENT-01
Manager Service Host name	vra01ims01.rainpole.local
Model Manager Web Service Host name	vra01iws01.rainpole.local
vSphere Endpoint	nyc01vc01.rainpole.local

vRealize Orchestrator Configuration in ROBO

VMware vRealize Orchestrator provides a library of extensible workflows to allow you to create and run automated, configurable processes to manage your VMware vSphere infrastructure, as well as other VMware and third-party applications.

vRealize Orchestrator is composed of three distinct layers: an orchestration platform that provides the common features required for an orchestration tool, a plug-in architecture to integrate control of subsystems, and a library of workflows. vRealize Orchestrator is an open platform that you can extend with new plug-ins and libraries, and that can be integrated into larger architectures through the use of its REST API.

Add vCenter Server Instance to vRealize Orchestrator

Add each vCenter Server instance that contributes resources to vRealize Automation and that uses vRealize Orchestrator workflows to vRealize Orchestrator to allow vCenter Server and vRealize Orchestrator to communicate.

Install Java SE Development Kit that is required to run the vRealize Orchestrator Client.

Procedure

- 1 Log in to the vRealize Orchestrator Client.
 - a Open a Web browser and go to **https://vra01vro01a.rainpole.local:8281**.
 - b Click **Start Orchestrator Client**.
 - c On the VMware vRealize Orchestrator login page, log in to the vRealize Orchestrator Host A by using the following host name and credentials.

Setting	Value
Host name	vra01vro01a.rainpole.local:8281
User name	svc-vra
Password	svc-vra_password

- 2 In the left pane, click **Workflows**, and navigate to **Library > vCenter > Configuration**.

3 Right-click the **Add a vCenter Server instance** workflow and click **Start Workflow**.

- a On the **Set the vCenter Server Instance** page, configure the following settings and click **Next**.

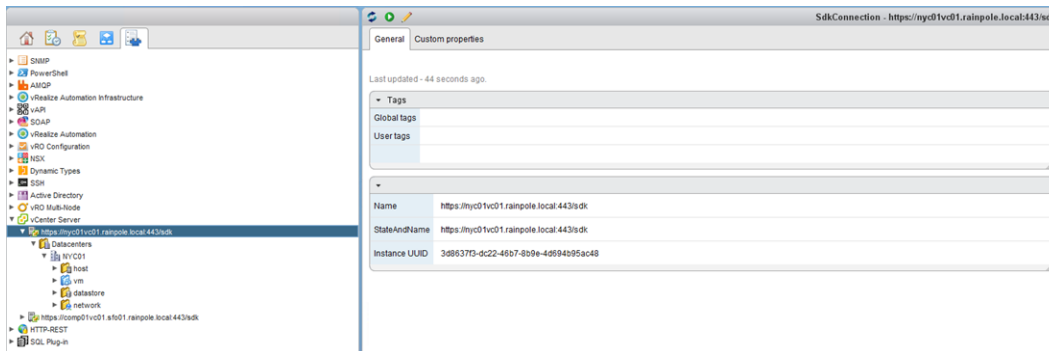
Setting	Value
IP or hostname of the vCenter Server instance to add	nyc01vc01.rainpole.local
HTTPS port of the vCenter Server instance	443
Location of SDK that you use to connect	/sdk
Will you orchestrate this instance	Yes
Do you want to ignore certificate warnings	Yes

- b On the **Set the connection properties** page, configure the following settings, and click **Submit**.

Setting	Value
Use a session per user	No
vCenter Server user name	svc-vro@rainpole.local
vCenter Server user password	svc-vro_password

4 To verify that the workflow completed successfully, click the **Inventory** tab and expand the **vCenter Server** tree control.

The vCenter Server instance you added will be visible in the inventory.



vRealize Business Installation in ROBO

vRealize Business is an IT financial management tool that provides transparency and control over the costs and quality of IT services, enabling alignment with the business and acceleration of IT transformation.

Install vRealize Business and integrate it with vRealize Automation to continuously monitor the cost of each individual virtual machine and the cost of the corresponding data center.

Procedure

1 Deploy the vRealize Business Data Collector in ROBO

VMware vRealize Business for Cloud allows users to gain greater visibility into financial aspects of their cloud infrastructure and lets them optimize and improve associated operations.

2 Configure NTP for vRealize Business in ROBO

Configure the network time protocol (NTP) on vRealize Business Data Collector virtual appliance from the virtual appliance management interface (VAMI).

3 Register the vRealize Business Data Collector with the Server in ROBO

As part of vRealize Business installation for ROBO, you connect the ROBO vRealize Business Data Collector with the vRealize Business Server previously deployed in the Hub.

4 Connect vRealize Business with the vCenter Server in ROBO

vRealize Business requires communication with the vCenter Server to collect data from the entire cluster. You perform this operation by using the vRealize Business Data Collector console.

Deploy the vRealize Business Data Collector in ROBO

VMware vRealize Business for Cloud allows users to gain greater visibility into financial aspects of their cloud infrastructure and lets them optimize and improve associated operations.

Procedure

1 Log in to vCenter Server by using the vSphere Web Client.

- a Open a Web browser and go to **`https://nyc01vc01.rainpole.local/vsphere-client`**.
- b Log in using the following credentials.

Setting	Value
User name	administrator@vsphere.local
Password	vsphere_admin_password

2 Click **Hosts and Clusters** and navigate to the **nyc01vc01.rainpole.local** vCenter Server object.

3 Right-click the **nyc01vc01.rainpole.local** object and select **Deploy OVF Template**.

4 On the **Select template** page, select **Local file**, browse to the location of the vRealize Business virtual appliance .ova file on your file system, and click **Next**.

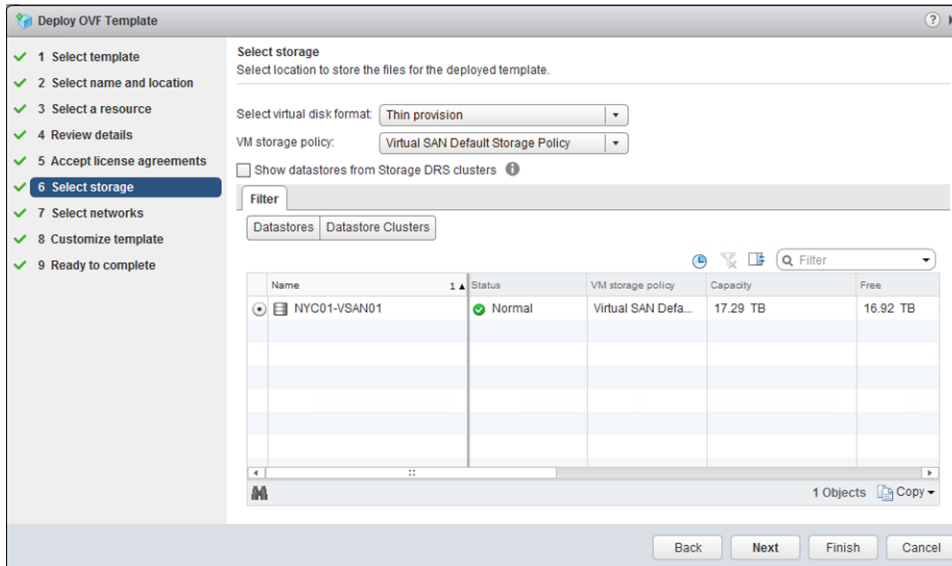
5 On the **Select name and location** page, enter the following information and click **Next**.

Setting	Value
Name	nyc01buc01.rainpole.local
Select a folder or datacenter	vRA01IAS

6 On the **Select a resource** page, select the **NYC01-MGMT** resource pool and click **Next**.

7 On the **Review details** page, examine the virtual appliance details, such as product, version, download and disk size, and click **Next**.

- 8 On the **Accept license agreements** page, accept the end user license agreements and click **Next**.
- 9 On the **Select storage** page, select the datastore.
 - a Select **Thin provision** from the **Select virtual disk format** drop-down menu.
 - b Select **Virtual SAN Default Storage Policy** from the **VM Storage Policy** drop-down menu.
 - c From the datastore table, select the **NYC01-VSAN01** vSAN datastore and click **Next**.



- 10 On the **Select networks** page, select the distributed port group that ends with Mgmt-NYC01-VXLAN from the **Destination Network** drop-down menu and click **Next**.
- 11 On the **Customize template** page, configure the following values and click **Next**.

Setting	Value
Currency	USD
Enable SSH service	Deselected
Enable Server	Deselected
Join the VMware Customer Experience Improvement Program	Selected
Root user password	<i>vrb_collector_root_password</i>
Default gateway	172.18.19.1
Domain Name	rainpole.local
Domain Name Servers	172.18.11.4,172.16.11.4
Domain Search Path	rainpole.local
Network 1 IP Address	172.18.19.54
Network 1 Netmask	255.255.255.0

Deploy OVF Template

1 Select template
2 Select name and location
3 Select a resource
4 Review details
5 Accept license agreements
6 Select storage
7 Select networks
8 Customize template
9 Ready to complete

Customize template
Customize the deployment properties of this software solution.

All properties have valid values [Show next...](#) [Collapse all...](#)

Networking Properties 6 settings

Default Gateway	The default gateway address for this VM. Leave blank if DHCP is desired. 172.18.19.1
Domain Name	The domain name of this VM. Leave blank if DHCP is desired. rainpole.local
Domain Name Servers	The domain name server IP Addresses for this VM (comma separated). Leave blank if DHCP is desired. 172.18.11.4, 172.16.11.4
Domain Search Path	The domain search path (comma or space separated domain names) for this VM. Leave blank if DHCP is desired. rainpole.local
Network 1 IP Address	The IP address for this interface. Leave blank if DHCP is desired. 172.18.19.54
Network 1 Netmask	The netmask or prefix for this interface. Leave blank if DHCP is desired. 255.255.255.0

Back Next Finish Cancel

12 On the **Ready to complete** page, review the configuration settings that you specified and click **Finish**.

13 Change the vRealize Business Remote Collector virtual appliance memory size.

- Right-click the **nyc01buc01.rainpole.local** virtual machine and select **Edit Settings**.
- Click **Virtual Hardware**, enter **2GB** for **Memory**, and click **OK**.

14 Navigate to the new appliance and power on the VM.

Configure NTP for vRealize Business in ROBO

Configure the network time protocol (NTP) on vRealize Business Data Collector virtual appliance from the virtual appliance management interface (VAMI).

Procedure

- Log in to the vRealize Business Data Collector appliance management console.
 - Open a Web browser and go to **https://nyc01buc01.rainpole.local:5480**.
 - Log in using the following credentials.

Setting	Value
User name	root
Password	vr_b_collector_root_password

2 Configure the appliance to use a time server.

- a Click the **Administration** tab and click **Time Settings**.
- b On the **Time Settings** page, enter the following settings and click **Save Settings**.

Setting	Description
Time Sync. Mode	Use Time Server
Time Server #1	ntp.rainpole.local

vRealize Business for Cloud

Administration System Telemetry Network Update Logout user root

Administration Time Settings SSL

Time Settings

Successfully updated the Time sync settings

Time Sync. Mode: Use Time Server

Time Server #1: ntp.rainpole.local

Time Server #2:

Time Server #3:

Time Server #4:

Time Server #5:

Current Time: 15 Mar, 2017 21:56:23 UTC +0000

Actions: Save Settings, Refresh

Register the vRealize Business Data Collector with the Server in ROBO

As part of vRealize Business installation for ROBO, you connect the ROBO vRealize Business Data Collector with the vRealize Business Server previously deployed in the Hub.

Because the tenant is configured in vRealize Automation, you register the vRealize Business Data Collector appliance with the vRealize Business Server using the following procedure.

- Generate a one-time key from vRealize Automation.
- Register the Data Collector to the vRealize Business Server.

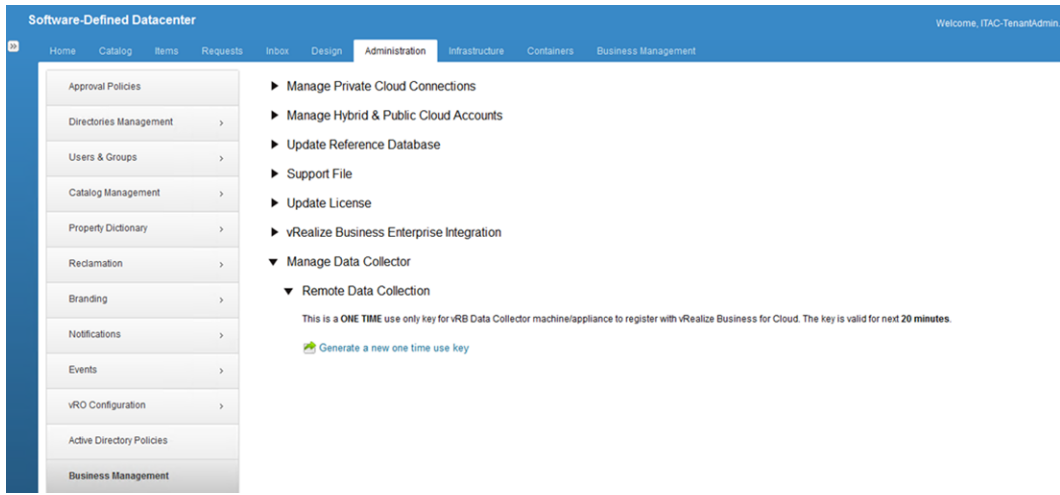
Procedure

- 1 Log in to the vRealize Automation Rainpole portal.
 - a Open a Web browser and go to **https://vra01svr01.rainpole.local/vcac/org/rainpole**.
 - b Log in using the following credentials.

Setting	Value
User name	itac-tenantadmin
Password	itac-tenantadmin_password
Domain	Rainpole.local

- 2 Generate a one-time use key for connecting vRealize Business Data Collector.
 - a Navigate to **Administration > Business Management**.
 - b Expand the **Manage Data Collector > Remote Data Collection** section.

- c Click **Generate a new one time use key**.
- d Save the one time use key as you need it later.



- 3 Log in to the vRealize Business Data Collector console.
 - a Open a Web browser and go to **https://nyc01buc01.rainpole.local:9443/dc-ui**.
 - b Log in using the following credentials.

Setting	Value
User name	root
Password	<i>vrb_collector_root_password</i>

4 Register the Data Collector with the vRealize Business Server.

- a Expand the **Registration with the vRealize Business Server** section.
- b Enter the following values and click **Register**.

After you click **Register**, a warning message informs you that the certificate is not trusted.

Setting	Value
Enter the vRB Server Url:	https://vra01bus01.rainpole.local
Enter the One Time Key:	one_time_use_key

vRealize Business for Cloud Data Collector

- ▶ Manage Private Cloud Connections
- ▶ Manage Hybrid & Public Cloud Accounts
- ▼ Registration with vRealize Business Server

You can connect your data collector with an existing vRB Server. You can have only one vRB server registered at a time.

Registered vRB URL : localhost

Register with vRealize Business

Enter the vRB Server Url :
The server URL must begin with https://

Enter the One Time Key :
The OTK is found in the One Time Key tab in the vRB Server
- ▶ Support File

- c Click **Install** and click **OK**.

vRealize Business Data Collector is now connected to vRealize Business Server.

Connect vRealize Business with the vCenter Server in ROBO

vRealize Business requires communication with the vCenter Server to collect data from the entire cluster. You perform this operation by using the vRealize Business Data Collector console.

Procedure

- 1 Log in to the vRealize Business Data Collector console.
 - a Open a Web browser and go to **https://nyc01buc01.rainpole.local:9443/dc-ui**.
 - b Log in using the following credentials.

Setting	Value
User name	root
Password	<i>vrb_collector_root_password</i>

- 2 Click **Manage Private Cloud Connections**, select **vCenter Server**, and click the **Add** icon.
- 3 In the **Add vCenter Server Connection** dialog box, enter the following settings and click **Save**.

Setting	Value
Name	nyc01vc01.rainpole.local
vCenter Server	nyc01vc01.rainpole.local
Username	svc-vra@rainpole.local
Password	<i>svc_vra_password</i>

Add vCenter Server Connections

Name:

vCenter Server:

Username:

Password:

- 4 In the **SSL Certificate warning** dialog box, click **Install**.
- 5 In the **Success** dialog box, click **OK**.

Create Anti-Affinity Rules for vRealize Automation Proxy Agent Virtual Machines in ROBO

After deploying the vRealize Automation proxy agents, set up anti-affinity rules.

A VM-Host anti-affinity (or affinity) rule specifies a relationship between a group of virtual machines and a group of hosts. Anti-affinity rules force specified virtual machines to remain apart during failover actions, and are a requirement for high availability.

Procedure

- 1 Log in to vCenter Server by using the vSphere Web Client.
 - a Open a Web browser and go to **<https://nyc01vc01.rainpole.local/vsphere-client>**.
 - b Log in using the following credentials.

Setting	Value
User name	administrator@vsphere.local
Password	vsphere_admin_password

- 2 From the **Home** page, click **Hosts and Clusters**.
- 3 Under **nyc01vc01.rainpole.local**, click **NYC01**.
- 4 Click the **Configure** tab and under **Configuration**, select **VM/Host Rules**.
- 5 Under **VM/Host Rules**, click **Add** to create a virtual machine anti-affinity rule.
- 6 In the **Create VM/Host Rule** dialog box, specify the first rule for the vRealize Automation virtual appliances.
 - a In the **Name** text box, enter **anti-affinity-rule-vra-ias**.
 - b Select the **Enable rule** check box.
 - c Select **Separate Virtual Machines** from the **Type** drop-down menu.
 - d Click **Add**, select the **nyc01ias01.rainpole.local** and **nyc01ias02.rainpole.local** virtual machines, click **OK**, and click **OK**.

Content Library Configuration in ROBO

Content libraries are container objects for VM templates, vApp templates, and other types of files.

vSphere administrators can use the templates in the library to deploy virtual machines and vApps in the vSphere inventory. Sharing templates and files across multiple vCenter Server instances in same or different locations brings out consistency, compliance, efficiency, and automation in deploying workloads at scale.

You create and manage a content library from a single vCenter Server instance, but you can share the library items to other vCenter Server instances if HTTP(S) traffic is allowed between them.

Connect to Content Library of the Compute vCenter Server Instance from ROBO

Connect to the content library in the hub to synchronize templates between the Consolidated vCenter Server instance and the Compute vCenter Server instance so that all of the templates in your environment are consistent.

Procedure

- 1 Log in to vCenter Server by using the vSphere Web Client.
 - a Open a Web browser and go to **`https://comp01vc01.sfo01.rainpole.local/vsphere-client`**.
 - b Log in using the following credentials.

Setting	Value
User name	administrator@vsphere.local
Password	vsphere_admin_password

- 2 From the **Home** page, click **Content Libraries** and click content library **SFO01-ContentLib01** that was created in the Compute vCenter Server in Region A.
- 3 Select the **Configure** tab and click **Copy Link**.
A subscription URL is saved to the clipboard.
- 4 Log out from the vSphere Web Client session to log back in to the ROBO vCenter Server.
- 5 Log in to vCenter Server by using the vSphere Web Client.
 - a Open a Web browser and go to **`https://nyc01vc01.rainpole.local/vsphere-client`**.
 - b Log in using the following credentials.

Setting	Value
User name	administrator@vsphere.local
Password	vsphere_admin_password

- 6 From the **Home** page, click **Content Libraries**, and click the **Create new library** icon.
The **New Content Library** wizard opens.
- 7 On the **Name and location** page, specify the following settings and click **Next**.

Setting	Value
Name	NYC01-ContentLib01
vCenter Server	nyc01vc01.rainpole.local

- 8 On the **Configure content library** page, select **Subscribed content library** specify the following settings, and click **Next**.

Setting	Value
Subscribed content library	Selected
Subscription URL	<i>SFO01-ContentLib01_subscription_URL</i>
Enable authentication	Selected
Password	<i>SFO01-ContentLib01_password</i>
Download all library content immediately	Selected

- 9 On the **Add storage** page, click the **Select a datastore** radio button, select the **NYC01-VSAN01** datastore to store the content library, and click **Next**.

The screenshot shows the 'New Content Library' wizard at the 'Ready to complete' step. On the left, a progress bar shows four steps: 1 Name and location, 2 Configure content library, 3 Add storage, and 4 Ready to complete (highlighted). The main area displays the following configuration:

- Name:** NYC01-ContentLib01
- Notes:**
- vCenter Server:** nyc01vc01.rainpole.local
- Type:** Subscribed Content Library
- Subscription URL:** <https://comp01vc01.sfo01.rainpole.local:443/cis/vcsp/lib/16e6fba9-86c9-455f-8039-d66b71d533b2/lib.json>
- Storage:** NYC01-VSAN01

At the bottom, there are four buttons: Back, Next, Finish, and Cancel.

- 10 On the **Ready to complete** page, click **Finish**.

Tenant Content Creation in ROBO

To provision virtual machines in the Consolidated vCenter Server instance, you configure the tenant to utilize vCenter Server compute resources.

Prerequisites

- Verify that a vCenter Server consolidated cluster has been deployed and configured. See "Deploy and Configure the Virtual Center Components"
- Verify that an NSX instance has been configured for use by the vCenter Server consolidated cluster. See "Deploy and Configure the NSX Instance"
- Proxy agents have been deployed.

Procedure

1 Preparing a Consolidated Cluster for the Rainpole Tenant in ROBO

To enable the provisioning of blueprints from vRealize Automation to a Consolidated Cluster, you create the virtual machine templates in the vCenter Server and create the logical switches for the provisioned workload virtual machines.

2 Add a Consolidated Cluster to the Rainpole Tenant in ROBO

Before provisioning blueprints to a Consolidated Cluster, a vSphere Endpoint needs to be created and compute clusters have to be added into a fabric group. The reservations of compute resources will be added into vRealize Automation for business groups.

3 Configure Single Machine Blueprints in ROBO

Virtual machine blueprints determine a machine's attributes, the manner in which it is provisioned, and its policy and management settings.

4 Configure Unified Single Machine Blueprints for Cross-ROBO Deployment

To provision blueprints from a specific vRealize Automation blueprint to multiple remote offices and branch offices, you must define the additional remote office and branch office locations in vRealize Automation, and associate the blueprints with those locations.

Preparing a Consolidated Cluster for the Rainpole Tenant in ROBO

To enable the provisioning of blueprints from vRealize Automation to a Consolidated Cluster, you create the virtual machine templates in the vCenter Server and create the logical switches for the provisioned workload virtual machines.

Create Logical Switches for Business Groups in ROBO

For each ROBO consolidated cluster, you create three logical switches for each business group which simulate networks for the web, database, and application tiers.

You repeat this procedure six times to create six logical switches. The "Logical Switch Names and Descriptions" table lists the logical switch names, and the business group and tier to which you assign each switch.

Table 3-2. Logical Switch Names and Descriptions

Logical Switch Name	Description	Primary IP address
Production-Web-VXLAN	Logical switch for Web tier of Production Business Group	172.18.20.1
Production-DB-VXLAN	Logical switch for Database tier of Production Business Group	172.18.21.1
Production-App-VXLAN	Logical switch for Application tier of Production Business Group	172.18.22.1
Development-Web-VXLAN	Logical switch for Web tier of Development Business Group	172.18.23.1
Development-DB-VXLAN	Logical switch for Database tier of Development Business Group	172.18.24.1
Development-App-VXLAN	Logical switch for Application tier of Development Business Group	172.18.25.1

Procedure

- 1 Log in to vCenter Server by using the vSphere Web Client.
 - a Open a Web browser and go to **https://nyc01vc01.rainpole.local/vsphere-client**.
 - b Log in using the following credentials.

Setting	Value
User name	administrator@vsphere.local
Password	vsphere_admin_password

- 2 Create a logical switch.
 - a Click **Networking & Security**.
 - b In the Navigator, select **Logical Switches**.
 - c From the **NSX Manager** drop-down menu, select **172.18.11.65** as the NSX Manager.
 - d Click the **New Logical Switch** icon.

The **New Logical Switch** dialog box appears.

- e In the **New Logical Switch** dialog box, enter the following settings, and click **OK**.

Setting	Value
Name	Production-Web-VXLAN
Description	Logical switch for Web tier of Production Business Group
Transport Zone	NYC01
Replication Mode	Hybrid
Enable IP Discovery	Selected
Enable MAC Learning	Deselected

New Logical Switch

Name: * Production-Web-VXLAN

Description: Logical switch for Web tier of Production Business Group

Transport Zone: * NYC01 [Change](#) [Remove](#)

Replication mode:
☐ Multicast
Multicast on Physical network used for VXLAN control plane.
☐ Unicast
VXLAN control plane handled by NSX Controller Cluster.
☒ Hybrid
Optimized Unicast mode. Offloads local traffic replication to physical network.

☒ Enable IP Discovery

☐ Enable MAC Learning

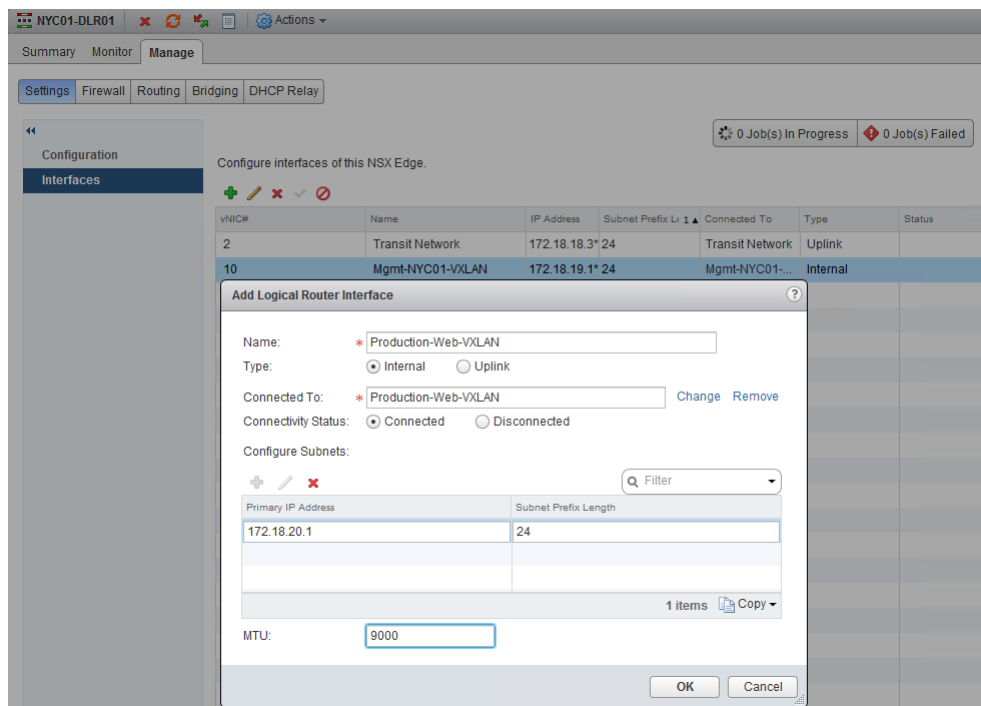
[OK](#) [Cancel](#)

- 3 Repeat this procedure to create the remaining logical switches.

- 4 Connect logical switches to NSX distributed logical router to enable routing.
 - a Click **Networking & Security**.
 - b In the Navigator, select **NSX Edges**.
 - c From the **NSX Manager** drop-down menu, select **172.18.11.65** as the NSX Manager.
 - d Double click the Logical Router **NYC01-DLR01**.
 - e Click **Manage > Settings > Interfaces**.
 - f Click **Add** icon. In the Add Logical Router Interface window, type in the following settings.

Setting	Value
Name	Production-Web-VXLAN
Type	Internal
Connected To	Production-Web-VXLAN
Primary IP Address	172.18.20.1
Subnet Prefix Length	24
MTU	9000

- g Click **OK** to save the configuration.



- 5 Repeat this procedure to enable routing for the remaining logical switches.

Create Customization Specifications in Consolidated vCenter Server in ROBO

Create two customization specifications, one for Linux and one for Windows, for use by the virtual machines you will deploy. Customization specifications are XML files that contain system configuration settings for the guest operating systems used by virtual machines. When you apply a specification to a guest operating system during virtual machine cloning or deployment, you prevent conflicts that might result if you deploy virtual machines with identical settings, such as duplicate computer names.

You will later use the customization specifications that you create when you create blueprints for use with vRealize Automation.

Procedure

1 Create a Customization Specification for Linux in ROBO

Create a Linux guest operating system specification that you can apply when you create blueprints for use with vRealize Automation. This customization specification can be used to customize virtual machine guest operating systems when provisioning new virtual machines from vRealize Automation.

2 Create a Customization Specification for Windows in ROBO

Create a Windows guest operating system specification that you can apply when you create blueprints for use with vRealize Automation. This customization specification can be used to customize virtual machine guest operating systems when provisioning new virtual machines from vRealize Automation.

Create a Customization Specification for Linux in ROBO

Create a Linux guest operating system specification that you can apply when you create blueprints for use with vRealize Automation. This customization specification can be used to customize virtual machine guest operating systems when provisioning new virtual machines from vRealize Automation.

Procedure

1 Log in to vCenter Server by using the vSphere Web Client.

- a Open a Web browser and go to **https://nyc01vc01.rainpole.local/vsphere-client**.
- b Log in using the following credentials.

Setting	Value
User name	administrator@vsphere.local
Password	vsphere_admin_password

2 Navigate to **Home > Operations and Policies > Customization Specification Manager**.

3 Select the vCenter Server **nyc01vc01.rainpole.local** from the drop-down menu.

4 Click the **Create a new specification** icon.

The **New VM Guest Customization Spec** wizard appears.

- 5 On the **Specify Properties** page, select **Linux** from the **Target VM Operating System** drop-down menu, enter **itac-linux-custom-spec** for the **Customization Spec Name**, and click **Next**.
- 6 On the **Set Computer Name** page, select **Use the virtual machine name**, enter **rainpole.local** in the **Domain Name** text box and click **Next**.
- 7 On the **Time Zone** page, specify the time zone as shown in the table below for the virtual machine, and click **Next**.

Setting	Value
Area	America
Location	New York
Hardware Clock Set To	Local Time

- 8 On the **Configure Network** page, click **Next**.
- 9 On the **Enter DNS and domain settings** page, leave the default settings, and click **Next**.
- 10 Click **Finish** to save your changes.

The customization specification that you created is listed in the **Customization Specification Manager**.

Create a Customization Specification for Windows in ROBO

Create a Windows guest operating system specification that you can apply when you create blueprints for use with vRealize Automation. This customization specification can be used to customize virtual machine guest operating systems when provisioning new virtual machines from vRealize Automation.

Procedure

- 1 Log in to vCenter Server by using the vSphere Web Client.
 - a Open a Web browser and go to **https://nyc01vc01.rainpole.local/vsphere-client**.
 - b Log in using the following credentials.

Setting	Value
User name	administrator@vsphere.local
Password	vsphere_admin_password

- 2 Navigate to **Home > Operations and Policies > Customization Specification Manager**.
- 3 Select the vCenter Server **nyc01vc01.rainpole.local** from the drop-down menu.
- 4 Click the **Create a new specification** icon.

The **New VM Guest Customization Spec** wizard appears.

- 5 On the **Specify Properties** page, select **Windows** from the **Target VM Operating System** drop-down menu, enter **itac-windows-joindomain-custom-spec** for the **Customization Spec Name**, and click **Next**.

