Deployment for Region A

Modified on 26 SEP 2017
VMware Validated Design 4.0
VMware Validated Design for Software-Defined Data Center 4.0

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

Contents

About VMware Validated Design Deployment for Region A

1

VMware Validated Design Deployment for Region A 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.

VMware Validated Design Deployment for Region A 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

The *VMware Validated Design Deployment for Region A* document 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 for Region A 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 Region A* document is updated with each release of the product or when necessary.

This table provides the update history of the *Deployment for Region A* document.

Revision	Description
26 SEP 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 Region A.
EN-002468-03	■ Step 6 omitted the configuration values for the PSC-TCP server pool. The correct configuration values have been added to this step in the accompanying table. See Create Platform Services Controller Server Pools in Region A.
EN-002468-02	■ Extended the permissions that are required for integrating vRealize Operations Manager and vRealize Log Insight. See Configure User Privileges on vRealize Operations Manager for Integration with vRealize Log Insight in Region A ■ Added step 9, which instructs users to configure the MTU value on the vMotion VMkernel adapter to 9000. See Create a vSphere Distributed Switch for the Management Cluster in Region A. ■ Added step 9, which instructs users to configure the MTU value on the vMotion VMkernel adapter to 9000. See Create a vSphere Distributed Switch for the Shared Edge and Compute Cluster in Region A.

Revision	Description
EN-002468-01	■ Step 1 incorrectly listed the FQDN as ending in .com. This has been corrected to read the sfo01psc01.sfo01.rainpole.local. See Update the Platform Services Controller SSO Configuration and Endpoints in Region A. ■ Steps 1b and 1c have been updated to make Bash your default command shell. See Replace the Platform Services Controller Certificates in Region A. ■ The default gateway IP address was incorrectly listed as 172.16.11.1. The correct IP address is 172.16.11.253. SeeDeploy the External Platform Services Controllers for the vCenter Servers in Region A. ■ Incorrectly instructed you to update host profile to the management cluster. It should instruct you to update the host profile for the Compute cluster. See Update the Host Profile for the Compute Cluster in Region A. ■ Step 5h incorrectly instructed you to configure the UDLR interface. The correct interface to configure is DLR. See Deploy NSX Edge Devices for North-South Routing in the Shared Edge and Compute Cluster in Region A. ■ Step 9m incorrectly stated that three neighbors were added to the Neighbors table. The correct number of neighbors added is four. See Enable and Configure Routing in the Shared Edge and Compute Cluster in Region A ■ The Distributed Firewall Rules have been updated to allow the administrator network access to vRealize Log Insight and vRealize Operations. See Create Distributed Firewall Rules, Create IP Sets for All Components of the Management Clusters in the SDDC, and Create Security Groups. ■ Step 10 incorrectly instructed you to save the vRealize Automation Server Pool. The correct pool member to save is the Platform Services Controller Pool. See Create Platform Services Controller Server Pools in Region A. ■ Steps 2 and 3 were duplicated. The duplicated step has been removed. See Configure Lockdown Mode on All ESXi Hosts in Region A. ■ Added a step to power on vSphere Data Protection after appliance deployment. See Deploy the vSphere Data Protection Virtual Appliance in Region A. ■ Use the UMDS Shared Repository as the Download Source in Update Manager in Region A now provides instructions about adding the repository of the Update Manager Download Service in Region A to the Update Manager on the Compute vCenter Server.
EN-002468-00	Initial release.

Region A Virtual Infrastructure Implementation

2

The Virtual Infrastructure in Region A is implemented through the following high level procedures.

Procedure

1 Install and Configure ESXi Hosts in Region A

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

2 Deploy and Configure the Platform Services Controller and vCenter Server Components in Region A

   Deploy and configure the cluster components for both the management cluster and the shared edge and compute cluster.

3 Deploy and Configure the Management Cluster NSX Instance in Region A

   This design uses two separate NSX instances per region. One instance is tied to the Management vCenter Server, and the other instance is tied to the Compute vCenter Server. Deploy and configure the NSX instance for the management cluster in Region A.

4 Deploy and Configure the Shared Edge and Compute Cluster Components in Region A

   Deploy and configure the shared edge and compute cluster components.

5 Deploy and Configure the Shared Edge and Compute Cluster NSX Instance in Region A

   Deploy and configure the NSX instance for the shared edge and compute cluster in Region A.

6 Deploy vSphere Data Protection in Region A

   Deploy vSphere Data Protection to provide the capability for backup and restore of SDDC management components.

7 Replace Certificates in Region A

   In this design, you replace user-facing certificates with certificates that are signed by a Microsoft Certificate Authority (CA). By default, virtual infrastructure management components use TLS/SSL certificates that are signed by the VMware Certificate Authority (VMCA). These certificates are not trusted by end-user devices.

Install and Configure ESXi Hosts in Region A

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

Procedure

1. Prerequisites for Installation of ESXi Hosts in Region A

   Install and configure the ESXi hosts for the management cluster and the shared edge and compute cluster by using the same process.

2. Install ESXi Interactively on All Hosts in Region A

   Install all ESXi hosts for all clusters interactively.

3. Configure the Network on All Hosts in Region A

   After the initial boot, use the ESXi Direct Console User Interface (DCUI) for initial host network configuration and administrative access.

4. Configure vSphere Standard Switch on a Host in the Management Cluster in Region A

   You must perform network configuration from the VMware Host Client only for the mgmt01esx01 host. You perform all other host networking configuration after the deployment of the vCenter Server system that manages the hosts.

5. Configure SSH and NTP on the First Host in Region A

   Time synchronization issues can result in serious problems with your environment. Configure NTP for each of your hosts in the management and the shared edge and compute clusters.

6. Set Up vSAN Datastore for the Management Cluster in Region A

   Before you can use vSAN storage in your environment, you must set it up.

Prerequisites for Installation of ESXi Hosts in Region A

Install and configure the ESXi hosts for the management cluster and the shared edge and compute cluster by using the same process.

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 two regional management networks 172.16.11.0/24 and 172.17.11.0/24 as this will be needed to join the common SSO domain.

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 hosts.

Table 2-1. Management Cluster Hosts in Region A

FQDN	IP	Management VLAN	Default Gateway	NTP Server
mgmt01esx01.sfo01.rainpole.local	172.16.11.101	1611	172.16.11.253	■ ntp.sfo01.rainpole.local ■ ntp.lax01.rainpole.local
mgmt01esx02.sfo01.rainpole.local	172.16.11.102	1611	172.16.11.253	■ ntp.sfo01.rainpole.local ■ ntp.lax01.rainpole.local
mgmt01esx03.sfo01.rainpole.local	172.16.11.103	1611	172.16.11.253	■ ntp.sfo01.rainpole.local ■ ntp.lax01.rainpole.local
mgmt01esx04.sfo01.rainpole.local	172.16.11.104	1611	172.16.11.253	■ ntp.sfo01.rainpole.local ■ ntp.lax01.rainpole.local

Table 2-2. Shared Edge and Compute Cluster Hosts in Region A

FQDN	IP	Management VLAN	Default Gateway	NTP Server
comp01esx01.sfo01.rainpole.local	172.16.31.101	1631	172.16.31.253	■ ntp.sfo01.rainpole.local ■ ntp.lax01.rainpole.local
comp01esx02.sfo01.rainpole.local	172.16.31.102	1631	172.16.31.253	■ ntp.sfo01.rainpole.local ■ ntp.lax01.rainpole.local
comp01esx03.sfo01.rainpole.local	172.16.31.103	1631	172.16.31.253	■ ntp.sfo01.rainpole.local ■ ntp.lax01.rainpole.local
comp01esx04.sfo01.rainpole.local	172.16.31.104	1631	172.16.31.253	■ ntp.sfo01.rainpole.local ■ ntp.lax01.rainpole.local

Install ESXi Interactively on All Hosts in Region A

Install all ESXi hosts for all clusters interactively.

Procedure

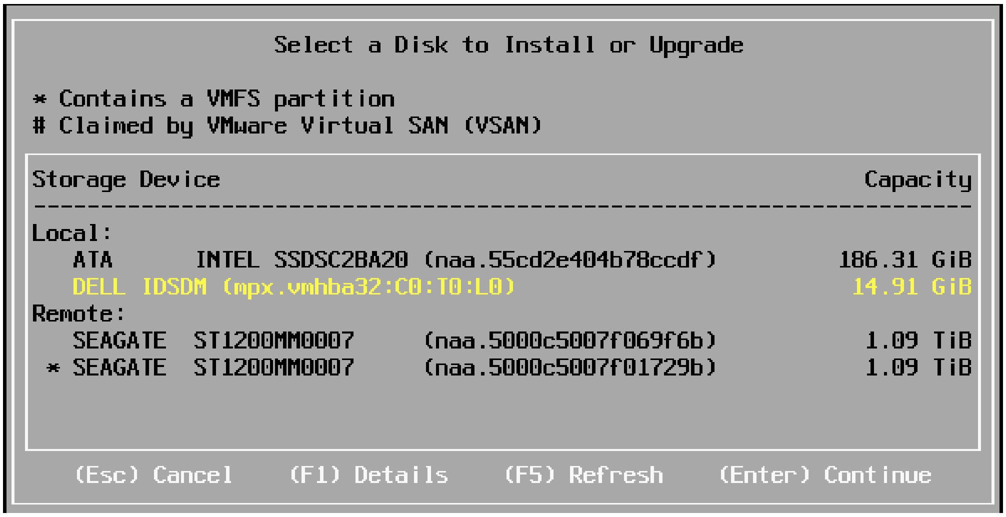
1 Power on the `mgmt01esx01` host in Region A.

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.



```
                  Select a Disk to Install or Upgrade

 * Contains a VMFS partition
 # Claimed by VMware Virtual SAN (VSAN)

 Storage Device                                                 Capacity
 ------------------------------------------------------------------------
 Local:
    ATA      INTEL SSDSC2BA20 (naa.55cd2e404b78ccdf)          186.31 GiB
    DELL IDSDM (mpx.vmhba32:C0:T0:L0)                          14.91 GiB
 Remote:
    SEAGATE  ST1200MM0007     (naa.5000c5007f069f6b)            1.09 TiB
  * SEAGATE  ST1200MM0007     (naa.5000c5007f01729b)            1.09 TiB


    (Esc) Cancel     (F1) Details     (F5) Refresh     (Enter) Continue
```

6 Select the keyboard layout, and press Enter.

7 Enter the ***esxi_root_user_password***, confirm, and press Enter.

8 On the **Confirm Install** screen, press F11 to start the installation.

9 After the installation has completed successfully, unmount the USB drive, and press Enter to reboot the host.

10 Repeat this procedure for all hosts in the data center, using the respective values for each host you configure.

Configure the Network on All Hosts in Region A

After the initial boot, use the ESXi Direct Console User Interface (DCUI) for initial host network configuration and administrative access.

Perform the following tasks to configure the host network settings:

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

Repeat this procedure for all hosts in the management and shared edge and compute pods. Enter the respective values from the prerequisites section for each host that you configure. See Prerequisites for Installation of ESXi Hosts in Region A.

Procedure

1 Open the DCUI on the physical ESXi host `mgmt01esx01`.

   a Open a console window to the host.

   b Press F2 to enter the DCUI.

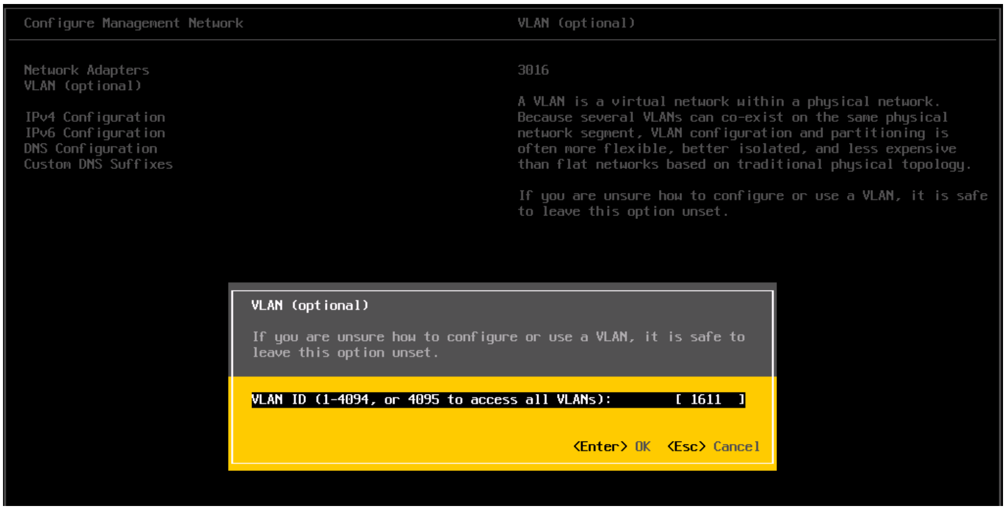
   c Enter **`root`** as login name, enter the ***esxi_root_user_password*** password, and press Enter.

2 Configure the network.

a Select **Configure Management Network** and press Enter.

b Select **VLAN (Optional)** and press Enter.

c Enter **1611** as the VLAN ID for the Management Network and press Enter.

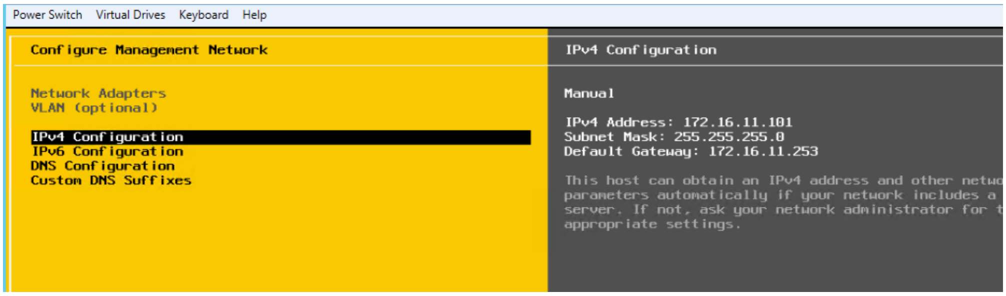


```
Configure Management Network                                  VLAN (optional)

Network Adapters                                              3016
VLAN (optional)
                                                              A VLAN is a virtual network within a physical network.
IPv4 Configuration                                            Because several VLANs can co-exist on the same physical
IPv6 Configuration                                            network segment, VLAN configuration and partitioning is
DNS Configuration                                             often more flexible, better isolated, and less expensive
Custom DNS Suffixes                                           than flat networks based on traditional physical topology.

                                                              If you are unsure how to configure or use a VLAN, it is safe
                                                              to leave this option unset.

                            VLAN (optional)

                            If you are unsure how to configure or use a VLAN, it is safe to
                            leave this option unset.

                            VLAN ID (1-4094, or 4095 to access all VLANs):        [ 1611   ]

                                                                <Enter> OK  <Esc> Cancel
```

d Select **IPv4 Configuration** and press Enter.

e Configure IPv4 network using the following settings, and press Enter.

Setting	Value
Set static IPv4 address and network configuration	Selected
IPv4 Address	172.16.11.101
Subnet Mask	255.255.255.0
Default Gateway	172.16.11.253



```
Configure Management Network                    IPv4 Configuration

Network Adapters                                Manual
VLAN (optional)
                                                IPv4 Address: 172.16.11.101
IPv4 Configuration                              Subnet Mask: 255.255.255.0
IPv6 Configuration                              Default Gateway: 172.16.11.253
DNS Configuration
Custom DNS Suffixes                             This host can obtain an IPv4 address and other netwo
                                                parameters automatically if your network includes a
                                                server. If not, ask your network administrator for t
                                                appropriate settings.
```

f Select **DNS Configuration** and press Enter.

g Configure the DNS by using the following settings, and press Enter.

Setting	Value
Use the following DNS Server address and hostname	Selected
Primary DNS Server	172.16.11.5
Alternate DNS Server	172.16.11.4
Hostname	mgmt01esx01.sfo01.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 management and shared edge and compute pods.

Configure vSphere Standard Switch on a Host in the Management Cluster in Region A

You must perform network configuration from the VMware Host Client only for the mgmt01esx01 host. You perform all other host 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://mgmt01esx01.sfo01.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 **1611** for **VLAN ID**, and click **OK**.

Configure SSH and NTP on the First Host in Region A

Time synchronization issues can result in serious problems with your environment. Configure NTP for each of your hosts in the management and the shared edge and compute clusters.

Procedure

1 Log in to the mgmt01esx01.sfo01.rainpole.local host using the VMware Host Client.

   a Open a Web browser and go to **`mgmt01esx01.sfo01.rainpole.local`**.

Setting	Value
User name	root
Password	*esxi_root_user_password*

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.sfo01.rainpole.local,ntp.lax01.rainpole.local`** as NTP servers.

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

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

Set Up vSAN Datastore for the Management Cluster in Region A

Before you can use vSAN storage in your environment, you must set it up.

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 Open an SSH client to connect to the ESXi Shell on mgmt01esx01.sfo01.rainpole.local.

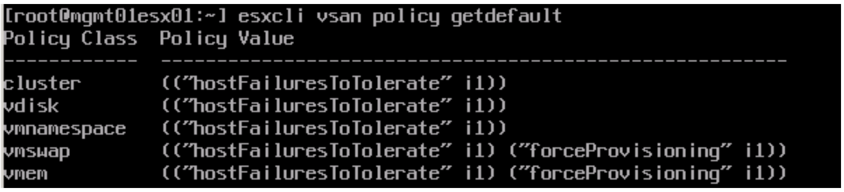
   a Open a console window to the host.

   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.

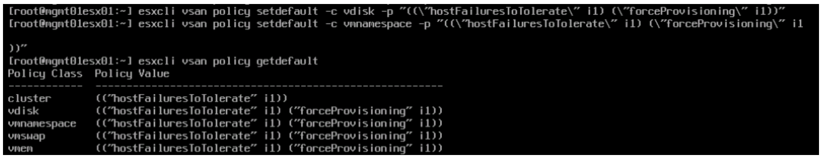
```
esxcli vsan policy getdefault
```



```
[root@mgmt01esx01:~] 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
```



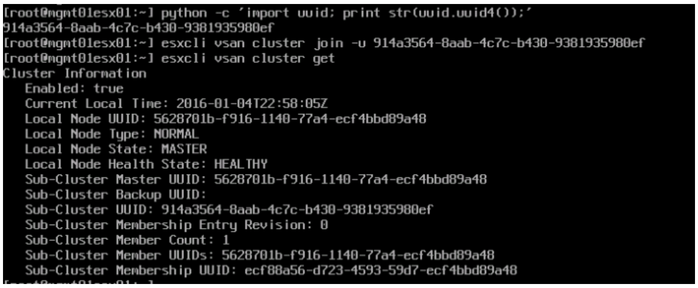
```
[root@mgmt01esx01:~] esxcli vsan policy setdefault -c vdisk -p "((\"hostFailuresToTolerate\" i1) (\"forceProvisioning\" i1))"
[root@mgmt01esx01:~] esxcli vsan policy setdefault -c vmnamespace -p "((\"hostFailuresToTolerate\" i1) (\"forceProvisioning\" i1

))"
[root@mgmt01esx01:~] 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.

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

Note You need the `$UUID_GENERATED` from the generated output for the next command.

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



```
[root@mgmt01esx01:~] python -c 'import uuid; print str(uuid.uuid4());'
914a3564-8aab-4c7c-b430-9381935980ef
[root@mgmt01esx01:~] esxcli vsan cluster join -u 914a3564-8aab-4c7c-b430-9381935980ef
[root@mgmt01esx01:~] 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
```

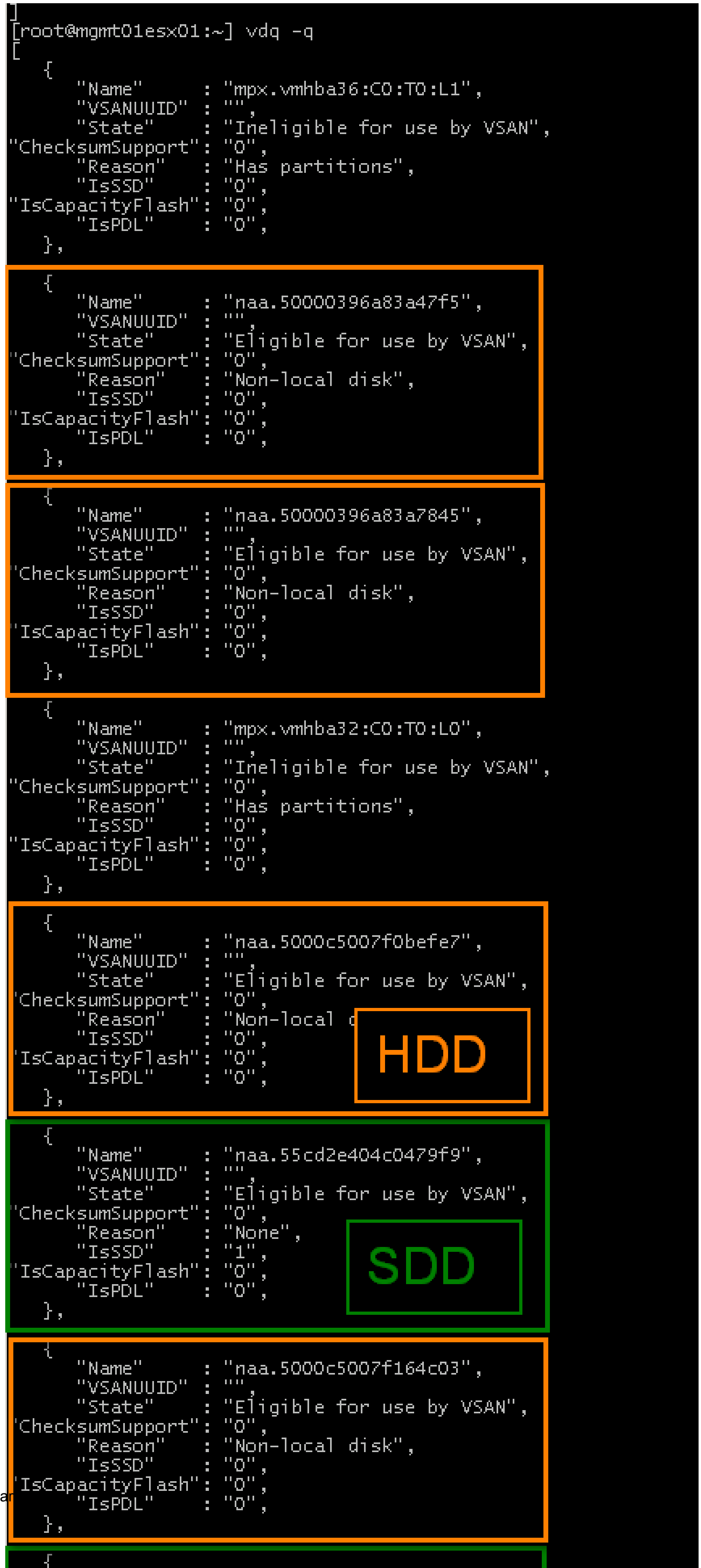
5 List the devices and determine the device name for the SSD and HDD.

These disks will be used to provision the vSAN datastore.

```
vdq -q
```

Identify all devices that can be used by vSAN.

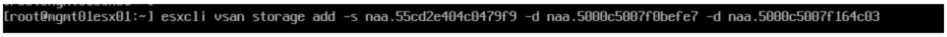
Property	SDD Value	HDD Value
State	Eligible for use by VSAN	Eligible for use by VSAN
IsSSD	1	0



```
]
[root@mgmt01esx01:~] 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 d
      "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",
   },

   {
```

6 Create vSAN datastore using available SSD and HDD disks determined from previous step.

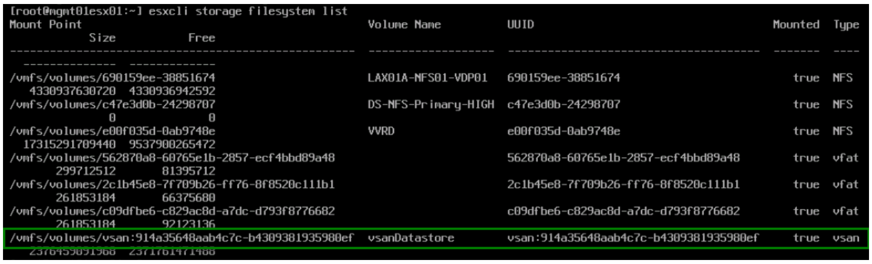
```
esxcli vsan storage add –s SSD_Device_name –d HDD_Device Name
```



```
[root@mgmt01esx01:~] esxcli vsan storage add -s naa.55cd2e404c0479f9 -d naa.5000c5007f0befe7 -d naa.5000c5007f164c03
```

7 Confirm that the vSAN datastore has been created.

```
esxcli storage filesystem list
```



```
[root@mgmt01esx01:~] esxcli storage filesystem list
Mount Point                                        Volume Name         UUID                                   Mounted  Type
           Size          Free
-------------------------------------------------  ------------------  -------------------------------------  -------  ----
  -------------  -------------
/vmfs/volumes/690159ee-38851674                    LAX01A-NFS01-VDP01  690159ee-38851674                         true  NFS
   4330937630720  4330936942592
/vmfs/volumes/c47e3d0b-24298707                    DS-NFS-Primary-HIGH c47e3d0b-24298707                         true  NFS
              0              0
/vmfs/volumes/e00f035d-0ab9748e                    VVRD                e00f035d-0ab9748e                         true  NFS
  17315291709440  9537900265472
/vmfs/volumes/562870a8-60765e1b-2857-ecf4bbd89a48                      562870a8-60765e1b-2857-ecf4bbd89a48       true  vfat
      299712512      81395712
/vmfs/volumes/2c1b45e8-7f709b26-ff76-8f8520c111b1                      2c1b45e8-7f709b26-ff76-8f8520c111b1       true  vfat
      261853184      66375680
/vmfs/volumes/c09dfbe6-c829ac8d-a7dc-d793f8776682                      c09dfbe6-c829ac8d-a7dc-d793f8776682       true  vfat
      261853184      92123136
/vmfs/volumes/vsan:914a35648aab4c7c-b4309381935980ef vsanDatastore     vsan:914a35648aab4c7c-b4309381935980ef    true  vsan
   2376459091968  2371761471488
```

A vSAN datastore is now created and ready for the Management vCenter Server installation.

Deploy and Configure the Platform Services Controller and vCenter Server Components in Region A

Deploy and configure the cluster components for both the management cluster and the shared edge and compute cluster.

Procedure

1 Deploy the External Platform Services Controllers for the vCenter Servers in Region A

Two external Platform Services Controller instances must be deployed in Region A. One will be associated with the management cluster, and one will be associated with the shared edge and compute cluster. Work through this procedure twice, using the vCenter Server appliance ISO file and the customized data for each instance.

2 Join the Platform Services Controllers to Active Directory in Region A

After you have successfully installed the Platform Services Controller instances, you must add the appliances to your Active Directory domain. After that, add the Active Directory domain as an identity source to vCenter Single Sign-On. When you do, users in the Active Directory domain are visible to vCenter Single Sign-On and can be assigned permissions to view or manage SDDC components. This procedure will be done for the Platform Services Controllers for the management cluster and the shared edge and compute cluster.

3. Replace the Platform Services Controller Certificates in Region A

   You replace the machine SSL certificate on each Platform Services Controller instance with a custom certificate that is signed by the certificate authority (CA) available on the parent Active Directory (AD) server.

4. Update the Platform Services Controller SSO Configuration and Endpoints in Region A

   Before installing vCenter Server the Platform Services Controller endpoints must be updated to reflect the name of the load balancers virtual IP.

5. Deploy the Management vCenter Server Instance in Region A

   You can now install the vCenter Server appliance for the management applications and assign a license.

6. Configure the Management Cluster in Region A

   You must now create and configure the management cluster.

7. Create a vSphere Distributed Switch for the Management Cluster in Region A

   After all ESXi hosts have been added to the clusters, create a vSphere Distributed Switch to handle the traffic of the management applications in the SDDC. You must also create port groups to prepare your environment to migrate the Platform Services Controller and vCenter Server instances to the distributed switch.

8. Set vSAN Storage Policy in Region A

   This step is to set the vSAN storage policy for the Platform Services Controller and vCenter Server appliances.

9. Create vSAN Disk Groups for the Management Cluster in Region A

   vSAN disk groups must be created on each host that is contributing storage to the vSAN datastore.

10. Enable vSphere HA on the Management Cluster in Region A

    After vSphere vSphere Distributed Switch has been created and connected with all hosts, enable vSphere HA on the cluster.

11. Change Advanced Options on the ESXi Hosts in the Management Cluster in Region A

    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.

12. Mount NFS Storage for the Management Cluster in Region A

    You must mount an NFS datastore where vSphere Data Protection will later be deployed.

13. Create and Apply the Host Profile for the Management Cluster in Region A

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

14. Set vSAN Policy on Management Virtual Machines in Region A

    After you apply the host profile to all of the hosts, set the storage policy of the Management Virtual Machines to the vSAN Default Storage Policy.

15. Create the VM and Template Folders in Region A

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

16 Create Anti-Affinity Rules for the Platform Services Controller in Region A

Anti-Affinity rules prevent virtual machines from running on the same host. This helps to maintain redundancy in the event of host failures.

17 Create VM Groups to Define Startup Order in the Management Cluster in Region A

VM Groups allow you to define the startup order of virtual machines. Startup orders are used during vSphere HA events such that vSphere HA powers on virtual machines in the correct order.

Deploy the External Platform Services Controllers for the vCenter Servers in Region A

Two external Platform Services Controller instances must be deployed in Region A. One will be associated with the management cluster, and one will be associated with the shared edge and compute cluster. Work through this procedure twice, using the vCenter Server appliance ISO file and the customized data for each instance.

Repeat this procedure for each platform services controller, using the respective values for each indicated in the procedure steps.

Procedure

1 Log in to the Windows host that has access to your data center as an administrator.

2 Start the **vCenter Server Appliance Installer** wizard.

a Browse to the vCenter Server Appliance ISO file.

b Open the `<dvd-drive>:\vcsa-ui-installer\win32\Installer.exe` application file.

3 Complete Stage 1 of the **vCenter Server Appliance Deployment** 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, click **Platform Services Controller** and click **Next**.

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

Setting	Value
FQDN or IP Address	mgmt01esx01.sfo01.rainpole.local
HTTPS port	443
User name	root
Password	*esxi_root_user_password*

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	Management Value	Edge/Compute Value
VM name	mgmt01psc01	comp01psc01
Root password	*mgmtpsc_root_password*	*comppsc_root_password*
Confirm root password	*mgmtpsc_root_password*	*comppsc_root_password*

h On the **Select datastore** page, select the **vsanDatastore** datastore, select the **Enable Thin Disk Mode** check box, and click **Next**.

i On the **Configure network settings** page, enter the following settings and click **Next**.

Setting	Management Value	Edge/Compute Value
Network	VM Network	VM Network
IP version	IPv4	IPv4
IP assignment	static	static
System name	mgmt01psc01.sfo01.rainpole.local	comp01psc01.sfo01.rainpole.local
IP address	172.16.11.61	172.16.11.63
Subnet mask or prefix length	255.255.255.0	255.255.255.0
Default gateway	172.16.11.253	172.16.11.253
DNS servers	172.16.11.5,172.16.11.4	172.16.11.5,172.16.11.4

j On the **Ready to complete stage 1** page, review the configuration and click **Finish** to start the deployment.

k When the deployment completes, click **Continue** to proceed to second stage of the installation, setting up the Platform Services Controller Appliance.

4 Complete Stage 2 of the **Set Up Platform Services Controller Appliance** 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.sfo01.rainpole.local
SSH access	Enabled

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

Setting	Management Value	Edge/Compute Value
SSO configuration	Create a new SSO domain	Join an existing SSO domain
Platform Services Controller	N/A	mgmt01psc01.sfo01.rainpole.local
HTTPS port	N/A	443
SSO domain name	vsphere.local	vsphere.local
SSO password	*sso_password*	*sso_password*
Confirm password	*sso_password*	N/A
Site name	SFO01	N/A

d On the **SSO Site Name** page, select **Join an existing site** radio button, choose **SFO01** from the **SSO site name** drop-down menu, and click **Next.** This page will only appear during the deployment of the second Platform Services Controller. It will not occur during the initial deployment.

e On the **Configure CEIP** page, verify that the **Join the VMware's Customer Experience Improvement Program (CEIP)**check box is checked and click **Next**.

f On the **Ready to complete** page, review the configuration and click **Finish** to complete the setup.

g Click **OK** on the Warning.

5 Repeat this procedure for each platform services controller, using the respective values for each.

Join the Platform Services Controllers to Active Directory in Region A

After you have successfully installed the Platform Services Controller instances, you must add the appliances to your Active Directory domain. After that, add the Active Directory domain as an identity source to vCenter Single Sign-On. When you do, users in the Active Directory domain are visible to vCenter Single Sign-On and can be assigned permissions to view or manage SDDC components. This procedure will be done for the Platform Services Controllers for the management cluster and the shared edge and compute cluster.

Repeat this procedure twice, once for the of the management cluster and again for the shared edge and compute cluster.

Procedure

1 Log in to the Platform Services Controller administration interface.

   a Open a Web browser and go to the URL for either the Management or Edge/Compute cluster.

Setting	Management Value	Edge/Compute Value
PSC Link	https://mgmt01psc01.sfo01.rainpole.local	https://comp01psc01.sfo01.rainpole.local

   b Click the link for **Platform Services Controller web interface**.

   c Log in using the following credentials.

Setting	Value
User name	administrator@vsphere.local
Password	*vsphere_admin_password*

2 Add the management Platform Services Controller instance to the Active Directory domain.

   a In the **Navigator**, click **Appliance Settings**, click the **Manage** tab, and click **Join**.

   b In the **Join Active Directory Domain** dialog box, enter the following settings and click **OK**.

Setting	Value
Domain	sfo01.rainpole.local
User name	*ad_admin_acct*@sfo01.rainpole.local
Password	*ad_admin_password*

3 Reboot the Platform Services Controller instance to apply the changes.

   a Click the **Appliance settings** tab, and click the **VMware Platform Services Appliance** link.

   b Log in to the VMware vCenter Server Appliance administration interface with the following credentials.

Setting	Value
User name	root
Password	*psc_root_password*

   c On the **Summary** page, click **Reboot**.

   d In the **System Reboot** dialog box, click **Yes**.

   e Wait for the reboot process to finish.

4 After the reboot process finishes, log in to **`https://mgmt01psc01.sfo01.rainpole.local`** again using the following credentials.

Setting	Value
User name	administrator@vsphere.local
Password	*vsphere_admin_password*

5. Verify that the Platform Services Controller has successfully joined the domain, click **Appliance Settings** and click the **Manage** tab.

6. Add Active Directory as a vCenter Single Sign-On identity source for the Management cluster.

   Note This step should only be performed on the Platform Services Controller for the Management cluster. Do not repeat this step when joining the Edge/Compute Platform Services Controller to Active Directory.

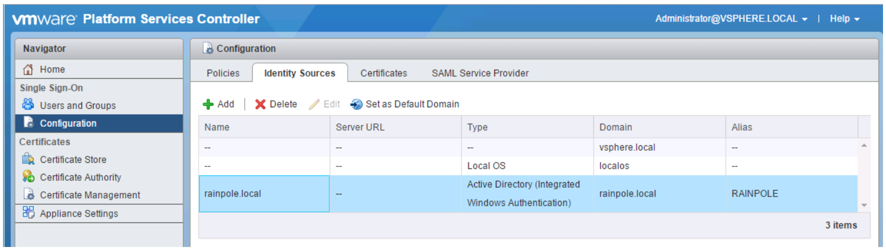
   a In the **Navigator**, click **Configuration** and click the **Identity Sources** tab.

   b Click the **Add** icon to add a new identity source.

   c In the **Add Identity Source** dialog box, select the following settings and click **OK**.

Setting	Value
Identity source type	Active Directory (Integrated Windows Authentication)
Domain name	SFO01.RAINPOLE.LOCAL
Use machine account	Selected

   d Under **Identity Sources**, select the **rainpole.local** identity source and click **Set as Default Domain** to make `rainpole.local` the default domain.



Name	Server URL	Type	Domain	Alias
--	--	--	vsphere.local	--
--	--	Local OS	localos	--
rainpole.local	--	Active Directory (Integrated Windows Authentication)	rainpole.local	RAINPOLE

   e In the confirmation dialog box, click **Yes**.

7. Repeat steps 1 thru 5 of this procedure for the Platform Services Controller for the shared edge and compute cluster.

Replace the Platform Services Controller Certificates in Region A

You replace the machine SSL certificate on each Platform Services Controller instance with a custom certificate that is signed by the certificate authority (CA) available on the parent Active Directory (AD) server.

You must repeat this procedure twice: first on the Platform Services Controller for the Management vCenter Server (mgmt01psc01.sfo01.rainpole.local), and then on the Platform Services Controller for the Compute vCenter Server (comp01psc01.sfo01.rainpole.local).

Table 2-3. Certificate-Related Files on Platform Services Controllers

Platform Services Controller	Certificate File Name	Replacement Order
mgmt01psc01.sfo01.rainpole.local	■ sfo01psc01.sfo01.1.cer ■ sfo01psc01.sfo01.key ■ root64.cer	First
comp01psc01.sfo01.rainpole.local	■ sfo01psc01.sfo01.1.cer ■ sfo01psc01.sfo01.key ■ root64.cer	Second

Procedure

1 Change the Platform Services Controller command shell to the Bash shell to allow secure copy (`scp`) connections.

   a SSH to **`mgmt01psc01.sfo01.rainpole.local`** and login using the following credentials.

Setting	Value
Username	root
Password	*mgmtpsc_root_password*

   b Enter `shell` and press Enter.

   c Run the command `chsh -s "/bin/bash" root`.

2 Copy the generated certs to the Platform Services Controller.

   a Use the `scp` command to copy the contents of the folder `C:\CertGenVVD\SignedByMCSACerts\sfo01psc01.sfo01` to the folder `/tmp/certs`.

   b Use the `scp` command to copy the `Root64.cer` file from the folder `C:\CertGenVVD\SignedByMCSACerts\RootCA` to the folder`/tmp/certs`.

3 Replace the certificate on the Platform Services Controller.

   a Start the vSphere Certificate Manager utility on the Platform Services Controller.

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

   b Select **Option 1 (Replace Machine SSL certificate with Custom Certificate)**.

   c Enter the default vCenter Single Sign-On user name **`administrator@vsphere.local`** and the ***`vsphere_admin`*** password.

   d Select **Option 2 (Import custom certificate(s) and key(s) to replace existing Machine SSL certificate)**.

   e When prompted for the custom certificate enter **`/tmp/certs/sfo01psc01.sfo01.1.cer`**.

   f When prompted for the custom key enter **`/tmp/certs/sfo01psc01.sfo01.key`**.

   g When prompted for the signing certificate enter **`/tmp/certs/Root64.cer`**.

   h When prompted to Continue operation enter **Y**.

   i The Platform Services Controller services will restart automatically.

4 Repeat steps 3 thru Step 3 to replace the certificate on comp01psc01.sfo01.rainpole.local.

Update the Platform Services Controller SSO Configuration and Endpoints in Region A

Before installing vCenter Server the Platform Services Controller endpoints must be updated to reflect the name of the load balancers virtual IP.

Prerequisites

Before completing this procedure a DNS A record must be created. This A record is the FQDN of the load balancer with the IP address of mgmt01psc01.sfo01.rainpole.local. After the load balancer is setup this DNS record is changed to the virtual IP of the load balancer.

Procedure

1 Create a DNS record for the load balancer FQDN. Create a DNS A record using the values listed below.

   a Open a remote desktop connection to your DNS server.

   b Create a DNS A record with the values below:

FQDN	IP
sfo01psc01.sfo01.rainpole.local	172.16.11.61

Note After the load balancer is configured the IP address will be updated to reflect the load balancer's VIP instead of the IP address of mgmt01psc01.sfo01.rainpole.local

2 Update the Platform Services Controller SSO configuration on `mgmt01psc01.sfo01.rainpole.local`.

   a Open an SSH connection to **`mgmt01psc01.sfo01.rainpole.local`**.

   b Log in using the following credentials.

Setting	Value
User name	root
Password	*mgmtpsc_root_password*

   c Enter **`cd /usr/lib/vmware-sso/bin/`** and press `Enter`.

   d Enter **`python updateSSOConfig.py --lb-fqdn=sfo01psc01.sfo01.rainpole.local`** and press `Enter`.

3 Update the Platform Services Controller SSO configuration on `comp01psc01.sfo01.rainpole.local`.

   a Open an SSH connection to `comp01psc01.sfo01.rainpole.local`.

   b Log in using the following credentials.

Setting	Value
User name	root
Password	*comppsc_root_password*

   c Enter **`cd /usr/lib/vmware-sso/bin/`**and press **`Enter`**.

   d Enter **`python updateSSOConfig.py --lb-fqdn=sfo01psc01.sfo01.rainpole.local`** and press **`Enter`**.

4 Update the Platform Services Controller endpoints.

   Only perform this procedure on one of the Platform Services Controllers.

   a Open an SSH connection to **mgmt01psc01.sfo01.rainpole.local**.

   b Log in using the following credentials.

Setting	Value
User name	root
Password	*mgmtpsc_root_password*

   c Enter **`cd /usr/lib/vmware-sso/bin/`** and press **`Enter`**.

   d Enter **`python UpdateLsEndpoint.py -lb-fqdn=sfo01psc01.sfo01.rainpole.local --user=Administrator@vsphere.local`** and press **`Enter`**.

   e Enter the *vsphere_admin_password* when prompted.

Deploy the Management vCenter Server Instance in Region A

You can now install the vCenter Server appliance for the management applications and assign a license.

Procedure

1 Start the **vCenter Server Appliance Deployment** 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 Deployment** 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**, select the **vCenter Server (Requires External Platform Services Controller)** radio button 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	mgmt01esx01.sfo01.rainpole.local
HTTPS port	443
User name	root
Password	*esxi_root_user_password*

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	mgmt01vc01
Root password	*mgmtvc_root_password*
Confirm root password	*mgmtvc_root_password*

h On the **Select deployment size** page, select **Small vCenter Server** 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	mgmt01vc01.sfo01.rainpole.local
IP address	172.16.11.62
Subnet mask or prefix length	255.255.255.0
Default gateway	172.16.11.253
DNS servers	172.16.11.5,172.16.11.4

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** 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.sfo01.rainpole.local
SSH access	Enabled

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

Setting	Value
Platform Services Controller	sfo01psc01.sfo01.rainpole.local
HTTPS port	443
SSO domain name	vsphere.local
SSO password	*sso_password*

  d On the **Ready to Complete** page, review your entries and click **Finish**.

  e Click **OK** on the Warning.

4 Add new licenses for this vCenter Server instance and the management cluster ESXi hosts.

  a Open a Web browser and go to **`https://mgmt01vc01.sfo01.rainpole.local/vsphere-client`**.

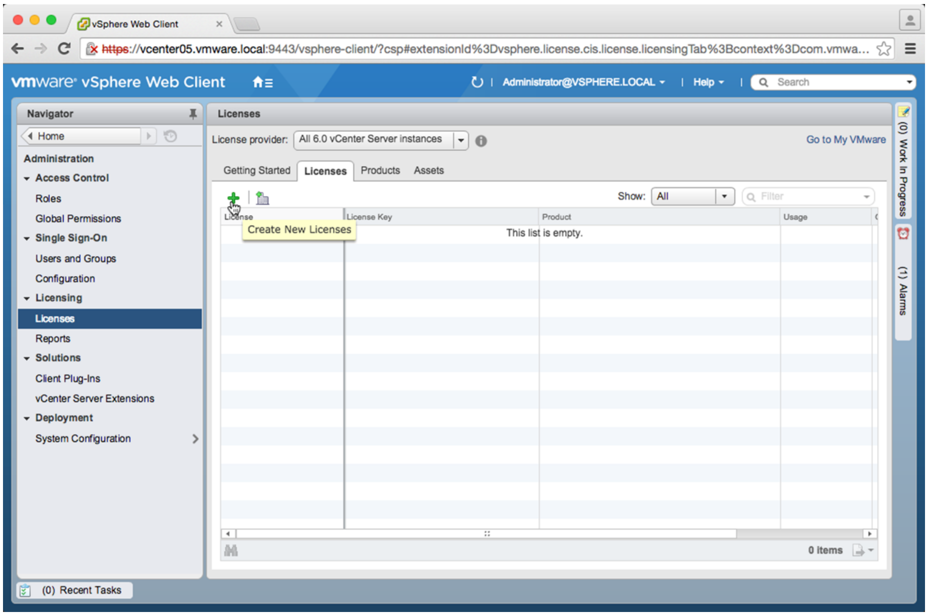
  b Log in using the following credentials.

Setting	Value
User name	administrator@vsphere.local
Password	*vsphere_admin_password*

  c Click the **Home** icon above the **Navigator** and choose the **Administration** menu item.

  d On the **Administration** page, click **Licenses** and click the **Licenses** tab.

e Click the **Create New Licenses** icon to add license keys.



f On the **Enter license keys** page, enter license keys for vCenter Server, ESXi and vSAN, one per line, and click **Next**.

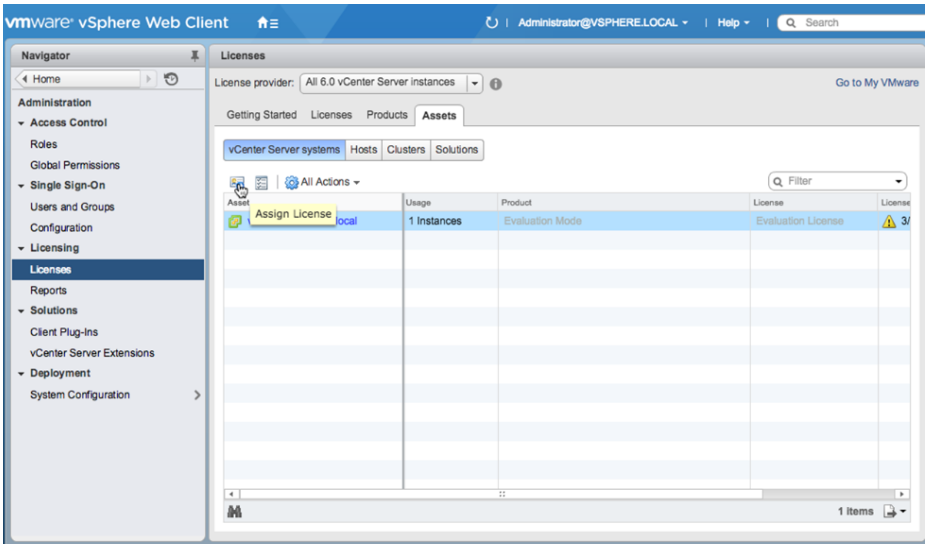
g On the **Edit license name** page, enter a descriptive name for each license key and click **Next**.

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

5 Assign the newly added licenses to the vCenter Server asset.

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**.

6 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 **Add** button.

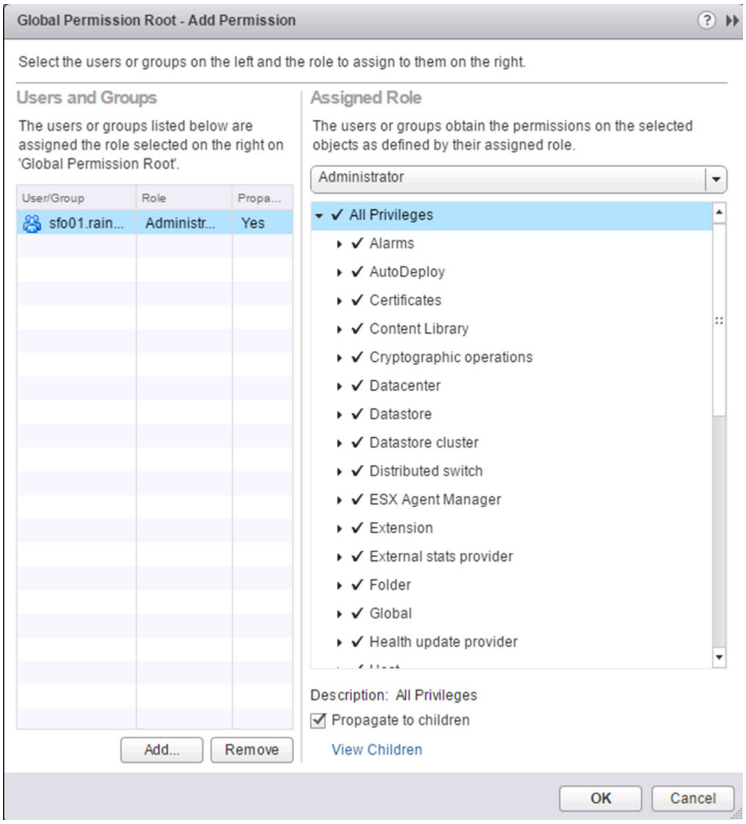
d In the **Global Permissions Root - Add Permissions** window, click the **Add** button.

e Select **sfo01.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**.



Global Permission Root - Add Permission

Select the users or groups on the left and the role to assign to them on the right.

Users and Groups

The users or groups listed below are assigned the role selected on the right on 'Global Permission Root'.

User/Group	Role	Propa...
sfo01.rain...	Administr...	Yes

Assigned Role

The users or groups obtain the permissions on the selected objects as defined by their assigned role.

Administrator

Description: All Privileges

☑ Propagate to children

Configure the Management Cluster in Region A

You must now create and configure the management cluster.

This process consists of the following actions:

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

Procedure

1. Log in to the Management 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*

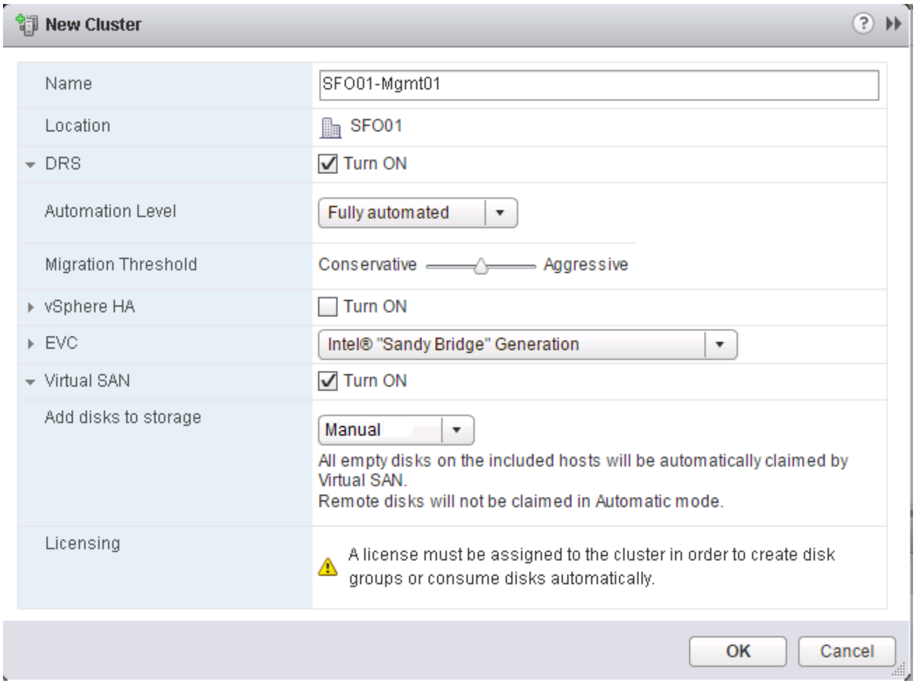
2. Create a Datacenter object.
   a. In the **Navigator**, click **Hosts and Clusters.**
   b. Right-click **mgmt01vc01.sfo01.rainpole.local** and click **New Datacenter**.
   c. In the **New Datacenter** dialog box, enter **`SFO01`** as Datacenter name and click **OK**.

3 Create the management cluster.

   a Right-click the **SFO01** datacenter and click **New Cluster**.

   b In the **New Cluster** wizard, enter the following values and click **OK**.

Setting		Value
Name		SFO01-Mgmt01
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** **Add disks to storage**	Selected **Manual**



New Cluster

Name	SFO01-Mgmt01
Location	SFO01
DRS	☑ Turn ON
Automation Level	Fully automated
Migration Threshold	Conservative ———△——— Aggressive
vSphere HA	□ Turn ON
EVC	Intel® "Sandy Bridge" Generation
Virtual SAN	☑ Turn ON
Add disks to storage	Manual All empty disks on the included hosts will be automatically claimed by Virtual SAN. Remote disks will not be claimed in Automatic mode.
Licensing	⚠ A license must be assigned to the cluster in order to create disk groups or consume disks automatically.

4 Add a host to the management cluster.

   a Right-click the **SFO01-Mgmt01** cluster, and click **Add Host**.

   b On the **Name and location** page, enter `mgmt01esx01.sfo01.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 management cluster.

Setting	Value
Host 2	mgmt01esx02.sfo01.rainpole.local
Host 3	mgmt01esx03.sfo01.rainpole.local
Host 4	mgmt01esx04.sfo01.rainpole.local

6 Add an ESXi host to the active directory domain

a In the **Navigator**, click **Hosts and Clusters** and expand the entire **mgmt01vc01.sfo01.rainpole.local** tree.

b Select the **mgmt01esx01.sfo01.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	sfo01.rainpole.local
Using credentials	Selected
User name	*ad_admin_acct*@sfo01.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 **mgmt01esx01.sfo01.rainpole.local** tree.

b Select the **mgmt01esx01.sfo01.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 **SFO01-Mgmt01** cluster.

b Click the **Datastores** tab.

c Select **vsanDatastore**, and select **Actions > Rename**.

d In the **Datastore - Rename** dialog box, enter **`SFO01A-VSAN01-MGMT01`** as the datastore name, and click **OK**.

Create a vSphere Distributed Switch for the Management Cluster in Region A

After all ESXi hosts have been added to the clusters, create a vSphere Distributed Switch to handle the traffic of the management applications in the SDDC. You must also create port groups to prepare your environment to migrate the Platform Services Controller and vCenter Server instances to the distributed switch.

Procedure

1 Log in to the Management 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 Create vSphere Distributed Virtual Switch.

a In the **Navigator**, click **Networking** and expand the **mgmt01vc01.sfo01.rainpole.local** tree.

b Right-click the **SFO01** datacenter, and select **Distributed Switch > New Distributed Switch** to start the **New Distributed Switch** wizard .

c On the **Name and location** page, enter **`vDS-Mgmt`** 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–Mgmt` distributed switch.

a Right-click the **vDS-Mgmt** distributed switch, and select **Settings > Edit Settings**.

b Click the **Advanced** tab.

c Enter **`9000`** as MTU (Bytes) value, and click **OK**.

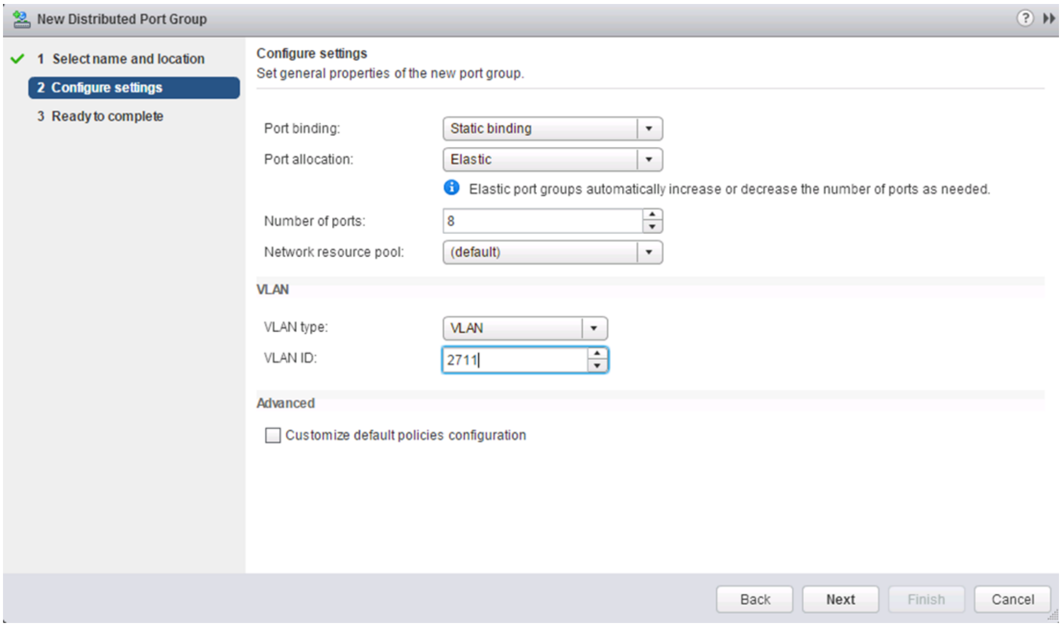
4 Create port groups in the `vDS–Mgmt` distributed switch for the management traffic types.

a Right-click the **vDS-Mgmt** 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-Mgmt-Management	Ephemeral - no binding	VLAN	1611
vDS-Mgmt-vMotion	Static binding	VLAN	1612
vDS-Mgmt-VSAN	Static binding	VLAN	1613
vDS-Mgmt-NFS	Static binding	VLAN	1615
vDS-Mgmt-VR	Static binding	VLAN	1616
vDS-Mgmt-Ext-Management	Static binding	VLAN	130
vDS-Mgmt-Uplink01	Static binding	VLAN	2711
vDS-Mgmt-Uplink02	Static binding	VLAN	2712

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



New Distributed Port Group

✓ 1 Select name and location

2 Configure settings

3 Ready to complete

Configure settings

Set general properties of the new port group.

Port binding: Static binding

Port allocation: Elastic

Elastic port groups automatically increase or decrease the number of ports as needed.

Number of ports: 8

Network resource pool: (default)

VLAN

VLAN type: VLAN

VLAN ID: 2711

Advanced

□ Customize default policies configuration

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-Mgmt** 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, mgmt01esx01.sfo01.rainpole.local, to the `vDS-Mgmt` distributed switch by migrating their VMkernel and virtual machine network adapters.

   a Right-click the **vDS-Mgmt** 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 **mgmt01esx01.sfo01.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 1** 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-Mgmt-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-Mgmt-vSAN** port group, click **OK**, and click **Next**.

   e On the **Port properties** page, select the **Virtual SAN** check box and click **Next**.

   f On the **IPv4 settings** page, select **Use static IPv4 settings**, enter IP address **`172.16.13.101`**, enter subnet **`255.255.255.0`**, and click **Next**.

   g Click **Finish**.

h Repeat steps 7c. - 7f. to create the remaining VMkernel network adapters.

Port Group	Port Properties	IPv4 Address	Netmask
vDS-Mgmt-VR	■ vSphere Replication traffic ■ vSphere Replication NFC traffic	172.16.16.101	255.255.255.0
vDS-Mgmt-NFS	N/A	172.16.15.101	255.255.255.0

i On the **Analyze impact** page, click **Next**.

j 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 **mgmt01vc01.sfo01.rainpole.local** tree.

b Click on **mgmt01esx01.sfo01.rainpole.local**.

c Click the **Configure** tab then select **VMkernel adapters**.

d Click the **Add host networking** icon and select **VMkernel Netowrk Adapter** and click **Next**.

e On the **Add Networking** page, select **Select an existing network**, browse to select the **vDS-Mgmt-vMotion** port group, click **OK**, and click **Next**.

f On the **Port properties** page, select **vMotion** from the **TCP/IP Stack** drop-down and click **Next.**

g On the **IPv4 settings** select **Use static IPv4 settings** enter IP address `172.16.12.101`, enter 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 the previous step, 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 on **Routing** and enter `172.16.12.253` for the **default gateway** and click **OK**.

11 Migrate the Management Platform Services Controller and vCenter Server instances from the standard switch to the distributed switch.

a In the **Navigator**, click **Networking** and expand the **mgmt01vc01.sfo01.rainpole.local** tree.

b Right-click the **vDS-Mgmt** 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-Mgmt-Management

d On the **Select VMs to migrate** page, select **mgmt01psc01.sfo01.rainpole.local**, **comp01psc01.sfo01.rainpole.local** and **mgmt01vc01.sfo01.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-Mgmt** 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
Virtual SAN Traffic	High
NFS Traffic	Low
vMotion Traffic	Low
vSphere Replication (VR) Traffic	Low
Management Traffic	Normal
vSphere Data Protection Backup Traffic	Low
Virtual Machine Traffic	High
Fault Tolerance Traffic	Low
iSCSI Traffic	Low

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

a In the **Navigator**, click **Networking** and expand the **SFO01** datacenter.

b Right-click the **vDS-Mgmt** 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 *mgmt01esx01.sfo01.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 2**, 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 **SFO01** datacenter.

b Select the **vDS-MGMT** 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 **mgmt01vc01.sfo01.rainpole.local** tree.

b Click on **mgmt01esx01.sfo01.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 Region A

This step is to set the vSAN storage policy for the Platform Services Controller and vCenter Server appliances.

Procedure

1 Log in to the Management 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 Reset the vSAN Storage Policy to default for the ESXi host that is used for bootstrap.

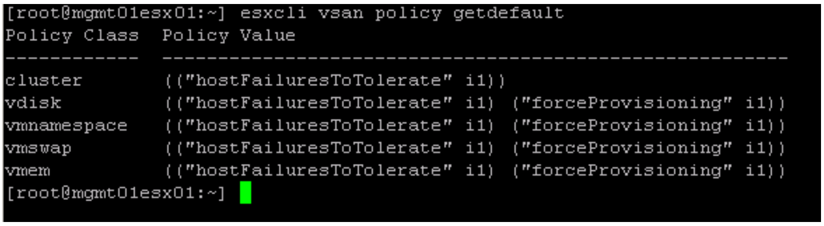
a Open an SSH connection to the ESXi host `mgmt01esx01.sfo01.rainpole.local`.

b Log in using the following credentials.

Setting	Value
User name	root
Password	*esxi_root_user_password*

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

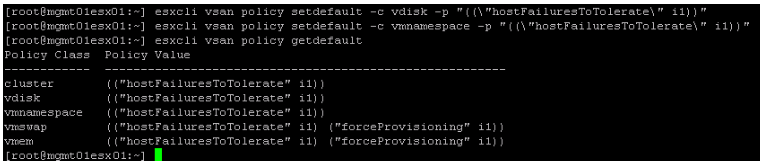
```
esxcli vsan policy getdefault
```



```
[root@mgmt01esx01:~] 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@mgmt01esx01:~]
```

d Modify the default vSAN storage policy to force provisioning of vSAN datastore.

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