- 6 On the **Set Registration Information** page, enter **Rainpole** for the virtual machine owner's **Name** and **Organization**, and click **Next**.
- 7 On the **Set Computer Name** page, select **Use the virtual machine name**, and click **Next**.
The operating system uses this name to identify itself on the network.
- 8 On the **Enter Windows License** page, provide licensing information for the Windows operating system, enter the **volume_license_key** license key, and click **Next**.
- 9 Specify the administrator password for use with the virtual machine, and click **Next**.
- 10 On the **Time Zone** page, select **(GMT-05:00) Eastern Time(US & Canada)**, and click **Next**.
- 11 On the **Run Once** page, click **Next**.
- 12 On the **Configure Network** page, click **Next**.
- 13 On the **Set Workgroup or Domain** page, select **Windows Server Domain**, configure the following settings, and click **Next**.

Setting	Value
Domain	rainpole.local
User name	svc-domain@rainpole.local
Password	svc-domain_password

- 14 On the **Set Operating System Options** page, select **Generate New Security ID (SID)**, and click **Next**.
- 15 Click **Finish** to save your changes.

The customization specification that you created is listed in the **Customization Specification Manager**.

Create Virtual Machines Using VM Templates in the Content Library in ROBO

vRealize Automation cannot directly access virtual machine templates in the content library. You must create a virtual machine using the virtual machine templates in the content library, then convert the template in vCenter Server. Perform this procedure on each Consolidated vCenter Server cluster you add to vRealize Automation.

Repeat this procedure three times for each VM Template in the content library. The table below lists the VM Templates and the guest OS each template uses to create a virtual machine.

Table 3-3. VM Templates and their Guest Operating Systems

VM Template Name	Guest OS
redhat6-enterprise-64	Red Hat Enterprise Server 6 (64-bit)
windows-2012r2-64	Windows Server 2012 R2 (64-bit)
windows-2012r2-64-sql2012	Windows Server 2012 R2 (64-bit)

Procedure

- 1 Log in to the Consolidated vCenter Server by using the vSphere Web Client.
 - a Open a Web browser and go to **https://nyc01vc01.rainpole.local/vsphere-client**.
 - b Log in using the following credentials.

Setting	Value
User name	administrator@vsphere.local
Password	vsphere_admin_password

- 2 Navigate to **Home > VMs and Templates**.
- 3 Expand the **nyc01vc01.rainpole.local** vCenter Server.
- 4 Right-click the **NYC01** data center and select **New Folder > New VM and Template Folder**.
- 5 Create a new folder and label it **VM Templates**.
- 6 Navigate to **Home > Content Libraries**.
- 7 Click **NYC01-ContentLib01 > Templates**.
- 8 Right-click the VM Template **redhat6-enterprise-64** and click **New VM from This Template**.
The **New Virtual Machine from Content Library** wizard opens.
- 9 On the **Select name and location** page, use the same template name.

Note Use the same template name to create a common service catalog that works across different vCenter Server instances within your datacenter environment.

- 10 Select **VM Templates** as the folder for this virtual machine, and click **Next**.
- 11 On the **Select a resource** page, expand cluster **NYC01** and select resource pool **User-VM**.
- 12 On the **Review details** page, verify the template details, and click **Next**.
- 13 On the **Select storage** page, select the **NYC01-VSAN01** datastore and **Thin Provision** from the **Select virtual disk format** drop-down menu.
- 14 On the **Select networks** page, select **vDS-NYC01-Management** for the **Destination Network**, and click **Next**.

Note vRealize Automation will change the network according to the blueprint configuration.

- 15 On the **Ready to complete** page, review the configurations you made for the virtual machine, and click **Finish**.

A new task for creating the virtual machine appears in the **Recent Tasks** pane. After the task is complete, the new virtual machine is created.

- 16 Repeat this procedure for all of the VM Templates in the content library.

Convert the Virtual Machines to VM Templates in ROBO

You can convert a virtual machine directly to a template instead of making a copy by cloning.

Repeat this procedure three times for each of the VM Templates in the content library. The table below lists the VM Templates and the guest OS each template uses to create a virtual machine.

Table 3-4. VM Templates and their Guest Operating Systems

VM Template Name	Guest OS
redhat6-enterprise-64	Red Hat Enterprise Server 6 (64-bit)
windows-2012r2-64	Windows Server 2012 R2 (64-bit)
windows-2012r2-64-sql2012	Windows Server 2012 R2 (64-bit)

Procedure

- 1 Log in to the Consolidated vCenter Server by using the vSphere Web Client.
 - a Open a Web browser and go to **`https://nyc01vc01.rainpole.local/vsphere-client`**.
 - b Log in using the following credentials.

Setting	Value
User name	administrator@vsphere.local
Password	vsphere_admin_password

- 2 Navigate to **Home > VMs and Templates**.
- 3 In the **Navigator** pane, expand **nyc01vc01.rainpole.local > NYC01 > VM Templates**.
- 4 Right-click the **redhat6-enterprise-64** virtual machine located in the VM Templates folder, and click **Template > Convert to Template**.
- 5 Click **Yes** to confirm the template conversion.

Add a Consolidated Cluster to the Rainpole Tenant in ROBO

Before provisioning blueprints to a Consolidated Cluster, a vSphere Endpoint needs to be created and compute clusters have to be added into a fabric group. The reservations of compute resources will be added into vRealize Automation for business groups.

Create a vSphere Endpoint in vRealize Automation in ROBO

To allow vRealize Automation to manage the infrastructure, IaaS administrators create endpoints and configure user-credentials for those endpoints. When you create a vSphere Endpoint, vRealize Automation can communicate with the vSphere environment and discover compute resources that are managed by vCenter Server, collect data, and provision machines.

Procedure

- 1 Log in to the vRealize Automation Rainpole portal.
 - a Open a Web browser and go to **`https://vra01svr01.rainpole.local/vcac/org/rainpole`**.
 - b Log in using the following credentials.

Setting	Value
User name	itac-tenantadmin
Password	<i>itac-tenantadmin_password</i>
Domain	rainpole.local

- 2 Navigate to **Infrastructure > Endpoints > Credentials** and click **New**.
- 3 On the **Credentials** page, configure the vRealize Automation credential for the administrator of nyc01vc01.rainpole.local with the following settings, and click **Save**.

Setting	Value
Name	nyc01vc01 admin
Description	Administrator of nyc01vc01.rainpole.local
User Name	svc-vra@rainpole.local
Password	<i>svc-vra_password</i>

- 4 Remain on the **Credentials** page and click **New** once again.
- 5 Configure the NSX administrator credentials of nyc01nsxm01.rainpole.local with the following settings, and click the **Save** icon.

Setting	Value
Name	nyc01nsxm01 admin
Description	Administrator of NSX Manager nyc01nsxm01.rainpole.local
User Name	svc-vra@rainpole.local
Password	<i>svc-vra_password</i>

- 6 Navigate to **Infrastructure > Endpoints > Endpoints** and click **New > Virtual > vSphere (vCenter)**.

- 7 On the **New Endpoint - vSphere (vCenter)** page, create a vSphere Endpoint with the following settings, and click **OK**.

Note The vSphere Endpoint Name must be identical to the name that you used to install the proxy agents.

Setting	Value
Name	nyc01vc01.rainpole.local
Address	https://nyc01vc01.rainpole.local/sdk
Credentials	nyc01vc01 admin
Specify manager for network and security platform	Selected
Address	https://nyc01nsxm01.rainpole.local
Credentials	nyc01nsxm01 admin

Create a Fabric Group with the Consolidated Cluster in ROBO

IaaS administrators can organize virtualization compute resources and cloud endpoints into fabric groups by type and intent. One or more fabric administrators manage the resources in each fabric group. Fabric administrators are responsible for creating reservations on the compute resources in their groups to allocate fabric to specific business groups. Fabric groups are created in a specific tenant, but their resources can be made available to users who belong to business groups in all tenants.

Procedure

- 1 Log in to the vRealize Automation Rainpole portal.
 - a Open a Web browser and go to **https://vra01svr01.rainpole.local/vcac/org/rainpole**.
 - b Log in using the following credentials.

Setting	Value
User name	itac-tenantadmin
Password	<i>itac-tenantadmin_password</i>
Domain	rainpole.local

- 2 Select **Infrastructure > Endpoints > Fabric Groups**.
- 3 Click **New Fabric Group**, enter the following settings and click **OK**.

Setting	Value
Name	NYC01 Fabric Group
Fabric administrators	ug-ITAC-TenantAdmins@rainpole.local

- 4 Select cluster **NYC01** from the **Compute resources** table, and click **OK**.

Note It might take several minutes for vRealize Automation to connect to the vCenter Server system and associated clusters. If you are still not able to see the compute cluster after sufficient time has passed, try to restart both proxy agent services in the virtual machines **nyc01ias01.rainpole.local** and **nyc01ias02.rainpole.local**.

- 5 Log out of the vRealize Automation portal.

Run Data Collection for the Consolidated Cluster in ROBO

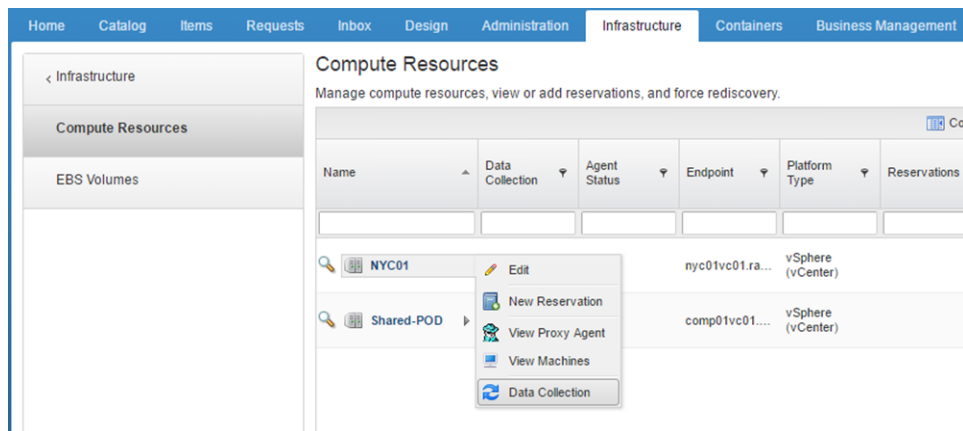
You need to run data collection for the consolidated cluster before you can provision blueprints into that cluster.

Procedure

- 1 Log in to the vRealize Automation Rainpole portal.
 - a Open a Web browser and go to **https://vra01svr01.rainpole.local/vcac/org/rainpole**.
 - b Log in using the following credentials.

Setting	Value
User name	itac-tenantadmin
Password	itac-tenantadmin_password
Domain	rainpole.local

- 2 Navigate to **Infrastructure > Compute Resources > Compute Resources**.
- 3 In the **Compute Resource** column, hover the mouse pointer over the cluster **NYC01**, and click **Data Collection**.



- 4 Click on the **Request now** buttons in each field on the page.
Wait a few seconds for the data collection process to complete.

- 5 Click **Refresh**, and verify that the **Status** for both **Inventory** and **Network and Security Inventory** shows **Succeeded**.

The screenshot shows the VMware vSphere Data Collection interface. The top navigation bar includes links for Home, Catalog, Items, Requests, Inbox, Design, Administration, Infrastructure (selected), Containers, and Business Management. On the left, a sidebar shows the Infrastructure tree with Compute Resources and EBS Volumes. The main content area is titled 'Data Collection' and contains two sections: 'Compute Resource' and 'Inventory'.

Compute Resource

- Name: NYC01
- Platform type: vSphere (vCenter)
- Data collection: ☒ On ☐ Off

Inventory

- Last completed: 3/16/2017 3:28 PM UTC-07:00
- Status: Succeeded
- Data collection: ☒ On ☐ Off
- Frequency (hours): (Leave blank for daily data collection)
- [Request now](#)

Create External Network Profiles in ROBO

Before members of a business group can request virtual machines, fabric administrators must create network profiles to define the subnet and routing configuration for those virtual machines. Each network profile is configured for a specific network port group or virtual network to specify IP address and routing configuration for virtual machines provisioned to that network.

Repeat this procedure six times to create the following external network profiles.

- NYC01-Production-App
- NYC01-Production-DB
- NYC01-Production-Web
- NYC01-Development-App
- NYC01-Development-DB
- NYC01-Development-Web

Procedure

- 1 Log in to the vRealize Automation Rainpole portal.
 - a Open a Web browser and go to **https://vra01svr01.rainpole.local/vcac/org/rainpole**.
 - b Log in using the following credentials.

Setting	Value
User name	itac-tenantadmin
Password	<i>itac-tenantadmin_password</i>
Domain	rainpole.local

- 2 Navigate to **Infrastructure > Reservations > Network Profiles**, and click **New > External**.
- 3 On the **New Network Profile - External** page, specify the network profiles on the **General** tab.
 - a Add the values for the Production Group External Network Profile.

Setting	Production Web Value	Production DB Value	Production App Value
Name	NYC01-Production-Web	NYC01-Production-DB	NYC01-Production-App
Description	External Network profile for Web Tier of Production Business Group	External Network profile for DB Tier of Production Business Group	External Network profile for App Tier of Production Business Group
Subnet mask	255.255.255.0	255.255.255.0	255.255.255.0
Gateway	172.18.20.1	172.18.21.1	172.18.22.1

- b Add the values for the Development Group External Network Profile.

Setting	Development Web Value	Development DB Value	Development App Value
Name	NYC01-Development-Web	NYC01-Development-DB	NYC01-Development-App
Description	External Network profile for Web Tier of Development Business Group	External Network profile for DB Tier of Development Business Group	External Network profile for App Tier of Development Business Group
Subnet mask	255.255.255.0	255.255.255.0	255.255.255.0
Gateway	172.18.23.1	172.18.24.1	172.18.25.1

- 4 Click the **DNS** tab. Enter the following values for the profile you are creating.

Setting	Value
Primary DNS	172.18.11.4
Secondary DNS	172.16.11.4
DNS suffix	rainpole.local
DNS search suffix	rainpole.local

- 5 Click the **Network Ranges** tab.

- 6 On the **Network Ranges** tab, click the **New** button and enter the following values for the profile you are creating.

- a Enter the following values for Production Business Network Range.

Setting	Production Web Value	Production DB Value	Production App Value
Name	Production-Web	Production-DB	Production-App
Description	Static IP range for Web Tier of Production Group	Static IP range for DB Tier of Production Group	Static IP range for App Tier of Production Group
Start IP	172.18.20.20	172.18.21.20	172.18.22.20
End IP	172.18.20.250	172.18.21.250	172.18.22.250

- b Enter the following values for Development Business IP Range.

Setting	Development Web Value	Development DB Value	Development App Value
Name	Development-Web	Development-DB	Development-App
Description	Static IP range for Web Tier of Development Group	Static IP range for DB Tier of Development Group	Static IP range for App Tier of Development Group
Start IP	172.18.23.20	172.18.24.20	172.18.25.20
End IP	172.18.23.250	172.18.24.250	172.18.25.250

- c Click **OK** to save the network range.

- 7 Click **OK** to save the network profile.

- 8 Repeat this procedure to create additional external network profiles.

When all of the network profiles have been added, the **Network Profiles** page displays six profiles.

Create Reservation Policies in ROBO

You use reservation policies to group similar reservations together. Create the reservation policy tag first, then add the policy to reservations to allow a tenant administrator or business group manager to use the reservation policy in a blueprint.

When you request a machine, it can be provisioned on any reservation of the appropriate type that has sufficient capacity for the machine. You can apply a reservation policy to a blueprint to restrict the machines provisioned from that blueprint to a subset of available reservations. A reservation policy is often used to collect resources into groups for different service levels, or to make a specific type of resource easily available for a particular purpose. You can add multiple reservations to a reservation policy, but a reservation can belong to only one policy. You can assign a single reservation policy to more than one blueprint. A blueprint can have only one reservation policy. A reservation policy can include reservations of different types, but only reservations that match the blueprint type are considered when selecting a reservation for a particular request.

Procedure

- 1 Log in to the vRealize Automation Rainpole portal.
 - a Open a Web browser and go to **https://vra01svr01.rainpole.local/vcac/org/rainpole**.
 - b Log in using the following credentials.

Setting	Value
User name	itac-tenantadmin
Password	<i>itac-tenantadmin_password</i>
Domain	rainpole.local

- 2 Navigate to **Infrastructure > Reservation > Reservation Policies**.
- 3 Click the **New** icon, configure the following settings, and click the **Save** icon.

Setting	Value
Name	NYC01-Production-Policy
Description	Reservation policy for Production Business Group in NYC01

- 4 Click the **New** icon, configure the following settings, and click the **Save** icon.

Setting	Value
Name	NYC01-Development-Policy
Description	Reservation policy for Development Business Group in NYC01

- 5 Click the **New** icon, configure the following settings, and click the **Save** icon.

Setting	Value
Name	NYC01-Edge-Policy
Description	Reservation policy for Tenant Edge resources in NYC01

Create Reservations for the Consolidated Cluster in ROBO

Before members of a business group can request machines, fabric administrators must allocate resources to them by creating a reservation. Each reservation is configured for a specific business group to grant them access to request machines on a specified compute resource.

Perform this procedure twice to create compute resource reservations for both the Production and Development business groups.

Table 3-5. Business Group Names

Group	Name
Production	NYC01-Prod-Res01
Development	NYC01-Dev-Res01

Procedure

- 1 Log in to the vRealize Automation Rainpole portal.
 - a Open a Web browser and go to **https://vra01svr01.rainpole.local/vcac/org/rainpole**.
 - b Log in using the following credentials.

Setting	Value
User name	itac-tenantadmin
Password	<i>itac-tenantadmin_password</i>
Domain	rainpole.local

- 2 Navigate to **Infrastructure > Reservations > Reservations** and select **New > vSphere (vCenter)**.
- 3 On the **New Reservation - vSphere (vCenter)** page, click the **General** tab, and configure the following values for each group.

Setting	Production Group Value	Development Group Value
Name	NYC01-Prod-Res01	NYC01-Dev-Res01
Tenant	rainpole	rainpole
Business Group	Production	Development
Reservation Policy	NYC01-Production-Policy	NYC01-Development-Policy
Priority	100	100
Enable This Reservation	Selected	Selected

- 4 On the **New Reservation - vSphere (vCenter)** page, click the **Resources** tab.
 - a Select **NYC01(nyc01vc01.rainpole.local)** from the **Compute Resource** drop-down menu.
 - b In the **This Reservation** column of the **Memory (GB)** table, enter **200**.

- c In the **Storage (GB)** table, select the check box for datastore **NYC01-VSAN01**, and enter **2000** in the **This Reservation Reserved** text box, enter **1** in the **Priority** text box, and click **OK**.
- d Select **User-VM** from the **Resource pool** drop-down menu.

New Reservation - vSphere (vCenter)

Create a reservation to allocate provisioning resources to a business group in a tenant. You also can copy an existing reservation to use as a starting point.

General Resources Network Properties Alerts

* Compute resource: NYC01 (nyc01vc01.rainpole.local)

Machine quota: Unlimited

* Memory (GB):

Physical	Total Reserved	Total Allocated	This Reservation
1024	0	0	200

* Storage (GB):

Storage Path	Physical	Free	Total Reserved	This Reservation Reserved	This Reservation Allocated	Priority
NYC01-NFS0...	4033	1299	0			
NYC01-VSAN01	17706	17299	0	2000	0	1

Resource pool: User-VM

- 5 On the **New Reservation - vSphere (vCenter)** page, click the **Network** tab.
- 6 On the **Network** tab, select the network path check boxes listed in the table below from the **Network Paths** list, and select the corresponding network profile from the **Network Profile** drop-down menu for the business group whose reservation you are configuring.
 - a Configure the Production Business Group with the following values.

Production Network Path	Production Group Network Profile
vxw-dvs-xxxxx-Production-Web-VXLAN	NYC01-Production-Web
vxw-dvs-xxxxx-Production-DB-VXLAN	NYC01-Production-DB
vxw-dvs-xxxxx-Production-App-VXLAN	NYC01-Production-App

- b Configure the Development Business Group with the following values.

Development Network Path	Development Group Network Profile
vxw-dvs-xxxxx-Development-Web-VXLAN	NYC01-Development-Web
vxw-dvs-xxxxx-Development-DB-VXLAN	NYC01-Development-DB
vxw-dvs-xxxxx-Development-App-VXLAN	NYC01-Development-App

The screenshot shows the 'New Reservation - vSphere (vCenter)' window in the vRealize Automation console. The 'Network' tab is active, displaying a table of network configurations. The table has two columns: 'Network Adapter' and 'Network Profile'. Several adapters are listed, including vDS-NYC01-DVUplinks-36, vDS-NYC01-Management, vDS-NYC01-NFS, vDS-NYC01-Uplink01, vDS-NYC01-Uplink02, vDS-NYC01-vMotion, and vDS-NYC01-VSAN. Below these, there are vxxv-dvs-36 virtual switch entries for different VMs. The 'vds-NYC01-VSAN' adapter is selected, and the 'NYC01-Production-Web' profile is chosen for it. The 'OK' button is at the bottom right.

Network Adapter	Network Profile
vDS-NYC01-DVUplinks-36	
vDS-NYC01-Management	
vDS-NYC01-NFS	
vDS-NYC01-Uplink01	
vDS-NYC01-Uplink02	
vDS-NYC01-vMotion	
vDS-NYC01-VSAN	
vxxv-dvs-36-virtualwire-1-sid-5000-Transit Network	
vxxv-dvs-36-virtualwire-2-sid-5001-Mgmt-NYC01-VXLAN	
vxxv-dvs-36-virtualwire-3-sid-5002-Production-Web-VXLAN	NYC01-Production-Web
vxxv-dvs-36-virtualwire-4-sid-5003-Production-DB-VXLAN	NYC01-Production-DB
vxxv-dvs-36-virtualwire-5-sid-5004-Production-App-VXLAN	NYC01-Production-Web
vxxv-dvs-36-virtualwire-6-sid-5005-Development-Web-VXLAN	
vxxv-dvs-36-virtualwire-7-sid-5006-Development-DB-VXLAN	

7 Click **OK** to save the reservation.

8 Repeat this procedure to create a reservation for the Development Business Group.

Create Reservations for the User Edge Resources in ROBO

Before members of a business group can request virtual machines, fabric administrators must allocate resources to that business group by creating a reservation. Each reservation is configured for a specific business group to grant them access to request virtual machines on a specified compute resource.

Perform this procedure twice to create Edge reservations for both the Production and Development business groups.

Table 3-6. Business Group Names

Group	Name
Production	NYC01-Edge01-Prod-Res01
Development	NYC01-Edge01-Dev-Res01

Procedure

- 1 Log in to the vRealize Automation Rainpole portal.
 - a Open a Web browser and go to **`https://vra01svr01.rainpole.local/vcac/org/rainpole`**.
 - b Log in using the following credentials.

Setting	Value
User name	itac-tenantadmin
Password	<i>itac-tenantadmin_password</i>
Domain	rainpole.local

- 2 Navigate to **Infrastructure > Reservations > Reservations**, and click **New vSphere (vCenter)**.

- 3 On the **New Reservation - vSphere (vCenter)** page, click the **General** tab, and configure the following values for your business group.

Setting	Production Group Value	Development Group Value
Name	NYC01-Edge01-Prod-Res01	NYC01-Edge01-Dev-Res01
Tenant	rainpole	rainpole
Business Group	Production	Development
Reservation Policy	NYC01-Edge-Policy	NYC01-Edge-Policy
Priority	100	100
Enable This Reservation	Selected	Selected

- 4 On the **New Reservation - vSphere (vCenter)** page, click the **Resources** tab.
- Select **NYC01(nyc01vc01.rainpole.local)** from the **Compute resource** drop-down menu.
 - Enter **200** in the **This Reservation** column of the **Memory (GB)** table.
 - In the **Storage (GB)** table, select the check box for datastore **NYC01-VSAN01**, enter **2000** in the **This Reservation Reserved** text box, enter **1** in the **Priority** text box, and click **OK**.
 - Select **User-Edge** from the **Resource pool** drop-down menu.

Home Catalog Items Requests Inbox Design Administration Infrastructure Containers Business Management

< Infrastructure

Key Pairs

Reservations

Reservation Policies

Network Profiles

New Reservation - vSphere (vCenter)

Create a reservation to allocate provisioning resources to a business group in a tenant. You also can copy an existing reservation to use as a starting point.

Copy from existing reservation: --Select an item to copy--

General Resources Network Properties Alerts

* Compute resource: NYC01 (nyc01vc01.rainpole.local)

Machine quota: Unlimited

* Memory (GB):

Physical	Total Reserved	Total Allocated	This Reservation
1024	400	0	200

* Storage (GB):

	Storage Path	Physical	Free	Total Reserved	This Reservation Reserved	This Reservation Allocated	Priority
<input type="checkbox"/>	NYC01-NFS...	4033	1299	0			
<input checked="" type="checkbox"/>	NYC01-VSA...	17706	17299	4000	2000	0	1

Resource pool: User-Edge

OK Cancel

- 5 On the **New Reservation - vSphere (vCenter)** page, click the **Network** tab.
- 6 On the **Network** tab, select the network path check boxes listed in the table below from the **Network Paths** list, and select the corresponding network profile from the **Network Profile** drop-down menu for the business group whose reservation you are configuring.

Production Business Group

Production Port Group	Production Network Profile
vxxw-dvs-xxxxx-Production-Web-VXLAN	NYC01-Production-Web
vxxw-dvs-xxxxx-Production-DB-VXLAN	NYC01-Production-DB
vxxw-dvs-xxxxx-Production-App-VXLAN	NYC01-Production-App

Development Business Group

Development Port Group	Development Network Profile
vxxw-dvs-xxxxx-Development -Web-VXLAN	NYC01-Development -Web
vxxw-dvs-xxxxx-Development -DB-VXLAN	NYC01-Development -DB
vxxw-dvs-xxxxx-Development -App-VXLAN	NYC01-Development -App

The screenshot shows the 'New Reservation - vSphere (vCenter)' dialog box. The 'Network' tab is active, displaying a table of network adapters and their profiles. The selected network adapter is 'vxxw-dvs-36-virtualwire-3-sid-5002-Production-Web-VXLAN', and its network profile is 'NYC01-Production-Web'.

Network Adapter	Network Profile
vDS-NYC01-DVUplinks-36	
vDS-NYC01-Management	
vDS-NYC01-NFS	
vDS-NYC01-Uplink01	
vDS-NYC01-Uplink02	
vDS-NYC01-vMotion	
vDS-NYC01-VSAN	
vxxw-dvs-36-virtualwire-1-sid-5000-Transit Network	
vxxw-dvs-36-virtualwire-2-sid-5001-Mgmt-NYC01-VXLAN	
vxxw-dvs-36-virtualwire-3-sid-5002-Production-Web-VXLAN	NYC01-Production-Web
vxxw-dvs-36-virtualwire-4-sid-5003-Production-DB-VXLAN	NYC01-Production-DB
vxxw-dvs-36-virtualwire-5-sid-5004-Production-App-VXLAN	NYC01-Production-App
vxxw-dvs-36-virtualwire-6-sid-5005-Development-Web-VXLAN	
vxxw-dvs-36-virtualwire-7-sid-5006-Development-DB-VXLAN	

- Click **OK** to save the reservation.
- Repeat the procedure to create the Edge reservation for the Development Business Group.

Configure Single Machine Blueprints in ROBO

Virtual machine blueprints determine a machine's attributes, the manner in which it is provisioned, and its policy and management settings.

Procedure

1 Create a Service Catalog in ROBO

A service catalog provides a common interface for consumers of IT services to request services, track their requests, and manage their provisioned service items.

2 Create a Single Machine Blueprint in ROBO

Create a blueprint for cloning the windows-2012r2-64 virtual machine using the specified resources on the Consolidated vCenter Server. Tenants can later use this blueprint for automatic provisioning. A blueprint is the complete specification for a virtual, cloud, or physical machine. Blueprints determine a machine's attributes, the manner in which it is provisioned, and its policy and management settings.

3 Configure Entitlements of Blueprints in ROBO

You entitle users to the actions and items that belong to the service catalog by associating each blueprint with an entitlement.

Create a Service Catalog in ROBO

A service catalog provides a common interface for consumers of IT services to request services, track their requests, and manage their provisioned service items.

Procedure

- 1 Log in to the vRealize Automation Rainpole portal.
 - a Open a Web browser and go to **`https://vra01svr01.rainpole.local/vcac/org/rainpole`**.
 - b Log in using the following credentials.

Setting	Value
User name	itac-tenantadmin
Password	<i>itac-tenantadmin_password</i>
Domain	rainpole.local

- 2 Navigate to the **Administration** tab, click **Catalog Management > Services**, and click **New**. The **New Service** page appears.
- 3 In the **New Service** page, configure the following settings, and click **OK**.

Setting	Value
Name	NYC01 Service Catalog
Description	Default setting (blank)
Status	Active
Icon	Default setting (blank)
Status	Default setting (blank)
Hours	Default setting (blank)
Owner	Default setting (blank)
Support Team	Default setting (blank)
Change Window	Default setting (blank)

Create a Single Machine Blueprint in ROBO

Create a blueprint for cloning the windows-2012r2-64 virtual machine using the specified resources on the Consolidated vCenter Server. Tenants can later use this blueprint for automatic provisioning. A blueprint is the complete specification for a virtual, cloud, or physical machine. Blueprints determine a machine's attributes, the manner in which it is provisioned, and its policy and management settings.

Repeat this procedure to create six blueprints.

Blueprint Name	VM Template	Reservation Policy	Service Catalog	Add to Entitlement
Windows Server 2012 R2 - NYC01 Prod	windows-2012r2-64 (nyc01vc01.rainpole.local)	NYC01-Production-Policy	NYC01 Service Catalog	Prod-SingleVM-Entitlement
Windows Server 2012 R2 - NYC01 Dev	windows-2012r2-64 (nyc01vc01.rainpole.local)	NYC01-Development-Policy	NYC01 Service Catalog	Dev-SingleVM-Entitlement
Windows Server 2012 R2 With SQL2012 - NYC01 Prod	windows-2012r2-64-sql2012(nyc01vc01.rainpole.local)	NYC01-Production-Policy	NYC01 Service Catalog	Prod-SingleVM-Entitlement
Windows Server 2012 R2 With SQL2012 - NYC01 Dev	windows-2012r2-64-sql2012(nyc01vc01.rainpole.local)	NYC01-Development-Policy	NYC01 Service Catalog	Dev-SingleVM-Entitlement
Redhat Enterprise Linux 6 - NYC01 Prod	redhat6-enterprise-64(nyc01vc01.rainpole.local)	NYC01-Production-Policy	NYC01 Service Catalog	Prod-SingleVM-Entitlement
Redhat Enterprise Linux 6 - NYC01 Dev	redhat6-enterprise-64(nyc01vc01.rainpole.local)	NYC01-Development-Policy	NYC01 Service Catalog	Dev-SingleVM-Entitlement

Procedure

- 1 Log in to the vRealize Automation Rainpole portal.
 - a Open a Web browser and go to **`https://vra01svr01.rainpole.local/vcac/org/rainpole`**.
 - b Log in using the following credentials.