```
[root@mgmt01esx01:~] esxcli vsan policy setdefault -c vdisk -p "((\"hostFailuresToTolerate\" i1))"
[root@mgmt01esx01:~] esxcli vsan policy setdefault -c vmnamespace -p "((\"hostFailuresToTolerate\" i1))"
[root@mgmt01esx01:~] 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@mgmt01esx01:~]
```

Create vSAN Disk Groups for the Management Cluster in Region A

vSAN disk groups must be created on each host that is contributing storage to the vSAN datastore.

Procedure

1 Log in to the Management 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 In the **Navigator**, select **Hosts and Clusters** and expand the **mgmt01vc01.sfo01.rainpole.local** tree.

3 Click on the **SFO01-Mgmt01** cluster and click the **Configure** tab.

4 Under **Virtual SAN**, click **Disk Management**.

5 Click on **mgmt01esx02.sfo01.rainpole.local** and click on 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**.

7 Repeat steps 5 and 6 for **mgmt01esx03.sfo01.rainpole.local** and **mgmt01esx04.sfo01.rainpole.local**.

8 Assign a license to vSAN.

   a Right Click the **SFO01-Mgmt01** cluster and select **Assign License**.

   b In the **SFO01-Mgmt01 - Assign License** window select the previously added **VSAN License** and click **OK.**

Enable vSphere HA on the Management Cluster in Region A

After vSphere vSphere Distributed Switch has been created and connected with all hosts, enable vSphere HA on the cluster.

Procedure

1 Log in to the Management 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 In the Navigator, click **Host and Clusters**.

   a Expand the **mgmt01vc01.sfo01.rainpole.local** inventory.

   b Select the **SFO01-Mgmt01** cluster.

3 Click the **Configure** tab and click **vSphere Availability**.

4 Click **Edit**.

5 In the **Edit Cluster Settings** dialog box, select the **Turn on vSphere HA** check box.

6 Under **Virtual Machine Monitoring**, under **Failures and Responses**, select the following values:

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

7 Click **Admission Control**.

8 Under **Admission Control** enter the 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%

9 Click **OK**.

Change Advanced Options on the ESXi Hosts in the Management Cluster in Region A

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 the Management 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 Change the default ESX Admins group.

a In the **Navigator**, click **Hosts and Clusters**.

b Expand the entire **mgmt01vc01.sfo01.rainpole.local** vCenter inventory tree, and select the **mgmt01esx01.sfo01.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 **mgmt01vc01.sfo01.rainpole.local** vCenter inventory tree, and select the **mgmt01esx01.sfo01.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 **mgmt01vc01.sfo01.rainpole.local** vCenter inventory tree, and select the **mgmt01esx01.sfo01.rainpole.local** host.

c Click the **Configure** tab, click **System > Advanced System Settings**.

d Click the **Edit** button.

e In the **filter** box, enter `ssh` and wait for the search results.

f Change the value of **UserVars.SuppressShellWarning** to **1** and click **OK**.

Mount NFS Storage for the Management Cluster in Region A

You must mount an NFS datastore where vSphere Data Protection will later be deployed.

Procedure

1 Log in to the Management 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 In the **Navigator**, click **Host and Clusters** and expand the **mgmt01vc01.sfo01.rainpole.local** tree.

3 Click on **mgmt01esx01.sfo01.rainpole.local**.

4 Click on **Datastores**.

5 Click the **Create a New Datastore** icon.

The **New Datastore** wizard opens.

6 On the **Type** page, select **NFS** and click **Next**.

7 On the **Select NFS version** page, select **NFS 3** and click **Next.**

8 On the **Name and configuration** page, enter the following datastore information and click **Next**.

Setting	Value
Datastore Name	SFO01A-NFS01-VDP01
Folder	/V2D_vDP_MgmtA_4TB
Server	172.16.15.251

Create and Apply the Host Profile for the Management Cluster in Region A

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

Procedure

1 Log in to the Management 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 Create a Host Profile from *mgmt01esx01.sfo01.rainpole.local*.

a In the **Navigator**, select **Hosts and Clusters** and expand the **mgmt01vc01.sfo01.rainpole.local** tree.

b Right-click **mgmt01esx01.sfo01.rainpole.local** and choose **Host Profiles > Extract Host Profile**.

c In the **Extract Host Profile** window, enter **`SFO01-Mgmt01`** as the name of the host profile and click **Next**.

d On 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 **mgmt01vc01.sfo01.rainpole.local** tree.

b Right-click the **SFO01-Mgmt01** cluster, and choose **Host Profiles > Attach Host Profile**.

c In the **Attach Host Profile** window, click **SFO01-Mgmt01**, select the **Skip Host Customization** box, and click **Finish**.

4 Create Host Customizations for the hosts in the management cluster.

   a Click on the **Home** icon and choose **Policies and Profiles** from the drop down menu.

   b In the **Navigator**, click **Host Profiles**.

   c Right-click **SFO01-Mgmt01** and choose **Export Host Customizations**. Click **Save**.

   d Choose a safe place to store the *SFO01-Mgmt01_host_customizations.csv* that is generated.

   e Open the file with 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
mgmt01esx01.sfo01.rainpole.local	*ad_admin_password*	*ad_admin_acct@sfo01.rainpole.local*	mgmt01esx01
mgmt01esx02.sfo01.rainpole.local	*ad_admin_password*	*ad_admin_acct@sfo01.rainpole.local*	mgmt01esx02
mgmt01esx03.sfo01.rainpole.local	*ad_admin_password*	*ad_admin_acct@sfo01.rainpole.local*	mgmt01esx03
mgmt01esx04.sfo01.rainpole.local	*ad_admin_password*	*ad_admin_acct@sfo01.rainpole.local*	mgmt01esx04

ESXi Host	Host virtual NIC vDS-Mgmt:vDS-Mgmt-Management:management->IP address settings Host IPv4 address	Host virtual NIC vDS-Mgmt:vDS-Mgmt-Management:management->IP address settings SubnetMask
mgmt01esx01.sfo01.rainpole.local	172.16.11.101	255.255.255.0
mgmt01esx02.sfo01.rainpole.local	172.16.11.102	255.255.255.0
mgmt01esx03.sfo01.rainpole.local	172.16.11.103	255.255.255.0
mgmt01esx04.sfo01.rainpole.local	172.16.11.104	255.255.255.0

ESXi Host	Host virtual NIC vDS-Mgmt:vDS-Mgmt-NFS:<UNRESOLVED>->IP address settings Host IPv4 address	Host virtual NIC vDS-Mgmt:vDS-Mgmt-NFS:<UNRESOLVED>->IP address settingsSubnetMask
mgmt01esx01.sfo01.rainpole.local	172.16.15.101	255.255.255.0
mgmt01esx02.sfo01.rainpole.local	172.16.15.102	255.255.255.0
mgmt01esx03.sfo01.rainpole.local	172.16.15.103	255.255.255.0
mgmt01esx04.sfo01.rainpole.local	172.16.15.104	255.255.255.0

ESXi Host	Host virtual NIC vDS-Mgmt:vDS-Mgmt-VR:vSphereReplication,vSphereReplicationNFC->IP address settingsHost IPv4 address	Host virtual NIC vDS-Mgmt:vDS-Mgmt-VR:vSphereReplication,vSphereReplicationN >IP address settingsSubnetMask
mgmt01esx01.sfo01.rainpole.local	172.16.16.101	255.255.255.0
mgmt01esx02.sfo01.rainpole.local	172.16.16.102	255.255.255.0
mgmt01esx03.sfo01.rainpole.local	172.16.16.103	255.255.255.0
mgmt01esx04.sfo01.rainpole.local	172.16.16.104	255.255.255.0

ESXi Host	Host virtual NIC vDS-Mgmt:vDS-Mgmt-VSAN:vsan->IP address settings Host IPv4 address	Host virtual NIC vDS-Mgmt:vDS-Mgmt-VSAN:vsan->IP address settings SubnetMask
mgmt01esx01.sfo01.rainpole.local	172.16.13.101	255.255.255.0
mgmt01esx02.sfo01.rainpole.local	172.16.13.102	255.255.255.0

ESXi Host	Host virtual NIC vDS-Mgmt:vDS-Mgmt-VSAN:vsan->IP address settings Host IPv4 address	Host virtual NIC vDS-Mgmt:vDS-Mgmt-VSAN:vsan->IP address settings SubnetMask
mgmt01esx03.sfo01.rainpole.local	172.16.13.103	255.255.255.0
mgmt01esx04.sfo01.rainpole.local	172.16.13.104	255.255.255.0

ESXi Host	Host virtual NIC vDS-Mgmt:vDS-Mgmt-vMotion:vmotion->IP address settings Host IPv4 address	Host virtual NIC vDS-Mgmt:vDS-Mgmt-vMotion:vmotion->IP address settings SubnetMask
mgmt01esx01.sfo01.rainpole.local	172.16.12.101	255.255.255.0
mgmt01esx02.sfo01.rainpole.local	172.16.12.102	255.255.255.0
mgmt01esx03.sfo01.rainpole.local	172.16.12.103	255.255.255.0
mgmt01esx04.sfo01.rainpole.local	172.16.12.104	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 On the **Select hosts** page, click **Next**.

k On the **Customize hosts** page, click the **Browse** button to find the customization CSV file where it was stored, and then click **Finish**.

5 Remediate the hosts in the management cluster.

a On the **Policies and Profiles** page, click **SFO01-Mgmt01**, click the **Monitor** tab, and then click the **Compliance** tab.

b Click **SFO01-Mgmt01** in the **Host/Cluster** column and click **Check Host Profile Compliance**. This compliance test will show that the first host is Compliant, but the other hosts are Not Compliant.

c Click on each of the non-compliant hosts, click **Remediate Hosts Based on its Host Profile**, and then click **Finish** on the wizard that appears.

All hosts should show a `Compliant` status in the **Host Compliance** column.

6 Schedule nightly compliance checks.

a On the **Policies and Profiles** page, click **SFO01-Mgmt01**, 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 *SFO01-Mgmt01 Complance 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 on Management Virtual Machines in Region A

After you apply the host profile to all of the hosts, set the storage policy of the Management Virtual Machines 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 the Management 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 In the **Navigator**, click **Hosts and Clusters**.

3 Expand the **mgmt01vc01.sfo01.rainpole.local** tree.

4 Select the **mgmt01psc01** 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.

9 Repeat this step to apply the Virtual SAN Default Storage Policy on **comp01psc01** and **mgmt01vc01** virtual machines.

Create the VM and Template Folders in Region A

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

You repeat this procedure eight times to create all of the management application folders listed in the following table.

Table 2-4. Folders for the Management Applications in Region A

Management Applications	Folder
vCenter Server and Platform Services Controllers	MGMT01
vRealize Automation, vRealize Orchestrator, and vRealize Business	vRA01
vRealize Automation (Proxy Agent) and vRealize Business (Data Collector)	vRA01IAS
vRealize Operations Manager	vROps01
vRealize Operations Manager (Remote Collectors)	vROps01RC
vRealize Log Insight	vRLI01
NSX Manager, Controllers, and Edges	NSX01
VMware Site Recovery Manger and vSphere Data Protection	BCDR01

Procedure

1 Log in to the Management 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 Create folders for each of the management applications.

  a In the **Navigator**, click **VMs and Templates**.

  b Expand the **mgmt01vc01.sfo01.rainpole.local** control tree.

  c Right-click the **SFO01** 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.

3 Move the vCenter Server and Platform Services Controller virtual machines to the `MGMT01` folder.

  a In the **Navigator**, click **VMs and Templates**.

  b Expand the **mgmt01vc01.sfo01.rainpole.local** tree.

  c Expand the **Discovered Virtual Machines** folder.

  d Drag **mgmt01vc01**, **mgmt01psc01**, and **comp01psc01** to the `MGMT01` folder.

4 Delete the **Discovered Virtual Machines** folder.

   a In the **Navigator**, click **VMs and Templates**.

   b Expand the **mgmt01vc01.sfo01.rainpole.local** tree.

   c Right-click the **Discovered Virtual Machines** folder and choose **Remove from Inventory**.

Create Anti-Affinity Rules for the Platform Services Controller in Region A

Anti-Affinity rules prevent virtual machines from running on the same host. This helps to maintain redundancy in the event of host failures.

Procedure

1 Log in to the Management 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 In the **Navigator**, select **Hosts and Clusters** and expand the **mgmt01vc01.sfo01.rainpole.local** control tree.

3 Select the **SFO01-Mgmt01** cluster and click the **Configure** tab.

4 On the **Configure** page, click **VM/Host Rules**.

5 On the **VM/Host Rules** page, click the **Add** button to create a new VM/Hosts Rule.

6 In the **Create VM/Host Rule** dialog, enter `anti-affinity-rule-psc` in the **Name** field, ensure the **Enable rule** checkbox is selected, select **Separate Virtual Machines** from the **Type** drop down menu, and click the **Add** button.

7 In the **Add Rule Member** dialog, select **mgmt01psc01** and **comp01psc01** and click **OK**.

8 Click **OK** to create the rule.

Create VM Groups to Define Startup Order in the Management Cluster in Region A

VM Groups allow you to define the startup order of virtual machines. Startup orders are used during vSphere HA events such that vSphere HA powers on virtual machines in the correct order.

Procedure

1 Log in to the Management 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 In the **Navigator**, select **Host and Clusters** and expand the **mgmt01vc01.sfo01.rainpole.local** tree.

3 Create a VM Group for the Platform Services Controllers.

   a Select the **SFO01-Mgmt01** cluster and click the **Configure** tab.

   b On the **Configure** page, click **VM/Host Groups**.

   c On the **VM/Host Groups** page, click the **Add** button.

   d In the **Create VM/Host Group** dialog, enter `Platform Services Controllers` in the **Name** field, select **VM Group** from the **Type** drop down, and click the **Add** button.

   e In the **Add VM/Host Group Member** dialog, select **mgmt01psc01** and **comp01psc01** and click **OK**.

4 Create a VM Group for the vCenter Server virtual machine.

   a Select the **SFO01-Mgmt01** cluster and click the **Configure** tab.

   b On the **Configure** page, click **VM/Host Groups**.

   c On the **VM/Host Groups** page, click the **Add** button.

   d In the **Create VM/Host Group** dialog, enter `vCenter Servers` in the **Name** field, select **VM Group** from the **Type** drop down, and click the **Add** button.

   e In the **Add VM/Host Group Member** dialog, select **mgmt01vc01** and click **OK**.

5 Create a Rule to power on the Platform Services Controllers followed by the vCenter Servers.

   a Select the **SFO01-Mgmt01** cluster and click the **Configure** tab.

   b On the **Configure** page, click **VM/Host Rules**.

   c On the **VM/Host Rules** page, click the **Add** button.

   d In the **Create VM/Host Rule** dialog, enter `SDDC Management Virtual Machines` in the **Name** field, ensure the **Enable rule** check box is selected, select **Virtual Machines to Virtual Machines** from the **Type** drop down.

   e Select **Platform Services Controllers** from the **First restart VMs in VM group** drop down.

   f Select **vCenter Servers** from the **Then restart VMs in VM group** and click **OK**.

Deploy and Configure the Management Cluster NSX Instance in Region A

This design uses two separate NSX instances per region. One instance is tied to the Management vCenter Server, and the other instance is tied to the Compute vCenter Server. Deploy and configure the NSX instance for the management cluster in Region A.

Procedure

1 Deploy the NSX Manager for the Management Cluster NSX Instance in Region A

For this 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 Deploy the NSX Controllers for the Management Cluster NSX Instance in Region A

After the NSX Manager is successfully connected to the Management vCenter Server, you must promote it to the primary role and deploy the three NSX Controller nodes that form the NSX Controller cluster.

3 Prepare the ESXi Hosts in the Management Cluster for NSX in Region A

You must install the NSX kernel modules on the management cluster ESXi hosts to be able to use NSX.

4 Configure the NSX Logical Network for the Management Cluster in Region A

After all the deployment tasks are ready, you must configure the NSX logical network.

5 Update the Host Profile for the Management Cluster in Region A

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

6 Deploy the Platform Services Controllers Load Balancer in Region A

You configure load balancing for all services and components related to Platform Services Controllers (PSC) using an NSX Edge load balancer.

7 Configure NSX Dynamic Routing in the Management Cluster in Region A

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 management cluster, deploying two NSX Edge devices and a Universal Distributed Logical Router (UDLR).

8 Distributed Firewall Configuration for Management Applications

Configuring a distributed firewall for use with your SDDC increases the security level of your environment by allowing only the network traffic that is required for the SDDC to run. The firewall rules you define allow access to management applications.

9 Test the Management Cluster NSX Configuration in Region A

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.

10 Deploy Application Virtual Networks in Region A

Deploy the application virtual networks.

11 Deploy the NSX Load Balancer in Region A

Deploy a load balancer for use by management applications connected to the AVN, `Mgmt-xRegion01-VXLAN`.

Deploy the NSX Manager for the Management Cluster NSX Instance in Region A

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

First assign a domain service account that NSX uses to the vCenter Server Administrator role. After that deploy the NSX Manager virtual appliance for the management cluster. After the NSX Manager is deployed connect it to the Management vCenter Server instance.

Procedure

1 Assign an NSX Domain Service Account and Deploy the NSX Manager Appliance in Region A

Assign a domain service account for use by NSX to access the vCenter Server Administrator role.

2 Connect NSX Manager to the Management vCenter Server in Region A

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

3 Assign Administrative Access to NSX in Region A

Assign the administrator@vsphere.local account access to NSX.

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

Assign a domain service account for use by NSX to access the vCenter Server Administrator role.

Procedure

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

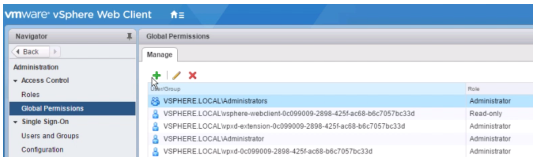
a Open a Web browser and go to **`https://mgmt01vc01.sfo01.rainpole.local/vsphere-client`**.

b Log in using the following credentials.

Setting	Value
User name	administrator@vsphere.local
Password	*vsphere_admin_password*

2 In the **Navigator**, click **Administration** and click **Global Permissions**.

3 Click the **Add** icon.



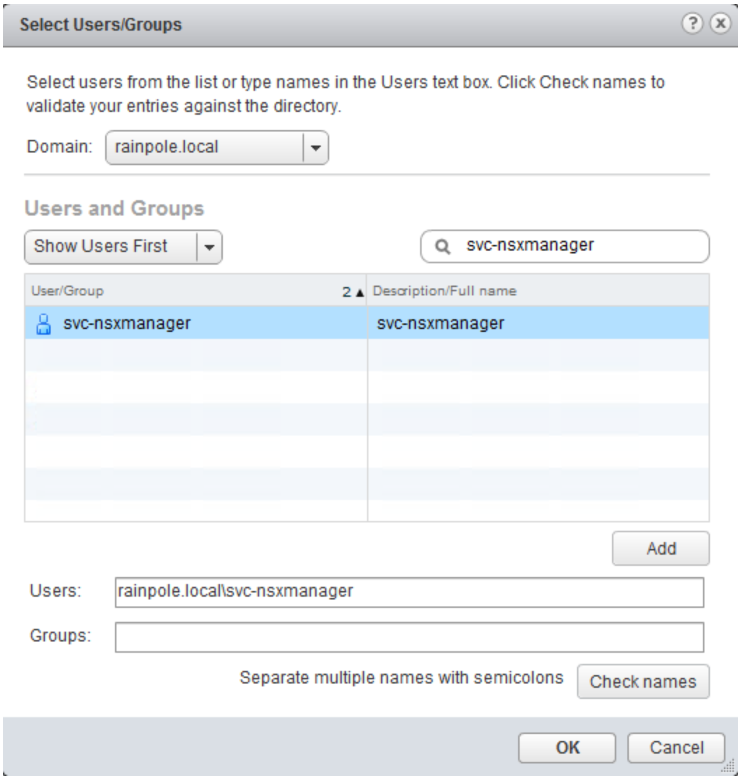
User/Group	Role
VSPHERE.LOCAL\Administrators	Administrator
VSPHERE.LOCAL\vsphere-webclient-0c099009-2898-425f-ac68-b6c7057bc33d	Read-only
VSPHERE.LOCAL\vpxd-extension-0c099009-2898-425f-ac68-b6c7057bc33d	Administrator
VSPHERE.LOCAL\Administrator	Administrator
VSPHERE.LOCAL\vpxd-0c099009-2898-425f-ac68-b6c7057bc33d	Administrator

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**.



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

Search: svc-nsxmanager

User/Group	Description/Full name
svc-nsxmanager	svc-nsxmanager

Users: rainpole.local\svc-nsxmanager

Groups:

Separate multiple names with semicolons

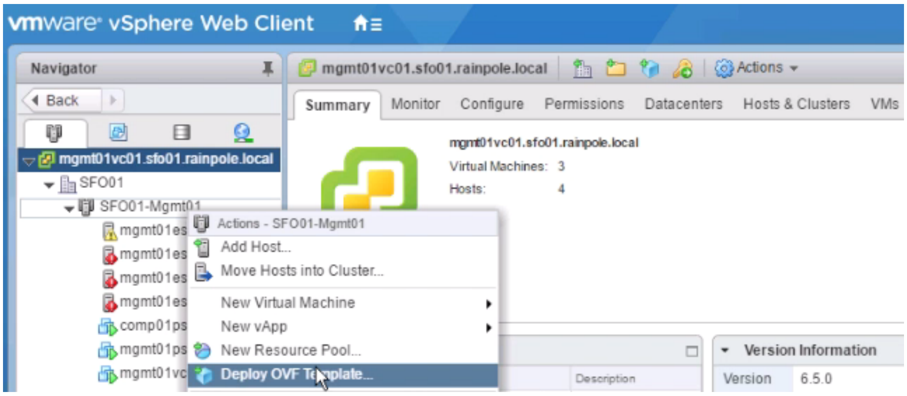
8 Click **OK**.

9 In the **Global Permission Root - Add Permission** dialog box, select **Administrator** as the **Assigned Role** and select the **Propagate to children** check box.

10 Click **OK**.

11 In the **Navigator**, expand the entire **mgmt01vc01.sfo01.rainpole.local** tree control.

12 Right-click the **SFO01-Mgmt01** cluster 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	mgmt01nsxm01
Datacenter or folder	NSX01

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

Setting	Value
Cluster	SFO01-Mgmt01

16 On the **Review details** page, review the **extra configuration option** check box, and 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
VM storage policy	vSAN Default Storage Policy
Datastore	SFO01A-VSAN01-MGMT01

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

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

Setting	Value
DNS Server List	172.16.11.5,172.16.11.4
Domain Search List	sfo01.rainpole.local
Default IPv4 Gateway	172.16.11.253
Hostname	mgmt01nsxm01.sfo01.rainpole.local

Setting	Value
Network 1 IPv4 Address	172.16.11.65
Network 1 Netmask	255.255.255.0
Enable SSH	Selected
NTP Server List	■ ntp.sfo01.rainpole.local ■ ntp.lax01.rainpole.local
CLI "admin" User Password / enter	*mgmtnsx_admin_password*
CLI "admin" User Password / confirm	*mgmtnsx_admin_password*
CLI Privilege Mode Password / enter	*mgmtnsx_priviledge_password*
CLI Privilege Mode Password / confirm	*mgmtnsx_priviledge_password*

21 On the **Ready to complete** page, click **Finish**.

22 In the **Navigator**, expand the entire **mgmt01vc01.sfo01.rainpole.local** tree, select the mgmt01nsxm01 VM, and click the **Power on** button.

Connect NSX Manager to the Management vCenter Server in Region A

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

Procedure

1 Log in to the Management NSX Manager appliance user interface.

   a Open a Web browser and go to `https://mgmt01nsxm01.sfo01.rainpole.local`.

   b Log in using the following credentials.

Setting	Value
User name	admin
Password	*nsx_manager_admin_password*

2 Click **Manage vCenter Registration**.

3 Under **Lookup Service**, click **Edit**.

4 In the **Lookup Service** dialog box, enter the following settings and click **OK**.

Setting	Value
Lookup Service IP	sfo01psc01.sfo01.rainpole.local
Lookup Service Port	443
SSO Administrator User Name	administrator@vsphere.local
Password	*vsphere_admin_password*

5 In the **Trust Certificate?** dialog box, click **Yes**.

6 Under **vCenter Server**, click **Edit**.

7 In the **vCenter Server** dialog box, enter the following settings, and click **OK**.

Setting	Value
vCenter Server	mgmt01vc01.sfo01.rainpole.local
vCenter User Name	svc-nsxmanager@rainpole.local
Password	*svc-nsxmanager_password*

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 the `Connected` status.

Assign Administrative Access to NSX in Region A

Assign the administrator@vsphere.local account access to NSX.

Procedure

1 Log out from the Management vCenter Server session in the vSphere Web Client.

2 Log in to the Management 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	svc-nsxmanager@rainpole.local
Password	*svc-nsxmanager_password*

3 In the **Navigator**, click **Networking & Security** and click **NSX Managers**.

4 Under **NSX Managers**, click the **172.16.11.65** instance.

5 Click the **Manage** tab and click **Users**.

6 Click the **Add** icon.

7 On the **Identify User** page, select the **Specify a vCenter user** radio button, enter **`administrator@vsphere.local`** in the text box, and click **Next**.

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

Deploy the NSX Controllers for the Management Cluster NSX Instance in Region A

After the NSX Manager is successfully connected to the Management vCenter Server, you must promote it to the primary role and 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://mgmt01vc01.sfo01.rainpole.local/vsphere-client`.

   b. Log in using the following credentials.

Setting	Value
User name	administrator@vsphere.local
Password	*vsphere_admin_password*

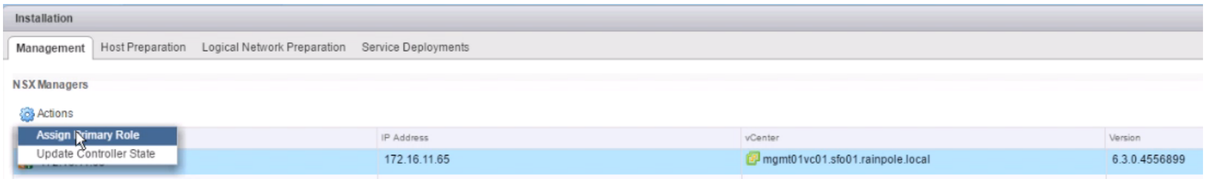
2. Promote the NSX Manager to the primary role.

   a. Under **Inventories**, click **Networking & Security**.

   b. In the **Navigator**, click **Installation**.

   c. On the **Management** tab, select the **172.16.11.65** instance.

   d. Click the **Actions** menu and click **Assign Primary Role**.



IP Address	vCenter	Version
172.16.11.65	mgmt01vc01.sfo01.rainpole.local	6.3.0.4556899

   e. In the **Assign Primary Role confirmation** dialog box, click **Yes**.

3. Configure an IP pool for the NSX Controller cluster.

   a. In the **Navigator**, click **NSX Managers**.

   b. Under **NSX Managers**, click the **172.16.11.65** instance.

   c. Click the **Manage** tab, click **Grouping Objects**, click **IP Pools**, and click the **Add New IP Pool** icon.

   d. In the **Add Static IP Pool** dialog box, enter the following settings and click **OK**.

Setting	Value
Name	Mgmt01-NSXC01
Gateway	172.16.11.253
Prefix Length	24
Primary DNS	172.16.11.5
Secondary DNS	172.16.11.4
DNS Suffix	sfo01.rainpole.local
Static IP Pool	172.16.11.118-172.16.11.120

4 Deploy the NSX Controller cluster.

   a In the **Navigator**, click **Networking & Security** to go back, and click **Installation**.

   b 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-mgmt-01
NSX Manager	172.16.11.65
Datacenter	SFO01
Cluster/Resource Pool	SFO01-Mgmt01
Datastore	SFO01A-VSAN01-MGMT01
Folder	NSX01
Connected To	vDS-Mgmt-Management
IP Pool	Mgmt01-NSXC01
Password	*mgmtnsx_controllers_password*
Confirm Password	*mgmtnsx_controllers_password*

   d After the **Status** of the controller node changes to `Connected`, repeat the step and deploy the two remaining NSX Controller nodes in the controller cluster with the same configuration.

5 Configure DRS affinity rules for the NSX Controller nodes.

   a Go back to the **Home** page.

   b In the **Navigator**, click **Hosts and Clusters**, and expand the **mgmt01vc01.sfo01.rainpole.local** tree control.

   c Select the **SFO01-Mgmt01** cluster, and click the **Configure** tab.

   d Under **Configuration**, click **VM/Host Rules**.

   e Click **Add**.

   f In the **SFO01-Mgmt01 - 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 **SFO01-Mgmt01 - Create VM/Host Rule** dialog box, click **OK**.

Prepare the ESXi Hosts in the Management Cluster for NSX in Region A

You must install the NSX kernel modules on the management cluster ESXi hosts to be able to use NSX.

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.

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

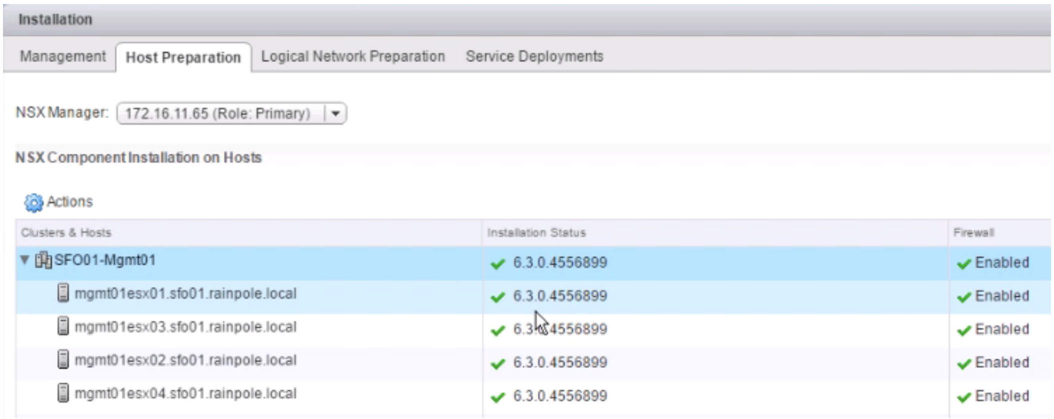
a In the **Navigator**, click **Networking & Security**.

b Click **Installation**, and click the **Host Preparation** tab.

c Select **172.16.11.65** from the **NSX Manager** drop-down menu.

d Under **Installation Status**, click **Install** for the SFO01-Mgmt01 cluster and click **Yes** in the confirmation dialog box.

3 Verify that the **Installation Status** column displays the NSX version for all hosts in the cluster, confirming that the NSX kernel modules are successfully installed.



NSX Manager: 172.16.11.65 (Role: Primary)

NSX Component Installation on Hosts

Clusters & Hosts	Installation Status	Firewall
SFO01-Mgmt01	✓ 6.3.0.4556899	✓ Enabled
mgmt01esx01.sfo01.rainpole.local	✓ 6.3.0.4556899	✓ Enabled
mgmt01esx03.sfo01.rainpole.local	✓ 6.3.0.4556899	✓ Enabled
mgmt01esx02.sfo01.rainpole.local	✓ 6.3.0.4556899	✓ Enabled
mgmt01esx04.sfo01.rainpole.local	✓ 6.3.0.4556899	✓ Enabled

Configure the NSX Logical Network for the Management Cluster in Region A

After all the deployment tasks are ready, you must configure the NSX logical network.

To configure the NSX logical network, you 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://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 Configure the Segment ID allocation.

   a In the **Navigator**, click **Networking & Security**.

   b Click **Installation**, click **Logical Network Preparation**, and click **Segment ID**.

   c Select **172.16.11.65** from the **NSX Manager** drop-down menu.

   d Click **Edit**, enter the following settings, and click **OK**.

Setting	Value
Segment ID pool	5000-5200
Enable Multicast addressing	Selected
Multicast addresses	239.1.0.0-239.1.255.255
Universal Segment ID Pool	30000-39000
Enable Universal Multicast addressing	Selected
Universal Multicast addresses	239.2.0.0-239.2.255.255

3 Configure the VXLAN networking.

   a Click the **Host Preparation** tab.

   b Under **VXLAN**, click **Not Configured** on the **SFO01-Mgmt01** row, enter the following settings, and click **OK**.

Setting	Value
Switch	vDS-Mgmt
VLAN	1614
MTU	9000
VMKNic IP Addressing	Use DHCP
VMKNic Teaming Policy	Load Balance - SRCID
VTEP	2

4 Configure the transport zone.

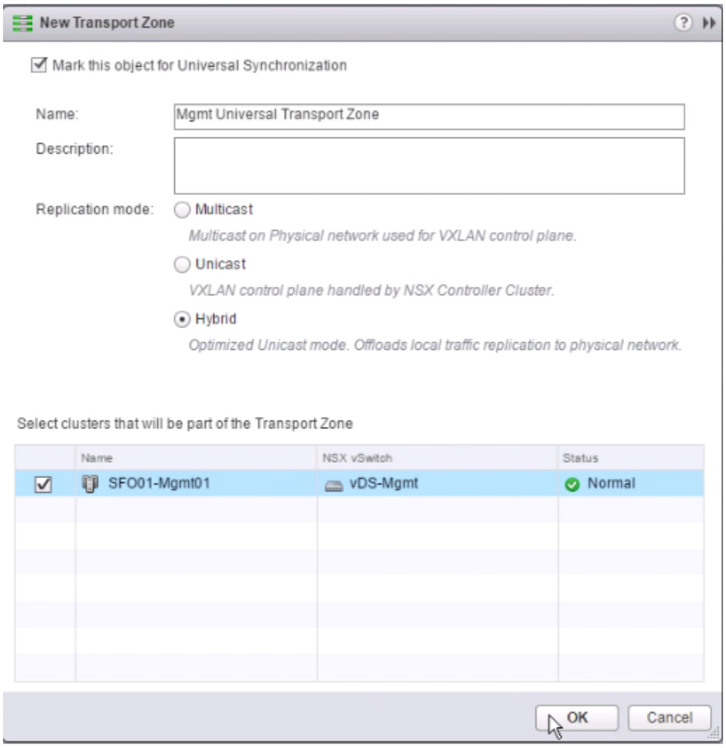
   a On the **Installation** page, click the **Logical Network Preparation** tab and click **Transport Zones**.

   b Select **172.16.11.65** from the **NSX Manager** drop-down menu.

c Click the **Add New Transport zone** icon.

d In the **New Transport Zone** dialog box, enter the following settings and click **OK**.

Setting	Value
Mark this object for Universal Synchronization	Selected
Name	Mgmt Universal Transport Zone
Replication mode	Hybrid
Select clusters that will be part of the Transport Zone	SFO01-Mgmt01



☑ Mark this object for Universal Synchronization

Name: Mgmt Universal Transport Zone

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
☑	SFO01-Mgmt01	vDS-Mgmt	✓ Normal

Update the Host Profile for the Management Cluster in Region A

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://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 Update the Host Profile to the management cluster.

   a In the **Navigator**, select **Policies and Profiles**.

   b Click **Host Profiles**, right click **SFO01-Mgmt01**, and select **Copy Settings from Host**.

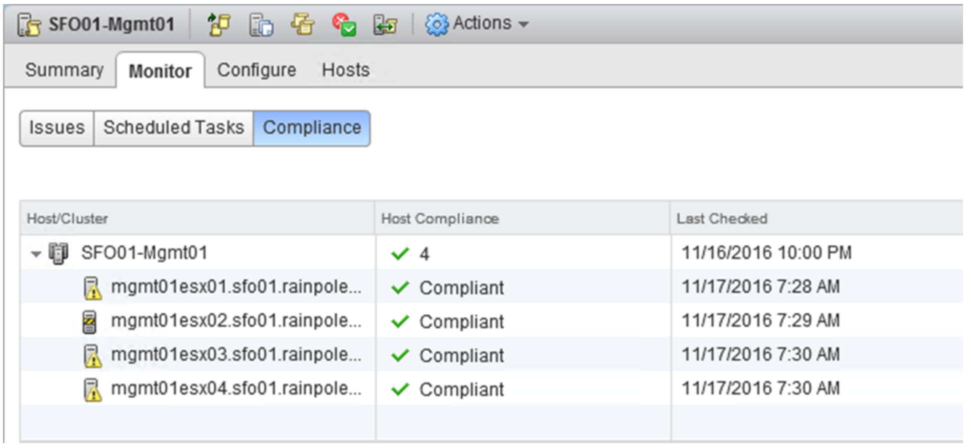
   c Select **mgmt01esx01.sfo01.rainpole.local**, click **Ok**.

3 Verify compliance for the hosts in the management cluster.

   a Click the **Monitor** tab and click **Compliance**.

   b Select **SFO01-Mgmt01** and click the **Host Profile Compliance** button.

   All hosts should display a **Host Compliance** status of `Compliant`.



Host/Cluster	Host Compliance	Last Checked
SFO01-Mgmt01	✓ 4	11/16/2016 10:00 PM
mgmt01esx01.sfo01.rainpole...	✓ Compliant	11/17/2016 7:28 AM
mgmt01esx02.sfo01.rainpole...	✓ Compliant	11/17/2016 7:29 AM
mgmt01esx03.sfo01.rainpole...	✓ Compliant	11/17/2016 7:30 AM
mgmt01esx04.sfo01.rainpole...	✓ Compliant	11/17/2016 7:30 AM

Deploy the Platform Services Controllers Load Balancer in Region A

You configure load balancing for all services and components related to Platform Services Controllers (PSC) using an NSX Edge load balancer.

Procedure

1 Deploy the Platform Services Controller NSX Load Balancer in Region A

   The first step in deploying load balancing for the Platform Services Controller is to deploy the edge services gateway.

2 Create Platform Services Controller Application Profiles in Region A

   Create an application profile to define the behavior of a particular type of network traffic. After configuring a profile, you associate the profile with a virtual server. The virtual server then processes traffic according to the values specified in the profile. Using profiles enhances your control over managing network traffic, and makes traffic-management tasks easier and more efficient.

3 Create Platform Services Controller Server Pools in Region A

   A server pool consists of backend server members. After you create a server pool, you associate a service monitor with the pool to manage and share the backend servers flexibly and efficiently.

4 Create Virtual Servers in Region A

   After load balancing is set up, the NSX load balancer distributes network traffic across multiple servers. When a virtual server receives a request, it chooses the appropriate pool to send traffic to. Each pool consists of one or more members. You create virtual servers for all of the configured server pools.

5 Update DNS Records for the Platform Services Controller Load Balancer in Region A

   You must modify the DNS Address in Region A after setting up load balancing.

Deploy the Platform Services Controller NSX Load Balancer in Region A

The first step in deploying load balancing for the Platform Services Controller is to deploy the edge services gateway.

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 Click **Networking & Security**.

3 In the **Navigator**, click **NSX Edges**.

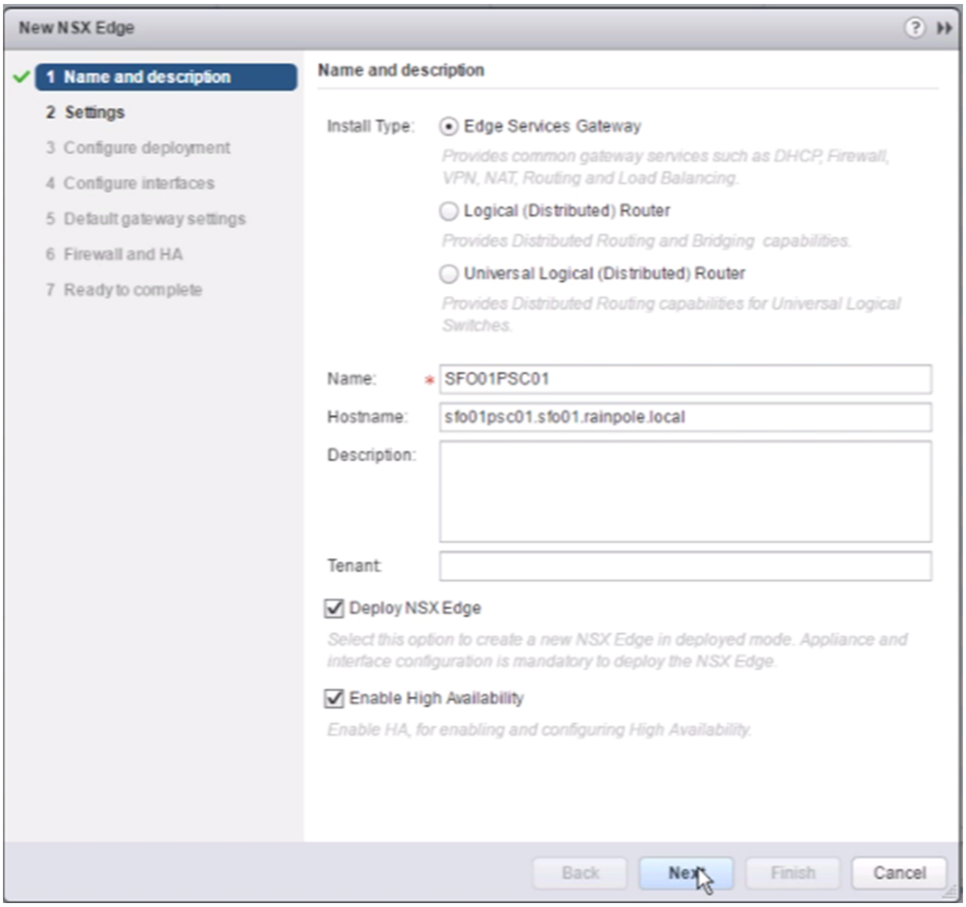
4 Select **172.16.11.65** from the NSX Manager drop-down menu.

5 Click the **Add** icon tab to create an NSX Edge.

   The **New NSX Edge** wizard appears.

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

Setting	Value
Install Type	Edge Services Gateway
Name	SFO01PSC01
Hostname	sfo01psc01.sfo01.rainpole.local
Deploy NSX EDGE	Selected
Enable High Availability	Selected



Name and description

Install Type: ● Edge Services Gateway

Provides common gateway services such as DHCP, Firewall, VPN, NAT, Routing and Load Balancing.

○ Logical (Distributed) Router

Provides Distributed Routing and Bridging capabilities.

○ Universal Logical (Distributed) Router

Provides Distributed Routing capabilities for Universal Logical Switches.

Name: * SFO01PSC01

Hostname: sfo01psc01.sfo01.rainpole.local

Description:

Tenant:

☑ Deploy NSX Edge

Select this option to create a new NSX Edge in deployed mode. Appliance and interface configuration is mandatory to deploy the NSX Edge.

☑ Enable High Availability

Enable HA, for enabling and configuring High Availability.

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

Setting	Value
User Name	admin
Password	*edge_admin_password*
Enable SSH access	Selected
Enable FIPS mode	Deselected
Enable auto rule generation	Selected
Edge Control Level logging	INFO

8 On the **Configure deployment** page, perform the following configuration steps and click **Next**.

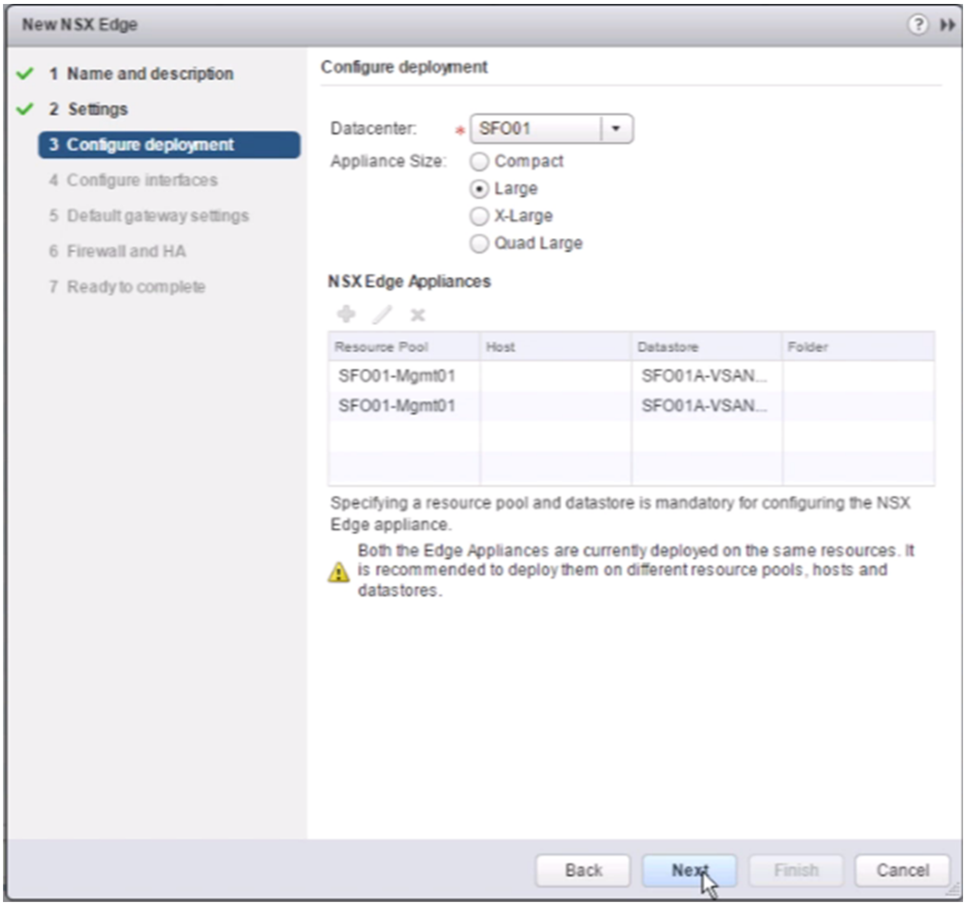
a Select **SF001**, from the **Datacenter** drop-down menu.

b Click **Large** to specify the **Appliance Size**.

c Click the **Add** icon, enter the following settings, and click **OK**.

Setting	Value
Resource pool	SFO01-Mgmt01
Datastore	SFO01A-VSAN01-MGMT01
Folder	NSX01

d To create a second appliance, click the **Add** icon again, make the same selections in the **New NSX Appliance** dialog box, and click **OK**.



Configure deployment

Datacenter: * SFO01

Appliance Size: ○ Compact ● Large ○ X-Large ○ Quad Large

NSX Edge Appliances

Resource Pool	Host	Datastore	Folder
SFO01-Mgmt01		SFO01A-VSAN...	
SFO01-Mgmt01		SFO01A-VSAN...	

Specifying a resource pool and datastore is mandatory for configuring the NSX Edge appliance.

⚠ Both the Edge Appliances are currently deployed on the same resources. It is recommended to deploy them on different resource pools, hosts and datastores.

9 On the **Configure Interfaces** page, click the **Add** icon to configure the PSCLB interface, enter the following settings, click **OK**, and click **Next**.

Setting	Value
Name	PSCLB
Type	Internal
Connected To	vDS-Mgmt-Management
Connectivity Status	Connected
Primary IP Address	172.16.11.71

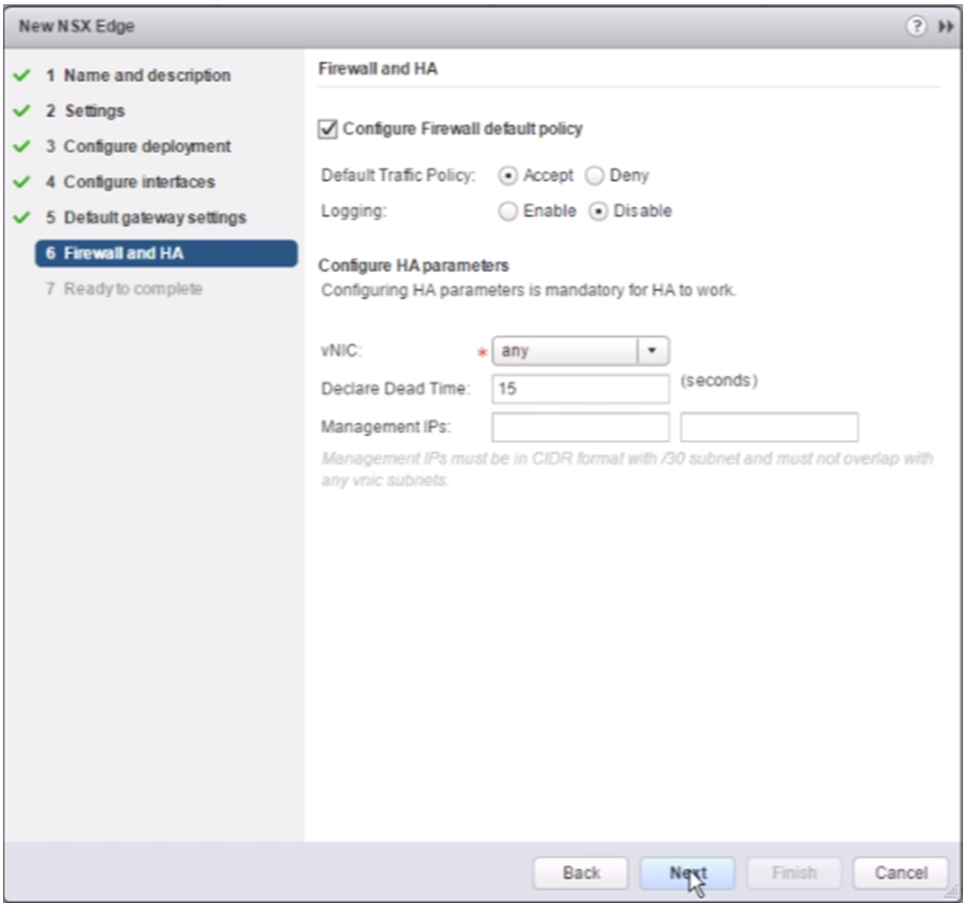
Subnet Prefix Length	24
MTU	9000
Send ICMP Redirect	Selected

10 On the **Default gateway** settings page, enter the following settings and click **Next**.

Setting	Value
Gateway IP	172.16.11.253
MTU	9000

11 On the **Firewall and HA** page, select the following settings and click **Next**.

Setting	Value
Configure Firewall default policy	Selected
Default Traffic Policy	Accept
Logging	Disable
vNIC	any
Declare Dead Time	15



Firewall and HA

☑ Configure Firewall default policy

Default Trafic Policy: ● Accept ○ Deny

Logging: ○ Enable ● Disable

Configure HA parameters

Configuring HA parameters is mandatory for HA to work.

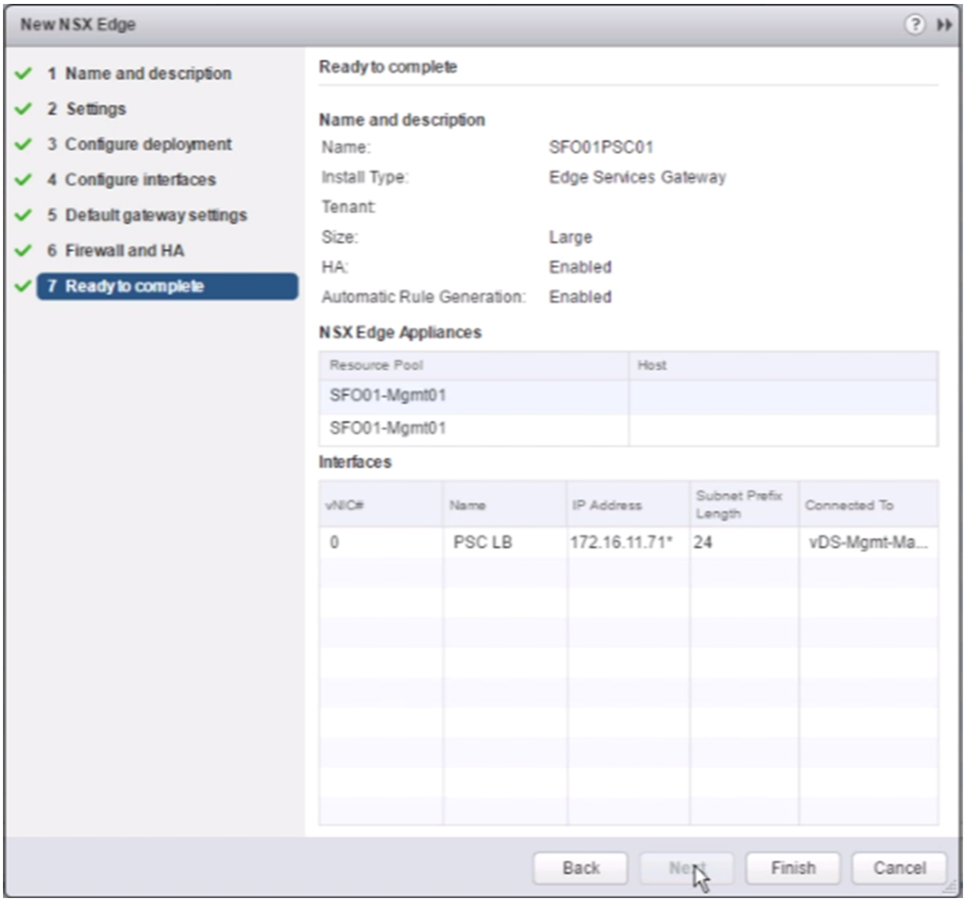
vNIC: * any

Declare Dead Time: 15 (seconds)

Management IPs:

Management IPs must be in CIDR format with /30 subnet and must not overlap with any vnic subnets.

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



Ready to complete

Name and description

Name:	SFO01PSC01
Install Type:	Edge Services Gateway
Tenant:	
Size:	Large
HA:	Enabled
Automatic Rule Generation:	Enabled

NSX Edge Appliances

Resource Pool	Host
SFO01-Mgmt01	
SFO01-Mgmt01	

Interfaces

vNIC#	Name	IP Address	Subnet Prefix Length	Connected To
0	PSC LB	172.16.11.71*	24	vDS-Mgmt-Ma...

13 Enable HA logging.

a In the **Navigator**, click **NSX Edges**.

b Select **172.16.11.65** from the **NSX Manager** drop-down menu.

c Double-click the device labeled **SFO01PSC01**.

d Click the **Manage** tab and click the **Settings** tab.

e Click **Change** in the **HA Configuration** window.

f Select the `Enable Logging` checkbox and click **OK**.

14 Enable the Load Balancer service.

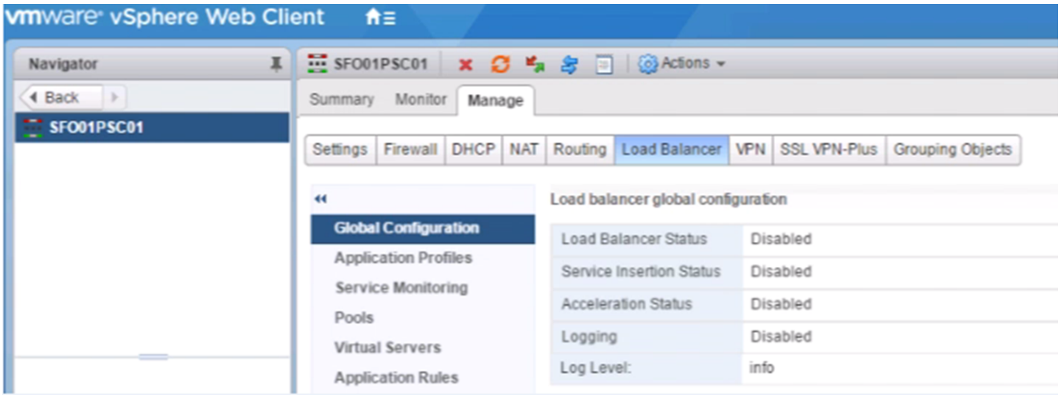
a In the **Navigator**, click **NSX Edges**.

b Select **172.16.11.65** from the **NSX Manager** drop-down menu.

c Double-click the device labeled **SFO01PSC01**.

d Click the **Manage** tab, click the **Load Balancer** tab, click **Global Configuration**, and click **Edit**.

The **Edit load balancer global configuration** dialog box appears.



Load balancer global configuration

Load Balancer Status	Disabled
Service Insertion Status	Disabled
Acceleration Status	Disabled
Logging	Disabled
Log Level:	info

15 In the **Edit load balancer global configuration** dialog box, select **Enable Load Balancer** and click **OK**.

Create Platform Services Controller Application Profiles in Region A

Create an application profile to define the behavior of a particular type of network traffic. After configuring a profile, you associate the profile with a virtual server. The virtual server then processes traffic according to the values specified in the profile. Using profiles enhances your control over managing network traffic, and makes traffic-management tasks easier and more efficient.

Procedure

1 Log in to the Management 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.

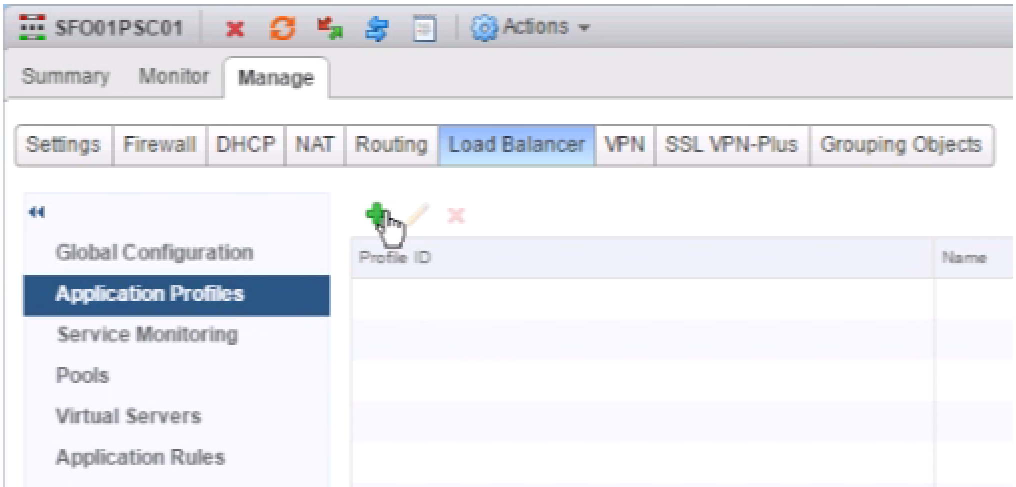
Setting	Value
User name	administrator@vsphere.local
Password	*vsphere_admin_password*

2 Click **Networking & Security**.

3 In the **Navigator**, click **NSX Edges**.

4 From the **NSX Manager** drop-down menu, select **172.16.11.65** as the NSX Manager and double-click the **SFO01PSC01** NSX Edge to manage its network settings.

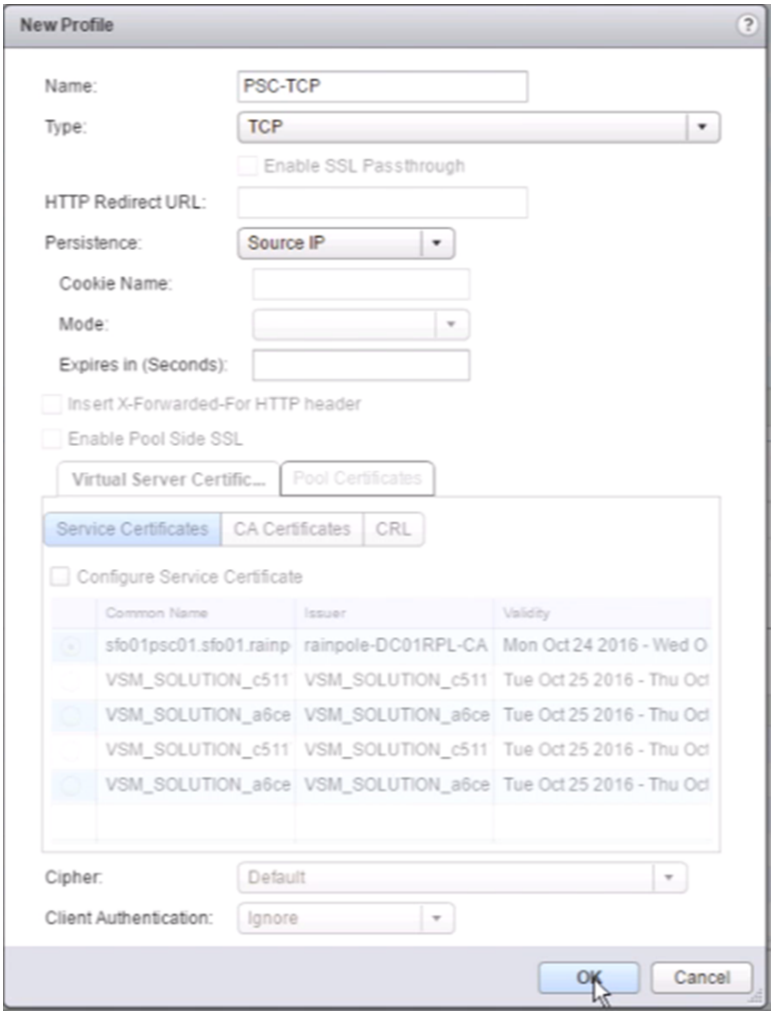
5 Click the **Manage** tab, click **Load Balancer**, and select **Application Profiles**.



6 Click the **Add** icon and in the **New Profile** dialog box, enter the following values.

Setting	Value	Value
Name	PSC-TCP	PSC-HTTPS
Type	TCP	HTTPS
Enable SSL Passthrough	Deselected	Selected

Setting	Value	Value
Persistence	Source IP	Source IP
Expires in (Seconds)	60	60



New Profile

Name: PSC-TCP

Type: TCP

□ Enable SSL Passthrough

HTTP Redirect URL:

Persistence: Source IP

Cookie Name:

Mode:

Expires in (Seconds):

□ Insert X-Forwarded-For HTTP header

□ Enable Pool Side SSL

□ Configure Service Certificate

	Common Name	Issuer	Validity
○	sfo01psc01.sfo01.rainp	rainpole-DC01RPL-CA	Mon Oct 24 2016 - Wed O
○	VSM_SOLUTION_c511	VSM_SOLUTION_c511	Tue Oct 25 2016 - Thu Oct
○	VSM_SOLUTION_a6ce	VSM_SOLUTION_a6ce	Tue Oct 25 2016 - Thu Oct
○	VSM_SOLUTION_c511	VSM_SOLUTION_c511	Tue Oct 25 2016 - Thu Oct
○	VSM_SOLUTION_a6ce	VSM_SOLUTION_a6ce	Tue Oct 25 2016 - Thu Oct

Cipher: Default

Client Authentication: Ignore

7 Click **OK** to save the configuration.

Create Platform Services Controller Server Pools in Region A

A server pool consists of backend server members. After you create a server pool, you associate a service monitor with the pool to manage and share the backend servers flexibly and efficiently.

Repeat this procedure to create two server pools. Use the values indicated in the procedure to create the first and second server pools.

Procedure

1 Log in to the Management 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 Click **Networking & Security**.

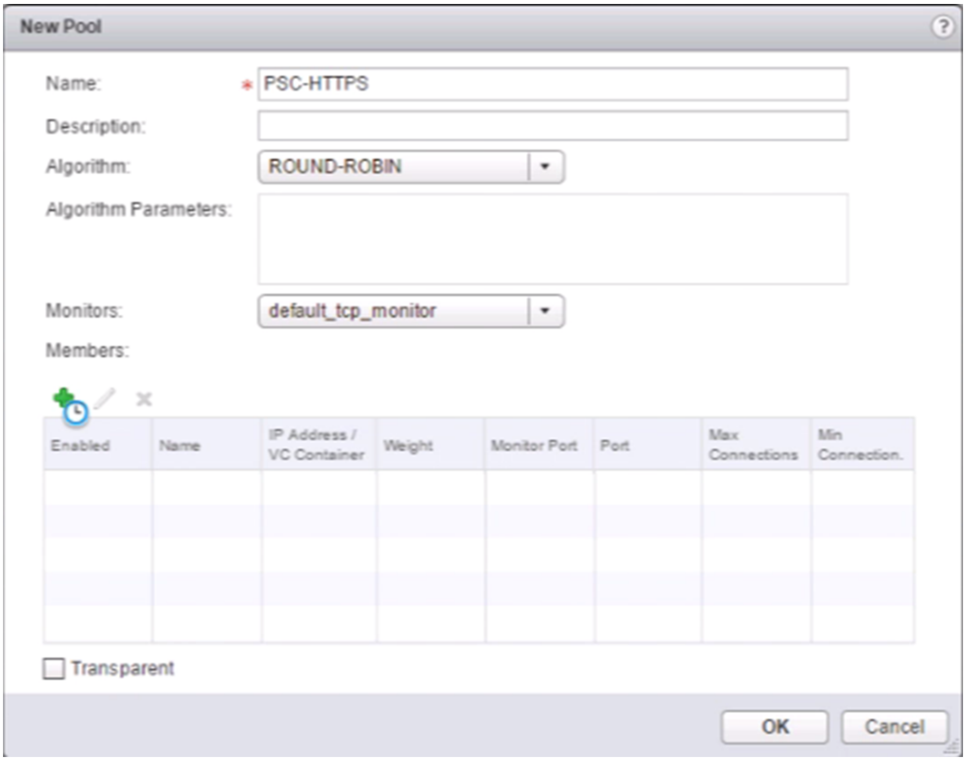
3 In the **Navigator**, click **NSX Edges**.

4 From the **NSX Manager** drop-down menu, select **172.16.11.65** as the NSX Manager and double-click the **SFO01PSC01** NSX Edge to manage its network settings.

5 Click the **Manage** tab, click **Load Balancer**, and select **Pools**.

6 Click the **Add** icon and in the **New Pool** dialog box, enter the following values.

Setting	Value	Value
Name	PSC-HTTPS	PSC-TCP
Algorithm	ROUND-ROBIN	ROUND-ROBIN
Monitors	default-tcp-monitor	default_tcp_monitor



New Pool

Name: * PSC-HTTPS

Description:

Algorithm: ROUND-ROBIN

Algorithm Parameters:

Monitors: default_tcp_monitor

Members:

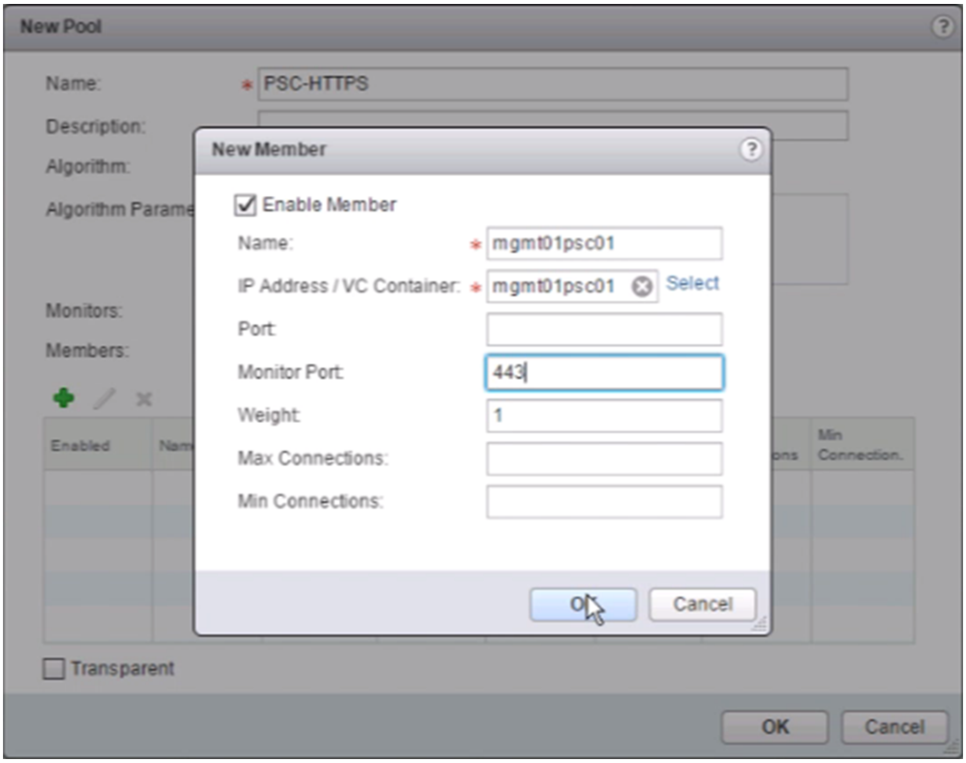
Enabled	Name	IP Address / VC Container	Weight	Monitor Port	Port	Max Connections	Min Connection.

□ Transparent

7 **New Members** dialog box, click the **Add** icon to add the first pool member.

8 In the **New Member** dialog box, enter the following values, and click **OK**.

Setting	Values for First Server Pool	Values for Second Server Pool
Enable Member	Selected	Selected
Name	mgmt01psc01	mgmt01psc01
IP Address/VC Container	mgmt01psc01	mgmt01psc01
Port		
Monitor Port	443	389
Weight	1	1



New Pool

Name: * PSC-HTTPS

New Member

☑ Enable Member

Name: * mgmt01psc01

IP Address / VC Container: * mgmt01psc01

Port:

Monitor Port: 443

Weight: 1

Max Connections:

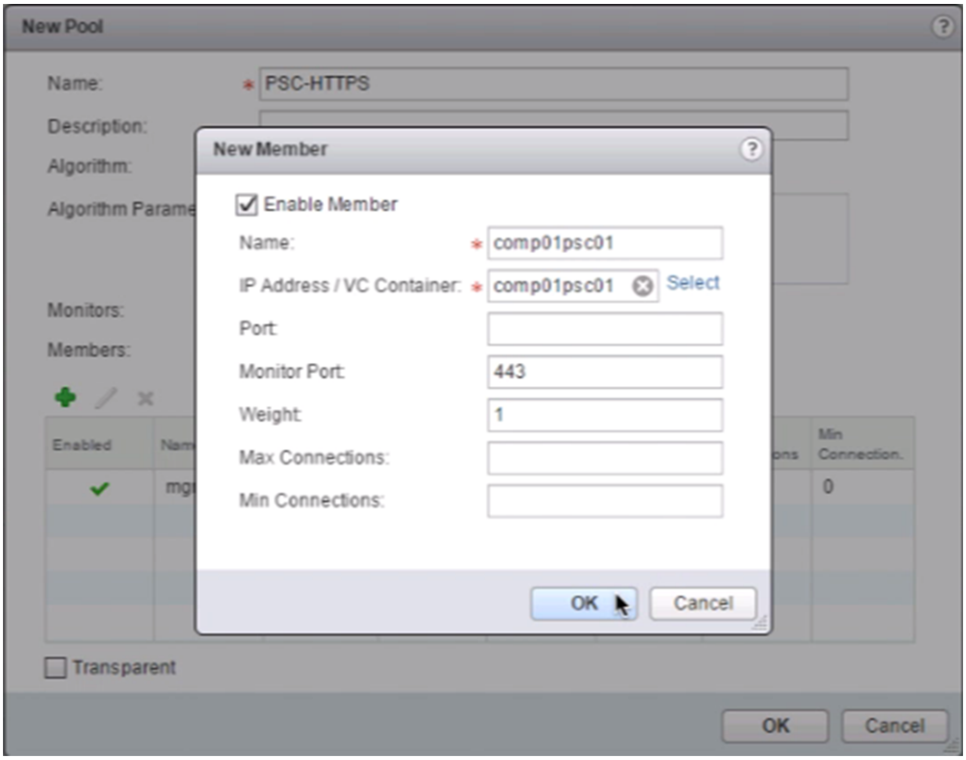
Min Connections:

☐ Transparent

9 **Under Members**, click the **Add** icon to add the second pool member.

10 In the **New Member** dialog box, enter the following values, click **OK** and click **OK** to save the Platform Services Controller Pool.

Setting	Values for First Server Pool	Values for Second Server Pool
Enable Member	Selected	Selected
Name	comp01psc01	comp01psc01
IP Address/VC Container	comp01psc01	comp01psc01
Port		
Monitor Port	443	389
Weight	1	1



New Pool

Name: * PSC-HTTPS

New Member

☑ Enable Member

Name: * comp01psc01

IP Address / VC Container: * comp01psc01

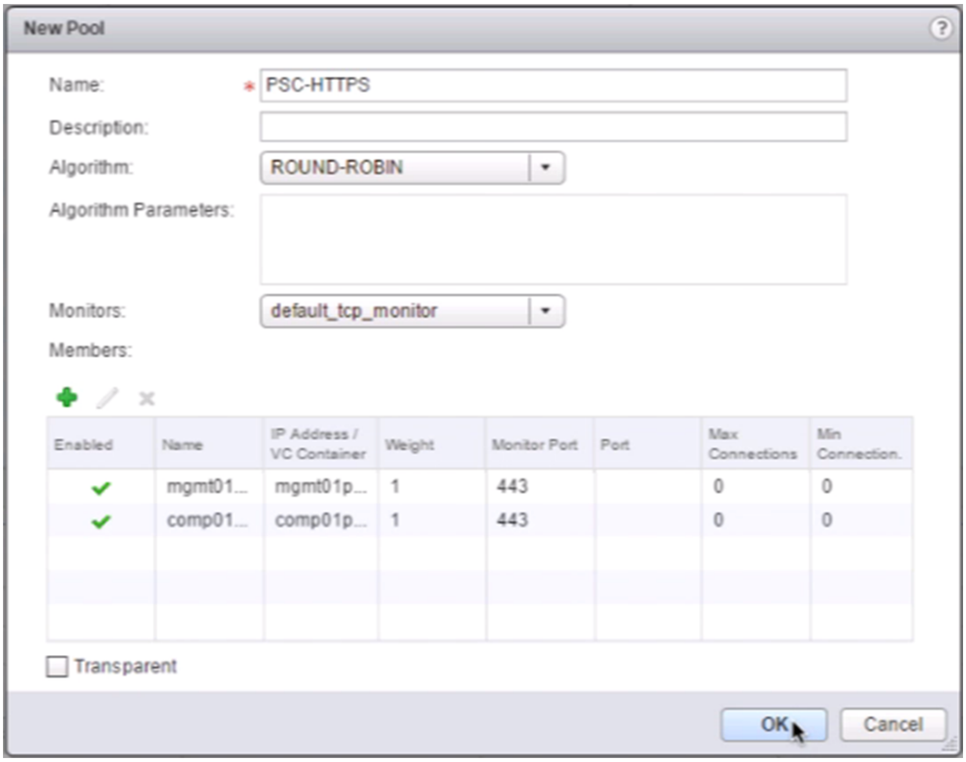
Port:

Monitor Port: 443

Weight: 1

Max Connections:

Min Connections:



New Pool

Name: * PSC-HTTPS

Description:

Algorithm: ROUND-ROBIN

Algorithm Parameters:

Monitors: default_tcp_monitor

Members:

Enabled	Name	IP Address / VC Container	Weight	Monitor Port	Port	Max Connections	Min Connection.
✓	mgmt01...	mgmt01p...	1	443		0	0
✓	comp01...	comp01p...	1	443		0	0

□ Transparent

11 Repeat the procedure to create the remaining server pool.

Create Virtual Servers in Region A

After load balancing is set up, the NSX load balancer distributes network traffic across multiple servers. When a virtual server receives a request, it chooses the appropriate pool to send traffic to. Each pool consists of one or more members. You create virtual servers for all of the configured server pools.

Procedure

1 Log in to the Management 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 Click **Networking & Security**.

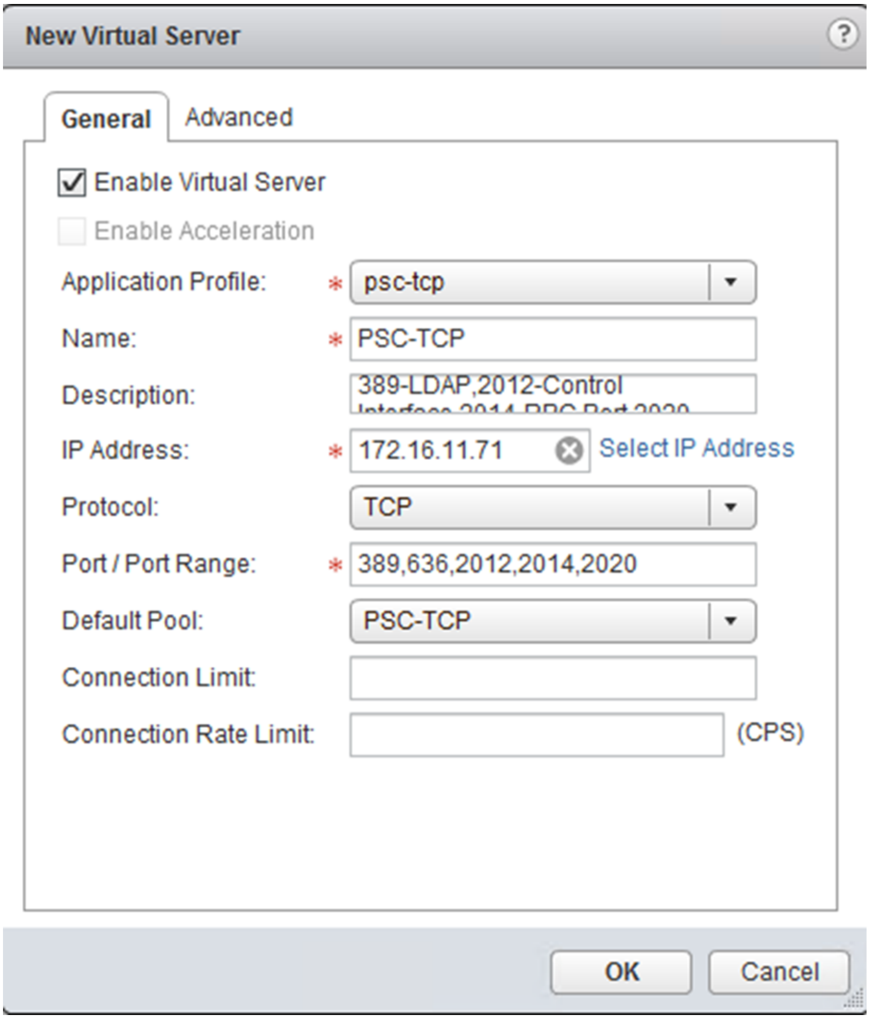
3 In the **Navigator**, click **NSX Edges**.

4 From the **NSX Manager** drop-down menu, select **172.16.11.65** as the NSX Manager and double-click the **SFO01PSC01** NSX Edge to manage its network settings.

5 Click the **Manage** tab, click **Load Balancer**, and select **Virtual Servers**.

6 Click the **Add** icon, and in the **New Virtual Server** dialog box configure the values for the virtual server you are adding, and click **OK**.

Setting	Value	Value
Enable Virtual server	Selected	Selected
Application Profile	PSC-TCP	PSC-HTTPS
Name	PSC-TCP	PSC-HTTPS
Description	389-LDAP,2012-Control Interface,2014-RPC Port,2020-Authentication,636-SSL LDAP	Data from the vSphere Web Client
IP Address	172.16.11.71	172.16.11.71
Protocol	TCP	HTTPS
Port	389,636,2012,2014,2020	443
Default Pool	PSC-TCP	PSC-HTTPS



☑ Enable Virtual Server

□ Enable Acceleration

Application Profile: * psc-tcp

Name: * PSC-TCP

Description: 389-LDAP,2012-Control Interface,2014-RPC Port,2020

IP Address: * 172.16.11.71

Protocol: TCP

Port / Port Range: * 389,636,2012,2014,2020

Default Pool: PSC-TCP

Connection Limit:

Connection Rate Limit: (CPS)

7 Repeat Step 6 to create a virtual server for each component. Upon completion, verify that you have successfully entered the virtual server names and their respective configuration values.

Update DNS Records for the Platform Services Controller Load Balancer in Region A

You must modify the DNS Address in Region A after setting up load balancing.

For the Platform Services Controller Load Balancer, you edit the DNS entry of sfo01psc01.sfo01.rainpole.local to point to the virtual IP address (VIP) of the Load Balancer (172.16.11.71) instead of pointing to the IP address of mgmt01spc01.

Procedure

1 Log in to DNS server **dc01sfo.lsfo01.rainpole.local** that resides in the sfo01.rainpole.local domain.

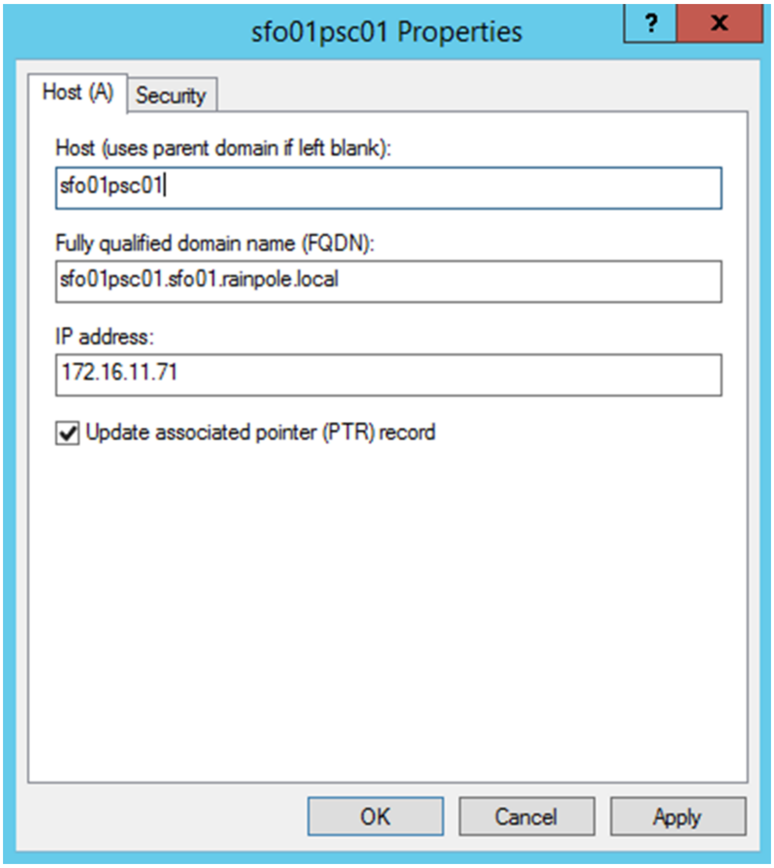
2 Open the Windows **Start** menu, enter **dns** in the **Search** text box and press Enter.

The **DNS Manager** dialog box appears.

3 In the **DNS Manager** dialog box, under **Forward Lookup Zones**, select the **sfo01.rainpole.local** domain and locate the sfo01psc01 record on the right.

4 Double-click the **sfo01psc01** record, change the IP address of the record from 172.16.11.61 to **`172.16.11.71`**, and click **OK**.

Setting	Value
Fully Qualified domain name (FQDN)	sfo01psc01.sfo01.rainpole.local
IP Address	172.16.11.71
Update Associated Pointer (PTR) record	Selected



sfo01psc01 Properties

Host (uses parent domain if left blank): sfo01psc01

Fully qualified domain name (FQDN): sfo01psc01.sfo01.rainpole.local

IP address: 172.16.11.71

☑ Update associated pointer (PTR) record

Configure NSX Dynamic Routing in the Management Cluster in Region A

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 management cluster, deploying two NSX Edge devices and a Universal Distributed Logical Router (UDLR).

Procedure

1 Create a Universal Logical Switch for Use as the Transit Network in the Management Cluster in Region A

Create a universal logical switch for use as the transit network.

2 Deploy NSX Edge Devices for North-South Routing in Region A

Deploy two NSX Edge devices for North-South Routing.

3 Disable the Firewall Service in Region A

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

4 Enable and Configure Routing in Region A

Enable Border Gateway Protocol (BGP) to exchange routing information between the NSX Edge services gateways.

5 Verify Peering of Upstream Switches and Establishment of BGP in Region A

The NSX Edge devices need to establish a connection to each of it's 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 Universal Distributed Logical Router in Region A

Deploy the universal distributed logical router (UDLR).

7 Configure Universal Distributed Logical Router for Dynamic Routing in Region A

Configure the universal distributed logical router (UDLR) to use dynamic routing.

8 Verify Establishment of BGP for the Universal Distributed Logical Router in Region A

The universal distributed logical routers (UDLR) needs to establish a connection to Edge Services Gateway before BGP updates can be exchanged. Verify that the UDLR is successfully peering, and that BGP routing has been established.

Create a Universal Logical Switch for Use as the Transit Network in the Management Cluster in Region A

Create a universal logical switch for use as the transit network.

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 Under **Inventories**, click **Networking & Security**.

3 In the **Navigator**, click **Logical Switches**.

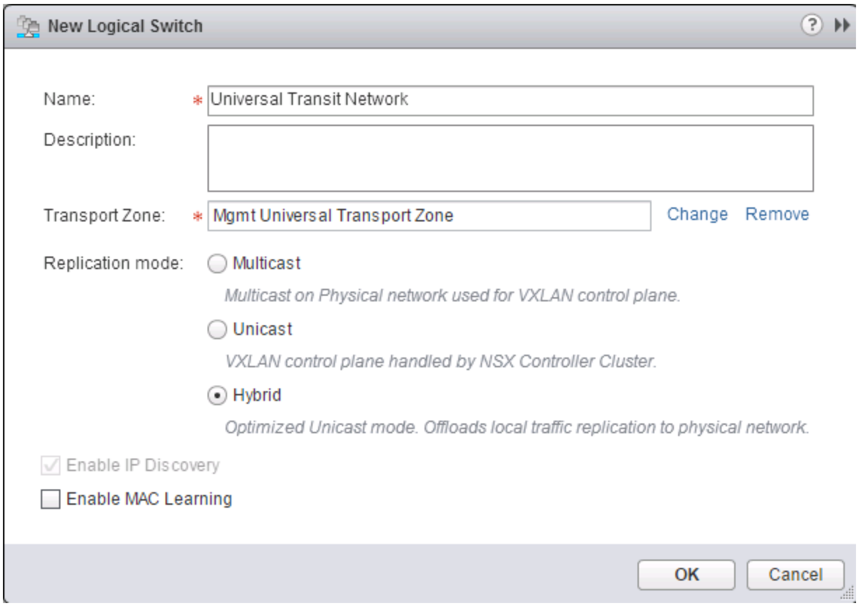
4 Select the instance labeled **172.16.11.65**.

5 Click the **Add** icon.

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

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

Setting	Value
Name	Universal Transit Network
Transport Zone	Mgmt Universal Transport Zone
Replication Mode	Hybrid



New Logical Switch

Name: * Universal Transit Network

Description:

Transport Zone: * Mgmt Universal Transport Zone

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

Deploy NSX Edge Devices for North-South Routing in Region A

Deploy two NSX Edge devices for North-South Routing.

Perform this procedure two times to deploy two NSX Edge devices.

Table 2-5. NSX Edge Devices

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

Table 2‑6. NSX Edge Interfaces Settings

Interface	Primary IP Address SFOMGMT-ESG01	Primary IP Address SFOMGMT-ESG02
Uplink01	172.27.11.2	172.27.11.3
Uplink02	172.27.12.3	172.27.12.2
SFOMGMT-UDLR01	192.168.10.1	192.168.10.2

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 Under **Inventories**, click **Networking & Security**.

3 In the **Navigator**, click **NSX Edges**.

4 Select **172.16.11.65** 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	SFOMGMT-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	*edge_admin_password*
Enable SSH access	Selected
Enable FIPS mode	Deselected
Enable auto rule generation	Selected
Edge Control Level logging	INFO

c On the **Configure deployment** page, click **Large** 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	SFO01-Mgmt01
Datastore	SFO01A-VSAN01-MGMT01
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-Mgmt-Uplink01
Connectivity Status	Connected
Primary IP Address	172.27.11.2
Subnet Prefix Length	24
MTU	9000
Send ICMP Redirect	Selected

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

Setting	Value
Name	Uplink02
Type	Uplink
Connected To	vDS-Mgmt-Uplink02
Connectivity Status	Connected
Primary IP Address	172.27.12.3
Subnet Prefix Length	24
MTU	9000
Send ICMP Redirect	Selected

g Click the **Add** to configure the UDLR interface, enter the following settings click **OK**, and click **Next**.

Setting	Value
Name	SFOMGMT-UDLR01
Type	Internal
Connected To	Universal Transit Network
Connectivity Status	Connected
Primary IP Address	192.168.10.1
Subnet Prefix Length	24
MTU	9000
Send ICMP Redirect	Selected

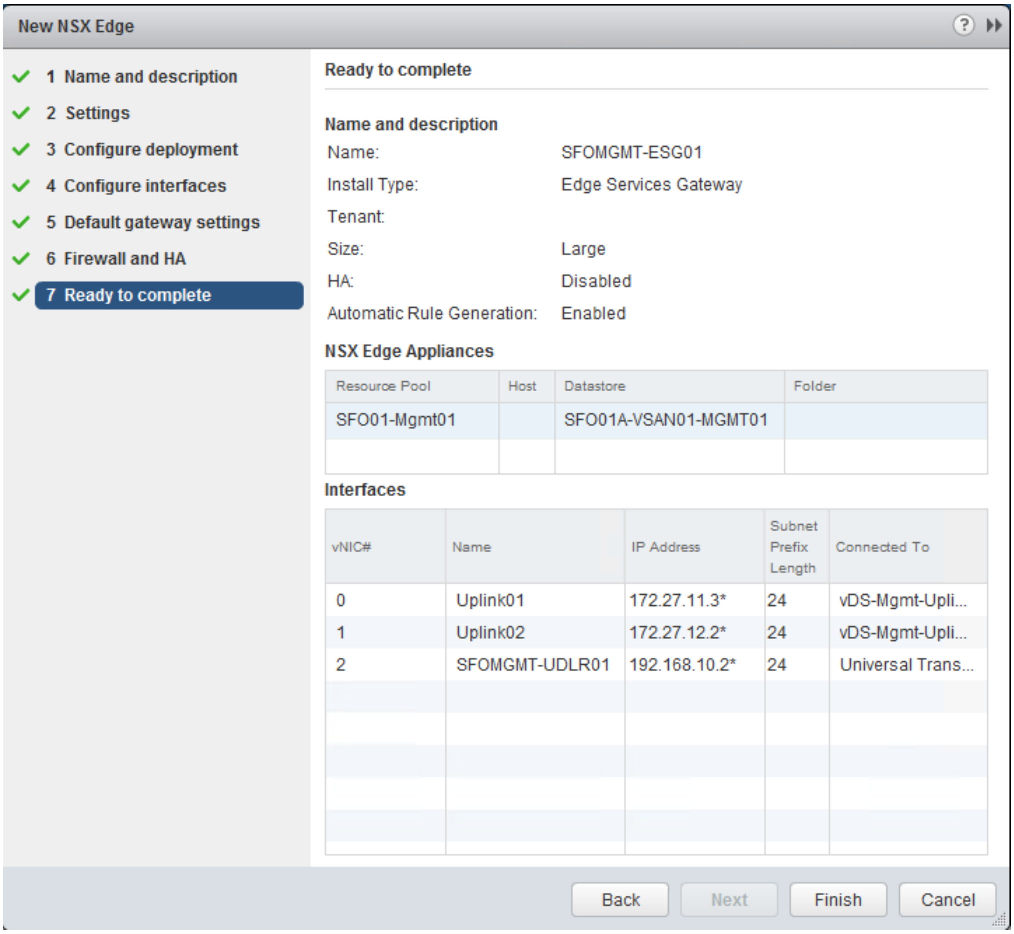
h On the **Default gateway settings** page, deselect the **Configure Default Gateway** check box and click **Next**.

i On the **Firewall and HA** page, click **Next**.

j On the **Ready to complete** page, review the configuration settings that 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 SFOMGMT-ESG02, the **Ready to complete** page in the **New NSX Edge** wizard must display the following values.



Ready to complete

Name and description

Name:	SFOMGMT-ESG01
Install Type:	Edge Services Gateway
Tenant:	
Size:	Large
HA:	Disabled
Automatic Rule Generation:	Enabled

NSX Edge Appliances

Resource Pool	Host	Datastore	Folder
SFO01-Mgmt01		SFO01A-VSAN01-MGMT01	

Interfaces

vNIC#	Name	IP Address	Subnet Prefix Length	Connected To
0	Uplink01	172.27.11.3*	24	vDS-Mgmt-Upli...
1	Uplink02	172.27.12.2*	24	vDS-Mgmt-Upli...
2	SFOMGMT-UDLR01	192.168.10.2*	24	Universal Trans...

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 **mgmt01vc01.sfo01.rainpole.local** tree.

c Select the **SFO01-Mgmt01** cluster, and click the **Configure** tab.

d Under **Configuration**, click **VM/Host Rules**.

e Click **Add**.

f In the **SFO01-Mgmt01 - 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 **SFO01-Mgmt01 - Create VM/Host Rule** dialog box, click **OK**.

Disable the Firewall Service in Region A

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

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

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 Under **Inventories**, click **Networking & Security**.

3 In the **Navigator**, click **NSX Edges**.

4 Select **172.16.11.65** from the **NSX Manager** drop-down menu.

5 Double-click the **SFOMGMT-ESG01** NSX Edge device.

6 Click the **Manage** tab, then click **Firewall**.

7 In the **Firewall** page, click the **Disable** button.

8 Click **Publish Changes**.

9 Repeat this procedure for the NSX Edge device SFOMGMT-ESG02.

Enable and Configure Routing in Region A

Enable Border Gateway Protocol (BGP) to exchange routing information between the NSX Edge services gateways.

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

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. Under **Inventories**, click **Networking & Security**.

3. In the **Navigator**, click **NSX Edges**.

4. Select **172.16.11.65** from the **NSX Manager** drop-down menu.

5. Double-click the **SFOMGMT-ESG01** NSX Edge device.

6. Click the **Manage** tab, and click **Routing**.

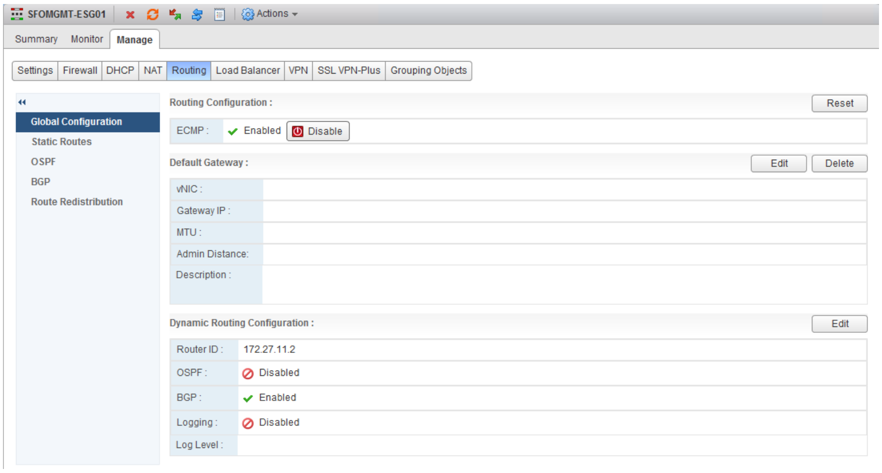
7. On the **Global Configuration** page, enter the following settings.

   a. Click **Enable** for ECMP.

   b. Click **Edit** for **Dynamic Routing Configuration**.

   c. Select **Uplink01** as the **Router ID**.

   d. Click **Publish Changes**.



Routing Configuration :

ECMP :	✓ Enabled

Default Gateway :

vNIC :	
Gateway IP :	
MTU :	
Admin Distance:	
Description :	

Dynamic Routing Configuration :

Router ID :	172.27.11.2
OSPF :	⊘ Disabled
BGP :	✓ Enabled
Logging :	⊘ Disabled
Log Level :	

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	192.168.11.0/24
Next Hop	192.168.10.3
Interface	SFOMGMT-UDLR01
MTU	9000
Admin Distance	210

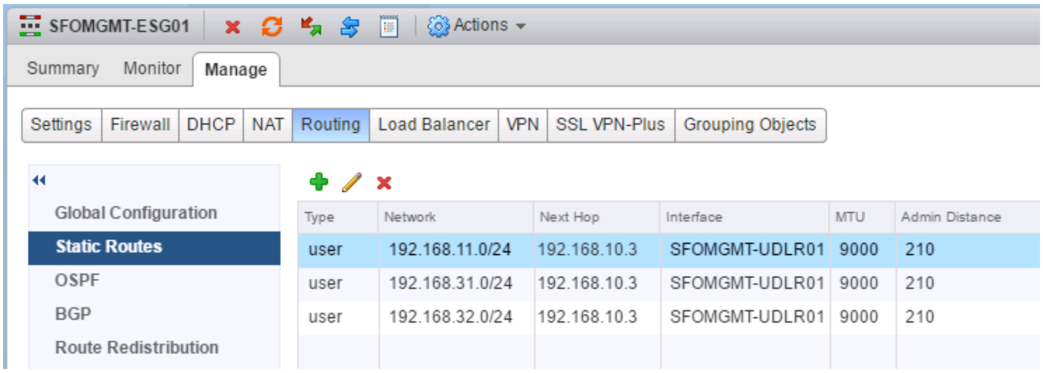
b Click the **Add** icon, enter the following settings, and click **OK**.

Setting	Value
Network	192.168.31.0/24
Next Hop	192.168.10.3
Interface	SFOMGMT-UDLR01
MTU	9000
Admin Distance	210

c Click the **Add** icon, enter the following settings, and click **OK**.

Setting	Value
Network	192.168.32.0/24
Next Hop	192.168.10.3
Interface	SFOMGMT-UDLR01
MTU	9000
Admin Distance	210

d Click **Publish Changes**.

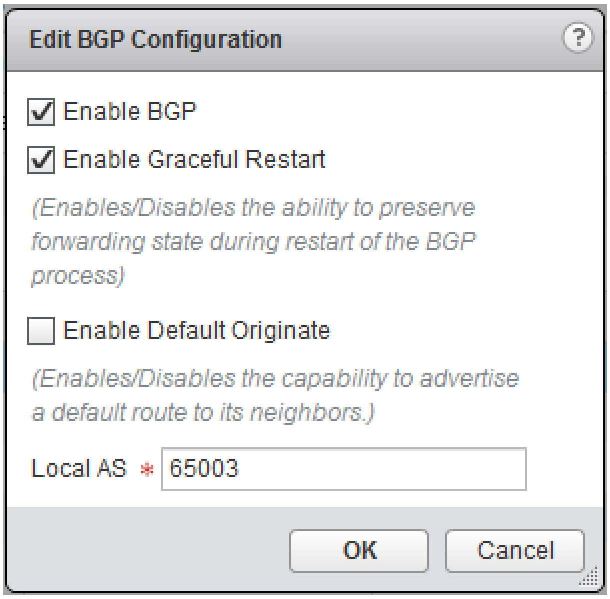


Type	Network	Next Hop	Interface	MTU	Admin Distance
user	192.168.11.0/24	192.168.10.3	SFOMGMT-UDLR01	9000	210
user	192.168.31.0/24	192.168.10.3	SFOMGMT-UDLR01	9000	210
user	192.168.32.0/24	192.168.10.3	SFOMGMT-UDLR01	9000	210

9 On the **Routing** tab, select **BGP** to configure it.

a Click **Edit**, enter the following settings, and click **OK**.

Setting	Value
Enable BGP	Selected
Enable Graceful Restart	Selected
Enable Default Originate	Deselected
Local AS	65003



Edit BGP Configuration

☑ Enable BGP

☑ Enable Graceful Restart

(Enables/Disables the ability to preserve forwarding state during restart of the BGP process)

□ Enable Default Originate

(Enables/Disables the capability to advertise a default route to its neighbors.)

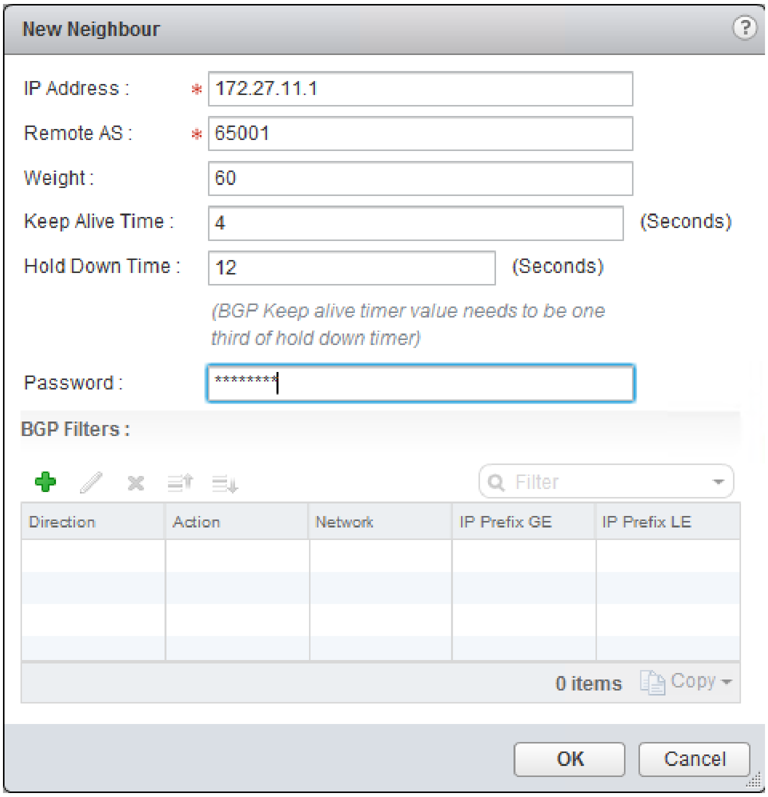
Local AS * 65003

b On the **BGP** page, 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 and click **OK**.

Setting	Value
IP Address	172.27.11.1
Remote AS	65001
Weight	60
Keep Alive Time	4
Hold Down Time	12
Password	*BGP_password*



New Neighbour

IP Address : * 172.27.11.1

Remote AS : * 65001

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

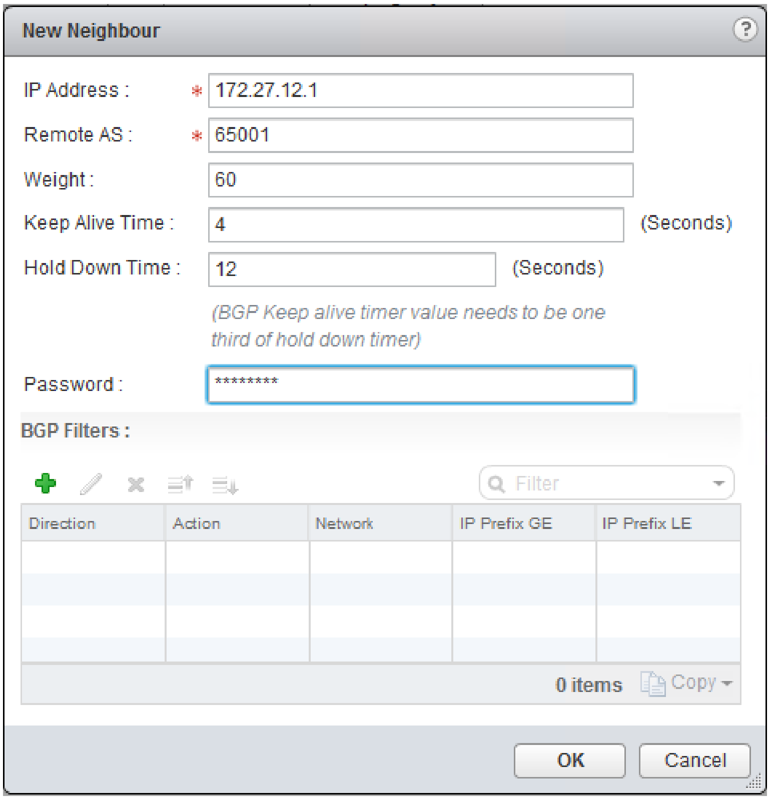
0 items

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 172.27.12.1.

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

Setting	Value
IP Address	172.27.12.1
Remote AS	65001
Weight	60
Keep Alive Time	4
Hold Down Time	12
Password	*BGP_password*



New Neighbour

IP Address : * 172.27.12.1

Remote AS : * 65001

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

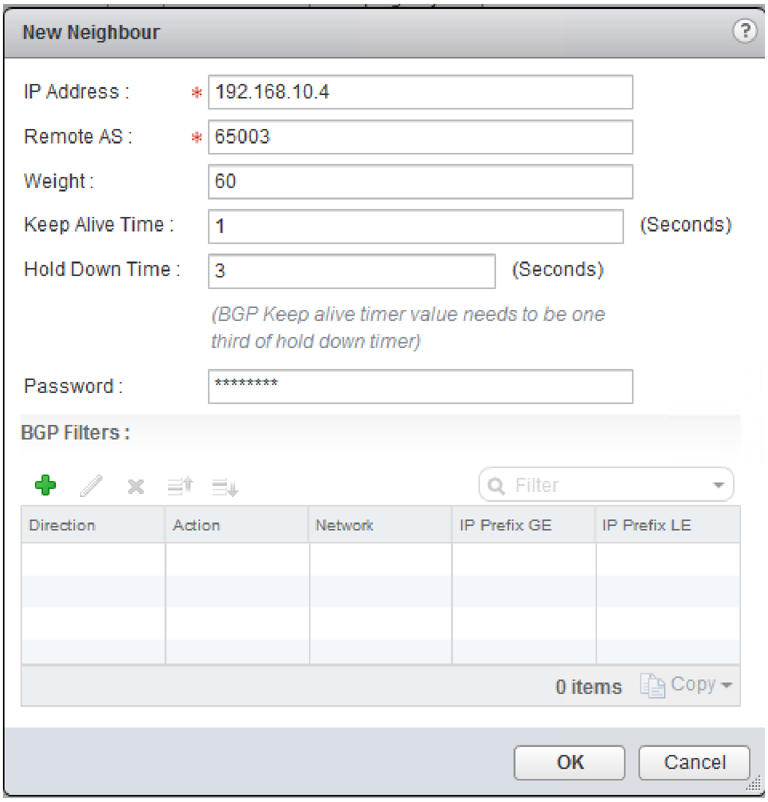
0 items

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

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

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

Setting	Value
IP Address	192.168.10.4
Remote AS	65003
Weight	60
Keep Alive Time	1
Hold Down Time	3
Password	*BGP_password*



New Neighbour

IP Address : * 192.168.10.4

Remote AS : * 65003

Weight : 60

Keep Alive Time : 1 (Seconds)

Hold Down Time : 3 (Seconds)

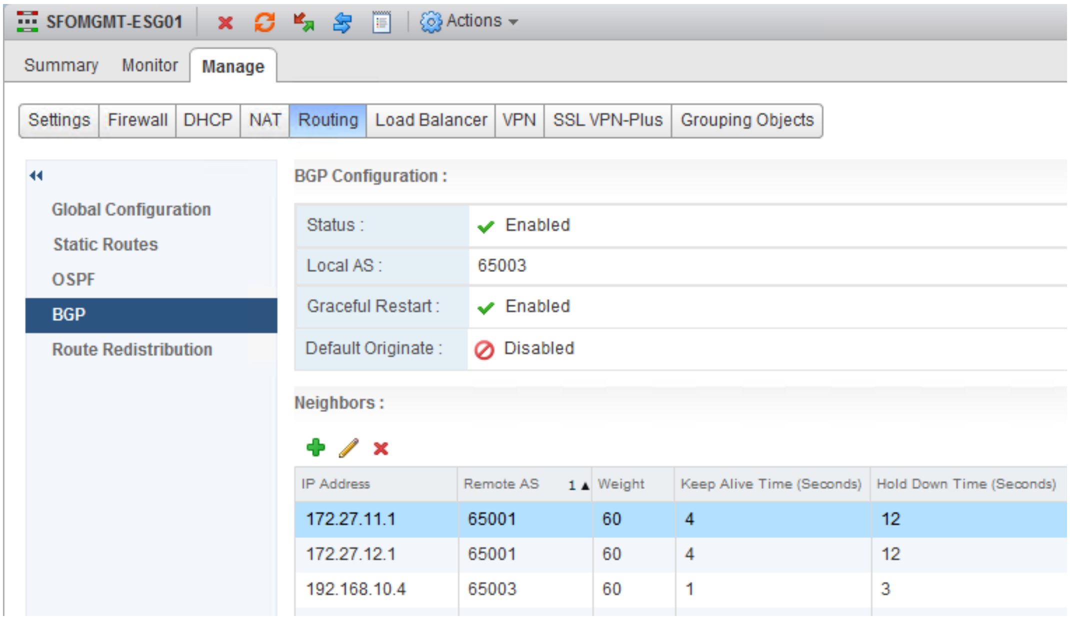
(BGP Keep alive timer value needs to be one third of hold down timer)

Password : ********

BGP Filters :

Direction	Action	Network	IP Prefix GE	IP Prefix LE

h Click **Publish Changes**.



BGP Configuration :

Status :	✓ Enabled
Local AS :	65003
Graceful Restart :	✓ Enabled
Default Originate :	⊘ Disabled

Neighbors :

IP Address	Remote AS	Weight	Keep Alive Time (Seconds)	Hold Down Time (Seconds)
172.27.11.1	65001	60	4	12
172.27.12.1	65001	60	4	12
192.168.10.4	65003	60	1	3

The three neighbors you added appear in the **Neighbors** table.

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

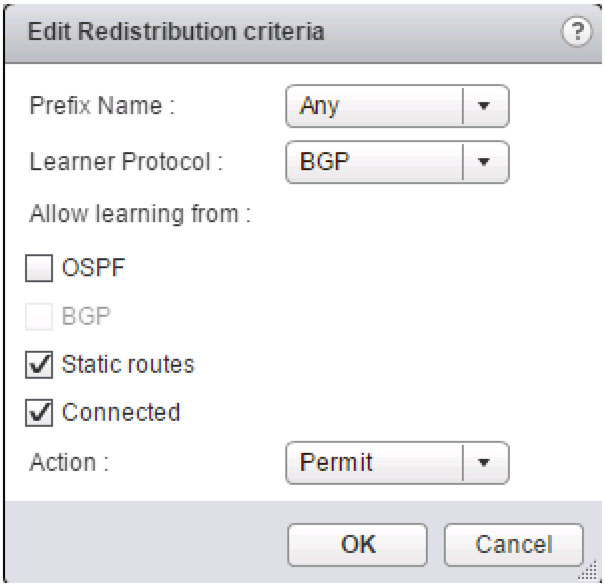
a On the **Route Redistribution** page, click the **Edit** button.

b In the **Change redistribution settings** dialog box, select the **BGP** check box and click **OK**.

c Click the **Add** icon for **Route Redistribution Table**.

d 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



Edit Redistribution criteria

Prefix Name : Any

Learner Protocol : BGP

Allow learning from :

☐ OSPF

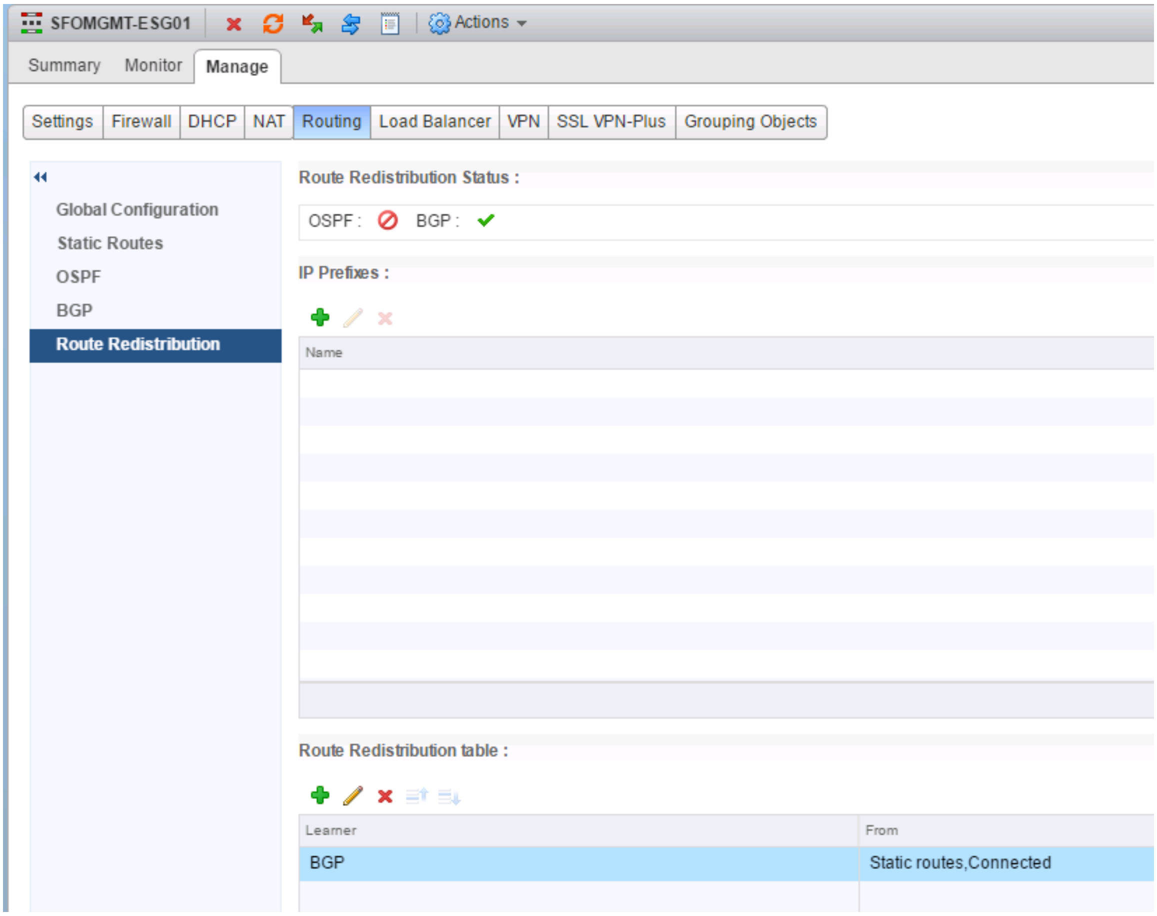
☐ BGP

☑ Static routes

☑ Connected

Action : Permit

e Click **Publish Changes**.



Route Redistribution Status :

OSPF : ⊘ BGP : ✓

IP Prefixes :

Name

Route Redistribution table :

Learner	From
BGP	Static routes,Connected

The route redistribution configuration appears in the **Route Redistribution** table.

11 Repeat this procedure for the NSX Edge device SFOMGMT-ESG02.

Verify Peering of Upstream Switches and Establishment of BGP in Region A

The NSX Edge devices need to establish a connection to each of it's 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: `SFOMGMT-ESG01` and `SFOMGMT-ESG02`.

Procedure

1 Log in to the NSX Edge device using a Secure Shell (SSH) client.

   a Open an SSH connection to the NSX Edge device **`SFOMGMT-ESG01`**.

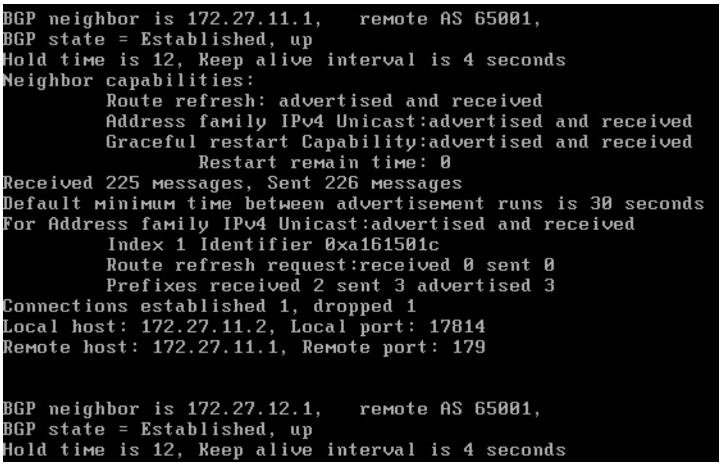
   b Log in using the following credentials.

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.

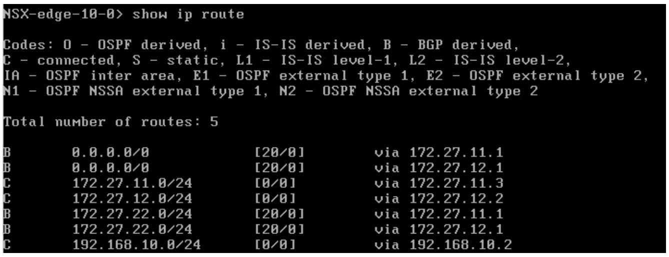
Note You have not yet created the universal distributed logical router (UDLR), so it will not display the `Established, UP` status message.



```
BGP neighbor is 172.27.11.1,   remote AS 65001,
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 225 messages, Sent 226 messages
Default minimum time between advertisement runs is 30 seconds
For Address family IPv4 Unicast:advertised and received
         Index 1 Identifier 0xa161501c
         Route refresh request:received 0 sent 0
         Prefixes received 2 sent 3 advertised 3
Connections established 1, dropped 1
Local host: 172.27.11.2, Local port: 17814
Remote host: 172.27.11.1, Remote port: 179


BGP neighbor is 172.27.12.1,   remote AS 65001,
BGP state = Established, up
Hold time is 12, Keep alive interval is 4 seconds
```

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 and 172.27.22.0/24. You can identify BGP networks by the letter `B` in the left-side column. Lines beginning with `C` (connected) have only a single route.



```
NSX-edge-10-0> show ip 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: 5

B       0.0.0.0/0            [20/0]        via 172.27.11.1
B       0.0.0.0/0            [20/0]        via 172.27.12.1
C       172.27.11.0/24       [0/0]         via 172.27.11.3
C       172.27.12.0/24       [0/0]         via 172.27.12.2
B       172.27.22.0/24       [20/0]        via 172.27.11.1
B       172.27.22.0/24       [20/0]        via 172.27.12.1
C       192.168.10.0/24      [0/0]         via 192.168.10.2
```

4 Repeat this procedure for the NSX Edge device `SFOMGMT-ESG02`.

Deploy the Universal Distributed Logical Router in Region A

Deploy the universal distributed logical router (UDLR).

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 Under **Inventories**, click **Networking & Security**.

3 In the **Navigator**, click **NSX Edges**.

4 Select **172.16.11.65** from the **NSX Manager** drop-down menu.

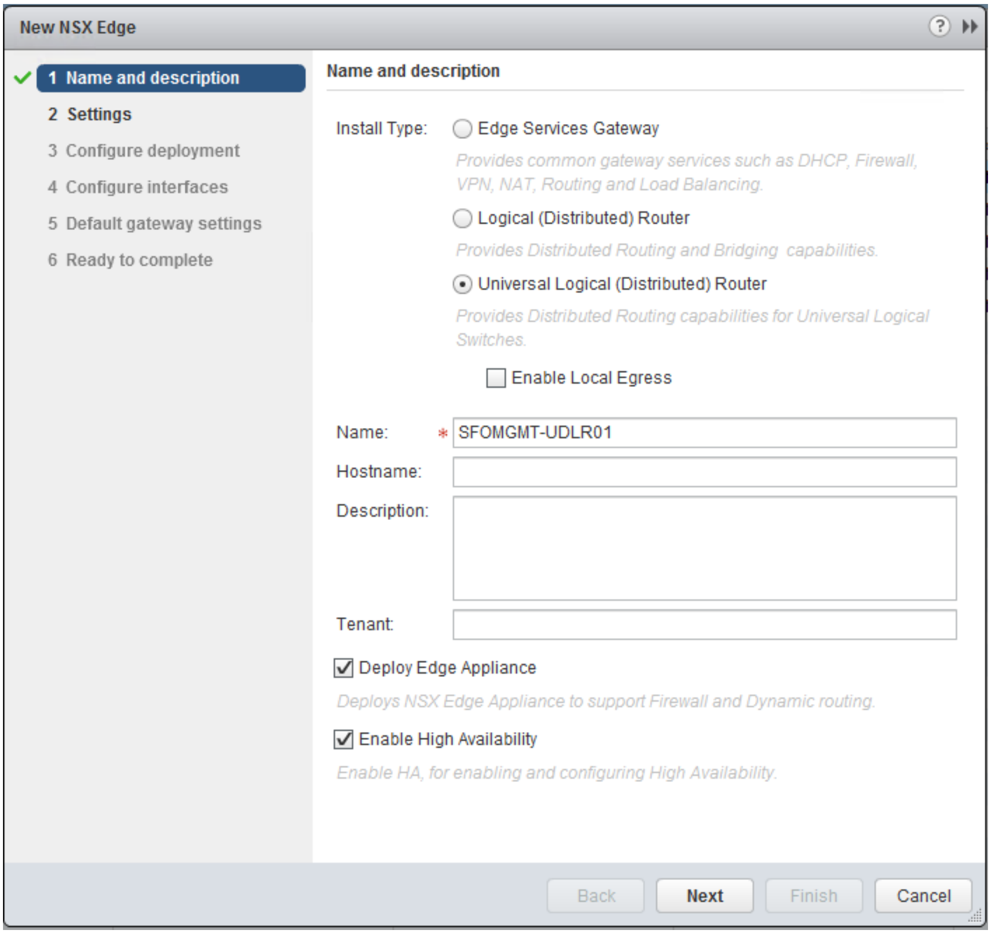
5 Click the **Add** icon to create a new UDLR.

   The **New NSX Edge** wizard appears.

6 Complete the **New NSX Edge** wizard to deploy and configure the UDLR.

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

Setting	Value
Universal Logical (Distributed) Router	Selected
Name	SFOMGMT-UDLR01
Deploy Edge Appliance	Selected
Enable High Availability	Selected



New NSX Edge

Name and description

Install Type:

○ Edge Services Gateway

Provides common gateway services such as DHCP, Firewall, VPN, NAT, Routing and Load Balancing.

○ Logical (Distributed) Router

Provides Distributed Routing and Bridging capabilities.

● Universal Logical (Distributed) Router

Provides Distributed Routing capabilities for Universal Logical Switches.

□ Enable Local Egress

Name: * SFOMGMT-UDLR01

Hostname:

Description:

Tenant:

☑ Deploy Edge Appliance

Deploys NSX Edge Appliance to support Firewall and Dynamic routing.

☑ Enable High Availability

Enable HA, for enabling and configuring High Availability.

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

Setting	Value
User Name	admin
Password	*udlr_admin_password*
Enable SSH access	Selected
Edge Control Level logging	INFO

c On the **Configure deployment** page, 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 and click **OK**.

Setting	Value
Cluster/Resource Pool	SFO01-Mgmt01
Datastore	SFO01A-VSAN01-MGMT01

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

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

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

Setting	Value
Cluster/Resource Pool	SFO01-Mgmt01
Datastore	SFO01A-VSAN01-MGMT01
Folder	NSX01

g On the **Configure interfaces** page, under **HA Interface Configuration**, click **Change** and connect to **vDS-Mgmt-Management**.

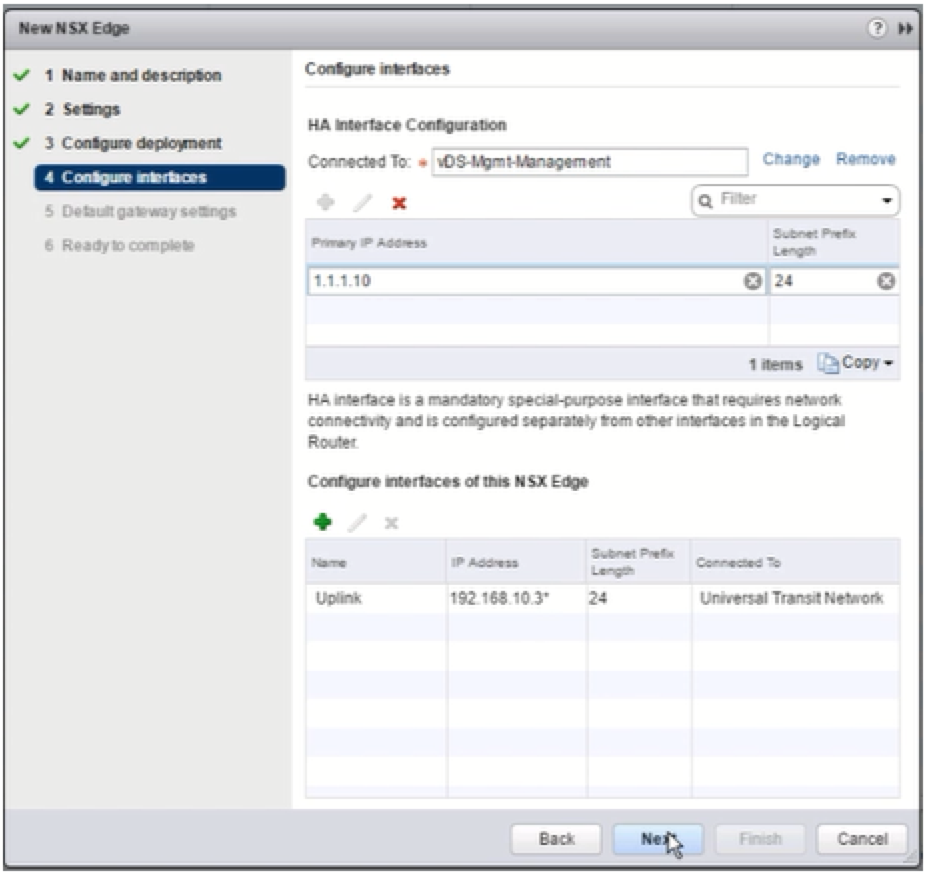
h On the **Configure interfaces** page, click the **Add** icon to configure Primary IP Address.

Options	Description
Setting	Value
Primary IP Address	1.1.1.10
Subnet Prefix Length	24

i On the **Configure interfaces** page, click the **Add** icon to configure interface.

j In the **Add Interface** dialog box, enter the following settings, click **OK**, and click **Next**.

Setting	Value
Name	Uplink
Type	Uplink
Connected To	Universal Transit Network
Connectivity Status	Connected
Primary IP Address	192.168.10.3
Subnet Prefix Length	24
MTU	9000



Configure interfaces

HA Interface Configuration

Connected To: * vDS-Mgmt-Management

Primary IP Address	Subnet Prefix Length
1.1.1.10	24

1 items

HA interface is a mandatory special-purpose interface that requires network connectivity and is configured separately from other interfaces in the Logical Router.

Configure interfaces of this NSX Edge

Name	IP Address	Subnet Prefix Length	Connected To
Uplink	192.168.10.3*	24	Universal Transit Network

k On the **Default gateway settings** page, deselect **Configure Default Gateway** and click **Next**.

l On the **Ready to complete** page, click **Finish**.

Configure Universal Distributed Logical Router for Dynamic Routing in Region A

Configure the universal distributed logical router (UDLR) to use dynamic routing.

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 Under **Inventories**, click **Networking & Security**.

3 In the **Navigator**, click **NSX Edges**.

4 Select **172.16.11.65** from the **NSX Manager** drop-down menu.

5 Enable HA logging.

   a Double-click the device labeled **SFOMGMT-UDLR01**.

   b Click the **Manage** tab and click the **Settings** tab

   c Click **Change** in the **HA Configuration** window.

   d Select the **Enable Logging** checkbox and click **OK**.

6 Configure the routing for the Universal Distributed Logical Router.

   a Double-click **SFOMGMT-UDLR01**.

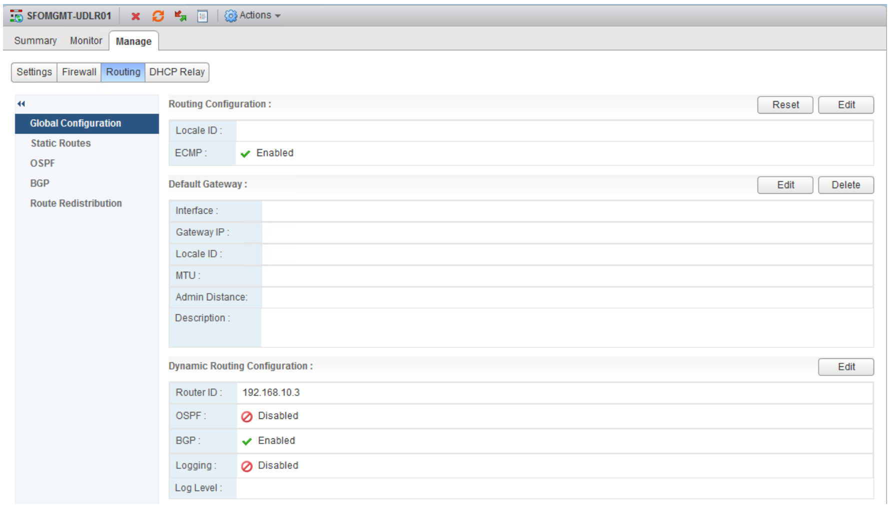
   b Click the **Manage** tab and click **Routing**.

   c On the **Global Configuration** page, perform the following configuration steps.

   d Click **Edit** under **Routing Configuration**, select **Enable ECMP**, and click **OK**.

e Click **Edit** under **Dynamic Routing Configuration**, select **Uplink** as the **Router ID**, and click **OK**.

f Click **Publish Changes**.



Routing Configuration :

Locale ID :

ECMP : ✓ Enabled

Default Gateway :

Interface :

Gateway IP :

Locale ID :

MTU :

Admin Distance:

Description :

Dynamic Routing Configuration :

Router ID : 192.168.10.3

OSPF : Disabled

BGP : ✓ Enabled

Logging : Disabled

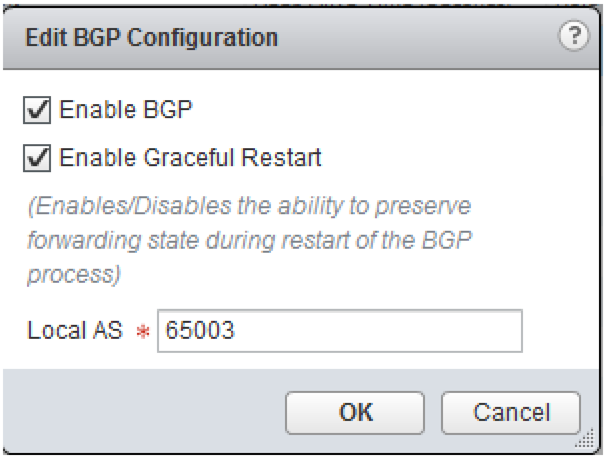
Log Level :

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

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

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	65003



☑ Enable BGP

☑ Enable Graceful Restart

(Enables/Disables the ability to preserve forwarding state during restart of the BGP process)

Local AS * 65003

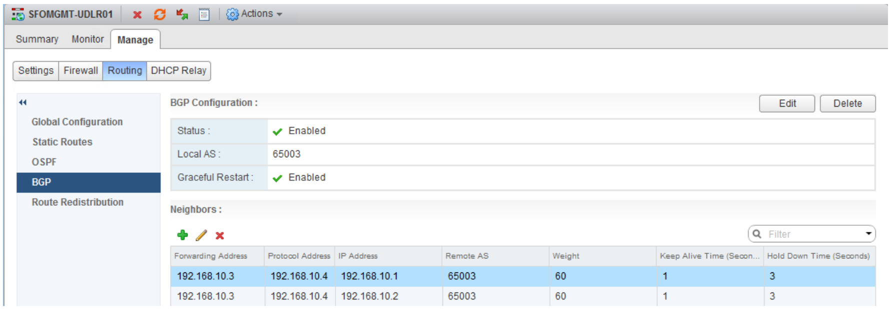
c Click the **Add** icon to add a Neighbor.

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

You repeat this step two times to configure the UDLR for both NSX Edge devices: SFOMGMT-ESG01 and SFOMGMT-ESG02.

Setting	SFOMGMT-ESG01 Value	SFOMGMT-ESG02 Value
IP Address	192.168.10.1	192.168.10.2
Forwarding Address	192.168.10.3	192.168.10.3
Protocol Address	192.168.10.4	192.168.10.4
Remote AS	65003	65003
Weight	60	60
Keep Alive Time	1	1
Hold Down Time	3	3
Password	*BGP_password*	*BGP_password*

e Click **Publish Changes**.



BGP Configuration :

Status :	✓ Enabled
Local AS :	65003
Graceful Restart :	✓ Enabled

Neighbors :

Forwarding Address	Protocol Address	IP Address	Remote AS	Weight	Keep Alive Time (Secon...	Hold Down Time (Seconds)
192.168.10.3	192.168.10.4	192.168.10.1	65003	60	1	3
192.168.10.3	192.168.10.4	192.168.10.2	65003	60	1	3

8 On the left, select **Route Redistribution** to configure it.

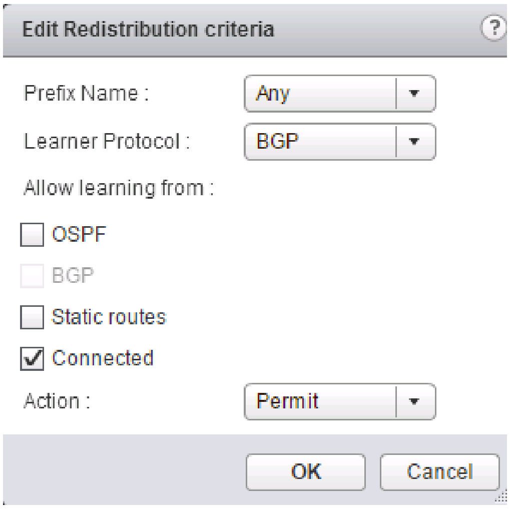
a Click **Edit**.

b In the Change redistribution settings dialog box, enter the following settings and click **OK**.

Setting	Value
OSPF	Deselected
BGP	Selected

c On the **Route Redistribution** page, select the default **OSPF** entry and click **Edit** button.

d Select **BGP** from the **Learner Protocol** drop-down menu, and click **OK**.



Edit Redistribution criteria

Prefix Name : Any

Learner Protocol : BGP

Allow learning from :

□ OSPF

□ BGP

□ Static routes

☑ Connected

Action : Permit

e Click **Publish Changes**.

Verify Establishment of BGP for the Universal Distributed Logical Router in Region A

The universal distributed logical routers (UDLR) needs to establish a connection to Edge Services Gateway before BGP updates can be exchanged. Verify that the UDLR is successfully peering, and that BGP routing has been established.

Procedure

1 Log in to the UDLR by using a Secure Shell (SSH) client.

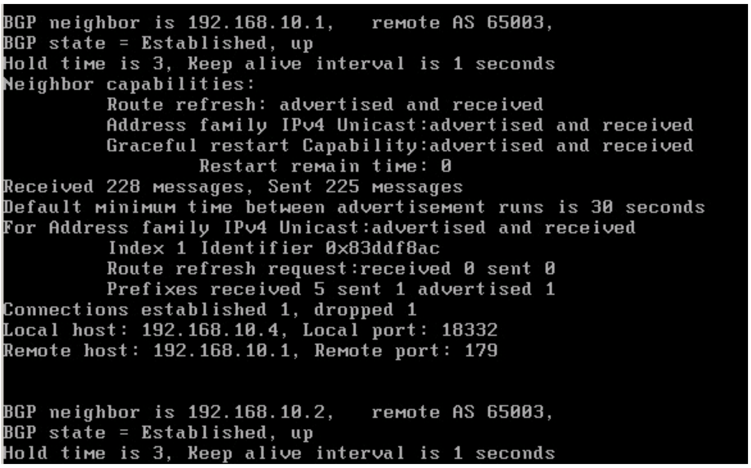
   a Open an SSH connection to `UDLR01`, he UDLR whose peering and BGP configuration you want to verify.

   b Log in using the following credentials.

Setting	Value
User name	admin
Password	*udlr_admin_password*

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

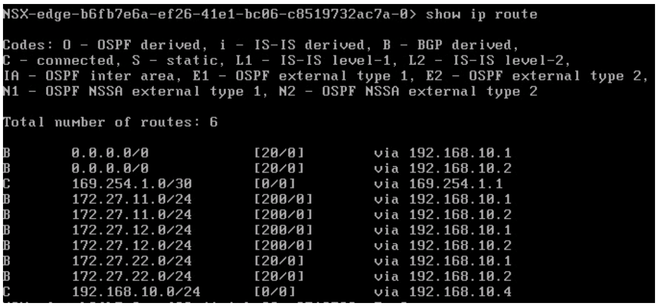
   The BGP State will display `Established, UP` if you have successfully peered with the Edge Service Gateway.



```
BGP neighbor is 192.168.10.1,   remote AS 65003,
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 228 messages, Sent 225 messages
Default minimum time between advertisement runs is 30 seconds
For Address family IPv4 Unicast:advertised and received
         Index 1 Identifier 0x83ddf8ac
         Route refresh request:received 0 sent 0
         Prefixes received 5 sent 1 advertised 1
Connections established 1, dropped 1
Local host: 192.168.10.4, Local port: 18332
Remote host: 192.168.10.1, Remote port: 179


BGP neighbor is 192.168.10.2,   remote AS 65003,
BGP state = Established, up
Hold time is 3, Keep alive interval is 1 seconds
```

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, 172.27.11.0/24, 172.27.12.0/24, and 172.27.22.0/24. You can identify BGP networks by the letter `B` in the left-side column. Lines beginning with `C` (connected) have only a single route.



```
NSX-edge-b6fb7e6a-ef26-41e1-bc06-c8519732ac7a-0> show ip 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: 6