Setting	Value
User name	itac-tenantadmin
Password	<i>itac-tenantadmin_password</i>
Domain	rainpole.local

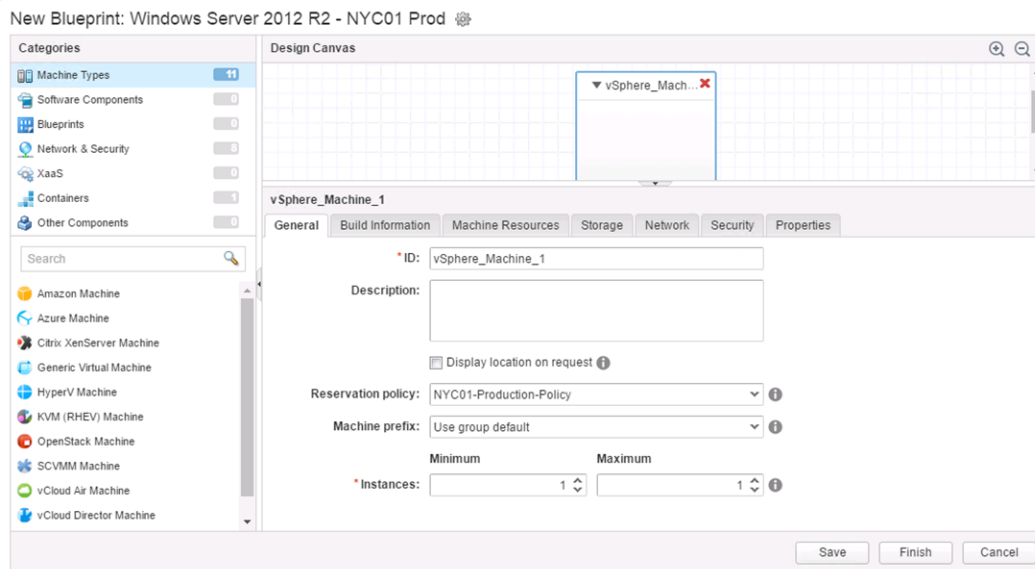
- 2 Navigate to **Design > Blueprints**.
- 3 Click **New**.

- 4 In the **New Blueprint** dialog box, configure the following settings on the **General** tab, and click **OK**.

Setting	Value
Name	Windows Server 2012 R2 - NYC01 Prod
Archive (days)	15
Deployment limit	Default setting (blank)
Minimum	30
Maximum	270

- 5 Select and drag the **vSphere Machine** icon to the **Design Canvas**.
- 6 Click the **General** tab, configure the following settings, and click **Save**.

Setting	Default
ID	Default setting (vSphere_Machine_1)
Description	Default setting (blank)
Display location on request	Deselected
Reservation policy	NYC01-Production-Policy
Machine prefix	Default setting (blank)
Minimum	Default setting (blank)
Maximum	Default setting (blank)



- 7 Click the **Build Information** tab, configure the following settings, and click **Save**.

Setting	Value
Blueprint type	Server
Action	Clone

Setting	Value
Provisioning workflow	CloneWorkflow
Clone from	windows-2012r2-64
Customization spec	itac-windows-joindomain-custom-spec

- 8 Click the **Machine Resources** tab, configure the following settings, and click **Save**.

Setting	Minimum	Maximum
CPU	2	4
Memory (MB):	4096	16384
Storage	Default setting (blank)	Default setting (60)

- 9 Click the **Network** tab.

- Select **Network & Security** in the **Categories** section to display the list of available network and security components.
- Select the **Existing Network** component and drag it onto the **Design Canvas**.
- Click in the **Existing network** text box and select the **NYC01-Production-Web** network profile.

Blueprint Name	Existing network
Windows Server 2012 R2 - NYC01 Prod	NYC01-Production-Web
Windows Server 2012 R2 - NYC01 Dev	NYC01-Development-Web
Windows Server 2012 R2 With SQL2012 - NYC01 Prod	NYC01-Production-DB
Windows Server 2012 R2 With SQL2012 - NYC01 Dev	NYC01-Development-DB
Redhat Enterprise Linux 6 - NYC01 Prod	NYC01-Production-App
Redhat Enterprise Linux 6 - NYC01 Dev	NYC01-Development-App

- Click **Save**.
- Select **vSphere_machine** properties from the design canvas.
- Select the **Network** tab, click **New**, configure the following settings, and click **OK**.

Network	Assignment Type	Address
NYC01ProductionWeb	Static IP	Default setting (blank)
NYC01DevelopmentWeb	Static IP	Default setting (blank)
NYC01ProductionDB	Static IP	Default setting (blank)
NYC01DevelopmentDB	Static IP	Default setting (blank)
NYC01ProductionApp	Static IP	Default setting (blank)
NYC01DevelopmentApp	Static IP	Default setting (blank)

- Click **Finish** to save the blueprint.

- 10 Select the blueprint **Windows Server 2012 R2 -NYC01 Prod** and click **Publish**.

11 Repeat this procedure to create additional blueprints.

Configure Entitlements of Blueprints in ROBO

You entitle users to the actions and items that belong to the service catalog by associating each blueprint with an entitlement.

Repeat this procedure to associate the six blueprints with their entitlement.

Blueprint Name	VM Template	Reservation Policy	Service Catalog	Add to Entitlement
Windows Server 2012 R2 - NYC01 Prod	windows-2012r2-64 (nyc01vc01.rainpole.local)	NYC01-Production-Policy	NYC01 Service Catalog	Prod-SingleVM-Entitlement
Windows Server 2012 R2 - NYC01 Dev	windows-2012r2-64 (nyc01vc01.rainpole.local)	NYC01-Development-Policy	NYC01 Service Catalog	Dev-SingleVM-Entitlement
Windows Server 2012 R2 With SQL2012 - NYC01 Prod	windows-2012r2-64-sql2012(nyc01vc01.rainpole.local)	NYC01-Production-Policy	NYC01 Service Catalog	Prod-SingleVM-Entitlement
Windows Server 2012 R2 With SQL2012 - NYC01 Dev	windows-2012r2-64-sql2012(nyc01vc01.rainpole.local)	NYC01-Development-Policy	NYC01 Service Catalog	Dev-SingleVM-Entitlement
Redhat Enterprise Linux 6 - NYC01 Prod	redhat6-enterprise-64(nyc01vc01.rainpole.local)	NYC01-Production-Policy	NYC01 Service Catalog	Prod-SingleVM-Entitlement
Redhat Enterprise Linux 6 - NYC01 Dev	redhat6-enterprise-64(nyc01vc01.rainpole.local)	NYC01-Development-Policy	NYC01 Service Catalog	Dev-SingleVM-Entitlement

Procedure

- 1 Log in to the vRealize Automation Rainpole portal.
 - a Open a Web browser and go to **`https://vra01svr01.rainpole.local/vcac/org/rainpole`**.
 - b Log in using the following credentials.

Setting	Value
User name	itac-tenantadmin
Password	<i>itac-tenantadmin_password</i>
Domain	rainpole.local

- 2 Select the **Administration** tab and navigate to **Catalog Management > Catalog Items**.
- 3 On the **Configure Catalog Items** pane, select the **Windows Server 2012 R2 - NYC01 Prod** blueprint in the **Catalog Items** list and click **Configure**.
- 4 On the **General** tab of the **Configure Catalog Items** dialog box, select **NYC01 Service Catalog** from the **Service** drop-down menu, and click **OK**.

- 5 Associate the blueprint with the **Prod-SingleVM-Entitlement** entitlement.
 - a Click **Entitlements** on the left of the Configure Catalog Item pane and select **Prod-SingleVM-Entitlement**.
The **Edit Entitlement** pane appears.
 - b Select the **Items & Approvals** tab and add the **Windows Server 2012 R2 -NYC01 Prod** blueprint to the **Entitled Items** list.
 - c Click **Finish**.
- 6 Select the **Catalog** tab and verify that the blueprint is listed in the **Service Catalog**.
- 7 Click **Request** button to request a virtual machine using **Windows Server 2012 R2 - NYC01 Prod** blueprint.
- 8 Click **Requests** tab to monitor the status of the provision request. Verify the request completes successfully.
- 9 Repeat this procedure to associate all of the blueprints with their entitlement.

Configure Unified Single Machine Blueprints for Cross-ROBO Deployment

To provision blueprints from a specific vRealize Automation blueprint to multiple remote offices and branch offices, you must define the additional remote office and branch office locations in vRealize Automation, and associate the blueprints with those locations.

Procedure

- 1 [Add Data Center Locations to the Compute Resource Menu in ROBO](#)
You can configure new data center locations and resources in the Compute Resource menu of the vRealize Automation deployment selection screen, allowing you to more easily select new compute resources for deployment. To add a new location to the Compute Resource menu, you edit an XML file on the vRealize Automation server.
- 2 [Associate Compute Resources with a Location in ROBO](#)
Each data center location has its own compute resources, which you associate with that site for its dedicated use.
- 3 [Create a Property Definition for the Data Center Location in ROBO](#)
Property definitions let you more easily control which location to deploy a blueprint, and based on that choice, which storage and network resources to use with that blueprint.
- 4 [Create a vRealize Orchestrator Action to Provide Network Profiles for Remote Sites](#)
Create a vRealize Orchestrator Action to provide available network profiles for different remote office locations.
- 5 [Create a Property Definition using the vRealize Orchestrator Action in ROBO](#)
Create a Custom Property Definition using the vRealize Orchestrator Action.

6 Add a Property Group with Cross-ROBO deployment custom properties**7 Create a Reservation Policy for the Unified Blueprint in ROBO**

When tenant administrators and business group managers create a new blueprint, the option to add a reservation policy becomes available. To add a reservation policy to an existing blueprint, edit the blueprint.

8 Specify Reservation Information for the Unified Blueprint in ROBO

Each reservation is configured for a specific business group to grant them access to request specific physical machines.

9 Create a Service Catalog for the Unified Blueprint in ROBO

The service catalog provides a common interface for consumers of IT services to request and manage the services and resources they need. Users can browse the catalog to request services, track their requests, and manage their provisioned service items.

10 Create an Entitlement for the Unified Blueprint Catalog in ROBO

Entitle all blueprints in the Unified Blueprint Catalog to the Production and Development business groups. Entitlements determine which users and groups can request specific catalog items or perform specific actions. Entitlements are specific to a business group, and allow users in different business groups to access the blueprint catalog.

11 Create Unified Single Machine Blueprints in ROBO

A blueprint is the complete specification for a virtual, cloud, or physical machine. Blueprints determine a machine's attributes, the manner in which it is provisioned, and its policy and management settings. Create three blueprints from which to clone the virtual machine for your environment using pre-configured resources on the vCenter Server compute cluster in Region A and the consolidated cluster in ROBO. Tenants use these blueprints to automatically provision virtual machines.

12 Test the Cross-ROBO Deployment of the Unified Single Machine Blueprints

The data center environment is now ready for the multi-site deployment of virtual machines using vRealize Automation. Test your environment and confirm the successful provisioning of virtual machines using the blueprints you created to both Region A and ROBO.

Add Data Center Locations to the Compute Resource Menu in ROBO

You can configure new data center locations and resources in the Compute Resource menu of the vRealize Automation deployment selection screen, allowing you to more easily select new compute resources for deployment. To add a new location to the Compute Resource menu, you edit an XML file on the vRealize Automation server.

Perform this procedure for both IaaS Web server virtual machines: vra01iws01a and vra01iws01b.

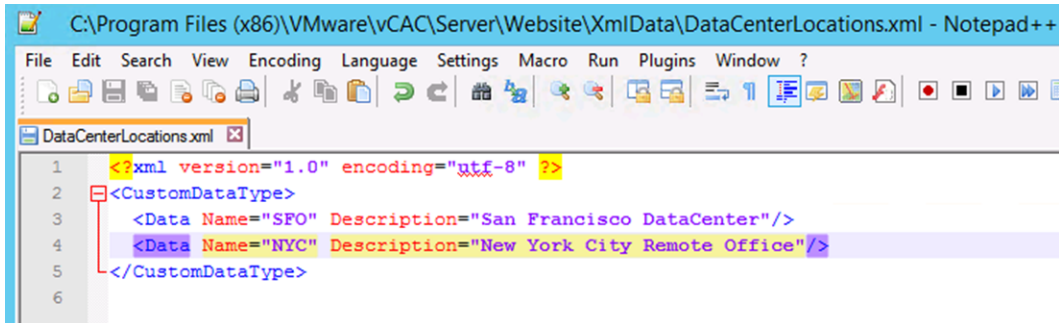
Procedure

- 1 Log in to the vSphere Web Client.
 - a Open a Web browser and go to
https://mgmt01vc01.sfo01.rainpole.local/vsphere-client.
 - b Log in using the following credentials.

Setting	Value
User name	administrator@vsphere.local
Password	vcenter_admin_password

- 2 Open a VM console to the IaaS Web server virtual machine **vra01iws01a**, and log in using administrator credentials.
 - a Open the file C:\Program Files (x86)\VMware\VCAC\Server\Website\XmlData\DataCenterLocations.xml in a text editor.
 - b Update the Data Name and Description attributes to use the following settings.

Data Name	Description
SFO	San Francisco DataCenter
NYC	New York City Remote Office



- 3 Save and close the file.
- 4 Restart the IaaS Web server virtual machine **vra01iws01a**.
Wait until the virtual machine restarts and is successfully running.
- 5 Repeat this procedure for the IaaS web server virtual machine **vra01iws01b**.

Associate Compute Resources with a Location in ROBO

Each data center location has its own compute resources, which you associate with that site for its dedicated use.

Repeat this procedure for each consolidated cluster in each ROBO location.

Location	Consolidated/Compute Cluster
SFO	SFO01-Comp01
NYC	NYC01

Procedure

- 1 Log in to the vRealize Automation Rainpole portal.
 - a Open a Web browser and go to **https://vra01svr01.rainpole.local/vcac/org/rainpole**.
 - b Log in using the following credentials.

Setting	Value
User name	itac-tenantadmin
Password	<i>itac-tenantadmin_password</i>
Domain	rainpole.local

- 2 Select **Infrastructure > Compute Resources > Compute Resources**.
- 3 Using the mouse pointer, point to the compute resource **SFO01-Comp01** and click **Edit**.
- 4 Select **SFO** from the **Locations** drop-down menu.

This will be the data center location for the **SFO01-Comp01** cluster.

The screenshot shows the 'Infrastructure Service Portal' interface. The left sidebar has a tree view with 'Infrastructure' selected, containing 'Compute Resources' and 'EBS Volumes'. The main area is titled 'Edit Compute Resource' with a subtitle 'To modify the compute resource, make the changes below.' There are two tabs: 'General' (active) and 'Configuration'. The 'General' tab shows the following fields:

- Name:** SFO01-Comp01
- Proxy agent name:** vSphere-Agent-01
- Description:** (empty text box)
- Location:** SFO (selected in a dropdown menu)
- Fabric groups:** A list box containing 'LAX Fabric Group' and 'SFO Fabric Group'. The 'SFO Fabric Group' is selected with a checkmark.
- Custom properties:** A section with '+ New', 'Edit', and 'Delete' icons. Below is a table with columns 'Name', 'Value', and 'Encrypted'. The table is currently empty, with the text 'No data to display' at the bottom.

At the bottom right of the form are 'OK' and 'Cancel' buttons.

- 5 Click **OK**.
- 6 Repeat this to set data center location for **NYC01** cluster.

Create a Property Definition for the Data Center Location in ROBO

Property definitions let you more easily control which location to deploy a blueprint, and based on that choice, which storage and network resources to use with that blueprint.

Procedure

- 1 Log in to the vRealize Automation Rainpole portal.
 - a Open a Web browser and go to **https://vra01svr01.rainpole.local/vcac/org/rainpole**.
 - b Log in using the following credentials.

Setting	Value
User name	itac-tenantadmin
Password	<i>itac-tenantadmin_password</i>
Domain	rainpole.local

- 2 Select **Administration > Property Dictionary > Property Definitions**.
- 3 Click **New** to create a property definition.
- 4 Enter **Vrm.DataCenter.Location** in the **Name** text box.

Note The property definition name is case sensitive, and must exactly match the property name used in the blueprint or build profile.

- 5 Enter **Where to deploy** in the **Label** text box.
- 6 In the **Visibility** section, select the **All Tenants** radio button and specify to which tenant the property is available.
- 7 (Optional) Enter a property description in the **Description** text box.
Describe the purpose of the property, and any information that might help the consumer use the property.
- 8 Enter **1** for **Display order**.
- 9 Select **String** from the **Data type** drop-down menu.
- 10 Select **Yes** from the **Required** drop-down menu.
- 11 Select **Dropdown** from the **Display As** drop-down menu.
- 12 Select **Static list** for **Values**.
- 13 Deselect **Enable custom value entry**.

- 14 Click **New** in the **Static list** area and enter a property name and value from the following table. Click **OK** to save both predefined values.

Name	Value
San Francisco	SFO
New York City	NYC

- 15 Click **OK** to save the property definition.

The property is created and available on the **Property Definitions** page.

Create a vRealize Orchestrator Action to Provide Network Profiles for Remote Sites

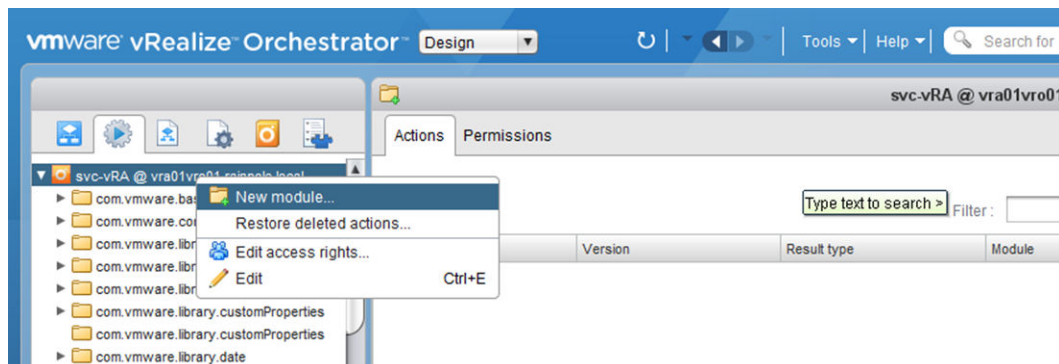
Create a vRealize Orchestrator Action to provide available network profiles for different remote office locations.

Procedure

- 1 Open a Web browser and go to **https://vra01vro01a.rainpole.local:8281**.
 - a Click **Start Orchestrator Client**.
 - b On the VMware vRealize Orchestrator login page, log in to the vRealize Orchestrator Host A by using the following host name and credentials.

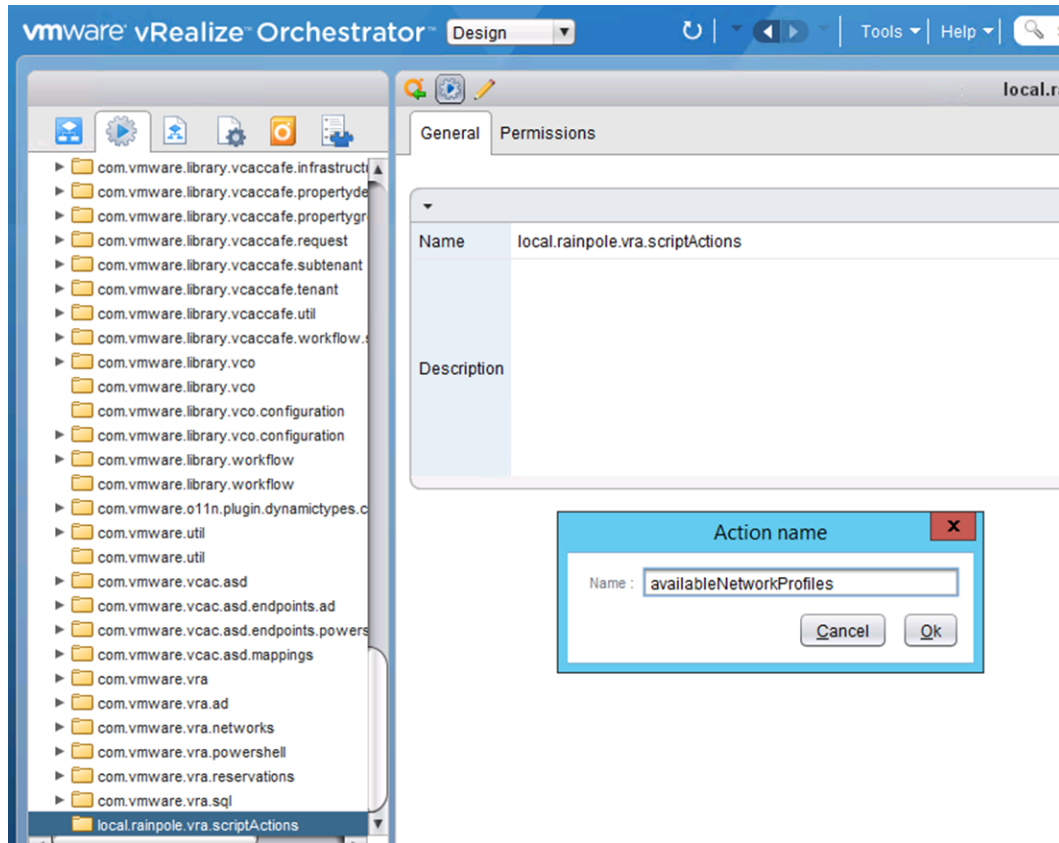
Setting	Value
Host name	vra01vro01.rainpole.local:8281
User name	svc-vra
Password	svc-vra_password

- 2 Select **Design Mode** from the drop-down list located in the upper left of the vRealize Orchestrator Client.
- 3 Select the **Actions** icon from the left navigation panel.
- 4 Right click **svc-vRA @ vra01vro01.rainpole.local** and select **New module**.

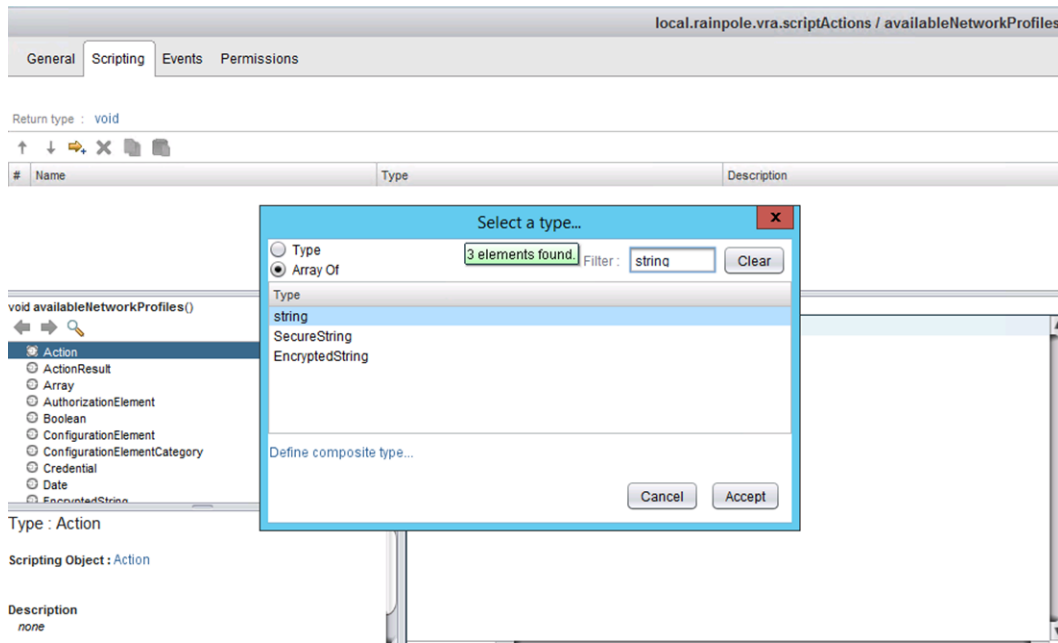


- 5 Enter **local.rainpole.vra.scriptActions** for the **Name** in the pop-up **Module Name** window.

- 6 Select **local.rainpole.vra.scriptActions** from the left panel.
- 7 Click **Add Actions** icon.
- 8 Enter **availableNetworkProfiles** in the **Action Name** dialog box.

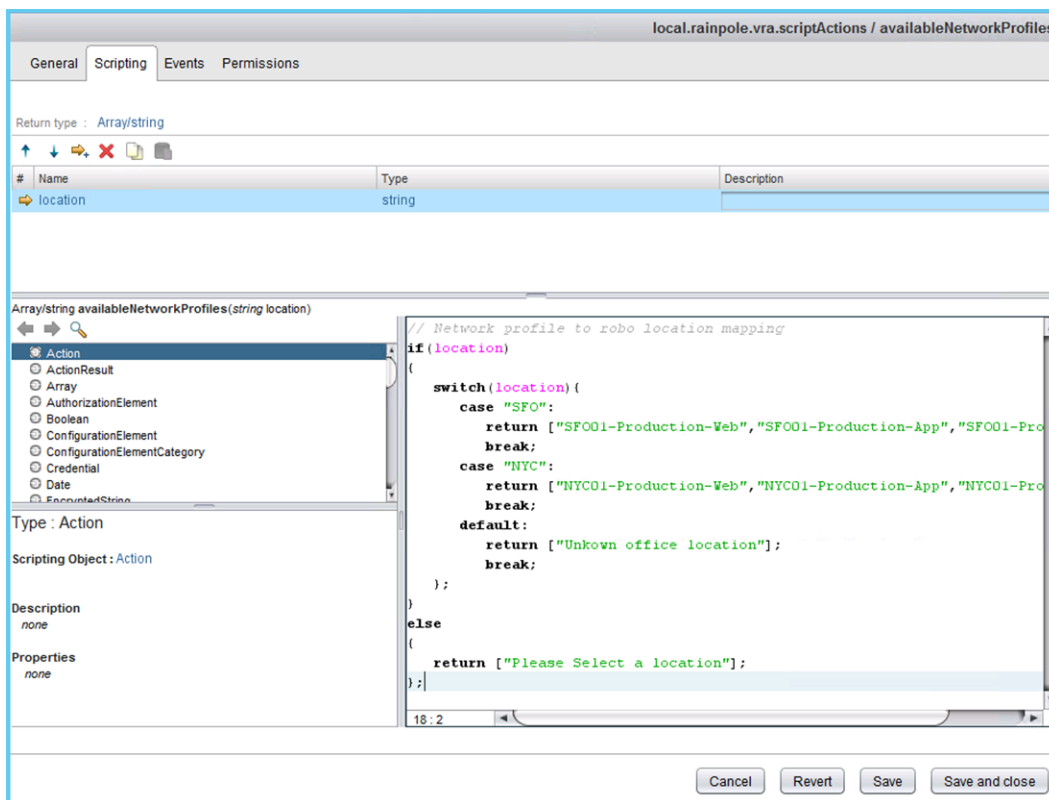


- 9 Click **Scripting** tab.
- 10 Click **void** on the right of **Return type**.
- 11 On the **Select a type** pop-up window, select **Array of** and enter **string** in the **Filter** text box.
- 12 Select **string** in the **Type** list.



- 13 Click **Accept** to save the return type.
- 14 Click the **Add parameter** icon to add a input parameter.
- 15 Click the default input parameter name **arg0**.
- 16 Enter location for the **Attribute Name** in the pop up **Choose attribute name** window and click **OK**.
- 17 Copy and paste the following code for this Action.

```
// Network profile to robo location mapping
if(location)
{
    switch(location){
        case "SF0":
            return ["SF001-Production-Web","SF001-Production-App","SF001-Production-DB"];
            break;
        case "NYC":
            return ["NYC01-Production-Web","NYC01-Production-App","NYC01-Production-DB"];
            break;
        default:
            return ["Unkown office location"];
            break;
    };
}
else
{
    return ["Please Select a location"];
};
```



18 Click **Save and close** to save the action.

19 Log out of the vRealize Orchestrator client.

Create a Property Definition using the vRealize Orchestrator Action in ROBO

Create a Custom Property Definition using the vRealize Orchestrator Action.

Procedure

- 1 Log in to the vRealize Automation Rainpole portal.
 - a Open a Web browser and go to **https://vra01svr01.rainpole.local/vcac/org/rainpole**.
 - b Log in using the following credentials.

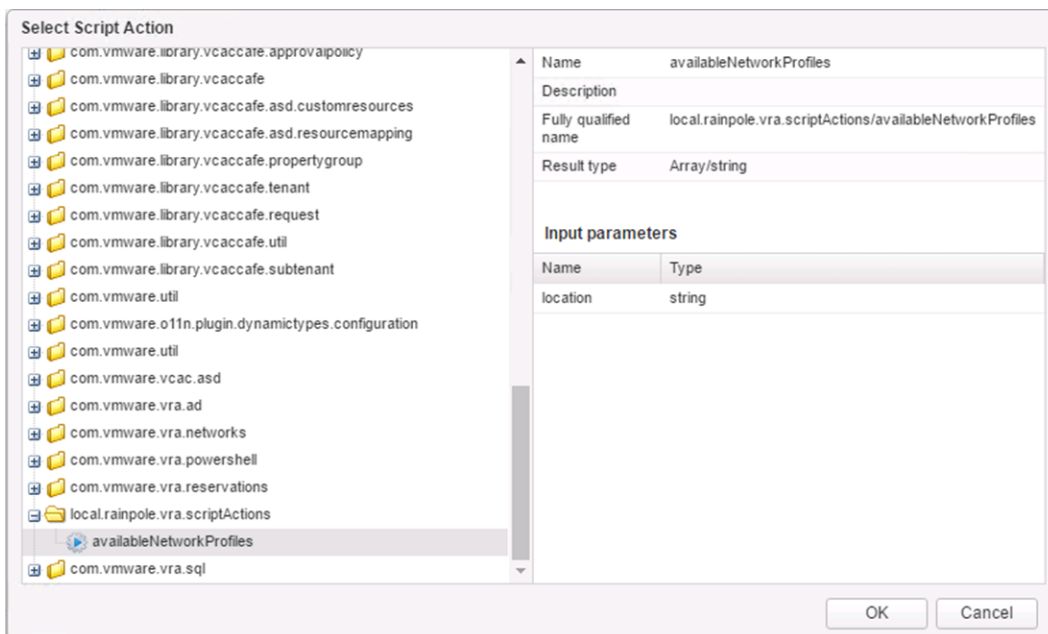
Setting	Value
User name	itac-tenantadmin
Password	itac-tenantadmin_password
Domain	rainpole.local

- 2 Select **Administration > Property Dictionary > Property Definitions**.
- 3 Click **New** to create a new property definition.

- 4 Enter **VirtualMachine.Network0.NetworkProfileName** in the **Name** text box.

Note The property definition name is case sensitive, and must match exactly the property name used in the blueprint or build profile.

- 5 Enter **Select a network** in the **Label** text box.
- 6 In the **Visibility** section, select the **All Tenants** radio button and specify to which tenant the property is available.
- 7 (Optional) Enter a property description in the **Description** text box.
Describe the intent of the property and any information that might help the consumer best use the property.
- 8 Enter 2 for **Display order**.
- 9 Select **String** from the **Data type** drop-down menu.
- 10 Select **Yes** from the **Required** drop-down menu.
- 11 Select **Dropdown** from the **Display As** drop-down menu.
- 12 Select **External values** for **Values**.
- 13 Click **Select** button for **Script action**.
- 14 In the pop up **Select Script Action** window, expand **local.rainpole.vra.scriptActions** and select **availableNetworkProfiles**. Click **OK**.



- 15 Select **location** in the **Input parameters** table and click **Edit** icon.

- 16 Check the checkbox for **Bind** and enter **Vrm.DataCenter.Location** for the **value**. Click **OK** to save the input parameter binding.

Create Property Definition

*** Name:** VirtualMachine.Network0.NetworkProfileName
To avoid conflict with vRealize Automation properties, use a prefix such as a company or feature name followed by a dot for all custom property names.

*** Label:** Which network to connect to

Visibility: ☒ All tenants ☐ This tenant

Description:

Display order: 2
You can control the order in which custom properties display on request forms. Set an order index of 1 to display this property at the top of the list.

*** Data type:** String

*** Required:** Yes

*** Display as:** Dropdown

*** Values:** ☐ Static list ☒ External values

Enable custom value entry: ☐

Script action: local.rainpole.vra.scriptActions... [Change...](#)

Input parameters: [Edit](#)

Name	Bind	Value
location	Yes	Vrm.DataCenter.Location

OK Cancel

- 17 Click **OK** to save the property definition.

The property is created and made available on the **Property Definitions** page.

Add a Property Group with Cross-ROBO deployment custom properties

Procedure

- 1 Log in to the vRealize Automation Rainpole portal.
 - a Open a Web browser and go to <https://vra01svr01.rainpole.local/vcac/org/rainpole>.
 - b Log in using the following credentials.