B       0.0.0.0/0           [20/0]        via 192.168.10.1
B       0.0.0.0/0           [20/0]        via 192.168.10.2
C       169.254.1.0/30      [0/0]         via 169.254.1.1
B       172.27.11.0/24      [200/0]       via 192.168.10.1
B       172.27.11.0/24      [200/0]       via 192.168.10.2
B       172.27.12.0/24      [200/0]       via 192.168.10.1
B       172.27.12.0/24      [200/0]       via 192.168.10.2
B       172.27.22.0/24      [20/0]        via 192.168.10.1
B       172.27.22.0/24      [20/0]        via 192.168.10.2
C       192.168.10.0/24     [0/0]         via 192.168.10.4
```

Distributed Firewall Configuration for Management Applications

Configuring a distributed firewall for use with your SDDC increases the security level of your environment by allowing only the network traffic that is required for the SDDC to run. The firewall rules you define allow access to management applications.

You define explicit rules for the distributed firewall which allow access to management applications.

Procedure

1 Add vCenter Server Instances to the NSX Distributed Firewall Exclusion List

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

2 Create IP Sets for All Components of the Management Clusters in the SDDC

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

3 Create Security Groups

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

4 Create Distributed Firewall Rules

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.

Add vCenter Server Instances to the NSX Distributed Firewall Exclusion List

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://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 Exclude vCenter Server instances in Region A from firewall protection.

a In the **Navigator**, click **Networking & Security**.

b Click **NSX Managers** and select the **172.16.11.65** instance.

c Click **Manage** and then click **Exclusion List**.

d Click the **Add** button.

e Add **mgmt01vc01** to the **Selected Objects** list, and click **OK**.

Create IP Sets for All Components of the Management Clusters in the SDDC

Create IP sets for all management applications in the management clusters. 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. For applications that are load balanced include their VIP in the IP Set.

Table 2-7. IP Sets for the Management Clusters Components in the SDDC

Name	IP Addresses
Site Recovery Manager	*Site-Recovery-Manger_IP's*
Platform Services Controller Instances	*Platform-Service-Controller_IP's*
vCenter Server Instances	*vCenter-Server_IP's*
vSphere Replication	*vSphere-Replication_IP's*
vRealize Automation Appliances	*vRealize-Automation-Appliances_IP's*
vRealize Automation Windows	*vRealize-Automation-Windows _IP's*
vRealize Automation Proxy Agents	*vRealize-Automation-Proxy-Agents-IP's*
vRealize Orchestrator	*vRealize-Orchestrtor_IP's*
vRealize Business Server	*vRealize-Business_IP*
vRealize Business Data Collector	*vRealize-Business-Data-Collector_IP*'s
vSphere Data Protection	*vSphere-Data-Protection_IP's*
vRealize Operations Manager	*vRealize-Operations-Manager_IP's*
vRealize Operations Manager Remote Collectors	*vRealize-Operations-Manager-Remote-Collectors_IP's*
vRealize Log Insight	*vRealize-Log-Insight_IP's*
Update Manager Download Service	*UMDS_IP's*
SDDC	*Management-VLAN_Subnets, Management-VXLAN_Subnets*
Administrators	*vDS-Mgmt-Ext-Management_Subnet*

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 Create an IP set for Site Recovery Manger.

   a In the **Navigator**, click **Networking & Security**.

   b Click **NSX Managers** and select the **172.16.11.65** instance.

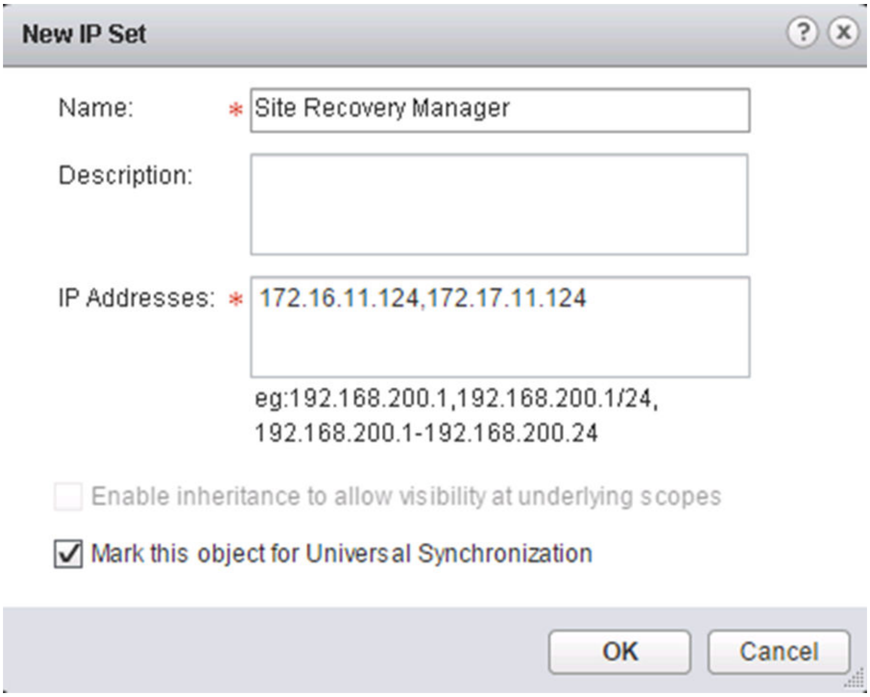
   c Click **Manage**, click **Grouping Objects**, and click **IP Sets**.

d Click the **Add** icon.

e In the **New IP Set** dialog box, configure the values for the IP set that you are adding, and click **OK**.

For all IP sets that you configure, select the **Mark this object for Universal Synchronization** check box.

Setting	Value
Name	Site Recovery Manager
IP Addresses	172.16.11.124,172.17.11.124
Mark this object for Universal Synchronization	Selected



New IP Set

Name: * Site Recovery Manager

Description:

IP Addresses: * 172.16.11.124,172.17.11.124

eg:192.168.200.1,192.168.200.1/24, 192.168.200.1-192.168.200.24

□ Enable inheritance to allow visibility at underlying scopes

☑ Mark this object for Universal Synchronization

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

Create Security Groups

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 2‑8. Security Groups for the Management Clusters Components in the SDDC

Name	Object Type	Selected Object
Site Recovery Manager	IP Sets	Site Recovery Manager
Platform Services Controller Instances	IP Sets	Platform Services Controller Instances
vCenter Server Instances	IP Sets	vCenter Server Instances
vSphere Replication	IP Sets	vSphere Replication
vRealize Automation Appliances	IP Sets	vRealize Automation Appliances
vRealize Automation Windows	IP Sets	vRealize Automation Windows
vRealize Orchestrator	IP Sets	vRealize Orchestrator
vRealize Business Server	IP Sets	vRealize Business Server
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	IP Sets	vRealize Operations Manager
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
SDDC	IP Sets	SDDC
Administrators	IP Sets	Administrators
Windows Servers	Security Groups	■ Site Recovery Manger ■ vRealize Automation Windows ■ vRealize Automation Proxy Agents
VMware Appliances	Security Groups	■ Platform Services Controller Instances ■ vCenter Server Instances ■ vSphere Replication ■ vRealize Automation Appliances ■ vRealize Orchestrator ■ vRealize Business Server ■ vRealize Business Data Collector ■ vSphere Data Protection ■ vRealize Operations Manager ■ 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://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 In the **Navigator**, click **Networking & Security** and click **NSX Managers**.

3 Select the **172.16.11.65** NSX Manger 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 **`Site Recovery Manager`** in the **Name** text box, select the **Mark this object for Universal Synchronization** check box, and click **Next**.

   For all security groups that you configure, select the **Mark this object for Universal Synchronization** check box.

6 On the **Select objects to include** page, select **IP Sets** from the **Object Type** drop-down menu, select **Site Recovery Manger** from the list of available objects, click the **Add** button, and click **Next**.

7 On the **Ready to Complete** page, verify the configuration values that you entered and click **Finish**.

8 Repeat this procedure to create all of the necessary security groups.

Create Distributed Firewall Rules

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.

You create firewall rules that allow administrators to connect to the different VMware solutions, rules to allow user access to the vRealize Automation portal, and to provide external connectivity to the SDDC.

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. 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 **172.16.11.65**.

   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 **Mark this section for Universal Synchronization** 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.

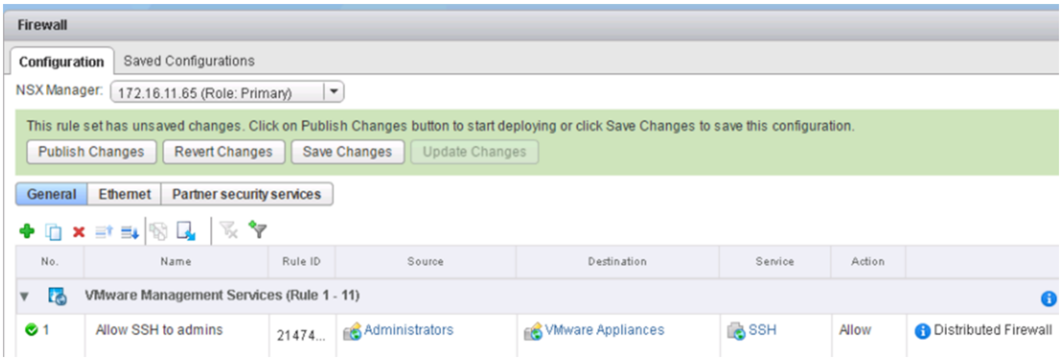
   b. In the **Name** cell of the new rule, click the **Edit** icon to change the rule name to `Allow SSH to admins`.

   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**.



NSX Manager: 172.16.11.65 (Role: Primary)

This rule set has unsaved changes. Click on Publish Changes button to start deploying or click Save Changes to save this configuration.

No.	Name	Rule ID	Source	Destination	Service	Action	
VMware Management Services (Rule 1 - 11)							
1	Allow SSH to admins	21474...	Administrators	VMware Appliances	SSH	Allow	Distributed Firewall

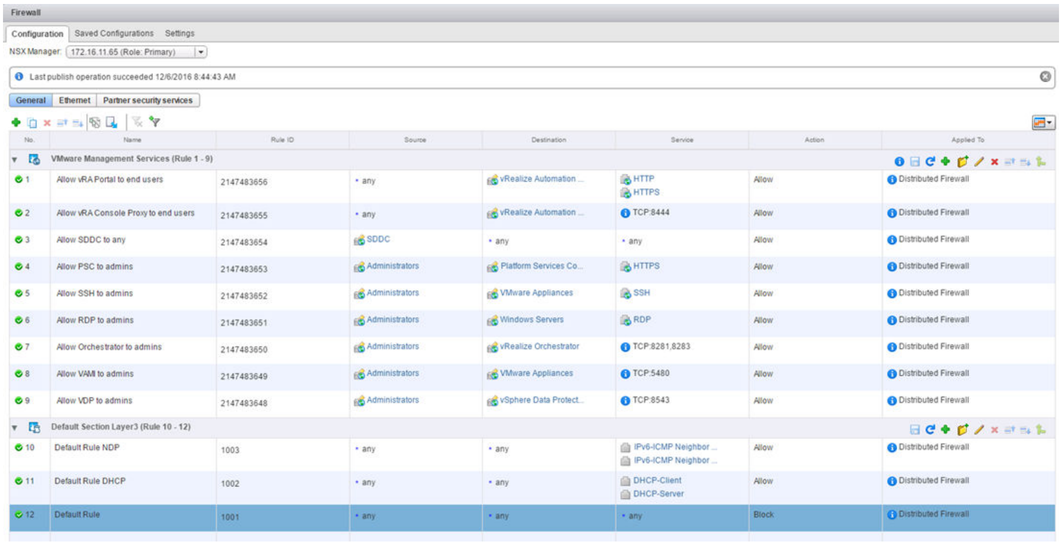
4. Repeat the previous step to create the following distributed firewall rules.

Name	Source	Destination	Service / Port
Allow vRA Portal to end users	* any	vRealize Automation Appliances	HTTP, HTTPS
Allow vRA Console Proxy to end users	* any	vRealize Automation Appliances	TCP:8444
Allow SDDC to any	SDDC	* any	* any
Allow PSC to admins	Administrators	Platform Services Controller Instances	HTTPS
Allow SSH to admins	Administrators	VMware Appliances	SSH

Name	Source	Destination	Service / Port
Allow RDP to admins	Administrators	Windows Servers	RDP
Allow Orchestrator to admins	Administrators	vRealize Orchestrator	TCP:8281,8283
Allow vROPs to admins	Administrators	vRealize Operations Manager	HTTP, HTTPS
Allow vRLI to admins	Administrators	vRealize Log Insight	HTTP, HTTPS
Allow VAMI to admins	Administrators	VMware Appliances	TCP:5480
Allow VDP to admins	Administrators	VMware Appliances	TCP:8543

5. Click **Publish Changes**.
6. Change the default rule action from allow to block for Region A.
   a. Under **Default Section Layer3**, in the **Action** column for the Default Rule, change the action to **Block** and click **Save**.
   b. Click **Publish Changes**.
7. Change the default rule action from allow to block for Region B.
   a. From the **NSX Manager** drop-down menu, select **172.17.11.65**.
   b. Under **Default Section Layer3**, in the **Action** column for the Default Rule, change the action to **Block** and click **Save**.
   c. Click **Publish Changes**.

By allowing only the network traffic that is required by the SDDC to pass, network security is improved.



NSX Manager: 172.16.11.65 (Role: Primary)

Last publish operation succeeded 12/6/2016 8:44:43 AM

No.	Name	Rule ID	Source	Destination	Service	Action	Applied To
	VMware Management Services (Rule 1 - 9)						
1	Allow vRA Portal to end users	2147483656	any	vRealize Automation ...	HTTP HTTPS	Allow	Distributed Firewall
2	Allow vRA Console Proxy to end users	2147483655	any	vRealize Automation ...	TCP:8444	Allow	Distributed Firewall
3	Allow SDDC to any	2147483654	SDDC	any	any	Allow	Distributed Firewall
4	Allow PSC to admins	2147483653	Administrators	Platform Services Co...	HTTPS	Allow	Distributed Firewall
5	Allow SSH to admins	2147483652	Administrators	VMware Appliances	SSH	Allow	Distributed Firewall
6	Allow RDP to admins	2147483651	Administrators	Windows Servers	RDP	Allow	Distributed Firewall
7	Allow Orchestrator to admins	2147483650	Administrators	vRealize Orchestrator	TCP:8281,8283	Allow	Distributed Firewall
8	Allow VAMI to admins	2147483649	Administrators	VMware Appliances	TCP:5480	Allow	Distributed Firewall
9	Allow VDP to admins	2147483648	Administrators	vSphere Data Protect...	TCP:8543	Allow	Distributed Firewall
	Default Section Layer3 (Rule 10 - 12)						
10	Default Rule NDP	1003	any	any	IPv6-ICMP Neighbor ... IPv6-ICMP Neighbor ...	Allow	Distributed Firewall
11	Default Rule DHCP	1002	any	any	DHCP-Client DHCP-Server	Allow	Distributed Firewall
12	Default Rule	1001	any	any	any	Block	Distributed Firewall

Test the Management Cluster NSX Configuration in Region A

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.

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 Use the Ping Monitor to test connectivity.

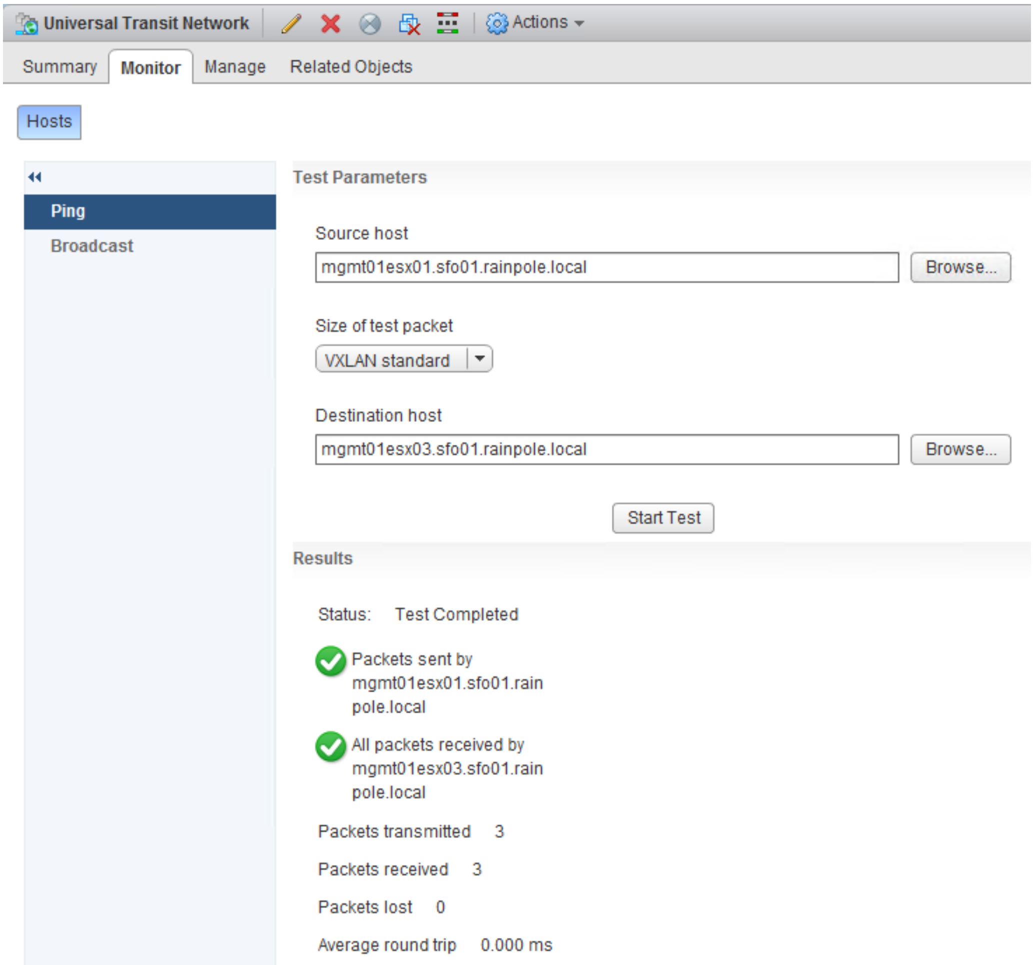
   a Under **Logical Switches**, double-click **Universal Transit Network**.

   b Click the **Monitor** tab.

   c From the **Source host** drop-down menu select **mgmt01esx01.sfo01.rainpole.local**.

d From the **Destination host** drop-down menu select **mgmt01esx03.sfo01.rainpole.local**.

e Click **Start Test**.



Test Parameters

Source host: mgmt01esx01.sfo01.rainpole.local

Size of test packet: VXLAN standard

Destination host: mgmt01esx03.sfo01.rainpole.local

Results

Status: Test Completed

✓ Packets sent by mgmt01esx01.sfo01.rainpole.local

✓ All packets received by mgmt01esx03.sfo01.rainpole.local

Packets transmitted 3

Packets received 3

Packets lost 0

Average round trip 0.000 ms

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 Region A

Deploy the application virtual networks.

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. Create a Universal Logical Switch for workloads that move between sites.

   a. Under **Inventories**, click **Networking & Security**.

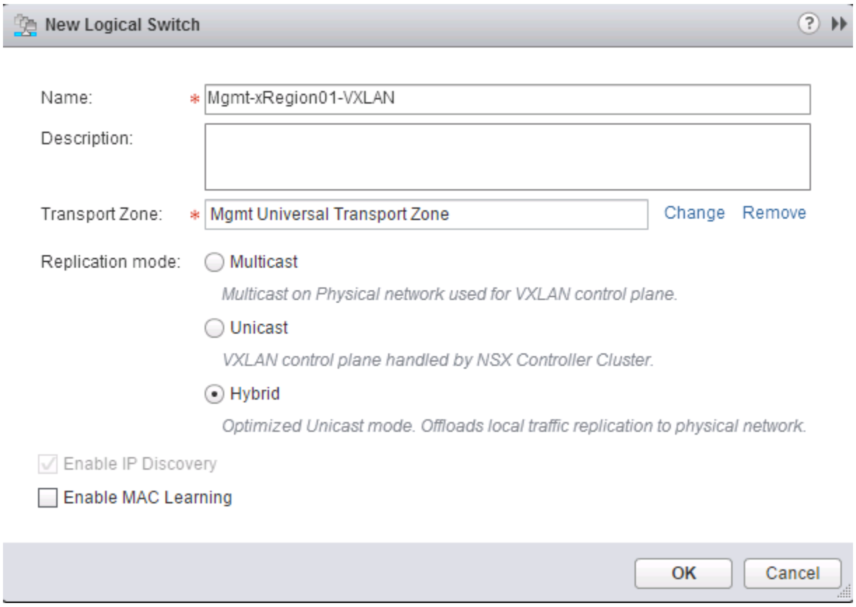
   b. In the **Navigator**, click **Logical Switches**.

   c. Select **172.16.11.65** 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-xRegion01-VXLAN
Transport Zone	Mgmt Universal Transport Zone
Replication Mode	Hybrid



New Logical Switch

Name: * Mgmt-xRegion01-VXLAN

Description:

Transport Zone: * Mgmt Universal Transport Zone 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

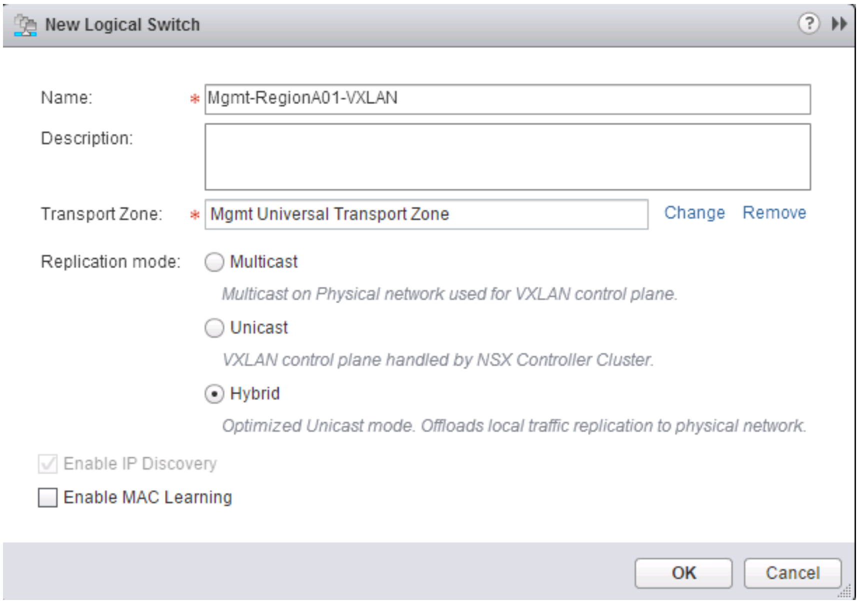
□ Enable MAC Learning

3 Create a Universal Logical Switch for workloads specific to Region A.

   a On the **Logical Switches** page, click the **Add** icon to create a new Logical Switch.

   b In the **New Logical Switch** dialog box, enter the following settings, and click **OK**.

Setting	Value
Name	Mgmt-RegionA01-VXLAN
Transport Zone	Mgmt Universal Transport Zone
Replication Mode	Hybrid



Name: * Mgmt-RegionA01-VXLAN

Description:

Transport Zone: * Mgmt Universal Transport Zone

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

4 Connect Mgmt-xRegion01-VXLAN to the Universal Distributed Logical Router.

   a On the **Logical Switches** page, select the **Mgmt-xRegion01-VXLAN** Logical Switch.

   b Click the **Connect Edge** icon.

   c On the **Connect an Edge** page, select **SFOMGMT-UDLR01** and click **Next**.

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

Setting	Value
Name	Mgmt-xRegion01-VXLAN
Type	Internal
Connected To	Mgmt-xRegion01-VXLAN
Connectivity Status	Connected
Primary IP Address	192.168.11.1
Subnet Prefix Length	24

   e On the **Ready to complete** page, click **Finish**.

5 Connect Mgmt-RegionA01-VXLAN to the UDLR01 Universal Distributed Logical Router.

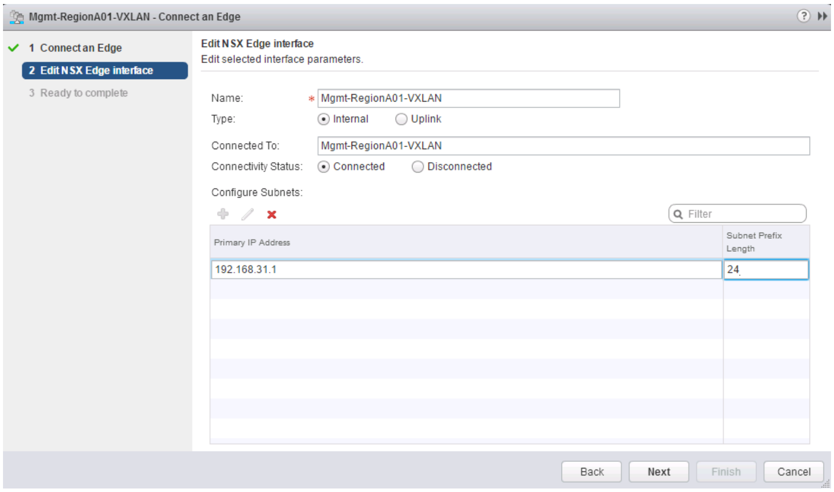
a On the **Logical Switches** page, select the **Mgmt-RegionA01-VXLAN** Logical Switch.

b Click the **Connect Edge** icon.

c On the **Connect an Edge** page, select **SFOMGMT-UDLR01** and click **Next**.

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

Setting	Value
Name	Mgmt-RegionA01-VXLAN
Type	Internal
Connected To	Mgmt-RegionA01-VXLAN
Connectivity Status	Connected
Primary IP Address	192.168.31.1
Subnet Prefix Length	24



Mgmt-RegionA01-VXLAN - Connect an Edge

1 Connect an Edge
2 Edit NSX Edge interface
3 Ready to complete

Edit NSX Edge interface
Edit selected interface parameters.

Name: * Mgmt-RegionA01-VXLAN
Type: ● Internal ○ Uplink
Connected To: Mgmt-RegionA01-VXLAN
Connectivity Status: ● Connected ○ Disconnected
Configure Subnets:

Primary IP Address	Subnet Prefix Length
192.168.31.1	24

e On the **Ready to complete** page, click **Finish**.

6 Configure the MTU for the Logical Switches.

a Double-click **SFOMGMT-UDLR01**.

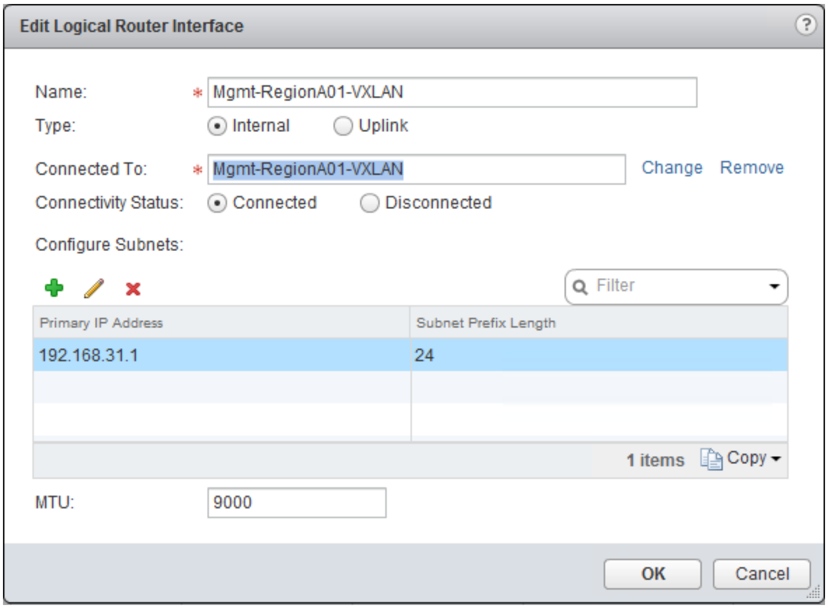
b Click the **Manage** tab and click **Settings**.

c On the **Settings** page, click on **Interfaces**.

d Under **Interfaces**, select **Mgmt-RegionA01-VXLAN**, and click **Edit**.

e On the **Edit Logical Router Interface**,configure **MTU** , and click **OK**.

Setting	Value
Mgmt-RegionA01-VXLAN	9000
Mgmt-xRegion01-VXLAN	9000



Edit Logical Router Interface

Name: * Mgmt-RegionA01-VXLAN

Type: ● Internal ○ Uplink

Connected To: * Mgmt-RegionA01-VXLAN

Connectivity Status: ● Connected ○ Disconnected

Configure Subnets:

Primary IP Address	Subnet Prefix Length
192.168.31.1	24

1 items

MTU: 9000

Deploy the NSX Load Balancer in Region A

Deploy a load balancer for use by management applications connected to the AVN, `Mgmt-xRegion01-VXLAN`.

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 Under **Inventories**, click **Networking & Security**.

3 In the **Navigator**, click **NSX Edges**.

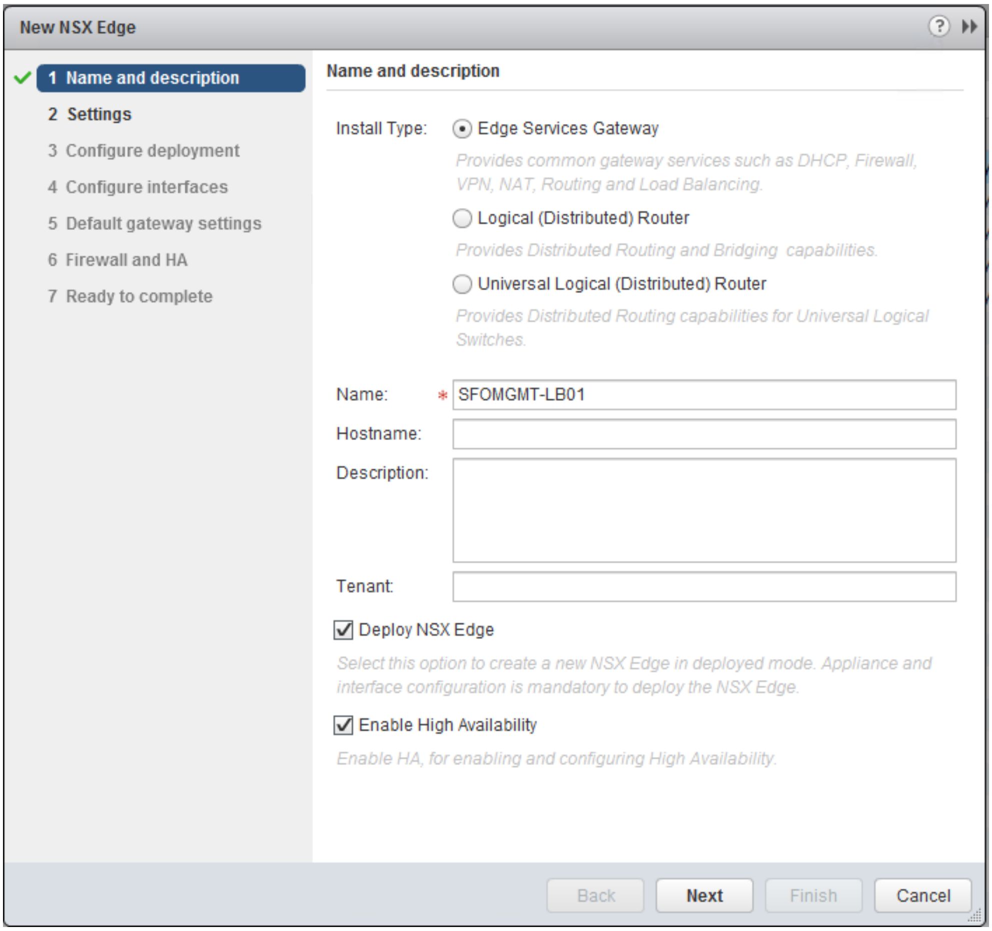
4 Select **172.16.11.65** from the **NSX Manager** drop-down menu.

5 Click the **Add** icon to create an NSX Edge.

The **New NSX Edge** wizard appears.

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

Setting	Value
Install Type	Edge Services Gateway
Name	SFOMGMT-LB01
Deploy NSX Edge	Selected
Enable High Availability	Selected



Name and description

Install Type: ● Edge Services Gateway

Provides common gateway services such as DHCP, Firewall, VPN, NAT, Routing and Load Balancing.

○ Logical (Distributed) Router

Provides Distributed Routing and Bridging capabilities.

○ Universal Logical (Distributed) Router

Provides Distributed Routing capabilities for Universal Logical Switches.

Name: * SFOMGMT-LB01

Hostname:

Description:

Tenant:

☑ Deploy NSX Edge

Select this option to create a new NSX Edge in deployed mode. Appliance and interface configuration is mandatory to deploy the NSX Edge.

☑ Enable High Availability

Enable HA, for enabling and configuring High Availability.

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

Setting	Value
User Name	admin
Password	*edge_admin_password*
Enable SSH access	Selected
Enable FIPS mode	Deselected

Setting	Value
Enable auto rule generation	Selected
Edge Control Level logging	INFO

8 On the **Configure deployment** page, perform the following configuration steps and click **Next**.

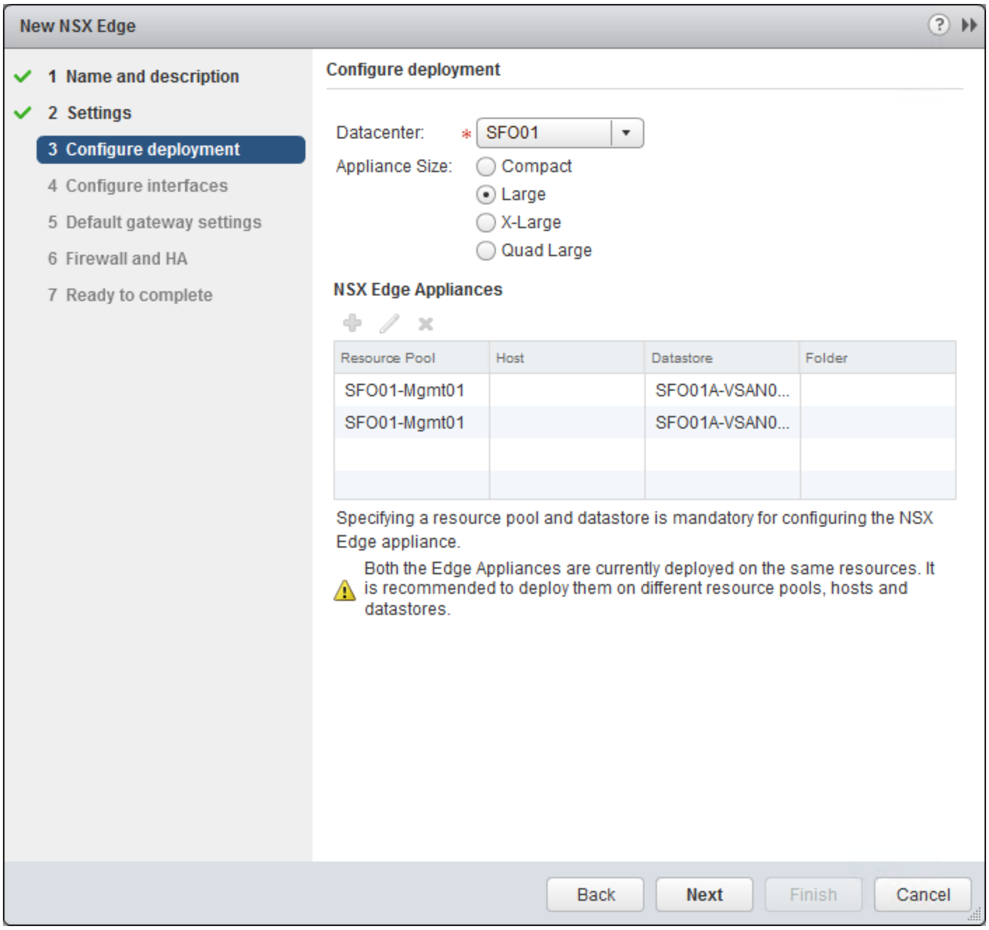
a Select **SF001**, from the **Datacenter** drop-down menu.

b Click **Large** to specify the **Appliance Size**.

c Click the **Add** icon, enter the following settings, and click **OK**.

Setting	Value
Resource pool	SFO01-Mgmt01
Datastore	SFO01A-VSAN01-MGMT01
Folder	NSX01

d To create a second appliance, click the **Add** icon again, make the same selections in the **New NSX Appliance** dialog box, and click **OK**.



Configure deployment

Datacenter: * SFO01

Appliance Size: ○ Compact ● Large ○ X-Large ○ Quad Large

NSX Edge Appliances

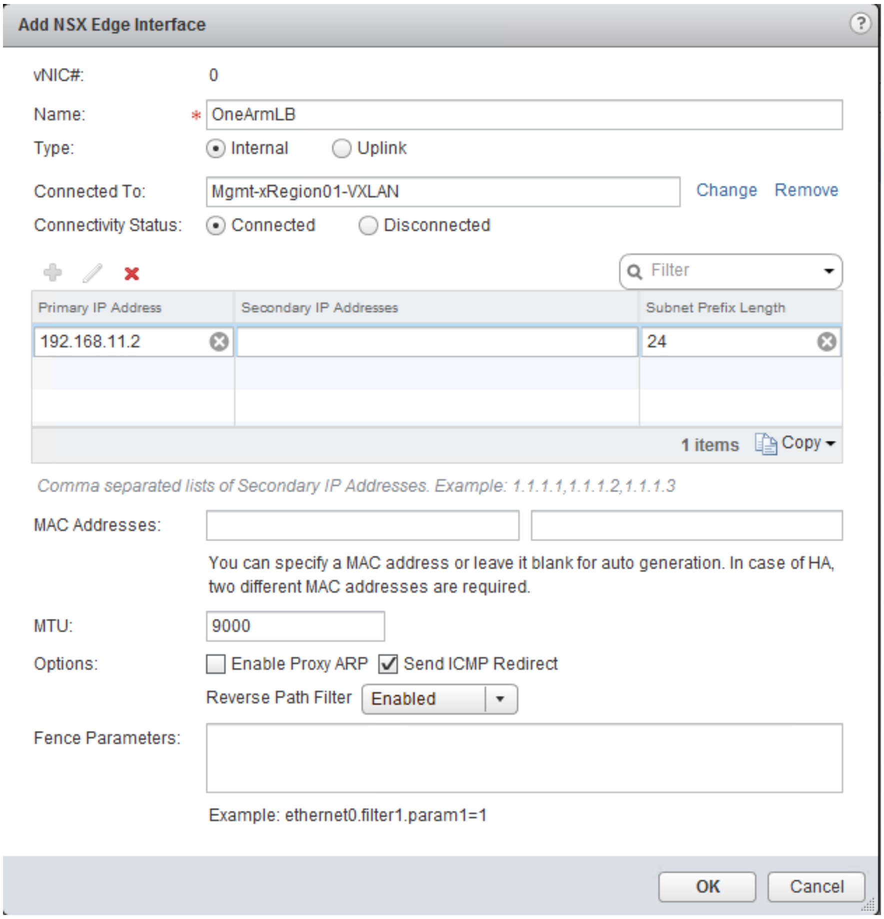
Resource Pool	Host	Datastore	Folder
SFO01-Mgmt01		SFO01A-VSAN0...	
SFO01-Mgmt01		SFO01A-VSAN0...	

Specifying a resource pool and datastore is mandatory for configuring the NSX Edge appliance.

⚠ Both the Edge Appliances are currently deployed on the same resources. It is recommended to deploy them on different resource pools, hosts and datastores.

9 On the **Configure Interfaces** page, click the **Add** icon to configure the OneArmLB interface, enter the following settings, click **OK**, and click **Next**.

Setting	Value
Name	OneArmLB
Type	Internal
Connected To	Mgmt-xRegion01-VXLAN
Connectivity Status	Connected
Primary IP Address	192.168.11.2
Subnet Prefix Length	24
MTU	9000
Send ICMP Redirect	Selected



Add NSX Edge Interface

vNIC#: 0

Name: * OneArmLB

Type: ● Internal ○ Uplink

Connected To: Mgmt-xRegion01-VXLAN Change Remove

Connectivity Status: ● Connected ○ Disconnected

Primary IP Address	Secondary IP Addresses	Subnet Prefix Length
192.168.11.2		24

1 items Copy

Comma separated lists of Secondary IP Addresses. Example: 1.1.1.1,1.1.1.2,1.1.1.3

MAC Addresses:

You can specify a MAC address or leave it blank for auto generation. In case of HA, two different MAC addresses are required.

MTU: 9000

Options: □ Enable Proxy ARP ☑ Send ICMP Redirect

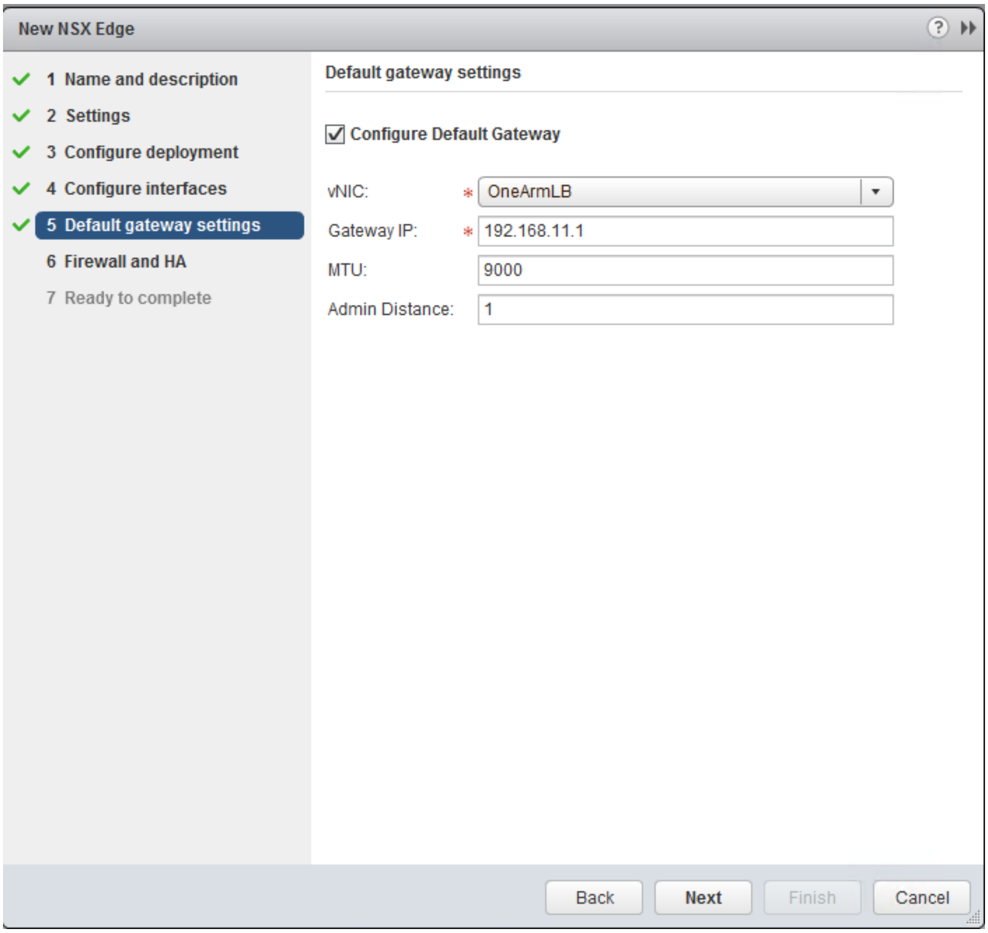
Reverse Path Filter Enabled

Fence Parameters:

Example: ethernet0.filter1.param1=1

10 On the **Default gateway** settings page, enter the following settings and click **Next**.

Setting	Value
Gateway IP	192.168.11.1
MTU	9000



New NSX Edge

- ✓ 1 Name and description
- ✓ 2 Settings
- ✓ 3 Configure deployment
- ✓ 4 Configure interfaces
- ✓ 5 Default gateway settings
- 6 Firewall and HA
- 7 Ready to complete

Default gateway settings

☑ Configure Default Gateway

vNIC: * OneArmLB

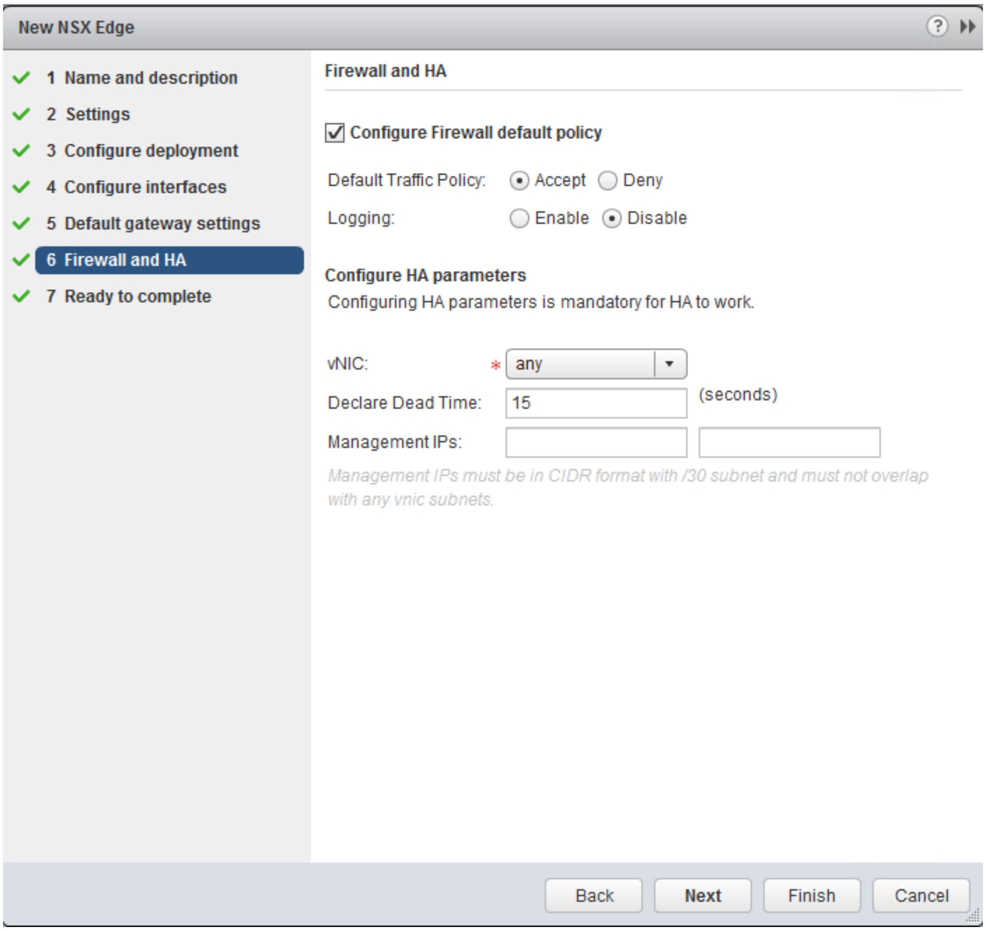
Gateway IP: * 192.168.11.1

MTU: 9000

Admin Distance: 1

11 On the **Firewall and HA** page, select the following settings and click **Next**.

Setting	Value
Configure Firewall default policy	Selected
Default Traffic Policy	Accept
Logging	Disable
vNIC	any
Declare Dead Time	15



New NSX Edge

Firewall and HA

☑ Configure Firewall default policy

Default Traffic Policy: ● Accept ○ Deny

Logging: ○ Enable ● Disable

Configure HA parameters

Configuring HA parameters is mandatory for HA to work.

vNIC: * any

Declare Dead Time: 15 (seconds)

Management IPs:

Management IPs must be in CIDR format with /30 subnet and must not overlap with any vnic subnets.

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

13 Enable HA logging.

a In the Navigator, click **NSX Edges**.

b Select **172.16.11.65** from the **NSX Manager** drop-down menu.

c Double-click the device labeled **SFOMGMT01-LB01**.

d Click the **Manage** tab and click the **Settings** tab.

e Click **Change** in the **HA Configuration** window.

f Select the **Enable Logging** checkbox and click **OK**.

14 Enable the Load Balancer service.

a In the **Navigator**, click **NSX Edges**.

b Select **172.16.11.65** from the **NSX Manager** drop-down menu.

c Double-click the device labeled **SFOMGMT01-LB01**.

d Click the **Manage** tab, click the **Load Balancer** tab, click **Global Configuration**, and click **Edit**.

15 In the **Edit load balancer global configuration** dialog box, select **Enable Load Balancer** and click **OK**.

Deploy and Configure the Shared Edge and Compute Cluster Components in Region A

Deploy and configure the shared edge and compute cluster components.

Procedure

1 Deploy the Compute vCenter Server Instance in Region A

After you install and configure the external Platform Services Controller instance for the shared edge and compute cluster, you can now install the vCenter Server appliance and assign a license.

2 Add New vCenter Server Licenses in Region A

(Optional) If a license was not assigned during deployment of the Management vCenter Server and ESXi hosts, you may add new licenses for this vCenter Server instance if needed.

3 Add the Shared Edge and Compute vCenter to the vCenter Servers VM Group in Region A

After the vCenter Server for the Shared Edge and Computer cluster is deployed it must be added to the vCenter VM Group.

4 Exclude the Compute vCenter Server from the Distributed Firewall in Region A

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

5 Configure the Shared Edge and Compute Cluster in Region A

After you deploy the Compute vCenter Server, you must create and configure the shared edge and compute cluster.

6 Create a vSphere Distributed Switch for the Shared Edge and Compute Cluster in Region A

After all ESXi hosts have been added to the cluster, create a vSphere Distributed Switch.

7 Enable vSphere HA on the Shared Edge and Compute Cluster in Region A

After vSphere vSphere Distributed Switch has been created and connected with all hosts, enable vSphere HA on the cluster.

8 Change Advanced Options on the ESXi Hosts on the ESXi Hosts in the Shared Edge and Compute Cluster in Region A

Change the default ESX Admins group to achieve greater levels of security by removing a known administrative access point.

9 Mount NFS Storage for the Shared Edge and Compute Cluster in Region A

You must mount an NFS datastore for the content library consumed by vRealize Automation for virtual machine provisioning.

10 Create and Apply the Host Profile for the Shared Edge and Compute Cluster in Region A

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

11 Configure Lockdown Mode on All ESXi Hosts in Region A

To increase security of your ESXi hosts, you put them in Lockdown mode, so that administrative operations can be performed only from vCenter Server.

Deploy the Compute vCenter Server Instance in Region A

After you install and configure the external Platform Services Controller instance for the shared edge and compute cluster, you can now install the vCenter Server appliance and assign a license.

Procedure

1 Start the **vCenter Server Appliance Deployment** wizard.

   a Browse the vCenter Server Appliance ISO file.

   b Open the `<dvd-drive>:\vcsa-ui-installer\win32\Installer` application file.

2 Complete the **vCenter Server Appliance Deployment** wizard to perform the first stage of the installation.

   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**, select the **vCenter Server (Requires External Platform Services Controller)** radio button 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	mgmt01vc01.sfo01.rainpole.local
HTTPS port	443
User name	administrator@vsphere.local
Password	*vsphere_admin_password*

   f In the **Certificate Warning** dialog box, click **Yes** to accept the host certificate.

   g On the **Select folder** page, choose **MGMT01**.

   h On the **Select compute resource** page, choose the **SFO01-Mgmt01** cluster.

   i On the **Set up appliance VM** page, enter the following settings and click **Next**.

Setting	Value
VM name	comp01vc01
Root password	*compvc_root_password*
Confirm root password	*compvc_root_password*

j On the **Select deployment size** page, select **Large vCenter Server**, and click **Next**.

k On the **Select datastore** page, select the **SFO01A-VSAN01-MGMT01** datastore, select the **Enable Thin Disk Mode** check box, and click **Next**.

l On the **Configure network settings** page, enter the following settings and click **Next**.

Setting	Value
Network	vDS-Mgmt-Management
IP version	IPv4
IP assignment	static
System name	comp01vc01.sfo01.rainpole.local
IP address	172.16.11.64
Subnet mask or prefix length	255.255.255.0
Default gateway	172.16.11.253
DNS servers	172.16.11.5,172.16.11.4

m On the **Ready to complete stage 1** page, review the configuration and click **Finish** to start the deployment.

n Once the deployment completes, click **Continue** to proceed to stage two of the installation.

3 Complete the **Set Up vCenter Server Appliance** wizard to complete the second stage of the installation.

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.sfo01.rainpole.local
SSH access	Enabled

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

Setting	Value
Platform Services Controller	sfo01psc01.sfo01.rainpole.local
HTTPS port	443
SSO domain name	vsphere.local
SSO password	*sso_password*

d On the **Ready to complete** page, review the configuration and click **Finish**.

e Click **OK** on the Warning.

Add New vCenter Server Licenses in Region A

(Optional) If a license was not assigned during deployment of the Management vCenter Server and ESXi hosts, you may add new licenses for this vCenter Server instance if needed.

Procedure

1 Log in to the Compute 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 Click the **Home** icon above the **Navigator** and choose the **Administration** menu item.

3 On the **Administration** page, click **Licenses** and click the **Licenses** tab.

4 Click the **Create New Licenses** icon to add license keys.

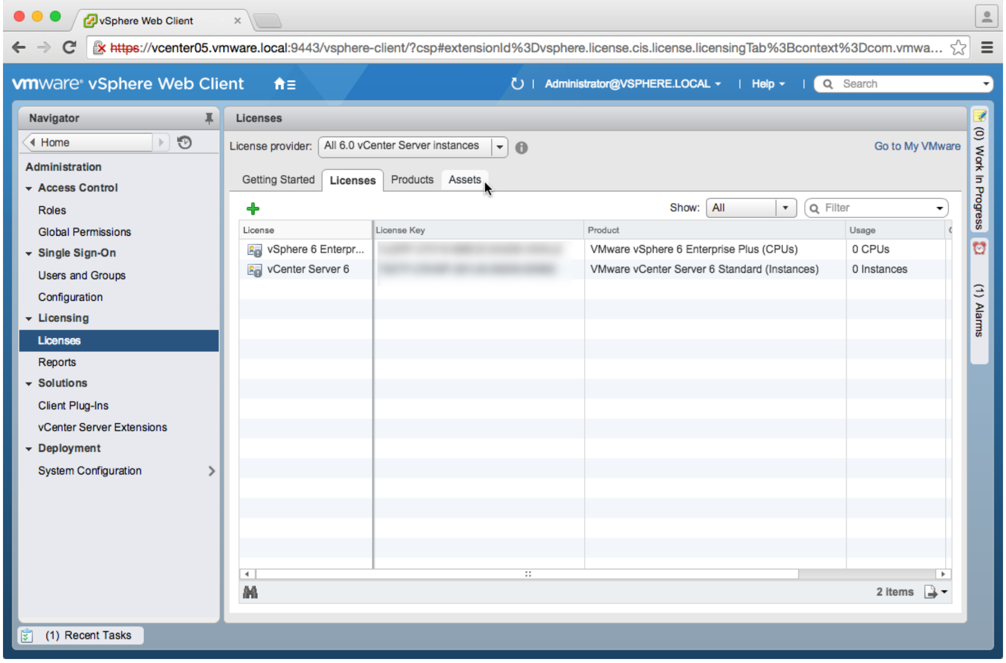
5 On the **Enter license keys** page, enter license keys for vCenter Server and ESXi, one per line, and click **Next**.

6 On the **Edit license name** page, enter a descriptive name for each license key, and click **Next**.

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

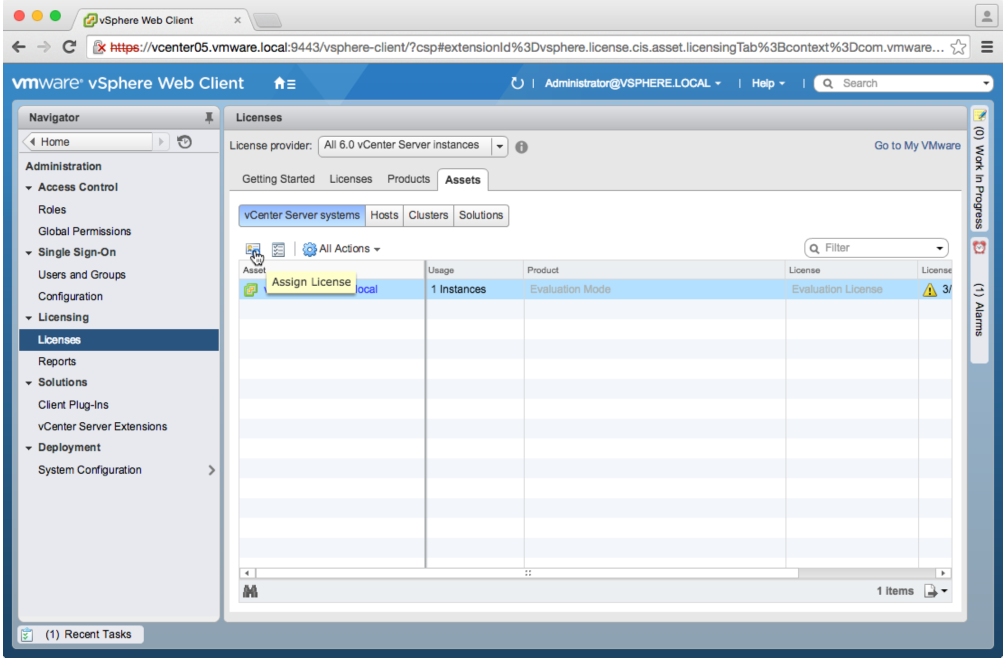
8 Assign the newly added licenses to the respective assets.

a Click the **Assets** tab.



License	License Key	Product	Usage
vSphere 6 Enterpr...	[redacted]	VMware vSphere 6 Enterprise Plus (CPUs)	0 CPUs
vCenter Server 6	[redacted]	VMware vCenter Server 6 Standard (Instances)	0 Instances

b Select the vCenter Server instance, and click the **Assign License** icon.



Asset	Usage	Product	License	License
v...local	1 Instances	Evaluation Mode	Evaluation License	⚠ 3/

c Select the vCenter Server license that you entered in the previous step and click **OK**.

Add the Shared Edge and Compute vCenter to the vCenter Servers VM Group in Region A

After the vCenter Server for the Shared Edge and Computer cluster is deployed it must be added to the vCenter VM Group.

Procedure

1 Log in to the Management 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 In the **Navigator**, select **Hosts and Clusters** and expand the **mgmt01vc01.sfo01.rainpole.local tree**.

3 Select the **SFO01-Mgmt01** cluster and click **Configure**.

4 On the **Configure** page, click **VM/Host Groups**.

5 On the **VM/Host Groups** page, select the **vCenter Servers** VM Group.

6 Under **VM/Host Group Members**, click the **Edit** button.

7 In the **Add Group Member** dialog, select **comp01vc01** and click **OK**.

Exclude the Compute vCenter Server from the Distributed Firewall in Region A

Exclude vCenter Server from all of your distributed firewall rules. This ensures that network access between vCenter Server and NSX 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://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 In the Navigator, click **Networking & Security**.

3 Click **NSX Managers** and select the **172.16.11.65** instance.

4 Click **Manage** and then click **Exclusion** List.

5 Click the **Add** button.

6 Add **comp01vc01** to the **Selected Objects** list, and click **OK**.

Configure the Shared Edge and Compute Cluster in Region A

After you deploy the Compute vCenter Server, you must create and configure the shared edge and compute cluster.

To create and configure the shared edge and compute cluster you perform the following procedures:

- Create the cluster.
- Configure DRS.
- Add the hosts to the cluster.
- Add the hosts to the active directory domain.
- Create resource pools.

Procedure

1 Log in to the Compute 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 Log in to the Compute 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*

3 Create a data center object.

   a In the **Navigator**, click **Hosts and Clusters**.

   b Right-click the **comp01vc01.sfo01.rainpole.local** instance, and select **New Datacenter**.

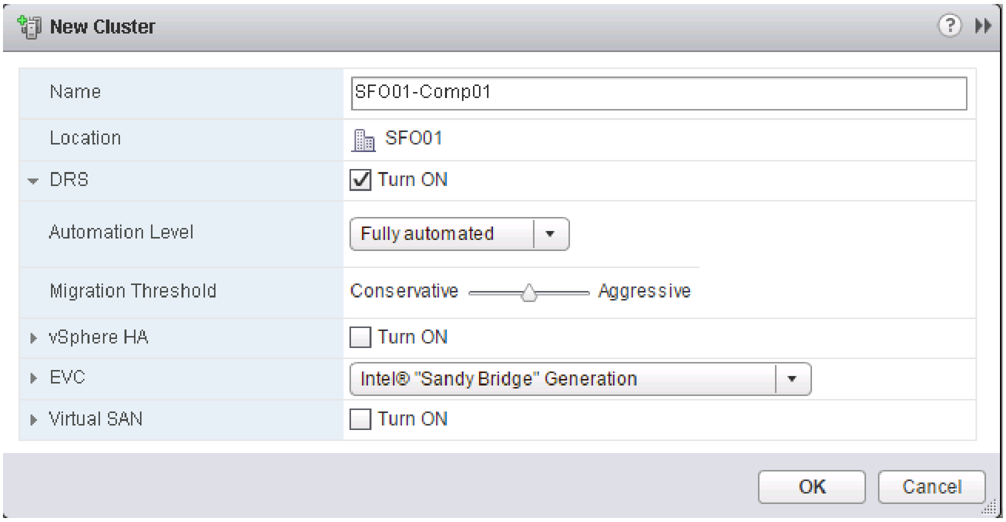
   c In the **New Datacenter** dialog box, enter **`SFO01`** as name, and click **OK**.

4 Create the shared edge and compute cluster.

   a Right-click the **SFO01** datacenter and click **New Cluster**.

   b In the **New Cluster** wizard, enter the following values and click **OK**.

Setting		**Value**
Name		SFO01-Comp01
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**	Deselected



New Cluster

Name	SFO01-Comp01
Location	SFO01
DRS	☑ Turn ON
Automation Level	Fully automated
Migration Threshold	Conservative — Aggressive
vSphere HA	□ Turn ON
EVC	Intel® "Sandy Bridge" Generation
Virtual SAN	□ Turn ON

5 Add a host to the shared edge and compute cluster.

   a Right-click the **SFO01-Comp01** cluster, and click **Add Host**.

   b On the **Name and location** page, enter **`comp01esx01.sfo01.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**.

6 Repeat the previous step to add the remaining hosts to the cluster.

Setting	Value
Host 2	comp01esx02.sfo01.rainpole.local
Host 3	comp01esx03.sfo01.rainpole.local
Host 4	comp01esx04.sfo01.rainpole.local

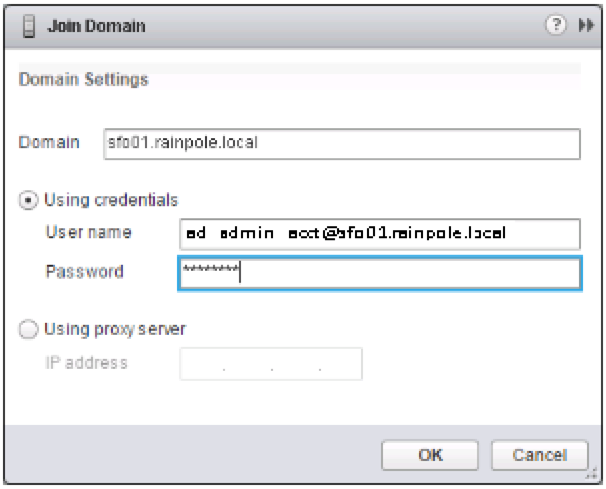
7 Add an ESXi host to the active directory domain

- a In the **Navigator**, click **Hosts and Clusters** and expand the entire **comp01vc01.sfo01.rainpole.local** tree.
- b Select the **comp01esx01.sfo01.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	sfo01.rainpole.local
User name	*ad_admin_acct*@sfo01.rainpole.local
Password	*ad_admin_password*



Domain sfo01.rainpole.local

● Using credentials

User name ad admin acct@sfo01.rainpole.local

Password ********

○ Using proxy server

IP address . . .

8 Set the Active Directory Service to Start and stop with host.

a In the **Navigator**, click **Hosts and Clusters** and expand the entire **comp01vc01.sfo01.rainpole.local** tree.

b Select the **comp01esx01.sfo01.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**.

9 Configure a resource pool for the shared edge and compute cluster.

   a Right the **SFO01-Comp01** cluster and select **New Resource Pool**.

   b In the **New Resource Pool** dialog box, enter the following values and click **OK**.

Setting	Value
Name	SDDC-EdgeRP01
CPU-Shares	High
CPU-Reservation	0
CPU-Reservation Type	Expandable selected
CPU-Limit	Unlimited
Memory-Shares	Normal
Memory-Reservation	16 GB
Memory-Reservation type	Expandable selected
Memory-Limit	Unlimited

10 Repeat step Step 9 to add two more additional resource pools.

Setting	Resource Pool 2	Resource Pool 3
Name	User-EdgeRP01	User-VMRP01
CPU-Shares	Normal	Normal
CPU-Reservation	0	0
CPU-Reservation Type	Expandable selected	Expandable selected
CPU-Limit	Unlimited	Unlimited
Memory-Shares	Normal	Normal
Memory-Reservation	0	0
Memory-Reservation type	Expandable selected	Expandable selected
Memory-Limit	Unlimited	Unlimited

Create a vSphere Distributed Switch for the Shared Edge and Compute Cluster in Region A

After all ESXi hosts have been added to the cluster, create a vSphere Distributed Switch.

Procedure

1 Log in to the Compute 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 Create a vSphere Distributed Switch for the shared edge and compute cluster.

  a In the **Navigator**, click **Networking** and expand the **comp01vc01.sfo01.rainpole.local** control tree.

  b Right-click the **SFO01** datacenter and select **Distributed Switch > New Distributed Switch** to start the **New Distributed Switch** wizard .

  c On the **Name and location** page, enter `vDS-Comp01` as the name and click **Next**.

  d On the **Select version** page, ensure the **Distributed switch version: 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-Comp01 distributed switch.

  a Right-click the **vDS-Comp01** distributed switch and select **Settings > Edit Settings**.

  b Click the **Advanced** tab.

  c Enter `9000` as **MTU (Bytes)** value and click **OK**.

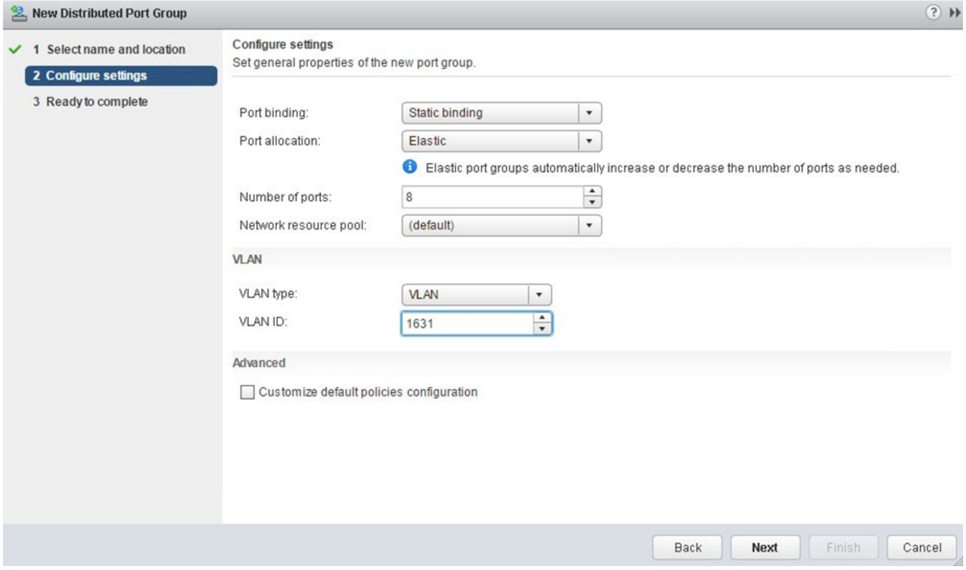
4 Create port groups in the vDS-Comp01 distributed switch.

a Right-click the **vDS-Comp01** 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-Comp01-Management	Static binding	VLAN	1631
vDS-Comp01-vMotion	Static binding	VLAN	1632
vDS-Comp01-VSAN	Static binding	VLAN	1633
vDS-Comp01-NFS	Static binding	VLAN	1615
vDS-Comp01-Uplink01	Static binding	VLAN	1625
vDS-Comp01-Uplink02	Static binding	VLAN	2713

Note You create the VXLAN port group at a later time during the configuration of NSX Manager.



Configure settings

Set general properties of the new port group.

Port binding: Static binding

Port allocation: Elastic

Elastic port groups automatically increase or decrease the number of ports as needed.

Number of ports: 8

Network resource pool: (default)

VLAN

VLAN type: VLAN

VLAN ID: 1631

Advanced

□ Customize default policies configuration

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-Comp01** distributed switch and select **Distributed Port Groups > Manage Distributed Port Groups**.

b Select **Teaming and failover** and click **Next**.

c Click the **Select distributed port groups** button, add all port groups and click **Next**.

d Select **Route based on physical NIC load** under **Load Balancing** and click **Next**.

e Click **Finish**.

6 Connect the ESXi host, comp01esx01.sfo01.rainpole.local, to the vDS-Comp01 distributed switch by migrating its VMkernel and virtual machine network adapters.

   a Right-click the **vDS-Comp01** 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 **comp01esx01.sfo01.rainpole.local** and click **OK**.

   e On the **Select hosts** page, click **Next**.

   f On the **Select network adapter tasks** page, ensure both **Manage physical adapters** and **Manage VMkernel adapters** check boxes are checked 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 1** 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-Comp01-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 and existing network**, browse to select the **vDS-Comp01-NFS** port group, click **OK**, and click **Next**.

   e Under **Port properties** click **Next**.

   f Under **IPv4 settings** select **Use static IPv4 settings**, enter the IP address `172.16.25.101` and 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 **comp01vc01.sfo01.rainpole.local** tree.

   b Click on **comp01esx01.sfo01.rainpole.local**.

   c Click the **Configure** tab then select **VMkernel adapters**.

   d Click the **Add host networking** icon and select **VMkernel Netowrk Adapter** and click Next.

   e On the **Add Networking** page, select **Select an existing network**, browse to select the **vDS-Comp01-vMotion** port group, click **OK**, and click **Next**.

   f On the **Port properties** page, select **vMotion** from the **TCP/IP Stack dropdown** and click **Next**.

g Under **IPv4 settings** select **Use static IPv4 settings,** enter the IP address `172.16.32.101`, 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 the previous step, 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 on **Routing** and enter `172.16.32.253` for the **default gateway** address and click **OK**.

11 Define Network I/O Control shares for the different traffic types on the `vDS–Comp01` distributed switch.

a In the **Navigator**, click **Networking**, and click the **SFO01** datacenter.

b Click the **vDS-Comp01** distributed switch.

c Click the **Configure** tab and click **Resource Allocation**.

d Under **System Traffic**, edit each of the following traffic types with the values from the table.

Setting	Value
Traffic Type	High
vSAN TRaffic	Low
NFS Traffic	Low
vMotion Traffic	Low
vSphere Replication Traffic	Low
Management Traffic	Normal
vSphere Data Protection Backup Traffic	Low
Virtual Machine Traffic	High
Fault Tolerance Traffic	Low
iSCSI Traffic	Low

12 Migrate the last physical adapter from the standard switch to the vDS-Comp01 distributed switch.

a In the **Navigator**, click **Networking** and expand the **SFO01** datacenter.

b Right-click the **vDS-Comp01** 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 **comp01esx01.sfo01.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, under **comp01esx01.sfo01.rainpole.local**, select **vmnic0**, and click **Assign uplink**.

  i In the **Select an Uplink** dialog box, select **Uplink 2** and click **OK.**

  j On the **Analyze Impact** page, click **Next**.

  k On the **Ready to complete** page, click **Finish**.

13 Enable vSphere Distributed Switch Health Check.

  a In the **Navigator**, click **Networking** and expand the **SFO01** datacenter.

  b Select the **vDS-Comp01** 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**.

14 Delete the vSphere Standard Switch.

  a In the **Navigator**, click on **Hosts and Clusters** and expand the **comp01vc01.sfo01.rainpole.local** control tree.

  b Click on **comp01esx01.sfo01.rainpole.local** and then click on **Configure**.

  c On the **Configure** page select **Virtual Switches**.

  d On the **Virtual Switches** page, select **vSwitch0**, and then click the **Remove selected switch** button.

  e In the **Remove Standard Switch** dialog box, click **Yes.**

Enable vSphere HA on the Shared Edge and Compute Cluster in Region A

After vSphere vSphere Distributed Switch has been created and connected with all hosts, enable vSphere HA on the cluster.

Procedure

1 Log in to the Compute 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 In the **Navigator**, click **Hosts and Clusters**.

   a Expand the **comp01vc01.sfo01.rainpole.local** inventory.

   b Select the **SFO01-Mgmt01** cluster.

3 Click the **Configure** tab and click **vSphere Availability**.

4 Click **Edit**.

5 In the **Edit Cluster Settings** dialog box, select the **Turn on vSphere HA** check box.

6 In the **Edit Cluster Settings** dialog box, under **Failures and Responses**, select the following values.

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

7 Click **Admission Control**.

8 Under the **Admission Control** settings, enter the 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%

9 Click **OK**.

Change Advanced Options on the ESXi Hosts on the ESXi Hosts in the Shared Edge and Compute Cluster in Region A

Change the default ESX Admins group to achieve greater levels of security by removing a known administrative access point.

Procedure

1 Log in to the Compute 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 Change the default ESX Admins group.

   a In the **Navigator**, click **Hosts and Clusters**.

   b Expand the vCenter Server inventory tree, and select the **comp01.esx01.sfo01.rainpole.local** host.

   c Click the **Configure** tab and under **System**, click **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 Disable the SSH warning banner.

   a In the **Navigator**, click **Hosts and Clusters**.

   b Expand the vCenter Server inventory tree, and select the **comp01.esx01.sfo01.rainpole.local** host.

   c Click the **Configure** tab and under **System**, click **Advanced System Settings**.

   d Click the **Edit** button.

   e In the filter box, enter `ssh` and wait for the search results.

   f Change the value of **UserVars.SuppressShellWarning** to `1` and click **OK**.

Mount NFS Storage for the Shared Edge and Compute Cluster in Region A

You must mount an NFS datastore for the content library consumed by vRealize Automation for virtual machine provisioning.

Create a datastore for the SFO01-Comp01 cluster.

Procedure

1 Log in to the Compute 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 In the **Navigator**, click **Hosts and Clusters** and expand the **comp01esx01.sfo01.rainpole.local tree**.

3 Click on **comp01esx01.sfo01.rainpole.local**.

4 Click on the **Datastores** tab.

5 Click the **Create a New Datastore** icon.

   The **New Datastore** wizard opens.

6 On the **Type** page, select **NFS** and click **Next**.

7 On the **NFS version** page, select **NFS 3** and click **Next**.

8 On the **Name and configuration** page, enter the following datastore information and click **Next**.

Setting	Value
Datastore Name	SFO01A-NFS01-VRALIB01
Folder	/V2D_vRA_ComputeA_1TB
server	172.16.25.251

9 On the **Ready to complete** page, review the configuration and click **Finish**.

Create and Apply the Host Profile for the Shared Edge and Compute Cluster in Region A

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

Procedure

1 Log in to the Compute 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 Create a Host Profile from comp01esx01.sfo01.rainpole.local.

   a In the **Navigator**, select **Hosts and Clusters** and expand the **comp01vc01.sfo01.rainpole.local** tree.

   b Right-click the ESXi host **comp01esx01.sfo01.rainpole.local** and choose **Host Profiles > Extract Host Profile**.

   c In the **Extract Host Profile** window, enter `SFO01-Comp01` for the **Name** and click **Next**.

   d In the **Ready to complete** window, click **Finish**.

3 Attach the Host Profile to the shared edge and compute cluster.

   a In the **Navigator**, select **Hosts and Clusters** and expand the **comp01vc01.sfo01.rainpole.local** tree.

   b Right-click on the **SFO01-Comp01** cluster, and choose **Host Profiles > Attach Host Profile**.

   c In the **Attach Host Profile** window, select the **SFO01-Comp01** Host Profile, select the **Skip Host Customization** checkbox, and click **Finish**.

4 Create Host Customizations for the hosts in the shared edge and compute cluster.

   a In the **Navigator**, select **Policies and Profiles**.

   b Click on **Host Profiles**, then right-click on **SFO01-Comp01**, and choose **Export Host Customizations**.

   c In the dialog box, click **Save**.

   d Choose a file location to save the *SFO01-Comp01_host_customizations.csv* file.

   e Open the *SFO01-Comp01_host_customizations.csv* in Excel.

f Edit the file using the following configuration value.

ESXi Host	Active Directory Configuration Password	Active Directory Configuration Username	NetStack Instance defaultTcpipStack->DNS configurationName for this host
comp01esx01.sfo01.rainpole.local	*ad_admin_password*	*ad_admin_acct@sfo01.rainpole.local*	comp01esx01
comp01esx02.sfo01.rainpole.local	*ad_admin_password*	*ad_admin_acct@sfo01.rainpole.local*	comp01esx02
comp01esx03.sfo01.rainpole.local	*ad_admin_password*	*ad_admin_acct@sfo01.rainpole.local*	comp01esx03
comp01esx04.sfo01.rainpole.local	*ad_admin_password*	*ad_admin_acct@sfo01.rainpole.local*	comp01esx04

ESXi Host	Host virtual NIC vDS-Comp01:vDS-Comp01-Management:management->IP address settingsIPv4 address	Host virtual NIC vDS-Comp01:vDS-Comp01-Management:management->IP address settingsSubnetMask
comp01esx01.sfo01.rainpole.local	172.16.31.101	255.255.255.0
comp01esx02.sfo01.rainpole.local	172.16.31.102	255.255.255.0
comp01esx03.sfo01.rainpole.local	172.16.31.103	255.255.255.0
comp01esx04.sfo01.rainpole.local	172.16.31.104	255.255.255.0

ESXi Host	Host virtual NIC vDS-Comp01:vDS-Comp01-NFS:<UNRESOLVED>->IP address settingsIPv4 address	Host virtual NIC vDS-Comp01:vDS-Comp01-Management:management->IP address settingsSubnetMask
comp01esx01.sfo01.rainpole.local	172.16.25.101	255.255.255.0
comp01esx02.sfo01.rainpole.local	172.16.25.102	255.255.255.0
comp01esx03.sfo01.rainpole.local	172.16.25.103	255.255.255.0
comp01esx04.sfo01.rainpole.local	172.16.25.104	255.255.255.0

ESXi Host	Host virtual NIC vDS-Comp01:vDS-Comp01-vMotion:vmotion->IP address settingsIPv4 address	Host virtual NIC vDS-Comp01:vDS-Comp01-vMotion:vmotion->IP address settingsSubnetMask
comp01esx01.sfo01.rainpole.local	172.16.32.101	255.255.255.0
comp01esx02.sfo01.rainpole.local	172.16.32.102	255.255.255.0
comp01esx03.sfo01.rainpole.local	172.16.32.103	255.255.255.0
comp01esx04.sfo01.rainpole.local	172.16.32.104	255.255.255.0

g Once the file has been updated, save it and close Excel.

h Click the **Configure** tab.

i Click the **Edit Host Customizations** button.

j In the **Edit Host Customizaions** window, select all hosts and click **Next**.

k Click the **Browse** button to use a customization file, locate the *SFO01-Comp01_host_customizations.csv* file saved earlier and select it and click **Open**, then click **Finish**.

5 Remediate the hosts in the shared edge and compute cluster.

a Click the Monitortab and click Compliance.

b Select **LAX01-Comp01** and click the **Check Host Profile Compliance** button.

c Select **comp01esx02.lax01.rainpole.local** and click the **Remediate host based on its host profile** button.

d Select **comp01esx03.lax01.rainpole.local** and click the **Remediate host based on its host profile** button.

e Select **comp01esx04.lax01.rainpole.local** and click the **Remediate host based on its host profile** button.

Note All hosts should now show a status of `Compliant`.

6 Schedule nightly compliance checks.

a On the **Policies and Profiles** page, click **SFO01-Comp01**, 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 **`SFO01-Comp01 Complance 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.

Configure Lockdown Mode on All ESXi Hosts in Region A

To increase security of your ESXi hosts, you put them in Lockdown mode, so that administrative operations can be performed only from vCenter Server.

vSphere supports an Exception User list, which is for service accounts that have to log in to the host directly. Accounts with administrator privileges that are on the Exception Users list can log in to the ESXi Shell. In addition, these users can log in to a host's DCUI in normal lockdown mode and can exit lockdown mode.

You repeat this procedure to enable normal lockdown mode for all hosts in the data center. The table below lists all of the hosts.

Table 2-9. Hosts in the data center

Host	FQDN
Management host 1	mgmt01esx01.sfo01.rainpole.local
Management host 2	mgmt01esx02.sfo01.rainpole.local
Management host 3	mgmt01esx03.sfo01.rainpole.local
Management host 4	mgmt01esx04.sfo01.rainpole.local
Shared Edge and Compute host 1	comp01esx01.sfo01.rainpole.local
Shared Edge and Compute host 2	comp01esx02.sfo01.rainpole.local
Shared Edge and Compute host 3	comp01esx03.sfo01.rainpole.local
Shared Edge and Compute host 4	comp01esx04.sfo01.rainpole.local

Procedure

1 Log in to the Compute 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 In the **Navigator**, click **Hosts and Clusters** and expand the entire **mgmt01vc01.sfo01.rainpole.local** tree control.

3 Select the **mgmt01esx01.sfo01.rainpole.local** host.

4 Click **Configure**.

5 Under **System**, select **Security Profile**.

6 In the **Lockdown Mode** panel, click **Edit**.

7 In the **Lockdown Mode** dialog box, select the **Normal** radio button, and click **OK**.

8 Repeat this procedure and enable normal lockdown mode for all remaining hosts in the data center.

Note Lockdown Mode settings are not part of Host Profiles and must be manually enabled on all hosts.

Deploy and Configure the Shared Edge and Compute Cluster NSX Instance in Region A

Deploy and configure the NSX instance for the shared edge and compute cluster in Region A.

Procedure

1. Deploy the NSX Manager for the Shared Edge and Compute Cluster NSX Instance in Region A

   You must first deploy the NSX Manager virtual appliance. After the NSX Manager is successfully deployed you must connect it to the Compute vCenter Server instance.

2. Deploy the NSX Controllers for the Shared Edge and Compute Cluster NSX Instance in Region A

   After the NSX Manager is successfully connected to the Compute vCenter Server, you must promote it to the primary role and deploy the three NSX Controller nodes that form the NSX Controller cluster.

3. Prepare the ESXi Hosts in the Shared Edge and Compute Cluster for NSX in Region A

   You must install the NSX kernel modules on the compute and edge clusters ESXi hosts so that you are able to use NSX.

4. Configure the NSX Logical Network for the Shared Edge and Compute Clusters in Region A

   After all deployment tasks are ready, configure the NSX logical network.

5. Update the Host Profile for the Compute Cluster in Region A

   After an authorized change is made to a host the Host Profile must be updated to reflect the changes..

6. Configure NSX Dynamic Routing in the Shared Edge and Compute Cluster in Region A

   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 compute and edge clusters, deploying two NSX Edge devices and a Universal Distributed Logical Router (UDLR).

7. Test the Shared Edge and Compute Cluster NSX Configuration in Region A

   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.

Deploy the NSX Manager for the Shared Edge and Compute Cluster NSX Instance in Region A

You must first deploy the NSX Manager virtual appliance. After the NSX Manager is successfully deployed you must connect it to the Compute vCenter Server instance.

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 Open the **Deploy OVF Template** wizard.

   a In the **Navigator**, expand the entire **mgmt01vc01.sfo01.rainpole.local** tree.

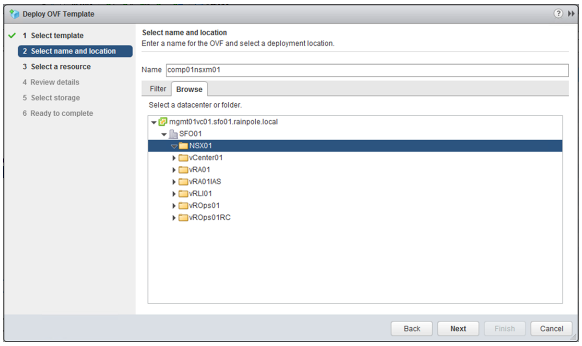
   b Right-click the **SFO01-Mgmt01** cluster, and click **Deploy OVF Template**.

3 Use the **Deploy OVF Template** wizard to deploy the NSX Manager virtual appliance.

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

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

Setting	Value
Name	comp01nsxm01.sfo01
Folder or Datacenter	NSX01



Deploy OVF Template

Select name and location

Enter a name for the OVF and select a deployment location.

Name comp01nsxm01

Select a datacenter or folder.

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

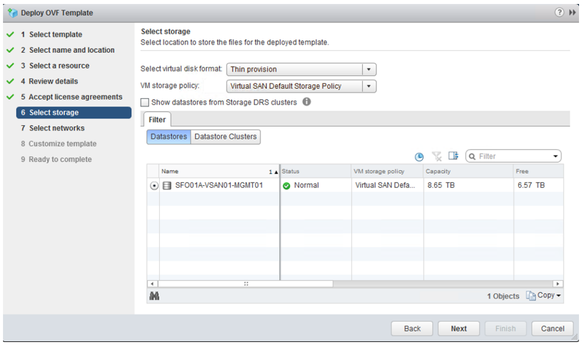
Setting	Value
Datacenter	SFO01
Cluster	SFO01-Mgmt01

   d On the **Review details** page, review the **extra configuration option** check box, and click **Next**.

   e On the **Accept License Agreements** page, click **Accept**, and click **Next**.

f On the **Select storage** page, enter the following settings, and click **Next**

Setting	Value
Select virtual disk format	Thin Provision
VM Storage Policy	vSAN Default Storage Policy
Datastore	SFO01A-VSAN01-MGMT01



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 storage
Select location to store the files for the deployed template.

Select virtual disk format: Thin provision
VM storage policy: Virtual SAN Default Storage Policy
□ Show datastores from Storage DRS clusters

Datastores | Datastore Clusters

Name	Status	VM storage policy	Capacity	Free
● SFO01A-VSAN01-MGMT01	✓ Normal	Virtual SAN Defa...	8.65 TB	6.57 TB

1 Objects

g On the **Select networks** page, Under **Destination Network**,select **vDS-Mgmt-Management**, and click **Next**.

h On the **Customize template** page, expand the different options, enter the following settings, and click **Next**.

Setting	Value
DNS Server List	172.16.11.5,172.16.11.4
Domain Search List	sfo01.rainpole.local
Default IPv4 Gateway	172.16.11.253
Hostname	comp01nsxm01.sfo01.rainpole.local
Network 1 IPv4 Address	172.16.11.66
Network 1 Netmask	255.255.255.0
Enable SSH	Selected
NTP Server List	■ ntp.sfo01.rainpole.local ■ ntp.lax01.rainpole.local
CLI "admin" User Password / enter	*compnsx_admin_password*
CLI "admin" User Password / confirm	*compnsx_admin_password*
CLI Privilege Mode Password / enter	*compnsx_priviledge_password*
CLI Privilege Mode Password / confirm	*compnsx_priviledge_password*

i On the **Ready to complete page**, click **Finish**.

j In the **Navigator**, expand the **mgmt01vc01.sfo01.rainpole.local** control tree,select the **comp01nsxm01** virtual machine, and click the **Power on** button.

4 Connect the NSX Manager to the Compute vCenter Server.

   a Open a Web browser and go to **`https://comp01nsxm01.sfo01.rainpole.local`**

   b Log in using the following credentials.

Setting	Value
User name	admin
Password	*compnsx_admin_password*

   c Click **Manage vCenter Registration**.

   d Under **Lookup Service**, click the **Edit** button.

   e In the **Lookup Service** dialog box, enter the following settings, and click **OK**.

Setting	Value
Lookup Service IP	sfo01psc01.sfo01.rainpole.local
Lookup Service Port	443
SSO Administrator User Name	administrator@vsphere.local
Password	*vsphere_admin_password*

   f In the **Trust Certificate?** dialog box, click **Yes**.

   g Under **vCenter Server**, click the **Edit** button.

   h In the **vCenter Server** dialog box, enter the following settings, and click **OK**.

Setting	Value
vCenter Server	comp01vc01.sfo01.rainpole.local
vCenter User Name	svc-nsxmanager@rainpole.local
Password	*svc-nsxmanager_password*

   i In the **Trust Certificate?** dialog box, click **Yes**.

   j Wait until the **Status** indicators for the Lookup Service and vCenter Server change to `connected`.

5 Log out from the vCenter Server session in the vSphere Web Client.

6 Log in to the Management 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	svc-nsxmanager@rainpole.local
Password	*svc-nsxmanager_password*

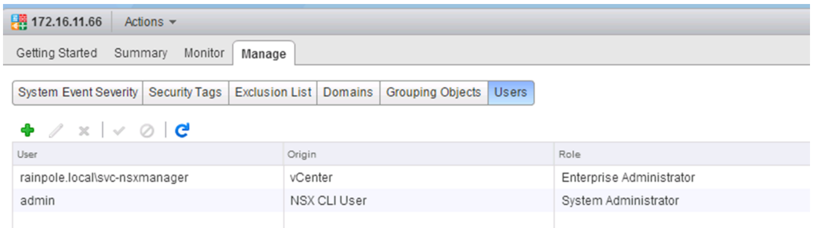
7 Assign the administrator@vsphere.local account access to NSX.

a In the **Navigator**, click **Network & Security**.

b Select **NSX Managers**.

c Select **172.16.11.66** from the tree control.

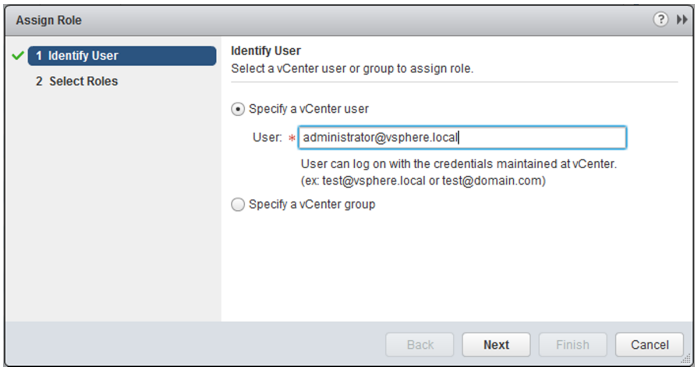
d Click the **Manage** tab, then click **Users**.



User	Origin	Role
rainpole.local\svc-nsxmanager	vCenter	Enterprise Administrator
admin	NSX CLI User	System Administrator

e Click the **Add** icon.

f On the **Identify User** page enter`administrator@vsphere.local` in the **User** text box and click **Next**.



Identify User

Select a vCenter user or group to assign role.

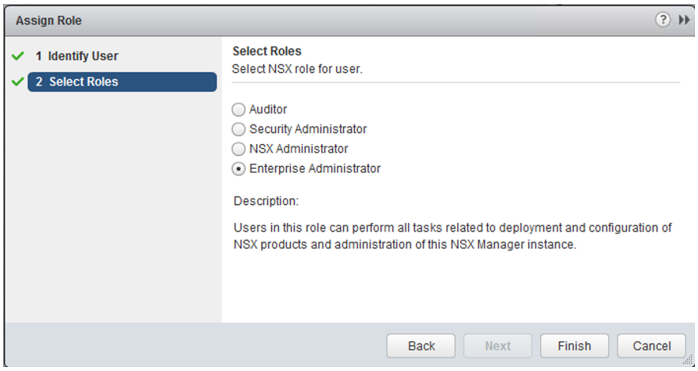
● Specify a vCenter user

User: * administrator@vsphere.local

User can log on with the credentials maintained at vCenter.
(ex: test@vsphere.local or test@domain.com)

○ Specify a vCenter group

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



Select Roles

Select NSX role for user.

○ Auditor
○ Security Administrator
○ NSX Administrator
● Enterprise Administrator

Description:

Users in this role can perform all tasks related to deployment and configuration of NSX products and administration of this NSX Manager instance.

8 Log out from the vCenter Server session in the vSphere Web Client.

Deploy the NSX Controllers for the Shared Edge and Compute Cluster NSX Instance in Region A

After the NSX Manager is successfully connected to the Compute vCenter Server, you must promote it to the primary role and deploy the three NSX Controller nodes that form the NSX Controller cluster.

It is important to deploy every node only after the previous one is successfully deployed.

To complete this procedure you must configure the datastore for the shared edge and compute cluster in Region A.

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 with the following credentials.

Setting	Value
User name	administrator@vsphere.local
Password	*vsphere_admin_password*

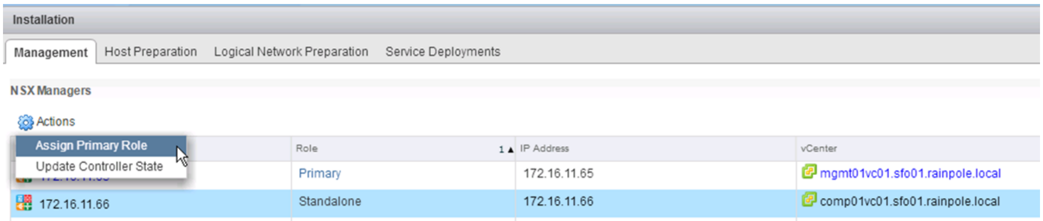
2 Promote the NSX Manager to the primary role.

   a Under **Inventories**, click **Networking & Security**.

   b In the **Navigator**, click **Installation**.

   c On the **Management** tab, click the **172.16.11.66** instance.

   d Click the **Actions** menu and click **Assign Primary Role**.



	Role	IP Address	vCenter
	Primary	172.16.11.65	mgmt01vc01.sfo01.rainpole.local
172.16.11.66	Standalone	172.16.11.66	comp01vc01.sfo01.rainpole.local

   e In the Assign Primary Role confirmation dialog box, click **Yes**.

3 Configure an IP pool for the NSX Controller Cluster.

   a In the **Navigator**, click **NSX Managers**.

   b Under **NSX Managers**, click the **172.16.11.66** instance.

c Click the **Manage** tab, click **Grouping Objects**, click **IP Pools**, and click the **Add New IP Pool** icon.

d In the **Add Static IP Pool** dialog box, enter the following settings and click **OK**.

Setting	Value
Name	Comp01-NSXC01
Gateway	172.16.31.253
Prefix Length	24
Primary DNS	172.16.11.5
Secondary DNS	172.16.11.4
DNS Suffix	sfo01.rainpole.local
Static IP Pool	172.16.31.118-172.16.31.120

4 Deploy the NSX Controller cluster.

a In the **Navigator**, click **Networking & Security** to go back, and click **Installation**.

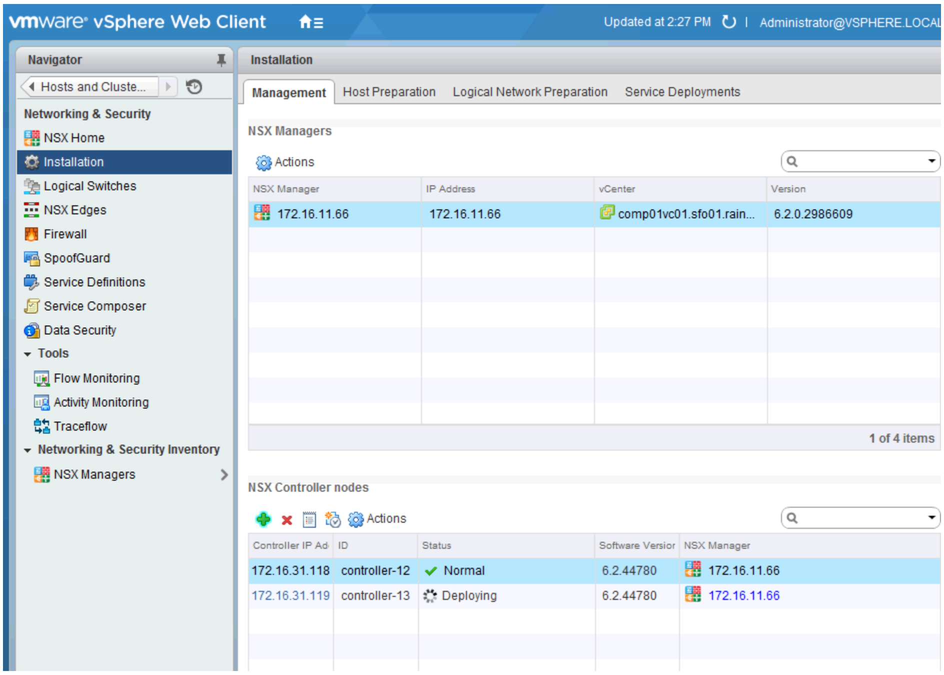
b Under **NSX Controller nodes**, click the **Add** icon to deploy three NSX Controller nodes with the same configuration.

c In the **Add Controller** page, enter the following settings and click **OK**.

> **Note** You may only configure the password during the deployment of the first controller. The other controllers will use the same password.

Setting	Value
Name	nsx-controller-comp-01
NSX Manager	172.16.11.66
Datacenter	SFO01
Cluster/Resource Pool	SDDC-EdgeRP01
Datastore	*sfo01_shared_edge_and_compute_datastore*
Connected To	vDS-Comp01-Management
IP Pool	Comp01-NSXC01
Password	*compnsx_controllers_password*
Confirm Password	*compnsx_controllers_password*

d After the **Status** of the controller node changes to `Connected`, repeat the step and deploy the remaining two NSX Controller nodes, with the same configuration to form the controller cluster.



NSX Managers

NSX Manager	IP Address	vCenter	Version
172.16.11.66	172.16.11.66	comp01vc01.sfo01.rain...	6.2.0.2986609

1 of 4 items

NSX Controller nodes

Controller IP Ad	ID	Status	Software Versior	NSX Manager
172.16.31.118	controller-12	✓ Normal	6.2.44780	172.16.11.66
172.16.31.119	controller-13	Deploying	6.2.44780	172.16.11.66

5 Configure DRS affinity rules for the NSX Controllers.

a Go back to the **Home** page.

b In the **Navigator**, click **Hosts and Clusters**, and expand the comp01vc01.sfo01.rainpole.local tree.

c Select the **SFO01-Comp01** cluster, and click the **Manage** tab.

d Under **Configuration**, click **VM/Host Rules**.

e Under **VM/Host Rules**, click **Add**.

f In the **SFO01-Comp01 - 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 **three NSX Controller VMs** and click **OK**.

h In the **SFO01-Comp01 - Create VM/Host Rule** dialog box click **OK** and click **OK**.

Prepare the ESXi Hosts in the Shared Edge and Compute Cluster for NSX in Region A

You must install the NSX kernel modules on the compute and edge clusters ESXi hosts so that you are able to use NSX.

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*

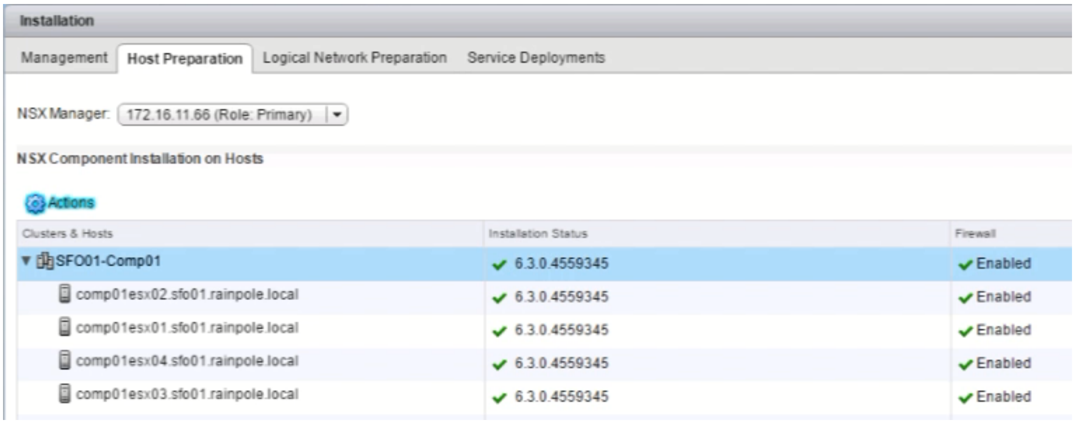
2 Install the NSX kernel modules on the shared edge and compute cluster ESXi hosts.

a In the **Navigator**, click **Networking & Security**, click **Installation**, and click the **Host Preparation** tab.

b Select **172.16.11.66** from the **NSX Manager** drop-down menu.

c Under **Installation Status**, click **Install** for the SFO01-Comp01 cluster and click **Yes** in the confirmation dialog box.

3 Verify that the Installation Status column displays the NSX version for all hosts in the cluster to confirm the successful installation of the NSX kernel modules.



NSX Manager: 172.16.11.66 (Role: Primary)

NSX Component Installation on Hosts

Clusters & Hosts	Installation Status	Firewall
SFO01-Comp01	✓ 6.3.0.4559345	✓ Enabled
comp01esx02.sfo01.rainpole.local	✓ 6.3.0.4559345	✓ Enabled
comp01esx01.sfo01.rainpole.local	✓ 6.3.0.4559345	✓ Enabled
comp01esx04.sfo01.rainpole.local	✓ 6.3.0.4559345	✓ Enabled
comp01esx03.sfo01.rainpole.local	✓ 6.3.0.4559345	✓ Enabled

Configure the NSX Logical Network for the Shared Edge and Compute Clusters in Region A

After all deployment tasks are ready, configure the NSX logical network.

Complete this process in three main steps:

- 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://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 Configure the Segment ID allocation.

   a In the **Navigator**, click **Networking & Security**.

   b Click **Installation**, click **Logical Network Preparation**, and click **Segment ID**.

c Select **172.16.11.66** from the **NSX Manager** drop-down menu.

d Click **Edit**, enter the following settings, and click **OK**.

Setting	Value
Segment ID pool	5300-9000
Enable Multicast addressing	Selected
Multicast addresses	239.3.0.0-239.3.255.255
Universal Segment ID Pool	20000-29000
Enable Universal Multicast addressing	Selected
Universal Multicast addresses	239.4.0.0-239.4.255.255

3 Configure the VXLAN networking.

a Click the **Host Preparation** tab.

b Under *VXLAN*, click **Not Configured** on the row labeled **SFO01-Comp01**, enter the following settings, and click **OK**.

Setting	Value
Switch	vDS-Comp01
VLAN	1634
MTU	9000
VMKNic IP Addressing	Use DHCP
VMKNic Teaming Policy	Load Balance - SRCID
VTEP	2

4 Configure the Universal transport zone.

a In the **Navigator**, click the **Logical Network Preparation** tab and click **Transport Zones**.

b Click the **Add New Transport zone** icon, enter the following settings, and click **OK**.

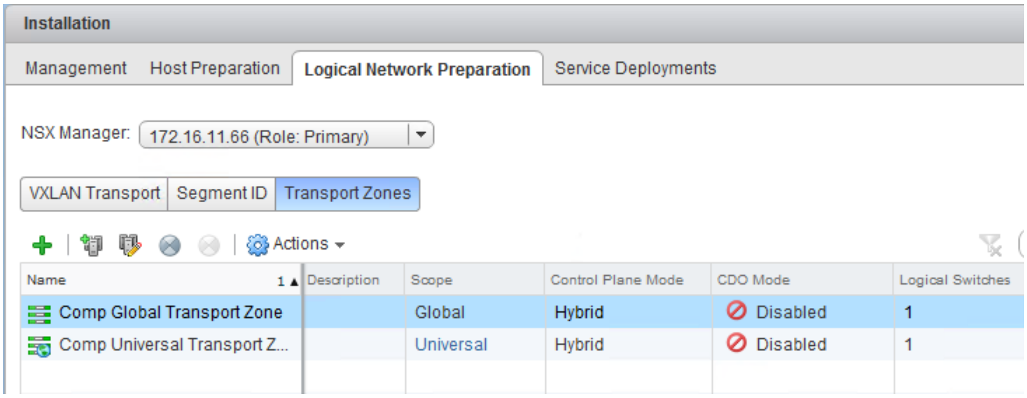
Setting	Value
Mark this object for Universal Synchronization	Selected
Name	Comp Universal Transport Zone
Replication mode	Hybrid
Select clusters part of the Transport Zone	SFO01-Comp01

5 Configure the Global transport zone.

   a In the **Navigator**, click the **Logical Network Preparation** tab and click **Transport Zones**.

   b Click the **Add New Transport zone** icon, enter the following settings, and click **OK**.

Setting	Value
Name	Comp Global Transport Zone
Replication mode	Hybrid
Select clusters part of the Transport Zone	SFO01-Comp01



Installation

NSX Manager: 172.16.11.66 (Role: Primary)

Name	Description	Scope	Control Plane Mode	CDO Mode	Logical Switches
Comp Global Transport Zone		Global	Hybrid	⊘ Disabled	1
Comp Universal Transport Z...		Universal	Hybrid	⊘ Disabled	1

Update the Host Profile for the Compute Cluster in Region A

After an authorized change is made to a host the Host Profile must be updated to reflect the changes..

Procedure

1 Log in to the Management 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 Update the Host Profile to the compute cluster.

   a In the **Navigator**, select **Policies and Profiles**

   b Click on **Host Profiles** then right click on **SFO01-Comp01** and select **Copy Settings from Host.**

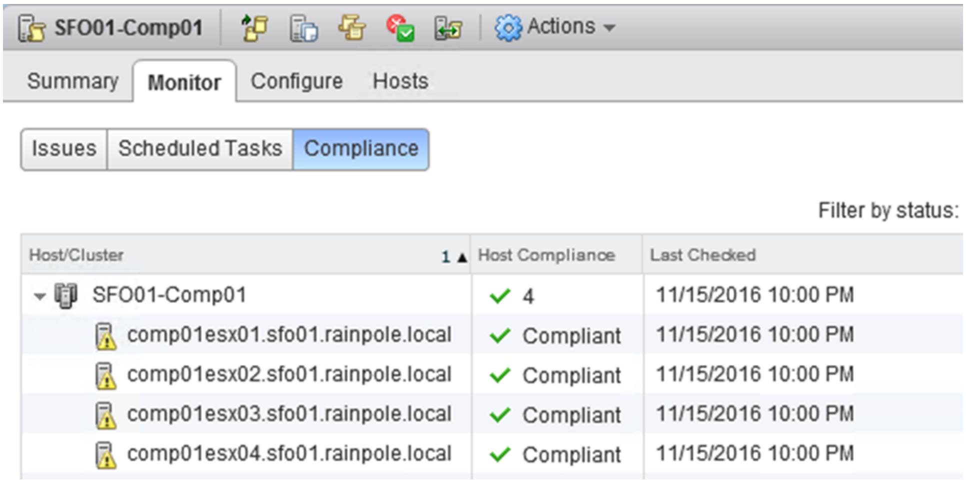
   c Select **comp01esx01.sfo01.rainpole.local**, click **OK**.

3 Verify compliance for the hosts in the compute cluster.

   a Click the **Monitor** tab and click **Compliance**.

   b Select **SFO01-Comp01** and click the **Check Host Profile Complaince** button.

   All hosts should show the status `Compliant`



Host/Cluster 1 ▲	Host Compliance	Last Checked
SFO01-Comp01	✓ 4	11/15/2016 10:00 PM
comp01esx01.sfo01.rainpole.local	✓ Compliant	11/15/2016 10:00 PM
comp01esx02.sfo01.rainpole.local	✓ Compliant	11/15/2016 10:00 PM
comp01esx03.sfo01.rainpole.local	✓ Compliant	11/15/2016 10:00 PM
comp01esx04.sfo01.rainpole.local	✓ Compliant	11/15/2016 10:00 PM

Configure NSX Dynamic Routing in the Shared Edge and Compute Cluster in Region A

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 compute and edge clusters, deploying two NSX Edge devices and a Universal Distributed Logical Router (UDLR).

Procedure

1 Create a Universal Logical Switch for Use as the Transit Network in the Shared Edge and Compute Cluster in Region A

   Create universal and global transit logical switches for use as the transit networks in the cluster.

2 Deploy NSX Edge Devices for North-South Routing in the Shared Edge and Compute Cluster in Region A

   Deploy NSX Edge Devices for North-South routing in the shared edge and compute cluster.

3 Disable the Firewall Service in the Shared Edge and Compute Cluster in Region A

   Disable the firewall of the two NSX Edge services gateways.

4 Enable and Configure Routing in the Shared Edge and Compute Cluster in Region A

   Enable the Border Gateway Protocol (BGP) to exchange routing information between the NSX Edge services gateways.

5 Verify Peering of Upstream Switches and Establishment of BGP in the Shared Edge and Compute Cluster in Region A

The NSX Edge devices need to establish a connection to each of it's 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 Universal Distributed Logical Router in the Shared Edge and Compute Cluster in Region A

Deploy the universal distributed logical routers (UDLR).

7 Configure Universal Distributed Logical Router for Dynamic Routing in Shared Edge and Compute Cluster in Region A

Configure the universal distributed logical router (UDLR) in the shared edge and compute cluster to use dynamic routing.

8 Verify Establishment of BGP for the Universal Distributed Logical Router in the Shared Edge and Compute Cluster in Region A

The universal distributed logical router (UDLR) needs to establish a connection to Edge Services Gateway before BGP updates can be exchanged. Verify that the UDLR is successfully peering, and that BGP routing has been established.

9 Deploy the Distributed Logical Router in the Shared Edge and Compute Cluster in Region A

Deploy the distributed logical routers (DLR).

10 Configure Distributed Logical Router for Dynamic Routing in Shared Edge and Compute Cluster in Region A

Configure the distributed logical router (DLR) in the shared edge and compute cluster to use dynamic routing.

11 Verify Establishment of BGP for the Distributed Logical Router in the Shared Edge and Compute Cluster in Region A

The distributed logical router (DLR) needs to establish a connection to Edge Services Gateway before BGP updates can be exchanged. Verify that the DLR is successfully peering, and that BGP routing has been established.

Create a Universal Logical Switch for Use as the Transit Network in the Shared Edge and Compute Cluster in Region A

Create universal and global transit logical switches for use as the transit networks in the cluster.

Procedure

1 Log in to the Management 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 Under **Inventories**, click **Networking & Security**.

3 In the **Navigator**, click **Logical Switches**.

4 Select **172.16.11.66** from the **NSX Manager** drop-down menu and click the **Add** icon.

5 In the **New Logical Switch** dialog box, enter the following settings and click **OK**.

Setting	Value
Name	Universal Transit Network
Transport Zone	Comp Universal Transport Zone
Replication Mode	Hybrid

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

Setting	Value
Name	Global Transit Network
Transport Zone	Comp Global Transport Zone
Replication Mode	Hybrid

Deploy NSX Edge Devices for North-South Routing in the Shared Edge and Compute Cluster in Region A

Deploy NSX Edge Devices for North-South routing in the shared edge and compute cluster.

Perform this procedure two times to deploy two NSX Edge devices: SFOCOMP-ESG01 and SFOCOMP-ESG02.

Table 2‑10. NSX Edge Devices

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

Table 2-11. NSX Edge Interfaces Settings

Interface	Primary IP Address SFOCOMP-ESG01	Primary IP Address SFOCOMP-ESG02
Uplink01	172.16.35.2	172.16.35.3
Uplink02	172.27.13.3	172.27.13.2
SFOCOMP-UDLR01	192.168.100.1	192.168.100.2
SFOCOMP-DLR01	192.168.101.1	192.168.101.2

To complete this procedure use the datastore that you configured for the shared edge and compute cluster.

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 Use the following credentials to log in.

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 **172.16.11.66** 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**.

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

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

Setting	Value
User Name	admin
Password	*edge_admin_password*
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	SDDC-EdgeRP01
Datastore	*sfo01_shared_edge_and_compute_datastore*

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-Comp01-Uplink01
Connectivity Status	Connected
Primary IP Address	172.16.35.2
Subnet Prefix Length	24
MTU	9000
Send ICMP Redirect	Selected

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

Setting	Value
Name	Uplink02
Type	Uplink
Connected To	vDS-Comp01-Uplink02
Connectivity Status	Connected
Primary IP Address	172.27.13.3
Subnet Prefix Length	24
MTU	9000
Send ICMP Redirect	Selected

g Click the **Add** icon to configure the UDLR interface, enter the following settings, click **OK**, and click **Next**.

Setting	Value
Name	SFOCOMP-UDLR01
Type	Internal
Connected To	Universal Transit Network
Connectivity Status	Connected
Primary IP Address	192.168.100.1
Subnet Prefix Length	24
MTU	9000
Send ICMP Redirect	Selected

h Click the **Add** icon to configure the DLR interface, enter the following settings, click **OK**, and click **Next**.

Setting	Value
Name	SFOCOMP-DLR01
Type	Internal
Connected To	Global Transit Network
Connectivity Status	Connected
Primary IP Address	192.168.101.1
Subnet Prefix Length	24
MTU	9000
Send ICMP Redirect	Selected

i On the **Default gateway settings** page, deselect the **Configure Default Gateway** check box and click **Next**.

j On the **Firewall and HA** page click **Next**.

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

6 Repeat this procedure to configure another NSX edge by using the settings for the second NSX Edge device.

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 **comp01vc01.sfo01.rainpole.local** tree.

c Select the **SFO01-Comp01** cluster, and click the **Configure** tab.

d Under **Configuration**, click **VM/Host Rules**.

e Click **Add**.

f In the **SFO01-Comp01 - 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 NSX ESG's just deployed and click **OK**.

h In the **SFO01-Comp01 - Create VM/Host Rule** dialog box, click **OK**.

Disable the Firewall Service in the Shared Edge and Compute Cluster in Region A

Disable the firewall of the two NSX Edge services gateways.

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

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 Under **Inventories**, click **Networking & Security**.

3 In the **Navigator**, click **NSX Edges**.

4 Select **172.16.11.66** from the **NSX Manager** drop-down menu.

5 Double-click the **SFOCOMP-ESG01** NSX Edge device.

6 Click the **Manage** tab and click **Firewall**.

7 On the **Firewall** page, click the **Disable** button.

8 Click **Publish changes**.

9 Repeat this procedure for the NSX Edge services gateway SFOCOMP-ESG02.

Enable and Configure Routing in the Shared Edge and Compute Cluster in Region A

Enable the Border Gateway Protocol (BGP) to exchange routing information between the NSX Edge services gateways.

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

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 Under **Inventories**, click **Networking & Security**.

3 In the **Navigator**, click **NSX Edges**.

4 Select **172.16.11.66** from the **NSX Manager** drop-down menu.

5 Double-click the **SFOCOMP-ESG01** NSX Edge device.

6 Click the **Manage** tab and click **Routing**.

7 Configure settings on the **Global Configuration** page.

   a Click the **Enable** button for ECMP.

   b To configure dynamic routing, click the **Edit** button next to Dynamic Routing Configuration.

   c Select **Uplink01** as the Router ID and click **OK**.

   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	*UDLR_Compute_Workload_Subnet*
Next Hop	192.168.100.3
Interface	SFOCOMP-UDLR01
MTU	9000
Admin Distance	210

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

b Click the **Add** icon, enter the following settings, and click **OK**.

Setting	Value
Network	*DLR_Compute_Workload_Subnet*
Next Hop	192.168.101.3
Interface	SFOCOMP-DLR01
MTU	9000
Admin Distance	210

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

c 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**.

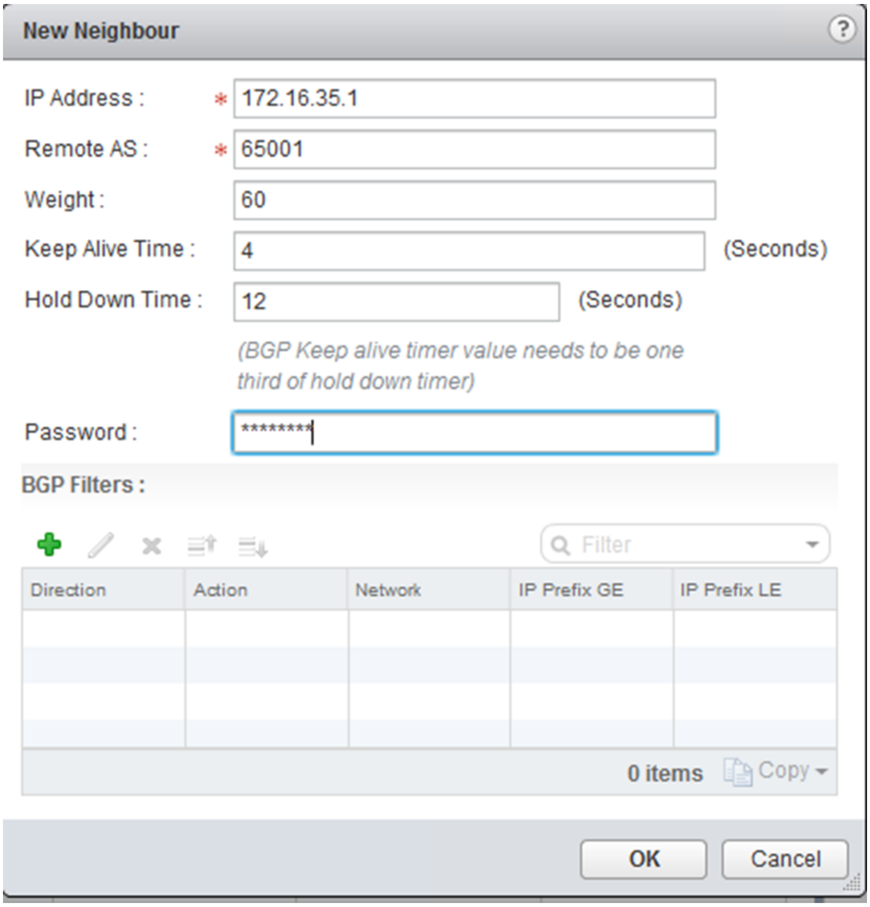
Setting	Value
Enable BGP	Selected
Enable Graceful Restart	Selected
Enable Default Originate	Deselected
Local AS	65000

b On the **BGP** page, 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 and click **OK**.

Setting	Value
IP Address	172.16.35.1
Remote AS	65001
Weight	60
Keep Alive Time	4
Hold Down Time	12
Password	*BGP_password*



New Neighbour

IP Address : * 172.16.35.1

Remote AS : * 65001

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

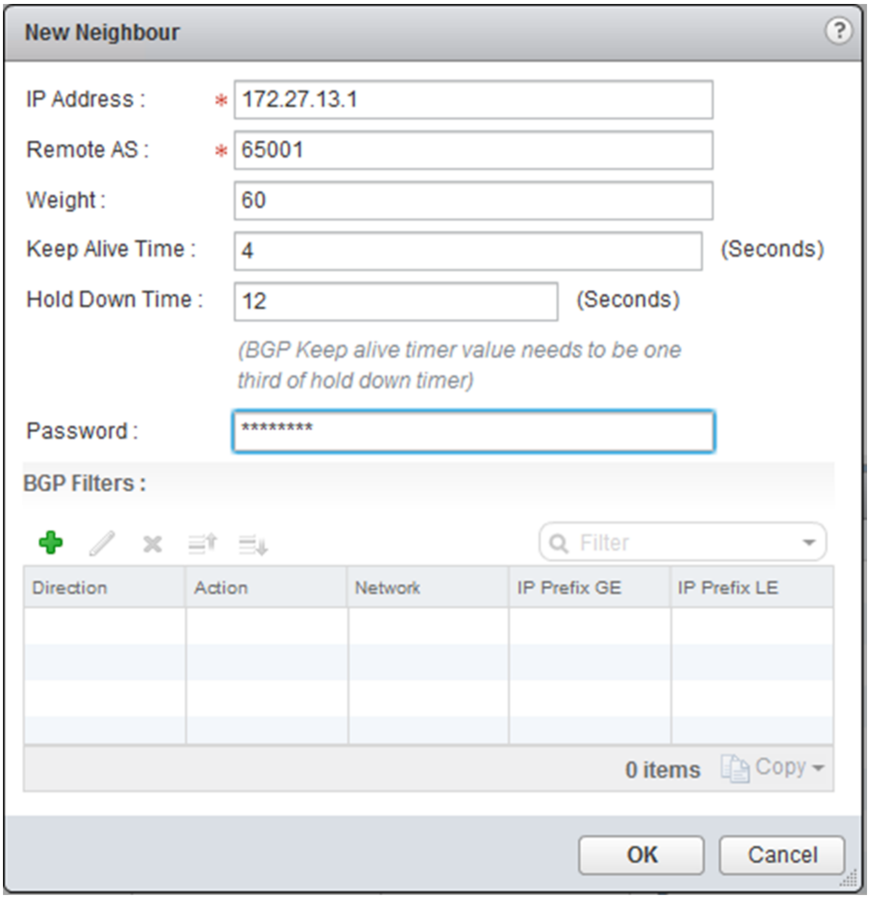
d Click the **Add** icon to add another Neighbor.

The **New Neighbor** dialog box appears.

e Add the second Top of Rack switch, whose IP address is `172.27.13.1`.

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

Setting	Value
IP Address	172.27.13.1
Remote AS	65001
Weight	60
Keep Alive Time	4
Hold Down Time	12
Password	*BGP_password*



New Neighbour

IP Address : * 172.27.13.1

Remote AS : * 65001

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

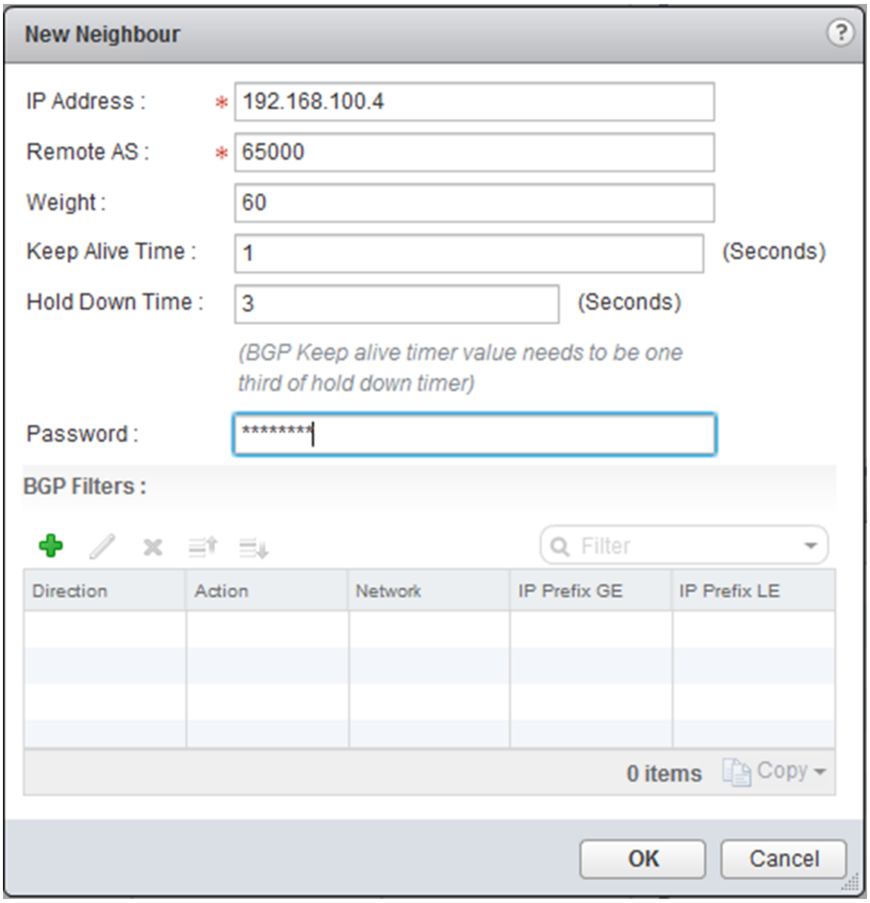
g Click the **Add** icon to add another Neighbor.

The **New Neighbor** dialog box appears.

h Configure the universal distributed logical router (UDLR) as a neighbor.

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

Setting	Value
IP Address	192.168.100.4
Remote AS	65000
Weight	60
Keep Alive Time	1
Hold Down Time	3
Password	*BGP_password*



New Neighbour

IP Address : * 192.168.100.4

Remote AS : * 65000

Weight : 60

Keep Alive Time : 1 (Seconds)

Hold Down Time : 3 (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

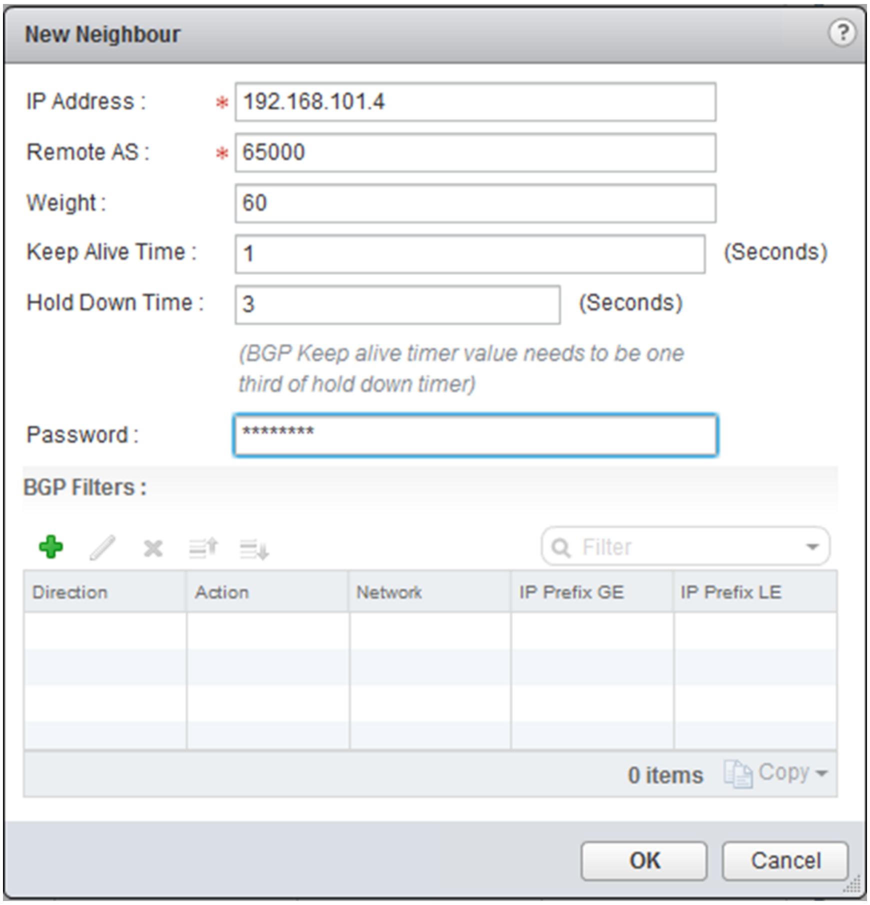
j Click the **Add** icon to add another Neighbor.

The **New Neighbor** dialog box appears.

k Configure the distributed logical router (DLR) as a neighbor.

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

Setting	Value
IP Address	192.168.101.4
Remote AS	65000
Weight	60
Keep Alive Time	1
Hold Down Time	3
Password	*BGP_password*



New Neighbour

IP Address : * 192.168.101.4

Remote AS : * 65000

Weight : 60

Keep Alive Time : 1 (Seconds)

Hold Down Time : 3 (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

m Click **Publish Changes**.

The four neighbors you added appear in the Neighbors table.

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

a On the **Route Redistribution** page, click the **Edit** button.

b In the **Change redistribution settings** dialog box, select the **BGP** check box and click **OK**.

c Click the **Add** icon for Route Redistribution Table.

d 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 the **Publish Changes** button.

The route redistribution configuration appears in the **Route Redistribution** table. Confirm that the configuration values you entered are correct.

11 Repeat this procedure for the NSX Edge device SFOCOMP-ESG02.

Verify Peering of Upstream Switches and Establishment of BGP in the Shared Edge and Compute Cluster in Region A

The NSX Edge devices need to establish a connection to each of it's 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: SFOCOMP-ESG01 and SFOCOMP-ESG02.

Procedure

1 Log in to the NSX Edge device using a Secure Shell (SSH) client.

a Open an SSH connection to the SFOCOMP-ESG01 NSX Edge device.

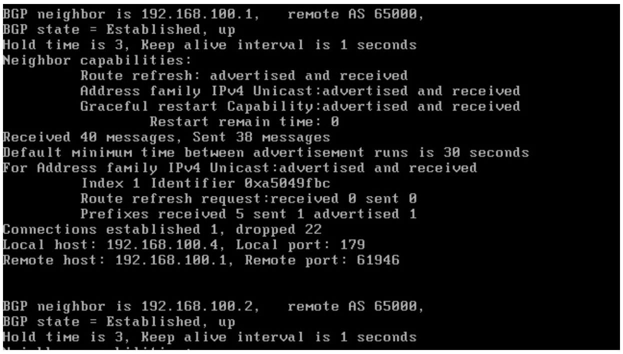
b Log in using the following credentials.

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.

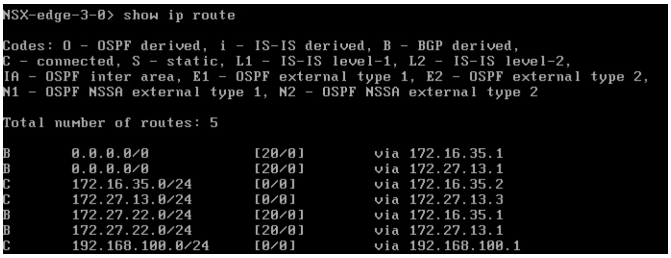
Note You have not yet created the universal distributed logical router or the distributed logical router, as such they will not display the `Established, UP` status message.



```
BGP neighbor is 192.168.100.1,   remote AS 65000,
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 40 messages, Sent 38 messages
Default minimum time between advertisement runs is 30 seconds
For Address family IPv4 Unicast:advertised and received
         Index 1 Identifier 0xa5049fbc
         Route refresh request:received 0 sent 0
         Prefixes received 5 sent 1 advertised 1
Connections established 1, dropped 22
Local host: 192.168.100.4, Local port: 179
Remote host: 192.168.100.1, Remote port: 61946


BGP neighbor is 192.168.100.2,   remote AS 65000,
BGP state = Established, up
Hold time is 3, Keep alive interval is 1 seconds
```

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` and `172.27.22.0/24`. You can identify BGP networks by the letter `B` in the left-side column. Lines beginning with `C` (connected) have only a single route.



```
NSX-edge-3-0> show ip 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: 5

B       0.0.0.0/0            [20/0]        via 172.16.35.1
B       0.0.0.0/0            [20/0]        via 172.27.13.1
C       172.16.35.0/24       [0/0]         via 172.16.35.2
C       172.27.13.0/24       [0/0]         via 172.27.13.3
B       172.27.22.0/24       [20/0]        via 172.16.35.1
B       172.27.22.0/24       [20/0]        via 172.27.13.1
C       192.168.100.0/24     [0/0]         via 192.168.100.1
```

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

Deploy the Universal Distributed Logical Router in the Shared Edge and Compute Cluster in Region A

Deploy the universal distributed logical routers (UDLR).

Procedure

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 Under **Inventories**, click **Networking & Security**.

3 In the **Navigator**, click **NSX Edges**.

4 Select **172.16.11.66** from the **NSX Manager** drop-down menu.

5 Click the **Add** icon to create a new UDLR,

The **New NSX Edge** wizard appears.

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

Setting	Value
Universal Logical (Distributed) Router	Selected
Name	SFOCOMP-UDLR01
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	*udlr_admin_password*
Enable SSH access	Selected
Edge Control Level logging	INFO

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

The A**dd 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	SDDC-EdgeRP01
Datastore	*sfo01_shared_edge_and_compute_datastore*
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
Cluster/Resource Pool	SDDC-EdgeRP01
Datastore	*sfo01_shared_edge_and_compute_datastore*
Folder	NSX01

12 On the **Configure interfaces** page, under **HA Interface Configuration**, click **Select** and connect to **vDS-Comp01-Management**.

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

   a Click the **Add** icon.

Setting	Value
Primary IP Address	1.2.1.1
Subnet Prefix Length	24

   b Enter the following settings in the **Add Interface** dialog box, and click **OK**.

   The **Add Interface** dialog box appears.

Setting	Value
Name	Uplink
Type	Uplink
Connected To	Universal Transit Network
Connectivity Status	Connected
Primary IP Address	192.168.100.3
Subnet Prefix Length	24
MTU	9000

14 On the **Default gateway settings** page, deselect **Configure Default Gateway** and click **Next**.

15 On the **Ready to complete** page, click **Finish**.

Configure Universal Distributed Logical Router for Dynamic Routing in Shared Edge and Compute Cluster in Region A

Configure the universal distributed logical router (UDLR) in the shared edge and compute cluster to use dynamic routing.

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 Under **Inventories**, click **Networking & Security**.

3 In the **Navigator**, click **NSX Edges**.

4 Select **172.16.11.66** from the **NSX Manager** drop-down menu.

5 Enable HA logging.

   a Double-click the device labeled **SFOCOMP-UDLR01**.

   b Click the **Manage** tab and click the **Settings** tab.

   c Click **Change** in the **HA Configuration** window.

   d Select the `Enable Logging` checkbox and click **OK**.

6 Configure the routing for the Universal Distributed Logical Router.

   a Double-click **SFOCOMP-UDLR01**.

   b Click the **Manage** tab and click **Routing**.

   c On the **Global Configuration** page, perform the following configuration steps.

   d Click the **Edit** button under **Routing Configuration**, select **Enable ECMP**, and click **OK**.

   e Click the **Edit** button under **Dynamic Routing Configuration**, select **Uplink** as the Router ID, and click **OK**.

   f Click **Publish Changes**.

7 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	65000

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

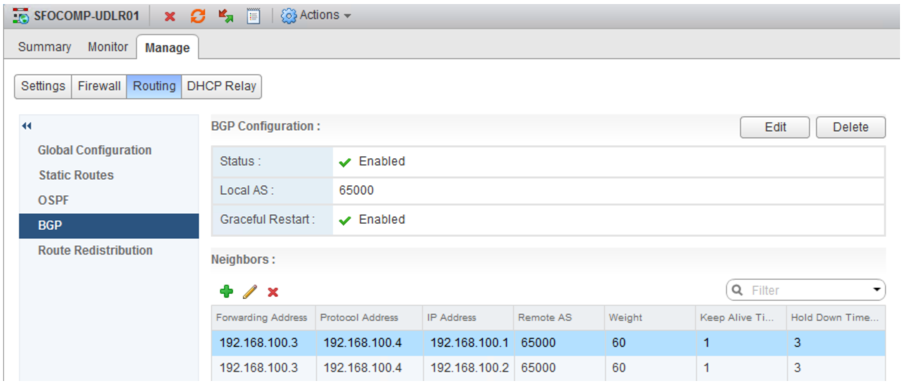
   The **New Neighbor** dialog box appears.

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

You repeat this step two times to configure the UDLR for both NSX Edge devices: SFOCOMP-ESG01 and SFOCOMP-ESG02.

Setting	SFOCOMP-ESG01 Value	SFOCOMP-ESG02 Value
IP Address	192.168.100.1	192.168.100.2
Forwarding Address	192.168.100.3	192.168.100.3
Protocol Address	192.168.100.4	192.168.100.4
Remote AS	65000	65000
Weight	60	60
Keep Alive Time	1	1
Hold Down Time	3	3
Password	*bgp_password*	*bgp_password*

e Click **Publish Changes**.



BGP Configuration :

Status :	✓ Enabled
Local AS :	65000
Graceful Restart :	✓ Enabled

Neighbors :

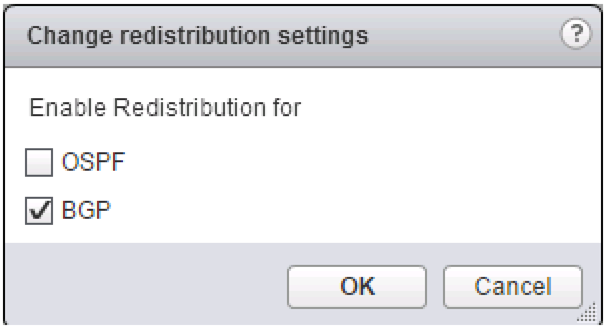
Forwarding Address	Protocol Address	IP Address	Remote AS	Weight	Keep Alive Ti...	Hold Down Time...
192.168.100.3	192.168.100.4	192.168.100.1	65000	60	1	3
192.168.100.3	192.168.100.4	192.168.100.2	65000	60	1	3

8 On the left, select **Route Redistribution** to configure it.

a Click the *Edit* button.

b In the **Change redistribution settings** dialog box, enter the following settings, and click **OK**.

Setting	Value
OSPF	Deselected
BGP	Selected



Change redistribution settings

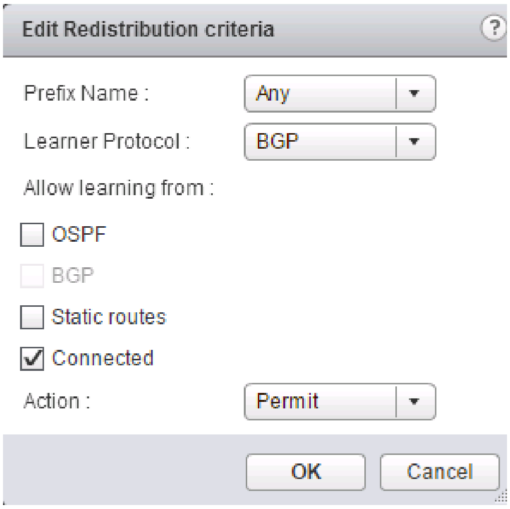
Enable Redistribution for

☐ OSPF

☑ BGP

c On the **Route Redistribution** page, select the default **OSPF** entry and click the **Edit** button.

d Select **BGP** from the **Learner Protocol** drop-down menu, and click **OK**.



Edit Redistribution criteria

Prefix Name : Any

Learner Protocol : BGP

Allow learning from :

☐ OSPF

☐ BGP

☐ Static routes

☑ Connected

Action : Permit

e Click **Publish Changes**.

Verify Establishment of BGP for the Universal Distributed Logical Router in the Shared Edge and Compute Cluster in Region A

The universal distributed logical router (UDLR) needs to establish a connection to Edge Services Gateway before BGP updates can be exchanged. Verify that the UDLR is successfully peering, and that BGP routing has been established.

Procedure

1 Log in to the SFOCOMP-UDLR01 by using a Secure Shell (SSH) client.

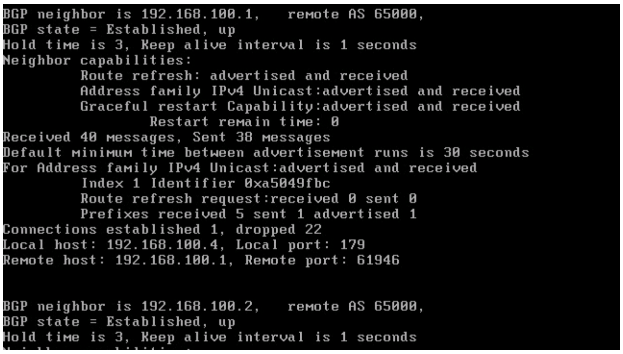
   a Open an SSH connection to SFOCOMP-UDLR01, the UDLR whose peering and BGP configuration you want to verify.

   b Log in using the following credentials.

Setting	Value
User name	admin
Password	*udlr_admin_password*

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

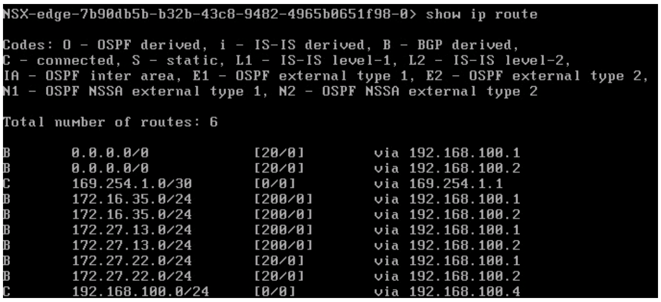
   The `BGP State` will display `Established, UP` if you have successfully peered with the Edge Service Gateway.



```
BGP neighbor is 192.168.100.1,   remote AS 65000,
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 40 messages, Sent 38 messages
Default minimum time between advertisement runs is 30 seconds
For Address family IPv4 Unicast:advertised and received
         Index 1 Identifier 0xa5049fbc
         Route refresh request:received 0 sent 0
         Prefixes received 5 sent 1 advertised 1
Connections established 1, dropped 22
Local host: 192.168.100.4, Local port: 179
Remote host: 192.168.100.1, Remote port: 61946


BGP neighbor is 192.168.100.2,   remote AS 65000,
BGP state = Established, up
Hold time is 3, Keep alive interval is 1 seconds
```

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`, `172.16.35.0/24`, `172.27.13.0/24`, and `172.27.22.0/24`. You can identify BGP networks by the letter `B` in the left-side column. Lines beginning with `C` (connected) have only a single route.



```
NSX-edge-7b90db5b-b32b-43c8-9482-4965b0651f98-0> show ip 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: 6

B       0.0.0.0/0            [20/0]        via 192.168.100.1
B       0.0.0.0/0            [20/0]        via 192.168.100.2
C       169.254.1.0/30       [0/0]         via 169.254.1.1
B       172.16.35.0/24       [200/0]       via 192.168.100.1
B       172.16.35.0/24       [200/0]       via 192.168.100.2
B       172.27.13.0/24       [200/0]       via 192.168.100.1
B       172.27.13.0/24       [200/0]       via 192.168.100.2
B       172.27.22.0/24       [20/0]        via 192.168.100.1
B       172.27.22.0/24       [20/0]        via 192.168.100.2
C       192.168.100.0/24     [0/0]         via 192.168.100.4
```

Deploy the Distributed Logical Router in the Shared Edge and Compute Cluster in Region A

Deploy the distributed logical routers (DLR).

Procedure

Procedure

1 Log in to the Compute 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 Under Inventories, click **Networking & Security**.

3 In the Navigator, click **NSX Edges**.

4 Select **172.16.11.66** 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	SFOCOMP-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	*dlr_admin_password*
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	SDDC-EdgeRP01
Datastore	*sfo01_shared_edge_and_compute_datastore*

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	SDDC-EdgeRP01
Datastore	*sfo01_shared_edge_and_compute_datastore*

12 On the **Configure interfaces** page, under **HA Interface Configuration**, click **Select** and connect to **vDS-Comp01-Management**.

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

Setting	Value
Primary IP Address	1.3.1.1
Subnet Prefix Length	24

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	Uplink
Type	Uplink
Connected To	Global Transit Network
Connectivity Status	Connected
Primary IP Address	192.168.101.3
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 Shared Edge and Compute Cluster in Region A

Configure the distributed logical router (DLR) in the shared edge and compute cluster to use dynamic routing.

Procedure

1 Log in to the Compute 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 Under **Inventories**, click **Networking & Security**.

3 In the **Navigator**, click **NSX Edges**.

4 Select **172.16.11.66** from the **NSX Manager** drop-down menu.

5 Configure the routing for the Distributed Logical Router.

   a Double-click **SFOCOMP-DLR01**.

   b Click the **Manage** tab and click **Routing**.

   c On the **Global Configuration** page, perform the following configuration steps.

   d Click the **Edit** button under **Routing Configuration**, select **Enable ECMP**, and click **OK**.

   e Click the **Edit** button under **Dynamic Routing Configuration**, select **Uplink** as the Router ID, and click **OK**.

   f Click **Publish Changes**.

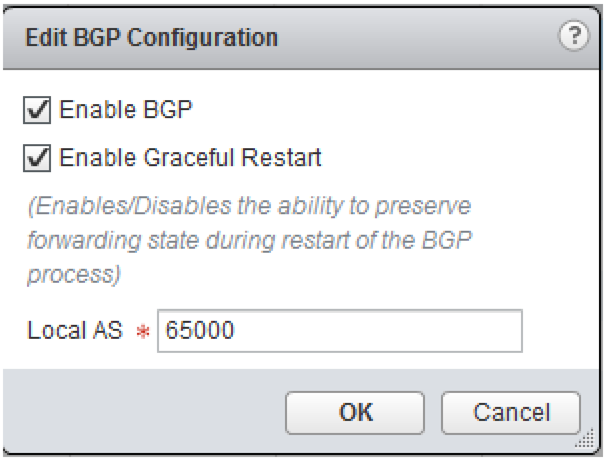
6 On the left, select **BGP** to configure it.

   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	65000



Edit BGP Configuration

☑ Enable BGP

☑ Enable Graceful Restart

(Enables/Disables the ability to preserve forwarding state during restart of the BGP process)

Local AS * 65000

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

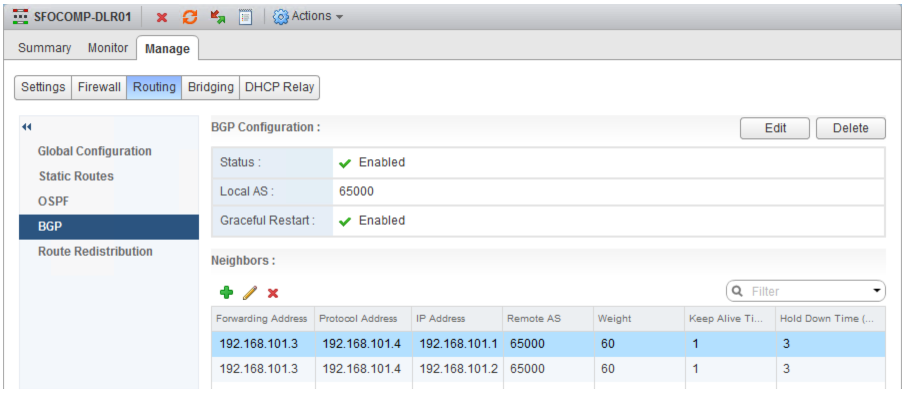
   The **New Neighbor** dialog box appears.

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: SFOCOMP-ESG01 and SFOCOMP-ESG02.

Setting	SFOCOMP-ESG01 Value	SFOCOMP-ESG02 Value
IP Address	192.168.101.1	192.168.101.2
Forwarding Address	192.168.101.3	192.168.101.3
Protocol Address	192.168.101.4	192.168.101.4
Remote AS	65000	65000
Weight	60	60
Keep Alive Time	1	1
Hold Down Time	3	3
Password	*bgp_password*	*bgp_password*

e Click **Publish Changes**.



BGP Configuration :

Status : ✓ Enabled

Local AS : 65000

Graceful Restart : ✓ Enabled

Neighbors :

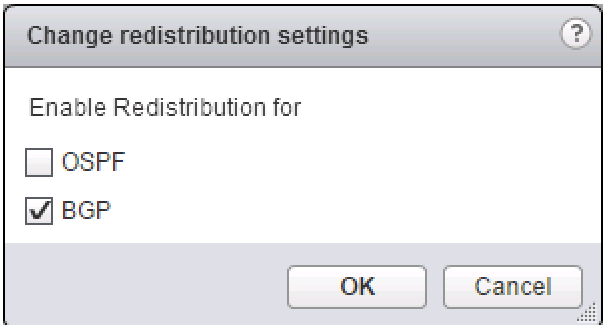
Forwarding Address	Protocol Address	IP Address	Remote AS	Weight	Keep Alive Ti...	Hold Down Time (...
192.168.101.3	192.168.101.4	192.168.101.1	65000	60	1	3
192.168.101.3	192.168.101.4	192.168.101.2	65000	60	1	3

7 On the left, select **Route Redistribution** to configure it.

a Click the **Edit** button.

b In the **Change redistribution settings** dialog box, enter the following settings, and click **OK**.

Setting	Value
OSPF	Deselected
BGP	Selected



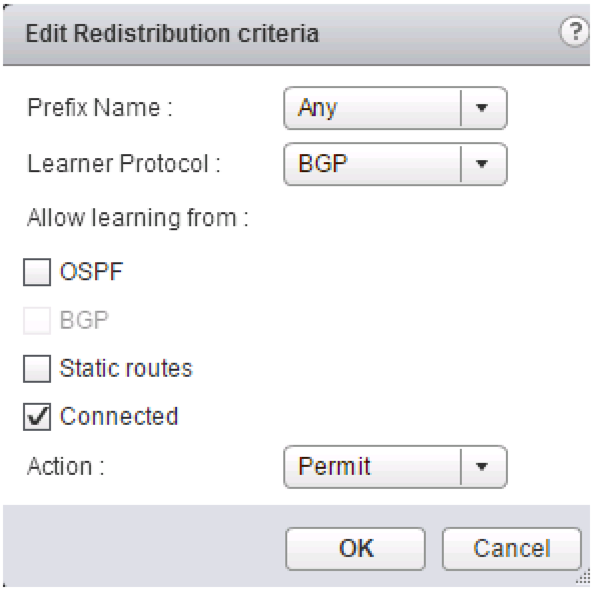
Enable Redistribution for

□ OSPF

☑ BGP

c On the **Route Redistribution** page, select the default **OSPF** entry and click the **Edit** button.

d Select **BGP** from the **Learner Protocol** drop-down menu, and click **OK**.



Prefix Name : Any

Learner Protocol : BGP

Allow learning from :

□ OSPF

□ BGP

□ Static routes

☑ Connected

Action : Permit

e Click **Publish Changes**.

Verify Establishment of BGP for the Distributed Logical Router in the Shared Edge and Compute Cluster in Region A

The distributed logical router (DLR) needs to establish a connection to Edge Services Gateway before BGP updates can be exchanged. Verify that the DLR is successfully peering, and that BGP routing has been established.

Procedure

1 Log in to the SFOCOMP-DLR01 by using a Secure Shell (SSH) client.

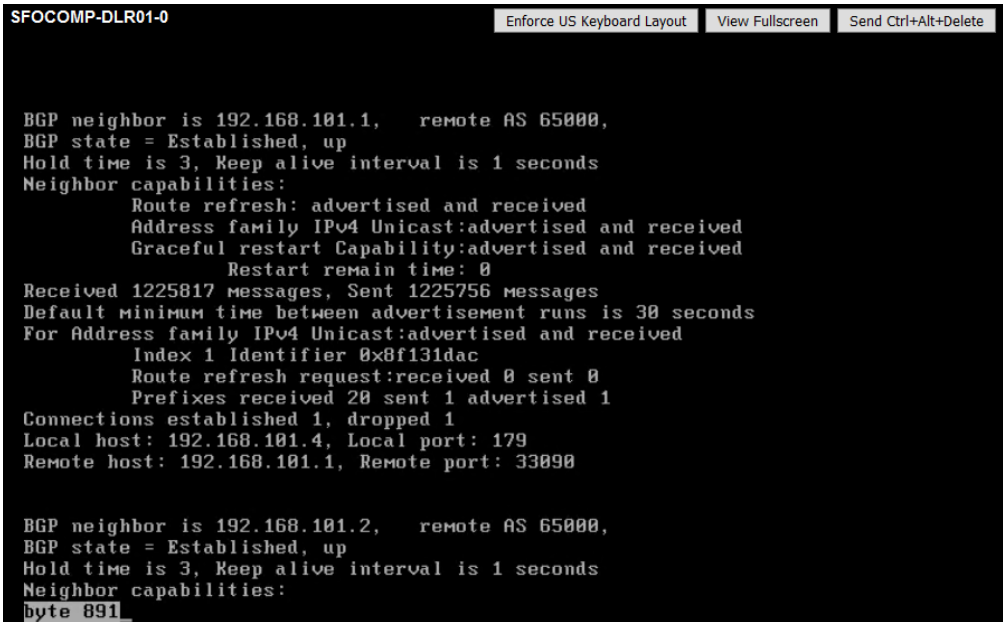
   a Open an SSH connection to SFOCOMP-DLR01, the DLR whose peering and BGP configuration you want to verify.

   b Log in using the following credentials.

Setting	Value
User name	admin
Password	*dlr_admin_password*

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

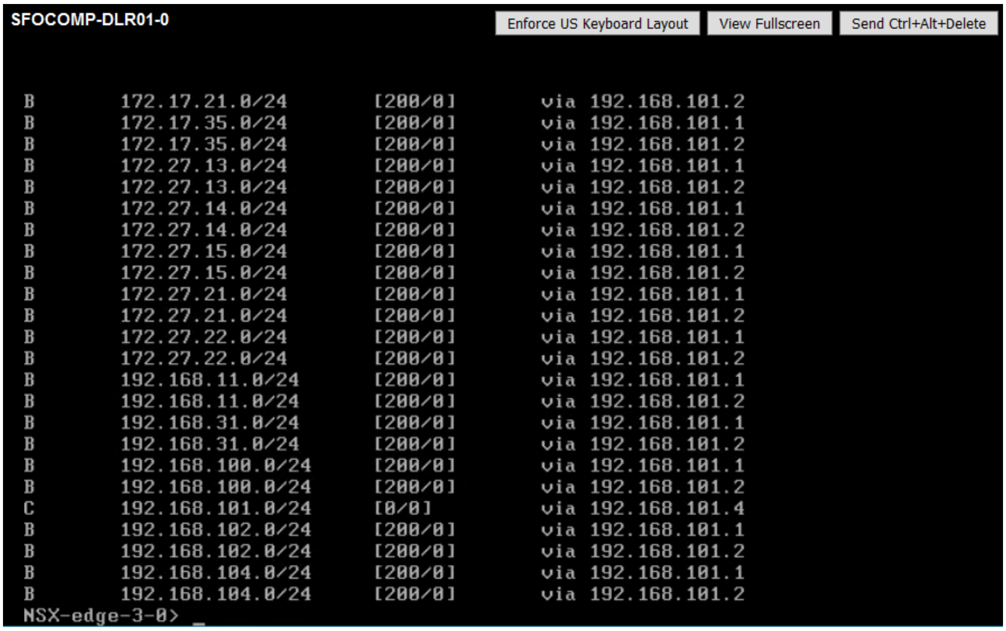
   The `BGP State` will display `Established,UP` if you have successfully peered with the Edge Service Gateway.



```
BGP neighbor is 192.168.101.1,   remote AS 65000,
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 1225817 messages, Sent 1225756 messages
Default minimum time between advertisement runs is 30 seconds
For Address family IPv4 Unicast:advertised and received
         Index 1 Identifier 0x8f131dac
         Route refresh request:received 0 sent 0
         Prefixes received 20 sent 1 advertised 1
Connections established 1, dropped 1
Local host: 192.168.101.4, Local port: 179
Remote host: 192.168.101.1, Remote port: 33090


BGP neighbor is 192.168.101.2,   remote AS 65000,
BGP state = Established, up
Hold time is 3, Keep alive interval is 1 seconds
Neighbor capabilities:
byte 891_
```

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`, `172.16.35.0/24`, `172.27.13.0/24`, and `172.27.22.0/24`. You can identify BGP networks by the letter `B` in the left-side column. Lines beginning with `C` (connected) have only a single route.



```
B       172.17.21.0/24      [200/0]      via 192.168.101.2
B       172.17.35.0/24      [200/0]      via 192.168.101.1
B       172.17.35.0/24      [200/0]      via 192.168.101.2
B       172.27.13.0/24      [200/0]      via 192.168.101.1
B       172.27.13.0/24      [200/0]      via 192.168.101.2
B       172.27.14.0/24      [200/0]      via 192.168.101.1
B       172.27.14.0/24      [200/0]      via 192.168.101.2
B       172.27.15.0/24      [200/0]      via 192.168.101.1
B       172.27.15.0/24      [200/0]      via 192.168.101.2
B       172.27.21.0/24      [200/0]      via 192.168.101.1
B       172.27.21.0/24      [200/0]      via 192.168.101.2
B       172.27.22.0/24      [200/0]      via 192.168.101.1
B       172.27.22.0/24      [200/0]      via 192.168.101.2
B       192.168.11.0/24     [200/0]      via 192.168.101.1
B       192.168.11.0/24     [200/0]      via 192.168.101.2
B       192.168.31.0/24     [200/0]      via 192.168.101.1
B       192.168.31.0/24     [200/0]      via 192.168.101.2
B       192.168.100.0/24    [200/0]      via 192.168.101.1
B       192.168.100.0/24    [200/0]      via 192.168.101.2
C       192.168.101.0/24    [0/0]        via 192.168.101.4
B       192.168.102.0/24    [200/0]      via 192.168.101.1
B       192.168.102.0/24    [200/0]      via 192.168.101.2
B       192.168.104.0/24    [200/0]      via 192.168.101.1
B       192.168.104.0/24    [200/0]      via 192.168.101.2
NSX-edge-3-0> _
```

Test the Shared Edge and Compute Cluster NSX Configuration in Region A

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.

Procedure

1 Log in to the Compute 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 Use the Ping Monitor to test connectivity.

   a In the Navigator, click **Networking & Security**.

   b Under **Logical Switches**, double-click **Universal Transit Network** .

   c Click the **Monitor** tab.

   d Under **Test Parameters**, select **comp01esx01.sfo01.rainpole.local** as the Source host.

   e Under the Test Parameters, select **comp01esx02.sfo01.rainpole.local** as the Destination Host, and click **Start Test** .

   f There must be no error messages listed under **Results**.

Deploy vSphere Data Protection in Region A

Deploy vSphere Data Protection to provide the capability for backup and restore of SDDC management components.

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

- vCenter Server
  - Management vCenter Server and connected external Platform Services Controller
  - Compute vCenter Server and connected external Platform Services Controller
- NSX for vSphere
  - NSX Manager for the management cluster
  - NSX Manager for the shared compute and edge cluster
- vRealize Automation
- vRealize Operations Manager
- vRealize Log Insight

Procedure

1 Prerequisites for Deploying vSphere Data Protection in Region A

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

2 Deploy the vSphere Data Protection Virtual Appliance in Region A

   Deploy vSphere Data Protection as a virtual appliance on the management cluster in Region A.

3 Configure Service Account Access in vSphere for Integration with vSphere Data Protection in Region A

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

4 Register vSphere Data Protection with Management vCenter Server in Region A

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

Prerequisites for Deploying vSphere Data Protection in Region A

Before you deploy vSphere Data Protection in Region A, 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 Region A of the SDDC deployment.

Table 2-12. IP Addresses and Host Names for vSphere Data Protection in Region A

Network Setting	Value
IP address	172.16.11.81
FQDN	mgmt01vdp01.sfo01.rainpole.local
Primary DNS server	172.16.11.4
Secondary DNS server	172.16.11.5
Default gateway	172.16.11.253
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	■ Virtual disk provisioning. ■ Thin ■ Required storage ■ 4 TB NFS
Software Features	■ vSphere ■ Management vCenter Server ■ Management cluster with enabled DRS and HA. ■ vSphere Distributed Switch configured for the vSphere management network
Installation Package	Download the vSphere Data Protection virtual appliance `.ova` file to the machine where you use the vSphere Web Client.

Deploy the vSphere Data Protection Virtual Appliance in Region A

Deploy vSphere Data Protection as a virtual appliance on the management cluster in Region A.

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 In the vSphere Web Client, navigate to the SFO01-Mgmt01 cluster object.

Inventory Object	Value
vCenter Server	mgmt01vc01.sfo01.rainpole.local
Data center	SFO01
Cluster	SFO01-Mgmt01

3 Right-click the **SFO01-Mgmt01** 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	mgmt01vdp01
vCenter Server	mgmt01vc01.sfo01.rainpole.local
Data center	SFO01

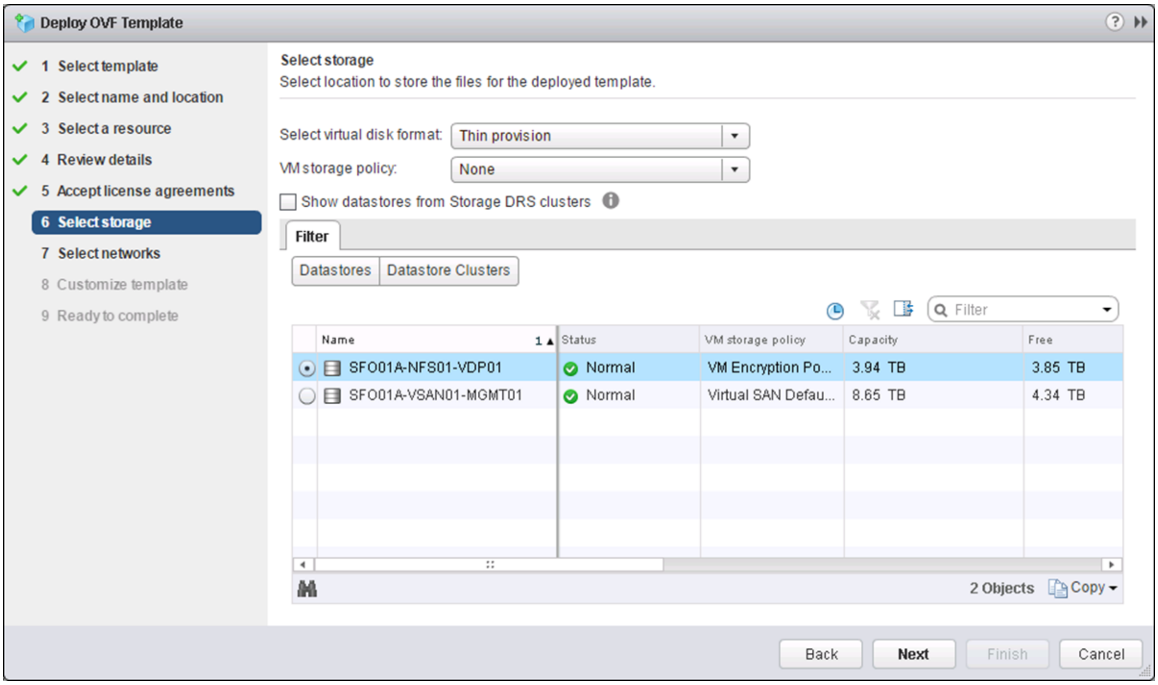
6 On the **Select a resource** page, click the **Browse** tab, select the **SFO01-Mgmt01** cluster, and click **Next**.

7 On the **Review details** page, examine the virtual appliance details, such as product name, 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	SFO01A-NFS01-VDP01
Select virtual disk format	Thin provision
VM storage policy	None



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 storage
Select location to store the files for the deployed template.

Select virtual disk format: Thin provision

VM storage policy: None

□ Show datastores from Storage DRS clusters

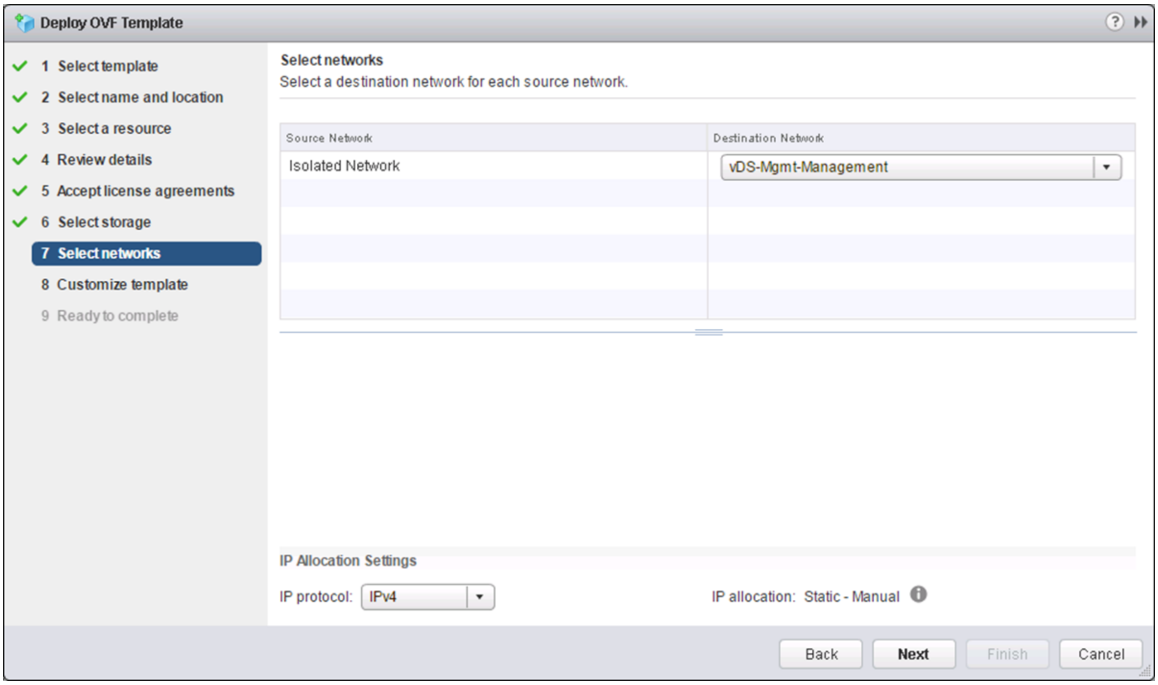
Filter

Datastores | Datastore Clusters

	Name	Status	VM storage policy	Capacity	Free
●	SFO01A-NFS01-VDP01	Normal	VM Encryption Po...	3.94 TB	3.85 TB
○	SFO01A-VSAN01-MGMT01	Normal	Virtual SAN Defau...	8.65 TB	4.34 TB

2 Objects

10 On the **Select networks** page, select the **vDS-Mgmt-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-Mgmt-Management

IP Allocation Settings

IP protocol: IPv4

IP allocation: Static - Manual

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

IPv4 Setting	Value
Default gateway	172.16.11.253
DNS server	172.16.11.5, 172.16.11.4
Static IPv4 address	172.16.11.81
Subnet mask	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**.

Configure Service Account Access in vSphere for Integration with vSphere Data Protection in Region A

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

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 Management vCenter Server.

Define a User Role in vSphere for Integration with vSphere Data Protection in Region A

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 Region A.

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	■ Alarms.Create Alarm ■ Alarms.Modify Alarms ■ 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 extensions ■ 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 ■ Session.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 use device ■ Virtual Machine.Configuration.Memory ■ Virtual Machine.Configuration.Modify device setting ■ Virtual Machine.Configuration.Raw device

Setting	Value
	■ 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 Operations 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.ViMware 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 snapshot ■ vApp.Export ■ vApp.Import ■ vApp.vApp application configuration

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

4 The Management vCenter Server for Region A propagates the role to the other linked vCenter Server instances.

Configure User Privileges in vSphere for Integration with vSphere Data Protection for Region A

Assign global permissions in Region A 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 vCenter Server inventory.

Prerequisites

- Verify that the Management vCenter Server for Region A are connected to the Active Directory domain.
- Verify that the users and groups from the rainpole.local domain are available on the Management vCenter Server in Region A.

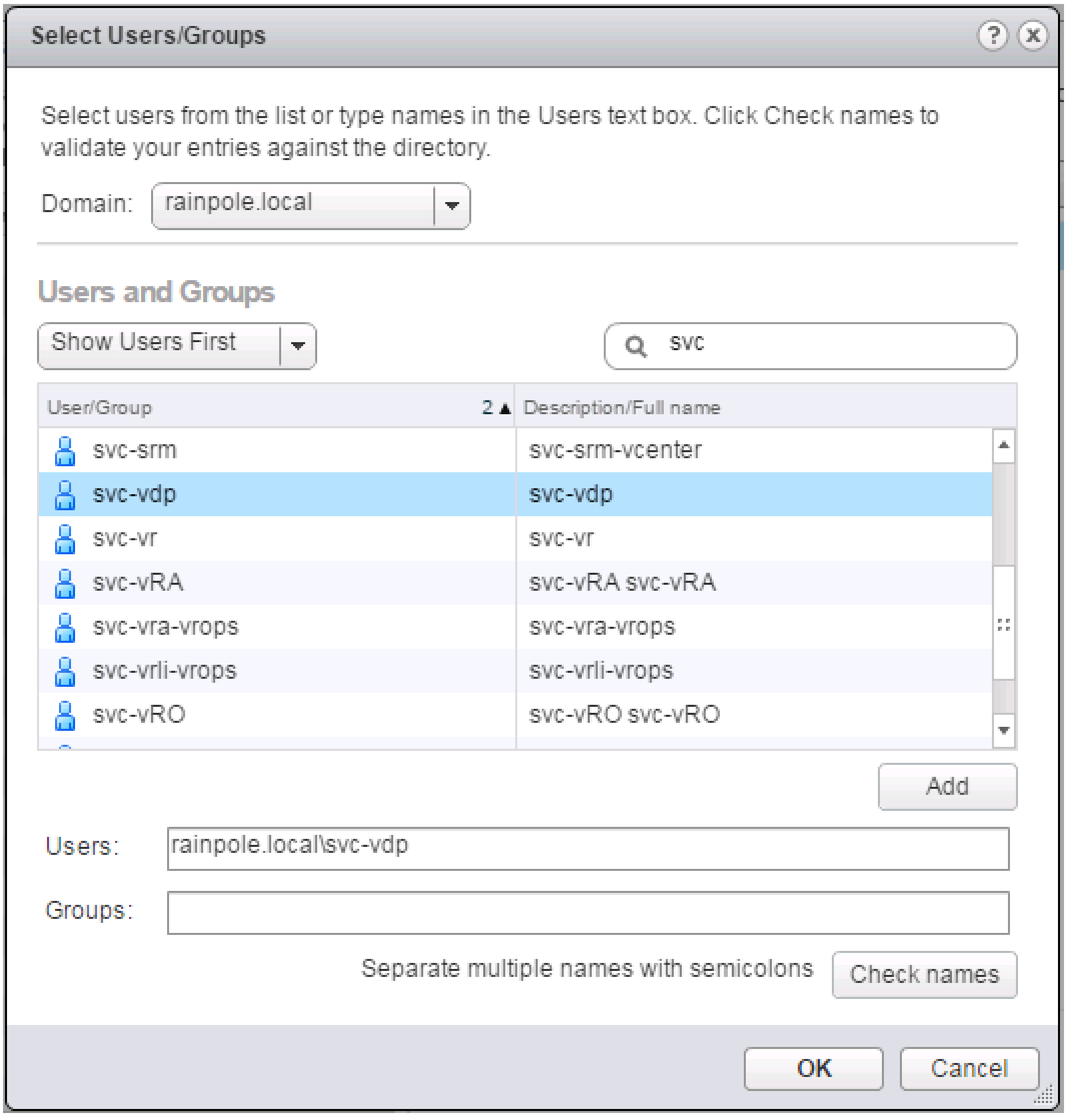
Procedure

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. From the **Home** menu, select **Administration**.
3. Assign global permissions to the svc-vdp@rainpole.local service account.
   a. In the vSphere Web Client, select navigate **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-vdp** user, click **Add**, and click OK.



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

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

Users: rainpole.local\svc-vdp

Groups:

Separate multiple names with semicolons

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**, and click **OK**.

The global permissions of the svc-vdp service account propagate to all linked vCenter Server instances.

Register vSphere Data Protection with Management vCenter Server in Region A

After you deploy the virtual appliance for vSphere Data Protection on the management cluster in Region A, 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://mgmt01vdp01.sfo01.rainpole.local:8543/vdp-configure`.

   b. Log in using the following credentials.

Setting	Value
User name	root
Password	changeme

   The vSphere Data Protection configuration wizard 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: ~!@#,.)

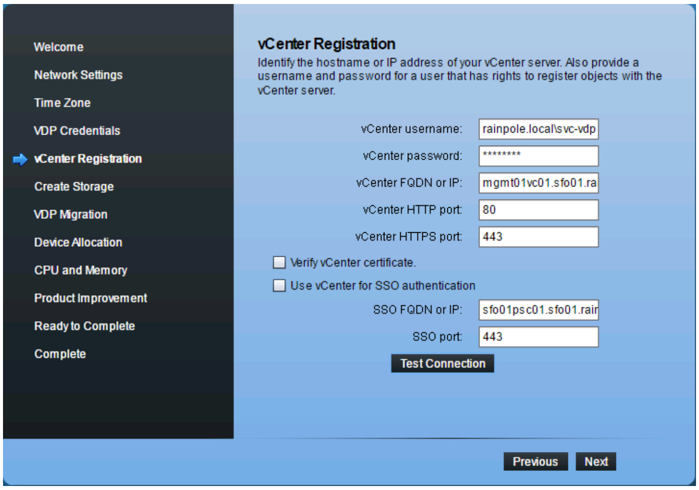
6 On the **vCenter Registration** page, configure the settings for registration with the Management vCenter Server.

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	mgmt01vc01.sfo01.rainpole.local
vCenter HTTP port	80
vCenter HTTPS port	443
Verify vCenter certificate	Deselected

b Enter the settings for vCenter Single Sign-On on the Management Platform Services Controller.

Single Sign-On Setting	Value
Use vCenter for SSO authentication	Deselected
SSO FQDN or IP	sfo01psc01.sfo01.rainpole.local
SSO port	443



vCenter Registration

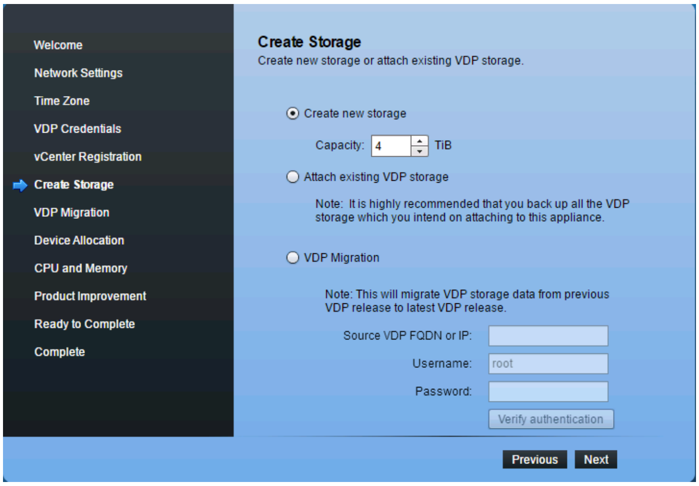
Identify the hostname or IP address of your vCenter server. Also provide a username and password for a user that has rights to register objects with the vCenter server.

vCenter username: rainpole.local\svc-vdp
vCenter password: ********
vCenter FQDN or IP: mgmt01vc01.sfo01.ra
vCenter HTTP port: 80
vCenter HTTPS port: 443
□ Verify vCenter certificate.
□ Use vCenter for SSO authentication
SSO FQDN or IP: sfo01psc01.sfo01.rair
SSO port: 443

c Click **Test Connection**, and in the success message box, click **OK**.

d On the **vCenter Registration** page, click **Next**.

7 On the **Create Storage** page, select **Create new storage**, in the **Capacity** text box, enter **4** TiB and click **Next**.



Create Storage

Create new storage or attach existing VDP storage.

● Create new storage

Capacity: 4 TiB

○ Attach existing VDP storage

Note: It is highly recommended that you back up all the VDP storage which you intend on attaching to this appliance.

○ VDP Migration

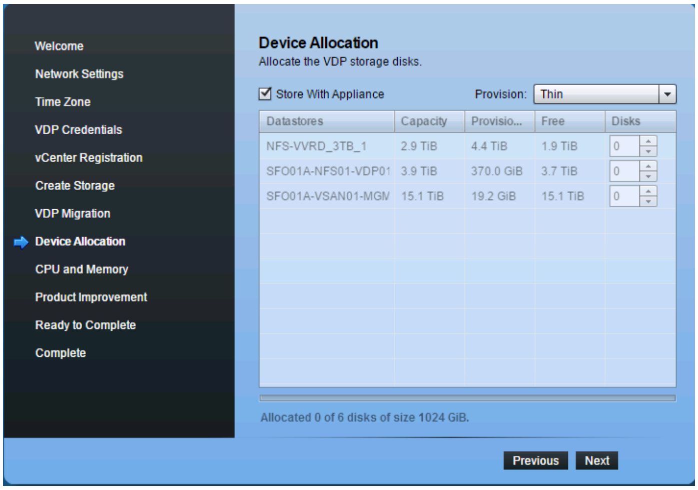
Note: This will migrate VDP storage data from previous VDP release to latest VDP release.

Source VDP FQDN or IP:

Username: root

Password:

8 On the **Device Allocation** page, from the **Provision** drop-down menu, select **Thin** and click **Next**.



Device Allocation

Allocate the VDP storage disks.

☑ Store With Appliance

Provision: Thin

Datastores	Capacity	Provisio...	Free	Disks
NFS-VVRD_3TB_1	2.9 TiB	4.4 TiB	1.9 TiB	0
SFO01A-NFS01-VDP01	3.9 TiB	370.0 GiB	3.7 TiB	0
SFO01A-VSAN01-MGN	15.1 TiB	19.2 GiB	15.1 TiB	0

Allocated 0 of 6 disks of size 1024 GiB.

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 the **Run performance analysis on storage configuration** and **Restart the appliance if successful** check boxes, 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 Verify that the vSphere Data Protection is accessible in the vSphere Web Client after you complete the initial configuration of vSphere Data Protection.

   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	admininistrator@vsphere.local
Password	*vsphere_admin_password*

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

Replace Certificates in Region A

In this design, you replace user-facing certificates with certificates that are signed by a Microsoft Certificate Authority (CA). By default, virtual infrastructure management components use TLS/SSL certificates that are signed by the VMware Certificate Authority (VMCA). These certificates are not trusted by end-user devices.

Infrastructure administrators connect to different SDDC components, such as vCenter Server systems or a Platform Services Controller from a Web browser to perform configuration, management and troubleshooting. The authenticity of the network node to which the administrator connects must be confirmed with a valid TLS/SSL certificate.

You can use other Certificate Authorities according to the requirements of your organization. You do not replace certificates for machine-to-machine communication. If necessary, you can manually mark these certificates as trusted.

1 Management vCenter Server

2 Management NSX Manager

3 Compute vCenter Server

4 Compute NSX Manager

5 vSphere Data Protection

Procedure

1 Replace the vCenter Server Certificates in Region A

   After you replace the Platform Services Controller certificate, you replace the vCenter Server machine SSL certificate. You generate a vCenter Server certificate manually or by using the CertGenVVD tool.

2 Replace the NSX Manager Certificates in Region A

   After you replace the certificates of all Platform Services Controller instances and all vCenter Server instances, replace the certificates for the NSX Manager instances.

3 Install a CertGenVVD-Generated Certificate on vSphere Data Protection in Region A

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 Region A with the certificate that is generated by `CertGenVVD`.

Replace the vCenter Server Certificates in Region A

After you replace the Platform Services Controller certificate, you replace the vCenter Server machine SSL certificate. You generate a vCenter Server certificate manually or by using the CertGenVVD tool.

You replace certificates twice, once for each vCenter Server instance. You can start replacing certificates on Management vCenter Server mgmt01vc01.sfo01.rainpole.local first.

Table 2-13. Certificate-Related Files on the vCenter Server Instances

vCenter Server FQDN	Files for Certificate Replacement	Replacement Order
mgmt01vc01.sfo01.rainpole.local	■ mgmt01vc01.sfo01.key ■ mgmt01vc01.sfo01.1.cer ■ chainRoot64.cer	After you replace the certificate on the management Platform Services Controller.
comp01vc01.sfo01.rainpole.local	■ comp01vc01.sfo01.key ■ comp01vc01.sfo01.1.cer ■ chainRoot64.cer	After you replace the certificate on the compute Platform Services Controller.

Procedure

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

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 mgmt01vc01.sfo01.rainpole.local.

   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/chainRoot64.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 the default vCenter Single Sign-On user name **`administrator@vsphere.local`** and the ***`vsphere_admin_password`*** password.

d When prompted for the Infrastructure Server IP, enter the IP address of the Platform Services Controller that manages this vCenter Server instance.

Option	IP Address of Connected Platform Services Controller
mgmt01vc01.sfo01.rainpole.local	172.16.11.61
comp01vc01.sfo01.rainpole.local	172.16.11.63

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	Input to the vSphere Certificate Manager Utility
mgmt01vc01.sfo01.rainpole.local	Please provide valid custom certificate for Machine SSL. File : **`/tmp/ssl/mgmt01vc01.sfo01.1.cer`** Please provide valid custom key for Machine SSL. File : **`/tmp/ssl/mgmt01vc01.sfo01.key`** Please provide the signing certificate of the Machine SSL certificate. File : **`/tmp/ssl/chainRoot64.cer`**
comp01vc01.sfo01.rainpole.local	Please provide valid custom certificate for Machine SSL. File : **`/tmp/ssl/comp01vc01.sfo01.1.cer`** Please provide valid custom key for Machine SSL. File : **`/tmp/ssl/comp01vc01.sfo01.key`** Please provide the signing certificate of the Machine SSL certificate. File : **`/tmp/ssl/chainRoot64.cer`**

4 After Status shows `100% Completed`, wait several minutes until all vCenter Server services are restarted.

5 After you replace the certificate on the mgmt01vc01.sfo01.rainpole.local vCenter Server, repeat the procedure to replace the certificate on the compute vCenter Server comp01vc01.sfo01.rainpole.local.

Replace the NSX Manager Certificates in Region A

After you replace the certificates of all Platform Services Controller instances and all vCenter Server instances, replace the certificates for the NSX Manager instances.

You replace certificates twice, once for each NSX Manager. You first start replacing certificates on the NSX Manager for the mgmt01nsxm01.sfo01.rainpole.local management cluster.

Table 2-14. Certificate-Related Files on the NSX Manager Instances in Region A

NSX Manager FQDN	Certificate File Name	Replacement Time
mgmt01nsxm01.sfo01.rainpole.local	■ mgmt01nsxm01.sfo01.chain.cer from manual generation ■ mgmt01nsxm01.sfo01.4.p12 from the automation generation	After you replace the certificate on the Management vCenter Server
comp01nsxm01.sfo01.rainpole.local	■ comp01nsxm01.sfo01.chain.cer from manual generation ■ comp01nsxm01.sfo01.4.p12 from the automation generation	After you replace the certificate on the Compute vCenter Server

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.

NSX Manager	URL
NSX Manager for the management cluster	https://mgmt01nsxm01.sfo01.rainpole.local
NSX Manager for the shared compute and edge cluster	https://comp01nsxm01.sfo01.rainpole.local

b Log in using the following credentials.

Setting	Value
User name	admin
Password	*nsx_manager_admin_password*

2 On the **Manage** tab, click **SSL Certificates**, click **Import** and provide the certificate chain file.

3 Restart the NSX Manager to propagate the CA-signed certificate.

a In the right corner of the NSX Manager page, click the **Settings** icon.

b From the drop-down menu, select **Reboot Appliance**.

4 Re-register the NSX Manager to the Management vCenter Server.

a Open a Web browser and go to the NSX Manager Web interface.

Setting	Value
NSX Manager for the management cluster	https://mgmt01nsxm01.sfo01.rainpole.local
NSX Manager for the shared compute and edge cluster	https://comp01nsxm01.sfo01.rainpole.local

b Log in using the following credentials.

Setting	Value
User name	admin
Password	*nsx_mngr_admin_password*

c Click **Manage vCenter Registration**.

d Under **Lookup Service**, click the **Edit** button.

e In the **Lookup Service** dialog box, enter the following settings, and click **OK**.

Setting	Value
Lookup Service IP	sfo01psc01.sfo01.rainpole.local
Lookup Service Port	443
SSO Administrator User Name	administrator@vsphere.local
Password	*vsphere_admin_password*

f In the **Trust Certificate?** dialog box, click **Yes**.

g Under **vCenter Server**, click the **Edit** button.

h In the **vCenter Server** dialog box, enter the following settings, and click **OK**.

Setting	Value for the NSX Manager for the Management Cluster	Value for the NSX Manager for the Shared Edge and Compute Cluster
vCenter Server	mgmt01vc01.sfo01.rainpole.local	comp01vc01.sfo01.rainpole.local
vCenter User Name	svc-nsxmanager@rainpole.local	
Password	*svc-nsxmanager_password*	

i In the **Trust Certificate?** dialog box, click **Yes**.

j Wait until the Status indicators for the Lookup Service and vCenter Server change to `Connected`.

5 Repeat the steps for the NSX Manager for the shared compute and edge cluster.

Install a CertGenVVD-Generated Certificate on vSphere Data Protection in Region A

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 Region A 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.

   a. Open an SSH connection to the virtual machine mgmt01vdp01.sfo01.rainpole.local.

   b. 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
   ```

Region A Cloud Management Platform Implementation

3

The Cloud Management Platform (CMP) consists of integrated products that support the management of public, private and hybrid cloud environments. The VMware 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 first site in the enterprise.

This chapter includes the following topics:

Prerequisites for Cloud Management Platform Implementation in Region A

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

DNS Entries and IP Address Mappings in Region A

Before you deploy vRealize Automation, verify that your environment satisfies the requirements for this deployment.

IP Addresses and Host Names

Verify that the static IP address and FQDNs that are listed in the table below are available for the vRealize Automation application virtual network for the first region of the SDDC deployment.

Table 3-1. IP Addresses and FQDNs for the vRealize Automation Instance in Region A

Role	IP Address	FQDN
vRealize Automation Server Appliances	192.168.11.51	vra01svr01a.rainpole.local
	192.168.11.52	vra01svr01b.rainpole.local
vRealize Automation Server VIP	192.168.11.53	vra01svr01.rainpole.local
vRealize Automation for IWS	192.168.11.54	vra01iws01a.rainpole.local
	192.168.11.55	vra01iws01b.rainpole.local
vRealize Automation IWS VIP	192.168.11.56	vra01iws01.rainpole.local
vRealize Automation Model Manager IMS	192.168.11.57	vra01ims01a.rainpole.local
	192.168.11.58	vra01ims01b.rainpole.local
vRealize Automation IMS VIP	192.168.11.59	vra01ims01.rainpole.local
vRealize DEM Workers	192.168.11.60	vra01dem01.rainpole.local
	192.168.11.61	vra01dem02.rainpole.local
MS SQL Server for vRealize Automation	192.168.11.62	vra01mssql01.rainpole.local
vRealize Orchestrator	192.168.11.63	vra01vro01a.rainpole.local
	192.168.11.64	vra01vro01b.rainpole.local
vRealize Orchestrator VIP	192.168.11.65	vra01vro01.rainpole.local
vRealize Business for vRealize Automation	192.168.11.66	vra01bus01.rainpole.local

Table 3-2. IP Addresses and Host Name for the vRA Proxy Agents and vRB Data Collector in Region A

Role	IP Address	FQDN
vRealize Automation Proxy Agent	192.168.31.52	vra01ias01.sfo01.rainpole.local
	192.168.31.53	vra01ias02.sfo01.rainpole.local
vRealize Business Data Collector	192.168.31.54	vra01buc01.sfo01.rainpole.local
Default gateway	192.168.31.1	
DNS server	172.16.11.5	
Subnet mask	255.255.255.0	
ntp	172.16.11.251 172.16.11.252	ntp.sfo01.rainpole.local
	172.17.11.251 172.17.11.252	ntp.lax01.rainpole.local

vRealize Automation Deployment Prerequisites

Before you install and use vRealize Automation, your environment must meet the following prerequisites.

Prerequisite	Value
Storage	■ Virtual disk provisioning. ■ Required storage per node.
Operating system	Windows 2012 R2 Standard
Database	Microsoft SQL Server 2012 Standard Edition
Installation package	Download the vRealize Automation virtual appliance `.ova` file. Download the vRealize Orchestrator virtual appliance `.ova` file. Download the vRealize Business virtual appliance `.ova` file.
License	Verify that you have obtained a license that covers the use of vRealize Automation. Verify that you have obtained a license that covers the use of vRealize Business for vRealize Automation.
Active directory	Verify that you have a parent Active Directory instance with the SDDC user roles configured for the rainpole.local domain. Verify the existence of the svc-vra user in the `rainpole.local` domain. Verify the existence of the svc-vro user in the `rainpole.local` domain.
Certification authority	Configure the root Active Directory domain controller as a certificate authority for the environment.
Java	Install Java SE Development Kit (JDK), which is required to run the vRealize Orchestrator Client.

SQL Server Configuration for the Cloud Management Platform in Region A

The Cloud Management Platform uses a Microsoft SQL Server database to store data for use by vRealize Automation and vRealize Orchestrator.

Microsoft SQL Server Recommendations in Region A

vRealize Automation, vRealize Orchestrator, and other VMware components use Microsoft SQL Server as a database to store information. While the specific configuration of SQL Server for use in your environment is not addressed in this implementation guide, high-level guidance is provided to ensure more reliable operation of your VMware components.

- Microsoft SQL Server should be configured with separate Operating System Level volumes (drive letters) for each of the following items. The separation of these items into separate logical volumes (drive letters) will help prevent database corruption should a single volume reach capacity.
  - Operating System
  - Database Application
  - SQL User Database Data Files
  - SQL User Database Log Files
  - SQL TempDB

  - SQL Backup Files

- To provide optimal performance for VMware vRealize databases, configure the SQL Server virtual machine (`vra01mssql01.rainpole.local`) with 8 vCPU and 16G vRAM.
- Configure the SQL Server virtual machine's (`vra01mssql01.rainpole.local`) primary DNS to point to 172.16.11.4 (region A's primary DNS) and its secondary DNS to point to 172.17.11.4 (region B's primary DNS).

For further guidance on the deployment and operation of a production installation of Microsoft SQL Server, see the Microsoft SQL Server documentation, or consult with a qualified Microsoft SQL Server database administrator.

Assign the SQL Server System Role to vRealize Automation in Region A

Assign the SQL Server system role **sysadmin** to the vRealize Automation service account.

vRealize Automation uses the SQL Server system role privilege to create and execute scripts on the SQL Server database. By default, only users who are members of the **sysadmin** system role, or the **db_owner** and **db_ddladmin** database roles, can create objects in the database.

Procedure

1 Log in to the `VRA01MSSQL01.rainpole.local` by using a Remote Desktop Protocol (RDP) client.

  a Open an RDP connection to the virtual machine `VRA01MSSQL01.rainpole.local`.

  b Log in using the following credentials.

Setting	Value
User name	Windows administrator user
Password	*windows_administrator_password*

2 From the **Start** menu, click **All Programs**, click **Microsoft SQL Server**, and click **SQL Server Management Studio**.

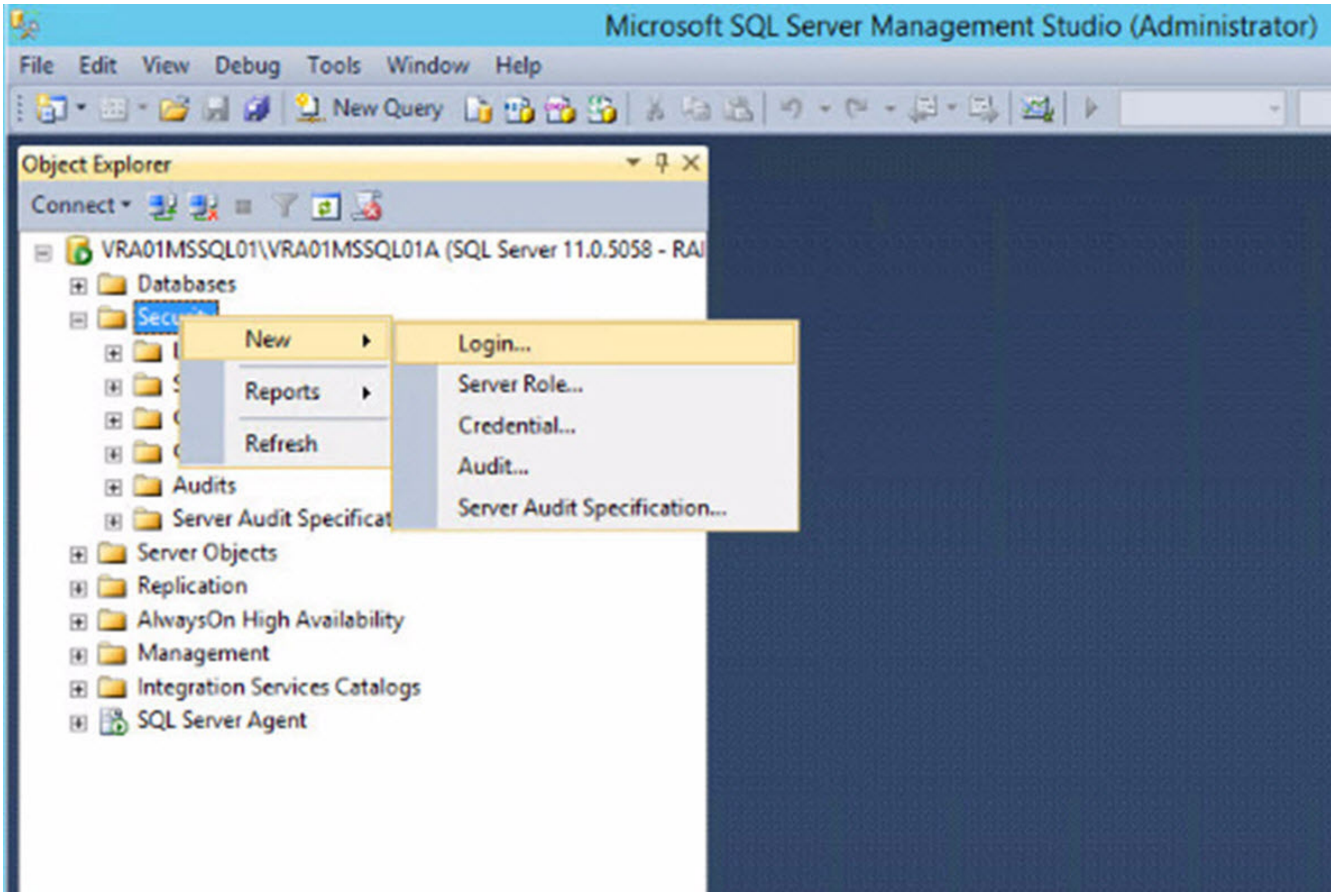
Note If SQL Server Management Studio doesn't appear in your **All Programs** menu, you may not have successfully installed SQL Server Management Studio. Verify that you have successfully installed SQL Server Management Studio, and then continue with this procedure.

3 In the Connect to Server dialog box, leave the default value of the **Server Name** text box, select **Windows Authentication** from the **Authentication** drop-down menu, and click **Connect**.

Note During the SQL Server installation, the **Database Engine** configuration wizard prompts you to provide the user name and password for the SQL Server administrator. If this user was not added during the SQL Server installation, select **SQL Authentication** from the **Authentication** drop-down menu, and enter the user name **`sa`** in the **User name** text box, and the password ***`sa_password`*** in the **Password** text box.

4 In Object Explorer, expand the server instance **VRA01MSSQL01**.

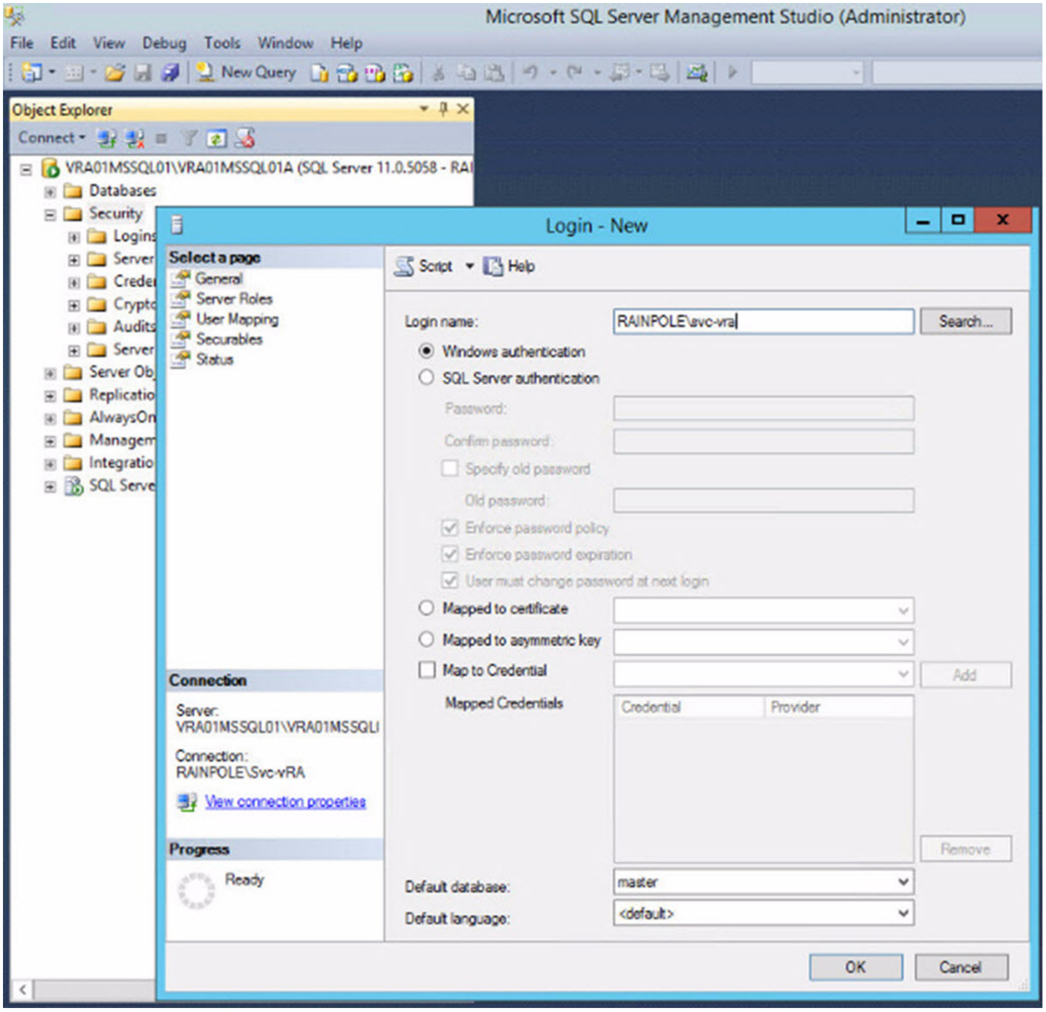
5 Right-click the **Security** folder, click **New**, and click **Login**.


Microsoft SQL Server Management Studio (Administrator)
File Edit View Debug Tools Window Help
New Query
Object Explorer
Connect
VRA01MSSQL01\VRA01MSSQL01A (SQL Server 11.0.5058 - RAI
Databases
Secu
New
Reports
Refresh
Login...
Server Role...
Credential...
Audit...
Server Audit Specification...
Audits
Server Audit Specificat
Server Objects
Replication
AlwaysOn High Availability
Management
Integration Services Catalogs
SQL Server Agent

The **Login Properties** dialog box opens.

6 Select the General page of the **Login Properties** dialog box.

7 From the Object Explorer Details pane select the General page, and enter `Rainpole\Svc-vRA` in the **Login name** text box.



Login name: RAINPOLE\svc-vra

● Windows authentication

Default database: master

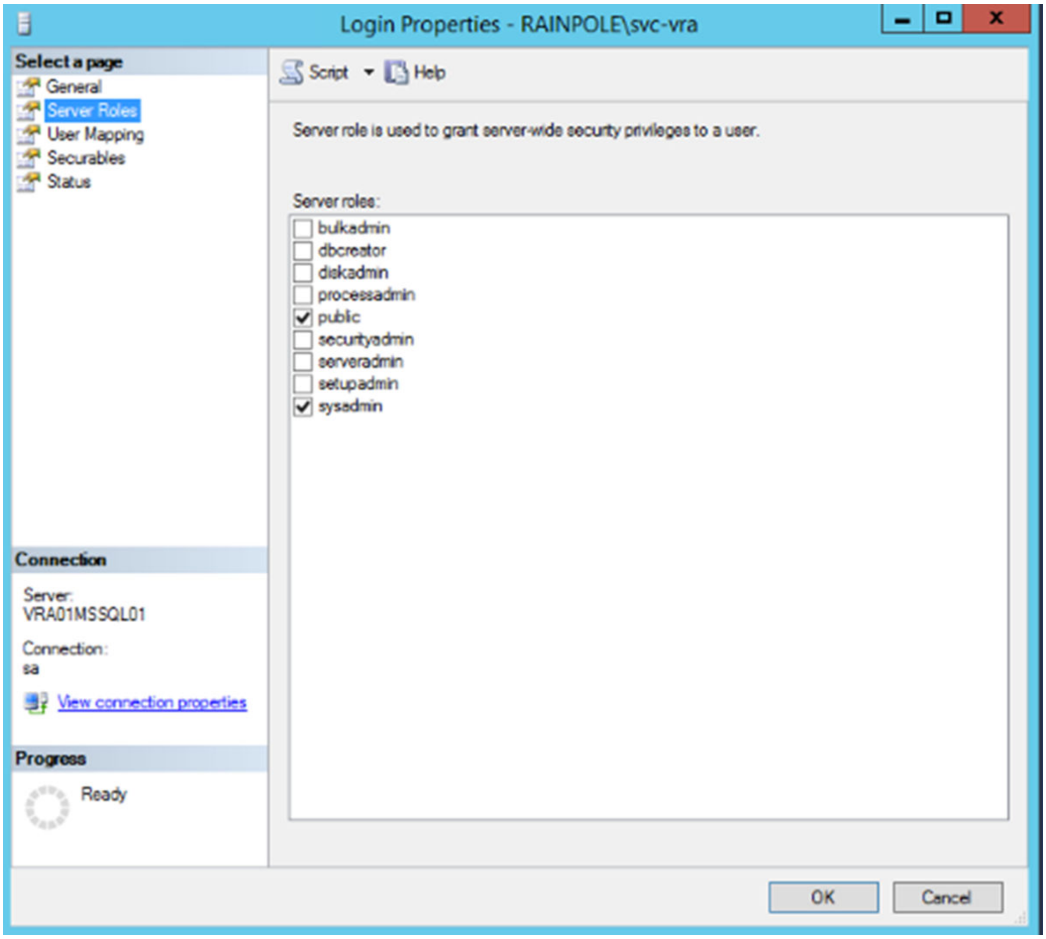
Default language: <default>

Server:
VRA01MSSQL01\VRA01MSSQLI

Connection:
RAINPOLE\Svc-vRA

8 In the **Object Explorer Details** pane, select the **Server Role** page.

9 In the Server roles list item field select the **sysadmin** check box, and click **OK**.



Server role is used to grant server-wide security privileges to a user.

Server roles:

- □ bulkadmin
- □ dbcreator
- □ diskadmin
- □ processadmin
- ☑ public
- □ securityadmin
- □ serveradmin
- □ setupadmin
- ☑ sysadmin

Server:
VRA01MSSQL01

Connection:
sa

Ready

Create a SQL Server Database for vRealize Orchestrator in Region A

vRealize Orchestrator requires a database for storing data related to workflows and actions. You must create an empty database specifically for use by vRealize Orchestrator. For information on creating a new database using Microsoft SQL Server, see the documentation supplied by your database vendor.

Procedure

1 Log in to the **`VRA01MSSQL01.rainpole.local`** by using a Remote Desktop Protocol (RDP) client.

   a Open an RDP connection to the virtual machine `VRA01MSSQL01.rainpole.local`.

   b Log in using the following credentials.

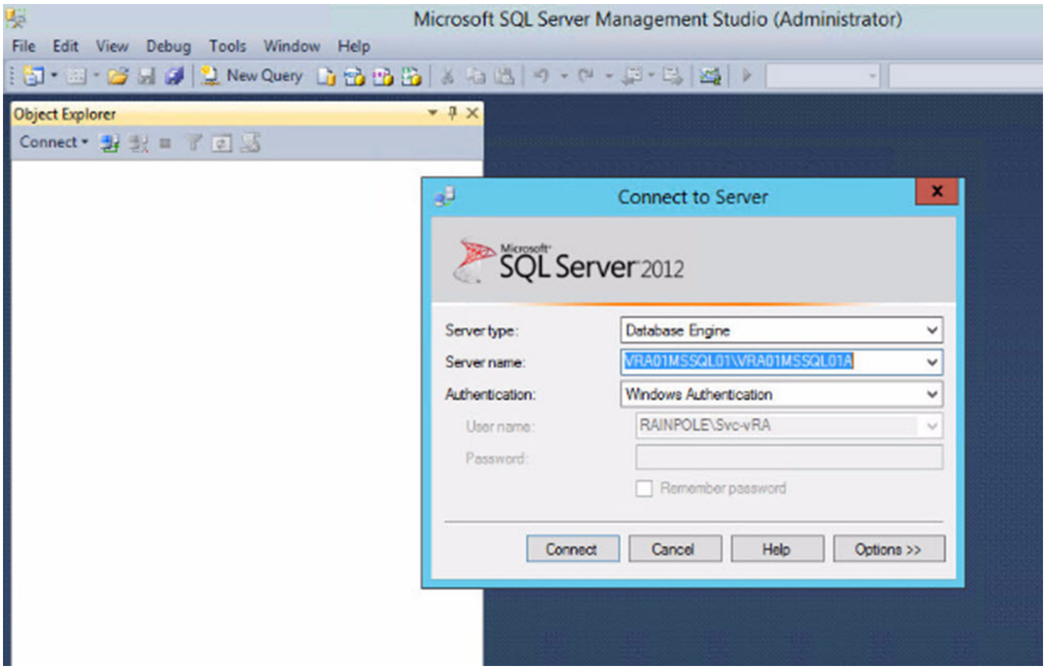
Setting	Value
User name	Windows administrator user
Password	*windows_administrator_password*

2 From the **Start** menu, click **All Programs**, click **Microsoft SQL Server**, and click **SQL Server Management Studio**.

Note If SQL Server Management Studio doesn't appear in your **All Programs** menu, you may not have successfully installed SQL Server Management Studio. Verify that you have successfully installed SQL Server Management Studio, and then continue with this procedure.

3 In the **Connect to Server** dialog box, leave the **Server Name** text box with its default value, select **Windows Authentication** from the **Authentication** drop-down menu, and click **Connect**.

Note During the SQL Server installation, the **Database Engine** configuration wizard prompts you to provide the SQL server **administrator rainpole\svc-vra** user name. If this user was not added during the SQL Server installation, select **SQL Authentication** from the **Authentication** drop-down menu, and enter the user name **sa** in the **User name** text box, and the password ***sa_password*** in the **Password** text box.


Microsoft SQL Server Management Studio (Administrator)
File Edit View Debug Tools Window Help
New Query
Object Explorer
Connect
Connect to Server
Microsoft SQL Server 2012
Connect
Cancel
Help
Options >>

Server type: Database Engine

Server name: VRA01MSSQL01\VRA01MSSQL01A

Authentication: Windows Authentication

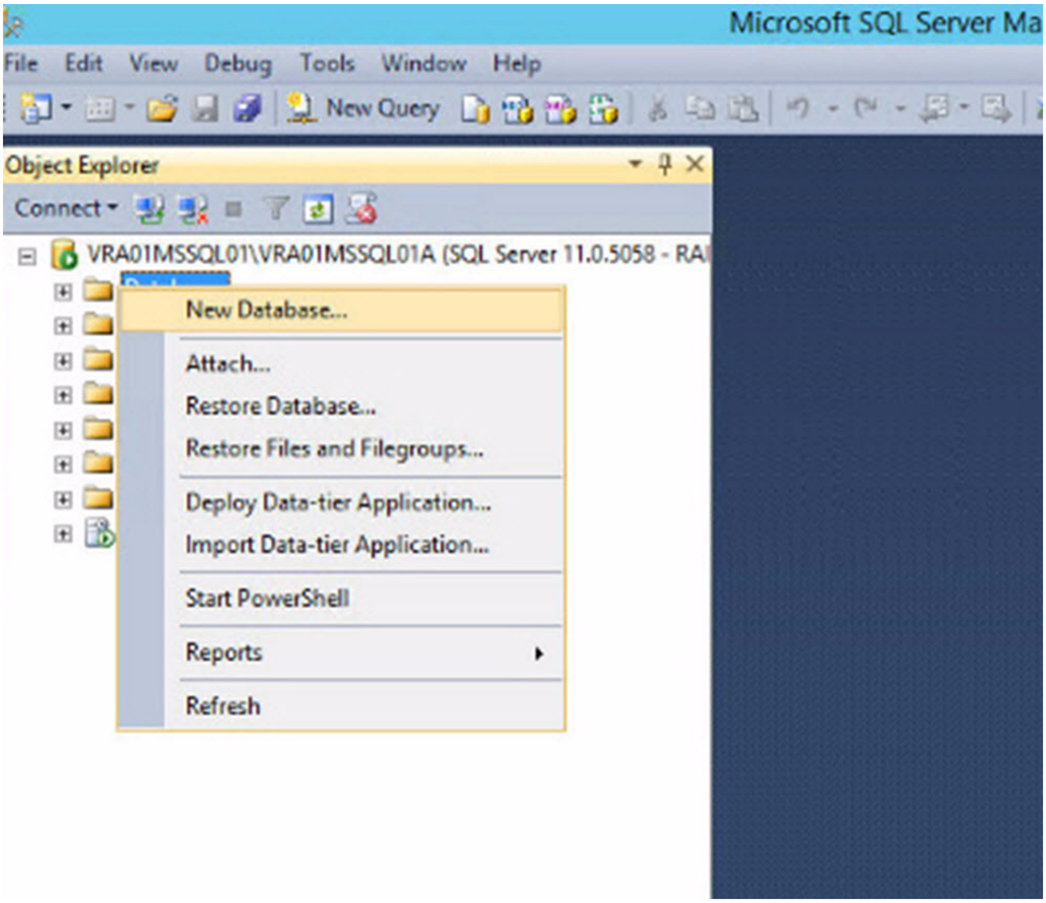
User name: RAINPOLE\Svc-vRA

Password:

□ Remember password

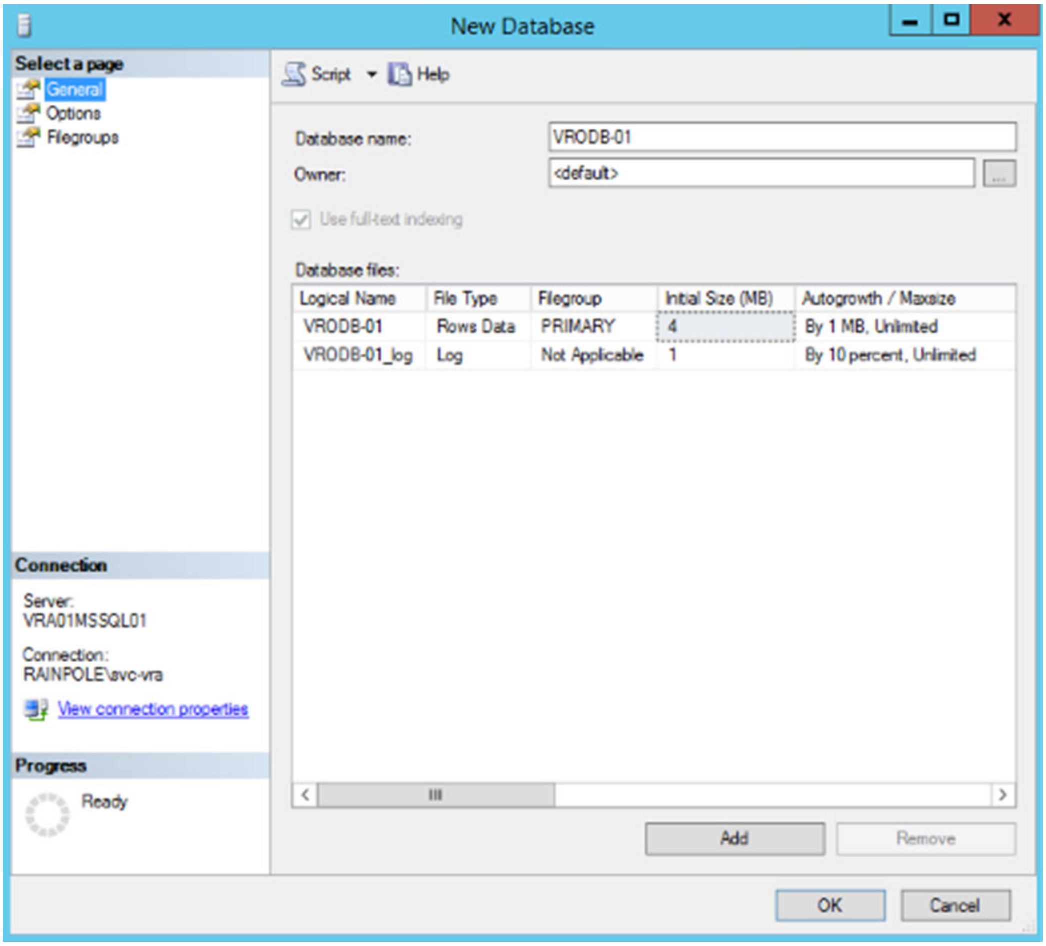
4 In Object Explorer, expand the server instance **VRA01MSSQL01**.

5 Right-click the **Databases** folder, and click **New Database**.


Microsoft SQL Server Ma
File Edit View Debug Tools Window Help
New Query
Object Explorer
Connect
VRA01MSSQL01\VRA01MSSQL01A (SQL Server 11.0.5058 - RA
New Database...
Attach...
Restore Database...
Restore Files and Filegroups...
Deploy Data-tier Application...
Import Data-tier Application...
Start PowerShell
Reports
Refresh

The **New Database** dialog box displays.

6 On the General page of the New Database dialog box, enter `VRODB-01` in the **Database name** text box.



Database name: VRODB-01

Owner: <default>

☑ Use full-text indexing

Database files:

Logical Name	File Type	Filegroup	Initial Size (MB)	Autogrowth / Maxsize
VRODB-01	Rows Data	PRIMARY	4	By 1 MB, Unlimited
VRODB-01_log	Log	Not Applicable	1	By 10 percent, Unlimited

Server:
VRA01MSSQL01

Connection:
RAINPOLE\svc-vra

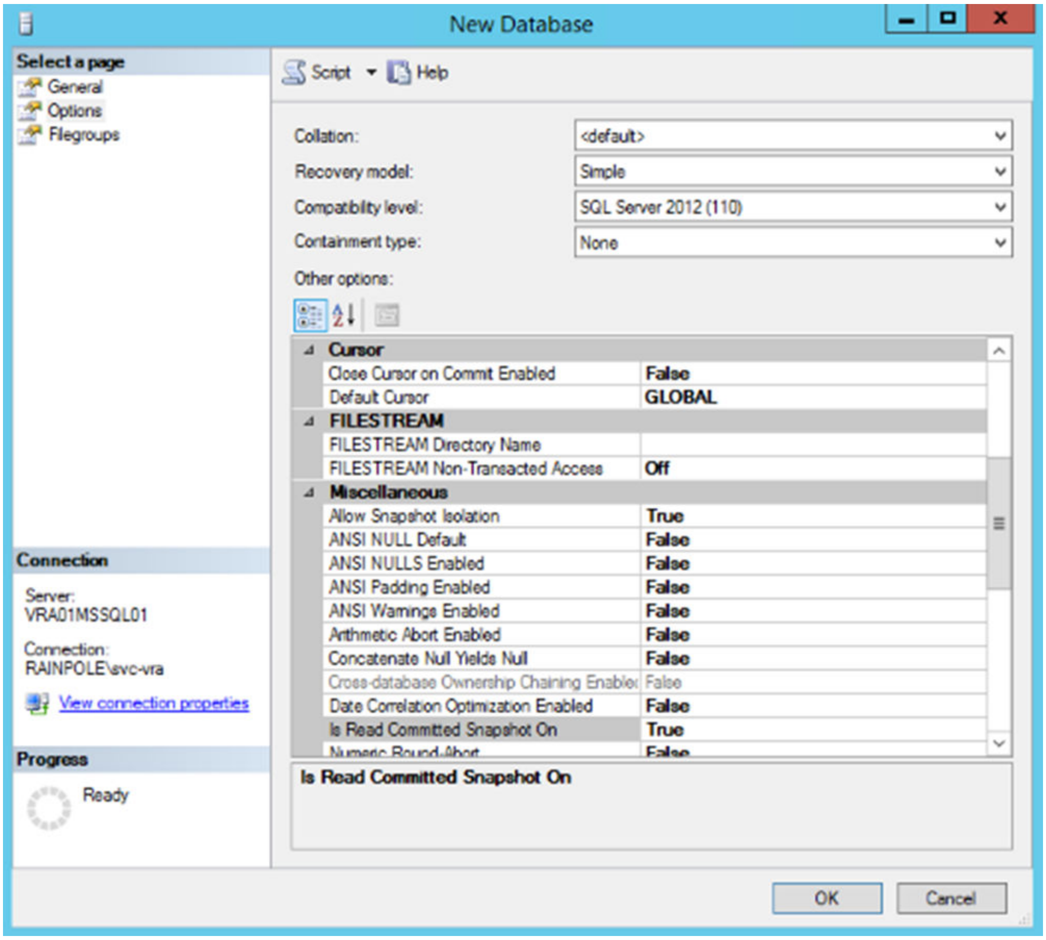
7 Select the **Options** page.