Setting	Value
User name	itac-tenantadmin
Password	itac-tenantadmin_password
Domain	rainpole.local

- 2 Select **Administration > Property Dictionary > Property Groups**. Click **New**.
- 3 Enter **Select Location for Deployment** in the **Name** text box.
- 4 If you enter the **Name** value first, the **ID** text box is populated with the same value.
- 5 In the **Visibility** section, select the **All Tenants** radio button to specify with which tenant the property is to be available.
- 6 (Optional) Enter a description of the property group.

- 7 Add property **Vrm.DataCenter.Location** to the group.
 - a Click **New** icon within the **Properties**.
 - b Select **Vrm.DataCenter.Location** as the property name.
 - c Deselect the **Encrypted** check box.
 - d Select the **Show in Request** check box.
 - e Click **OK** to add the property to the group.
- 8 Repeat this procedure to add the property **VirtualMachine.Network0.NetworkProfileName** to the group.
- 9 Click **OK** to save the property group.

Create a Reservation Policy for the Unified Blueprint in ROBO

When tenant administrators and business group managers create a new blueprint, the option to add a reservation policy becomes available. To add a reservation policy to an existing blueprint, edit the blueprint.

Procedure

- 1 Log in to the vRealize Automation Rainpole portal.
 - a Open a Web browser and go to **<https://vra01svr01.rainpole.local/vcac/org/rainpole>**.
 - b Log in using the following credentials.

Setting	Value
User name	itac-tenantadmin
Password	<i>itac-tenantadmin_password</i>
Domain	rainpole.local

- 2 Navigate to **Infrastructure > Reservations > Reservation Policies**.
 - a Click **New**.
 - b Type **UnifiedBlueprint-Policy** in the **Name** text box.
 - c Select **Reservation Policy** from the **Type** drop-down list.
 - d Type **Reservation policy for Unified Blueprint** in the **Description** text box.
 - e Click **OK**.

Specify Reservation Information for the Unified Blueprint in ROBO

Each reservation is configured for a specific business group to grant them access to request specific physical machines.

Before members of a business group can request machines, fabric administrators must allocate resources for them by creating a reservation. Each reservation is configured for a specific business group, and grants access to request machines on a specified compute resource.

Repeat this procedure twice to create reservations on both of the Region A Compute vCenter Cluster and ROBO Consolidated Cluster for the Production and Development business groups.

Region	Business Group	Reservation Name	Reservation Policy	Compute Resource	Resource Pool
Hub	Production	SFO01-Comp01-Prod-UnifiedBlueprint	UnifiedBlueprint-Policy	SFO01-Comp01(comp01vc01.sfo01.rainpole.local)	User-VMRP01
	Development	SFO01-Comp01-Dev-UnifiedBlueprint	UnifiedBlueprint-Policy	SFO01-Comp01(comp01vc01.sfo01.rainpole.local)	User-VMRP01
NYC	Production	NYC01-Prod-UnifiedBlueprint	UnifiedBlueprint-Policy	NYC01(nyc01vc01.rainpole.local)	User-VM
	Development	NYC01-Dev-UnifiedBlueprint	UnifiedBlueprint-Policy	NYC01(nyc01vc01.rainpole.local)	User-VM

Procedure

- 1 Log in to the vRealize Automation Rainpole portal.
 - a Open a Web browser and go to **`https://vra01svr01.rainpole.local/vcac/org/rainpole`**.
 - b Log in using the following credentials.

Setting	Value
User name	itac-tenantadmin
Password	<i>itac-tenantadmin_password</i>
Domain	rainpole.local

- 2 Navigate to **Infrastructure > Reservations > Reservations** and click **New > vSphere (vCenter)**.
- 3 On the **New Reservation - vSphere (vCenter)** page, click the **General** tab, and configure the following values.

Setting	Production Business Group Value	Development Business Group Value
Name	NYC01-Prod-UnifiedBlueprint	NYC01-Dev-UnifiedBlueprint
Tenant	rainpole	rainpole
Business Group	Production	Development
Reservation Policy	UnifiedBlueprint-Policy	UnifiedBlueprint-Policy

Setting	Production Business Group Value	Development Business Group Value
Priority	100	100
Enable This Reservation	Selected	Selected

- 4 On the **New Reservation - vSphere** page, click the **Resources** tab.
 - a Select **NYC01(nyc01vc01.rainpole.local)** from the **Compute Resource** drop-down menu.
 - b Enter **200** in the **This Reservation** column of the **Memory (GB)** table.
 - c In the **Storage (GB)** table, select the check box for datastore **NYC01-VSAN01** and enter **2000** in the **This Reservation Reserved** text box, enter **1** in the **Priority** text box, and click **OK**.
 - d Select **User-VM** from the **Resource Pool** drop-down menu.
- 5 On the **New Reservation - vSphere (vCenter)** page, click the **Network** tab.
- 6 On the **Network** tab, select the network path check boxes listed in the table below from the **Network Paths** list, and select the corresponding network profile from the **Network Profile** drop-down menu for the business group whose reservation you are configuring.

Production Business Group

Production Network Path	Production Group Network Profile
vxw-dvs-xxxxx-Production-Web-VXLAN	NYC01-Production-Web
vxw-dvs-xxxxx-Production-DB-VXLAN	NYC01-Production-DB
vxw-dvs-xxxxx-Production-App-VXLAN	NYC01-Production-App

Development Business Group

Development Network Path	Development Group Network Profile
vxw-dvs-xxxxx-Development-Web-VXLAN	NYC01-Development-Web
vxw-dvs-xxxxx-Development-DB-VXLAN	NYC01-Development-DB
vxw-dvs-xxxxx-Development-App-VXLAN	NYC01-Development-App

- 7 Click **OK** to save the reservation.
- 8 Repeat this procedure to create reservations on both Hub and NYC for both Production and Development Business Groups.

Create a Service Catalog for the Unified Blueprint in ROBO

The service catalog provides a common interface for consumers of IT services to request and manage the services and resources they need. Users can browse the catalog to request services, track their requests, and manage their provisioned service items.

After the service catalog is created, business group managers can create entitlements for services, catalog items, and resource actions to groups of users. The entitlement allows members of a particular business group, for example, the Production business group, to use the blueprint. Without an entitlement, users cannot use the blueprint.

Procedure

- 1 Log in to the vRealize Automation Rainpole portal.
 - a Open a Web browser and go to **https://vra01svr01.rainpole.local/vcac/org/rainpole**.
 - b Log in using the following credentials.

Setting	Value
User name	itac-tenantadmin
Password	<i>itac-tenantadmin_password</i>
Domain	rainpole.local

- 2 Click the **Administration** tab, and select **Catalog Management > Services**.
- 3 Click **New**.
 - a In the **New Service** dialog box type **Unified Single Machine Catalog** in the **Name** text box.
 - b Select **Active** from the **Status** drop-down menu.
 - c Click **OK**.

Create an Entitlement for the Unified Blueprint Catalog in ROBO

Entitle all blueprints in the Unified Blueprint Catalog to the Production and Development business groups. Entitlements determine which users and groups can request specific catalog items or perform specific actions. Entitlements are specific to a business group, and allow users in different business groups to access the blueprint catalog.

Perform this procedure twice, first to associate the Unified Blueprint Catalog with the Prod-SingleVM-Entitlement entitlement, and then once again to associate the Unified Blueprint Catalog with the Dev-SingleVM-Entitlement entitlement.

Procedure

- 1 Log in to the vRealize Automation Rainpole portal.
 - a Open a Web browser and go to **https://vra01svr01.rainpole.local/vcac/org/rainpole**.
 - b Log in using the following credentials.

Setting	Value
User name	itac-tenantadmin
Password	<i>itac-tenantadmin_password</i>
Domain	rainpole.local

- 2 Associate the **Unified Blueprint Catalog** with the **Prod-SingleVM-Entitlement** entitlement that you created earlier.

- a Select **Administration > Catalog Management > Entitlements**.
- b Click **Prod-SingleVM-Entitlement**.

The **Edit Entitlement** pane appears.

- c Select the **Items & Approvals** tab.
- d Navigate to **Entitled Services** and click the **Add** icon.
- e Check the box next to **Unified Single Machine Catalog** and click **OK**.
- f Click **Finish** to save your changes.

Create Unified Single Machine Blueprints in ROBO

A blueprint is the complete specification for a virtual, cloud, or physical machine. Blueprints determine a machine's attributes, the manner in which it is provisioned, and its policy and management settings. Create three blueprints from which to clone the virtual machine for your environment using pre-configured resources on the vCenter Server compute cluster in Region A and the consolidated cluster in ROBO. Tenants use these blueprints to automatically provision virtual machines.

Repeat this procedure to create three Unified Single Machine blueprints, one for each blueprint name listed in the following table.

Blueprint Name	VM Template	Reservation Policy	Service Catalog
Windows Server 2012 R2 - Unified	windows-2012r2-64 (nyc01vc01.rainpole.local)	UnifiedBlueprint-Policy	Unified Single Machine Catalog
Windows Server 2012 R2 With SQL2012 - Unified	windows-2012r2-64-sql2012(nyc01vc01.rainpole.local)	UnifiedBlueprint-Policy	Unified Single Machine Catalog
Redhat Enterprise Linux 6 - Unified	redhat6-enterprise-64(nyc01vc01.rainpole.local)	UnifiedBlueprint-Policy	Unified Single Machine Catalog

Procedure

- 1 Log in to the vRealize Automation Rainpole portal.
 - a Open a Web browser and go to **<https://vra01svr01.rainpole.local/vcac/org/rainpole>**.
 - b Log in using the following credentials.

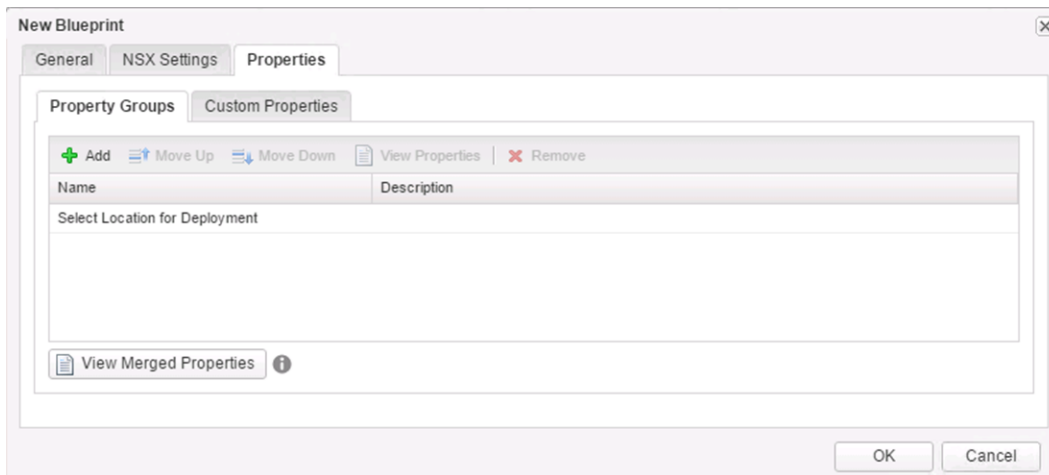
Setting	Value
User name	itac-tenantadmin
Password	<i>itac-tenantadmin_password</i>
Domain	rainpole.local

- 2 Navigate to **Design > Blueprints**.
- 3 Click **New**.

- 4 In the **New Blueprint** dialog box, configure the following settings on the **General** tab.

Setting	Value
Name	Windows Server 2012 R2 - Unified
Archive (days)	15
Deployment limit	Default setting (blank)
Minimum	30
Maximum	270

- 5 Click the **Properties** tab.
- Click **Add** on the **Property Groups** tab.
 - Select the property group **Select Location for Deployment** and click **OK**.



- 6 Click **OK**.
- 7 Select and drag the **vSphere Machine** icon to the Design Canvas.
- 8 Click the **General** tab, configure the following settings, and click **Save**.

Setting	Value
ID	vSphere_Machine_1
Reservation Policy	UnifiedBlueprint-Policy
Machine Prefix	Use group default
Minimum	Default setting
Maximum	Default setting

- 9 Click the **Build Information** tab, configure the following settings, and click **Save**.

Setting	Value
Blueprint Type	Server
Action	Clone

Setting	Value
Provisioning Workflow	CloneWorkflow
Clone from	windows-2012r2-64
Customization spec	itac-windows-joindomain-custom-spec

- 10 Click the **Machine Resources** tab, configure the following settings, and click **Save**.

Setting	Minimum	Maximum
CPU	1	4
Memory (MB):	4096	16384
Storage	50	60

- 11 Select the blueprint **Windows Server 2012 R2 - Unified** and click **Publish**.
- 12 Navigate to **Administration > Catalog Management > Catalog Items** and add the blueprint to the **Unified Single Machine Catalog**.
- In the **Catalog Items** list, click the blueprint labelled **Windows Server 2012 R2 - Unified**.
 - In the **Configure Catalog Items** dialog box, set **Service** to **Unified Single Machine Catalog**, and click **OK**.

Test the Cross-ROBO Deployment of the Unified Single Machine Blueprints

The data center environment is now ready for the multi-site deployment of virtual machines using vRealize Automation. Test your environment and confirm the successful provisioning of virtual machines using the blueprints you created to both Region A and ROBO.

Repeat this procedure twice to provision virtual machines in both the Region A and ROBO vCenter servers.

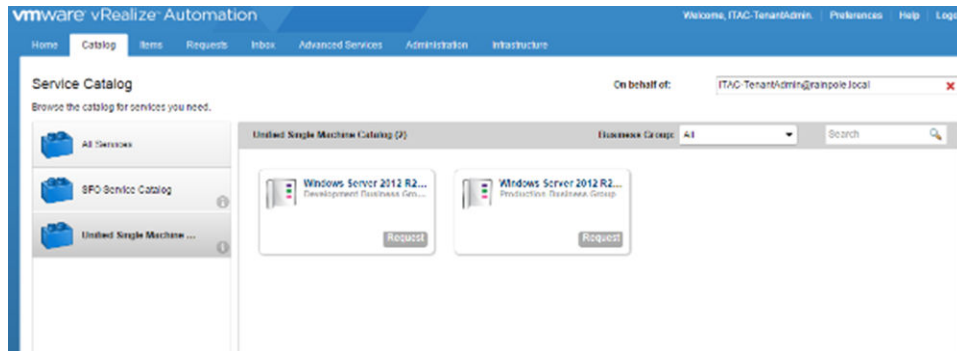
Region/ROBO	Compute vCenter Server
San Francisco	comp01vc01.sfo01.rainpole.local
New York City	nyc01vc01.rainpole.local

Procedure

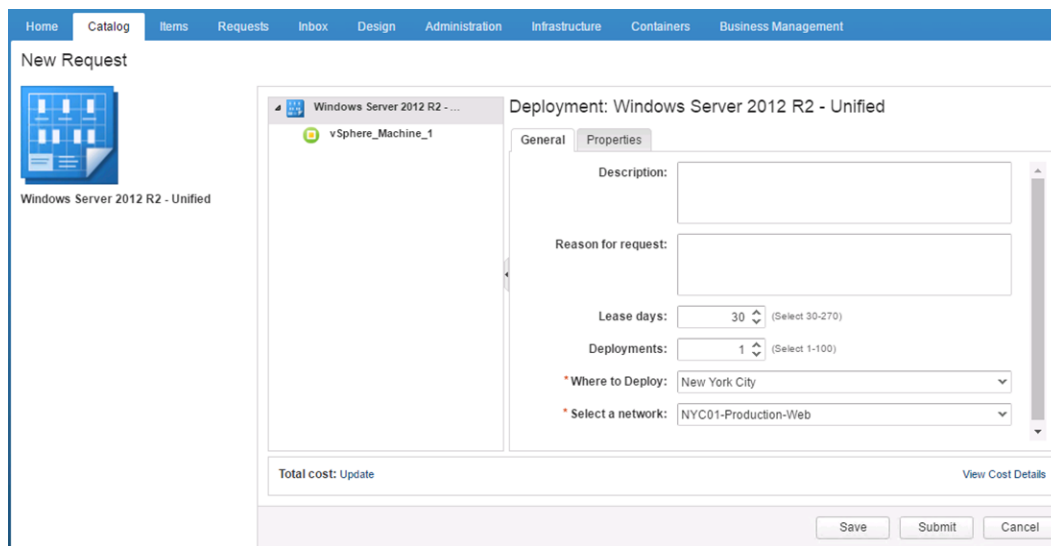
- Log in to the vRealize Automation Rainpole portal.
 - Open a Web browser and go to **https://vra01svr01.rainpole.local/vcac/org/rainpole**.
 - Log in using the following credentials.

Setting	Value
User name	itac-tenantadmin
Password	itac-tenantadmin_password
Domain	rainpole.local

- 2 Select the **Catalog** tab, and click **Unified Single Machine Catalog** from the catalog of available services.



- 3 Click the **Request** button for the **Windows Server 2012 R2 - Unified** blueprint.
The **New Request** window appears.
- 4 Select **New York City** for the **Where to Deploy** and **NYC01-Production-Web** for **Select a network**, and click **Submit**.



- 5 Verify the request finishes successfully.
 - a Select the **Requests** tab.
 - b Select the request you submitted and wait several minutes for the request to complete.
Click the **Refresh** icon every few minutes until a **Successful** message appears under **Status**.
 - c Click **View Details**.
 - d Under **Status Details**, verify that the virtual machine successfully provisioned.

- 6 Verify the virtual machine is provisioned in the ROBO consolidated cluster.
 - a Open a Web browser and go to **https://nyc01vc01.rainpole.local/vsphere-client**.
 - b Log in as the vCenter Server administrator using the following credentials.

Setting	Value
User name	administrator@vsphere.local
Password	vcenter_admin_password

- c Select **Home > VMs and Templates**.
 - d In the **Navigator** panel, expand the vCenter Server compute cluster **nyc01vc01.rainpole.local > NYC01 > VRM**, and verify the existence of the virtual machine.
 - e Right click that virtual machine and select **Edit settings**, verify the network adapter is connected to logical switch vxw-dvs-xxxxx-Production-Web-VXLAN.
- 7 Repeat this procedure for the hub.
 - a Provision virtual machines to the Hub Compute cluster.
 - b Verify the request finishes successfully and that the virtual machine is provisioned in the Hub Compute cluster.

You have successfully performed a cross-ROBO deployment of vRealize Automation single machine blueprints, provisioning virtual machines in both hub and ROBO.

Operations Implementation in ROBO

4

You deploy products for monitoring remote office and branch office (ROBO) locations, such as vRealize Operations Manager, vRealize Log Insight and vSphere Update Manager Download Service, on top of your vSphere infrastructure and NSX networking deployment for ROBO. You connect them to the SDDC management products in the ROBO location to collect local data and send it to the monitoring nodes in the SDDC hub.

This section includes the following topics:

- [vRealize Operations Manager Implementation in ROBO](#)
- [vRealize Log Insight Implementation in ROBO](#)
- [vSphere Update Manager Download Service Implementation in ROBO](#)

vRealize Operations Manager Implementation in ROBO

Deploy a pair of vRealize Operations Manager remote collectors in a ROBO, and connect them back to the analytics cluster that resides in the hub for consolidated data analysis.

Procedure

1 [Deploy vRealize Operations Manager in ROBO](#)

In a ROBO, deploy two remote collector nodes for vRealize Operations Manager to monitor the ROBO vCenter Server instance, NSX for vSphere and storage components in SDDC.

2 [Configure User Access in vSphere for Integration with vRealize Operations Manager in ROBO](#)

Configure operations services accounts with permissions that are required to enable vRealize Operations Manager access to monitoring data on the ROBO vCenter Server.

3 [Add vCenter Adapter Instances to vRealize Operations Manager for ROBO](#)

After you deploy the remote collector nodes of vRealize Operations Manager in the ROBO, add a vCenter Adapter instance for the ROBO vCenter Server instance.

4 [Connect vRealize Operations Manager to the NSX Manager in ROBO](#)

Configure the vRealize Operations Management Pack for NSX for vSphere to monitor the NSX networking services deployed in the vSphere cluster in the ROBO and view the vSphere hosts in the NSX transport zones. You can also access end-to-end logical network topologies between any two virtual machines or NSX objects for better visibility into logical connectivity. Physical host and network device relationship in this view also helps in isolating problems in the logical or physical network.

5 [Configure Service Account Privileges for Integration between vRealize Operations Manager and vRealize Automation in ROBO](#)

Configure the rights of the service accounts that vRealize Automation and vRealize Operations Manager use to communicate with each other.

6 [Add Storage Devices Adapters in vRealize Operations Manager for ROBO](#)

Configure a Storage Devices adapter for each ROBO location to collect monitoring data about the storage devices in the remote sites.

Deploy vRealize Operations Manager in ROBO

In a ROBO, deploy two remote collector nodes for vRealize Operations Manager to monitor the ROBO vCenter Server instance, NSX for vSphere and storage components in SDDC.

Deploying a separate group of remote collectors in ROBO makes the data collection in each remote location independent from the location of the analytics cluster.

Procedure

1 [Prerequisites for Deploying the Remote Collectors in ROBO](#)

Before you deploy the remote collector nodes of vRealize Operations Manager in ROBO, verify that your environment satisfies the requirements for this deployment.

2 [Deploy the Remote Collector Virtual Appliances in ROBO](#)

Use the vSphere Web Client to deploy the two virtual appliances for the remote collectors in the ROBO. The remote collectors are used to forward data from the vCenter Server instance in the ROBO to the analytics cluster of vRealize Operations Manager in the hub.

3 [Connect the Remote Collector Nodes to the Analytics Cluster in ROBO](#)

After you deploy the virtual appliances for the remote collector nodes on the ROBO vCenter Server, configure the settings of the remote collectors and connect them to the analytics cluster located in the hub.

4 [Configure a DRS Anti-Affinity Rule for vRealize Operations Manager Remote Collectors in ROBO](#)

To protect the vRealize Operations Manager virtual machines from a host-level failure, configure vSphere DRS to run the remote collector virtual machines on different hosts within the ROBO cluster.

5 Group Remote Collector Nodes in ROBO

After you configure the remote collector nodes for vRealize Operations Manager in ROBO, join the remote collectors in a group for adapter resiliency in the cases where the collector experiences network interruption or becomes unavailable.

Prerequisites for Deploying the Remote Collectors in ROBO

Before you deploy the remote collector nodes of vRealize Operations Manager in ROBO, verify that your environment satisfies the requirements for this deployment.

IP Addresses and Host Names

Verify that static IP addresses and FQDNs for the vRealize Operations Manager application virtual network are available for the ROBO site of the SDDC deployment. Allocate static IP addresses and host names for the 2 remote collector nodes.

Table 4-1. IP Addresses and Host Names for the Remote Collector Nodes in ROBO

Role	IP Address	FQDN
Remote collector 1	172.18.19.31	nyc01rmtcol01.rainpole.local
Remote collector 2	172.18.19.32	nyc01rmtcol02.rainpole.local
Default gateway	172.18.19.1	-
DNS server	172.18.11.4	-
Subnet mask	255.255.255.0	-

Deployment Prerequisites

Verify that your environment satisfies the following prerequisites to deployment vRealize Operations Manager remote collector nodes in ROBO.

Prerequisite	Value
Storage	<ul style="list-style-type: none"> ■ Virtual disk provisioning. <ul style="list-style-type: none"> ■ Thin ■ Required storage per node <ul style="list-style-type: none"> ■ Initial storage for node deployment: 1.6 GB
Software Features	<ul style="list-style-type: none"> ■ vSphere <ul style="list-style-type: none"> ■ ROBO vCenter Server ■ ROBO cluster with enabled DRS and HA ■ NSX for vSphere <ul style="list-style-type: none"> ■ Application virtual network for the 2-node remote collector cluster in ROBO ■ vRealize Operations Manager <ul style="list-style-type: none"> ■ 3-node analytics cluster in Region A ■ 2-node remote collector cluster in Region A ■ 2-node remote collector cluster in Region B
Installation Package	Download the .ova file of the vRealize Operations Manager virtual appliance on the machine where you use the vSphere Web Client.

Deploy the Remote Collector Virtual Appliances in ROBO

Use the vSphere Web Client to deploy the two virtual appliances for the remote collectors in the ROBO. The remote collectors are used to forward data from the vCenter Server instance in the ROBO to the analytics cluster of vRealize Operations Manager in the hub.

Procedure

- 1 Log in to vCenter Server by using the vSphere Web Client.
 - a Open a Web browser and go to **https://nyc01vc01.rainpole.local/vsphere-client**.
 - b Log in using the following credentials.

Setting	Value
User name	administrator@vsphere.local
Password	vsphere_admin_password

- 2 Navigate to the nyc01vc01.rainpole.local vCenter Server object.
- 3 Right-click the **nyc01vc01.rainpole.local** object and select **Deploy OVF Template**.
- 4 On the **Select template** page, select **Local file**, browse to the location of the vRealize Operations Manager OVA file on your file system, and click **Next**.
- 5 On the **Select name and location** page, enter a node name, select the inventory folder for the virtual appliance, and click **Next**.

Setting	Value
Names	<ul style="list-style-type: none"> ■ nyc01rmtcol01 for remote collector 1 ■ nyc01rmtcol02 for remote collector 2
vCenter Server	nyc01vc01.rainpole.local
Data center	NYC01
Folder	vROps01RC

- 6 On the **Select a resource** page, select the resource pool **NYC01-MGMT**, and click **Next**.

Setting	Value
Datacenter	NYC01
Resource Pool	NYC01-MGMT

- 7 On the **Review details** page, examine the virtual appliance details, such as product, version, download and disk size, and click **Next**.
- 8 On the **Accept license agreements** page, accept the end user license agreements and click **Next**.
- 9 On the **Select configuration** page, from the **Configuration** drop-down menu, select **Remote Collector (Standard)** deployment configuration of the virtual appliance, and click **Next**.

- 10 On the **Select storage** page, select the datastore indicated in the table below, and click **Next**.

Setting	Value
Select virtual disk format	Thin provision
VM Storage Policy	Virtual SAN Default Storage Policy
Datastore table	NYC01-VSAN01

- 11 On the **Setup networks** page, select the distributed port group on the vDS-NYC01 distributed switch that ends with Mgmt–NYC01–VXLAN and click **Next**.

- 12 On the **Customize template** page, set the IPv4 settings and select the time zone for the virtual appliance and click **Next**.

- a In the **Networking Properties** section, configure the following IPv4 settings.

Setting	Value
DNS server	172.18.11.4
Default gateway	172.18.19.1
Static IPv4 address	<ul style="list-style-type: none"> ■ 172.18.19.31 for remote collector 1 ■ 172.18.19.32 for remote collector 2
Subnet mask	255.255.255.0

- b From the **Timezone setting** drop-down menu, select the **Etc/UTC** time zone.

- 13 On the **Ready to complete** page, verify that the settings for deployment are correct and click **Finish**.

- 14 After the virtual appliance is deployed, right-click the virtual appliance object and select **Power > Power On**.

- 15 Change the default empty password for the root user.

- a In the vSphere Web Client, right-click the remote collector virtual appliance and select **Open Console** to open the remote console to the appliance.

Name	Role
nyc01rmtcol01	Remote collector 1
nyc01rmtcol02	Remote collector 2

- b Press ALT+F1 to switch to the command prompt.

- c At the command prompt, log in as the **root** user using empty password.

- d At the command prompt, change the default empty password for the root user account with a new *vrops_root_password* password.

- e Close the virtual appliance console.

- 16 Repeat the steps to deploy the second remote collector appliance.

Connect the Remote Collector Nodes to the Analytics Cluster in ROBO

After you deploy the virtual appliances for the remote collector nodes on the ROBO vCenter Server, configure the settings of the remote collectors and connect them to the analytics cluster located in the hub.

Procedure

- 1 Open a Web browser, and go to the initial setup user interface of each remote collector node virtual appliance.

Remote Collector Node	URL for Setup Interface
Remote collector 1	https://nyc01rmtcol01.rainpole.local
Remote collector 2	https://nyc01rmtcol02.rainpole.local

- 2 On the initial setup page, click **Expand an Existing Installation**.
- 3 On the **Getting Started** page, review the steps for creating a cluster, and click **Next**.
- 4 On the **Node Settings and Cluster Info** page, configure the settings of the node in the analytics cluster.

The screenshot shows the 'vRealize Operations Manager Initial Setup' window. On the left, a progress bar indicates four steps: 1. Getting Started (completed), 2. Node Settings and Cluster Info (current step), 3. Username and Password, and 4. Ready to Complete. The main content area is titled 'Enter node settings and cluster information' and includes instructions: 'Enter a name for this node and select a node type. Then enter credentials for the cluster to join this node to.'

Node Settings

Node name:

Node type:

Cluster Information

To join this node to a cluster, enter the IP address or fully qualified domain name of the cluster master node.

Master node IP address or FQDN:

The following certificate was found on the cluster:

Thumbprint:
D7:BD:D4:0E:2C:B0:56:58:DE:25:49:E0:E3:77:D4:A9:1F:AB:C5:68
Issuer Distinguished Name: CN=rainpole-DC01RPL-CA,DC=rainpole,DC=local
Subject Distinguished Name: CN=vrops-cluster-01.rainpole.local,OU=Rainpole,OU=Rainpole Inc.,L=SFO,ST=CA,C=US
Subject Alternate Name: vrops-cluster-01,vrops-mstrn-01,vrops-repln-02,vrops-datan-03,vrops-datan-04,vrops-cluster-01.rainpole.local,vrops-mstrn-01.rainpole.local,vrops-repln-02.rainpole.local,vrops-datan-03.rainpole.local,vrops-datan-04.rainpole.local,192.168.11.35

☒ Accept this certificate

At the bottom, there are four buttons: Back, Next, Finish, and Cancel.

- a Configure the name, type and master address of the node.

Setting	Value
Node name	■ nyc01rmtcol01 for remote collector 1
	■ nyc01rmtcol02 for remote collector 2
Node type	Remote Collector
Master node IP address or FQDN	vrops-mstrn-01.rainpole.local

- b Click **Validate** next to the **Master node IP address or FQDN** text box.

The certificate of the master node appears in the text box.

- c Validate that the master certificate is correct, and click **Accept this certificate**.

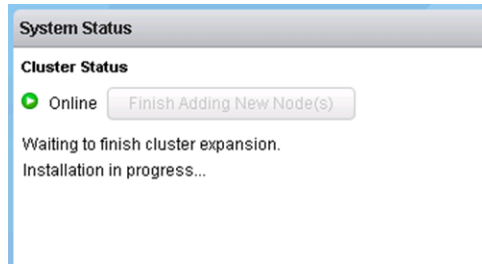
- d Click **Next**.

- 5 On the **Username and Password** page, select **Use cluster administrator user name and password**, enter the *vrops_admin_password* password for the admin user, and click **Next**.

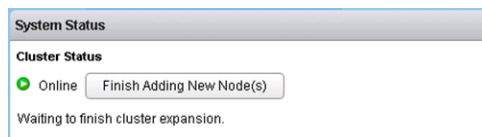
- 6 On the **Ready to Complete** page, click **Finish**.

Wait for the node to finish installation operation.

The **System Status** page of vRealize Operations Manager appears. The cluster admin interface displays that the configuration of the node is in progress.



- 7 Repeat the steps to configure the second remote collector node.
- 8 After the operation is complete, in the administration UI of vRealize Operations Manager, click **Finish Adding New Node(s)** next to **Cluster Status**.