8 On the **Options** page, specify the following values, and click **OK**.

a Select **Simple** from the **Recovery model** drop-down menu.

b In the **Miscellaneous** text box, specify **True** for the settings listed in the table below.

Setting	Value
Allow Snapshot Isolation	True
Is Read Committed Snapshot On	True



Server:
VRA01MSSQL01

Connection:
RAINPOLE\svc-vra

Collation: <default>

Recovery model: Simple

Compatibility level: SQL Server 2012 (110)

Containment type: None

Other options:

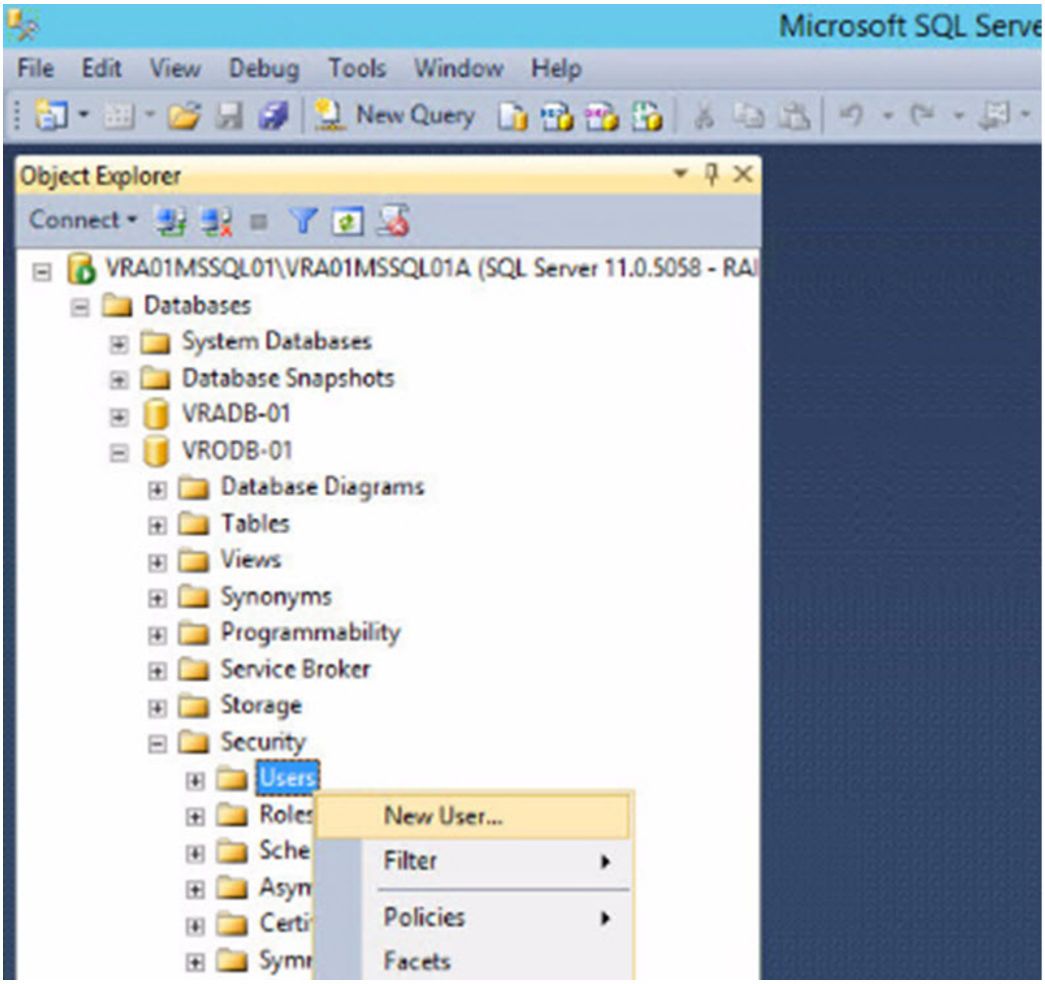
Cursor	
Close Cursor on Commit Enabled	False
Default Cursor	GLOBAL
FILESTREAM	
FILESTREAM Directory Name	
FILESTREAM Non-Transacted Access	Off
Miscellaneous	
Allow Snapshot Isolation	True
ANSI NULL Default	False
ANSI NULLS Enabled	False
ANSI Padding Enabled	False
ANSI Warnings Enabled	False
Arithmetic Abort Enabled	False
Concatenate Null Yields Null	False
Cross-database Ownership Chaining Enabled	False
Date Correlation Optimization Enabled	False
Is Read Committed Snapshot On	True
Numeric Round-Abort	False

Is Read Committed Snapshot On

9 In the **Object Explorer Details** pane, expand the **VRODB-01** database server.

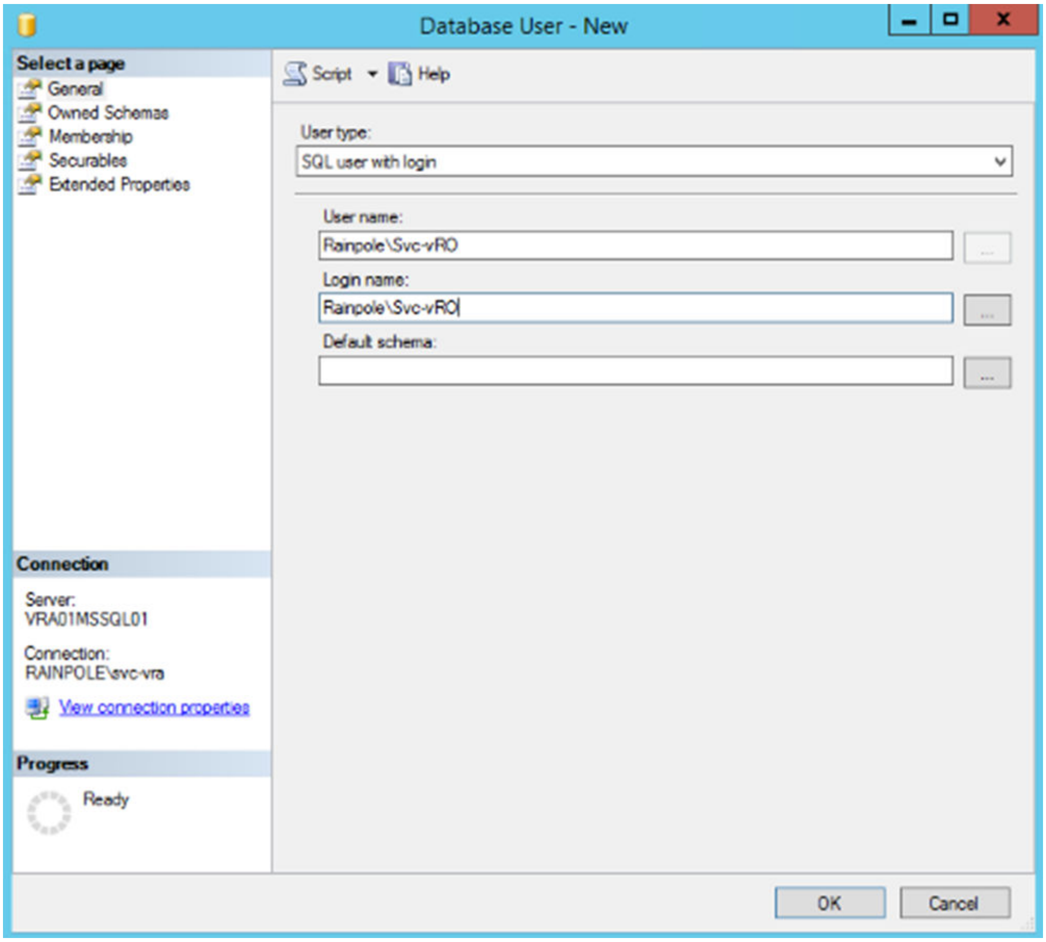
10 Expand the **Security** folder, then expand the **Users** folder.

11 Right-click the **User** folder and click **New User**.



12 In the **User name** text box enter the vRealize Orchestrator service account name **`RAINPOLE\svc-vro`**.

Setting	Value
User type	SQL user with login
User name	Rainpole\svc-vro
Login name	Rainpole\svc-vro



User type: SQL user with login

User name: Rainpole\Svc-vRO

Login name: Rainpole\Svc-vRO

Default schema:

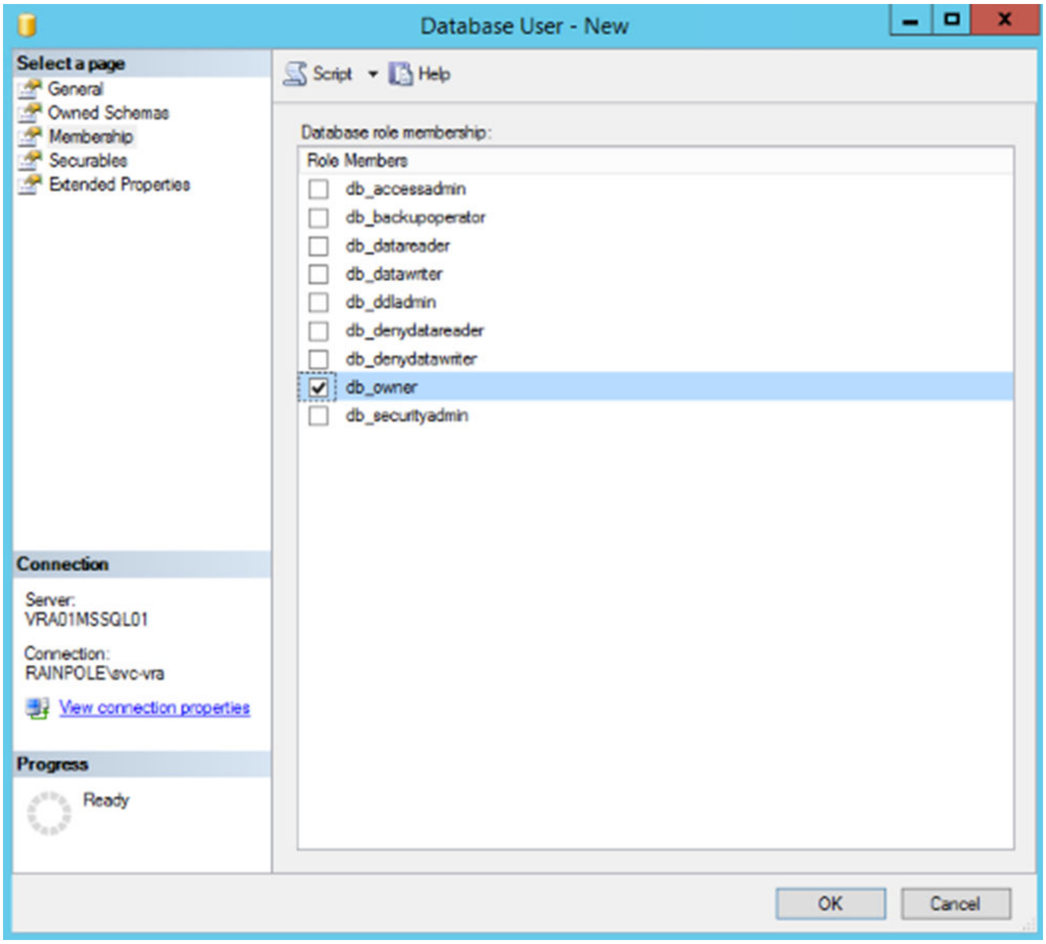
Server: VRA01MSSQL01

Connection: RAINPOLE\svc-vra

13 Select the **Membership** page.

The **Database User - New** page appears.

14 In the **Database role membership** list item field, select the **db_owner** check box, and click **OK**.



Database role membership:

Role Members
□ db_accessadmin
□ db_backupoperator
□ db_datareader
□ db_datawriter
□ db_ddladmin
□ db_denydatareader
□ db_denydatawriter
☑ db_owner
□ db_securityadmin

Connection

Server:
VRA01MSSQL01

Connection:
RAINPOLE\svc-vra

Configure Network Access for Distributed Transaction Coordinator in Region A

You configure network access and security between vRealize Automation and your Microsoft SQL Server database using Microsoft Distributed Transaction Coordinator (MSDTC). MSDTCcoordinates transactions that update two or more transaction-protected resources, such as databases, message queues, files systems, and so on. These transaction-protected resources may be on a single computer, or distributed across many networked computers.

Procedure

1 Log in to the `VRA01MSSQL01.rainpole.local` by using a Remote Desktop Protocol (RDP) client.

   a Open an RDP connection to the virtual machine `VRA01MSSQL01.rainpole.local`.

   b Log in using the following credentials.

Setting	Value
User name	Windows administrator user
Password	*windows_administrator_password*

2 From the **Start** menu, click **Run**, type `comexp.msc` in the **Open** text box, and click **OK**.

The Component Services manager displays. Component Services lets you manage Component Object Model (COM+) applications.

3 Using the navigation tree in the left-side pane, expand **Component Services > Computers > My Computer > Distributed Transaction List > Local DTC**.

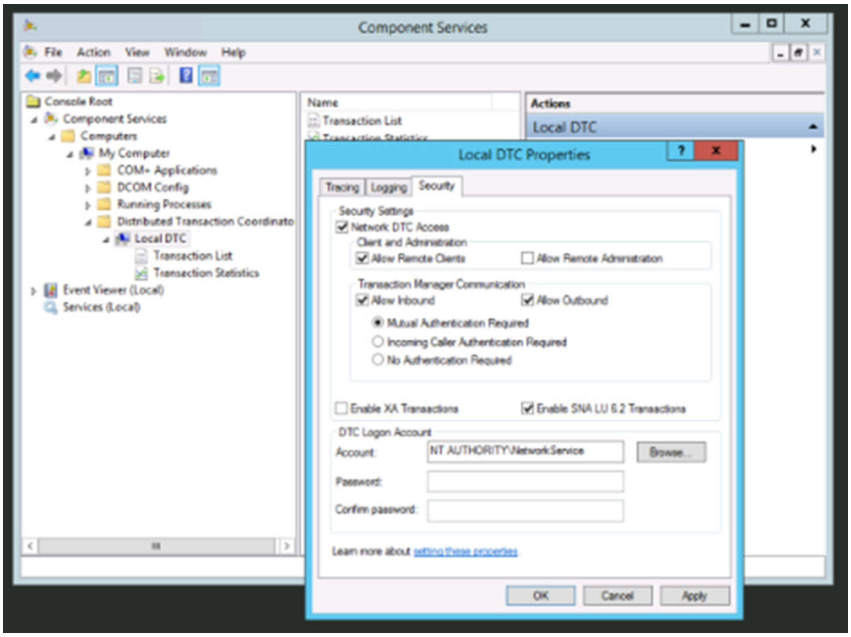
4 Right-click **Local DTC** and click **Properties**.

The **Local DTC Properties** dialog box displays.

5 Click the **Security** tab in the **Local DTC Properties** dialog box.

6 On the **Security** tab, configure the following values, and click **OK**.

Setting	Value
Network DTC Access	Selected
Allow Remote Clients	Selected
Allow Remote Administration	Deselected
Allow Inbound	Selected
Allow Outbound	Selected
Mutual Authentication Required	Selected
Enable XA Transactions	Deselected
Enable SNA LU 6.2 Transactions	Selected
Account	Leave the default setting (NT AUTHORITY\NetworkService)
Password	Leave blank



Security Settings

☑ Network DTC Access

Client and Administration

☑ Allow Remote Clients ☐ Allow Remote Administration

Transaction Manager Communication

☑ Allow Inbound ☑ Allow Outbound

● Mutual Authentication Required

○ Incoming Caller Authentication Required

○ No Authentication Required

☐ Enable XA Transactions ☑ Enable SNA LU 6.2 Transactions

DTC Logon Account

Account: NT AUTHORITY\NetworkService

Password:

Confirm password:

Learn more about setting these properties.

7 Click **Yes** to restart the MSDTC Service.

8 Click **OK** to confirm that the MSDTC Service has successfully restarted.

9 Close the Component Services manager.

Allow MS SQL Server and MSDTC access through Windows Firewall for vRealize Automation in Region A

You can configure Windows Firewall to allow or block specific traffic. For vRealize Automation to function correctly, ensure that network access to Microsoft Distributed Transaction Coordinator (MSDTC) and SQL Server is configured to allow access.

Procedure

1 Log in to the `VRA01MSSQL01.rainpole.local` by using a Remote Desktop Protocol (RDP) client.

   a Open an RDP connection to the virtual machine `VRA01MSSQL01.rainpole.local`.

   b Log in using the following credentials.

Setting	Value
User name	Windows administrator user
Password	*windows_administrator_password*

2 From the **Start** menu, click **Run**, type **`WF.msc`** in the **Open** text box, and click **OK**.

   The Windows Firewall with Advanced Security dialog box appears. You use Windows Firewall with Advanced Security to configure firewall properties for each network profile.

3 Allow Access for Microsoft SQL Server on TCP Port 1433.

   a In the navigation pane right-click **Windows Firewall with Advanced Security**, select and right-click **Inbound Rules**, and click **New Rule** in the action pane.

   The **New Inbound Rule Wizard** appears.

   b On the Rule Type page of the **New Inbound Rule Wizard**, select the **Port** radio button, and click **Next**.

   c On the Protocol and Ports page, select **TCP** and enter the port number **`1433`** in the **Specific local ports** text box, and click **Next**.

   d On the Action page, select **Allow the connection**, and click **Next**.

   e On the Profile page, select the **Domain**, **Private**, and **Public** profiles, and click **Next**.

   f On the Name page, enter a ***`Name`*** and ***`Description`*** for this rule, and click **Finish**.

4 Allow access for Microsoft Distributed Transaction Coordinator.

   a In the navigation pane right-click **Windows Firewall with Advanced Security**, select and right-click **Inbound Rules**, and click **New Rule** in the action pane.

   b On the Rule Type page click **Predefined**, click **Distributed Transaction Coordinator**, and click **Next**.

c On the Predefined Rules page, select all rules for **Distributed Transaction Coordinator (RPC-EPMAP)**, **Distributed Transaction Coordinator (RPC)**, **Distributed Transaction Coordinator (TCP-In)**, and click **Next**.

d On the Actionpage, select **Allow the connection**, and click **Finish**.

5 Exit the **Windows Firewall with Advanced Security** wizard.

Configure Service Account Privileges in Region A

For you to provision virtual machines and logical networks, configure privileges for vRealize Automation for the service account svc-vra@rainpole.local on both the Compute vCenter Server and the Compute Cluster NSX instance.

Configure Service Account Privileges on the Compute vCenter Server in Region A

Configure Administrator privileges for the svc-vra and svc-vro users on the Compute vCenter Server in Region A.

If you add more Compute vCenter Server instances in the future, perform this procedure on those instances as well.

Procedure

1 Log in to the Compute 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 In the **Navigator** pane, select **Global Inventory Lists > vCenter Servers**.

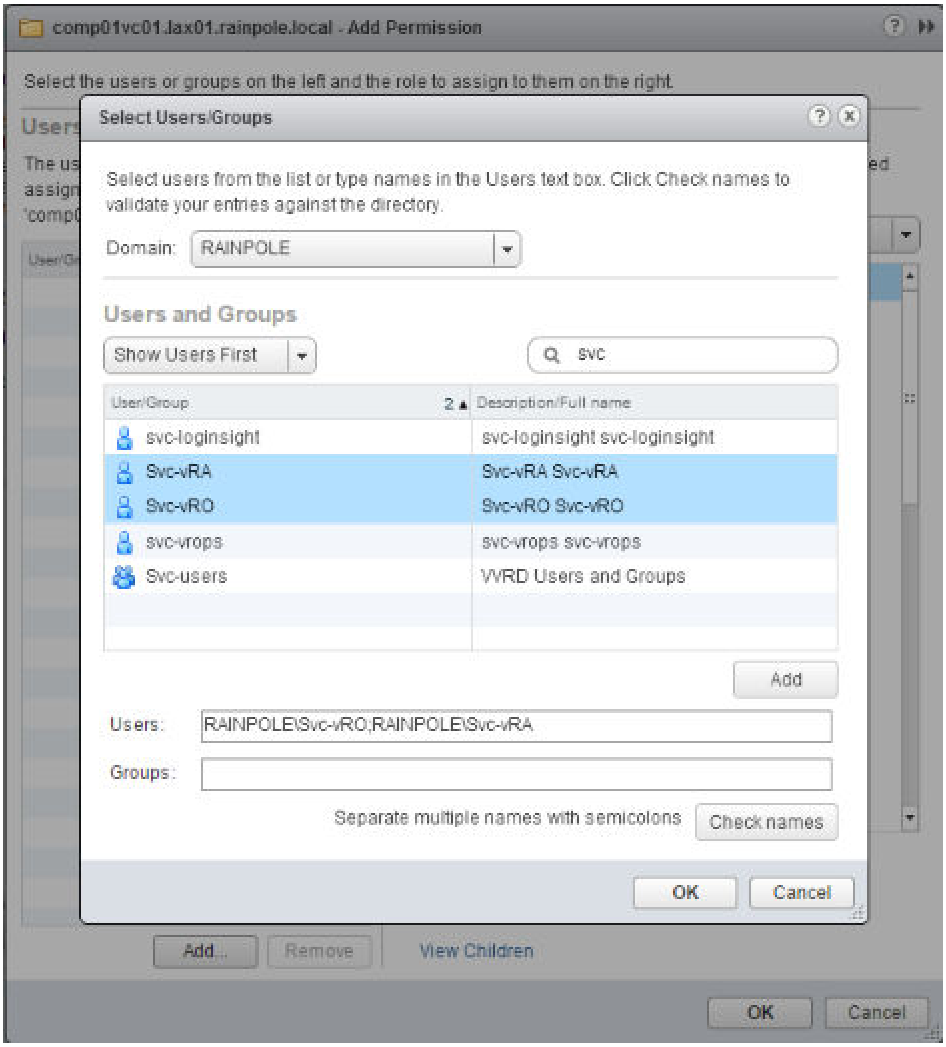
3 Right-click the **comp01vc01.sfo01.rainpole.local** instance and select **Add Permission**.

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` to filter user and group names.

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



comp01vc01.lax01.rainpole.local - Add Permission

Select the users or groups on the left and the role to assign to them on the right.

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

Users and Groups

svc

User/Group	Description/Full name
svc-loginsight	svc-loginsight svc-loginsight
Svc-vRA	Svc-vRA Svc-vRA
Svc-vRO	Svc-vRO Svc-vRO
svc-vrops	svc-vrops svc-vrops
Svc-users	VVRD Users and Groups

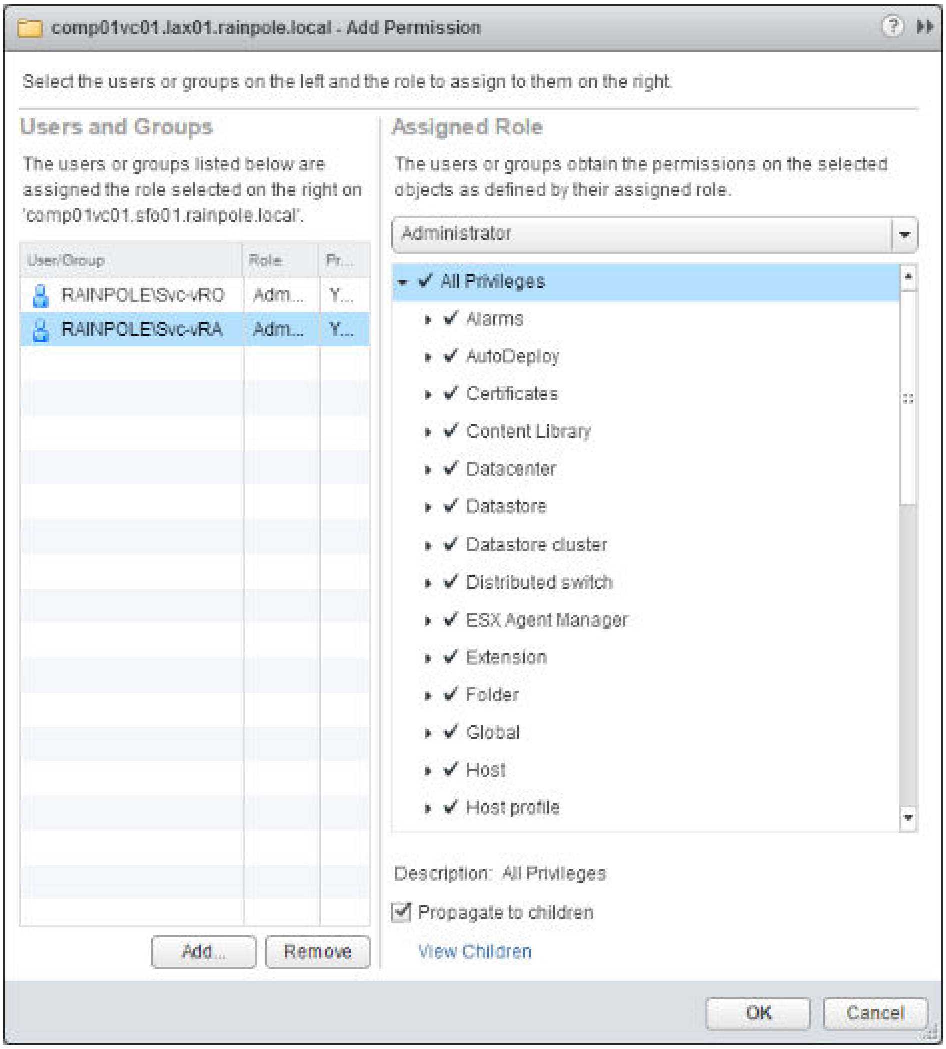
Users: RAINPOLE\Svc-vRO;RAINPOLE\Svc-vRA

Groups:

Separate multiple names with semicolons

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

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



comp01vc01.lax01.rainpole.local - Add Permission

Select the users or groups on the left and the role to assign to them on the right.

Users and Groups

The users or groups listed below are assigned the role selected on the right on 'comp01vc01.sfo01.rainpole.local'.

User/Group	Role	Pr...
RAINPOLE\Svc-vRO	Adm...	Y...
RAINPOLE\Svc-vRA	Adm...	Y...

Assigned Role

The users or groups obtain the permissions on the selected objects as defined by their assigned role.

Administrator

Description: All Privileges

☑ Propagate to children

Configure the Service Account Privilege on the Compute Cluster NSX Instance in Region A

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

Procedure

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

   a Open a Web browser and go to **`https://comp01vc01.sfo01.rainpole.local/vsphere-client`**.

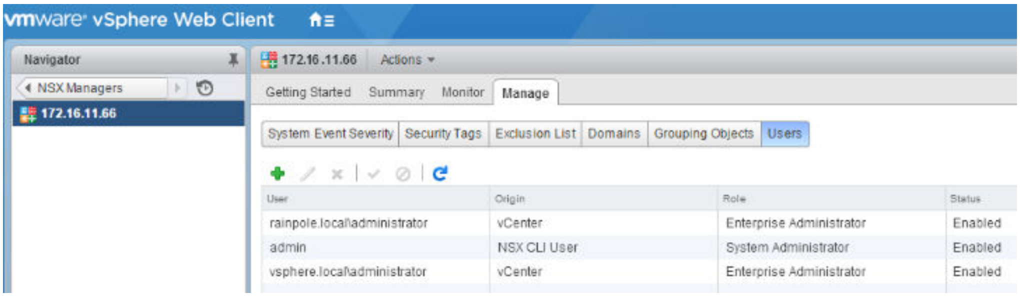
   b Log in using the following credentials.

Setting	Value
User name	administrator@vsphere.local
Password	*vsphere_admin_password*

2 In the **Navigator** pane, select **Networking & Security > NSX Managers**.

3 Double-click the Compute NSX Manager **172.16.11.66**.

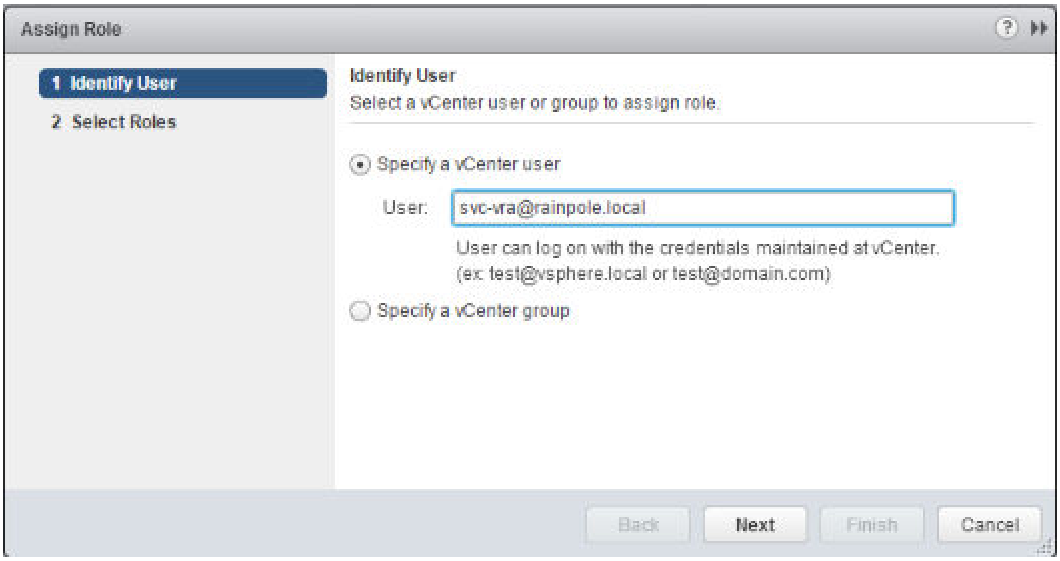
4 Click **Manage**, click **Users**,and click the **Add** icon.



User	Origin	Role	Status
rainpole.local\administrator	vCenter	Enterprise Administrator	Enabled
admin	NSX CLI User	System Administrator	Enabled
vsphere.local\administrator	vCenter	Enterprise Administrator	Enabled

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**.



Identify User

Select a vCenter user or group to assign role.

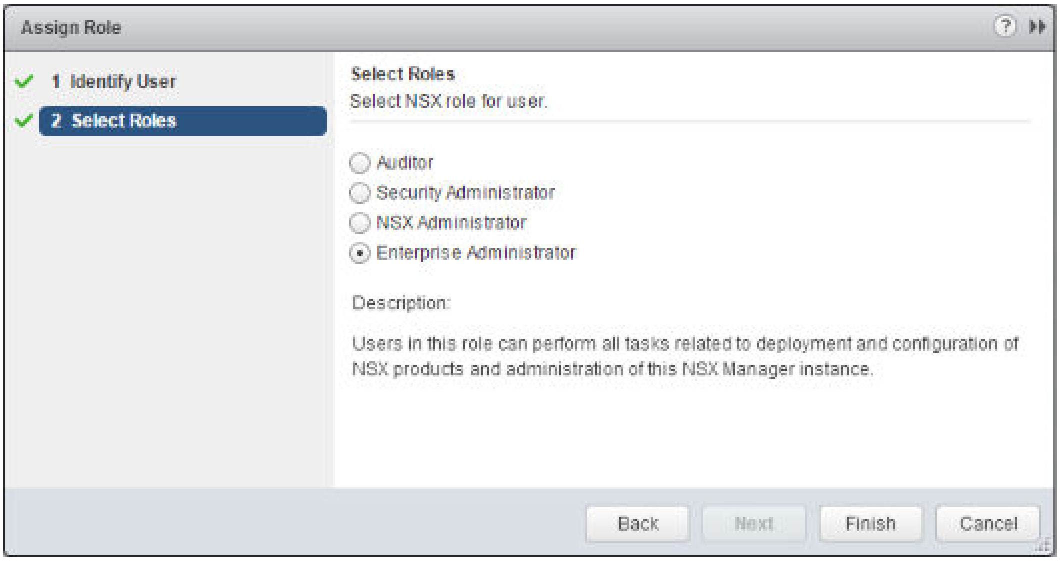
● Specify a vCenter user

User: svc-vra@rainpole.local

User can log on with the credentials maintained at vCenter.
(ex: test@vsphere.local or test@domain.com)

○ Specify a vCenter group

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



Select Roles

Select NSX role for user.

○ Auditor
○ Security Administrator
○ NSX Administrator
● Enterprise Administrator

Description:

Users in this role can perform all tasks related to deployment and configuration of NSX products and administration of this NSX Manager instance.

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

vRealize Automation Installation in Region A

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.

Load Balancing the Cloud Management Platform in Region A

You configure load balancing for all services and components related to vRealize Automation and vRealize Orchestrator by using an NSX Edge load balancer.

You must configure the load balancer before you deploy the vRealize Automation appliance. This is because you need the virtual IP (VIP) addresses to deploy the vRealize Automation appliance.

Add Virtual IP Addresses to the NSX Load Balancer in Region A

As the first step of configuring load balancing, you add virtual IP Addresses to the edge interfaces.

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*

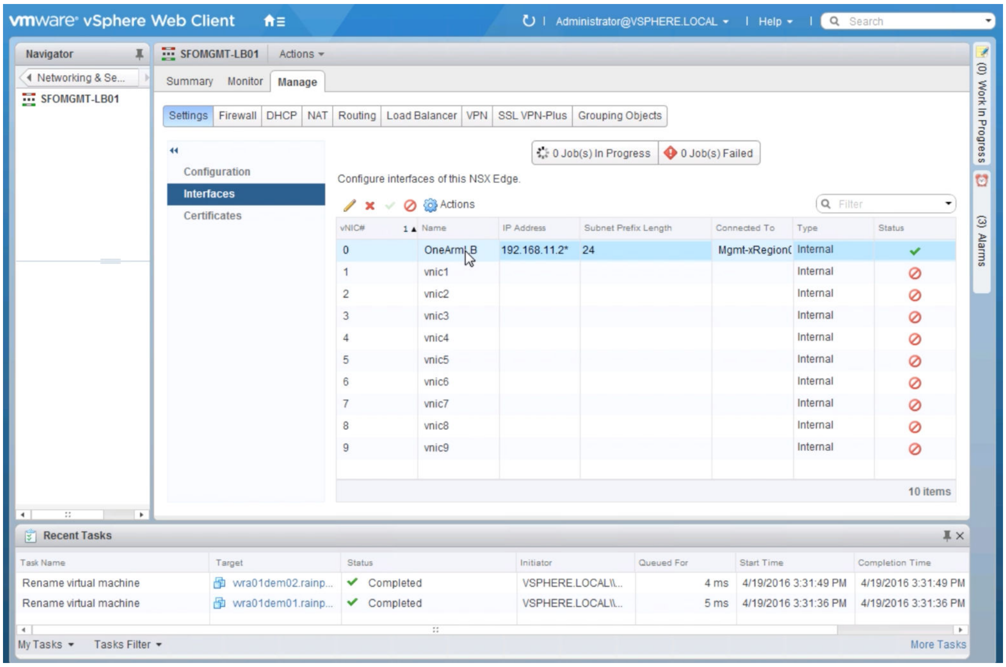
2 Click **Networking & Security**.

3 In the **Navigator**, click **NSX Edges**.

4 From the **NSX Manager** drop-down menu, select **172.16.11.65** as the NSX Manager and double-click the **SFOMGMT-LB01** NSX Edge to edit its network settings.

5 Click the **Manage** tab, click **Settings**, and select **Interfaces**.

6 Select the **OneArmLB** interface and click the **Edit** icon.



Configure interfaces of this NSX Edge.

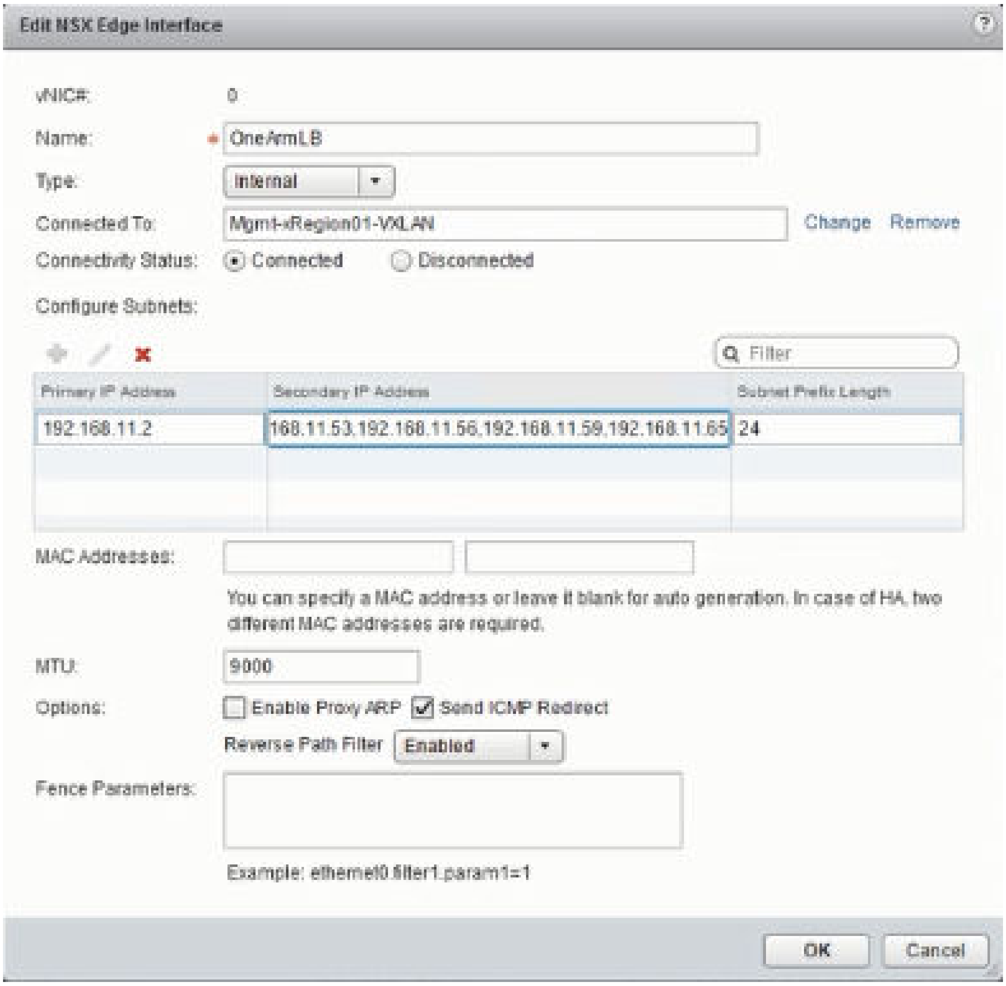
vNIC#	Name	IP Address	Subnet Prefix Length	Connected To	Type	Status
0	OneArmLB	192.168.11.2*	24	Mgmt-xRegion(	Internal	✓
1	vnic1				Internal	⊘
2	vnic2				Internal	⊘
3	vnic3				Internal	⊘
4	vnic4				Internal	⊘
5	vnic5				Internal	⊘
6	vnic6				Internal	⊘
7	vnic7				Internal	⊘
8	vnic8				Internal	⊘
9	vnic9				Internal	⊘

10 items

Task Name	Target	Status	Initiator	Queued For	Start Time	Completion Time
Rename virtual machine	wra01dem02.rainp...	✓ Completed	VSPHERE.LOCAL\\...	4 ms	4/19/2016 3:31:49 PM	4/19/2016 3:31:49 PM
Rename virtual machine	wra01dem01.rainp...	✓ Completed	VSPHERE.LOCAL\\...	5 ms	4/19/2016 3:31:36 PM	4/19/2016 3:31:36 PM

7 In the **Edit NSX Edge Interface** dialog box, add the VIP addresses of the vRealize Automation nodes in the **Secondary IP Addresses** text box.

Setting	Value
Secondary IP Address	192.168.11.53,192.168.11.56,192.168.11.59,192.168.11.65



Edit NSX Edge Interface

vNIC#: 0

Name: * OneArmLB

Type: Internal

Connected To: Mgmt-xRegion01-VXLAN

Connectivity Status: ● Connected ○ Disconnected

Configure Subnets:

Primary IP Address	Secondary IP Address	Subnet Prefix Length
192.168.11.2	168.11.53,192.168.11.56,192.168.11.59,192.168.11.65	24

MAC Addresses:

You can specify a MAC address or leave it blank for auto generation. In case of HA, two different MAC addresses are required.

MTU: 9000

Options: □ Enable Proxy ARP ☑ Send ICMP Redirect

Reverse Path Filter: Enabled

Fence Parameters:

Example: ethernet0.filter1.param1=1

8 Click **OK** to save the configuration.

Create Application Profiles in Region A

Create an application profile to define the behavior of a particular type of network traffic. After configuring a profile, you associate the profile with a virtual server. The virtual server then processes traffic according to the values specified in the profile. Using profiles enhances your control over managing network traffic, and makes traffic-management tasks easier and more efficient.

You repeat this procedure twice to create two application profiles.

Procedure

1 Log in to the Management 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.

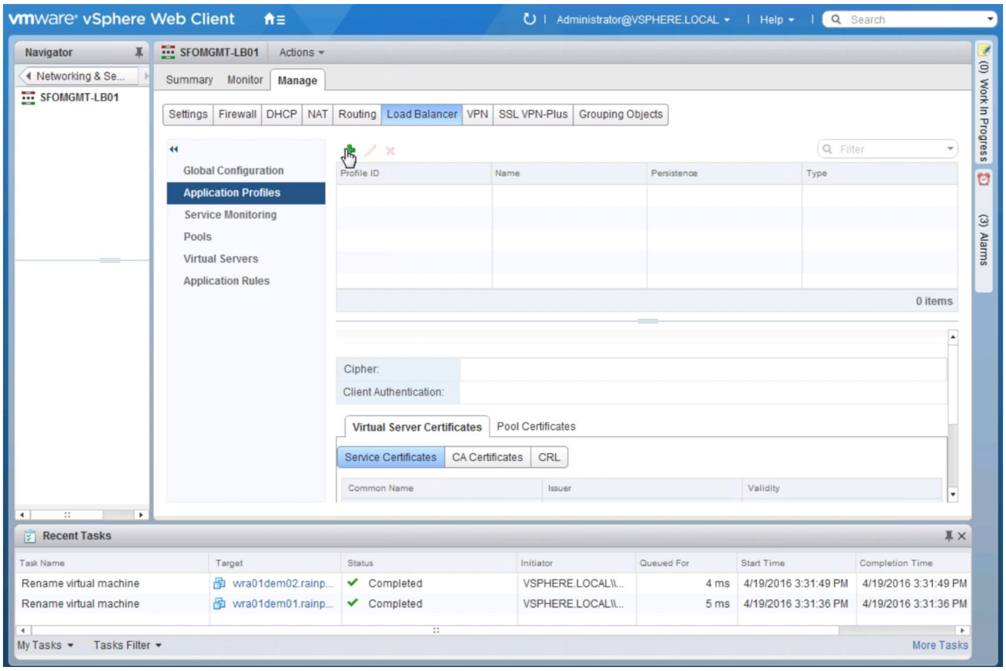
Setting	Value
User name	administrator@vsphere.local
Password	*vsphere_admin_password*

2 Click **Networking & Security**.

3 In the **Navigator**, click **NSX Edges**.

4 From the **NSX Manager** drop-down menu, select **172.16.11.65** as the NSX Manager and double-click the **SFOMGMT-LB01** NSX Edge to manage its network settings.

5 Click the **Manage** tab, click **Load Balancer**, and select **Application Profiles**.

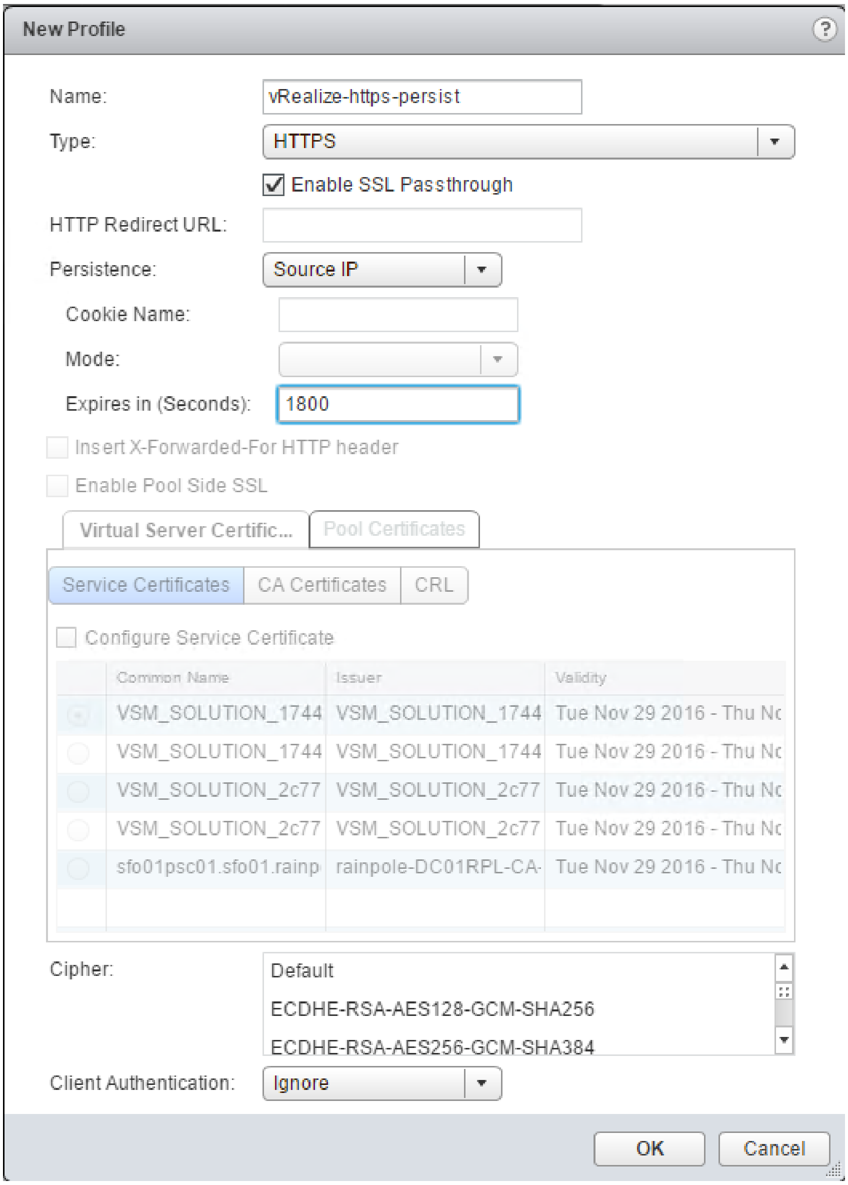


Task Name	Target	Status	Initiator	Queued For	Start Time	Completion Time
Rename virtual machine	wra01dem02.rainp...	✓ Completed	VSPHERE.LOCAL\\...	4 ms	4/19/2016 3:31:49 PM	4/19/2016 3:31:49 PM
Rename virtual machine	wra01dem01.rainp...	✓ Completed	VSPHERE.LOCAL\\...	5 ms	4/19/2016 3:31:36 PM	4/19/2016 3:31:36 PM

6 Click the **Add** icon and in the **New Profile** dialog box, enter the following values.

Setting	Value
Name	vRealize-https-persist
Type	HTTPS
Enable SSL Passthrough	Selected

Setting	Value
Persistence	Source IP
Expires in (Seconds)	1800



New Profile

Name: vRealize-https-persist

Type: HTTPS

☑ Enable SSL Passthrough

HTTP Redirect URL:

Persistence: Source IP

Cookie Name:

Mode:

Expires in (Seconds): 1800

□ Insert X-Forwarded-For HTTP header

□ Enable Pool Side SSL

□ Configure Service Certificate

	Common Name	Issuer	Validity
○	VSM_SOLUTION_1744	VSM_SOLUTION_1744	Tue Nov 29 2016 - Thu Nc
○	VSM_SOLUTION_1744	VSM_SOLUTION_1744	Tue Nov 29 2016 - Thu Nc
○	VSM_SOLUTION_2c77	VSM_SOLUTION_2c77	Tue Nov 29 2016 - Thu Nc
○	VSM_SOLUTION_2c77	VSM_SOLUTION_2c77	Tue Nov 29 2016 - Thu Nc
○	sfo01psc01.sfo01.rainp	rainpole-DC01RPL-CA-	Tue Nov 29 2016 - Thu Nc

Cipher: Default
ECDHE-RSA-AES128-GCM-SHA256
ECDHE-RSA-AES256-GCM-SHA384

Client Authentication: Ignore

7 Click **OK** to save the configuration.

8 Repeat the same steps to create the following application profile.

Setting	Value
Name	vRealize-https
Type	HTTPS
Enable SSL Passthrough	Selected
Persistence	None

Create Service Monitoring in Region A

The service monitor defines health check parameters for the load balancer. You create a service monitor for each component.

Procedure

1 Log in to the Management 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 Click **Networking & Security**.

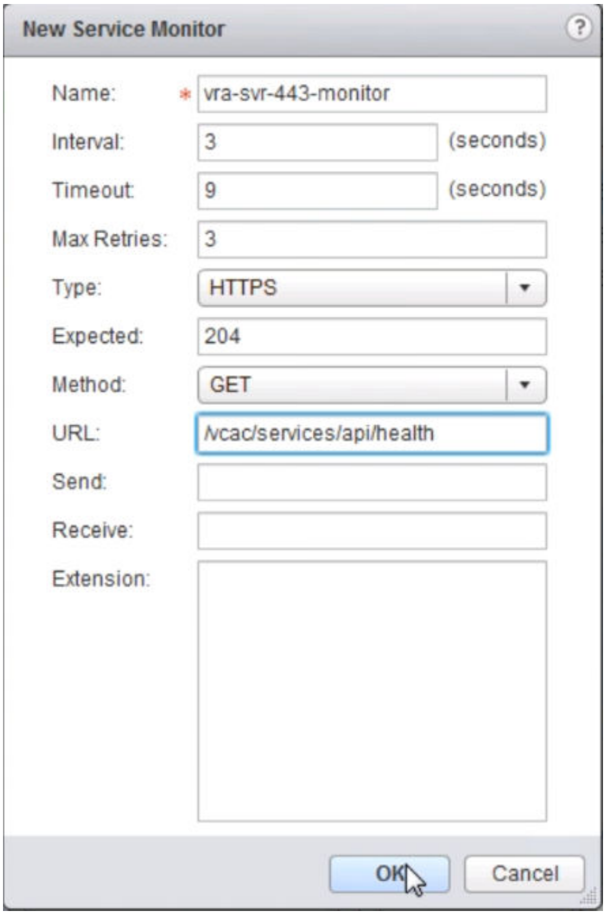
3 In the **Navigator**, click **NSX Edges**.

4 From the **NSX Manager** drop-down menu, select **172.16.11.65** as the NSX Manager and double-click the **SFOMGMT-LB01** NSX Edge to manage its network settings.

5 Click the **Manage** tab, click **Load Balancer**, and select **Service Monitoring**.

6 Click the **Add** icon and in the **New Service Monitor** dialog box, configure the values for the service monitor you are adding, and click **OK**.

Setting	vra-svr-443-monitor	vra-iaas-web-443-monitor	vra-iaas-mgr-443-monitor	vra-vro-8281-monitor
Name	vra-svr-443-monitor	vra-iaas-web-443-monitor	vra-iaas-mgr-443-monitor	vra-vro-8281-monitor
Interval	3	3	3	3
Timeout	9	9	9	9
Max Retries	3	3	3	3
Type	HTTPS	HTTPS	HTTPS	HTTPS
Expected	204			
Method	GET	GET	GET	GET
URL	/vcac/services/api/health	/wapi/api/status/web	/VMPSProvision	/vco/api/healthstatus
Receive		REGISTERED	ProvisionService	RUNNING



Name: *	vra-svr-443-monitor	
Interval:	3	(seconds)
Timeout:	9	(seconds)
Max Retries:	3	
Type:	HTTPS	
Expected:	204	
Method:	GET	
URL:	/vcac/services/api/health	
Send:		
Receive:		
Extension:		

7 Repeat Step 6 to create a service monitor for each component.

Upon completion, verify that you have successfully entered the monitor names and their respective configuration values.

Create Server Pools in Region A

A server pool consists of back-end server members. After you create a server pool, you associate a service monitor with the pool to manage and share the back-end servers flexibly and efficiently.

The following considerations explain the design of the server pools configuration.

- The configuration uses `NONE` as health monitor for all server pools. Until vRealize Automation is fully installed and started, the health monitor marks pool members as offline. Health monitors indicate the status of pool members correctly, only after vRealize Automaton is fully installed and initialized.
- The configuration disables the second pool member of 3 vRealize Automation VIPs (vra-svr-443, vra-iaas-web-443, vra-iaas-mgr-443). During the installation or power cycle of vRealize Automation, the service inside the second node might not be installed or initialized yet. In this period of time, if the load balancer passes a request to the second node, the request fails. If the second pool member is not disabled, you can experience random failures during vRealize Automation installation, and service initialization or registration failure during a vRealize Automation power cycle.

Perform the procedure multiple times to configure five different server pools.

Table 3-3. Server Pools for the Cloud Management Platform in Region A

			Members					
Pool Name	Algorithm	Monitors	Enable Member	Member Name	IP address	Port	Monitor Port	Weight
vra-svr-443	ROUND-ROBIN	NONE	Yes	vra01svr01a	192.168.11.51	443	443	1
			No	vra01svr01b	192.168.11.52			1
vra-iaas-web-443	ROUND-ROBIN	NONE	Yes	vra01iws01a	192.168.11.54	443	443	1
			No	vra01iws01b	192.168.11.55			1
vra-iaas-mgr-443	ROUND-ROBIN	NONE	Yes	vra01ims01a	192.168.11.57	443	443	1
			No	vra01ims01b	192.168.11.58			1
vra-vro-8281	ROUND-ROBIN	NONE	Yes	vra01vro01a	192.168.11.63	8281	8281	1
			No	vra01vro01b	192.168.11.64			1
vra-svr-8444	ROUND-ROBIN	NONE	Yes	vra01svr01a	192.168.11.51	8444	443	1
			Yes	vra01svr01b	192.168.11.52			1

Procedure

1 Log in to the Management 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.

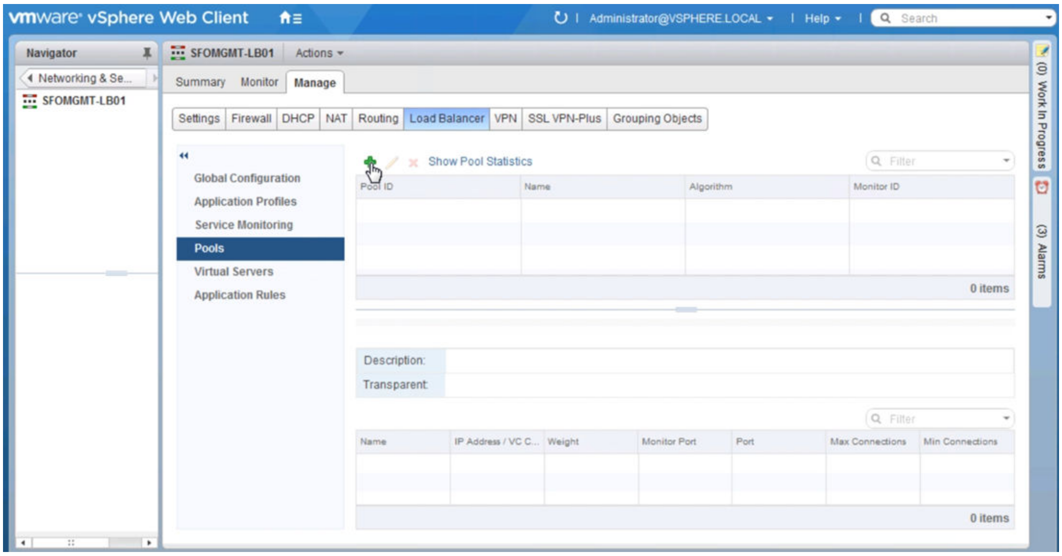
Setting	Value
User name	administrator@vsphere.local
Password	*vsphere_admin_password*

2 Click **Networking & Security**.

3 In the **Navigator**, click **NSX Edges**.

4 From the **NSX Manager** drop-down menu, select **172.16.11.65** as the NSX Manager and double-click the **SFOMGMT-LB01** NSX Edge to manage its network settings.

5 Click the **Manage** tab, click **Load Balancer**, and select **Pools**.



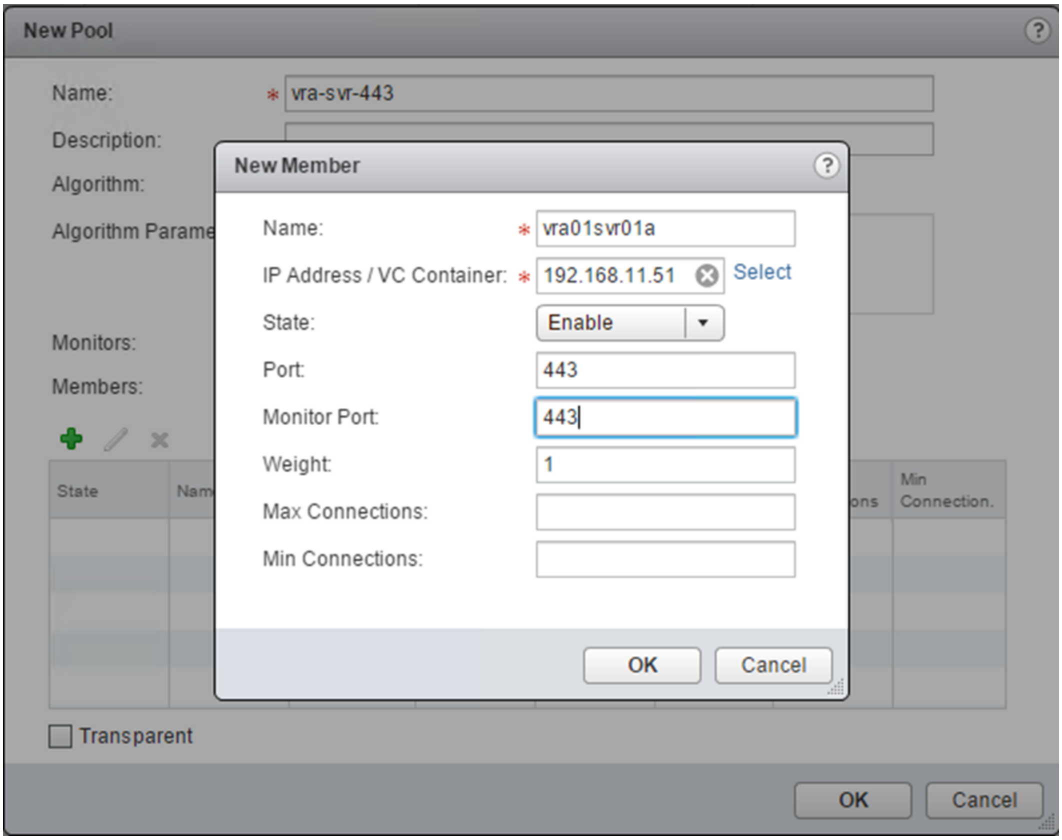
6 Click the **Add** icon and in the **New Pool** dialog box, enter the following values.

Setting	Value
Name	vra-svr-443
Algorithm	ROUND-ROBIN
Monitors	NONE

7 **New Members** dialog box, click the **Add** icon to add the first pool member.

8 In the **New Member** dialog box, enter the following values, and click **OK**.

Setting	Value
Name	vra01svr01a
IP Address/VC Container	192.168.11.51
State	Enable
Port	443
Monitor Port	443
Weight	1



New Pool

Name: * vra-svr-443

Description:

Algorithm:

Algorithm Parame

Monitors:

Members:

New Member

Name: * vra01svr01a

IP Address / VC Container: * 192.168.11.51

State: Enable

Port: 443

Monitor Port: 443

Weight: 1

Max Connections:

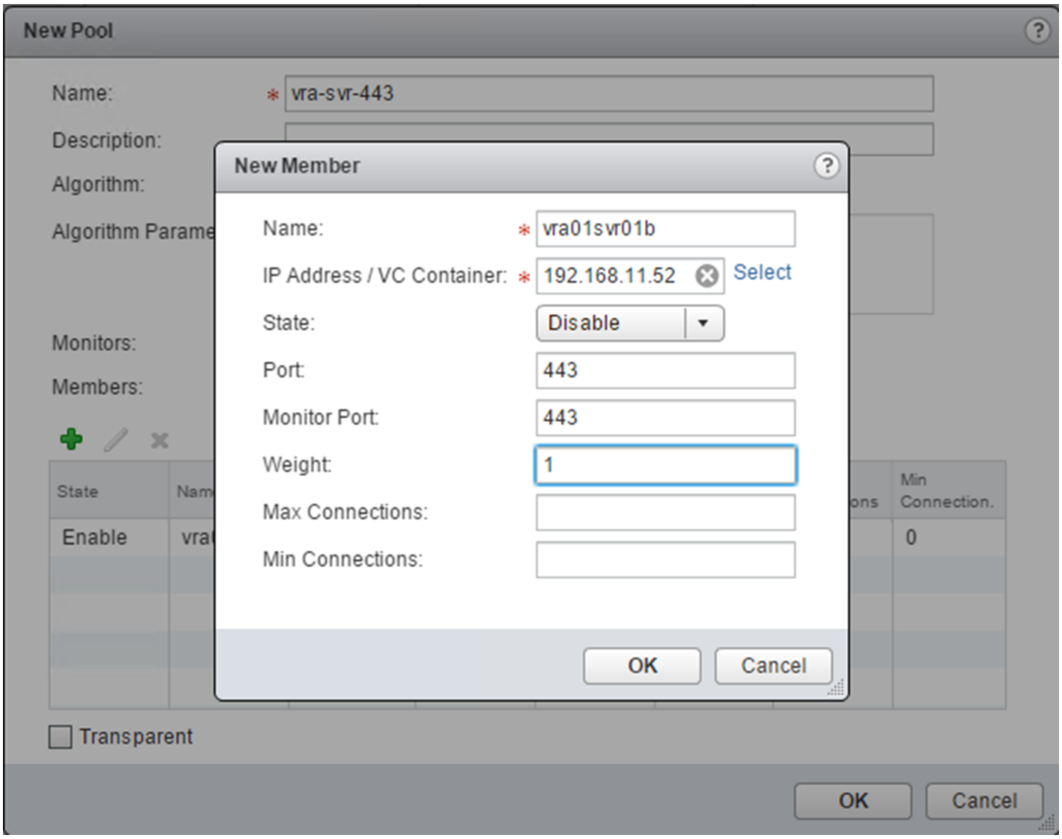
Min Connections:

□ Transparent

9 Under **Members**, click the **Add** icon to add the second pool member.

10 In the **New Member** dialog box, enter the following values, click **OK** and click **OK** to save the vRealize Automation server pool.

Setting	Description
Name	vra01svr01b
IP Address/VC Container	192.168.11.52
State	Disable
Port	443
Monitor Port	443
Weight	1



New Pool

Name: * vra-svr-443

Enable | vra | 0

New Member

Name: * vra01svr01b

IP Address / VC Container: * 192.168.11.52

State: Disable

Port: 443

Monitor Port: 443

Weight: 1

Max Connections:

Min Connections:

11 Repeat the procedure to create the remaining server pools.

Create Virtual Servers in Region A

After load balancing is set up, the NSX load balancer distributes network traffic across multiple servers. When a virtual server receives a request, it chooses the appropriate pool to send traffic to. Each pool consists of one or more members. You create virtual servers for all of the configured server pools.

Procedure

1 Log in to the Management 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.

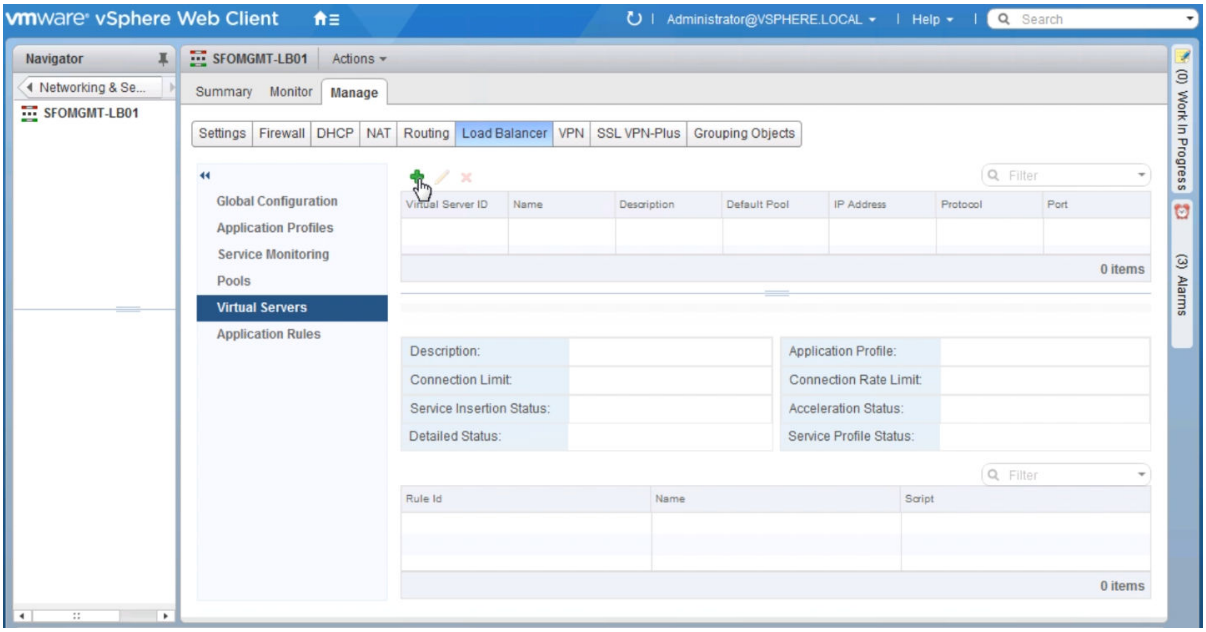
Setting	Value
User name	administrator@vsphere.local
Password	*vsphere_admin_password*

2 Click **Networking & Security**.

3 In the **Navigator**, click **NSX Edges**.

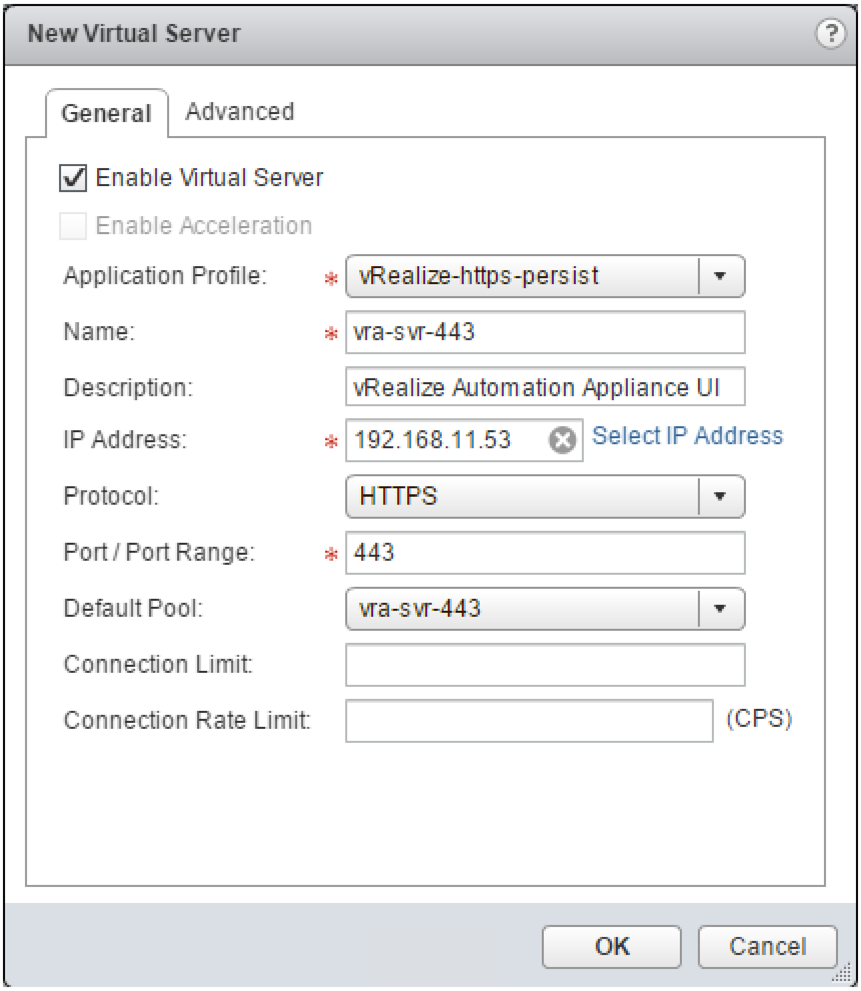
4 From the **NSX Manager** drop-down menu, select **172.16.11.65** as the NSX Manager and double-click the **SFOMGMT-LB01** NSX Edge to manage its network settings.

5 Click the **Manage** tab, click **Load Balancer**, and select **Virtual Servers**.



6 Click the **Add** icon, and in the **New Virtual Server** dialog box configure the values for the virtual server you are adding, and click **OK**.

Setting	vra-svr-443	vra-iaas-web-443	vra-iaas-mgr-443	vra-vro-8281	vra-svr-8444
Enable Virtual server	Selected	Selected	Selected	Selected	Selected
Application Profile	vRealize-https-persist	vRealize-https-persist	vRealize-https	vRealize-https	vRealize-https-persist
Name	vra-svr-443	vra-iaas-web-443	vra-iaas-mgr-443	vra-vro-8281	vra-svr-8444
Description	vRealize Automation Appliance UI	vRealize Automation IaaS Web UI	vRealize Automation IaaS Manager	vRealize Automation Orchestrator	vRealize Automation Remote Console Proxy
IP Address	192.168.11.53	192.168.11.56	192.168.11.59	192.168.11.65	192.168.11.53
Protocol	HTTPS	HTTPS	HTTPS	HTTPS	HTTPS
Port	443	443	443	8281	8444
Default Pool	vra-svr-443	vra-iaas-web-443	vra-iaas-mgr-443	vra-vro-8281	vra-svr-8444



☑ Enable Virtual Server

□ Enable Acceleration

Application Profile: *	vRealize-https-persist
Name: *	vra-svr-443
Description:	vRealize Automation Appliance UI
IP Address: *	192.168.11.53
Protocol:	HTTPS
Port / Port Range: *	443
Default Pool:	vra-svr-443
Connection Limit:	
Connection Rate Limit:	(CPS)

7 Repeat Step 6 to create a virtual server for each component. Upon completion, verify that you have successfully entered the virtual server names and their respective configuration values.

Deploy the vRealize Automation Appliance in Region A

The vRealize Automation appliance is a pre-configured virtual appliance that contains the vRealize Automation server.

The server includes the vRealize Automation appliance product console, which provides a single portal for self-service provisioning and management of cloud services, authoring, administration, and governance.

During deployment of the virtual appliances, a PostgreSQL appliance database is created automatically on the first vRealize Automation appliance. A replica database can be installed on a second vRealize Automation appliance to create a high-availability environment.

Perform this procedure twice to deploy two appliances by using the configuration values for host A for the first appliance, and the configuration values for host B for the second appliance.

Setting	Values for Host A	Values for Host B
Name	vra01svr01a.rainpole.local	vra01svr01b.rainpole.local
Select a folder or datacenter	vRA01	vRA01
Network	Mgmt-xRegion01-VXLAN (192.168.11.x)	Mgmt-xRegion01-VXLAN (192.168.11.x)
Cluster	SFO01-Mgmt01	SFO01-Mgmt01
Virtual Disk Format	Thin provision	Thin provision
VM Storage Policy	vSAN Default Storage Policy	vSAN Default Storage Policy
Datastore	SFO01A-VSAN01-MGMT01	SFO01A-VSAN01-MGMT01
Enable SSH service in the appliance	Selected	Selected
Hostname	vra01svr01a.rainpole.local	vra01svr01b.rainpole.local
Initial Root Password	*vra_appA_root_password*	*vra_appB_root_password*
Default gateway	192.168.11.1	192.168.11.1
Domain Name	rainpole.local	rainpole.local
Domain Name Servers	172.16.11.4,172.17.11.4	172.16.11.4,172.17.11.4
Domain Search Path	rainpole.local,sfo01.rainpole.local,lax01.rainpole.local	rainpole.local,sfo01.rainpole.local,lax01.rainpole.local
Network 1 IP Address	192.168.11.51	192.168.11.52
Network 1 Netmask	255.255.255.0	255.255.255.0

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 In the Navigator pane, select **Global Inventory Lists** > **vCenter Servers**.

3 Right-click the **mgmt01vc01.sfo01.rainpole.local** object and select **Deploy OVF Template**.

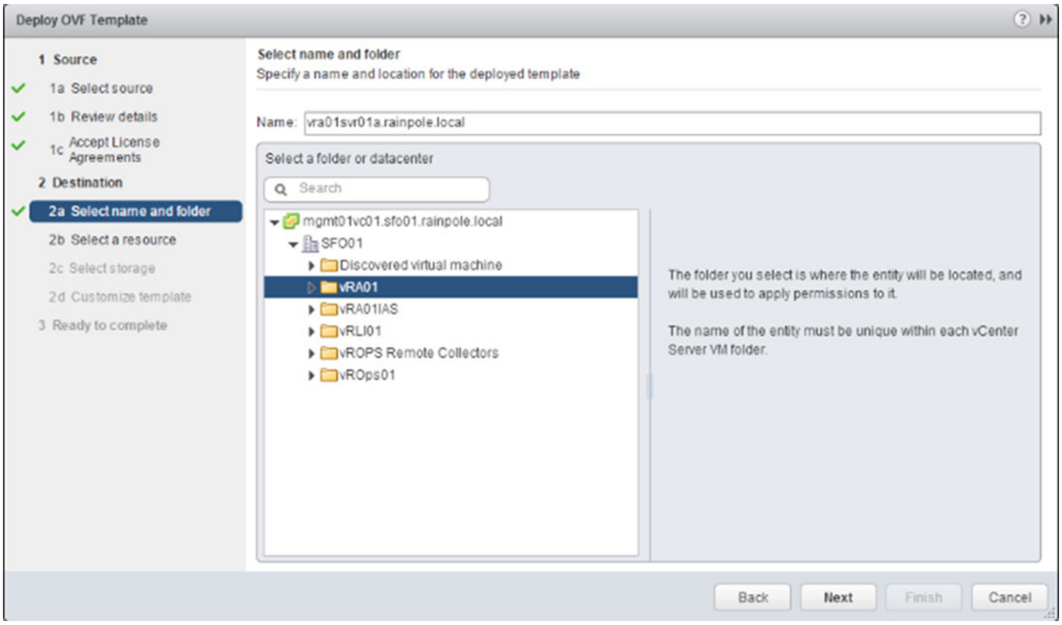
4 On the **Select source** page, select **Local file**, browse to the location of the vRealize Automation Virtual Machine Template file on your file system, and click **Next**.

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

6 On the **Accept License Agreements** page, accept the end user license agreements and click **Next**.

7 On the **Select name and folder** page, enter the following information, and click **Next**.

Setting	Value
Name	vra01svr01a.rainpole.local
Select a folder or datacenter	vRA01



Deploy OVF Template

Select name and folder

Specify a name and location for the deployed template

Name: vra01svr01a.rainpole.local

Select a folder or datacenter: vRA01

The folder you select is where the entity will be located, and will be used to apply permissions to it.

The name of the entity must be unique within each vCenter Server VM folder.

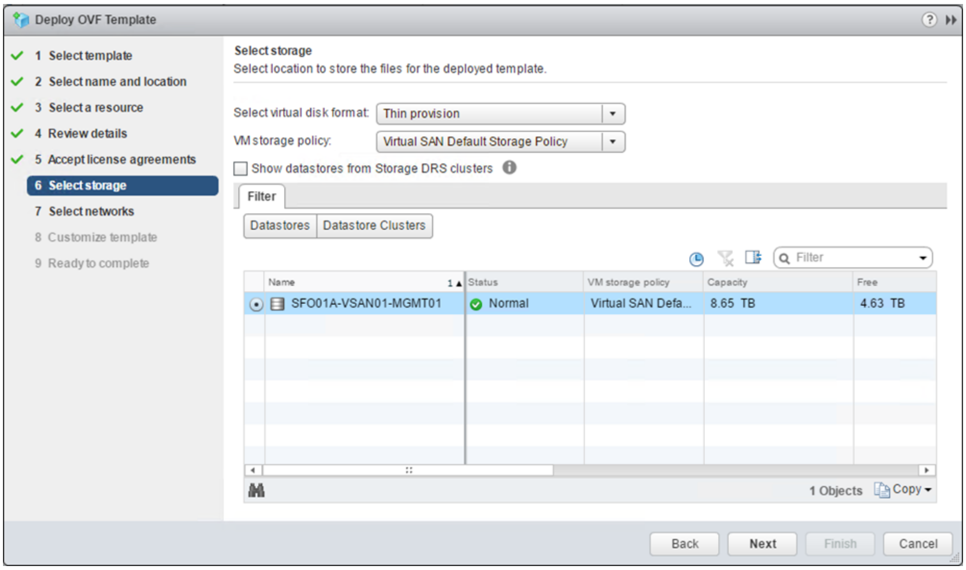
8 On the **Select a Resource** page, select cluster **SFO01-Mgmt01** and click **Next**.

9 On the **Select storage** page, select the datastore.

   a Select **Thin Provision** from the **Select virtual disk format** drop-down menu.

   b Select **vSAN Default Storage Policy** from the **VM storage policy** drop-down menu.

   c From the datastore table, select the **SFO01A-VSAN01-MGMT01** vSAN datastore and click **Next**.



Select storage

Select location to store the files for the deployed template.

Select virtual disk format: Thin provision

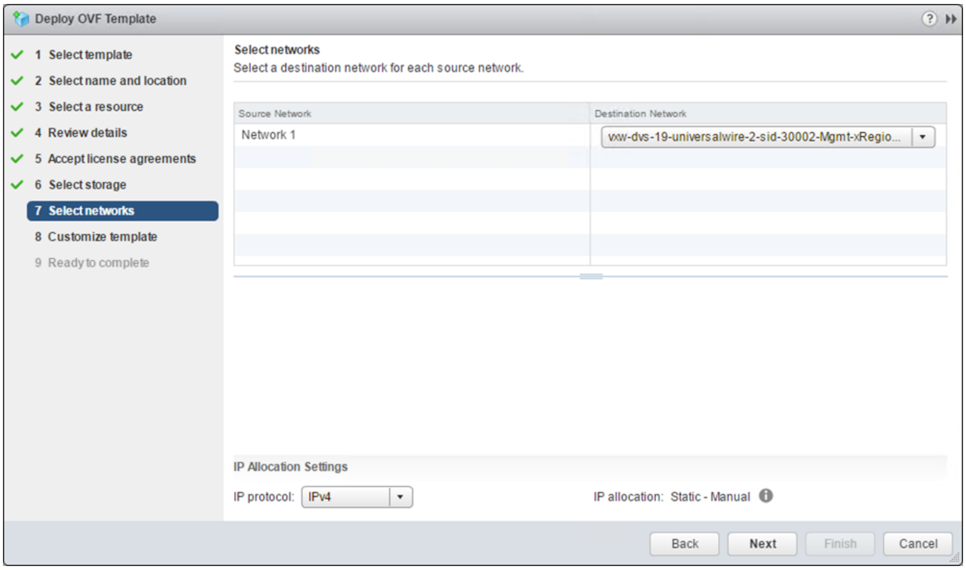
VM storage policy: Virtual SAN Default Storage Policy

□ Show datastores from Storage DRS clusters

	Name	Status	VM storage policy	Capacity	Free
●	SFO01A-VSAN01-MGMT01	✓ Normal	Virtual SAN Defa...	8.65 TB	4.63 TB

1 Objects

10 On the **Setup Networks** page, select the distributed port group that ends with `Mgmt-xRegion01-VXLAN` from the **Destination Network** drop-down menu and click **Next**.



Select networks

Select a destination network for each source network.

Source Network	Destination Network
Network 1	vxw-dvs-19-universalwire-2-sid-30002-Mgmt-xRegio...

IP Allocation Settings

IP protocol: IPv4

IP allocation: Static - Manual

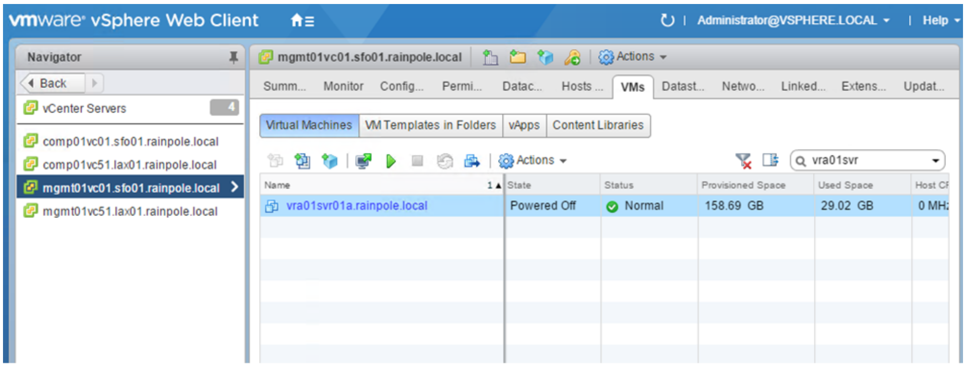
11 On the **Customize template** page, configure the following values and click **Next**.