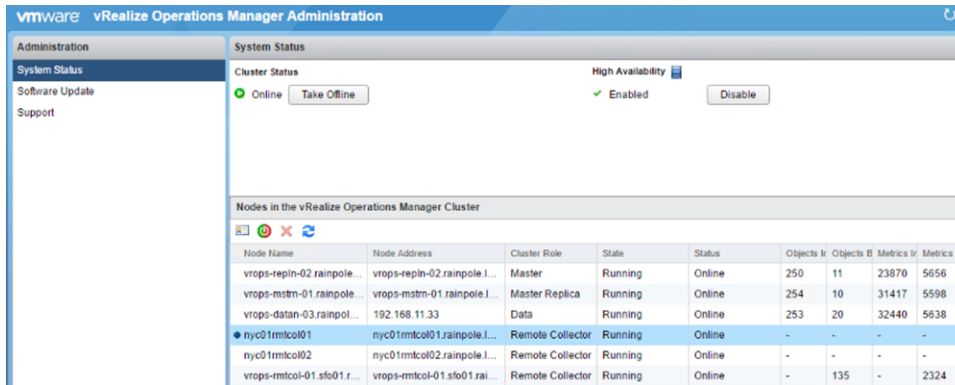


- 9 In the **Finish Adding New Node(s)** dialog box, click **OK** to confirm adding the nodes.

After the configuration of the remote collectors in the ROBO is complete, the cluster on the **System Status** page of the administration user interface consists of the following nodes:

- vrops-mstrn-01

- vrops-repln-02
- vrops-datan-03
- Two remote collectors for Region A vrops-rmtcol-01 and vrops-rmtcol-02
- Two remote collectors for Region B vrops-rmtcol-51 and vrops-rmtcol-52
- Two remote collectors for the ROBO site nyc01rmtcol01 and nyc01rmtcol02



Configure a DRS Anti-Affinity Rule for vRealize Operations Manager Remote Collectors in ROBO

To protect the vRealize Operations Manager virtual machines from a host-level failure, configure vSphere DRS to run the remote collector virtual machines on different hosts within the ROBO cluster.

Procedure

- 1 Log in to vCenter Server by using the vSphere Web Client.
 - a Open a Web browser and go to **<https://nyc01vc01.rainpole.local/vsphere-client>**.
 - b Log in using the following credentials.

Setting	Value
User name	administrator@vsphere.local
Password	vsphere_admin_password

- 2 Navigate to the **nyc01vc01.rainpole.local** vCenter Server object, and under the **NYC01** data center object select the **NYC01** cluster.
- 3 Click the **Configure** tab.
- 4 Under the **Configuration** group of settings, select **VM/Host Rules**.
- 5 On the **VM/Host Rules** page, click the **Add** button above the rules list.

- 6 In the **Create VM/Host Rule** dialog box, add a new anti-affinity rule for the virtual machines of the two remote collectors using the following values, and click **OK**.

Setting	Value
Name	anti-affinity-rule-vropsr
Enable rule	Selected
Type	Separate Virtual Machines
Members	<ul style="list-style-type: none"> ■ nyc01rmtcol01 ■ nyc01rmtcol02

Group Remote Collector Nodes in ROBO

After you configure the remote collector nodes for vRealize Operations Manager in ROBO, join the remote collectors in a group for adapter resiliency in the cases where the collector experiences network interruption or becomes unavailable.

Procedure

- 1 Log in to vRealize Operations Manager by using the administration console.
 - a Open a Web browser and go to **https://vrops-cluster-01.rainpole.local**.
 - b Log in using the following credentials.

Setting	Value
User name	admin
Password	<i>vrops_admin_password</i>

- 2 On the **Home** page, click **Administration > Collector Groups**.
- 3 Click the **Add** icon.
- 4 In the **Add New Collector Group** dialog box, configure the following settings, and click **Save**.

Setting	Value
Name	NYC01
Description	Remote collector group for NYC ROBO
nyc01rmtcol01	Selected
nyc01rmtcol02	Selected

Add New Collector Group

Name:

Description:

Members
Check or uncheck collectors to include or exclude them from the collector group.

	Collector Name	IP Address	Collector Group Name	Status
<input checked="" type="checkbox"/>	vRealize Operations Manager Collector-nyc01rmtcol01	172.18.19.31		✓ Online
<input checked="" type="checkbox"/>	vRealize Operations Manager Collector-nyc01rmtcol02	172.18.19.32		✓ Online
<input type="checkbox"/>	vRealize Operations Manager Collector-vrops-rmtcol-01.sf...	192.168.31.31	SFO01	✓ Online
<input type="checkbox"/>	vRealize Operations Manager Collector-vrops-rmtcol-02.sf...	192.168.31.32	SFO01	✓ Online

The **NYC01** collector group appears on the **Collector Groups** page under the **Administration** view of the user interface.

Collector Groups

Collector Group Name	Description
Default collector group (Default)	
NYC01	Remote collector group for NYC ROBO
SFO01	Remote collector group for Region A

NYC01

Members (2)
The following remote collectors are part of this collector group. Click Edit to add or remove collectors from this group.

Name	IP Address	Status	Number of Objects
vRealize Operations Manager Collector-nyc01rmtc...	172.18.19.31	✓	10
vRealize Operations Manager Collector-nyc01rmtc...	172.18.19.32	✓	10

Configure User Access in vSphere for Integration with vRealize Operations Manager in ROBO

Configure operations services accounts with permissions that are required to enable vRealize Operations Manager access to monitoring data on the ROBO vCenter Server.

You associate the `svc-xxx-vrops` services accounts in the Active Directory with user roles that have certain privileges and you assign the users to the vCenter Server ROBO instance.

Procedure

- 1 [Define a User Role in vSphere for Storage Devices Adapters in vRealize Operations Manager for ROBO](#)

On the ROBO vCenter Server, create a user role with privileges that are required for collecting data about storage devices in vRealize Operations Manager.

2 Configure User Privileges in vSphere for Integration with vRealize Operations Manager for ROBO

Assign global permissions in the ROBO to the operations service accounts svc-vrops and svc-mpsd-vrops to access monitoring data from the ROBO vCenter Server in vRealize Operations Manager.

Define a User Role in vSphere for Storage Devices Adapters in vRealize Operations Manager for ROBO

On the ROBO vCenter Server, create a user role with privileges that are required for collecting data about storage devices in vRealize Operations Manager.

Procedure

- 1 Log in to vCenter Server by using the vSphere Web Client.
 - a Open a Web browser and go to **https://nyc01vc01.rainpole.local/vsphere-client**.
 - b Log in using the following credentials.

Setting	Value
User name	administrator@vsphere.local
Password	vsphere_admin_password

- 2 On the **Home** page of the vSphere Web Client, click **Roles** under **Administration**.
- 3 Create a new role for collecting storage device data.
 - a On the **Roles** page, click the **Create role action** icon.
 - b In the **Create Role** dialog box, configure the role using the following configuration settings, and click **OK**.

Setting	Value
Role name	MPSD Metrics User
Privilege	<ul style="list-style-type: none"> ■ Host.CIM.CIM interaction ■ Host.Configuration.Storage partition configuration ■ Profile-driven storage.Profile-driven storage view ■ Storage views.View

This role inherits the **System.Anonymous**, **System.View**, and **System.Read** permissions.

Configure User Privileges in vSphere for Integration with vRealize Operations Manager for ROBO

Assign global permissions in the ROBO to the operations service accounts svc-vrops and svc-mpsd-vrops to access monitoring data from the ROBO vCenter Server in vRealize Operations Manager.

The svc-vrops user has read-only access on all objects in vCenter Server. The svc-mpsd-vrops user has rights that are specifically required for access to storage device information in vRealize Operations Manager on all objects in vCenter Server.

Prerequisites

- Verify that the ROBO vCenter Server is connected to the Active Directory domain.
- Verify that the users and groups from the rainpole.local domain are available in the ROBO vCenter Server.

Procedure

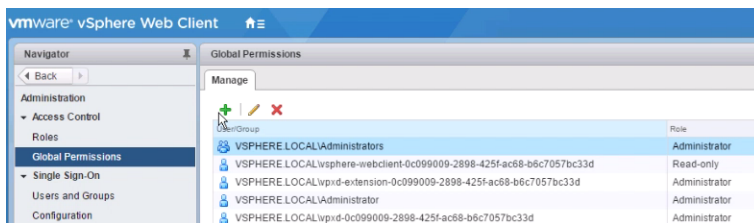
- 1 Log in to vCenter Server by using the vSphere Web Client.
 - a Open a Web browser and go to **https://nyc01vc01.rainpole.local/vsphere-client**.
 - b Log in using the following credentials.

Setting	Value
User name	administrator@vsphere.local
Password	vsphere_admin_password

- 2 From the **Home** menu, select **Administration**.
- 3 Assign global permissions to the svc-vrops@rainpole.local and svc-mpsd-vrops@rainpole.local users according to their roles.

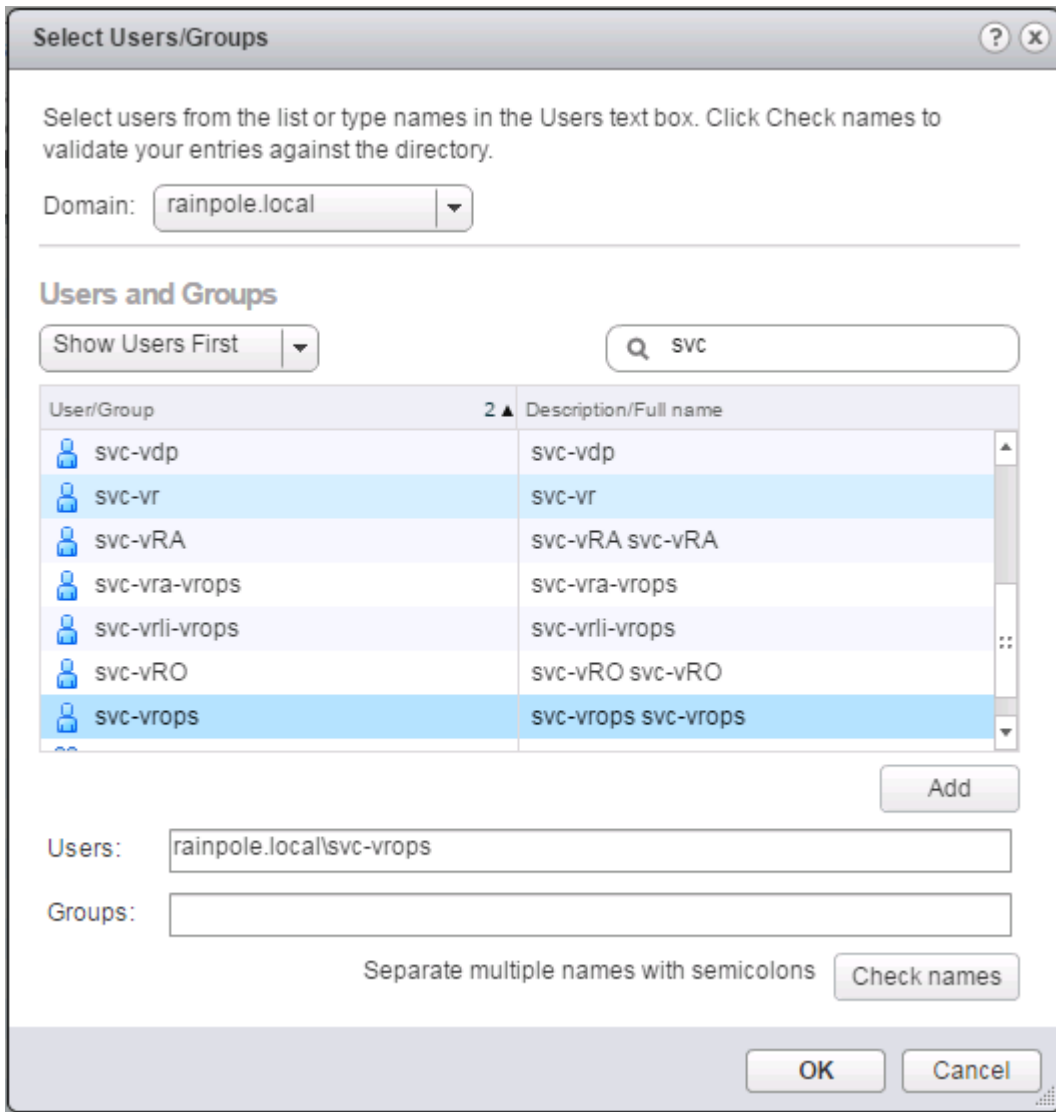
User	Role
svc-vrops@rainpole.local	Read-Only
svc-mpsd-vrops@rainpole.local	MPSD Metrics User

- a In the vSphere Web Client, navigate to **Administration** and click **Global Permissions**.
- b Click **Add Permission**.



- c In the **Global Permissions Root - Add Permission** dialog box, click **Add** to associate a user or a group with a role.
- d In the **Select Users/Groups** dialog box, from the **Domain** drop-down menu, select **rainpole.local**, in the filter box type **svc** and press Enter.

- e From the list of users and groups, select **svc-vrops**, click **Add** , and click **OK**.



- f In the **Global Permissions Root - Add Permission** dialog box, from the **Assigned Role** drop-down menu, select **Read-only**, ensure that **Propagate to children** is selected, and click **OK**.
- g Repeat the steps to assign the MPSP Metrics User role to the svc-mpsd-vrops user.

Add vCenter Adapter Instances to vRealize Operations Manager for ROBO

After you deploy the remote collector nodes of vRealize Operations Manager in the ROBO, add a vCenter Adapter instance for the ROBO vCenter Server instance.

Prerequisites

- Verify that the ROBO vCenter Server is running.

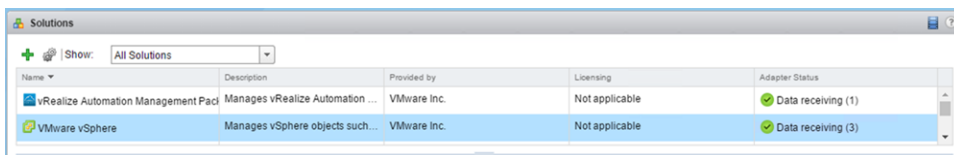
- Verify that the ROBO vCenter Server is configured with the rainpole.local Active Directory domain.
- Verify the custom read-only role for user svc-vrops has been added to the ROBO vCenter Server.

Procedure

- 1 Log in to vRealize Operations Manager by using the administration console.
 - a Open a Web browser and go to **https://vrops-cluster-01.rainpole.local**.
 - b Log in using the following credentials.

Setting	Value
User name	admin
Password	vrops_admin_password

- 2 In the left pane of vRealize Operations Manager, click **Administration** and click **Solutions**.
- 3 From the solution table on the **Solutions** page, select the **VMware vSphere** solution, and click the **Configure** icon at the top.



The **Manage Solution - VMware vSphere** dialog box appears.

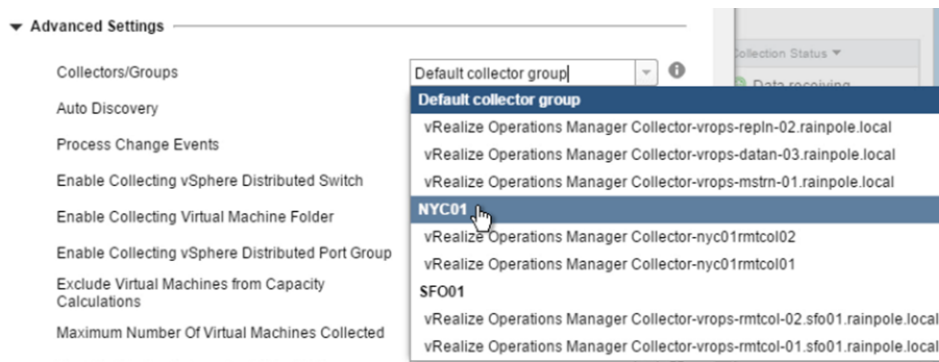
- 4 On the **Configure Adapters** page, from the **Adapter Type** table at the top, select **vCenter Adapter**.
The **Instance Name** list contains the vCenter Adapter instances for Region A and Region B of the hub.
- 5 Under **Instance Settings**, enter the settings for connection to the ROBO vCenter Server instance.
 - a Click the **Add** icon on the left side to add an adapter settings.
 - b Enter the name, description and FQDN of vCenter Server.

Setting	Value
Name	nyc01vc01-ROBO01
Description	vCenter Server for ROBO
vCenter Server	nyc01vc01.rainpole.local

- c Click the **Add** icon on the right side, configure the collection credentials for connection to the ROBO vCenter Server instance, and click **OK**.

Management vCenter Server	
Credentials Attribute	Value
Credential name	nyc01vc01-credentials for ROBO vCenter Server
User Name	svc-vrops@rainpole.local
Password	svc-vrops-password

- d Leave **Enable Actions** set to **Enable** so that vCenter Adapter can run actions on objects in the vCenter Server from vRealize Operations Manager.
- e Click **Test Connection** to validate the connection to vCenter Server instance.
- The vCenter Server certificate appears.
- f In the **Review and Accept Certificate** dialog box, verify the certificate information and click **OK**.
- g Click **OK** in the **Test Connection Info** dialog box.
- h Expand the **Advanced Settings** section of settings.
- i From the **Collectors/Groups** drop-down menu, select the **NYC01** group.



- j Specify a user account with administrator privileges to register vRealize Operations Manager with the vCenter Server instance.

Setting	Value
Registration user	administrator@vsphere.local
Registration password	vsphere_admin_password

After the registration, vCenter Server users can launch vRealize Operations Manager from and use health badges on the inventory objects in the vSphere Web Client.

- 6 Click **Define Monitoring Goals**.
- 7 In the **Define Monitoring Goals** page, under **Enable vSphere Hardening Guide Alerts?**, select **Yes**, leave the default configuration for the other options, and click **Save**.

Define Monitoring Goals

Please answer the following list of questions to create a new default policy or Save to modify the existing default policy. To adjust advanced settings of the default policy or create a new policy, proceed to Administration > Policies Page.

Which objects do you want to be alerted on in your environment?

[Learn More](#)

☐ Infrastructure objects except for Virtual Machines
☐ Virtual Machines only
☒ All vSphere objects

Which type of alerts do you want to enable? (Select all that apply)

[Learn More](#)

☒ Health alerts that usually require immediate attention.
☒ Risk alerts indicating that you should look into any problems in the near future
☒ Efficiency alerts indicating that you can reclaim resources.

Configure Memory Capacity based on?

[Learn More](#)

☒ vSphere Default
☐ Most Aggressive
☐ Most Conservative

Enable vSphere Hardening Guide Alerts?

[Learn More](#)

☒ Yes
☐ No

Save Cancel

- 8 Click **OK** in the **Default Policy Info** dialog box.
- 9 Click **Save Settings**.
- 10 In the **Review and Accept Certificate** dialog box, verify the certificate information and click **OK**.
- 11 Click **OK** in the **Adapter Instance Information** dialog box.
- 12 In the **Manage Solution - VMware vSphere** dialog box, click **Close**.
- 13 On the **Solutions** page, select **VMware vSphere** from the solution table to view the collection state and the collection status.

The **Collection State** column for the vCenter Adapters displays Collecting, and the **Collection Status** column displays Data receiving.

Solutions

Show: All Solutions

Name	Description	Provided by	Licensing	Adapter Status
vRealize Automation Management Pack	Manages vRealize Automation ...	VMware Inc.	Not applicable	Data receiving (1)
VMware vSphere	Manages vSphere objects such...	VMware Inc.	Not applicable	Data receiving (3)

VMware vSphere Solution Details

Adapter Type	Adapter Instance Name	Credential name	Collector	Collection State	Collection Status
vCenter Adapter	nyc01vc01-ROBO01	nyc01vc01-credentials for RO...	vRealize Operations Manager Collector-ny...	Collecting	Data receiving

Connect vRealize Operations Manager to the NSX Manager in ROBO

Configure the vRealize Operations Management Pack for NSX for vSphere to monitor the NSX networking services deployed in the vSphere cluster in the ROBO and view the vSphere hosts in the NSX transport zones. You can also access end-to-end logical network topologies between any two virtual machines or NSX objects for better visibility into logical connectivity. Physical host and network device relationship in this view also helps in isolating problems in the logical or physical network.

You configure the NSX-vSphere Adapter for collecting data from the NSX components in ROBO.

Procedure

1 [Configure User Privileges in NSX Manager for Integration with vRealize Operations Manager for ROBO](#)

Assign the operations local service account `svc-vrops-nsx` the permissions that are required to access monitoring data from the NSX Manager ROBO in vRealize Operations Manager.

2 [Add an NSX-vSphere Adapter Instance to vRealize Operations Manager for ROBO](#)

Configure the connection between vRealize Operations Manager and the NSX instance for the ROBO cluster.

Configure User Privileges in NSX Manager for Integration with vRealize Operations Manager for ROBO

Assign the operations local service account `svc-vrops-nsx` the permissions that are required to access monitoring data from the NSX Manager ROBO in vRealize Operations Manager.

Prerequisites

- Ensure that SSH has been enabled on the NSX Manager in ROBO.
- On a Windows host that has access to your data center, install a REST client. An example of a suitable REST client is the RESTClient add-on for the Mozilla Firefox web browser.

Procedure

- 1 Log in to the NSX Manager by using a Secure Shell (SSH) client.
 - a Open an SSH connection to the NSX Manager virtual machine `nyc01nsxm01.rainpole.local`
 - b Log in using the following credentials.

Setting	Value
User name	admin
Password	<code>nyc01nsx_admin_password</code>

2 Create the local service account svc-vrops-nsx on the NSX Manager instances.

- a Run the following command to switch to Privileged mode of the NSX Manager.

```
enable
```

- b Enter the admin password when prompted and press Enter.
- c Switch to Configuration mode.

```
configure terminal
```

- d Create the service account svc-vrops-nsx.

```
user svc-vrops-nsx password plaintext svc-vrops-nsx_password
```

- e Assign the svc-vrops-nsx user access to NSX Manager from the vSphere Web Client.

```
user svc-vrops-nsx privilege web-interface
```

- f Leave the Configuration mode .

```
exit
```

- g Commit these updates to the NSX Managers:

```
copy running-config startup-config
```

3 Assign the security_admin role to the svc-vrops-nsx service account.

- a Log in to the Windows host that has access to your data center.
- b In a Firefox browser, go to **chrome://restclient/content/restclient.html**
- c From the **Authentication** drop-down menu, select **Basic Authentication**.
- d In the **Basic Authorization** dialog box, enter the following credentials, select **Remember me** and click **Okay**.

Setting	Value
User name	admin
Password	nyc01nsx_admin_password

The Authorization: Basic XXX header appears in the **Headers** pane.

- e From the **Headers** drop-down menu, select **Custom Header**.

- f In the **Request Header** dialog box, enter the following header details and click **Okay**.

Request Header Attribute	Value
Name	Content-Type
Value	Application/xml

The Content-Type:Application/xml header appears in the **Headers** pane.

- g In the **Request** pane, from the **Method** drop-down menu, select **POST**, and in the **URL** text box, enter the following URL.

NSX Manager	POST URL
NSX Manager for the ROBO	https://nyc01nsxm01.rainpole.local/api/2.0/services/usermgmt/role/svc-vrops-nsx?isCli=true

- h In the **Request** pane, paste the following request body in the **Body** text box and click **Send**.

```
<accessControlEntry>
  <role>security_admin</role>
  <resource>
    <resourceId>globalroot-0</resourceId>
  </resource>
</accessControlEntry>
```

The screenshot shows the RESTClient application interface. At the top, there are tabs for File, Authentication, Headers, and View. On the right, there are links for Favorite Requests, Setting, and the RESTClient logo. The main area is titled "[+] Request". Below this, there is a form with a Method dropdown set to "POST" and a URL text box containing "https://nyc01nsxm01.rainpole.local/api/2.0/services/usermgmt/role/svc-vrops-nsx?isCli=true". A "SEND" button is to the right of the URL. Below the form is a "Headers" section with a "Remove All" button. It contains a table with two headers: "Header Name" and "Header Value". The table has two rows: "Content-Type" with value "Application/xml" and "Authorization" with value "Basic YWRtaW46Vk13YXJIMSE=". Below the headers is a "Body" section with a text area containing the XML request body: <accessControlEntry> <role>security_admin</role> <resource> <resourceId>globalroot-0</resourceId> </resource> </accessControlEntry>.

The Status changes to 204 No Content.

Add an NSX-vSphere Adapter Instance to vRealize Operations Manager for ROBO

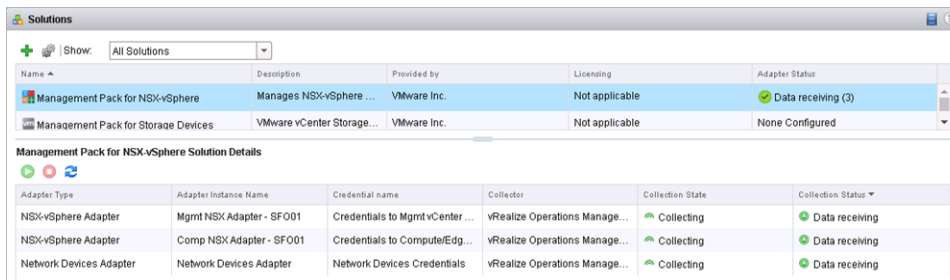
Configure the connection between vRealize Operations Manager and the NSX instance for the ROBO cluster.

Procedure

- 1 Log in to vRealize Operations Manager by using the administration console.
 - a Open a Web browser and go to **https://vrops-cluster-01.rainpole.local**.
 - b Log in using the following credentials.

Setting	Value
User name	admin
Password	vrops_admin_password

- 2 In the left pane of vRealize Operations Manager, click **Administration** and click **Solutions**.
- 3 On the **Solutions** page, select the **Management Pack for NSX-vSphere** from the solution table, and click **Configure**.



- 4 In the **Manage Solution - Management Pack for NSX-vSphere** dialog box, from the **Adapter Type** table at the top, select **NSX-vSphere Adapter**.

The **Instance Name** list contains the instances of the NSX Adapter for Region A and Region B of the hub.

- 5 Under **Instance Settings**, enter the settings for connection to the NSX Manager for the ROBO cluster.

- a Click the **Add** icon to add an adapter settings.
- b Enter the name, the FQDN of the ROBO NSX Manager and the FQDN of the ROBO vCenter Server instance that is connected to the NSX Manager.

Setting	Value for the NSX Manager for the ROBO cluster
Display Name	ROBO NSX Adapter - NYC01
Description	-
NSX Manager Host	nyc01nsxm01.rainpole.local
VC Host	nyc01vc01.rainpole.local
Enable Log Insight integration if configured	false

- c Click the **Add** icon next to the **Credential** text box, configure the credentials for the connection to NSX Manager and vCenter Server, and click **OK**.

Setting	Value for the NSX Manager for the ROBO cluster
Credential name	Credentials to ROBO VC and NSX Manager - NYC01
NSX User Name	svc-vrops-nsx
NSX Manager Password	<i>svc-vrops-nsx_password</i>
vCenter User Name	svc-vrops@rainpole.local
vCenter Password	<i>svc-vrops-password</i>

- d Expand the **Advanced Settings** pane.
 - e In the **Advanced Settings** pane, click the **Collectors/Groups** drop-down menu and select **NYC01**.
 - f Click **Test Connection** to validate the connection to the ROBO NSX Manager.
The NSX Manager certificate appears.
 - g In the **Review and Accept Certificate** dialog box, verify the certificate information and click **OK**.
 - h Click **OK** in the **Test Connection Info** dialog box.
 - i Click **Save Settings**.
 - j In the **Review and Accept Certificate** dialog box, verify the certificate information and click **OK**.
 - k Click **OK** in the **Adapter Instance** dialog box.
- 6 In the **Manage Solution - Management Pack for NSX-vSphere** dialog box, click **Close**.

The NSX-vSphere Adapters for ROBO is available on the **Solutions** page of the vRealize Operations Manager user interface. The **Collection State** of the adapters is **Collecting** and the **Collection Status** is **Data receiving**.

Name	Description	Provided by	Licensing	Adapter Status
Management Pack for NSX-vSphere	Manages NSX-vSphere objects, inc...	VMware Inc.	Not applicable	Data receiving (3)
Management Pack for vCenter Storage Devices	Manages vCenter Storage Devices, S...	VMware Inc.	Not applicable	Data receiving (3)

Adapter Type	Adapter Instance Name	Credential name	Collector	Collection State	Collection Status
NSX-vSphere Adapter	ROBO NSX Adapter - NYC01	Credentials to ROBO VC and...	vRealize Operations Manager Collector-ny...	Collecting	Data receiving

Configure Service Account Privileges for Integration between vRealize Operations Manager and vRealize Automation in ROBO

Configure the rights of the service accounts that vRealize Automation and vRealize Operations Manager use to communicate with each other.

You use these service accounts in the following cases:

- When vRealize Operations Manager collects statistics about the tenant workloads in vRealize Automation in ROBO.
- When vRealize Automation collects metrics to identify tenant workloads for reclamation in ROBO. Such workloads have low use of CPU, memory use, or disk space.

Configure User Privileges in vRealize Automation for Integration with vRealize Operations Manager in ROBO

Assign the permissions that are required to access monitoring data from vRealize Automation for the ROBO-specific fabric group in vRealize Operations Manager to the svc-vrops-vra operations service account.

Procedure

- 1 Log in to the vRealize Automation Rainpole portal.
 - a Open a Web browser and go to **`https://vra01svr01.rainpole.local/vcac/org/rainpole`**.
 - b Log in using the following credentials.

Setting	Value
User name	itac-tenantadmin
Password	itac-tenantadmin_password
Domain	Rainpole.local

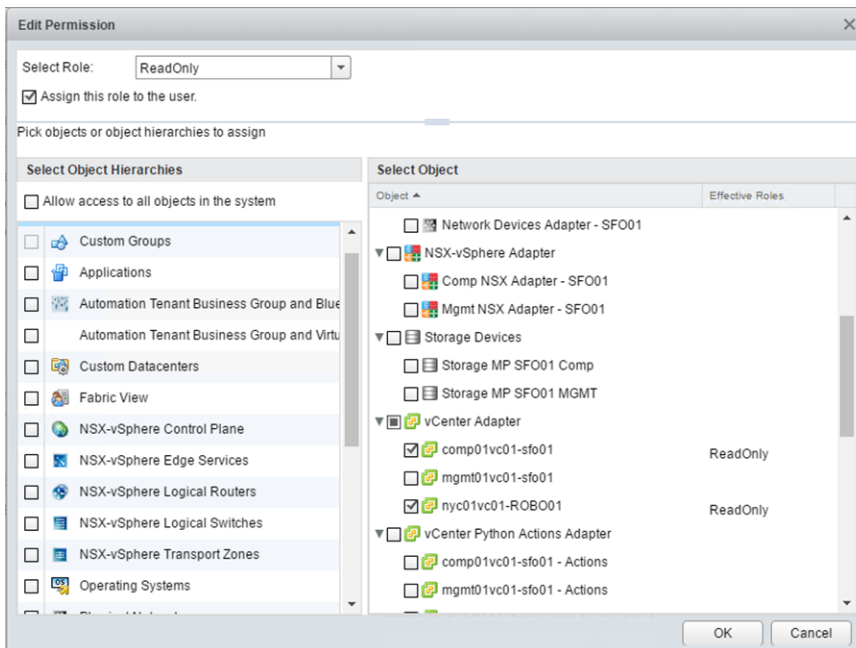
- 2 Navigate to **Infrastructure > Endpoints > Fabric Groups** to assign fabric administrator role to the svc-vrops-vra service account.
 - a On the **Fabric Groups** page, click **NYC01 Fabric Group**.
 - b On **Edit Fabric Group** page, enter **svc-vrops-vra** in **Fabric Administrators** search text box and click the **Search** icon.
 - c Click **svc-vrops-vra@rainpole.local** in the search result list to assign the fabric administrator role to the account, and click **OK**.

Configure User Privileges on vRealize Operations Manager for Tenant Workload Reclamation in ROBO

Configure read-only privileges for the `svc-vra-vrops@rainpole.local` service account on vRealize Operations Manager. You configure these privileges so that vRealize Automation can pull metrics from vRealize Operations Manager for reclamation of tenant workloads in the ROBO.

Procedure

- 1 Log in to vRealize Operations Manager by using the administration console.
 - a Open a Web browser and go to **`https://vrops-cluster-01.rainpole.local`**.
 - b Log in using the following credentials.
- | Setting | Value |
|-----------|-----------------------------------|
| User name | admin |
| Password | <code>vrops_admin_password</code> |
- 2 In the left pane of vRealize Operations Manager, click **Administration**, and click **Access Control**.
 - 3 On the **Access Control** page, click the **User Accounts** tab.
 - 4 Select the **svc-vra-vrops@rainpole.local** service account, and click **Edit** icon.
 - 5 On the **Edit Permission** page, to assign the ReadOnlY role to the `svc-vra-vrops@rainpole.local` service account, configure the following settings.
 - a Under **Select Object**, select **vCenter Adapter > nyc01vc01-ROBO01** and click **OK**.



Add Storage Devices Adapters in vRealize Operations Manager for ROBO

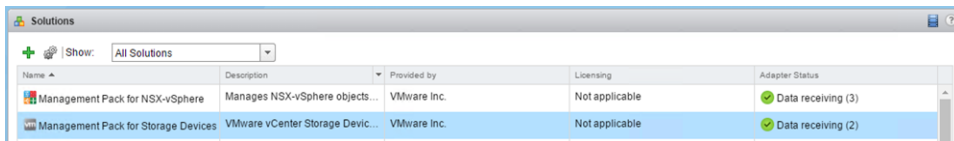
Configure a Storage Devices adapter for each ROBO location to collect monitoring data about the storage devices in the remote sites.

Procedure

- 1 Log in to vRealize Operations Manager by using the administration console.
 - a Open a Web browser and go to **`https://vrops-cluster-01.rainpole.local`**.
 - b Log in using the following credentials.

Setting	Value
User name	admin
Password	vrops_admin_password

- 2 In the left pane of vRealize Operations Manager, click **Administration** and click **Solutions**.
- 3 On the **Solutions** page, select **Management pack for Storage Devices** from solution table and click **Configure**.



- 4 In the **Manage Solution - Management Pack for Storage Devices** dialog box, from the **Adapter Type** table at the top, select **Storage Devices**.

The **Instance Name** list contains the instances of the Storage Devices Adapter for Region A and Region B from the Hub.

- 5 Under **Instance Settings**, enter the settings for connection to the ROBO vCenter Server instance.
 - a Click the **Add** icon to add an adapter setting.
 - b Enter the name, description, and FQDN of the vCenter Server instance.

Setting	Value for the for the ROBO cluster
Name	Storage MP NYC ROBO
Description	Connection to NYC ROBO vCenter
vCenter Server	nyc01vc01.rainpole.local
SNMP Community Strings	-

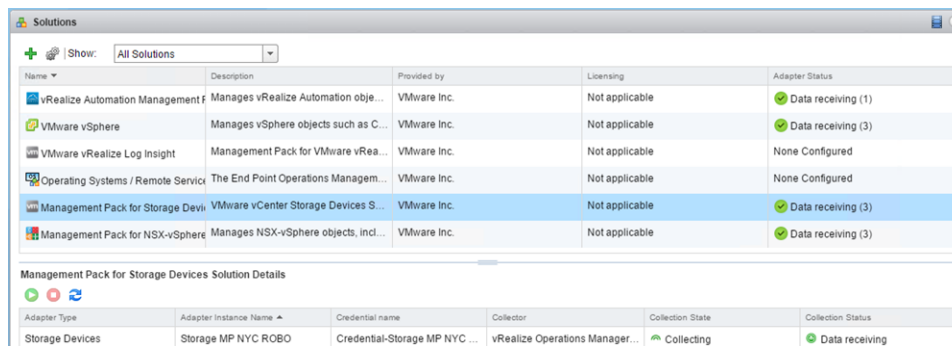
- c Click the **Add** icon, configure the credentials for connection to the ROBO vCenter Server, and click **OK**.

Setting	Value for the for the ROBO cluster
Credential name	Credential-Storage MP NYC ROBO
User Name	svc-mpsd-vrops@rainpole.local
Password	svc-mpsd-vrops-password

- d Click **Test Connection** to validate the connection to the ROBO vCenter Server instance.
- e In the **Review and Accept Certificate** dialog box, verify the vCenter Server certificate information and click **OK**.
- f Click **OK** in the **Test Connection** dialog box.
- g Expand the **Advanced Settings** section of settings, and from the **Collectors/Groups** drop-down menu, select the **NYC01** remote collector group.
- h Click **Save Settings**.
- i In the **Review and Accept Certificate** dialog box, click **OK**.
- j Click **OK** in the information box that appears.

- 6 In the **Manage Solution - Management Pack for Storage Devices** dialog box, click **Close**.

The Storage Devices Adapter for ROBO appear on the **Solutions** page of the vRealize Operations Manager user interface. The **Collection State** of the adapters is **Collecting** and the **Collection Status** is **Data receiving**.



Name	Description	Provided by	Licensing	Adapter Status
vRealize Automation Management f	Manages vRealize Automation obje...	VMware Inc.	Not applicable	✔ Data receiving (1)
VMware vSphere	Manages vSphere objects such as C...	VMware Inc.	Not applicable	✔ Data receiving (3)
VMware vRealize Log Insight	Management Pack for VMware vRea...	VMware Inc.	Not applicable	None Configured
Operating Systems / Remote Servi...	The End Point Operations Managem...	VMware Inc.	Not applicable	None Configured
Management Pack for Storage Devi...	VMware vCenter Storage Devices S...	VMware Inc.	Not applicable	✔ Data receiving (3)
Management Pack for NSX-vSphere	Manages NSX-vSphere objects, incl...	VMware Inc.	Not applicable	✔ Data receiving (3)

Adapter Type	Adapter Instance Name	Credential name	Collector	Collection State	Collection Status
Storage Devices	Storage MP NYC ROBO	Credential-Storage MP NYC ...	vRealize Operations Manager...	Collecting	✔ Data receiving

vRealize Log Insight Implementation in ROBO

Deploy vRealize Log Insight in a cluster configuration of 3 nodes in the ROBO region. This configuration is set up with an integrated load balancer and uses one master and two worker nodes.

Procedure

1 Deploy vRealize Log Insight in ROBO

Start the deployment of vRealize Log Insight in the ROBO by deploying the master and worker nodes and forming the vRealize Log Insight cluster.

2 [Install a CA-Signed Certificate on vRealize Log Insight in ROBO](#)

vRealize Log Insight comes with a default self-signed certificate that is generated and signed at installation time. After you start vRealize Log Insight in the ROBO, install a CA-signed certificate to secure the communication of vRealize Log Insight.

3 [Connect vRealize Log Insight to the vSphere Environment in ROBO](#)

Start collecting log information about the ESXi and vCenter Server instances in the ROBO.

4 [Connect vRealize Log Insight to vRealize Operations Manager in ROBO](#)

Install and configure the vRealize Log Insight Content Pack for vRealize Operations Manager in the ROBO for troubleshooting vRealize Operations Manager by using dashboards and alerts in the vRealize Log Insight UI.

5 [Connect vRealize Log Insight to the NSX Instances in ROBO](#)

Install and configure the vRealize Log Insight Content Pack for NSX for vSphere for log visualization and alerting of the NSX for vSphere real-time operation in the ROBO. You can use the NSX-vSphere dashboards to monitor logs about installation and configuration, and about virtual networking services.

6 [Connect vRealize Log Insight to vRealize Automation in ROBO](#)

Connect the vRealize Log to vRealize Automation to receive log information from the components of vRealize Automation in the ROBO in the vRealize Log Insight UI.

7 [Install the vRealize Log Insight Content Pack for vSAN in ROBO](#)

Install the content pack for VMware vSAN to add the dashboards for viewing log information in vRealize Log Insight in the ROBO.

8 [Configure Event Forwarding From ROBO to Region A and Region B](#)

According to vRealize Log Insight Design for ROBO, vRealize Log Insight forwards logging information to both Region A and Region B in the SDDC hub. In this way, both vRLI instances can ingest the ROBO logging data while still remaining independent of one another.

Deploy vRealize Log Insight in ROBO

Start the deployment of vRealize Log Insight in the ROBO by deploying the master and worker nodes and forming the vRealize Log Insight cluster.

Procedure

1 [Prerequisites for Deploying vRealize Log Insight in ROBO](#)

Before you deploy vRealize Log Insight in a ROBO, verify that your environment satisfies the requirements for this deployment.

2 [Deploy the Virtual Appliance for Each Node in the vRealize Log Insight Cluster in ROBO](#)

Use the vSphere Web Client to deploy each vRealize Log Insight node as a virtual appliance on the ROBO cluster.

3 Configure a DRS Anti-Affinity Rule for vRealize Log Insight in ROBO

To protect the vRealize Log Insight cluster in the ROBO from a host-level failure, configure vSphere DRS to run the worker virtual appliances on different hosts in the ROBO cluster.

4 Start the vRealize Log Insight Instance in ROBO

Configure and start the vRealize Log Insight master node in the ROBO. Before you form a cluster by adding the worker nodes, vRealize Log Insight must be initialized.

5 Join the Worker Nodes to vRealize Log Insight in ROBO

After you deploy the virtual appliances for vRealize Log Insight and start the vRealize Log Insight instance on the master node in the ROBO, join the two worker nodes to form a cluster.

6 Enable the Integrated Load Balancer of vRealize Log Insight in ROBO

After you join the master and the worker nodes to create a vRealize Log Insight cluster in the ROBO, enable the Integrated Load Balancer (ILB) for balancing incoming ingestion traffic of syslog data among the Log Insight nodes and for high availability.

7 Join vRealize Log Insight to the Active Directory in ROBO

To propagate user roles and allow user access in vRealize Log Insight that are maintained centrally and are inline with the other solutions in the SDDC, configure vRealize Log Insight in the ROBO to use the Active Directory (AD) domain as an authentication source.

Prerequisites for Deploying vRealize Log Insight in ROBO

Before you deploy vRealize Log Insight in a ROBO, verify that your environment satisfies the requirements for this deployment.

IP Addresses and Host Names

Verify that static IP addresses and FQDNs for vRealize Log Insight in the virtual application network are available for the ROBO SDDC deployment.

For the application virtual network, allocate 3 static IP addresses for the vRealize Log Insight nodes and one IP address for the integrated load balancer. Map host names to the IP addresses.

Note ROBO must be routable via the vSphere management network.

Table 4-2. IP Addresses and Host Name for the vRealize Log Insight Cluster in Region B

Role	IP Address	FQDN
Integrated load balancer VIP address	172.18.19.10	nyc01vrli01-cluster01.rainpole.local
Master node	172.18.19.11	nyc01vrli01.rainpole.local
Worker node 1	172.18.19.12	nyc01vrli02.rainpole.local
Worker node 2	172.18.19.13	nyc01vrli03.rainpole.local
Default gateway	172.18.19.1	-
DNS servers	172.18.11.4	-

Table 4-2. IP Addresses and Host Name for the vRealize Log Insight Cluster in Region B (Continued)

Role	IP Address	FQDN
Subnet mask	255.255.255.0	-
NTP servers	<ul style="list-style-type: none"> ■ 172.18.11.251 ■ 172.18.11.252 	ntp.rainpole.local

Deployment Prerequisites

Prerequisite	Value
Storage	<ul style="list-style-type: none"> ■ Virtual disk provisioning <ul style="list-style-type: none"> ■ Thin ■ Required storage per node <ul style="list-style-type: none"> ■ Initial storage for node deployment: 510 GB
Software Features	<ul style="list-style-type: none"> ■ vSphere <ul style="list-style-type: none"> ■ ROBO vCenter Server ■ ROBO consolidated cluster with DRS and HA enabled. ■ NSX for vSphere <ul style="list-style-type: none"> ■ Application virtual network for the 3-node vRealize Log Insight cluster
Installation Package	Download the .ova file of the vRealize Log Insight virtual appliance on the machine where you use the vSphere Web Client.
License	Obtain a license that covers the use of vRealize Log Insight.
Active Directory	Verify that you have a parent and child Active Directory domain controllers configured with the role-specific SDDC users and groups for the rainpole.local domain.
Certification Authority	Configure the Active Directory domain controller as a certificate authority for the environment.
E-mail account	Provide an email account to send vRealize Log Insight notifications from.

Deploy the Virtual Appliance for Each Node in the vRealize Log Insight Cluster in ROBO

Use the vSphere Web Client to deploy each vRealize Log Insight node as a virtual appliance on the ROBO cluster.

Procedure

- 1 Log in to vCenter Server by using the vSphere Web Client.
 - a Open a Web browser and go to **https://nyc01vc01.rainpole.local/vsphere-client**.
 - b Log in using the following credentials.

Setting	Value
User name	administrator@vsphere.local
Password	vsphere_admin_password

- 2 Navigate to the nyc01vc01.rainpole.local vCenter Server object.

- 3 Right-click **nyc01vc01.rainpole.local** and select **Deploy OVF Template**.
- 4 On the **Select source** page, select **Local file**, click **Browse** and browse to the location of the vRealize Log Insight .ova file on your local file system, and click **Next**.
- 5 On the **Select name and folder** page, make the following selections, and click **Next**.
 - a Enter a name for the node according to its role.

Name	Role
nyc01vrli01	Master node
nyc01vrli02	Worker node 1
nyc01vrli03	Worker node 2

- b Select the inventory folder for the virtual appliance.

Object	Value
vCenter Server	nyc01vc01.rainpole.local
Data center	NYC01
Folder	vRLI01

- 6 On the **Select a resource** page, select the resource pool **NYC01-MGMT**, and click **Next**.

Setting	Value
Datacenter	NYC01
Resource Pool	NYC01-MGMT

- 7 On the **Review details** page, examine the virtual appliance details, such as product, version, download size, and disk size, and click **Next**.
- 8 On the **Accept License Agreements** page, accept the end user license agreements and click **Next**.
- 9 On the **Select configuration** page, from the **Configuration** drop-down menu, select the **Small** deployment configuration, and click **Next**.
- 10 On the **Select storage** page, select the datastore for the vRealize Log Insight node.
By default, the virtual appliance disk is thin provisioned.
 - a From the **VM Storage Policy** drop-down menu, select **Virtual SAN Default Storage Policy**.
 - b From the datastore table, select the **NYC01-VSAN01** vSAN datastore and click **Next**.
- 11 On the **Setup networks** page, select the distributed port group on the vDS-NYC01 distributed switch that ends with Mgmt-NYC01-VXLAN, and click **Next**.

12 On the **Customize template** page, set the networking settings and the root user credentials for the virtual appliance.

- a In the **Networking Properties** section, configure the following networking settings.

Property	Value
Host name	<ul style="list-style-type: none"> ■ nyc01vrli01.rainpole.local for the master node ■ nyc01vrli02.rainpole.local for the worker node 1 ■ nyc01vrli03.rainpole.local for the worker node 2
Default gateway	172.18.19.1
DNS server	172.18.11.4
DNS searchpath	rainpole.local
DNS domain	rainpole.local
Static IPv4 address	<ul style="list-style-type: none"> ■ 172.18.19.11 for the master node ■ 172.18.19.12 for the worker node 1 ■ 172.18.19.13 for the worker node 2
Subnet mask	255.255.255.0

- b In the **Other Properties** section, enter and confirm a password for the root user and click **Next**.

The password must contain at least 8 characters, and must include:

- One uppercase character
- One lowercase character
- One digit
- One special character

Use this password if you log in to the console of the vRealize Log Insight virtual appliance.

13 On the **Ready to complete** page, click **Finish**.

The deployment of the virtual appliance starts.

14 Right-click the virtual appliance object and select the **Power > Power On** menu item.

15 Repeat the procedure to deploy the vRealize Log Insight virtual appliances for the remaining two nodes in the cluster.

Configure a DRS Anti-Affinity Rule for vRealize Log Insight in ROBO

To protect the vRealize Log Insight cluster in the ROBO from a host-level failure, configure vSphere DRS to run the worker virtual appliances on different hosts in the ROBO cluster.

Procedure

- 1 Log in to vCenter Server by using the vSphere Web Client.
 - a Open a Web browser and go to **`https://nyc01vc01.rainpole.local/vsphere-client`**.
 - b Log in using the following credentials.

Setting	Value
User name	administrator@vsphere.local
Password	vsphere_admin_password

- 2 Navigate to the nyc01vc01.rainpole.local vCenter Server object, and under the **NYC01** data center object select the **NYC01** cluster.
- 3 On the **Configure** tab, select **VM/Host Rules**.
- 4 In the **VM/Host Rules** list, click the **Add** button above the rules list, add a new anti-affinity rule called **anti-affinity-rule-vrli** for the vRealize Log Insight master and worker virtual machines, and click **OK**.

Rule Attribute	Value
Name	anti-affinity-rule-vrli
Enable rule	Yes
Type	Separate Virtual Machines
Members	<ul style="list-style-type: none"> ■ nyc01vrli01 ■ nyc01vrli02 ■ nyc01vrli03

Start the vRealize Log Insight Instance in ROBO

Configure and start the vRealize Log Insight master node in the ROBO. Before you form a cluster by adding the worker nodes, vRealize Log Insight must be initialized.

Procedure

- 1 Open a Web browser and go to **`https://nyc01vrli01.rainpole.local`**.
The initial configuration wizard opens.
- 2 On the **Setup** page, click **Next**.
- 3 On the **Choose Deployment Type** page, click **Start New Deployment**.

- 4 After the deployment is launched, on the **Admin Credentials** page, set the email address and the password of the admin user, and click **Save and Continue**.

The password must contain at least 8 characters, and contain one uppercase character, one lowercase character, one number, and one special character.

- 5 On the **License** page, enter the license key, click **Add New License Key**, and click **Continue**.
- 6 On the **General Configuration** page, enter the following settings and click **Save and Continue**.

Setting	Value
Email System Notifications to	<i>email address to receive system notifications</i>
Send HTTP Post System Notifications To	https://nyc01vrli01-cluster01.rainpole.local

- 7 On the **Time Configuration** page, enter the following settings, click **Test** and click **Save and Continue**.

Setting	Value
Sync Server Time With	NTP Server (recommended)
NTP Servers	ntp.rainpole.local

- 8 On the **SMTP Configuration** page, specify the properties of an SMTP server to enable outgoing alerts and system notification emails, and to test the email notification.
 - a Set the connection setting for the SMTP server that will send the email messages from vRealize Log Insight.

Contact your system administrator for details about the email server.

SMTP Option	Description
SMTP Server	FQDN of the SMTP server
Port	Server port for SMTP requests
SSL (SMTPS)	Sets whether encryption should be enabled for the SMTP transport option connection.
STARTTLS Encryption	Enable or disable the STARTTLS encryption.
Sender	Address that appears as the sender of the email.
Username	User name on the SMTP server.
Password	Password for the SMTP server you specified in Username.

- b To verify that the SMTP configuration is correct, enter a valid email address and click **Send > Test Email**.

vRealize Log Insight sends a test email to the address that you provided.

- 9 On the **Setup Complete** page, click **Finish**.

vRealize Log Insight starts operating in standalone mode.

Join the Worker Nodes to vRealize Log Insight in ROBO

After you deploy the virtual appliances for vRealize Log Insight and start the vRealize Log Insight instance on the master node in the ROBO, join the two worker nodes to form a cluster.

Procedure

- 1 For each worker node appliance, go to the initial setup UI in your Web browser.

Worker Node	HTTP URL
Worker node 1	https://nyc01vrli02.rainpole.local
Worker node 2	https://nyc01vrli03.rainpole.local

The initial configuration wizard opens.

- 2 Click the **Next** button on the **Welcome** page.
- 3 On the **Choose Deployment Type** page, click **Join Existing Deployment**.
- 4 On the **Join Existing Deployment** page, enter the master node FQDN **nyc01vrli01.rainpole.local** and click **Go**.

The worker node sends a request to the vRealize Log Insight master node to join the existing deployment.

- 5 After the worker node contacts the master node, click the **Click here to access the Cluster Management page** link.

The login page of the vRealize Log Insight user interface opens.

- 6 Log in to the vRealize Log Insight UI by using the following credentials.

Setting	Value
User name	admin
Password	vrli_admin_password

The **Cluster** page opens in the Log Insight user interface.

- 7 On the right of the notification message about adding the worker node, click **Allow**.

After you join the first worker node to the cluster, the user interface displays a warning message that another worker node must be added.

- 8 Repeat the steps to join the second worker node to the cluster.

After you add the second worker node, the **Cluster** page of the vRealize Log Insight UI contains the master and worker nodes as components of the cluster.


Enable the Integrated Load Balancer of vRealize Log Insight in ROBO

After you join the master and the worker nodes to create a vRealize Log Insight cluster in the ROBO, enable the Integrated Load Balancer (ILB) for balancing incoming ingestion traffic of syslog data among the Log Insight nodes and for high availability.

Procedure

- 1 Log in to the vRealize Log Insight user interface.
 - a Open a Web browser and go to **`https://nyc01vrli01.rainpole.local`**.
 - b Log in using the following credentials.

Setting	Value
User name	admin
Password	<i>vrli_admin_password</i>

- 2 Click the configuration drop-down menu icon  and select **Administration**.
- 3 Under **Management**, click **Cluster**.
- 4 Under **Integrated Load Balancer**, click **New Virtual IP Address**.
- 5 In the **New Virtual IP** dialog box, enter the following settings and click **Save**.

Setting	Value
IP	172.18.19.10
FQDN	nyc01vrli01-cluster01.rainpole.local

Join vRealize Log Insight to the Active Directory in ROBO

To propagate user roles and allow user access in vRealize Log Insight that are maintained centrally and are inline with the other solutions in the SDDC, configure vRealize Log Insight in the ROBO to use the Active Directory (AD) domain as an authentication source.

Figure 4-1. Procedure

Procedure

- 1 Log in to the vRealize Log Insight user interface.
 - a Open a Web browser and go to **`https://nyc01vrli01-cluster01.rainpole.local`**.
 - b Log in using the following credentials.

Setting	Value
User name	admin
Password	<i>vrli_admin_password</i>

- 2 On the **Authentication** page, select the checkbox to enable the support for Active Directory and configure the Active Directory settings.

- a Configure the Active Directory connection settings according to the details from your IT administrator.

Setting	Value
Enable Active Directory support	Selected
Default Domain	RAINPOLE.LOCAL
Domain Controller(s)	dc03rpl.rainpole.local
User Name	svc-loginsight
Password	<i>svc_loginsight_password</i>
Connection Type	Standard
Require SSL	Yes or No according to the instructions from the IT administrator

dc03rpl.rainpole.local is the on-site ROBO Active Directory domain controller.

- b Click **Test Connection** to verify the connection, and click **Save**.

Install a CA-Signed Certificate on vRealize Log Insight in ROBO

vRealize Log Insight comes with a default self-signed certificate that is generated and signed at installation time. After you start vRealize Log Insight in the ROBO, install a CA-signed certificate to secure the communication of vRealize Log Insight.

vRealize Log Insight uses a certificate for the following communication:

- Connection to the vRealize Log Insight UI
- SSL syslog transfers
- Communication from the Log Insight agents through the Ingestion API

vRealize Log Insight accepts only PEM encoded certificates that include the complete certification chain. The private key must not be encrypted by a pass phrase.



Replace the Certificate to vRealize Log Insight in ROBO

After you generate the PEM certificate chain file that contains the own certificate, the signer certificate and the private key file, upload the certificate chain to vRealize Log Insight in the ROBO.

Procedure

- 1 Log in to the vRealize Log Insight user interface.
 - a Open a Web browser and go to **https://nyc01vrli01-cluster01.rainpole.local**.
 - b Log in using the following credentials.

Setting	Value
User name	admin
Password	vrli_admin_password

- 2 In the vRealize Log Insight UI, click the configuration drop-down menu icon  and select **Administration**.
- 3 Under **Configuration**, click **SSL**.
- 4 On the **SSL Configuration** page, next to **New Certificate File (PEM format)** click **Choose File**, browse to the location of the `vrli.nyc01.2.chain.pem` file on your computer, and click **Save**.
The certificate is uploaded to vRealize Log Insight.
- 5 In a Web browser, go to **https://nyc01vrli01-cluster01.rainpole.local**.
A warning message that the connection is not trusted appears.
- 6 To review the certificate, click the padlock  icon in the address bar of the browser, and verify that the **Subject Alternative Name** contains the names of the vRealize Log Insight cluster nodes.
- 7 Import the certificate in your Web browser.

For example, in Google Chrome under the **HTTPS/TLS** settings click the **Manage certificates** button, and in the **Certificates** dialog box import `vrli.lax01.2.chain.pem`.

You can also use Certificate Manager on Windows or Keychain Access on MAC OS X.

Connect vRealize Log Insight to the vSphere Environment in ROBO

Start collecting log information about the ESXi and vCenter Server instances in the ROBO.

Procedure

1 Configure User Privileges in vSphere for Integration with vRealize Log Insight for ROBO

Assign global permissions in the ROBO to the operations service account svc-loginsight in order to collect log information from the vCenter Server instance and ESXi hosts using vRealize Log Insight. The svc-loginsight user account is specifically dedicated to collecting log information from vCenter Server and ESXi. Global permissions provide a consistent mechanism to define permissions across the ROBO.

2 Connect vRealize Log Insight to vSphere in ROBO

After you configure the svc-loginsight AD user with the vSphere privileges that are required for retrieving log information from the vCenter Server instance and ESXi hosts, in the ROBO connect vRealize Log Insight to vSphere.

3 Configure vCenter Server to Forward Log Events to vRealize Log Insight in ROBO

You can configure the ROBO vCenter Server appliance to forward system logs and events to the vRealize Log Insight cluster. You can then view and analyze all syslog information in the vRealize Log Insight Web interface.

Configure User Privileges in vSphere for Integration with vRealize Log Insight for ROBO

Assign global permissions in the ROBO to the operations service account svc-loginsight in order to collect log information from the vCenter Server instance and ESXi hosts using vRealize Log Insight. The svc-loginsight user account is specifically dedicated to collecting log information from vCenter Server and ESXi. Global permissions provide a consistent mechanism to define permissions across the ROBO.

Procedure

1 Log in to vCenter Server by using the vSphere Web Client.

- a Open a Web browser and go to **`https://nyc01vc01.rainpole.local/vsphere-client`**.
- b Log in using the following credentials.

Setting	Value
User name	administrator@vsphere.local
Password	vsphere_admin_password

2 From the **Home** menu, select **Administration**.

3 Under **Access Control**, click **Roles**.

4 Create a role for vRealize Log Insight.

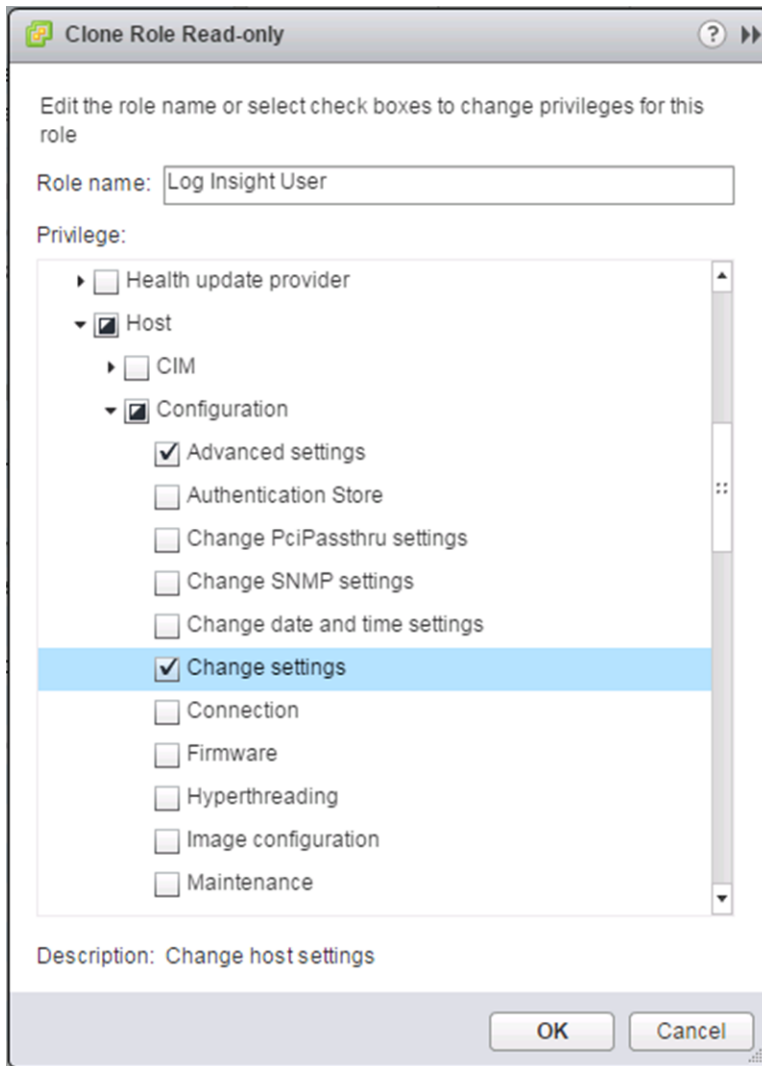
- a Select **Read-only** and click the **Clone** icon.

You clone the Read-only role because it includes the **System.Anonymous**, **System.View**, and **System.Read** privileges. vRealize Log Insight requires those privileges for accessing log information related to the vCenter Server instances.

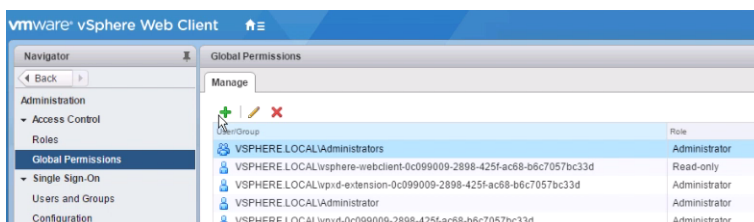
- b In the **Clone Role Read-only** dialog box, complete the configuration of the role and click **OK**.

Setting	Description
Role name	Log Insight User
Privilege	<ul style="list-style-type: none">■ Host.Configuration.Advanced settings■ Host.Configuration.Change settings■ Host.Configuration.Network configuration■ Host.Configuration.Security profile and firewall <p>The following privileges are inherited from the Read-only role.</p> <ul style="list-style-type: none">■ System.Anonymous■ System.View■ System.Read

These host privileges allow vRealize Log Insight to configure the syslog service on the ESXi hosts.