Option	Description
Enable SSH service in the appliance	Selected
Hostname	vra01svr01a.rainpole.local

Option	Description
Initial Root Password	*vra_appA_root_password*
Default gateway	192.168.11.1
Domain Name	rainpole.local
Domain Name Servers	172.16.11.4,172.17.11.4
Domain Search Path	rainpole.local,sfo01.rainpole.local,lax01.rainpole.local
Network 1 IP Address	192.168.11.51
Network 1 Netmask	255.255.255.0

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

13 Click vCenter server **mgmt01vc01.sfo01.rainpole.local**. Select **VMs** tab. Type **`vra01svr01`** in the search text box.


vmware® vSphere Web Client
Administrator@VSPHERE.LOCAL
Help
Navigator
Back
vCenter Servers 4
comp01vc01.sfo01.rainpole.local
comp01vc51.lax01.rainpole.local
mgmt01vc01.sfo01.rainpole.local
mgmt01vc51.lax01.rainpole.local
mgmt01vc01.sfo01.rainpole.local
Actions
Summ...
Monitor
Config...
Permi...
Datac...
Hosts ...
VMs
Datast...
Netwo...
Linked...
Extens...
Updat...
Virtual Machines
VM Templates in Folders
vApps
Content Libraries
Actions

vra01svr

Name	State	Status	Provisioned Space	Used Space	Host CI
vra01svr01a.rainpole.local	Powered Off	✓ Normal	158.69 GB	29.02 GB	0 MH:

14 Select virtual machine **vra01svr01a.rainpole.local** and click **Power On** icon.

Wait until the vRealize Automation appliance virtual machine is completely powered on. This may take several minutes.

15 From the **Virtual Machine Console**, verify that `vra01svr01a.rainpole.local` uses the configuration settings you specified.

16 Repeat the procedure to deploy the second vRealize Automation virtual machine `vra01svr01b.rainpole.local`.

Deploy Windows Virtual Machines for vRealize Automation in Region A

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.

Create vSphere Image Customization Specifications in Region A

Create vSphere image customization specifications to use with your vRealize Automation IaaS Servers and Proxy Agent deployments. The customization specification you create customizes the guest operating systems of the virtual machines that host the vRealize Automation IaaS Web Server and IaaS Manager Services.

Customization specifications are XML files that contain guest operating system settings for virtual machines. You create customization specifications with the **Guest Customization** wizard, and manage specifications using the Customization Specification Manager. vCenter Server saves the customized configuration parameters in the vCenter Server database. When you clone a virtual machine or deploy a virtual machine from a template, you can customize the guest operating system of the virtual machine to change properties such as the computer name, network settings, and license settings. When you apply an image customization specification to the 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.

Create a Customization Specification File for IaaS Servers in Region A

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

You can supply a custom sysprep answer file as an alternative to specifying many of the settings in the **Guest Customization** wizard. The vSphere Image Customization template sysprep answer file stores a number of customization settings such as computer name, licensing information, and workgroup or domain settings.

Procedure

1 Log in to the Management 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 From **Home** page, under **Operations and Policies**, click **Customization Specification Manager**.

3 Select **mgmt01vc01.sfo01.rainpole.local** from the **vCenter Server** drop-down menu.

4 Click the **New** icon.

   The **Guest Customization** wizard opens.

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

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

6 On the **Set Registration Information** page, configure the following values, 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, configure the following values, 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	*volume_license_key*
Include Server License Information	Selected
Server License Mode	Per seat

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

Setting	Value
Password	*local_administrator_pwd*
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 **Edit Network** dialog box opens.

13 In the **Edit Network** dialog box, on the **IPv4** page, configure the following values 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	192.168.11.1

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

a Specify the following DNS server settings.

Setting	Value
Use the following DNS server address	Selected
Preferred DNS Server	172.16.11.4
Alternate DNS Server	172.17.11.4

b Enter `rainpole.local` in the **For all connections with TCP/IP enabled** text box and click the **Add** button.

c Enter `sfo01.rainpole.local` in the **For all connections with TCP/IP enabled** text box and click the **Add** button.

d Enter `lax01.rainpole.local` in the **For all connections with TCP/IP enabled** text box and click the **Add** button.

e 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 configuration 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.

Create a Customization Specification File for IaaS Proxy Agent Servers in Region A

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

Procedure

1 Log in to the Management 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 From the **Home** page, click **Customization Specification Manager**.

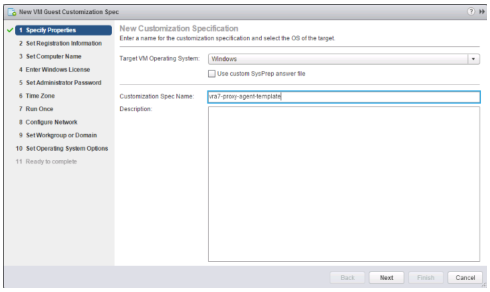
3 Select **mgmt01vc01.sfo01.rainpole.local** from the **vCenter Server** drop-down menu.

4 Click the **New** icon.

The **New VMGuest CustomizationSpec** wizard opens.

5 On the Specify Properties page, enter 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


New VM Guest Customization Spec
1 Specify Properties
2 Set Registration Information
3 Set Computer Name
4 Enter Windows License
5 Set Administrator Password
6 Time Zone
7 Run Once
8 Configure Network
9 Set Workgroup or Domain
10 Set Operating System Options
11 Ready to complete
Back
Next
Finish
Cancel

New Customization Specification

Enter a name for the customization specification and select the OS of the target.

Target VM Operating System: Windows

□ Use custom SysPrep answer file

Customization Spec Name: vra7-proxy-agent-template

Description:

6 On the **Set Registration Information** page, enter 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**.

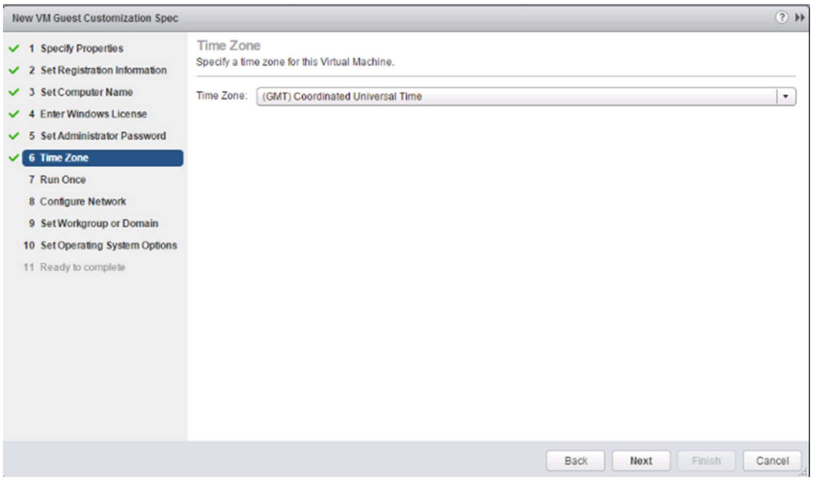
If you are using Microsoft License Server, or have multiple single license keys, leave the **Product Key** text box blank.

Setting	Value
Product Key	*volume_license_key*
Include Server License Information	Selected
Server License Mode	Per seat

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

Setting	Value
Password	*local_administrator_pwd*
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**.



New VM Guest Customization Spec

Time Zone

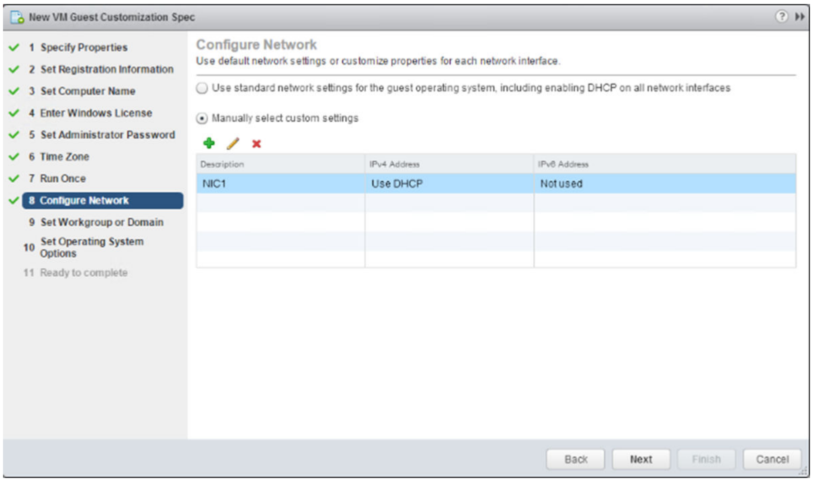
Specify a time zone for this Virtual Machine.

Time Zone: (GMT) Coordinated Universal Time

✓ 1 Specify Properties
✓ 2 Set Registration Information
✓ 3 Set Computer Name
✓ 4 Enter Windows License
✓ 5 Set Administrator Password
✓ 6 Time Zone
7 Run Once
8 Configure Network
9 Set Workgroup or Domain
10 Set Operating System Options
11 Ready to complete
Back
Next
Finish
Cancel

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**.



New VM Guest Customization Spec

1 Specify Properties
2 Set Registration Information
3 Set Computer Name
4 Enter Windows License
5 Set Administrator Password
6 Time Zone
7 Run Once
8 Configure Network
9 Set Workgroup or Domain
10 Set Operating System Options
11 Ready to complete

Configure Network

Use default network settings or customize properties for each network interface.

○ Use standard network settings for the guest operating system, including enabling DHCP on all network interfaces

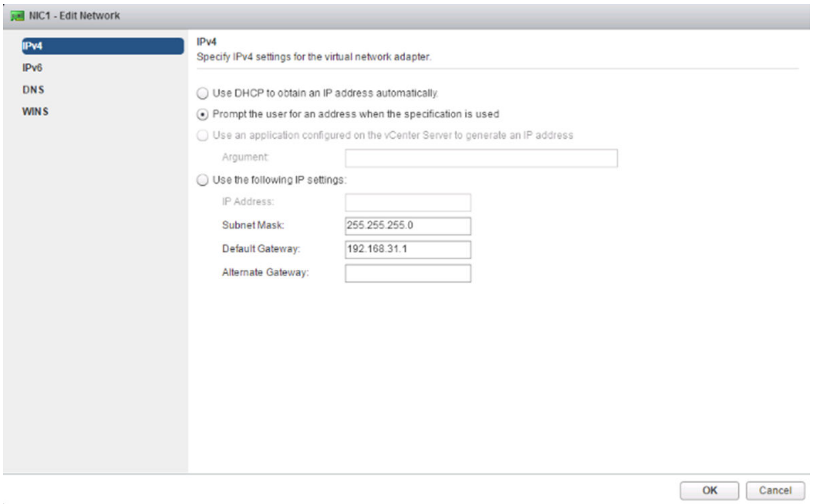
● Manually select custom settings

Description	IPv4 Address	IPv6 Address
NIC1	Use DHCP	Not used

The **Network Properties** dialog box displays.

13 In the **Edit Network** dialog box, on the IPv4 page, specify 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	192.168.31.1



NIC1 - Edit Network

IPv4

Specify IPv4 settings for the virtual network adapter.

○ Use DHCP to obtain an IP address automatically

● Prompt the user for an address when the specification is used

○ Use an application configured on the vCenter Server to generate an IP address

Argument:

○ Use the following IP settings:

IP Address:

Subnet Mask: 255.255.255.0

Default Gateway: 192.168.31.1

Alternate Gateway:

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

a Specify the following DNS server settings.

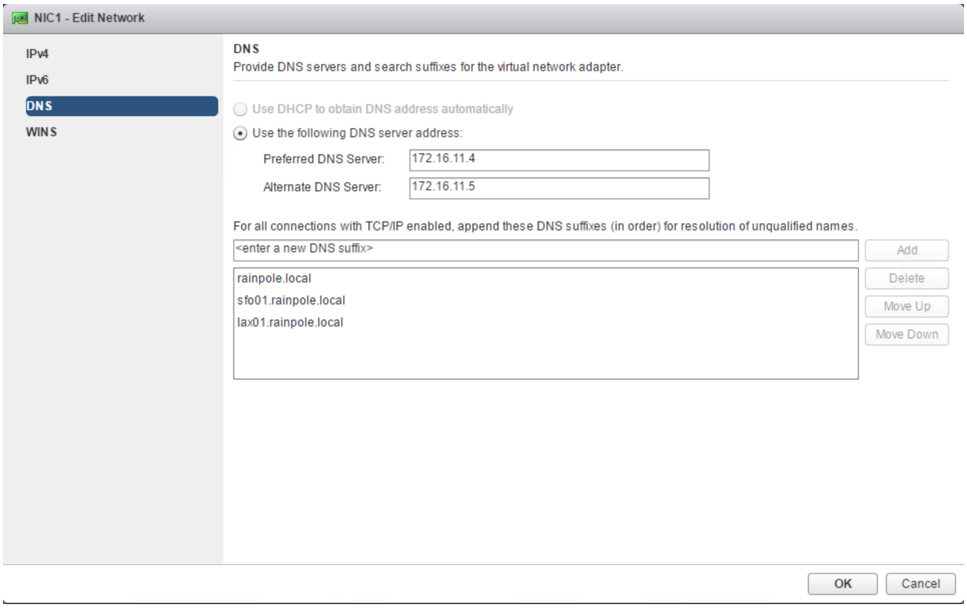
Setting	Value
Use the following DNS server address	Selected
Preferred DNS Server	172.16.11.4
Alternate DNS Server	172.16.11.5

b Enter `rainpole.local` in the **For all connections with TCP/IP enabled** text box and click the **Add** button.

c Enter `sfo01.rainpole.local` in the **For all connections with TCP/IP enabled** text box and click the **Add** button.

d Enter `lax01.rainpole.local` in the **For all connections with TCP/IP enabled** text box and click the **Add** button.

e Click **OK** to save settings and close the Edit Network dialog box, and click **Next**.



DNS

Provide DNS servers and search suffixes for the virtual network adapter.

○ Use DHCP to obtain DNS address automatically

● Use the following DNS server address:

Preferred DNS Server: 172.16.11.4

Alternate DNS Server: 172.16.11.5

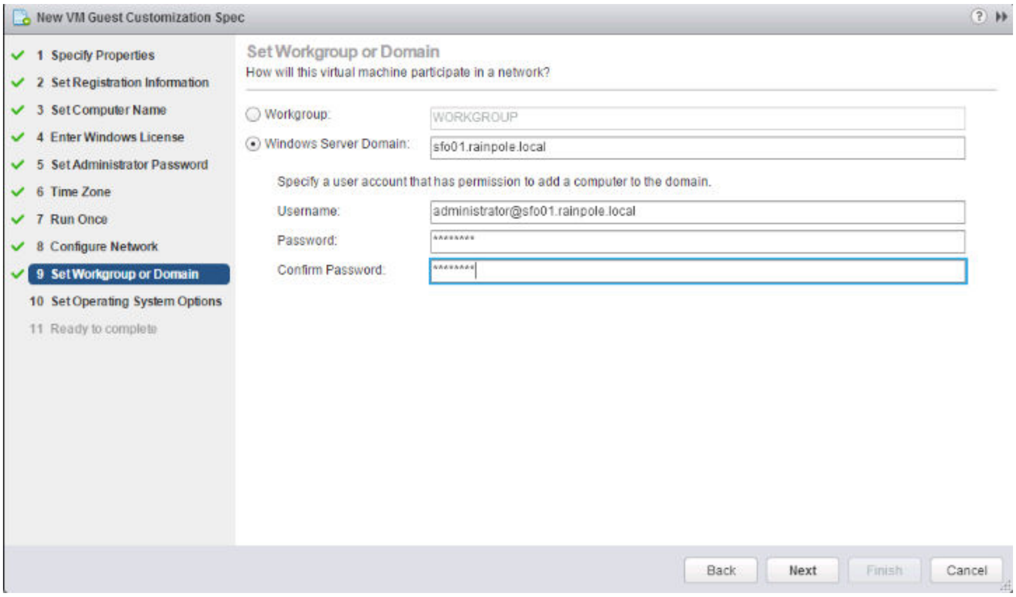
For all connections with TCP/IP enabled, append these DNS suffixes (in order) for resolution of unqualified names.

<enter a new DNS suffix>

rainpole.local
sfo01.rainpole.local
lax01.rainpole.local

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	sfo01.rainpole.local
Username	ad_admin_acct@sfo01.rainpole.local
Password	*ad_admin_password*


New VM Guest Customization Spec
1 Specify Properties
2 Set Registration Information
3 Set Computer Name
4 Enter Windows License
5 Set Administrator Password
6 Time Zone
7 Run Once
8 Configure Network
9 Set Workgroup or Domain
10 Set Operating System Options
11 Ready to complete
Back
Next
Finish
Cancel

Set Workgroup or Domain

How will this virtual machine participate in a network?

○ Workgroup: WORKGROUP

● Windows Server Domain: sfo01.rainpole.local

Specify a user account that has permission to add a computer to the domain.

Username: administrator@sfo01.rainpole.local

Password: ********

Confirm 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.

Create Windows Virtual Machines for vRealize Automation in Region A

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-template and the vra7-proxy-agent-template image customization specification templates and the windows-2012r2-64 VM template. A fully redundant vRealize Automation deployment requires eight virtual machines that run on Windows. Repeat this procedure eight times by using the information in the following table to create eight VMs.

Name for Virtual Machines	NetBIOS name	vCenter Folder	IP	vCPU number	Memory Size	Image Customization Specification Template	Network
vra01iws01a.rainpole.local	vra01iws01a	vRA01	192.168.11.54	2	4 GB	vra7-template	vxw-dvs-xxxx-Mgmt-xRegion01-VXLAN
vra01iws01b.rainpole.local	vra01iws01b	vRA01	192.168.11.55	2	4 GB	vra7-template	vxw-dvs-xxxx-Mgmt-xRegion01-VXLAN

Name for Virtual Machines	NetBIOS name	vCenter Folder	IP	vCPU number	Memory Size	Image Customization Specification Template	Network
vra01ims01a.rainpole.local	vra01ims01a	vRA01	192.168.11.57	2	4 GB	vra7-template	vxw-dvs-xxxx-Mgmt-xRegion01-VXLAN
vra01ims01b.rainpole.local	vra01ims01b	vRA01	192.168.11.58	2	4 GB	vra7-template	vxw-dvs-xxxx-Mgmt-xRegion01-VXLAN
vra01dem01.rainpole.local	vra01dem01	vRA01	192.168.11.60	2	6 GB	vra7-template	vxw-dvs-xxxx-Mgmt-xRegion01-VXLAN
vra01dem02.rainpole.local	vra01dem02	vRA01	192.168.11.61	2	6 GB	vra7-template	vxw-dvs-xxxx-Mgmt-xRegion01-VXLAN
vra01ias01.sfo01.rainpole.local	vra01ias01	vRA01IAS	192.168.31.52	2	4 GB	vra7-proxy-agent-template	vxw-dvs-xxxx-Mgmt-RegionA01-VXLAN
vra01ias02.sfo01.rainpole.local	vra01ias02	vRA01IAS	192.168.31.53	2	4 GB	vra7-proxy-agent-template	vxw-dvs-xxxx-Mgmt-RegionA01-VXLAN

Prerequisites

- Verify that you have created the Windows 2012 R2 template VM windows2012r2-template. See *Virtual Machine Template Specifications.*
- SHA512 is disabled in Windows for TLS 1.2 by default. If SHA512 certificates will be used for vRealize Automation, you need to install the windows update in Microsoft KB2973337.

Procedure

1 Log in to the Management 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 In the Navigator pane, select **Global Inventory Lists** > **vCenter Servers**. Click the **mgmt01vc01.sfo01.rainpole.local** instance.

3 Click **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 `vra01iws01a.rainpole.local` in the **Enter a name for the virtual machine** text box.

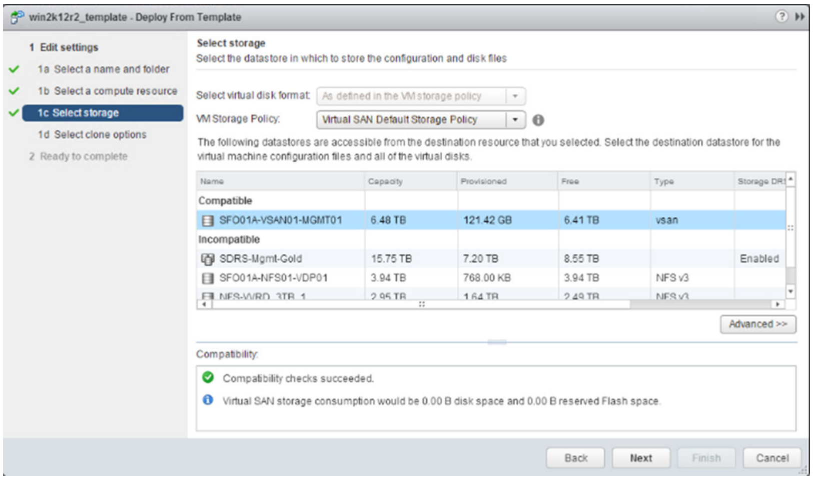
   b In the **Select a location for the virtual machine** pane, select the **vRA01** folder in the **SFO01** datacenter under **mgmt01vc01.sfo01.rainpole.local**, and click **Next**.

5 On the **Select a compute resource** page, select **SFO01-Mgmt01** and click **Next**.

6 On the **Select storage** page, select the datastore on which to create the virtual machine's disks.

   a Select **vSAN Default Storage Policy** from the**VM Storage Policy** drop-down menu.

   b Select the **SFO01A-VSAN01-MGMT01** vSAN datastore from the datastore table and click **Next.**



Select storage

Select the datastore in which to store the configuration and disk files

Select virtual disk format: As defined in the VM storage policy

VM Storage Policy: Virtual SAN Default Storage Policy

The following datastores are accessible from the destination resource that you selected. Select the destination datastore for the virtual machine configuration files and all of the virtual disks.

Name	Capacity	Provisioned	Free	Type	Storage DRS
Compatible					
SFO01A-VSAN01-MGMT01	6.48 TB	121.42 GB	6.41 TB	vsan	
Incompatible					
SDRS-Mgmt-Gold	15.75 TB	7.20 TB	8.55 TB		Enabled
SFO01A-NFS01-VDP01	3.94 TB	768.00 KB	3.94 TB	NFS v3	
NFS-VVRD_3TB_1	2.95 TB	1.64 TB	2.49 TB	NFS v3	

Compatibility:

Compatibility checks succeeded.

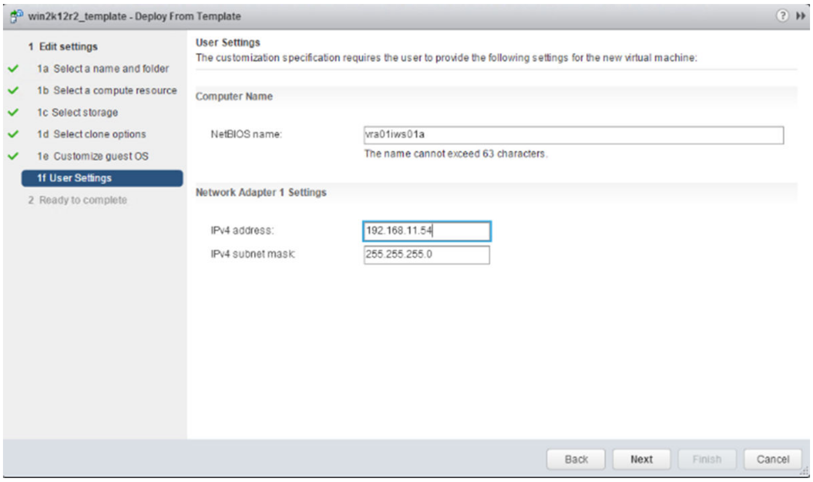
Virtual SAN storage consumption would be 0.00 B disk space and 0.00 B reserved Flash space.

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-template** from the table, and click **Next**.

9 On the **User Settings** page, enter the following values, and click **Next.**

Setting	Value
NetBIOS name	vra01iws01a
IPv4 address	192.168.11.54
IPv4 subnet mask	255.255.255.0


win2k12r2_template - Deploy From Template
1 Edit settings
✓ 1a Select a name and folder
✓ 1b Select a compute resource
✓ 1c Select storage
✓ 1d Select clone options
✓ 1e Customize guest OS
1f User Settings
2 Ready to complete
Back
Next
Finish
Cancel

User Settings

The customization specification requires the user to provide the following settings for the new virtual machine:

Computer Name

NetBIOS name: vra01iws01a

The name cannot exceed 63 characters.

Network Adapter 1 Settings

IPv4 address: 192.168.11.54

IPv4 subnet mask: 255.255.255.0

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

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 **vra01iws01a.rainpole.local** virtual machine and select **Edit Settings**.

13 Click **Virtual Hardware** and configure the settings for **CPU**, **Memory**, and the **Network adapter 1**.

a Select **2** from the **CPU** drop-down menu.

b Set the **Memory** settings to **4096 MB**.

c Expand **Network adapter 1** and select **vxw-dvs-xxxx-Mgmt-xRegion01-VXLAN** from the drop-down menu and click **OK**.

14 Right-click the virtual machine **vra01iws01a.rainpole.local**, and select **Power > Power on**.

15 From the Virtual Machine Console, verify that vra01iws01a.rainpole.local re-boots, 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.

a Verify that the IP address, computer name, and domain are correct.

b Verify vRealize Automation service account svc-vra@rainpole.local has been added to the Local Administrators Group.

17 Repeat this procedure to deploy and configure the remaining virtual machines.

Install vRealize Automation Management Agent on Windows IaaS VMs in Region A

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.

Perform this procedure multiple times to install the Management Agent on all Windows IaaS virtual machines listed below.

- vra01iws01a.rainpole.local
- vra01iws01b.rainpole.local
- vra01dem01.rainpole.local
- vra01dem02.rainpole.local
- vra01ims01a.rainpole.local
- vra01ims01b.rainpole.local
- vra01ias01.sfo01.rainpole.local
- vra01ias02.sfo01.rainpole.local

Procedure

1 Log in to the **`vra01iws01.rainpole.local`** virtual machine console using the vRealize Automation service account.

Setting	Value
Username	Rainpole\svc-vra
Password	svc-vra_password

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	https://vra01svr01a.rainpole.local:5480
Root username	root
Password	*vra_appA_root_password*

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, enter the following credentials and click **Next**.

Setting	Value
Username	rainpole\svc-vra
Password	*svc-vra_password*

5 On the **Ready to Install** page, click **Install**.

6 Repeat the procedure to install the Management Agent on the remaining Windows IaaS virtual machines.

Install the vRealize Automation Environment in Region A

You use the **Installation** wizard to deploy a distributed installation with load balancers for high availability and failover.

Once you start the wizard you must complete it. If you cancel the wizard, you must redeploy the appliance to run the wizard again.

Procedure

1 Log in to the first vRealize Automation appliance.

   a Open a Web browser and go to `https://vra01svr01a.rainpole.local:5480/`.

   b Log in using the following credentials.

Setting	Value
User name	root
Password	*vra_appA_root_password*

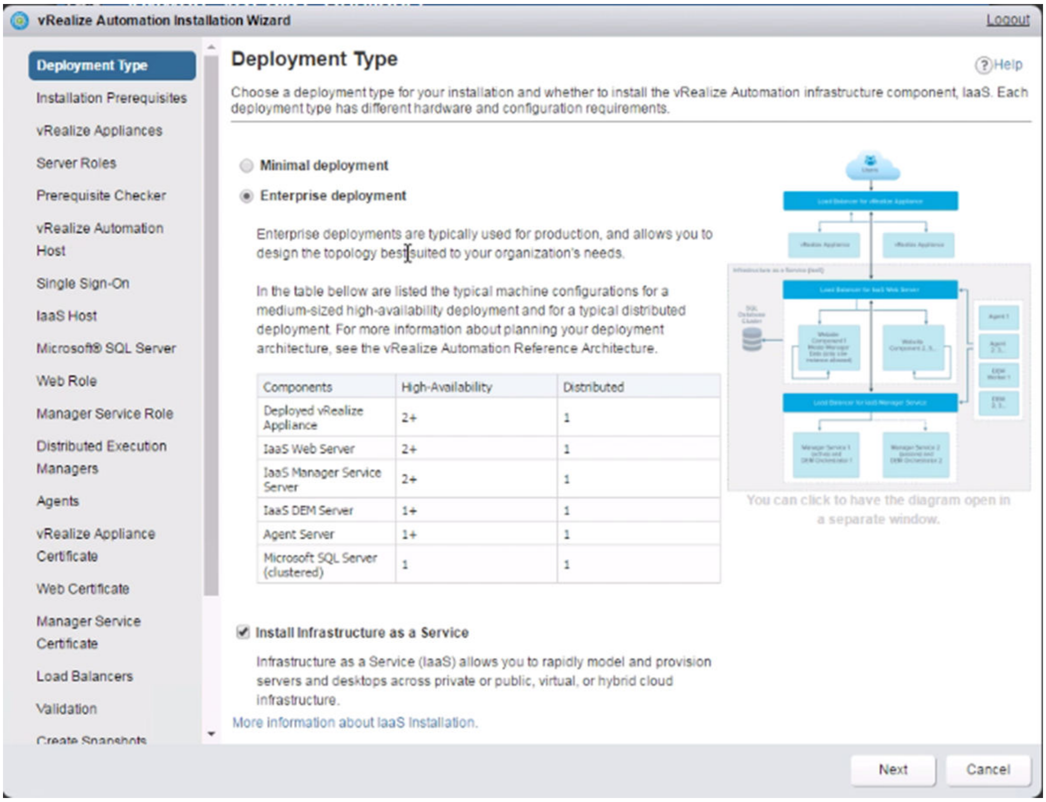
   The **vRealize Automation Installation** wizard appears.

2 On the **Welcome to the vRealize Automation Installation Wizard** page, click **Next**.

3 On the **End User License Agreement** page, accept the terms of the agreement and click **Next**.

4 On the **Deployment Type** page, specify the following settings and click **Next**.

Setting	Value
Enterprise deployment	Selected
Install Infrastructure as a Service	Selected



vRealize Automation Installation Wizard

Deployment Type

Choose a deployment type for your installation and whether to install the vRealize Automation infrastructure component, IaaS. Each deployment type has different hardware and configuration requirements.

○ Minimal deployment

● Enterprise deployment

Enterprise deployments are typically used for production, and allows you to design the topology best suited to your organization's needs.

In the table bellow are listed the typical machine configurations for a medium-sized high-availability deployment and for a typical distributed deployment. For more information about planning your deployment architecture, see the vRealize Automation Reference Architecture.

Components	High-Availability	Distributed
Deployed vRealize Appliance	2+	1
IaaS Web Server	2+	1
IaaS Manager Service Server	2+	1
IaaS DEM Server	1+	1
Agent Server	1+	1
Microsoft SQL Server (clustered)	1	1

You can click to have the diagram open in a separate window.

☑ Install Infrastructure as a Service

Infrastructure as a Service (IaaS) allows you to rapidly model and provision servers and desktops across private or public, virtual, or hybrid cloud infrastructure.

More information about IaaS Installation.

5 On the **Installation Prerequisites** page, specify the following time server settings, click **Change Time Settings**, and click **Next**.

Option	Value
Virtual Appliance Time Sync. Mode	Use Tim Server
Time Server	ntp.sfo01.rainpole.local
Time Server	ntp.lax01.rainpole.local

6 On the **Discovered Hosts** page, verify that all Windows IaaS virtual machines are listed and that the time offset is within the -1 / 0 / 1 values and click **Next**.

Note The Time Offset column shows the time delta between the vRealize Automation appliance and the Windows IaaS VMs. Time synchronization is critical. If there are values outside of the acceptable values, remediate those before you proceed.

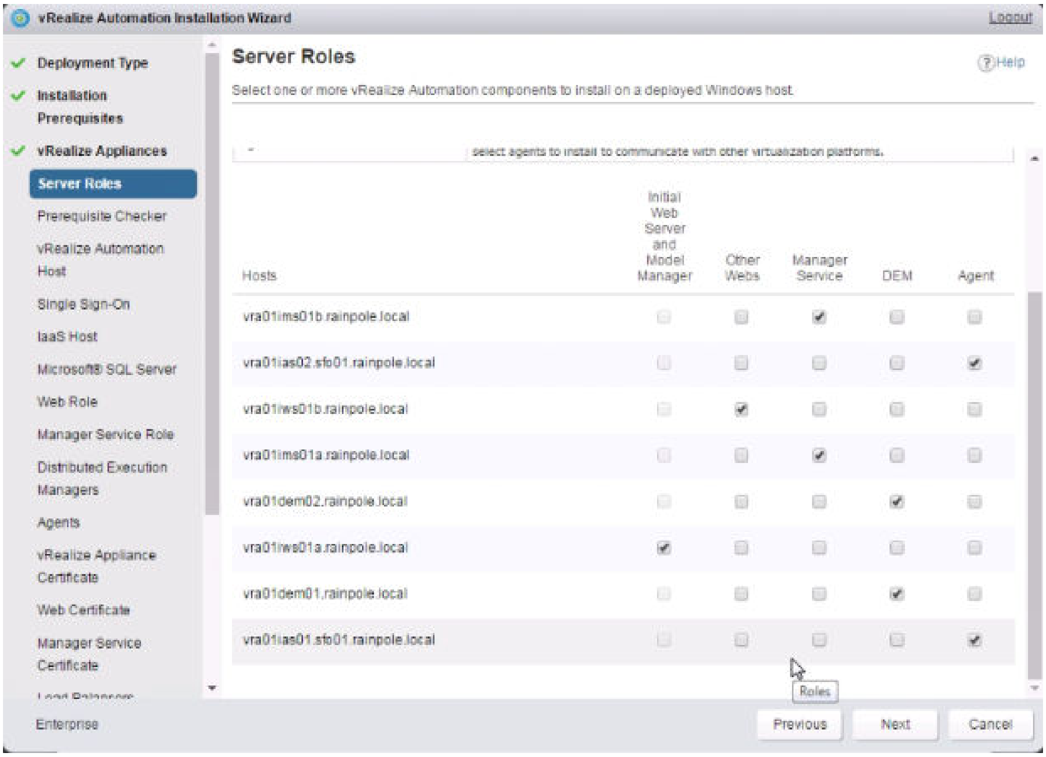
7 On the **vRealize Appliances** page, enter the following settings to add the second vRealize Appliance based on the table below, click **Next**.

Setting	Value
Host	vra01svr01b.rainpole.local
Admin User	root
Password	*vra_appB_root_password*

8 In the pop up certificate warning message box, click **OK** to proceed.

9 On the **Server Roles** page, select the respective check boxes for each server based on their role and click **Next**.

Hosts	Role
vra01iws01a.rainpole.local	Initial Web Server and Model Manager
vra01iws01b.rainpole.local	Other Webs
vra01ims01a.rainpole.local	Manager Service
vra01ims01b.rainpole.local	Manager Service
vra01dem01.rainpole.local	DEM
vra01dem02.rainpole.local	DEM
vra01ias01.sfo01.rainpole.local	Agent
vra01ias02.sfo01.rainpole.local	Agent



Server Roles

Select one or more vRealize Automation components to install on a deployed Windows host.

select agents to install to communicate with other virtualization platforms.

Hosts	Initial Web Server and Model Manager	Other Webs	Manager Service	DEM	Agent
vra01ims01b.rainpole.local	□	□	☑	□	□
vra01ias02.sfo01.rainpole.local	□	□	□	□	☑
vra01iws01b.rainpole.local	□	☑	□	□	□
vra01ims01a.rainpole.local	□	□	☑	□	□
vra01dem02.rainpole.local	□	□	□	☑	□
vra01iws01a.rainpole.local	☑	□	□	□	□
vra01dem01.rainpole.local	□	□	□	☑	□
vra01ias01.sfo01.rainpole.local	□	□	□	□	☑

10 On the **Prerequisite Checker** page, verify that the Windows servers for IaaS components are correctly configured.

a Click **Run** and wait for the prerequisite checker to complete.

b If warnings appear, click **Fix**.

c Verify that the status of all IaaS components changes to **OK** and click **Next**.

11 On the **vRealize Automation Host** page, enter `vra01svr01.rainpole.local` in the **vRealize Address** text box and click **Next**.

12 On the **Single Sign-On** page, enter and confirm *vra_administrator_password* for the default tenant account administrator@vsphere.local, and click **Next**.

13 On the **IaaS Host** page, configure the following values and click **Next**.

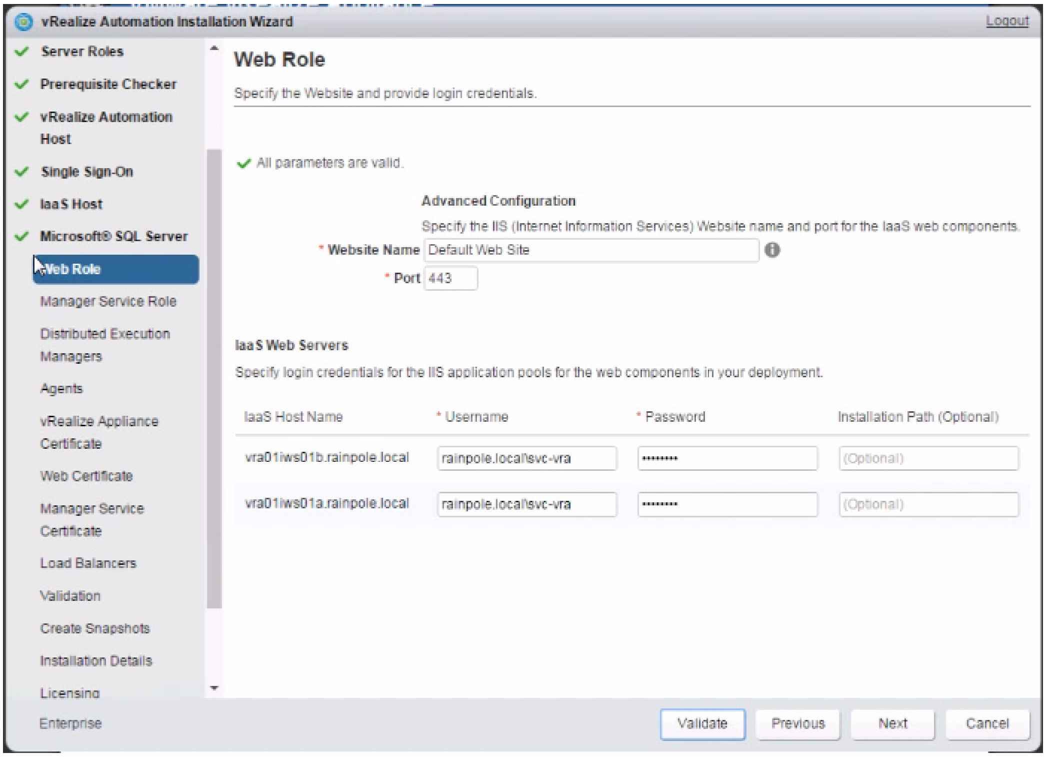
Option	Value
IaaS Web Address	vra01iws01.rainpole.local
Manager Service Address	vra01ims01.rainpole.local
Security Passphrase	*sql_db_pass*
Confirm Passphrase	*sql_db_pass*

14 On the **Microsoft SQL Server** page, configure the following values, click **Validate**, wait for successful validation, and click **Next**.

Option	Value
Server Name	vra01mssql01.rainpole.local
Database Name	VRADB-01
Create new database	Selected
Default Settings	Selected
Use SSL for database connection	Deselected
Windows Authentication	Selected

15 On the **Web Role** page, configure the following values for the IaaS servers, click **Validate**, wait for successful validation, and click **Next**.

Setting	Value
Website Name	Default Web Site
Port	443
vra01iws01a.rainpole.local Username	rainpole.local\svc-vra
vra01iws01a.rainpole.local Password	*svc-vra_password*
vra01iws01b.rainpole.local Username	rainpole.local\svc-vra
vra01iws01b.rainpole.local Password	*svc-vra_password*



Web Role

Specify the Website and provide login credentials.

✓ All parameters are valid.

Advanced Configuration

Specify the IIS (Internet Information Services) Website name and port for the IaaS web components.

* Website Name: Default Web Site

* Port: 443

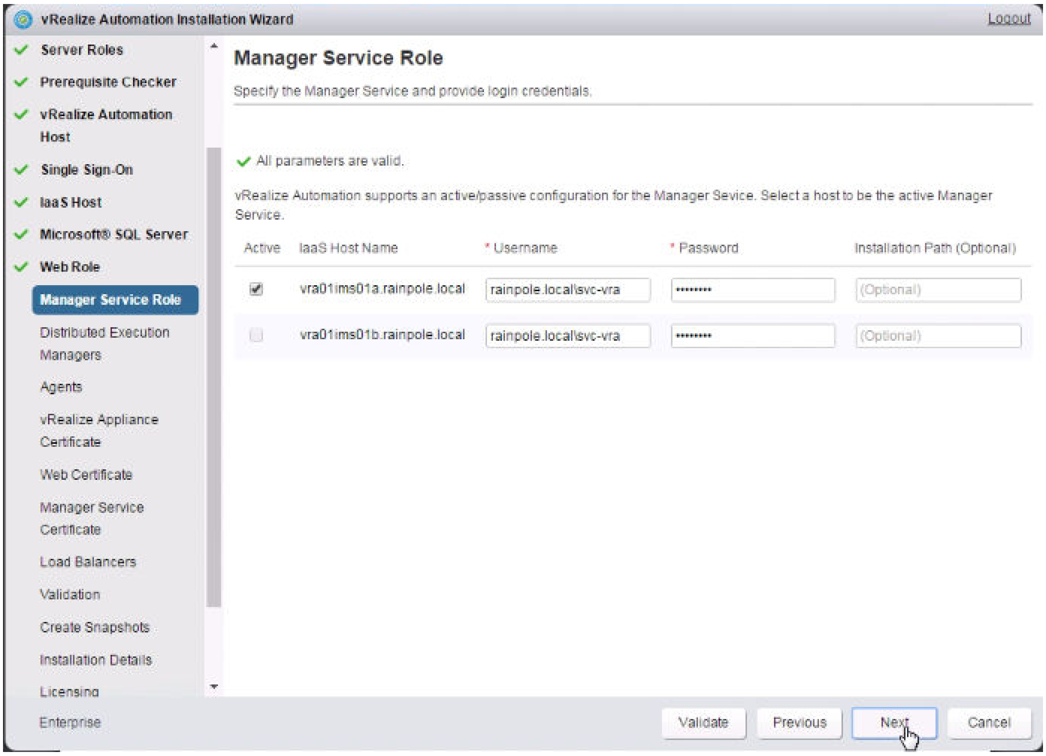
IaaS Web Servers

Specify login credentials for the IIS application pools for the web components in your deployment.

IaaS Host Name	* Username	* Password	Installation Path (Optional)
vra01iws01b.rainpole.local	rainpole.local\svc-vra	••••••••	(Optional)
vra01iws01a.rainpole.local	rainpole.local\svc-vra	••••••••	(Optional)

16 On the **Manager Service Role** page, configure the following values for the IaaS Web servers, click **Validate**, wait for successful validation, and click **Next**.

Active	IaaS Host Name	Username	Password
Selected	vra01ims01a.rainpole.local	rainpole.local\svc-vra	*svc-vra_password*
Deselected	vra01ims01b.rainpole.local	rainpole.local\svc-vra	*svc-vra_password*



Manager Service Role

Specify the Manager Service and provide login credentials.

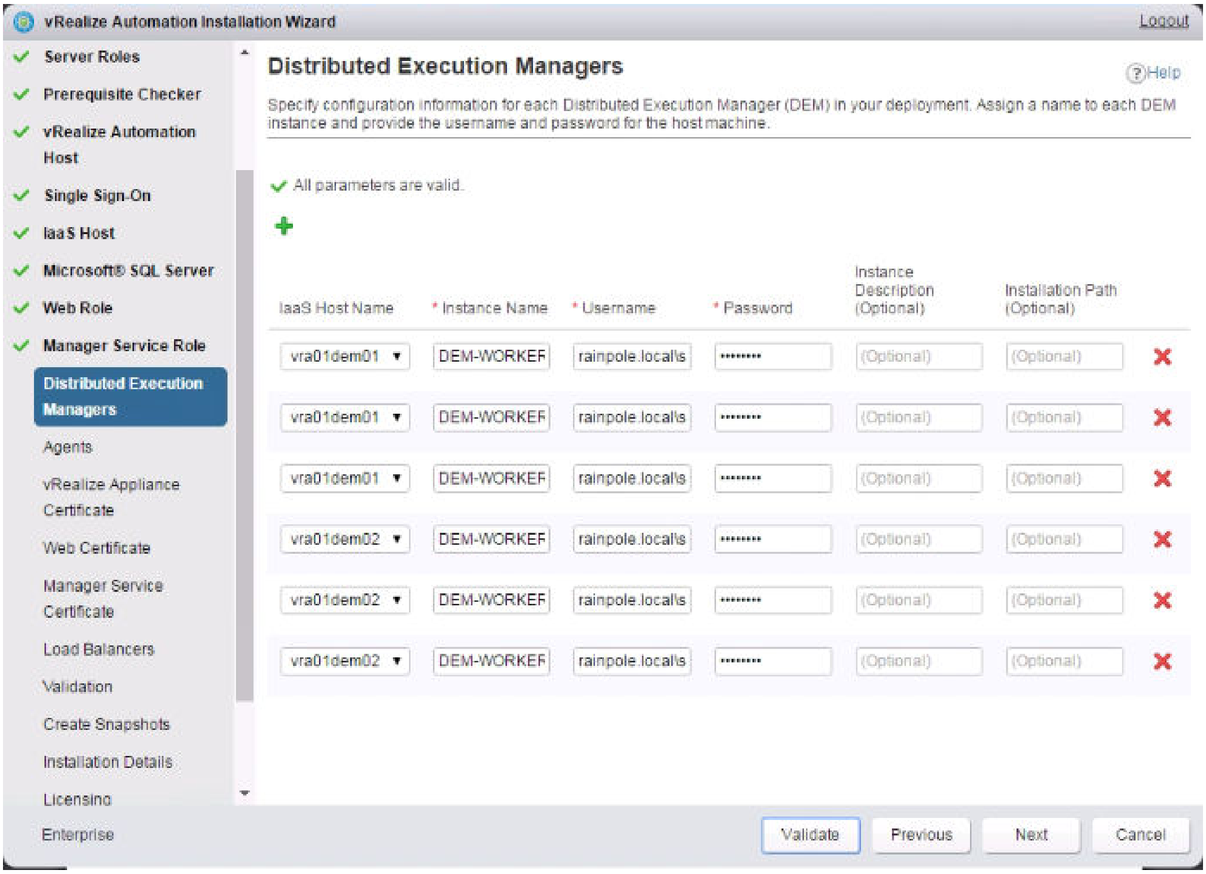
✓ All parameters are valid.

vRealize Automation supports an active/passive configuration for the Manager Sevice. Select a host to be the active Manager Service.

Active	IaaS Host Name	* Username	* Password	Installation Path (Optional)
☑	vra01ims01a.rainpole.local	rainpole.local\svc-vra	••••••••	(Optional)
□	vra01ims01b.rainpole.local	rainpole.local\svc-vra	••••••••	(Optional)

17 On the **Distributed Execution Managers** page, click the **Add** icon as needed, specify the following settings, click **Validate**, wait for successful validation, and click **Next**.

IaaS Host Name	Instance Name	Username	Password
vra01dem01	DEM-WORKER-01	rainpole.local\svc-vra	*svc-vra_password*
vra01dem01	DEM-WORKER-02	rainpole.local\svc-vra	*svc-vra_password*
vra01dem01	DEM-WORKER-03	rainpole.local\svc-vra	*svc-vra_password*
vra01dem02	DEM-WORKER-04	rainpole.local\svc-vra	*svc-vra_password*
vra01dem02	DEM-WORKER-05	rainpole.local\svc-vra	*svc-vra_password*
vra01dem02	DEM-WORKER-06	rainpole.local\svc-vra	*svc-vra_password*



Distributed Execution Managers

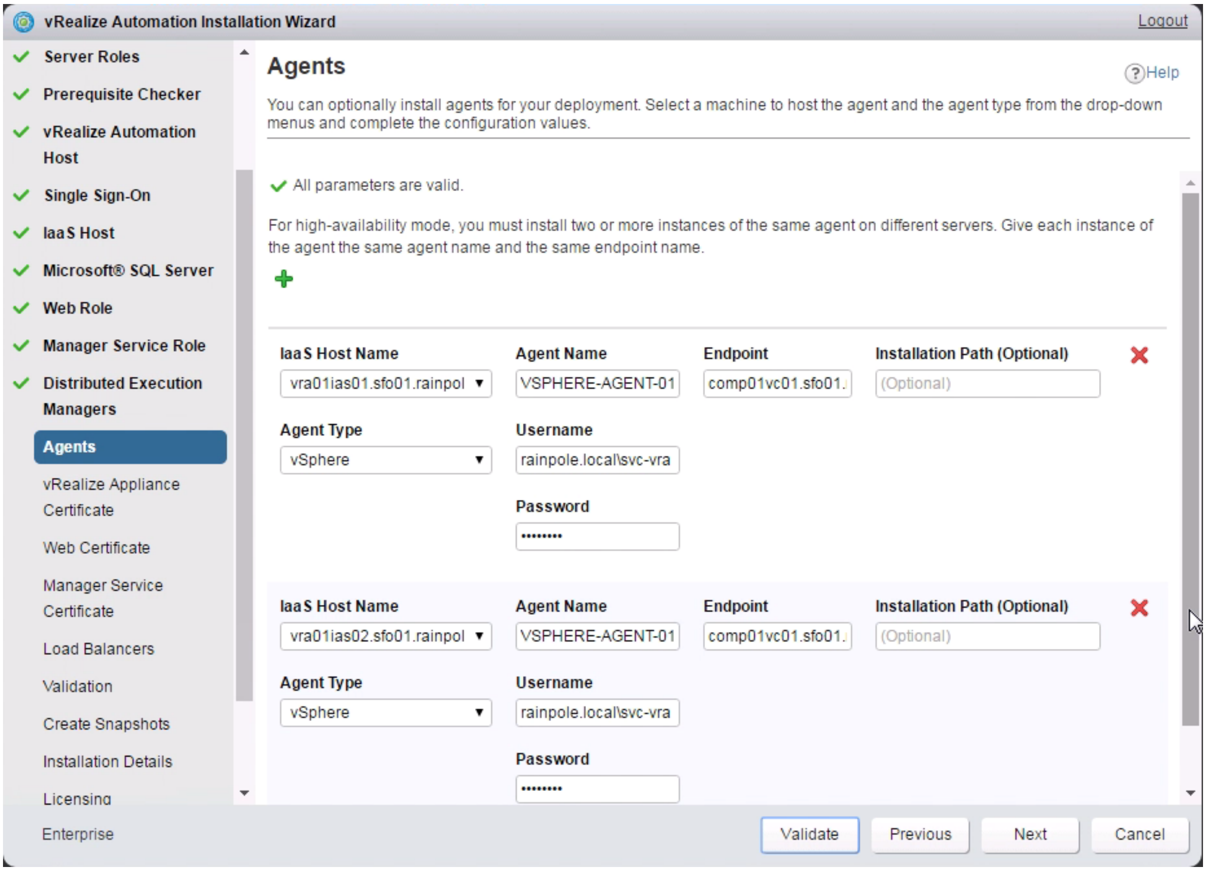
Specify configuration information for each Distributed Execution Manager (DEM) in your deployment. Assign a name to each DEM instance and provide the username and password for the host machine.

✓ All parameters are valid.

IaaS Host Name	* Instance Name	* Username	* Password	Instance Description (Optional)	Installation Path (Optional)	
vra01dem01 ▼	DEM-WORKEF	rainpole.local\s	••••••••	(Optional)	(Optional)	✕
vra01dem01 ▼	DEM-WORKEF	rainpole.local\s	••••••••	(Optional)	(Optional)	✕
vra01dem01 ▼	DEM-WORKEF	rainpole.local\s	••••••••	(Optional)	(Optional)	✕
vra01dem02 ▼	DEM-WORKEF	rainpole.local\s	••••••••	(Optional)	(Optional)	✕
vra01dem02 ▼	DEM-WORKEF	rainpole.local\s	••••••••	(Optional)	(Optional)	✕
vra01dem02 ▼	DEM-WORKEF	rainpole.local\s	••••••••	(Optional)	(Optional)	✕

18 On the **Agents** page, configure the following values, click **Validate**, wait for successful validation, and click **Next**.

IaaS Host Name	Agent Name	Endpoint	Agent Type	Username	Password
vra01ias01.sfo01.rainpole.local	VSPHERE-AGENT-01	comp01vc01.sfo01.rainpole.local	vSphere	rainpole.local\svc-vra	*svc-vra_password*
vra01ias02.sfo01.rainpole.local	VSPHERE-AGENT-01	comp01vc01.sfo01.rainpole.local	vSphere	rainpole.local\svc-vra	*svc-vra_password*



Agents

You can optionally install agents for your deployment. Select a machine to host the agent and the agent type from the drop-down menus and complete the configuration values.

✓ All parameters are valid.

For high-availability mode, you must install two or more instances of the same agent on different servers. Give each instance of the agent the same agent name and the same endpoint name.

IaaS Host Name	Agent Name	Endpoint	Installation Path (Optional)
vra01ias01.sfo01.rainpol	VSPHERE-AGENT-01	comp01vc01.sfo01.	(Optional)
Agent Type	**Username**		
vSphere	rainpole.local\svc-vra		
	Password		
	••••••••		

IaaS Host Name	Agent Name	Endpoint	Installation Path (Optional)
vra01ias02.sfo01.rainpol	VSPHERE-AGENT-01	comp01vc01.sfo01.	(Optional)
Agent Type	**Username**		
vSphere	rainpole.local\svc-vra		
	Password		
	••••••••		

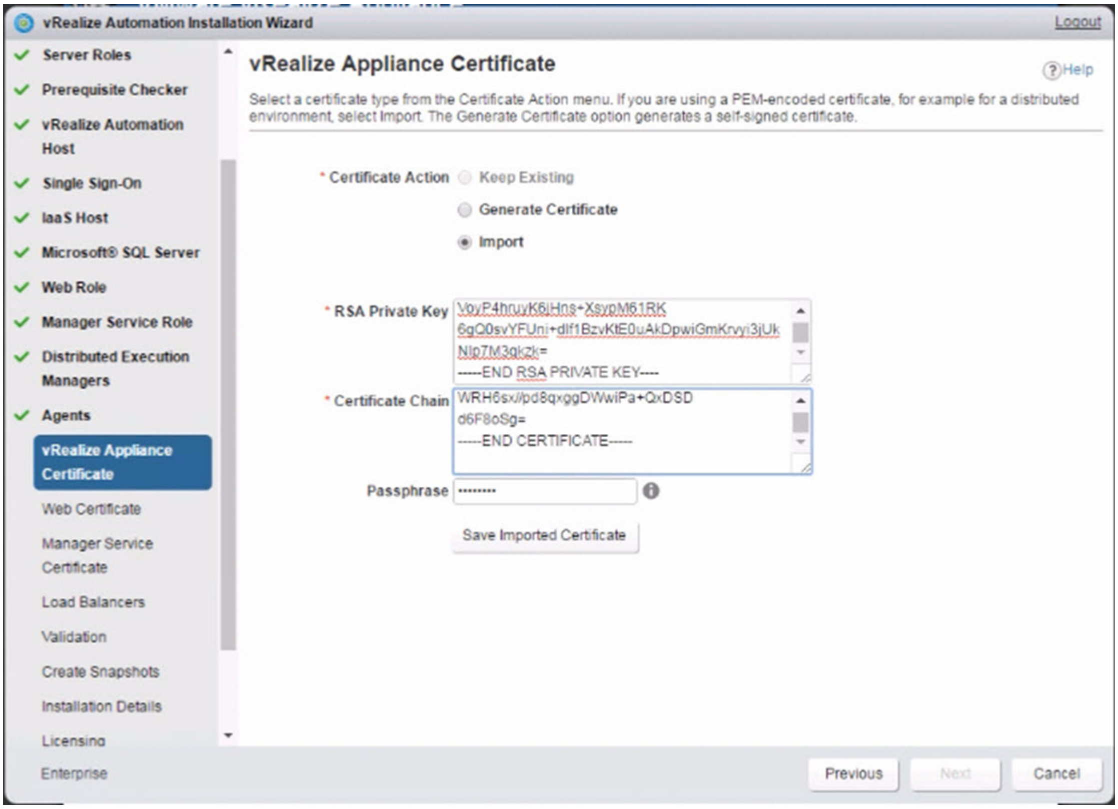
19 On the next three certificates configuration pages, configure the certificates for all vRealize Automation.

You complete three different certificate configuration pages for the different nodes using the same process and values from the `vrealize.key` file for the Private Key and the `vrealize-full.pem` file for all certificates stored in the `vra` folder. For more information on certificate configuration, see "Use the Certificate Generation Utility to Generate CA-Signed Certificates for the SDDC Management Components" in the *VMware Validated Design Planning and Preparation* document.

a On the vRealize Appliance Certificate page, specify the following settings, click **Save Imported Certificate**, and click **Next**.

Setting	Value
Certificate Action	Import
RSA Private Key	`-----END RSA PRIVATE KEY-----------BEGIN RSA PRIVATE KEY-----`*private_key_value*
Certificate Chain	`-----BEGIN CERTIFICATE-----`*Server_certificate_value*`-----END CERTIFICATE----------BEGIN CERTIFICATE-----`*Intermediate_CA_certificate_value*`-----END CERTIFICATE----------BEGIN CERTIFICATE-----`*Root_CA_certificate_value*`-----END CERTIFICATE-----`
Passphrase	*vra_cert_passphrase*

b Repeat this step on the **Web Certificate** and the **Manager Service Certificate** pages of the vRealize Automation Installation Wizard.



vRealize Appliance Certificate

Select a certificate type from the Certificate Action menu. If you are using a PEM-encoded certificate, for example for a distributed environment, select Import. The Generate Certificate option generates a self-signed certificate.

* Certificate Action ○ Keep Existing ○ Generate Certificate ● Import

* RSA Private Key
```
VoyP4hruyK6jHns+XsypM61RK
6gQ0svYFUni+dIf1BzvKtE0uAkDpwiGmKrvyi3jUk
NIp7M3qkzk=
-----END RSA PRIVATE KEY-----
```

* Certificate Chain
```
WRH6sx//pd8qxggDWwiPa+QxDSD
d6F8oSg=
-----END CERTIFICATE-----
```

Passphrase ••••••••

Save Imported Certificate

20 On the **Load Balancers** page, click **Next**.

Note You configured load balancing in Load Balancing the Cloud Management Platform in Region A

21 On the **Validation** page, click **Validate**, wait for successful validation, and click **Next**.

22 On the **Create Snapshots** page, do not close the wizard. Make snapshots of all vRealize Automation virtual machines.

a In a browser, go to `https://mgmt01vc01.sfo01.rainpole.local/vsphere-client` to log in to vCenter Server.

b Log in using the following credentials.

Setting	Value
User name	administrator@vsphere.local
Password	*vsphere_admin_password*

c From the **Home** page, click **VMs and Templates**.

d In the Navigator, expand the **mgmt01vc01.sfo01.rainpole.local > SFO01 > VRA01** folder.

e Right-click the **vra01dem01.rainpole.local** VM and select **Snapshots > Take Snapshot**.

f In the **Take VM Snapshot** dialog box, specify the following settings and click **OK**.

Setting	Value
Name	Prior to vRA IaaS component installation
Snapshot the virtual machine's memory	Selected
Quiesce guest file system	Selected

g Repeat the step to create snapshots of the remaining vRealize Automation VMs.

Virtual Machine	vCenter Folder
vra01svr01a.rainpole.local	VRA01
vra01svr01b.rainpole.local	VRA01
vra01mssql01.rainpole.local	VRA01
vra01iws01a.rainpole.local	VRA01
vra01iws01b.rainpole.local	VRA01
vra01ims01a.rainpole.local	VRA01
vra01ims01b.rainpole.local	VRA01
vra01dem01.rainpole.local	VRA01
vra01dem02.rainpole.local	VRA01
vra01ias01.sfo01.rainpole.local	VRA01IAS
vra01ias02.sfo01.rainpole.local	VRA01IAS

After you create snapshots of all virtual machines, return to the **vRealize Automation Installation** wizard.

23 On the **Create Snapshots** page, click **Next**.

24 On the **Installation Details** page, click **Install**.

25 On the **Installation Details** page, verify that all items complete successfully and click **Next**.

26 On the **Licensing** page, enter your *vRealize_Automation_License_Key*, click **Submit Key**, and click **Next.**

27 On the **Telemetry** page, select **Join the VMware Customer Experience Improvement Program** and click **Next.**

28 On the **Post-Installation Options** page, select **Continue** to proceed without creating initial content and click **Next.**

29 Click **Finish** to exit the wizard.

Configure vRealize Automation for a Large Scale Deployment in Region A

Increase the value of the `ProxyAgentBinding` and `maxStringContentLength` attributes to configure vRealize Automation Management Service to contain a large amount of data objects. For example, 3000 or more virtual machines from vSphere Center Server.

Repeat this procedure twice to configure the virtual machines in both region A (vra01ims01a.rainpole.local) and region B (vra01ims01b.rainpole.local)

Procedure

1 Log into the vra01ims01a.rainpole.local virtual machine console as the user rainpole\svr-vra.

2 Click the **Start** button on the taskbar to display the menu, enter **`Notepad`** in the search box, and click **Notepad** in the search results.

   Note Alternatively you can use any text editor installed on the Windows operating system in your environment that you prefer.

3 Right-click the **Notepad** application icon, or your preferred text editor, and select **Run As Administrator**.

4 Open the file `C:\Program Files (x86)\VMware\vCAC\Server\ManagerService.exe.config` for editing in Notepad or your preferred text editor.

5 Locate the following line in the `ManagerService.exe.config` file.

```
<binding name=”ProxyAgentServiceBinding” maxReceivedMessageSize=”13107200”>
<readerQuotas maxStringContentLength=”13107200” />
```

   Note Do not confuse these two lines with the lines that are very similar, but with the attribute binding `name = "ProvisionServiceBinding"`.

6 Replace the values of the following attributes by increasing them by a factor of 10 as shown in the table below.

Parameter	Values
maxReceivedMessageSize	131072000
maxStringContentLength	131072000

7 Save your changes to the `ManagerService.exe.config` file, close it, and exit the text editor.

8 Click **Start**, and then click **Restart** to restart the virtual machine.

9 Repeat this procedure for the vra01ims01b.rainpole.local virtual machine.

vRealize Automation Default Tenant Configuration in Region A

In shared cloud environments, where multiple companies, divisions or independent groups are using a common infrastructure fabric, it is necessary to set up virtual private clouds where authentication, resources, policy are customized to the needs of each group. Tenants are useful for isolating the users, resources and services of one tenant from those of other tenants.

Create a Local Tenant Administrator in Region A

Join the VMware Identity Manager connectors to the Active Directory domain to support Integrated Windows Authentication. Perform this operation in the default tenant **`vsphere.local`**.

Create a local user for the default tenant in vRealize Automation and assign the Tenant Administrator role to the default tenant.

Procedure

1 Log in to the vRealize Automation portal.

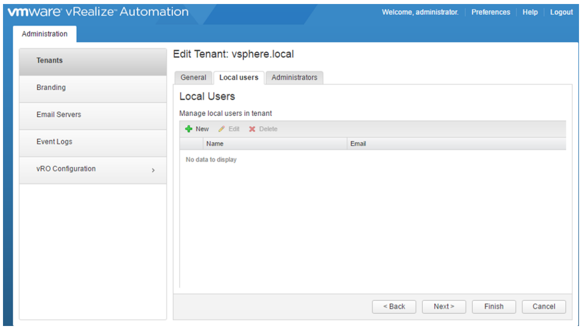
   a Open a Web browser and go to **`https://vra01svr01.rainpole.local/vcac`**.

   b Log in using the following credentials.

Setting	Value
User name	administrator
Password	*vra_administrator_password*

2 On the `Tenants` page, click the default tenant **vsphere.local** to edit its settings.

3 Click the **Local users** tab and click **New** to add a local user to the default tenant.



Edit Tenant: vsphere.local

Local Users

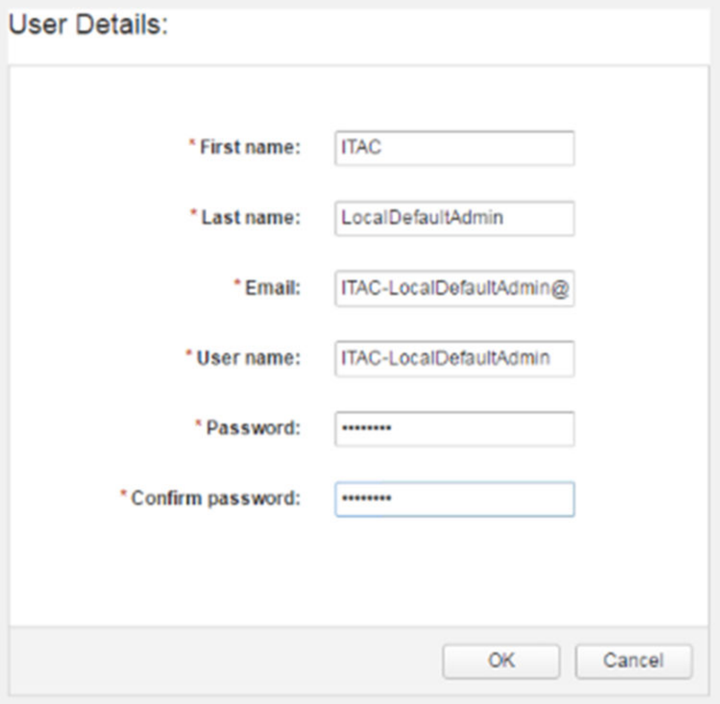
Manage local users in tenant

No data to display

4 In the **User Details** dialog box, specify the following settings, click **OK**, and click **Next**.

Setting	Value
First name	ITAC
Last name	LocalDefaultAdmin

Setting	Value
Email	ITAC-LocalDefaultAdmin@vsphere.local
User name	ITAC-LocalDefaultAdmin
Password	*itac-localdefaultadmin_password*
Confirm password	*itac-localdefaultadmin_password*



User Details:

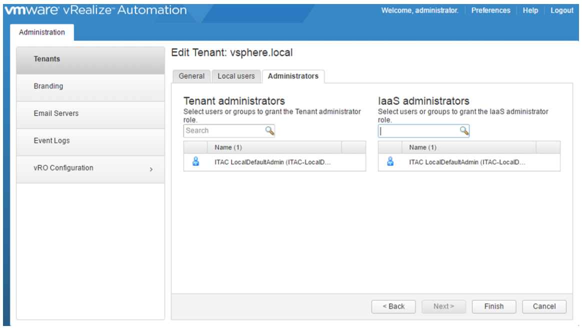
* First name:	ITAC
* Last name:	LocalDefaultAdmin
* Email:	ITAC-LocalDefaultAdmin@
* User name:	ITAC-LocalDefaultAdmin
* Password:	••••••••
* Confirm password:	••••••••

5 On the **Administrators** tab, specify tenant and infrastructure administrators.

a In the **Tenant administrators** search text box, enter **`ITAC-LocalDefaultAdmin`** and press Enter.

b In the **IaaS administrators** search text box, enter **`ITAC-LocalDefaultAdmin`** and press Enter.

c Click **Finish**.



Edit Tenant: vsphere.local

Tenant administrators
Select users or groups to grant the Tenant administrator role.

Name (1)
ITAC LocalDefaultAdmin (ITAC-LocalD...

IaaS administrators
Select users or groups to grant the IaaS administrator role.

Name (1)
ITAC LocalDefaultAdmin (ITAC-LocalD...

6 Log out from the vRealize Automation portal.

Join Connectors to an Active Directory Domain in Region A

To use an Active Directory domain for tenant authentication, you must join a VMware Identity Manager connector to vRealize Automation.

Each vRealize Automation appliance includes a connector that supports user authentication. By default, one connector is typically configured to perform directory synchronization. Perform the procedure by using the ITAC-LocalDefaultAdmin that you configured in the previous procedure.

Procedure

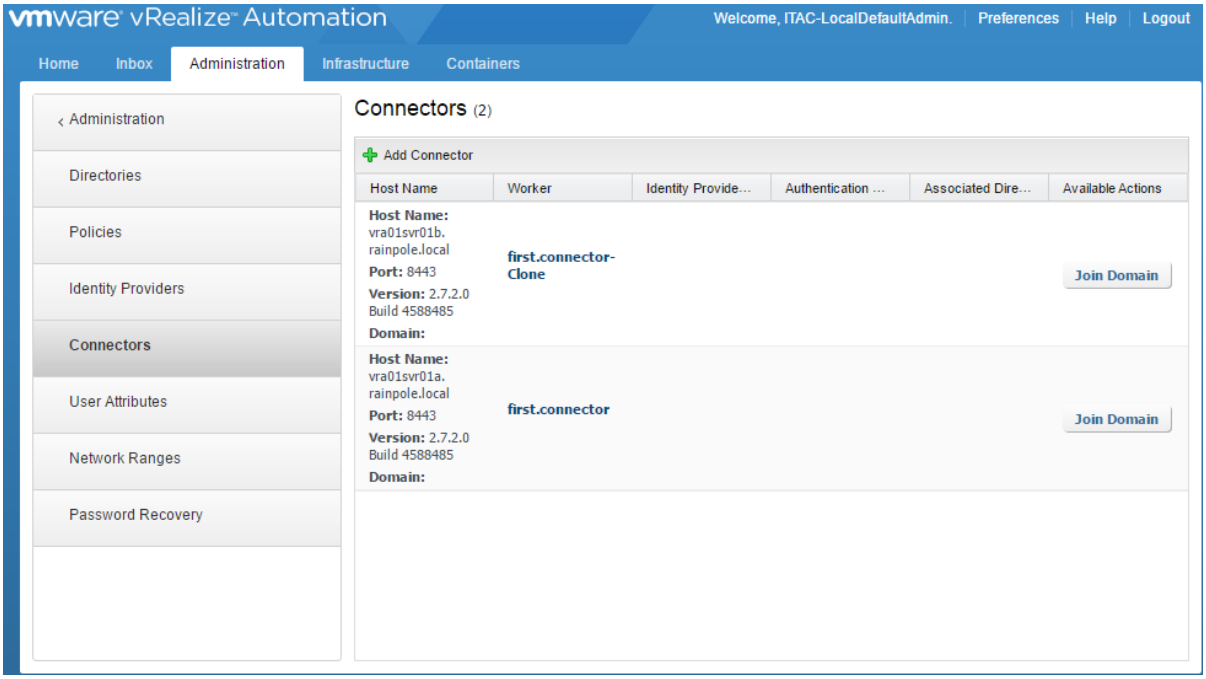
1 Log in to the vRealize Automation portal.

   a Open a Web browser and go to `https://vra01svr01.rainpole.local/vcac/org/vsphere.local`.

   b Log in using the following credentials.

Setting	Value
User name	ITAC-LocalDefaultAdmin
Password	*itac-localdefaultadmin_password*

2 Navigate to **Administration > Directories Management > Connectors**.

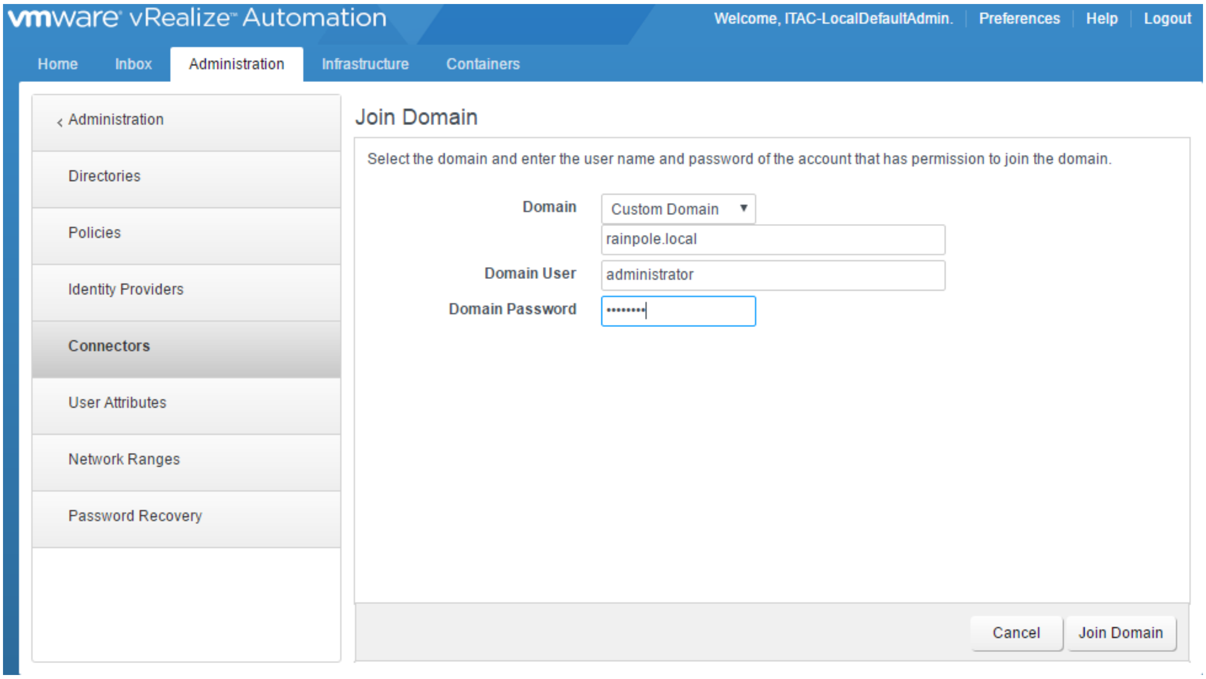


Connectors (2)

Host Name	Worker	Identity Provide...	Authentication ...	Associated Dire...	Available Actions
Host Name: vra01svr01b.rainpole.local **Port:** 8443 **Version:** 2.7.2.0 Build 4588485 **Domain:**	first.connector-Clone				Join Domain
Host Name: vra01svr01a.rainpole.local **Port:** 8443 **Version:** 2.7.2.0 Build 4588485 **Domain:**	first.connector				Join Domain

3 For the **first.connector**, click **Join Domain**, specify the following settings and click **Join Domain**.

Setting	Value
Domain	Custom Domain
	rainpole.local
Domain User	administrator
Domain Password	*domain_admin_password*



Join Domain

Select the domain and enter the user name and password of the account that has permission to join the domain.

Domain: Custom Domain
rainpole.local
Domain User: administrator
Domain Password: ••••••••

4 For the **first-connector-Clone**, click **Join Domain**, specify the following settings and click **Join Domain**.

Setting	Value
Domain	Custom Domain
	rainpole.local
Domain User	administrator
Domain Password	*domain_admin_password*

5 Log out from the vRealize Automation portal.

vRealize Automation Tenant Creation in Region A

You create additional vRealize Automation tenants so that users can access the applications and resources that they need to complete their work assignments.

A tenant is a group of users with specific privileges who work within a software instance. Administrators can create additional tenants so that users can log in and complete their work assignments. Administrators can create as many tenants as needed for system operation. Administrators must specify basic configuration such as name, login URL, local users, and administrators. The tenant administrator must also log in and set up an appropriate Active Directory connection and apply custom branding to tenants.

Create the Rainpole Tenant in Region A

The vRealize Automation Identity Manager provides Single-Sign On (SSO) capability for vRealize Automation users.

vRealize Automation Identity Manager is an authentication broker and security token exchange that interacts with the Active Directory to authenticate users. As the system administrator, you configure Identity Manager to provide access to vRealize Automation by the Rainpole tenant. The Rainpole tenant is the tenant through which you manage system-wide configuration, that includes global system defaults for branding, notifications, and monitor system logs.

Procedure

1 Log in to the vRealize Automation portal.

   a Open a Web browser and go to `https://vra01svr01.rainpole.local/vcac`.

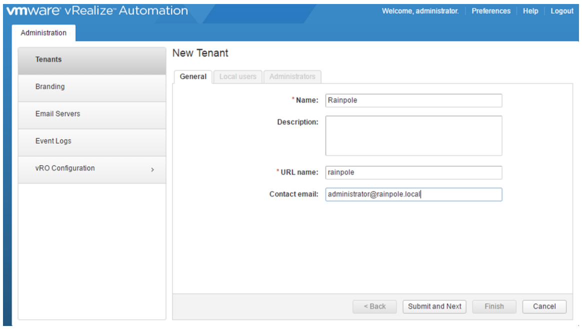
   b Log in using the following credentials.

Setting	Value
User name	administrator
Password	*vra_administrator_password*

2 On the **Tenants** page, click **New** to configure a new tenant.

3 On the **General** tab, enter the following settings for the Rainpole tenant, and click **Submit and Next**.

Setting	Value
Name	Rainpole
URL Name	rainpole
Contact email	administrator@rainpole.local



New Tenant

* Name: Rainpole

Description:

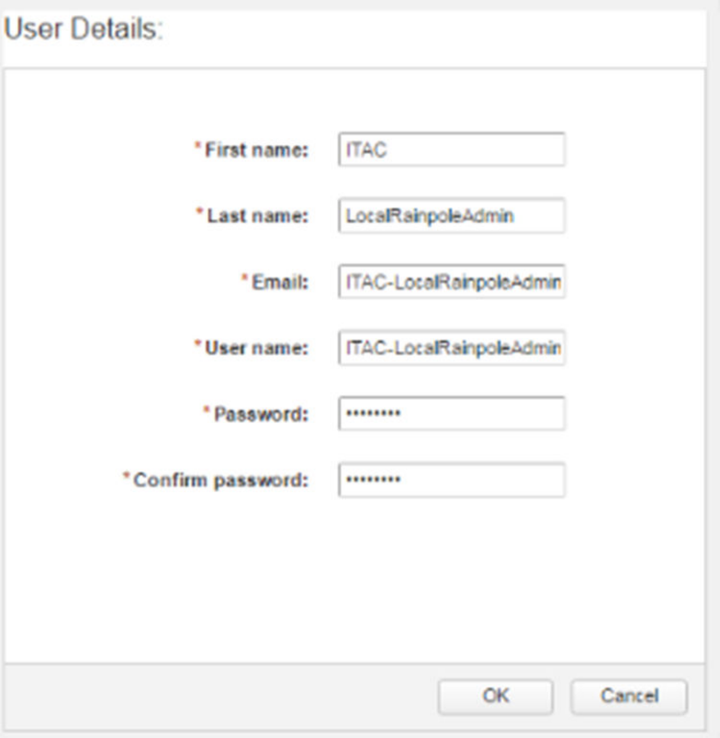
* URL name: rainpole

Contact email: administrator@rainpole.local

4 On the **Local Users** tab, click **New** to add a local user for the tenant.

5 In the **User Details** dialog box, specify the following settings, click **OK**, and click **Next**.

Setting	Value
First name	ITAC
Last name	LocalRainpoleAdmin
Email	ITAC-LocalRainpoleAdmin@rainpole.local
User name	ITAC-LocalRainpoleAdmin
Password	*itac-localrainpoleadmin_password*
Confirm password	*itac-localrainpoleadmin_password*



User Details:

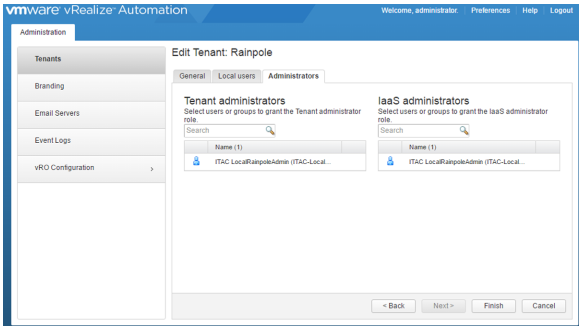
*First name:	ITAC
*Last name:	LocalRainpoleAdmin
*Email:	ITAC-LocalRainpoleAdmin
*User name:	ITAC-LocalRainpoleAdmin
*Password:	••••••••
*Confirm password:	••••••••

6 On the **Administrators** tab, specify tenant and infrastructure administrators.

   a Enter `ITAC-LocalRainpoleAdmin` in the **Tenant administrators** search text box and press **Enter**.

   b Enter `ITAC-LocalRainpoleAdmin` in the **IaaS administrators** search text box and press **Enter**.

   c Click **Finish**.



Edit Tenant: Rainpole

Tenant administrators

Select users or groups to grant the Tenant administrator role.

ITAC LocalRainpoleAdmin (ITAC-Local...

IaaS administrators

Select users or groups to grant the IaaS administrator role.

ITAC LocalRainpoleAdmin (ITAC-Local...

7 Log out of vRealize Automation portal.

Configure Identity Management for the vRealize Automation Tenant in Region A

In this design, vRealize Automation uses VMware Identity Manage to authenticate users.

Each tenant has to be associated with at least one directory as part of the tenant creation. You can add more directories if necessary. Perform the procedure by using the ITAC-LocalRainpoleAdmin that you configured.

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.

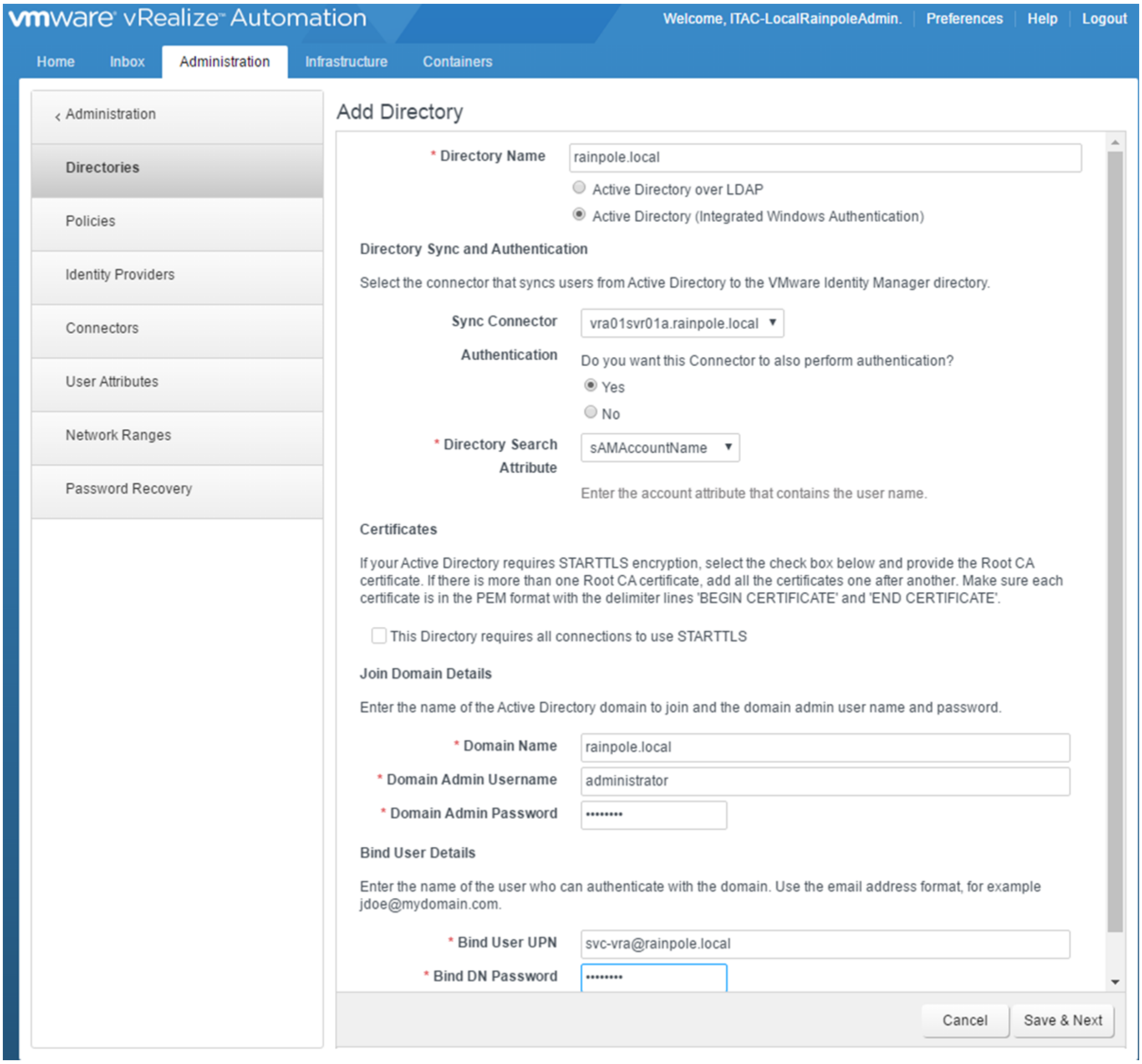
Setting	Value
User name	ITAC-LocalRainpoleAdmin
Password	*itac-localrainpoleadmin_password*

2 Navigate to **Administration > Directories Management > Directories**.

3 Click **Add Directory** and select **Add Active Directory over LDAP/IWA**, specify the following settings and click **Save & Next**.