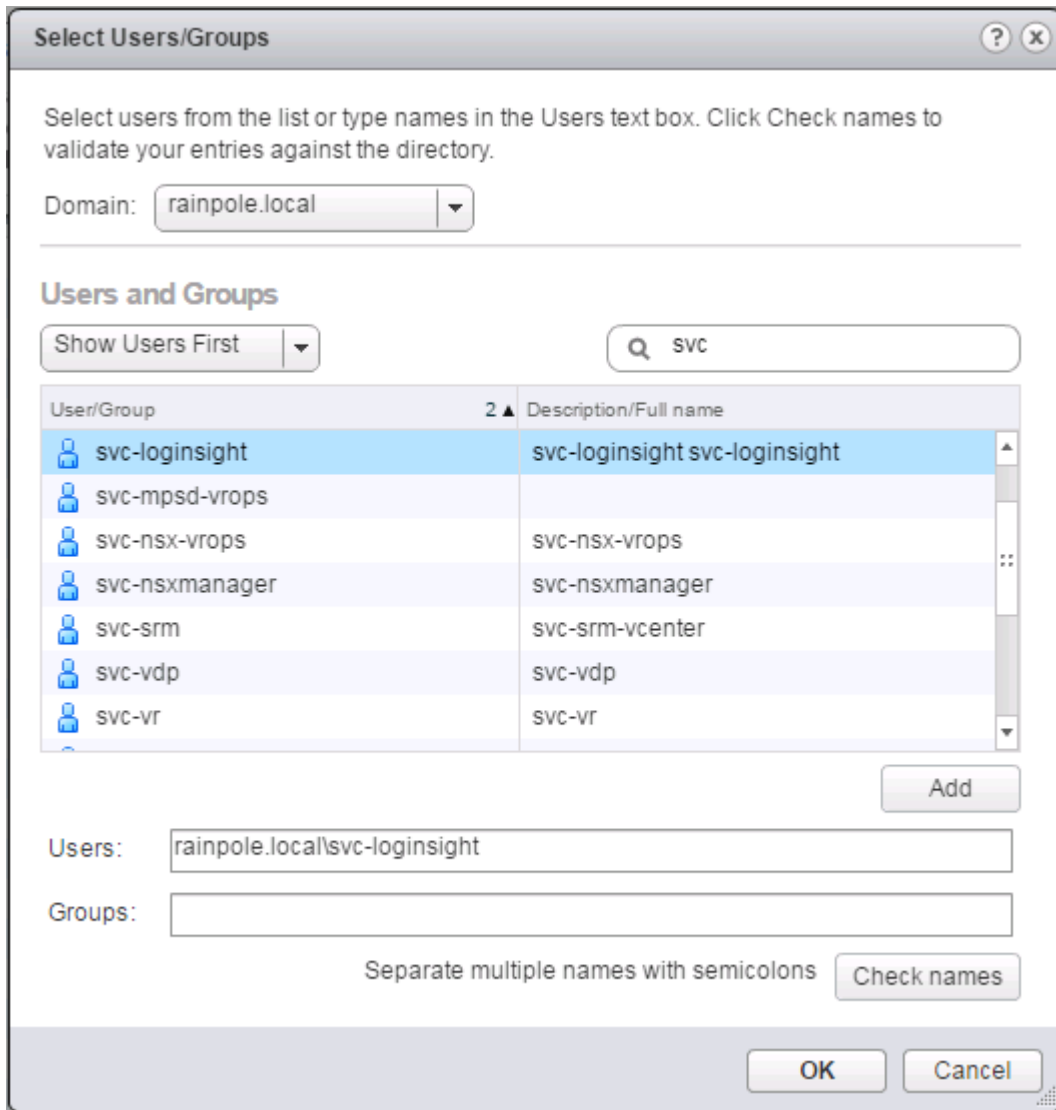


- 5 Assign global permissions to the svc-loginsight@rainpole.local service account.
 - a In the vSphere Web Client, select **Administration** from the **Home** menu and click **Global Permissions** under **Access Control**.
 - b On the **Manage** tab, click **Add Permission**.



- c In the **Global Permissions Root - Add Permission** dialog box, click **Add** to associate a user or a group with a role.

- d In the **Select Users/Groups** dialog box, from the **Domain** drop-down menu, select **rainpole.local**, in the filter box type **svc**, and press Enter.
- e From the list of users and groups, select the **svc-loginsight** user, click **Add**, and click **OK**.



- f In the **Add Permission** dialog box, from the **Assigned Role** drop-down menu, select **Log Insight User**, select **Propagate to children**, and click **OK**.

The global permissions of the svc-loginsight@rainpole.local user propagate to vSphere objects.


Connect vRealize Log Insight to vSphere in ROBO

After you configure the svc-loginsight AD user with the vSphere privileges that are required for retrieving log information from the vCenter Server instance and ESXi hosts, in the ROBO connect vRealize Log Insight to vSphere.

Procedure

- 1 Log in to the vRealize Log Insight user interface.
 - a Open a Web browser and go to **https://nyc01vrli01-cluster01.rainpole.local**.
 - b Log in using the following credentials.

Setting	Value
User name	admin
Password	vrli_admin_password

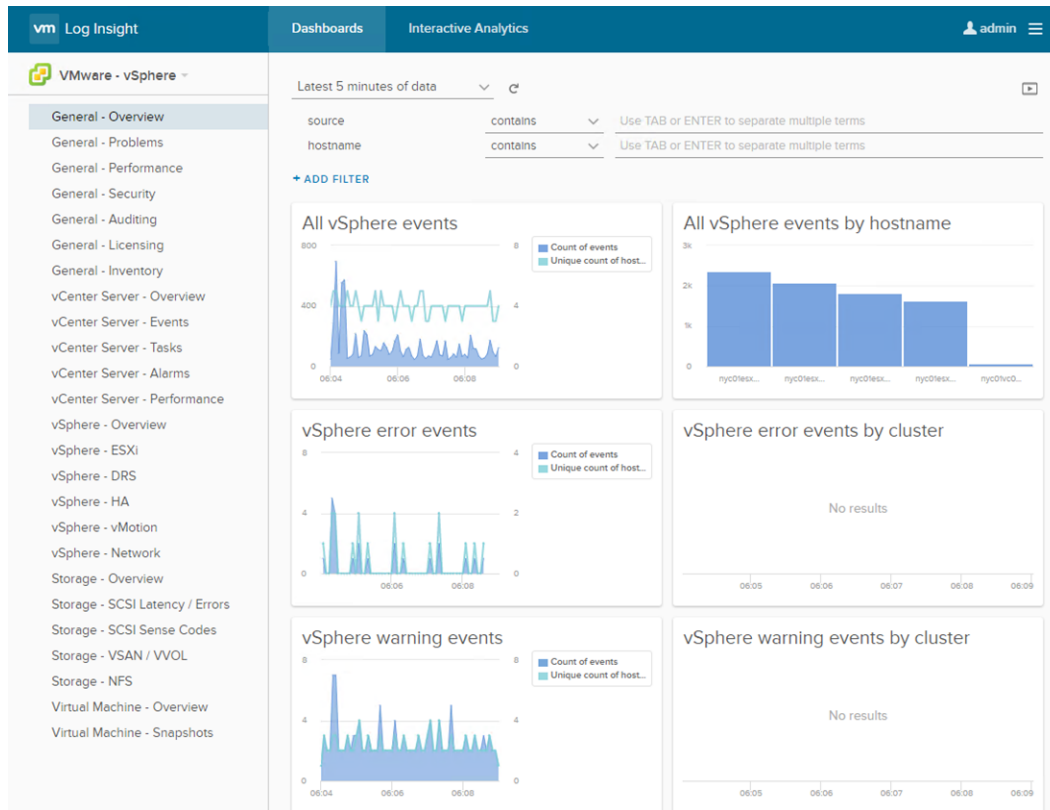
- 2 Click the configuration drop-down menu icon  and select **Administration**.
- 3 Under **Integration**, click **vSphere**.
- 4 In the **vCenter Servers** pane, enter the connection settings for the ROBO vCenter Server.
 - a Enter the host name, user credentials, and collection options for the vCenter Server instances, and click **Test Connection**.

vCenter Server Option	Value
Hostname	nyc01vc01.rainpole.local
Username	svc-loginsight@rainpole.local
Password	svc-loginsight_user_password
Collect vCenter Server events, tasks and alarms	Selected
Configure ESXi hosts to send logs to Log Insight	Selected

- b Click **Advanced Options** and examine the list of ESXi hosts that are connected to the vCenter Server instance to verify that you connect to the correct vCenter Server.
- 5 Click **Save**.

A progress dialog box appears.
- 6 Click **OK** in the confirmation dialog box that appears after vRealize Log Insight contacts the vCenter Server instance.

You see the vSphere dashboards under the **VMware - vSphere** content pack dashboard category.



Configure vCenter Server to Forward Log Events to vRealize Log Insight in ROBO

You can configure the ROBO vCenter Server appliance to forward system logs and events to the vRealize Log Insight cluster. You can then view and analyze all syslog information in the vRealize Log Insight Web interface.

Procedure

- 1 Redirect the log events from the ROBO vCenter Server appliance to vRealize Log Insight.
 - a Open a Web browser and go to **`https://nyc01vc01.rainpole.local:5480`**.
 - b Log in using the following credentials.

Setting	Value
User name	root
Password	<i>mgmtvc_root_password</i>

- c In the **Navigator**, click **Syslog Configuration**.
- d On the **Syslog Configuration** page, click **Edit**, configure the following settings, and click **OK**.

Setting	Value
Common Log Level	*
Remote Syslog Host	nyc01vrli01-cluster01.rainpole.local
Remote Syslog Port	514
Remote Syslog Protocol	UDP

- 2 Verify that the appliances are forwarding their syslog traffic to vRealize Log Insight.
 - a Open a Web browser and go to **https://nyc01vrli01-cluster01.rainpole.local**.
 - b Log in using the following credentials.

Setting	Value
User name	admin
Password	vrli_admin_password

- c In the vRealize Log Insight user interface, click **Dashboards** and select **VMware - vSphere** from the content pack dashboard drop-down menu.
- d Verify that the vCenter Server and Platform Services Controller nodes are present on the **All vSphere events by hostname** widget of the **General Overview** dashboard.

Connect vRealize Log Insight to vRealize Operations Manager in ROBO

Install and configure the vRealize Log Insight Content Pack for vRealize Operations Manager in the ROBO for troubleshooting vRealize Operations Manager by using dashboards and alerts in the vRealize Log Insight UI.

Procedure

- 1 [Enable the Integration of vRealize Log Insight in ROBO with vRealize Operations Manager](#)
Connect vRealize Log Insight in the ROBO with vRealize Operations Manager in the hub to launch vRealize Log Insight for ROBO from within vRealize Operations Manager and to send alerts to vRealize Operations Manager.
- 2 [Install the vRealize Log Insight Content Pack for vRealize Operations Manager in ROBO](#)
Install the content pack for vRealize Operations Manager to add the dashboards for viewing log information in vRealize Log Insight in the ROBO.

3 Configure the Log Insight Agent on vRealize Operations Manager to Forward Log Events to vRealize Log Insight in ROBO

After you install the content pack for vRealize Operations Manager, configure the Log Insight agent on the remote collector nodes of vRealize Operations Manager in the ROBO to send audit logs and system events to vRealize Log Insight.

Enable the Integration of vRealize Log Insight in ROBO with vRealize Operations Manager

Connect vRealize Log Insight in the ROBO with vRealize Operations Manager in the hub to launch vRealize Log Insight for ROBO from within vRealize Operations Manager and to send alerts to vRealize Operations Manager.


Prerequisites

- Verify that you have connected Realize Operations Manager in the Hub to the vCenter Server in ROBO.
- Verify that you have connected vRealize Log Insight in the ROBO to the vCenter Server in ROBO.
- Verify that you have configured the `svc-vrli-vrops@rainpole.local` service account within vRealize Operations Manager in the Hub.

Procedure

- 1 Log in to the vRealize Log Insight user interface.
 - a Open a Web browser and go to **`https://nyc01vrli01-cluster01.rainpole.local`**.
 - b Log in using the following credentials.

Setting	Value
User name	admin
Password	<i>vrli_admin_password</i>

- 2 In the vRealize Log Insight user interface, click the configuration drop-down menu icon  and select **Administration**.
- 3 Under **Integration**, click **vRealize Operations**.

- 4 On the **vRealize Operations Manager** pane, configure the integration settings for vRealize Operations Manager.
 - a Enter the host name and the user credentials for the vRealize Operations Manager instances.

vRealize Operations Manager Option	Value
Hostname	vrops-cluster-01.rainpole.local
Username	svc-vrli-vrops@rainpole.local
Password	svc-vrli-vrops_password

- b Click **Test Connection**.
 - c Select the **Enable alerts integration** check box.
- 5 Click **Save**.

A progress dialog box appears.


Install the vRealize Log Insight Content Pack for vRealize Operations Manager in ROBO

Install the content pack for vRealize Operations Manager to add the dashboards for viewing log information in vRealize Log Insight in the ROBO.

Procedure

- 1 Log in to the vRealize Log Insight user interface.
 - a Open a Web browser and go to **https://nyc01vrli01-cluster01.rainpole.local**.
 - b Log in using the following credentials.

Setting	Value
User name	admin
Password	vrli_admin_password

- 2 In the vRealize Log Insight user interface, click the configuration drop-down menu icon  and select **Content Packs**.
- 3 Under **Content Pack Marketplace**, select **Marketplace**.
- 4 In the list of content packs, locate the **VMware - vRops 6.x** content pack and click its icon.
- 5 In the **Install Content Pack** dialog box, accept the License Agreement, and click **Install**.

After the installation is complete, the **VMware - vRops 6.x** content pack appears in the **Installed Content Pack** list on the left.

Configure the Log Insight Agent on vRealize Operations Manager to Forward Log Events to vRealize Log Insight in ROBO

After you install the content pack for vRealize Operations Manager, configure the Log Insight agent on the remote collector nodes of vRealize Operations Manager in the ROBO to send audit logs and system events to vRealize Log Insight.

Procedure

- 1 On your computer, create a `liagent.ini` file for each of the 2 remote collector nodes of vRealize Operations Manager in the ROBO.

You can place each file in a node-specific folder.

- a Create an empty `liagent.ini` file and paste the following template configuration.

```
; Client-side configuration of VMware Log Insight Agent
; See liagent-effective.ini for the actual configuration used by VMware Log Insight Agent

[server]
; Log Insight server hostname or ip address
; If omitted the default value is LOGINSIGHT
hostname=<YOUR LOGINSIGHT HOSTNAME HERE>

; Set protocol to use:
; cfapi - Log Insight REST API
; syslog - Syslog protocol
; If omitted the default value is cfapi
;
;proto=cfapi

; Log Insight server port to connect to. If omitted the default value is:
; for syslog: 512
; for cfapi without ssl: 9000
; for cfapi with ssl: 9543
;port=9000

;ssl - enable/disable SSL. Applies to cfapi protocol only.
; Possible values are yes or no. If omitted the default value is no.
;ssl=no

; Time in minutes to force reconnection to the server
; If omitted the default value is 30
;reconnect=30

[storage]
;max_disk_buffer - max disk usage limit (data + logs) in MB:
; 100 - 2000 MB, default 200
;max_disk_buffer=200

[logging]
;debug_level - the level of debug messages to enable:
; 0 - no debug messages
; 1 - trace essential debug messages
```



```

; 2 - verbose debug messages (will have negative impact on performace)
;debug_level=0

[filelog|messages]
directory=/var/log
include=messages;messages.?

[filelog|syslog]
directory=/var/log
include=syslog;syslog.?

[filelog|COLLECTOR-collector]
tags = {"vmw_vr_ops_appname":"vROps",
"vmw_vr_ops_logtype":"COLLECTOR","vmw_vr_ops_clustername":"<YOUR CLUSTER NAME HERE>",
"vmw_vr_ops_clusterrole":"Master","vmw_vr_ops_nodename":"<YOUR NODE NAME HERE>",
"vmw_vr_ops_hostname":"<YOUR VROPS HOSTNAME HERE>"}
directory = /data/vcops/log
include = collector.log*
exclude_fields=hostname
event_marker=^\\d{4}-\\d{2}-\\d{2}[\\s]\\d{2}:\\d{2}:\\d{2}\\.\\d{3}

[filelog|COLLECTOR-collector_wrapper]
tags = {"vmw_vr_ops_appname":"vROps",
"vmw_vr_ops_logtype":"COLLECTOR","vmw_vr_ops_clustername":"<YOUR CLUSTER NAME HERE>",
"vmw_vr_ops_clusterrole":"Master","vmw_vr_ops_nodename":"<YOUR NODE NAME HERE>",
"vmw_vr_ops_hostname":"<YOUR VROPS HOSTNAME HERE>"}
directory = /data/vcops/log
include = collector-wrapper.log*
exclude_fields=hostname
event_marker=^\\d{4}-\\d{2}-\\d{2}[\\s]\\d{2}:\\d{2}:\\d{2}\\.\\d{3}

[filelog|COLLECTOR-collector_gc]
directory = /data/vcops/log
tags = {"vmw_vr_ops_appname":"vROps",
"vmw_vr_ops_logtype":"COLLECTOR","vmw_vr_ops_clustername":"<YOUR CLUSTER NAME HERE>",
"vmw_vr_ops_clusterrole":"Master","vmw_vr_ops_nodename":"<YOUR NODE NAME HERE>",
"vmw_vr_ops_hostname":"<YOUR VROPS HOSTNAME HERE>"}
include = collector-gc*.log*
exclude_fields=hostname
event_marker=^\\d{4}-\\d{2}-\\d{2}[\\w]\\d{2}:\\d{2}:\\d{2}\\.\\d{3}

[filelog|CALL_STACK-call_stack]
tags = {"vmw_vr_ops_appname":"vROps","vmw_vr_ops_logtype":"CALL_STACK",
"vmw_vr_ops_clustername":"<YOUR CLUSTER NAME HERE>","vmw_vr_ops_clusterrole":"Master",
"vmw_vr_ops_nodename":"<YOUR NODE NAME HERE>","vmw_vr_ops_hostname":"<YOUR VROPS HOSTNAME

```

```
HERE>"}
directory = /data/vcops/log/callstack
include = collector*.txt
exclude_fields=hostname
```

- b In the node-specific `liagent.ini` file, change the following parameters and save the file.

Parameter	Description	Location in <code>liagent.ini</code>	Configuration Instructions
<code>hostname</code>	IP address or FQDN of the Log Insight VIP	<code>[server]</code> section	Replace <code><YOUR LOGINSIGHT HOSTNAME HERE></code> with <code>nyc01vrli01-cluster01.rainpole.local</code> .
<code>proto</code>	Protocol that the agent uses to send events to the Log Insight server.	<code>[server]</code> section	Remove the <code>;</code> comment in front of the parameter to set the log protocol to <code>cfapi</code> .
<code>port</code>	Communication port that the agent uses to send events to the vRealize Log Insight server.	<code>[server]</code> section	Remove the <code>;</code> comment in front of the parameter to set the port to <code>9000</code> .
<code>vmw_vr_ops_clustername</code>	Name of the vRealize Operations Manager cluster	each <code>[filelog section_name]</code> section	Replace each <code><YOUR CLUSTER NAME HERE></code> with <code>vroops-cluster-01</code> .
<code>vmw_vr_ops_clusterrole</code>	Role of the vRealize Operations Manager node	each <code>[filelog section_name]</code> section	Set to <code>Remote Collector</code> .
<code>vmw_vr_ops_nodename</code>	Name of the vRealize Operations Manager node that is set during node initial configuration	each <code>[filelog section_name]</code> section	Replace each <code><YOUR NODE NAME HERE></code> with the following name: <ul style="list-style-type: none"> ■ <code>nyc01rmtcol01</code> for remote collector 1 ■ <code>nyc01rmtcol01</code> for remote collector 2
<code>vmw_vr_ops_hostname</code>	IP address or FQDN of the vRealize Operations Manager node	each <code>[filelog section_name]</code> section	Replace each <code><YOUR VROPS HOSTNAME NAME HERE></code> with the following FQDN: <ul style="list-style-type: none"> ■ <code>nyc01rmtcol01.rainpole.local</code> for remote collector 1 ■ <code>nyc01rmtcol01.rainpole.local</code> for remote collector 2

You change the `[server]` section as follows.

```
[server]
; Log Insight server hostname or ip address
; If omitted the default value is LOGINSIGHT
hostname=nyc01vrli01-cluster01.rainpole.local
```

```

; Set protocol to use:
; cfapi – Log Insight REST API
; syslog – Syslog protocol
; If omitted the default value is cfapi
;
proto=cfapi
; Log Insight server port to connect to. If omitted the default value is:
; for syslog: 512
; for cfapi without ssl: 9000
; for cfapi with ssl: 9543
port=9000
;ssl – enable/disable SSL. Applies to cfapi protocol only.
; Possible values are yes or no. If omitted the default value is no.
;ssl=no
; Time in minutes to force reconnection to the server
; If omitted the default value is 30
;reconnect=30

```

For example, on the remote collector node `vrops-rmtcol-51` you change the `[filelog|ANALYTICS-analytics]` section that is related to the logs files of the analytics module as follows.

```

[filelog|ANALYTICS-analytics]
tags = {"vmw_vr_ops_appname":"vROps",
"vmw_vr_ops_logtype":"COLLECTOR","vmw_vr_ops_clustername":"vrops-cluster-01",
"vmw_vr_ops_clusterrole":"Remote Collector","vmw_vr_ops_nodename":"nyc01rmtcol01",
"vmw_vr_ops_hostname":"nyc01rmtcol01.rainpole.local"}
directory = /data/vcops/log
include = analytics*.log*
exclude_fields=hostname

```

2 Enable SSH on each node of vRealize Operations Manager.

- a Open a Web browser and go to **`https://nyc01vc01.rainpole.local/vsphere-client`**.
- b Log in using the following credentials.

Setting	Value
User name	administrator@vsphere.local
Password	vsphere_admin_password

- c Under the **`nyc01vc01.rainpole.local`** vCenter Server, navigate to the virtual appliance for the node.

Virtual Appliance Name	Role
nyc01rmtcol01	Remote collector 1
nyc01rmtcol02	Remote collector 2

- d Right-click the appliance node and select **Open Console** to open the remote console to the appliance.
- e Press ALT+F1 to switch to the command prompt.

- f Log in using the following credentials.

Setting	Value
User name	root
Password	<i>vrops_root_password</i>

- g Start the SSH service by running the command.

```
service sshd start
```

- h Close the virtual appliance console.

3 Apply the Log Insight agent configuration.

- a On the appliance, replace the `liagent.ini` file in the `/var/lib/loginsight-agent` folder with the node-specific file on your computer.

You can use `scp`, FileZilla or WinSCP.

- b Restart the Log Insight agent on node by running the following console command as the root user.

```
/etc/init.d/liagentd restart
```

- c After restarting the agent, review the `liagent-effective.ini` to ensure that the uploaded `liagent.ini` file has been ingested by the daemon.

```
less liagent-effective.ini
```

- d Stop the SSH service on the virtual appliance by running the following command.


```
service sshd stop
```

4 Repeat the steps on the second remote collector node.

5 Configure the Linux Agent Group for the vRealize Operations Manager components from the vRealize Log Insight Web user interface.

- a Open a Web browser and go to **`https://nyc01vrli01-cluster01.rainpole.local`**.
- b Log in using the following credentials.

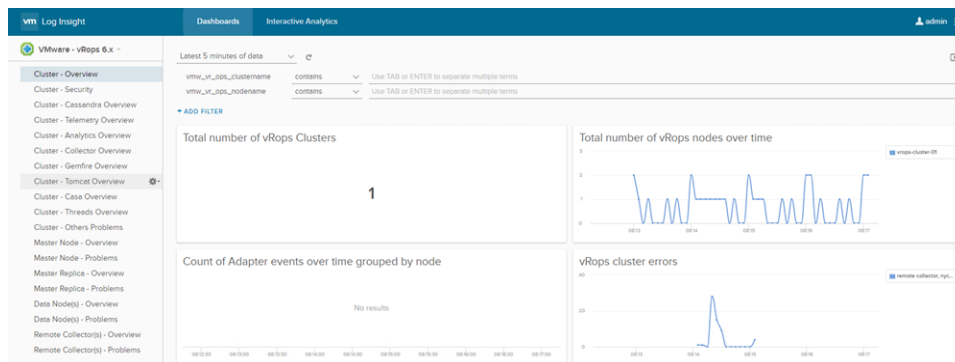
Setting	Value
User name	admin
Password	<i>vrli_admin_password</i>

- c Click the  configuration drop-down menu icon and select **Administration**.
- d Under **Management**, click **Agents**.

- e From the drop-down menu on the top, select **vRops 6.x - Sample** from the **Available Templates** section.
- f Click **Copy Template**.
- g In the **Copy Agent Group** dialog box, enter **vRops6 – Agent Group** in the name field and click **Copy**.
- h In the **agent filter** fields, enter the following values pressing Enter after each host name.

Filter	Operator	Value
Hostname	matches	■ nyc01rmtcol01.rainpole.local
		■ nyc01rmtcol02.rainpole.local
- i Click **Refresh** and verify that all the agents in the filter appear in the **Agents** list.
- j Click **Save New Group** at the bottom of the page.
- k Click the **Dashboard** tab and select the **VMware - vRops 6.x** dashboard from the drop-down menu on the left.

You see log information about the operation of the remote collectors of vRealize Operations Manager in ROBO on the **VMware - vRops 6.x** Log Insight dashboards.



Connect vRealize Log Insight to the NSX Instances in ROBO

Install and configure the vRealize Log Insight Content Pack for NSX for vSphere for log visualization and alerting of the NSX for vSphere real-time operation in the ROBO. You can use the NSX-vSphere dashboards to monitor logs about installation and configuration, and about virtual networking services.

Procedure

1 Install the vRealize Log Insight Content Pack for NSX for vSphere in ROBO

Install the content pack for NSX for vSphere to add the dashboards for viewing log information in vRealize Log Insight in the ROBO.

2 Configure NSX Managers to Forward Log Events to vRealize Log Insight in ROBO

Configure the NSX Manager for the ROBO cluster to send audit logs and system events to vRealize Log Insight that is deployed in the ROBO.

3 Configure the NSX Controllers to Forward Events to vRealize Log Insight in ROBO

Configure the NSX Controller instances for the ROBO cluster to forward log information to vRealize Log Insight in the ROBO by using the NSX REST API. You can use a REST client, such as the RESTClient add-on for Firefox, to enable log forwarding.

4 Configure the NSX Edge Instances to Forward Log Events to vRealize Log Insight in ROBO

Configure the NSX Edge logical router and service gateways for vRealize Operations Manager, vRealize Log Insight and vRealize Automation to forward log information to vRealize Log Insight in the ROBO.


Install the vRealize Log Insight Content Pack for NSX for vSphere in ROBO

Install the content pack for NSX for vSphere to add the dashboards for viewing log information in vRealize Log Insight in the ROBO.

Procedure

- 1 Log in to the vRealize Log Insight user interface.
 - a Open a Web browser and go to **https://nyc01vrli01-cluster01.rainpole.local**.
 - b Log in using the following credentials.

Setting	Value
User name	admin
Password	<i>vrli_admin_password</i>

- 2 In the vRealize Log Insight user interface, click the configuration drop-down menu icon  and select **Content Packs**.
- 3 Under **Content Pack Marketplace**, select **Marketplace**.
- 4 In the list of content packs, locate the **VMware - NSX-vSphere** content pack and click its icon.
- 5 In the **Install Content Pack** dialog box, accept the **License Agreement**, and click **Install**.

After the installation is complete, the **VMware - NSX-vSphere** content pack appears in the **Installed Content Packs** list on the left.

Configure NSX Managers to Forward Log Events to vRealize Log Insight in ROBO

Configure the NSX Manager for the ROBO cluster to send audit logs and system events to vRealize Log Insight that is deployed in the ROBO.

Procedure

- 1 On the Windows machine that has access to the ROBO infrastructure, log in to the NSX Manager Web Interface.
 - a Open a Web browser and go to **`https://nyc01nsxm01.rainpole.local`**.
 - b Log in using the following credentials.

Setting	Value
User name	admin
Password	<i>nycnsx_manager_admin_password</i>

- 2 On the main page of the appliance user interface, click **Manage Appliance Settings**.
- 3 Under **Settings**, click **General**, and in the **Syslog Server** pane, click **Edit**.
- 4 In the **Syslog Server** dialog box, configure the ROBO vRealize Log Insight as a syslog server by specifying the following settings and click **OK**.

Syslog Server Setting	Value
Syslog Server	nyc01vrli01-cluster01.rainpole.local
Port	514
Protocol	UDP

Configure the NSX Controllers to Forward Events to vRealize Log Insight in ROBO

Configure the NSX Controller instances for the ROBO cluster to forward log information to vRealize Log Insight in the ROBO by using the NSX REST API. You can use a REST client, such as the RESTClient add-on for Firefox, to enable log forwarding.

Prerequisites

On a Windows host that has access to your data center, install a REST client, such as the RESTClient add-on for Firefox or Postman add-on for Chrome.

Procedure

- 1 Log into the Windows machine that has access to the ROBO data center.
- 2 In a Firefox browser, go to **`chrome://restclient/content/restclient.html`**.

3 Specify the request headers for requests to the NSX Manager.

- a From the **Authentication** drop-down menu, select **Basic Authentication**.
- b In the **Basic Authorization** dialog box, enter the following credentials, select **Remember me** and click **Okay**.

Authentication Attribute	Value
Username	admin
Password	<i>nycnsx_admin_password</i>

The Authorization:Basic XXX header appears in the **Headers** pane.

- c From the **Headers** drop-down menu, select **Custom Header**.
- d In the **Request Header** dialog box, enter the following header details and click **Okay**.

Request Header Attribute	Value
Name	Content-Type
Value	application/xml

The Content-Type:application/xml header appears in the **Headers** pane.

4 Contact the NSX Manager to retrieve the IDs of the associated NSX Controllers.

- a In the **Request** pane, from the **Method** drop-down menu, select **GET**.
- b In the **URL** text box, enter the following URL, and click **Send**.

NSX Manager	URL
NSX Manager for the ROBO cluster	https://nyc01nsxm01.rainpole.local/api/2.0/vdn/controller

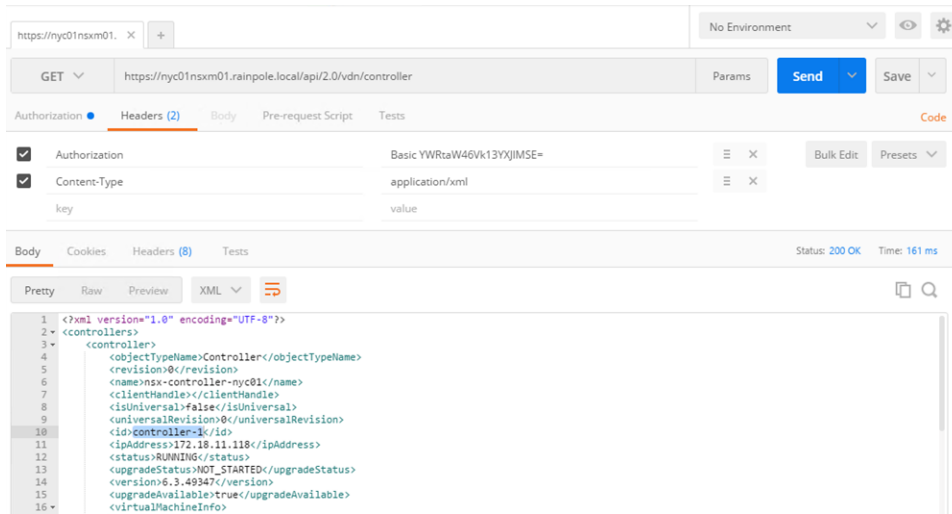
The RESTClient sends a query to the NSX Manager about the installed NSX controllers.

- c After the NSX Manager sends a response back, click the **Response Body (Preview)** tab under **Response**.

The response body contains a root `<controllers>` XML element that groups the details about the three controllers that form the controller cluster.

- d Within the `<controllers>` element, locate the `<controller>` element for each controller and write down the content of the `id` element.

Controller IDs have the `controller-id` format where *id* represents the sequence number of the controller in the cluster, for example, `controller-2`.



5 For each NSX Controller, send a request to configure vRealize Log Insight as a remote syslog server.

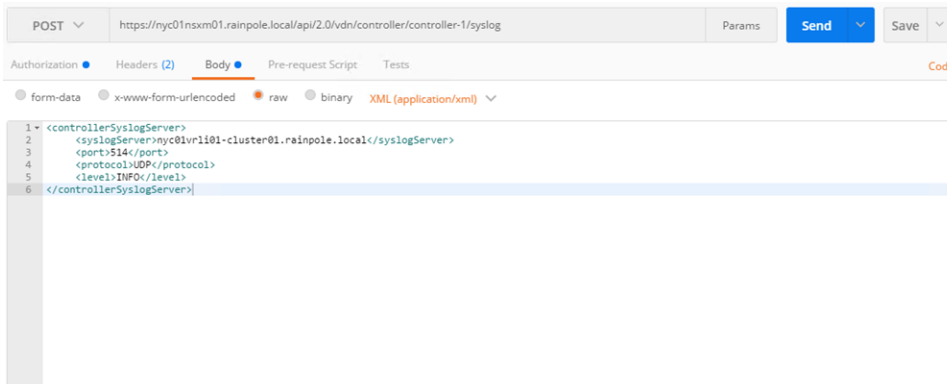
- a In the **Request** pane, from the **Method** drop-down menu, select **POST**, and in the **URL** text box, enter the following URL.

NSX Manager	NSX Controller in the Controller Cluster	POST URL
NSX Manager for the ROBO cluster	NSX Controller 1	https://nyc01nsxm01.rainpole.local/api/2.0/vdn/controller/controller-1/syslog
	NSX Controller 2	https://nyc01nsxm01.rainpole.local/api/2.0/vdn/controller/controller-2/syslog
	NSX Controller 3	https://nyc01nsxm01.rainpole.local/api/2.0/vdn/controller/controller-3/syslog

- b In the **Request** pane, paste the following request body in the **Body** text box and click **Send**.

```
<controllerSyslogServer>
  <syslogServer>nyc01vrli01-cluster01.rainpole.local</syslogServer>
  <port>514</port>
  <protocol>UDP</protocol>
  <level>INFO</level>
</controllerSyslogServer>
```

- c Repeat the steps for the next NSX Controller.



6 Verify the syslog configuration on each NSX Controller.

- a In the **Request** pane, from the **Method** drop-down menu, select **GET**, and in the **URL** text box, enter the controller-specific syslog URL from [Step 5](#).
- b After the NSX Manager sends a response back, click the **Response Body (Preview)** tab under **Response**.

The response body contains a root `<controllerSyslogServer>` element that represents the settings for the remote syslog server on the NSX Controller.

- c Verify that the value of the <syslogServer> element is nyc01vrli01-cluster01.rainpole.local.

GET https://nyc01nsxm01.rainpole.local/api/2.0/vdn/controller/controller-1/syslog

Authorization: Basic Auth

Username: admin

Password: *****

Body (XML):

```

1 <?xml version="1.0" encoding="UTF-8"?>
2 <controllerSyslogServer>
3   <syslogServer>nyc01vrli01-cluster01.rainpole.local</syslogServer>
4   <port>514</port>
5   <protocol>UDP</protocol>
6   <level>INFO</level>
7 </controllerSyslogServer>

```

- d Repeat the steps for the next NSX Controller.

Configure the NSX Edge Instances to Forward Log Events to vRealize Log Insight in ROBO

Configure the NSX Edge logical router and service gateways for vRealize Operations Manager, vRealize Log Insight and vRealize Automation to forward log information to vRealize Log Insight in the ROBO.

Procedure

- 1 Log in to vCenter Server by using the vSphere Web Client.
 - a Open a Web browser and go to **https://nyc01vc01.rainpole.local/vsphere-client**.
 - b Log in using the following credentials.

Setting	Value
User name	administrator@vsphere.local
Password	vsphere_admin_password

- 2 From the **Home** menu, select **Networking & Security**.
- 3 From the **Networking & Security** menu on the left, click **NSX Edges**.
- 4 On the **NSX Edges** page, select the NSX Manager instance from the **NSX Manager** drop-down menu.

NSX Manager Instance	IP Address
NSX Manager for the ROBO cluster	172.18.11.65

The edge devices in the scope of the NSX Manager appear.

5 Configure the log forwarding on each edge service gateway.

- a Double-click the edge device to open its user interface.

ROBO NSX Edge Service Gateway
NYC01-ESG01
NYC01-ESG02
NYC01-DLR01

- b On the NSX edge device page, click the **Manage** tab, click **Settings** and click **Configuration**.
- c In the **Details** panel, click **Change** next to **Syslog servers**.
- d In the **Edit Syslog Servers Configuration** dialog box, configure the following settings and click **OK**.

Setting	Value
Syslog server 1	172.18.19.10
Protocol	udp

- e Repeat the steps for the other NSX edge devices.

The vRealize Log Insight user interface in ROBO starts showing log data in the **NSX-vSphere-Overview** dashboard available under the **VMware - NSX-vSphere** group of content pack dashboards.

Connect vRealize Log Insight to vRealize Automation in ROBO

Connect the vRealize Log to vRealize Automation to receive log information from the components of vRealize Automation in the ROBO in the vRealize Log Insight UI.

Procedure

1 [Install the vRealize Log Insight Content Pack for vRealize Automation in ROBO](#)

Install the following content pack for vRealize Automation to add the dashboards for viewing log information in vRealize Log Insight in the ROBO.

2 [Configure the vRealize Automation Proxy Agents to Forward Log Events to vRealize Log Insight in ROBO](#)

Install the vRealize Log Insight agent to collect and forward events to vRealize Log Insight in the ROBO on the Windows virtual machines for the vSphere proxy agents.


Install the vRealize Log Insight Content Pack for vRealize Automation in ROBO

Install the following content pack for vRealize Automation to add the dashboards for viewing log information in vRealize Log Insight in the ROBO.

Procedure

- 1 Log in to the vRealize Log Insight user interface.
 - a Open a Web browser and go to **https://nyc01vrli01-cluster01.rainpole.local**.
 - b Log in using the following credentials.

Setting	Value
User name	admin
Password	<i>vrli_admin_password</i>

- 2 In the vRealize Log Insight user interface, click the configuration drop-down menu icon  and select **Content Packs**.
- 3 Under **Content Pack Marketplace**, select **Marketplace**.
- 4 In the list of content packs, locate the **VMware - vRA 7** content pack and click its icon.
- 5 In the **Install Content Pack** dialog box, accept the licensing agreement and click **Install**.

After the installation is complete, the **VMware - vRA 7** content pack appears in the **Installed Content Packs** list on the left.

Configure the vRealize Automation Proxy Agents to Forward Log Events to vRealize Log Insight in ROBO

Install the vRealize Log Insight agent to collect and forward events to vRealize Log Insight in the ROBO on the Windows virtual machines for the vSphere proxy agents.

Procedure

- 1 Install Log Insight Windows Agents in all the vRealize Automation Windows VMs.

- a Open a Remote Desktop Protocol (RDP) connection to each of the following vRealize Automation virtual machines.


vRealize Automation Component	Host Name/VM Name
vSphere Proxy Agent	nyc01ias01.rainpole.local
vSphere Proxy Agent	nyc01ias02.rainpole.local

- b Log in using the following credentials.

Setting	Value
User name	Windows administrator user
Password	<i>windows_administrator_password</i>

- c On the Windows host, open a Web browser and go to **https://nyc01vrli01-cluster01.rainpole.local**.
- d Log in using the following credentials.


Setting	Value
User name	admin
Password	<i>vrli_admin_password</i>

- e Click the **Configuration** drop-down menu icon  and select **Administration**.
- f Under **Management**, click **Agents**.
- g On the **Agents** page, click the **Download Log Insight Agent Version** link.
- h In the **Download Log Insight Agent Version** dialog box, click **Windows MSI (32-bit/64-bit)** and save the Log Insight Agent.msi file to the Windows host.
- i Double-click the .msi file to run the installer.
- j In the **VMware vRealize Log Insight Agent Setup** wizard, accept the license agreement and click **Next**.
- k With the Log Insight host name **nyc01vrli01-cluster01.rainpole.local** shown in the **Host** text box, click **Install**.
- l When the installation is complete, click **Finish**.
- m Repeat this operation on the other vSphere Proxy Agent.

2 Configure the Log Insight Windows Agents Group from the vRealize Log Insight user interface.

- a Open a Web browser and go to **https://nyc01vrli01-cluster01.rainpole.local**.
- b Log in using the following credentials.

Setting	Value
User name	admin
Password	vrli_admin_password

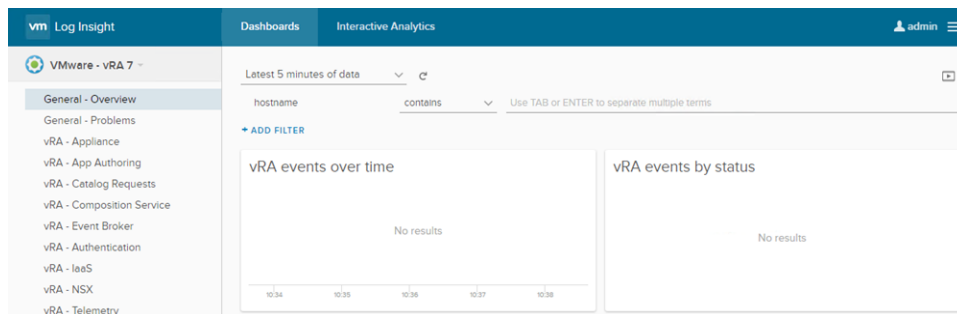
- c Click the configuration drop-down menu icon  and select **Administration**.
- d Under **Management**, click **Agents**.
- e From the drop-down on the top, select **vRealize Automation 7 - Windows** from the **Available Templates** section.
- f Click **Copy Template**.
- g In the **Copy Agent Group** dialog box, enter **vRA7 – Windows Agent Group** in the name text box and click **Copy**.
- h Configure the following agent filter.

Press Enter to separate the host names.

Filter	Operator	Values
Hostname	matches	nyc01ias01.rainpole.local nyc01ias02.rainpole.local

- i Click **Refresh** and verify that all the agents listed in the filter appear in the **Agents** list.
- j Click **Save New Group** at the bottom of the page.

All VMware vRA 7 dashboards become available on the vRealize Log Insight Home page.




Install the vRealize Log Insight Content Pack for vSAN in ROBO

Install the content pack for VMware vSAN to add the dashboards for viewing log information in vRealize Log Insight in the ROBO.

Procedure

- 1 Log in to the vRealize Log Insight user interface.
 - a Open a Web browser and go to **https://nyc01vrli01-cluster01.rainpole.local**.
 - b Log in using the following credentials.

Setting	Value
User name	admin
Password	vrli_admin_password

- 2 In the vRealize Log Insight user interface, click the configuration drop-down menu icon  and select **Content Packs**.
- 3 Under **Content Pack Marketplace**, select **Marketplace**.
- 4 In the list of content packs, locate the **VMware - vSAN** content pack and click its icon.
- 5 In the **Install Content Pack** dialog box accept the License Agreement, and click **Install**.

After the installation is complete, the **VMware - vSAN** content pack appears in the **Installed Content Packs** list on the left.

vSAN log information becomes available without additional configuration. The integration between vRealize Log Insight and vSphere accommodates the transfer of vSAN log information automatically.

Configure Event Forwarding From ROBO to Region A and Region B

According to vRealize Log Insight Design for ROBO, vRealize Log Insight forwards logging information to both Region A and Region B in the SDDC hub. In this way, both vRLI instances can ingest the ROBO logging data while still remaining independent of one another.

See *vRealize Log Insight Design and Logging Architecture* in the *VMware Validated Design Architecture and Design for Remote Office and Branch Office* documentation.

Procedure

- 1 [Configure Event Forwarding to Region A in ROBO](#)

You enable log forwarding from vRealize Log Insight in the ROBO to vRealize Log Insight in Region A and Region B to avoid losing ROBO-related logs in the event of disaster.
- 2 [Configure Event Forwarding to Region B in ROBO](#)

You enable log forwarding from vRealize Log Insight in the ROBO to vRealize Log Insight in Region B of the SDDC hub to prevent from losing ROBO-related logs in the event of disaster.

3 Add a Log Filter in Region A and Region B for ROBO

Add a filter to avoid creating a forwarding loop of ROBO logs between Region B and Region A. Using a filter prevents from looping when the Log Insight deployments in Region A and Region B forward logs to each other.

Configure Event Forwarding to Region A in ROBO

You enable log forwarding from vRealize Log Insight in the ROBO to vRealize Log Insight in Region A and Region B to avoid losing ROBO-related logs in the event of disaster.

You provide the following settings for log forwarding to vRealize Log Insight in Region B:

- Inject the SSL certificate for Region A and B in the Java keystore of each vRealize Log Insight node in ROBO.
- Target URL, protocol and tagging
- Disk cache

Disk cache represents the amount of local disk space to reserve for buffering events that you configure to be forwarded. Buffering is used when the remote destination is unavailable or unable to process the events being sent to it. If the local buffer becomes full and the remote destination is still unavailable, then the oldest local events are dropped and not forwarded to the remote destination even when the remote destination is back online.

Procedure

- 1 Import the root certificate from the vRealize Log Insight instance in Region A of the hub in the Java keystore on each vRealize Log Insight node in the ROBO.
 - a Open an SSH session to the vRealize Log Insight node.

Name	Role
nyc01vrli01.rainpole.local	Master node
nyc01vrli02.rainpole.local	Worker node 1
nyc01vrli03.rainpole.local	Worker node 2

- b Log in using the following credentials.

Setting	Value
User name	root
Password	<i>vrli_regionA_root_password</i>

- c Create a working directory on the vRealize Log Insight node.

```
mkdir /tmp/ssl
cd /tmp/ssl
```

- d Extract the root certificate from the destination vRealize Log Insight in the hub.

```
echo "" | openssl s_client -showcerts -servername vrli-mstr-01.sfo01.rainpole.local -connect
vrli-mstr-01.sfo01.rainpole.local:443 -prexit 2>/dev/null | sed -n -e '/BEGIN\
CERTIFICATE/,/END\ CERTIFICATE/ p' > cert.pem

csplit -f individual- cert.pem '/-----BEGIN CERTIFICATE-----/' '{*}'

root_cert=$(ls individual-* | sort -n -t- | tail -1)

cp -f -- "$root_cert" root.crt
```

- e Import the `root.crt` in the Java keystore of the vRealize Log Insight node.

```
cd /usr/java/default/lib/security/

../../bin/keytool -import -alias loginsight -file /tmp/ssl/root.crt -keystore cacerts
```

- f When prompted for a keystore password, type **changeit**

- g When prompted to accept the certificate, type **yes** .

- 2 Run `reboot` to restart the appliance.

- 3 Repeat [Step 1](#) to [Step 2](#) on the other vRealize Log Insight nodes in the ROBO.


Wait until all appliances are running again.

- 4 Log in to the vRealize Log Insight user interface.

- a Open a Web browser and go to **`https://nyc01vrli01-cluster01.rainpole.local`**.

- b Log in using the following credentials.

Setting	Value
User name	admin
Password	<i>vrli_admin_password</i>

- 5 In the vRealize Log Insight user interface, click the configuration drop-down menu icon  and select **Administration**.

- 6 Under **Management**, click **Event Forwarding**.

- 7 On the **Event Forwarding** page, click **New Destination** and enter the following forwarding settings in the **New Destination** dialog box.

Forwarding Destination Setting	Value
Name	NYC01 to SFO01
Host	vrli-cluster-01.sfo01.rainpole.local
Protocol	Ingestion API
Use SSL	Selected

Forwarding Destination Setting	Value
Tags	site='NYC01'
Advanced Settings	
Port	9543
Disk Cache	2000 MB
Worker Count	8

New Destination

Name

Host

Protocol ☒ Use SSL ⓘ

Tags ⓘ

☒ Forward complementary tags ⓘ

Filter *Forward all events* ⓘ

[+ ADD FILTER](#)

[Hide Advanced Settings](#)

Port ⓘ

Disk Cache MB ⓘ

Worker Count ⓘ

Test event forwarded successfully

- 8 In the **New Destination** dialog box, click **Test** to verify that the connection settings are correct.
- 9 Click **Save** to save the forwarding new destination.

The **Event Forwarding** page in the vRealize Log Insight user interface starts showing a summary of the forwarded events.

Configure Event Forwarding to Region B in ROBO

You enable log forwarding from vRealize Log Insight in the ROBO to vRealize Log Insight in Region B of the SDDC hub to prevent from losing ROBO-related logs in the event of disaster.

You provide the following settings for log forwarding in vRealize Log Insight in the ROBO:

- Target URL, protocol and tagging
- Filtering

Add a filter to avoid forwarding log events back to the Log Insight deployment in Region A. Using a filter prevents from looping when the Log Insight deployments in Region A and Region B forward logs to each other.


- Disk cache

Disk cache represents the amount of local disk space to reserve for buffering events that you configure to be forwarded. Buffering is used when the remote destination is unavailable or unable to process the events being sent to it. If the local buffer becomes full and the remote destination is still unavailable, then the oldest local events are dropped and not forwarded to the remote destination even when the remote destination is back online.

Procedure

- 1 Log in to the vRealize Log Insight user interface.
 - a Open a Web browser and go to **`https://nyc01vrli01-cluster01.rainpole.local`**.
 - b Log in using the following credentials.

Setting	Value
User name	admin
Password	<i>vrli_admin_password</i>

- 2 In the vRealize Log Insight user interface, click the configuration drop-down menu icon  and select **Administration**.
- 3 Under **Management**, click **Event Forwarding**.
- 4 On the **Event Forwarding** page, click **New Destination** and enter the following forwarding settings in the New Destination dialog box.

Forwarding Destination Option	Value
Name	NYC01 to LAX01
Host	vrli-cluster-51.lax01.rainpole.local
Protocol	Ingestion API
Use SSL	Selected
Tags	site='NYC01'

Forwarding Destination Option	Value
Advanced Settings	
Port	9543
Disk Cache	2000 MB
Worker Count	8

- 5 In the **New Destination** dialog box, click **Test** to verify that the connection settings are correct.
- 6 Click **Save** to save the forwarding new destination.

The **Event Forwarding** page in the vRealize Log Insight user interface starts showing a summary of the forwarded events.

Add a Log Filter in Region A and Region B for ROBO

Add a filter to avoid creating a forwarding loop of ROBO logs between Region B and Region A. Using a filter prevents from looping when the Log Insight deployments in Region A and Region B forward logs to each other.


You add a log filter on the vRealize Log Insight cluster in both Region A and Region B.

Region in the SDDC Hub	vRealize Log Insight URL in the SDDC Hub	Destination of the Log Filter
Region A	http://vrli-cluster-01.sfo01.rainpole.local	SFO01 to LAX01
Region B	http://vrli-cluster-51.lax01.rainpole.local	LAX01 to SFO01

Procedure

- 1 Log in to the vRealize Log Insight user interface.
 - a Open a Web browser and go to **https://vrli-cluster-01.sfo01.rainpole.local**.
 - b Log in using the following credentials.

Setting	Value
User name	admin
Password	vrli_admin_password

- 2 In the vRealize Log Insight user interface, click the configuration drop-down menu icon  and select **Administration**.
- 3 Under **Management**, click **Event Forwarding**.

- 4 Add an additional filter to prevent from forwarding loops.
 - a In the **Event Forwarding** page of the vRealize Log Insight user interface, click the **Edit** icon of the **SFO01 to LAX01** destination.
 - b In the **Edit Destination** dialog box, click **Add Filter** and enter the following filter attributes.

Filter Attribute	Value
Filter Type	site
Operator	does not match
Value	*

- 5 Click **Save**.
- 6 Repeat the procedure on the vRealize Log Insight instance in Region B of the hub.

The **Event Forwarding** page in the vRealize Log Insight user interface shows a summary of the forwarded events.

vSphere Update Manager Download Service Implementation in ROBO

Install the vSphere Update Manager Download Service (UMDS) on a Linux virtual machine to download and store binaries and metadata in a shared repository in the ROBO region.

Procedure

1 [Configure PostgreSQL Database on Your Linux-Based Host Operating System for UMDS in ROBO](#)

In the ROBO, configure a virtual machine with Ubuntu 14.04 Long Term Support (LTS) and a PostgreSQL database instance where you plan to install Update Manager Download Service (UMDS).

2 [Install UMDS on Ubuntu OS in ROBO](#)

After you install the PostgreSQL database on the UMDS virtual machine in the ROBO, install the UMDS software.

3 [Set Up the Data to Download with UMDS in ROBO](#)

By default, UMDS downloads patch binaries, patch metadata, and notifications for hosts. Specify which patch binaries and patch metadata to download using UMDS in the ROBO location.

4 [Install and Configure the UMDS Web Server in ROBO](#)

The UMDS server in the ROBO downloads upgrades, patch binaries, patch metadata, and notifications to a directory that you must share to vSphere Update Manager by using a Web server.

5 [Use the UMDS Shared Repository as the Download Source in Update Manager in ROBO](#)

You configure Update Manager to use the UMDS repository in the ROBO as a source for downloading ESXi patches, extensions, and notifications.

Configure PostgreSQL Database on Your Linux-Based Host Operating System for UMDS in ROBO

In the ROBO, configure a virtual machine with Ubuntu 14.04 Long Term Support (LTS) and a PostgreSQL database instance where you plan to install Update Manager Download Service (UMDS).

Prerequisites

- Create a virtual machine and install Ubuntu Linux (64-bit) Server 14.04 LTS OS for UMDS on the ROBO cluster.

Table 4-3. Virtual Machine Name and Placement for UMDS in ROBO

Setting	Value
Number of virtual machines	1
VM Name	nyc01umds01
vCenter Server	nyc01vc01.rainpole.local
Data center	NYC01
Folder	MGMT01
Resource Pool	NYC01-MGMT
Datastore	NYC01-VSAN01 (Thin Provision)
Guest OS	Ubuntu Linux (64-bit) Server 14.04 LTS
Network Portgroup	Distributed switch that ends with Mgmt-NYC01-VXLAN
Number of CPUs	2
Memory (GB)	2
Disk space (GB)	120
SCSI Controller	LSI Logic SAS
Virtual machine network adapter	VMXNET3
User account	svc-umds

Table 4-4. IP Addresses and Host Names for UMDS in ROBO

Role	IP Address	FQDN
Update Manager Download Service	172.18.19.67	nyc01umds01.rainpole.local
Default Gateway	172.18.19.1	
DNS server	172.18.11.4	
Subnet mask	255.255.255.0	
NTP Server	<ul style="list-style-type: none"> ■ 172.18.11.251 ■ 172.18.11.252 	ntp.rainpole.local

Procedure

- 1 Log in to vCenter Server by using the vSphere Web Client.
 - a Open a Web browser and go to **https://nyc01vc01.rainpole.local/vsphere-client**.
 - b Log in using the following credentials.

Setting	Value
User name	administrator@vsphere.local
Password	vsphere_admin_password

- 2 In the vSphere Web Client, right-click the **nyc01umds01** virtual machine and select **Open Console** to open the remote console to the virtual machine.
- 3 At the command prompt, log in as the **svc-umds** user using **svc-umds_password**.
- 4 Install VMtools and Secure Shell (SSH) server, and end the session.

```
sudo apt-get update
sudo apt-get -y install SSH
exit
```

- 5 Log back in to the UMDS virtual machine using SSH and the **svc-umds** service account credentials.
- 6 Install and start PostgreSQL and its dependencies:

```
sudo apt-get -y install vim perl tar sed psmisc unixodbc postgresql postgresql-contrib odbc-
postgresql
sudo service postgresql start
```

- 7 Log in as a PostgreSQL user, and create a database instance and a database user, by running the following commands.

When prompted, enter and confirm the *umds_db_user_password* password.

```
sudo su - postgres
createdb umds_db
createuser -d -e -r umds_db_user -P
```


8 Enable password authentication for the database user.

- a Navigate to the folder that contains the PostgreSQL configuration file `pg_hba.conf`.

Linux system	Default Location
Ubuntu 14.0.4	<code>/etc/postgresql/postgres_version/main</code>

```
cd /etc/postgresql/postgres_version/main
```

- b In the PostgreSQL configuration file, enable password authentication for the database user by inserting the following line right above `local all all peer`.

You can use the `vi` editor to make and save the changes.

#TYPE	DATABASE	USER	ADDRESS	METHOD
local	<code>umds_db</code>	<code>umds_db_user</code>		<code>md5</code>

- c Log out as a PostgreSQL user by running the following command.

```
logout
```

9 Configure the PostgreSQL driver and the data source name (DSN) for connection to the UMDS database.

- a Edit the ODBC configuration file.

```
sudo vi /etc/odbcinst.ini
```

- b Replace the file with the following content and save the change using `:wq`.

```
[PostgreSQL]
Description=PostgreSQL ODBC driver (Unicode version)
Driver=/usr/lib/x86_64-linux-gnu/odbc/psqlodbcw.so
Debug=0
CommLog=1
UsageCount=1
```

- c Edit the system file `/etc/odbc.ini`.

```
sudo vi /etc/odbc.ini
```

- d Replace the file with the following content and save the change using `:wq`,

```
[UMDS_DSN]
;DB_TYPE = PostgreSQL
;SERVER_NAME = localhost
;SERVER_PORT = 5432
;TNS_SERVICE = <database_name>
;USER_ID = <database_username>
Driver = PostgreSQL
DSN = UMDS_DSN
ServerName = localhost
PortNumber = 5432
Server = localhost
Port = 5432
UserID = umds_db_user
User = umds_db_user
Database = umds_db
```

- 10 Create a symbolic link between the UMDS and the PostgreSQL by running the following command.

```
ln -s /var/run/postgresql/.s.PGSQL.5432 /tmp/.s.PGSQL.5432
```

- 11 Restart PostgreSQL.

```
sudo service postgresql restart
```

Install UMDS on Ubuntu OS in ROBO

After you install the PostgreSQL database on the UMDS virtual machine in the ROBO, install the UMDS software.

Prerequisites

- Verify you have administrative privileges on the UMDS Ubuntu virtual machine.
- Mount the ISO file of the vCenter Server Appliance to the Linux machine.

Procedure

- 1 Log in to the UMDS virtual machine by using a Secure Shell (SSH) client.

- a Open an SSH connection to `nyc01umds01.rainpole.local`.
- b Log in using the following credentials.

Setting	Value
User name	<code>svc-umds</code>
Password	<code>svc-umds_password</code>

- 2 Mount the vCenter Server Appliance ISO to the UMDS virtual machine.

```
sudo mkdir -p /mnt/cdrom
sudo mount /dev/cdrom /mnt/cdrom
```

- 3 Unarchive the VMware-UMDS-6.5.0-*build_number*.tar.gz file:

```
tar -xzf /mnt/cdrom/umds/VMware-UMDS-6.5.0-build_number.tar.gz -C /tmp
```

- 4 Run the UMDS installation script.

```
sudo /tmp/vmware-umds-distrib/vmware-install.pl
```

- 5 Read and accept the EULA.
- 6 Press Enter to install UMDS in the default directory `/usr/local/vmware-umds` and enter **yes** to confirm directory creation.
- 7 Enter the UMDS proxy settings if needed according to the settings of your environment.
- 8 Press Enter to set the patch location to `/var/lib/vmware-umds` and enter **yes** to confirm directory creation.
- 9 Provide the database details.

Option	Description
Provide the database DSN	<code>UMDS_DSN</code>
Provide the database username	<code>umds_db_user</code>
Provide the database password	<code>umds_db_user_password</code>

- 10 Type **yes** and press Enter to install UMDS.

Set Up the Data to Download with UMDS in ROBO

By default, UMDS downloads patch binaries, patch metadata, and notifications for hosts. Specify which patch binaries and patch metadata to download using UMDS in the ROBO location.

Procedure

- 1 Log in to the UMDS virtual machine by using a Secure Shell (SSH) client.

- a Open an SSH connection to `nyc01umds01.rainpole.local`.
- b Log in using the following credentials.

Setting	Value
User name	<code>svc-umds</code>
Password	<code>svc-umds_password</code>

- 2 Navigate to the directory where UMDS is installed.

```
cd /usr/local/vmware-umds/bin
```

- 3 Disable the updates for older hosts and virtual appliances.

```
sudo ./vmware-umds -S -n
sudo ./vmware-umds -S -d embeddedEsx-5.5.0
sudo ./vmware-umds -S -d embeddedEsx-6.0.0
```

- 4 Configure automatic daily downloads by creating a cron job file.

```
cd /etc/cron.daily/
sudo touch umds-download
sudo chmod 755 umds-download
```

- 5 Edit the download command to the cron job.

```
sudo vi umds-download
```

- 6 Add the following lines to the file.

```
#!/bin/sh
/usr/local/vmware-umds/bin/vmware-umds -D
```

- 7 Test the UMDS Download cron job.

```
sudo ./umds-download
```

Install and Configure the UMDS Web Server in ROBO

The UMDS server in the ROBO downloads upgrades, patch binaries, patch metadata, and notifications to a directory that you must share to vSphere Update Manager by using a Web server.

The default folder to which UMDS downloads patch binaries and patch metadata on a Linux machine is `/var/lib/vmware-umds`. You share this folder out to the vSphere Update Manager instances within the region by using the Nginx Web server.

Procedure

- 1 Log in to the UMDS virtual machine by using a Secure Shell (SSH) client.
 - a Open an SSH connection to `nyc01umds01.rainpole.local`.
 - b Log in using the following credentials.

Setting	Value
User name	<code>svc-umds</code>
Password	<code>svc-umds_password</code>

- 2 Install the Nginx Web server with the following command.

```
sudo apt-get -y install nginx
```

- 3 Change the patch repository directory permissions by running the command.

```
sudo chmod -R 755 /var/lib/vmware-umds
```

- 4 Copy the default site configuration for use with the UMDS configuration.

```
sudo cp /etc/nginx/sites-available/default /etc/nginx/sites-available/umds
```

- 5 Edit the new `/etc/nginx/sites-available/umds` site configuration file and replace the `server {}` block with the following text.

```
server {
    listen 80 default_server;
    listen [::]:80 default_server ipv6only=on;

    root /var/lib/vmware-umds;
    index index.html index.htm;

    # Make site accessible from http://localhost/
    server_name localhost nyc01umds01 nyc01umds01.rainpole.local;

    location / {
        # First attempt to serve request as file, then
        # as directory, then fall back to displaying a 404.
        try_files $uri $uri/ =404;
```

```

        # Uncomment to enable naxsi on this location
        # include /etc/nginx/naxsi.rules
        autoindex on;
    }

```

- 6 Disable the existing default site.

```
sudo rm /etc/nginx/sites-enabled/default
```

- 7 Enable the new UMDS site.

```
sudo ln -s /etc/nginx/sites-available/umds /etc/nginx/sites-enabled/
```

- 8 Restart the Nginx Web service to apply the new configuration.

```
sudo service nginx restart
```

- 9 Ensure that you can browse the files of the UMDS Web server by opening a Web browser to **http://nyc01umds01.rainpole.local**.

Use the UMDS Shared Repository as the Download Source in Update Manager in ROBO

You configure Update Manager to use the UMDS repository in the ROBO as a source for downloading ESXi patches, extensions, and notifications.

Procedure

- 1 Log in to vCenter Server by using the vSphere Web Client.
 - a Open a Web browser and go to **https://nyc01vc01.rainpole.local/vsphere-client**.
 - b Log in using the following credentials.

Setting	Value
User name	administrator@vsphere.local
Password	vsphere_admin_password

- 2 On the **Home** page of the vSphere Web Client, click the **Update Manager** icon.
- 3 From the **Objects** tab, click the nyc01vc01.rainpole.local Update Manager instance for the ROBO.
- 4 On the **Manage** tab, click **Settings** and select **Download Settings**.
- 5 On the **Download sources** page, click **Edit**.

An **Edit Download Sources** dialog box opens.

- 6 Enter the following setting and click **OK**.

Setting	Value
Use a shared repository	Selected
URL	http://nyc01umds01.rainpole.local

The vSphere Web Client performs validation of the URL.

- 7 In the **Download Sources** pane, click **Download Now** to run the download patch definitions.