Setting	Value
Directory Name	rainpole.local
Directory Type	Active Directory (Integrated Windows Authentication)

Setting	Value
Sync Connector	vra01svr01a.rainpole.local
Authentication	Yes
Directory Search Attribute	sAMAccountName
Certificates	Deselected
Domain Name	rainpole.local
Domain Admin Username	domain administrator
Domain Admin Password	*domain_admin_password*
Bind User UPN	svc-vra@rainpole.local
Bind DN Password	*svc-vra_password*



Add Directory

* Directory Name: rainpole.local

○ Active Directory over LDAP

● Active Directory (Integrated Windows Authentication)

Directory Sync and Authentication

Select the connector that syncs users from Active Directory to the VMware Identity Manager directory.

Sync Connector: vra01svr01a.rainpole.local ▾

Authentication: Do you want this Connector to also perform authentication?

● Yes

○ No

* Directory Search Attribute: sAMAccountName ▾

Enter the account attribute that contains the user name.

Certificates

If your Active Directory requires STARTTLS encryption, select the check box below and provide the Root CA certificate. If there is more than one Root CA certificate, add all the certificates one after another. Make sure each certificate is in the PEM format with the delimiter lines 'BEGIN CERTIFICATE' and 'END CERTIFICATE'.

□ This Directory requires all connections to use STARTTLS

Join Domain Details

Enter the name of the Active Directory domain to join and the domain admin user name and password.

* Domain Name: rainpole.local

* Domain Admin Username: administrator

* Domain Admin Password: ••••••••

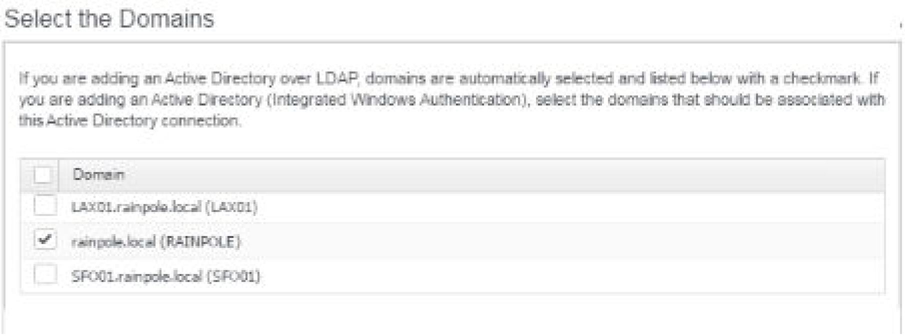
Bind User Details

Enter the name of the user who can authenticate with the domain. Use the email address format, for example jdoe@mydomain.com.

* Bind User UPN: svc-vra@rainpole.local

* Bind DN Password: ••••••••

4 On the **Select the Domains** page, select **rainpole.local (RAINPOLE)** and click **Next**.



Select the Domains

If you are adding an Active Directory over LDAP, domains are automatically selected and listed below with a checkmark. If you are adding an Active Directory (Integrated Windows Authentication), select the domains that should be associated with this Active Directory connection.

□	Domain
□	LAX01.rainpole.local (LAX01)
☑	rainpole.local (RAINPOLE)
□	SFO01.rainpole.local (SFO01)

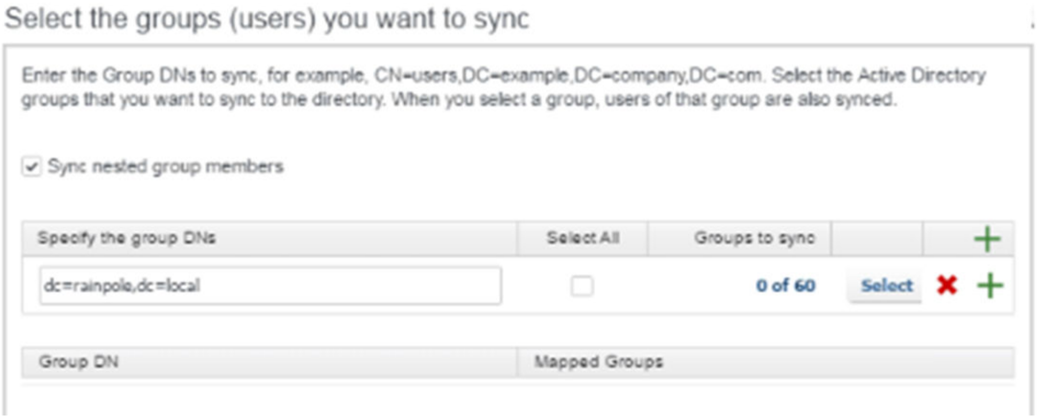
5 On the **Map User Attributes** page, click **Next**.

6 On the **Select the groups (users) you want to sync** page, enter the group DNs to sync.

   a Click the **Add** icon to add the distinguished name to the search criteria.

   b In the **Specify the group DNs** text box, enter `dc=rainpole,dc=local` and click **Find Groups**.

   c After the **Groups to sync** value updates, click **Select**.



Select the groups (users) you want to sync

Enter the Group DNs to sync, for example, CN=users,DC=example,DC=company,DC=com. Select the Active Directory groups that you want to sync to the directory. When you select a group, users of that group are also synced.

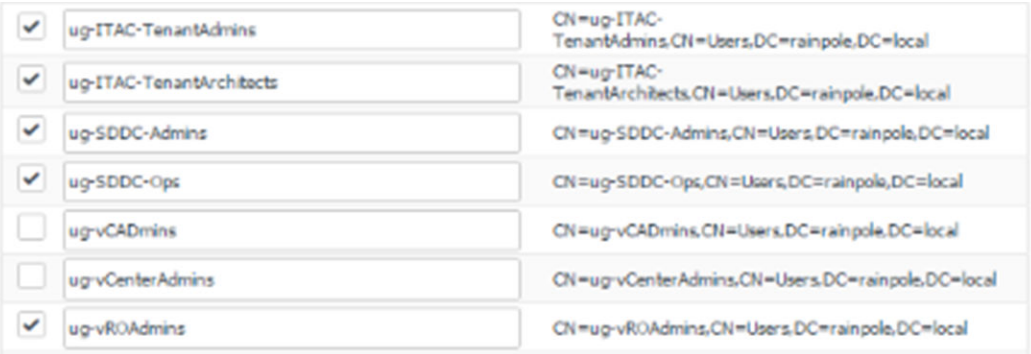
☑ Sync nested group members

Specify the group DNs	Select All	Groups to sync		+
dc=rainpole,dc=local	□	0 of 60	Select	✖ +

Group DN	Mapped Groups

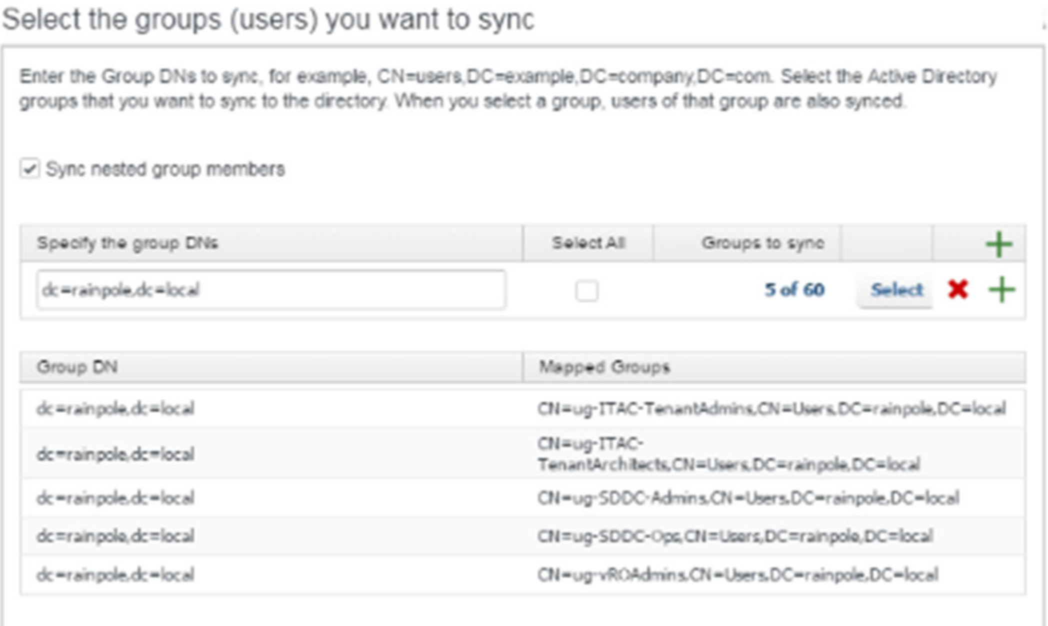
d Select the following groups and click **Save**.

- ug-ITAC-TenantAdmins
- ug-ITAC-TenantArchitects
- ug-SDDC-Admins
- ug-SDDC-Ops
- ug-vROAdmins



☑	ug-ITAC-TenantAdmins	CN=ug-ITAC-TenantAdmins,CN=Users,DC=rainpole,DC=local
☑	ug-ITAC-TenantArchitects	CN=ug-ITAC-TenantArchitects,CN=Users,DC=rainpole,DC=local
☑	ug-SDDC-Admins	CN=ug-SDDC-Admins,CN=Users,DC=rainpole,DC=local
☑	ug-SDDC-Ops	CN=ug-SDDC-Ops,CN=Users,DC=rainpole,DC=local
□	ug-vCADmins	CN=ug-vCADmins,CN=Users,DC=rainpole,DC=local
□	ug-vCenterAdmins	CN=ug-vCenterAdmins,CN=Users,DC=rainpole,DC=local
☑	ug-vROAdmins	CN=ug-vROAdmins,CN=Users,DC=rainpole,DC=local

e Click **Next**.



Select the groups (users) you want to sync

Enter the Group DNs to sync, for example, CN=users,DC=example,DC=company,DC=com. Select the Active Directory groups that you want to sync to the directory. When you select a group, users of that group are also synced.

☑ Sync nested group members

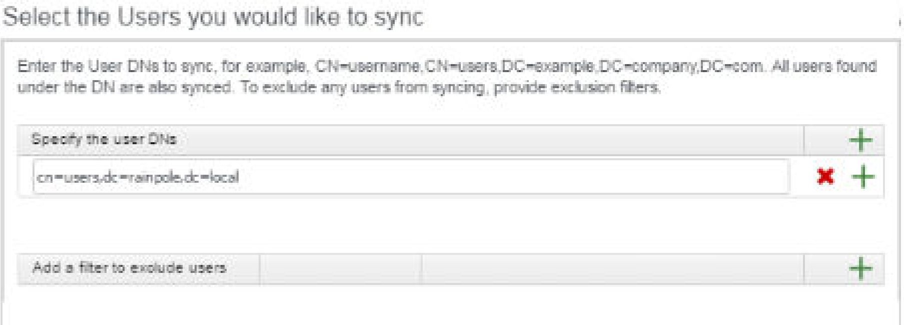
Specify the group DNs	Select All	Groups to sync		+
dc=rainpole,dc=local	□	5 of 60	Select	✖ +

Group DN	Mapped Groups
dc=rainpole,dc=local	CN=ug-ITAC-TenantAdmins,CN=Users,DC=rainpole,DC=local
dc=rainpole,dc=local	CN=ug-ITAC-TenantArchitects,CN=Users,DC=rainpole,DC=local
dc=rainpole,dc=local	CN=ug-SDDC-Admins,CN=Users,DC=rainpole,DC=local
dc=rainpole,dc=local	CN=ug-SDDC-Ops,CN=Users,DC=rainpole,DC=local
dc=rainpole,dc=local	CN=ug-vROAdmins,CN=Users,DC=rainpole,DC=local

7 On the **Select the Users you would like to sync** page, enter the user DNs to sync.

   a Click the **Add** icon to add the distinguished name to the search criteria.

   b In the **Specify the group DNs** text box, enter `cn=users,dc=rainpole,dc=local`, click the **Add** icon on the same row, and click **Next**.



Select the Users you would like to sync

Enter the User DNs to sync, for example, CN=username,CN=users,DC=example,DC=company,DC=com. All users found under the DN are also synced. To exclude any users from syncing, provide exclusion filters.

Specify the user DNs

cn=users,dc=rainpole,dc=local

Add a filter to exclude users

8 On the **Review** page, click **Sync Directory**.

Configure Directories Management for High Availability in Region A

Each vRealize Automation appliance includes a connector that supports user authentication, although only one connector is typically configured to perform directory synchronization.

To support Directories Management high availability, you must configure a second connector that corresponds to your second vRealize Automation appliance. That second connector connects to the same Identity Provider and, through VMware Identity Manager, points to the same Active Directory instance. With this configuration, if one appliance fails, the other can take over management of user authentication.

In a high availability environment, all nodes must serve the same set of users, authentication methods, and other Active Directory constructs. The most direct method to accomplish this is to promote the Identity Provider to the cluster by setting the load balancer host as the Identity Provider host. With this configuration, all authentication requests are directed to the load balancer, which forwards the request to either connector as appropriate.

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.

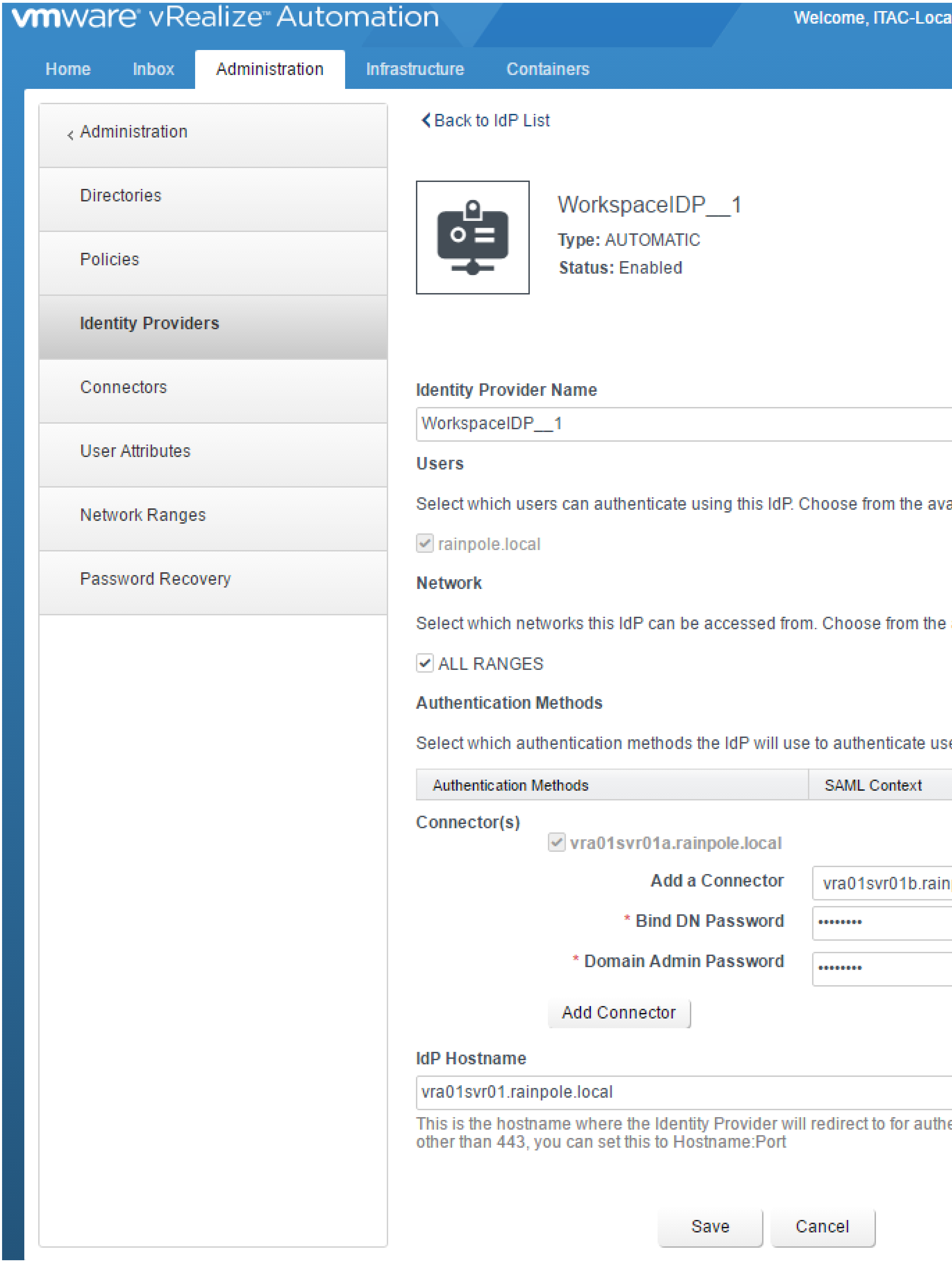
Setting	Value
User name	ITAC-LocalRainpoleAdmin
Password	*itac-localrainpoleadmin_password*
Domain	vsphere.local

2 Navigate to **Administration > Directories Management > Identity Providers**.

3 Click the name of the identity provider **WorkspaceIDP__1** to edit its settings.

4 Under **Connector(s)**, specify the following settings and click **Add Connector**.

Setting	Value
Add a Connector	vra01svr01b.rainpole.local
Bind DN Password	*svc-vra_password*
Domain Admin Password	*domain_admin_password*



vmware vRealize Automation

Welcome, ITAC-Loca

Home | Inbox | Administration | Infrastructure | Containers

‹ Administration
- Directories
- Policies
- Identity Providers
- Connectors
- User Attributes
- Network Ranges
- Password Recovery

‹ Back to IdP List

WorkspaceIDP__1

Type: AUTOMATIC

Status: Enabled

Identity Provider Name

WorkspaceIDP__1

Users

Select which users can authenticate using this IdP. Choose from the ava

☑ rainpole.local

Network

Select which networks this IdP can be accessed from. Choose from the

☑ ALL RANGES

Authentication Methods

Select which authentication methods the IdP will use to authenticate use

Authentication Methods	SAML Context

Connector(s)

☑ vra01svr01a.rainpole.local

Add a Connector vra01svr01b.rain

* **Bind DN Password** ••••••••

* **Domain Admin Password** ••••••••

Add Connector

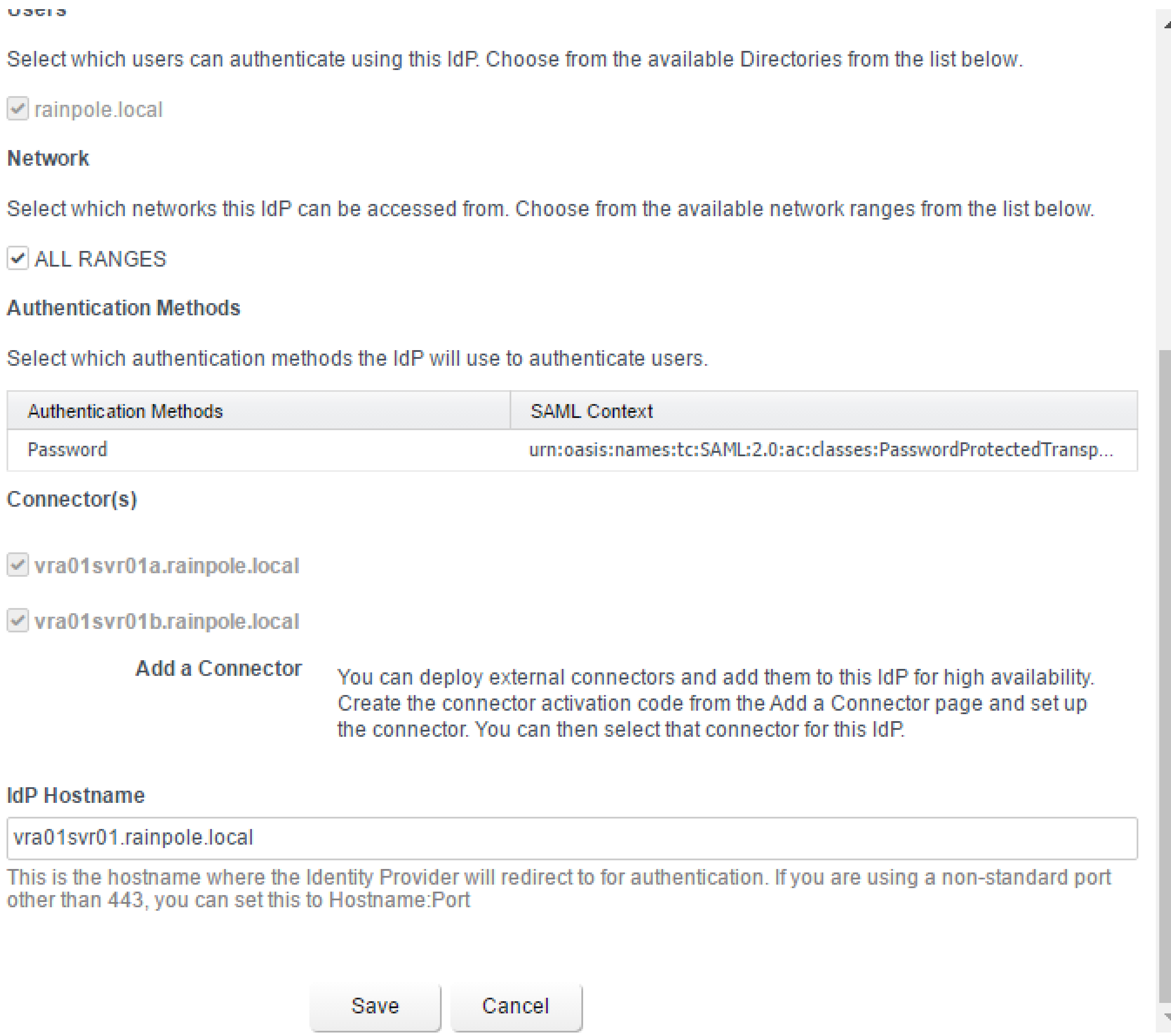
IdP Hostname

vra01svr01.rainpole.local

This is the hostname where the Identity Provider will redirect to for authe other than 443, you can set this to Hostname:Port

Save | Cancel

Wait until **vra01svr01b.rainpole.local** shows under **Connector(s)** before proceeding to the next step. This might take a few minutes.



Users

Select which users can authenticate using this IdP. Choose from the available Directories from the list below.

☑ rainpole.local

Network

Select which networks this IdP can be accessed from. Choose from the available network ranges from the list below.

☑ ALL RANGES

Authentication Methods

Select which authentication methods the IdP will use to authenticate users.

Authentication Methods	SAML Context
Password	urn:oasis:names:tc:SAML:2.0:ac:classes:PasswordProtectedTransp...

Connector(s)

☑ vra01svr01a.rainpole.local

☑ vra01svr01b.rainpole.local

Add a Connector — You can deploy external connectors and add them to this IdP for high availability. Create the connector activation code from the Add a Connector page and set up the connector. You can then select that connector for this IdP.

IdP Hostname

vra01svr01.rainpole.local

This is the hostname where the Identity Provider will redirect to for authentication. If you are using a non-standard port other than 443, you can set this to Hostname:Port

5 In the **IdP Hostname** text box, enter `vra01svr01.rainpole.local`, the host name of the load balancer, and click **Save**.

6 Log out of vRealize Automation portal.

Assign Tenant Administrative Roles to Active Directory Users in Region A

After vRealize Automation Directories Management is associated with your Active Directory domain, domain users can administer the tenant. Assign domain user groups for tenant and infrastructure administrators.

Procedure

1 Log in to the vRealize Automation portal.

  a Open a Web browser and go to **`https://vra01svr01.rainpole.local/vcac`**.

  b Log in using the following credentials.

Setting	Value
User name	administrator
Password	*vra_administrator_password*

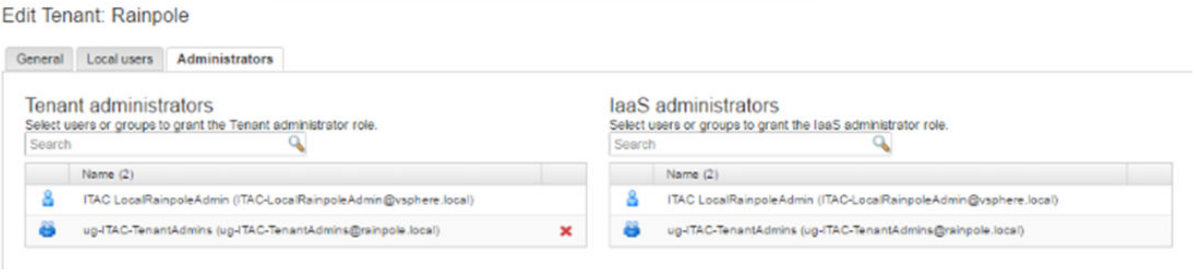
2 On the **Tenants** page, click the Rainpole tenant to edit its settings.

3 Click the **Administrators** tab to assign domain user groups for tenant and infrastructure administrators.

  a Enter **`ug-ITAC-TenantAdmins`** in the **Tenant administrators** search text box and press **Enter**.

  b Enter **`ug-ITAC-TenantAdmins`** in the **IaaS administrators** search text box and press **Enter**.

  c Click **Finish**.



Tenant administrators

Select users or groups to grant the Tenant administrator role.

Name (2)
ITAC LocalRainpoleAdmin (ITAC-LocalRainpoleAdmin@vsphere.local)
ug-ITAC-TenantAdmins (ug-ITAC-TenantAdmins@rainpole.local)

IaaS administrators

Select users or groups to grant the IaaS administrator role.

Name (2)
ITAC LocalRainpoleAdmin (ITAC-LocalRainpoleAdmin@vsphere.local)
ug-ITAC-TenantAdmins (ug-ITAC-TenantAdmins@rainpole.local)

Brand the Tenant Login Pages in Region A

You can apply custom branding on a per-customer basis to the vRealize Automation tenant login pages.

System administrators control the default branding for all tenants. As a tenant administrator, you change the branding of the portal. That includes the logo, the background color, and the information in the header and footer. If the branding for a tenant is changed, a tenant administrator can revert back to the system defaults.

Procedure

1 Log in to the vRealize Automation portal.

  a Open a Web browser and go to **`https://vra01svr01.rainpole.local/vcac`**.

  b Log in using the following credentials.

Setting	Value
User name	administrator
Password	*vra_administrator_password*

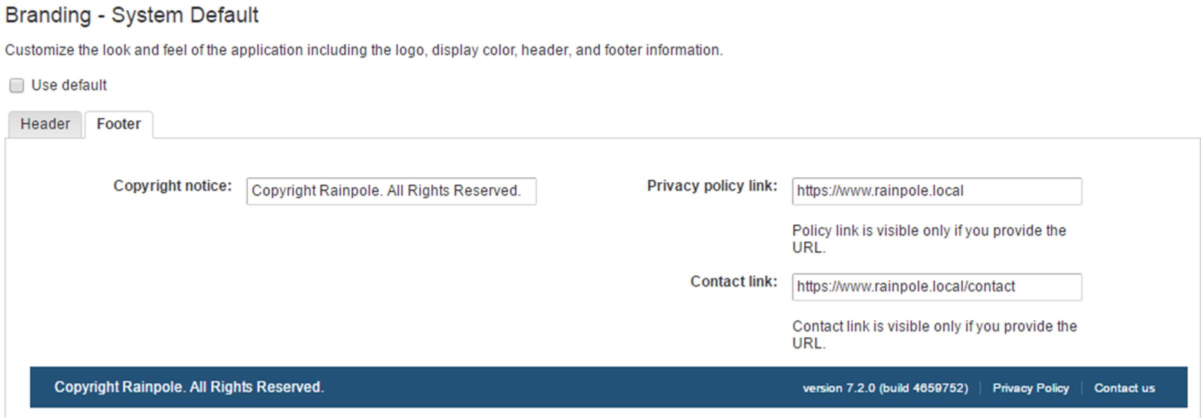
2 Navigate to **Administration > Branding** and deselect the **Use default** check box.

3 On the **Header** tab specify the following settings for the header branding.

Setting	Value
Company Name	Rainpole
Product Name	Infrastructure Service Portal
Background hex color	*3989C7*
Text hex color	*FFFFFF*

4 Click the **Footer** tab, specify the following settings for the footer branding and click **Finish**.

Setting	Value
Copyright notice	Copyright Rainpole. All Rights Reserved.
Privacy policy link	https://www.rainpole.local
Contact link	https://www.rainpole.local/contact



Branding - System Default

Customize the look and feel of the application including the logo, display color, header, and footer information.

□ Use default

Copyright notice: Copyright Rainpole. All Rights Reserved.

Privacy policy link: https://www.rainpole.local

Policy link is visible only if you provide the URL.

Contact link: https://www.rainpole.local/contact

Contact link is visible only if you provide the URL.

Copyright Rainpole. All Rights Reserved.

version 7.2.0 (build 4659752) | Privacy Policy | Contact us

Configure the Default Email Servers in Region A

System administrators configure inbound and outbound email servers to handle email notifications about events involving tenants' machines. System administrators can create only one inbound email server and one outbound email server. These servers are the defaults for all tenants.

If tenant administrators do not override the default email server settings before they enable notifications, vRealize Automation uses the globally configured email server.

Procedure

1 Log in to the vRealize Automation portal.

   a Open a Web browser and go to `https://vra01svr01.rainpole.local/vcac`.

   b Log in using the following credentials.

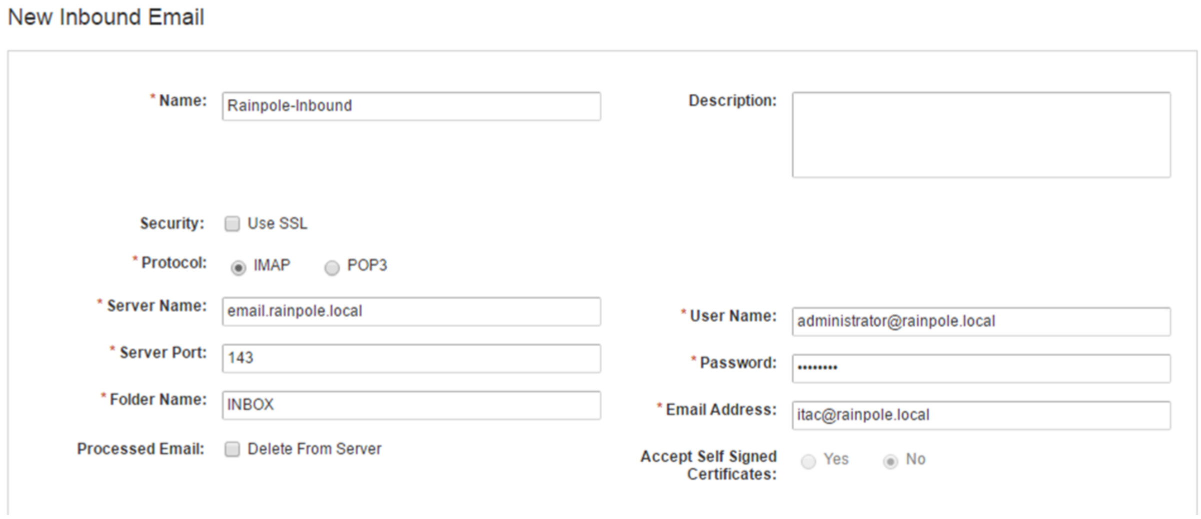
Setting	Value
User name	administrator
Password	*vra_administrator_password*

2 Navigate to **Administration > Email Servers** and click **New**.

3 In the **New Email Server** dialog box, select **Email - Inbound** and click **OK**.

4 On the **New Inbound Email** page, specify the following values, click **Test Connection** to verify that the settings are correct, and click **OK**.

Setting	Value
Name	Rainpole-Inbound
Security	Deselected
Protocol	IMAP
Server Name	email.rainpole.local
Server Port	143
Folder Name	INBOX
Processed Email	Deselected
User Name	administrator@rainpole.local
Password	*vra_administrator_password*
Email Address	itac@rainpole.local



New Inbound Email

* Name: Rainpole-Inbound

Description:

Security: □ Use SSL

* Protocol: ● IMAP ○ POP3

* Server Name: email.rainpole.local

* Server Port: 143

* Folder Name: INBOX

Processed Email: □ Delete From Server

* User Name: administrator@rainpole.local

* Password: ••••••••

* Email Address: itac@rainpole.local

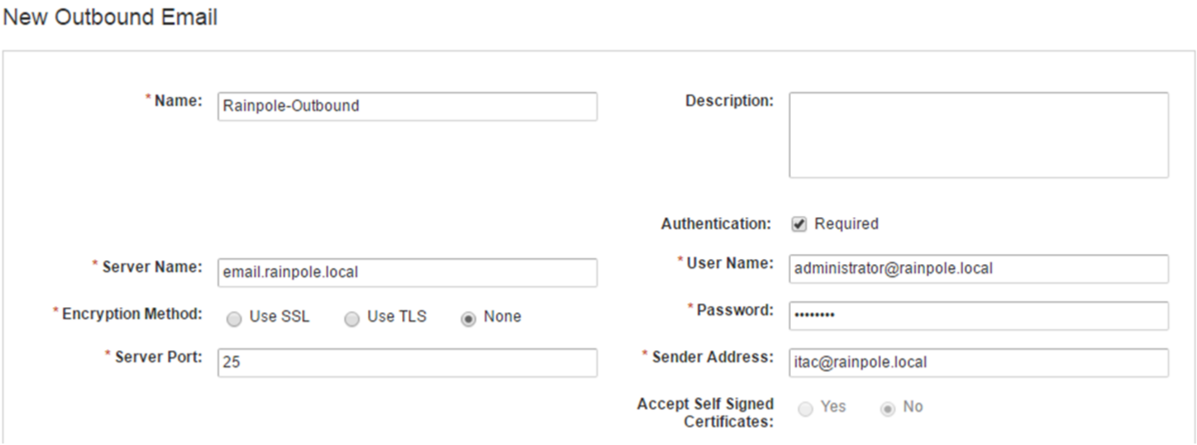
Accept Self Signed Certificates: ○ Yes ● No

5 On the **Email Servers** page, click **New** to configure the outbound server settings.

6 In the **New Email Server** dialog box, select **Email - Outbound** and click **OK**.

7 On the **New Outbound Email** page, specify the following values, click **Test Connection** to verify that the settings are correct, and click **OK**.

Setting	Value
Name	Rainpole-Outbound
Server Name	email.rainpole.local
Encryption Method	None
Server Port	25
Authentication	Selected
User Name	administrator@rainpole.local
Password	*vra_administrator_password*
Sender Address	itac@rainpole.local


New Outbound Email

* Name: Rainpole-Outbound
Description:
Authentication: ☑ Required
* Server Name: email.rainpole.local
* User Name: administrator@rainpole.local
* Encryption Method: ○ Use SSL ○ Use TLS ● None
* Password: ••••••••
* Server Port: 25
* Sender Address: itac@rainpole.local
Accept Self Signed Certificates: ○ Yes ● No

8 Log out of vRealize Automation portal.

vRealize Orchestrator Installation in Region A

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

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 can be extended with new plug-ins and libraries, and can be integrated into larger architectures through a REST API.

Install vRealize Orchestrator in Region A

Deploy and configure two vRealize Orchestrator appliances to provide the SDDC foundation orchestration engine.

Install and configure the multi-node plug-in to provide disaster recovery capability through vRealize Orchestrator content replication.

Prerequisites

- Verify that you have successfully generated a CA-Signed certificate for vRealize Orchestrator. See "Use the Certificate Generation Utility to Generate CA-Signed Certificates for the SDDC Management Components" in the *VMware Validated Design Planning and Preparation* document.
- Verify that you have created an empty SQL Server database for vRealize Orchestrator. See SQL Server Configuration for the Cloud Management Platform in Region A.
- Verify that you have downloaded the NSX Plug-in for vRealize Orchestrator `.vmoapp` file.

Deploy the vRealize Orchestrator Virtual Appliances in Region A

You deploy two vRealize Orchestrator virtual appliances.

Perform this procedure twice to deploy two appliances using the respective values in the following table for the different hosts.

vRealize Orchestrator Appliance	IP Address	FQDN
Host A	192.168.11.63	vra01vro01a.rainpole.local
Host B	192.168.11.64	vra01vro01b.rainpole.local

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 Navigate to the mgmt01vc01.sfo01.rainpole.local vCenter Server instance.

3 Right-click **mgmt01vc01.sfo01.rainpole.local** and select **Deploy OVF Template**.

4 On the **Select source** page, browse to the vRealize Orchestrator `.ova` file on your local machine and click **Next**.

5 On the **Review Details** page click **Next**.

6 On the **Accept License Agreements** page, accept the end user license agreement and click **Next**.

7 On the **Select name and folder** page, enter the following information for the host that you deploy and click **Next.**

Setting	Values for Host A	Values for Host B
Name	vra01vro01a.rainpole.local	vra01vro01b.rainpole.local
Select a folder or datacenter	vRA01	vRA01

8 On the **Select a resource** page, select the **SFO01-Mgmt01** cluster and click **Next**.

9 On the **Select storage** page, select the datastore.

a From the **Select virtual disk format** drop-down menu, select **Thin Provision**.

b From the **VM Storage Policy** drop-down menu, select **vSAN Default Storage Policy**.

c From the datastore table, select the **SFO01A-VSAN01-MGMT01** vSAN datastore and click **Next**.

10 On the **Setup networks** page, select the distributed port group on the distributed switch that ends with Mgmt-xRegion01-VXLAN and click **Next.**

11 On the **Customize template** page, select the following values and click **Next**.

Setting	Values for Host A	Values for Host B
Initial Root Password	*hostA_root_pwd*	*hostB_root_pwd*
Confirm Initial Root Password	*hostA_root_pwd*	*hostB_root_pwd*
Enable SSH service in the appliance	Selected	Selected
Hostname	vra01vro01a.rainpole.local	vra01vro01b.rainpole.local
Default Gateway	192.168.11.1	192.168.11.1
Domain Name	rainpole.local	rainpole.local
Domain Search Path	rainpole.local,sfo01.rainpole.local,lax01.rainpole.local	rainpole.local,sfo01.rainpole.local,lax01.rainpole.local
Domain Name Servers	172.16.11.4, 172.17.11.4	172.16.11.4, 172.17.11.4
Network 1 IP address	192.168.11.63	192.168.11.64
Network 1 Netmask	255.255.255.0	255.255.255.0

12 On the **Ready to complete** page, review the configuration settings, check **Power on the appliance after deployment**, and click **Finish**.

13 Repeat the procedure to deploy the vRealize Orchestrator virtual appliance for Host B.

Configure NTP for vRealize Orchestrator in Region A

Configure the network time protocol (NTP) for the vRealize Orchestrator appliances from the virtual appliance management interface (VAMI).

Perform this procedure twice, once for each of the vRealize Orchestrator virtual appliances.

Host	VAMI URL
Host A	https://vra01vro01a.rainpole.local:5480
Host B	https://vra01vro01b.rainpole.local:5480

Procedure

1 Log in to the vRealize Orchestrator virtual appliance management interface.

   a Open a Web browser and go to **`https://vra01vro01a.rainpole.local:5480`**.

   b Log in using the following credentials.

Setting	Value
User name	root
Password	*hostA_root_password*

2 Configure the appliance to use a time server.

   a Click the **Admin** tab and click **Time Settings**.

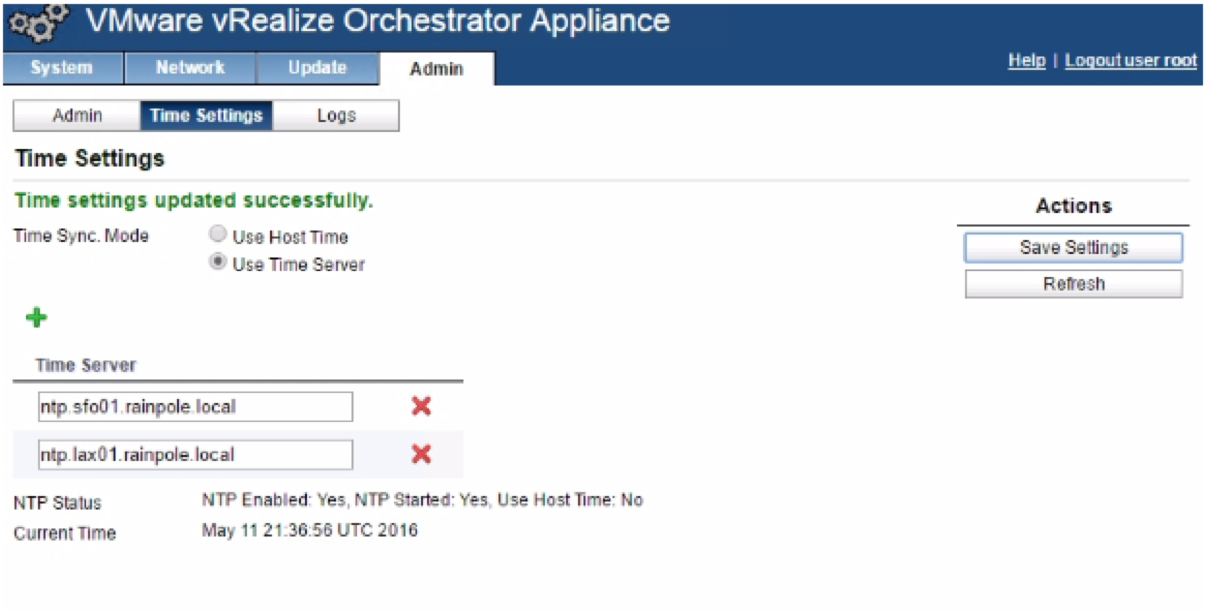
   b Under **Time Settings**, set **Time Sync Mode** to **Use Time Server**.

   c Click the **Add** button to enter a new time server.

   d In the **Time Server** text box, enter **`ntp.sfo01.rainpole.local`**.

e Click the **Add** icon to enter another time server.

f In the second **Time Server** text box, enter **`ntp.lax01.rainpole.local`** and click **Save Settings**.



Time Settings

Time settings updated successfully.

Time Sync. Mode ○ Use Host Time ● Use Time Server

Time Server

ntp.sfo01.rainpole.local

ntp.lax01.rainpole.local

NTP Status NTP Enabled: Yes, NTP Started: Yes, Use Host Time: No

Current Time May 11 21:36:56 UTC 2016

3 Repeat this procedure to configure the second vRealize Orchestrator virtual appliance, vra01vro01b.rainpole.local.

Configure the SQL Server Database for vRealize Orchestrator in Region A

To create a vRealize Orchestrator cluster, you must configure your deployment to use a shared database that accepts multiple connections. A shared database can accept connections from different vRealize Orchestrator instances.

Procedure

1 Log in to the vRealize Orchestrator Control Center.

a Open a Web browser and go to **`https://vra01vro01a.rainpole.local:8283/vco-controlcenter`**.

b Log in using the following credentials.

Setting	Value
User name	root
Password	*hostA_root_password*

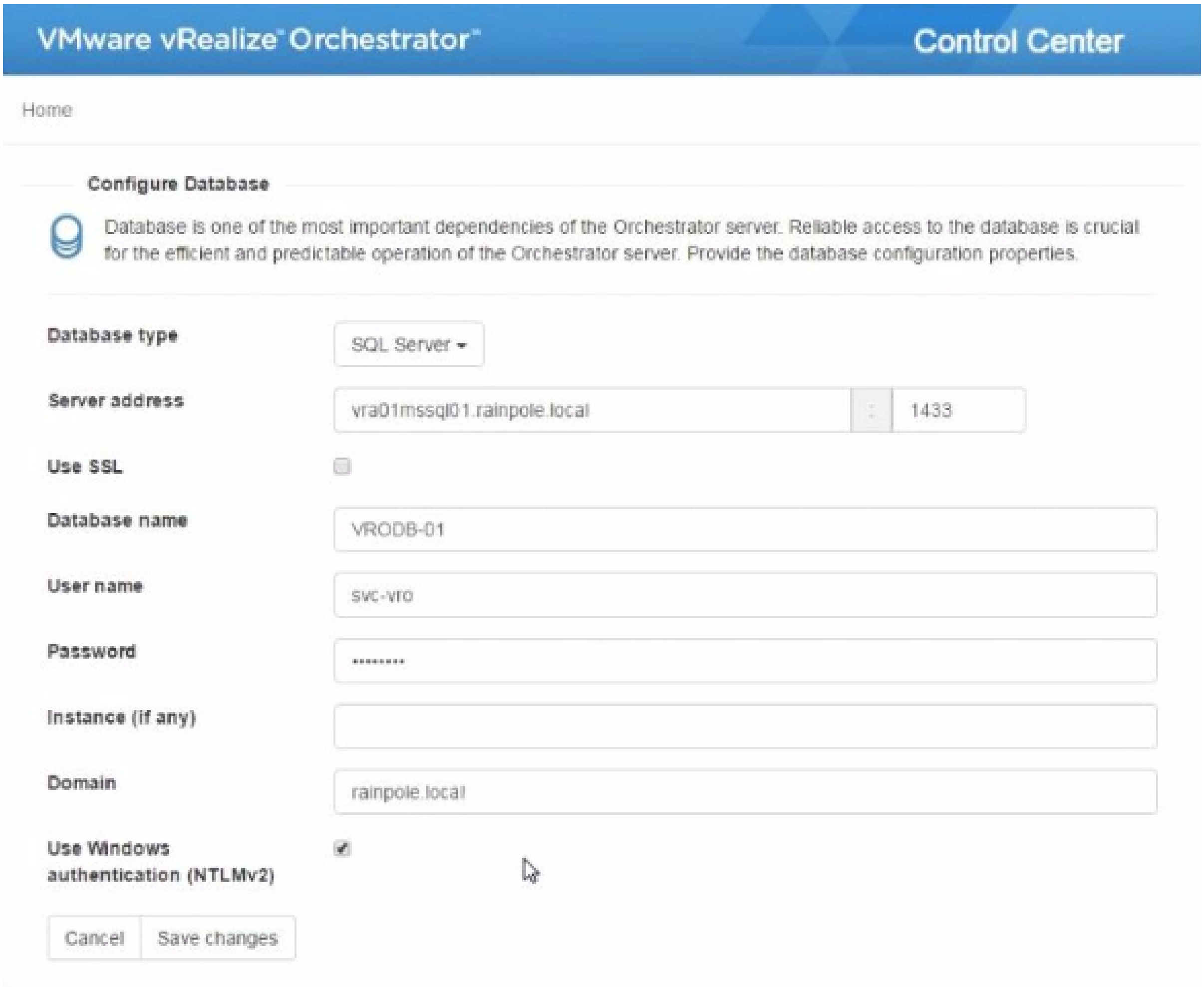
2 Configure the SQL Server database.

a On the **Home** page, under **Database**, click **Configure Database**.

b Enter the following settings to configure the database and click **Save Changes**.

Setting	Value
Database type	SQL Server
Server address	vra01mssql01.rainpole.local:1433
Use SSL	Deselected
Database name	VRODB-01
User name	svc-vro
Password	*svc_vro_password*
Domain	rainpole.local
Use Windows authentication mode (NTLMv2)	Selected

Leave the **Instance (if any)** text box empty if your SQL Server database was installed by using the default server instance name.



Configure Database

Database is one of the most important dependencies of the Orchestrator server. Reliable access to the database is crucial for the efficient and predictable operation of the Orchestrator server. Provide the database configuration properties.

Database type	SQL Server ▾
Server address	vra01mssql01.rainpole.local : 1433
Use SSL	□
Database name	VRODB-01
User name	svc-vro
Password	•••••••••
Instance (if any)	
Domain	rainpole.local
Use Windows authentication (NTLMv2)	☑

   c. Click **Save changes**.
   d. Click **Update Database**.

3. Force re-installation of the vRealize Orchestrator plug-ins.
   a. On the **Home** page, under **Manage**, click **Startup Options**.
   b. Click **Stop**, and click **Home**.
   c. On the **Home** page, under **Monitor and Control**, click **Troubleshooting**.
   d. Click **Force Plug-ins Reinstall**, and click **Home**.
   e. On the **Home** page, under **Manage**, click **Startup Options**.
   f. Click **Start**.

Generate the vRealize Orchestrator Certificate in Region A

vRealize Orchestrator uses two certificates. One of the certificates was previously created using an external Certificate Authority. In this procedure you create a second, self-signed certificate which is used by the appliance to sign workflow packages.

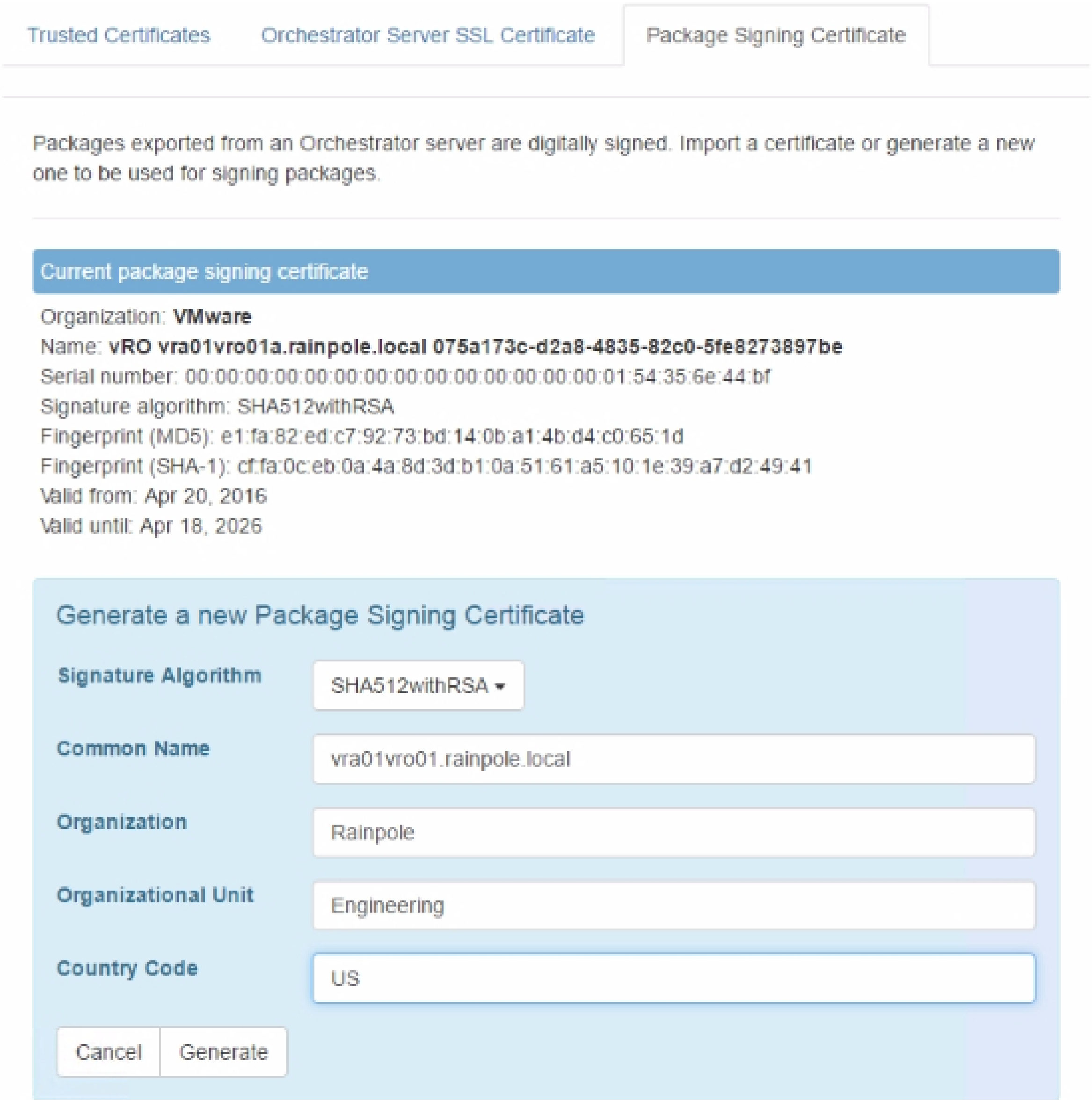
Procedure

1. Log in to the vRealize Orchestrator Control Center.
   a. Open a Web browser and go to `https://vra01vro01a.rainpole.local:8283/vco-controlcenter`.
   b. Log in using the following credentials.

Setting	Value
User name	root
Password	*hostA_root_password*

2. On the **Home** page, under **Manage**, click **Certificates**.
3. Click the **Package Signing Certificate** tab, and click **Generate**.
4. In the **Generate a new Package Signing Certificate** page, specify the following settings and click **Generate**.

Setting	Value
Signature Algorithm	SHA512withRSA
Common Name	vra01vro01.rainpole.local
Organization	Rainpole
Organizational Unit	Engineering
Country Code	US



Trusted Certificates
Orchestrator Server SSL Certificate
Package Signing Certificate

Packages exported from an Orchestrator server are digitally signed. Import a certificate or generate a new one to be used for signing packages.

Current package signing certificate

Organization: **VMware**
Name: **vRO vra01vro01a.rainpole.local 075a173c-d2a8-4835-82c0-5fe8273897be**
Serial number: 00:00:00:00:00:00:00:00:00:00:00:00:00:01:54:35:6e:44:bf
Signature algorithm: SHA512withRSA
Fingerprint (MD5): e1:fa:82:ed:c7:92:73:bd:14:0b:a1:4b:d4:c0:65:1d
Fingerprint (SHA-1): cf:fa:0c:eb:0a:4a:8d:3d:b1:0a:51:61:a5:10:1e:39:a7:d2:49:41
Valid from: Apr 20, 2016
Valid until: Apr 18, 2026

Generate a new Package Signing Certificate

Signature Algorithm	SHA512withRSA ▾
Common Name	vra01vro01.rainpole.local
Organization	Rainpole
Organizational Unit	Engineering
Country Code	US

Wait for confirmation that the certificate generates successfully.

5 Restart the vRealize Orchestrator appliance for the changes to take effect.

a Click **Home** and under **Manage**, click **Startup Options**.

b On the **Startup Options** page, click **Restart**.

Configure the Certificate for vRealize Orchestrator in Region A

Import the previously generated certificates for vRealize Orchestrator from the vRealize Orchestrator Control Center. You must import the certificates on both of the vRealize Orchestrator virtual machines.

For information about the certificate generation process, see "Use the Certificate Generation Utility to Generate CA-Signed Certificates for the SDDC Management Components" in the *VMware Validated Design Planning and Preparation* document.

Procedure

1. Log in to the vRealize Orchestrator Control Center.

   a. Open a Web browser and go to **`https://vra01vro01a.rainpole.local:8283/vco-controlcenter`**.

   b. Log in using the following credentials.

Setting	Value
User name	root
Password	*hostA_root_password*

2. From the **Home** page, under **Manage**, click **Certificates**.
3. Click the **Orchestrator Server SSL Certificate** tab, and click **Import > Import from a PEM-encoded file**.
4. Browse to the `vro.2.chain.pem` file in the `vro` folder on your local machine.
5. In the **Key Password** text box, enter the ***vro_vrealize_full_pem_pass*** password that you entered during certificate generation and click **Import**.
6. Restart the vRealize Orchestrator appliance for the changes to take effect.

   a. From the **Home** page, under **Manage**, click **Startup Options**.

   b. On the **Startup Options** page, click **Restart**.

Install the NSX Plugin for vRealize Orchestrator in Region A

Install the NSX Plugin for vRealize Orchestrator for the virtual appliance that will be part of your vRealize Orchestrator cluster.

Procedure

1. Log in to the vRealize Orchestrator Control Center.

   a. Open a Web browser and go to **`https://vra01vro01a.rainpole.local:8283/vco-controlcenter`**.

   b. Log in using the following credentials.

Setting	Value
User name	root
Password	*hostA_root_password*

2 Install the NSX Plug-in for vRealize Orchestrator.

   a From the **Home** page, under **Plug-Ins**, click **Manage Plug-Ins**.

   b Browse to the NSX Plug-in for vRealize Orchestrator `.vmoapp` file on your local machine, and click **Install**.

   c After the plug-in file loads in the vRealize Control Center, accept the EULA and click **Install**.

   Wait for confirmation that the plug-in to installed successfully

3 Restart the vRealize Orchestrator appliance for the changes to take effect.

   a Click **Home** and under **Manage**, click **Startup Options**.

   b On the **Startup Options** page, click **Restart**.

Configure Component Registry Authentication for vRealize Orchestrator in Region A

After you install the NSX plugin, configure the component registry authentication with vRealize Automation for vRealize Orchestrator.

Use component registry authentication mode when configuring vRealize Orchestrator as an external Orchestrator with a vRealize Automation system. This enables the usage of Single Sign-On authentication through vRealize Automation.

Procedure

1 Log in to the vRealize Orchestrator Control Center.

   a Open a Web browser and go to **`https://vra01vro01a.rainpole.local:8283/vco-controlcenter`**.

   b Log in using the following credentials.

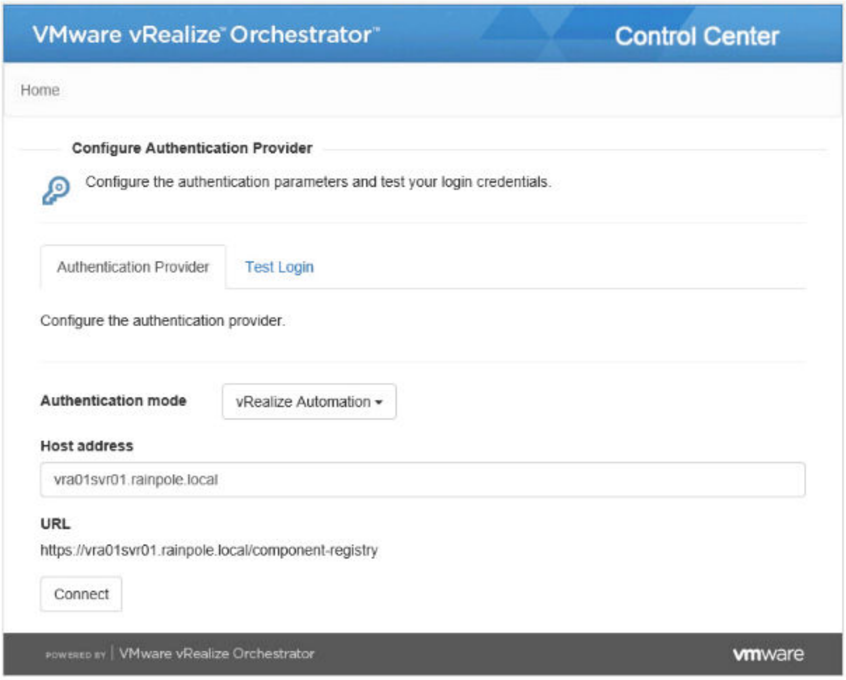
Setting	Value
User name	root
Password	*hostA_root_password*

2 Configure vRealize Automation as a vRealize Orchestrator authentication provider.

   a On the **Home** page, under **Manage** click **Configure Authentication Provider**.

   b On the **Authentication Provider** tab, select **vRealize Automation** from the **Authentication mode** drop-down menu.

c Enter **`vra01svr01.rainpole.local`** in the **Host address** text box and click **Connect**.


VMware vRealize Orchestrator™
Control Center
Home

Configure Authentication Provider

Configure the authentication parameters and test your login credentials.

Authentication Provider
Test Login

Configure the authentication provider.

Authentication mode: vRealize Automation ▾

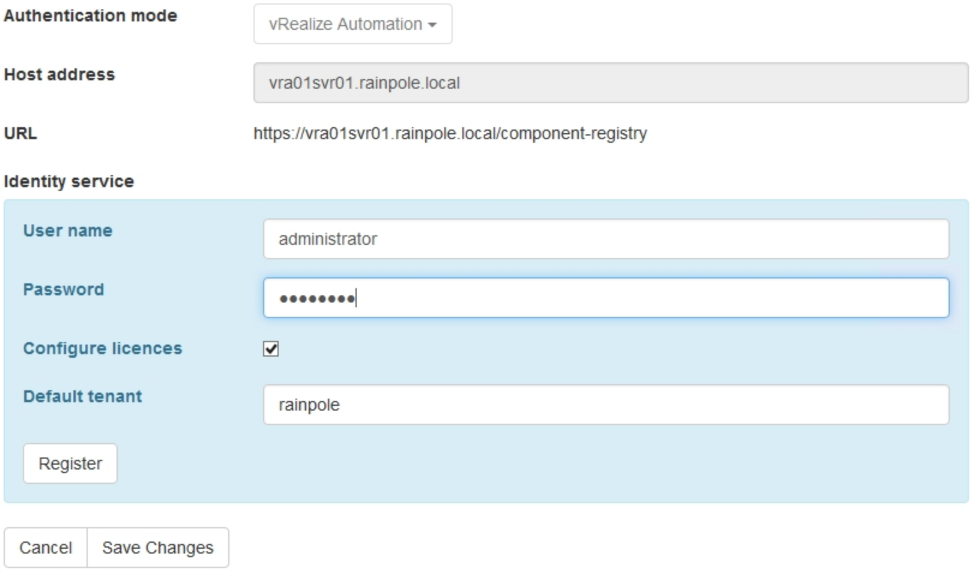
Host address: vra01svr01.rainpole.local

URL: https://vra01svr01.rainpole.local/component-registry

Connect
POWERED BY | VMware vRealize Orchestrator
vmware

d Click **Accept Certificate**, enter the following credentials of the vRealize Automation administrator account, and click **Register**.

Setting	Value
User name	administrator
Password	*vra_administrator_password*
Configure Licenses	Selected
Default Tenant	rainpole



Authentication mode: vRealize Automation

Host address: vra01svr01.rainpole.local

URL: https://vra01svr01.rainpole.local/component-registry

Identity service

User name: administrator

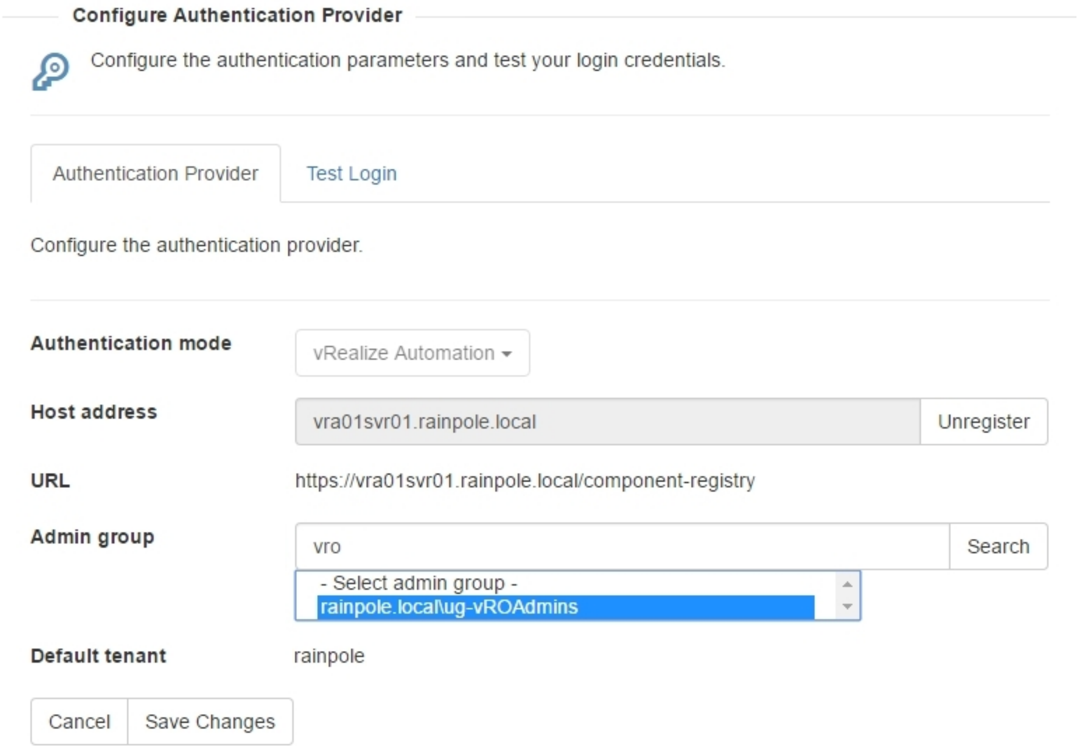
Password: ••••••••

Configure licences: ☑

Default tenant: rainpole

e In the **Admin group** text box, enter **vRO** and click **Search**.

f From the drop-down menu, select **rainpole.local\ug-vROAdmins** and click **Save Changes**.



Configure Authentication Provider

Configure the authentication parameters and test your login credentials.

Configure the authentication provider.

Authentication mode vRealize Automation

Host address vra01svr01.rainpole.local

URL https://vra01svr01.rainpole.local/component-registry

Admin group vro

- Select admin group -
rainpole.local\ug-vROAdmins

Default tenant rainpole

3 Restart the vRealize Orchestrator appliance for the changes to take effect.

a Click **Home** and under **Manage**, click **Startup Options**.

b On the **Startup Options** page, click **Restart**.

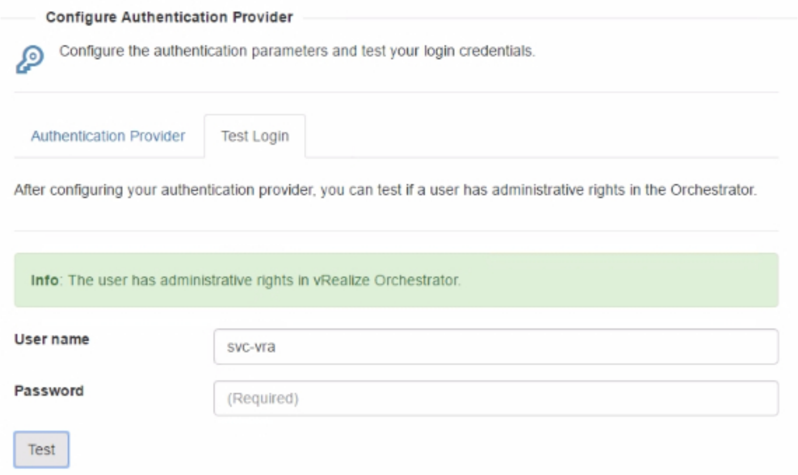
4 Test user administrative rights in vRealize Orchestrator.

   a Click **Home** and under **Manage**, click **Configure Authentication Provider**.

   b On the **Test Login** tab, enter the following credentials and click **Test**.

Setting	Value
User name	svc-vra
Password	*svc-vra_password*

A green banner with the following text appears: "`Info: The user has administrative rights in vRealize Orchestrator`" and confirms that configuration is successful.



Configure Authentication Provider

Configure the authentication parameters and test your login credentials.

After configuring your authentication provider, you can test if a user has administrative rights in the Orchestrator.

Info: The user has administrative rights in vRealize Orchestrator.

User name: svc-vra

Password: (Required)

Validate the Configuration in Region A

You can verify that vRealize Orchestrator is configured properly by opening the **Validate Configuration** page in the Control Center.

Procedure

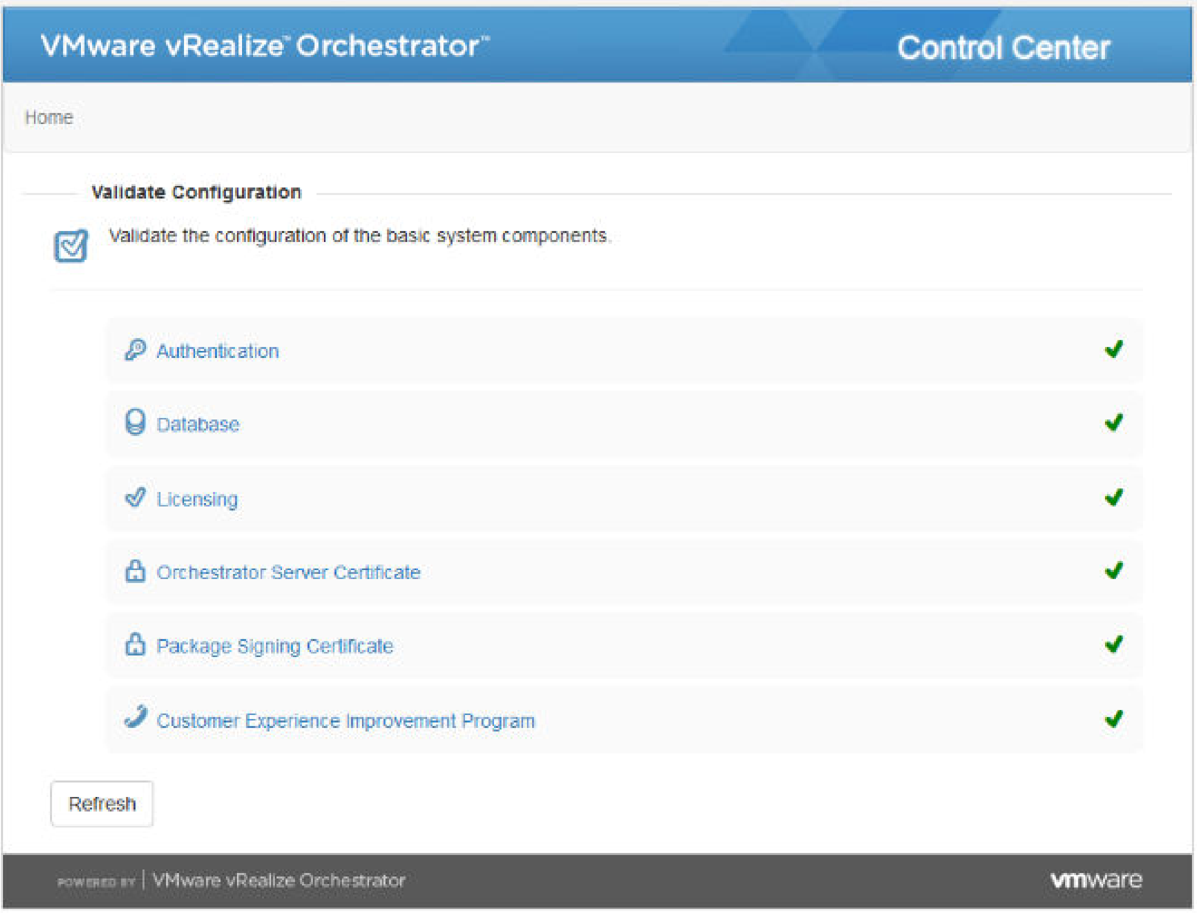
1 Log in to the vRealize Orchestrator Control Center.

   a Open a Web browser and go to **`https://vra01vro01a.rainpole.local:8283/vco-controlcenter`**.

   b Log in using the following credentials.

Setting	Value
User name	root
Password	*hostA_root_password*

2 On the **Home** page, under **Manage**, click **Validate Configuration** and verify that all check marks are green.



VMware vRealize® Orchestrator™
Control Center
Home

Validate Configuration

Validate the configuration of the basic system components.

- Authentication ✓
- Database ✓
- Licensing ✓
- Orchestrator Server Certificate ✓
- Package Signing Certificate ✓
- Customer Experience Improvement Program ✓

Refresh
POWERED BY | VMware vRealize Orchestrator
vmware

Configure vRealize Orchestrator Cluster Mode in Region A

An essential component of all services offered by the SDDC is high availability to the end user. To increase the availability of vRealize Orchestrator, configure a vRealize Orchestrator cluster. A vRealize Orchestrator cluster is a collection of two or more vRealize Orchestrator server instances that share a database.

The final step in cluster setup is configuration of the cluster mode by joining the second node to the first node.

Procedure

1 Log in to the vRealize Orchestrator Control Center.

  a Open a Web browser and go to **`https://vra01vro01b.rainpole.local:8283/vco-controlcenter`**.

  b Log in using the following credentials.

Setting	Value
User name	root
Password	*hostB_root_password*

2 Configure the vRealize Orchestrator cluster mode.

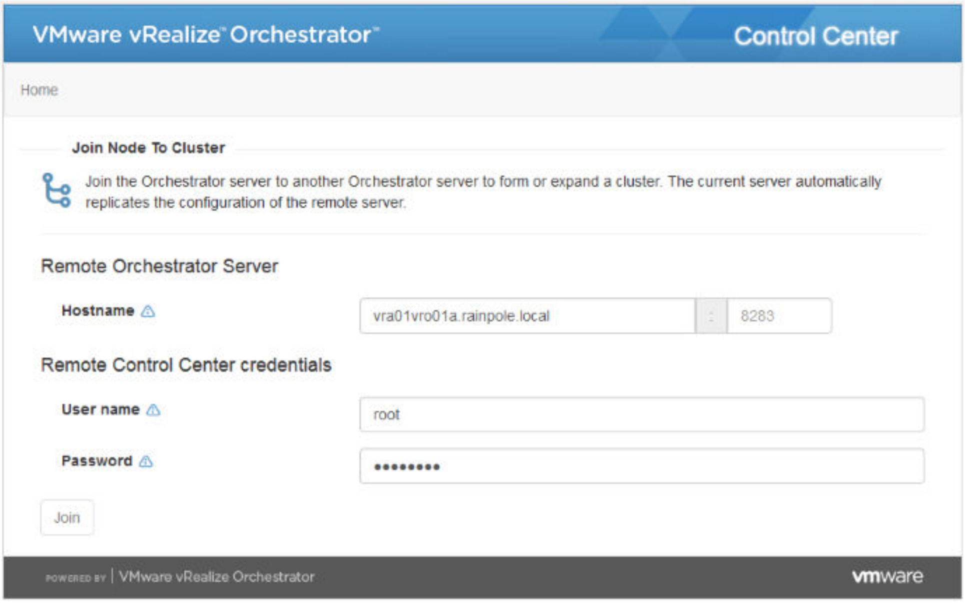
   a On the **Home** page, under **Manage**, click **Orchestrator Node Settings**.

   b In the **Number of active nodes** text box, enter **2**, and click **Save**.

   c Click **Join Node To Cluster**.

   d On the **Join Node To Cluster** page, enter the following values and click **Join** to join the second vRealize Orchestrator appliance to the cluster.

Setting	Value
Hostname	vra01vro01a.rainpole.local
User name	root
Password	*hostA_root_password*


VMware vRealize® Orchestrator™
Control Center
Home

Join Node To Cluster

Join the Orchestrator server to another Orchestrator server to form or expand a cluster. The current server automatically replicates the configuration of the remote server.

Remote Orchestrator Server

Hostname: vra01vro01a.rainpole.local : 8283

Remote Control Center credentials

User name: root

Password: ••••••••

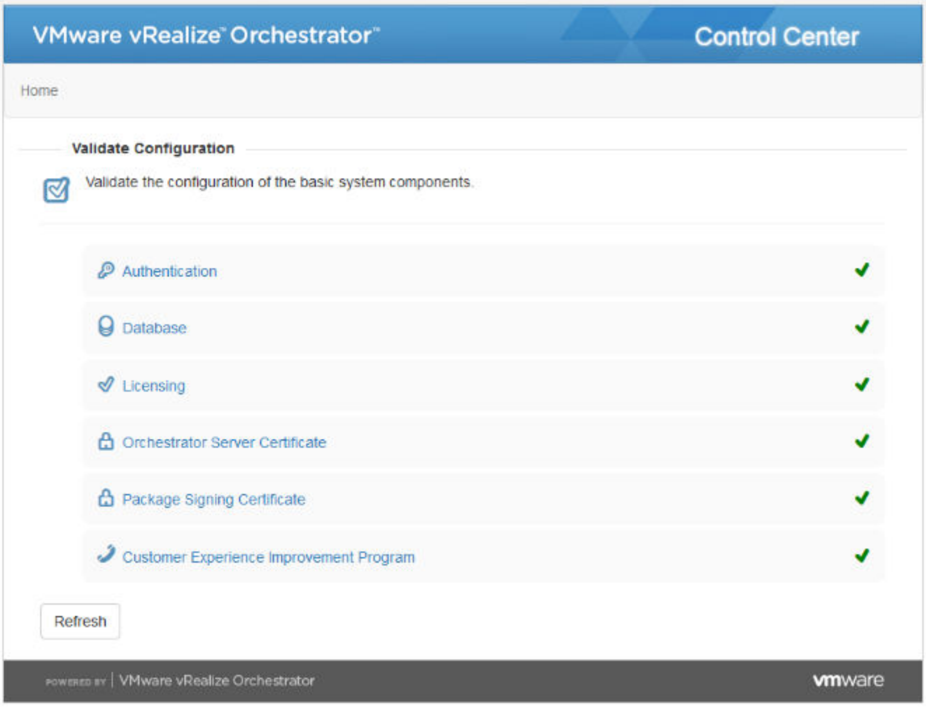
Join
POWERED BY | VMware vRealize Orchestrator
vmware

3 Restart the vRealize Orchestrator service for the changes to take effect.

   a Click **Home** and, under **Manage**, click **Startup Options**.

   b On the **Startup Options** page, click **Restart**.

4 On the **Home** page, under **Manage**, click **Validate Configuration** and verify that all check marks are green.


VMware vRealize Orchestrator
Control Center
Home
Refresh
POWERED BY | VMware vRealize Orchestrator
vmware

Validate Configuration

Validate the configuration of the basic system components.

- Authentication ✓
- Database ✓
- Licensing ✓
- Orchestrator Server Certificate ✓
- Package Signing Certificate ✓
- Customer Experience Improvement Program ✓

Add Compute vCenter Server Instance to vRealize Orchestrator in Region A

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

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 hostname 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**.

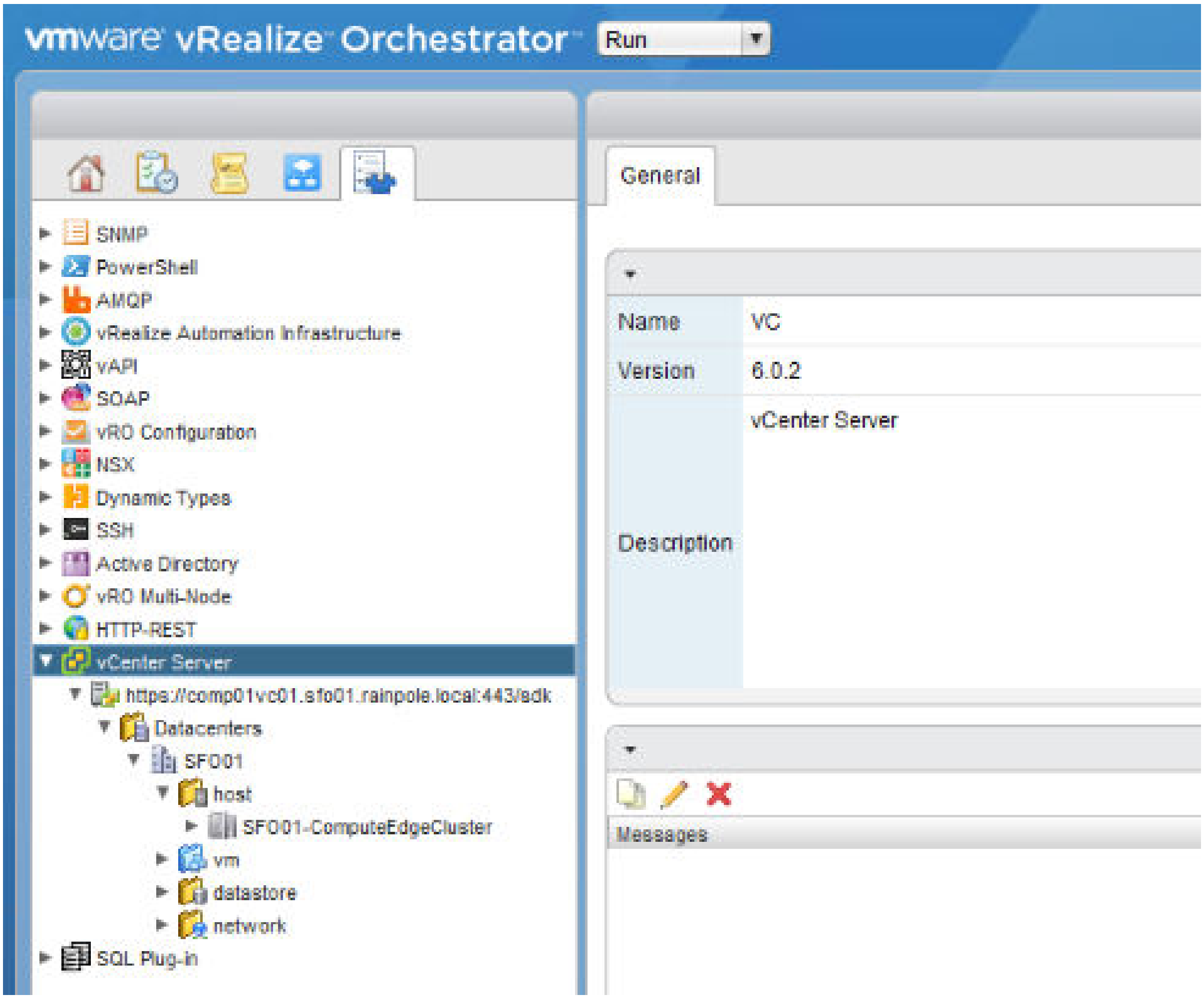
Setting	Value
IP or hostname of the vCenter Server instance to add	comp01vc01.sfo01.rainpole.local
HTTPS port of the vCenter Server instance	443
Location of SDK that you use to connect	/sdk
Will you orchestrate this instance	Yes
Do you want to ignore certificate warnings	Yes

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	rainpole.local\svc-vro
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.



Name	VC
Version	6.0.2
Description	vCenter Server

Integrate vRealize Orchestrator with vRealize Automation in Region A

Configure vRealize Automation to work with the external vRealize Orchestrator instance.

Configure vRealize Orchestrator Server in Region A

To use use vRealize Automation workflows to call vRealize Orchestrator workflows, you must configure vRealize Orchestrator to act as an endpoint.

Procedure

1 Log in to the vRealize Automation portal.

   a Open a Web browser and go to **`https://vra01svr01.rainpole.local/vcac`**.

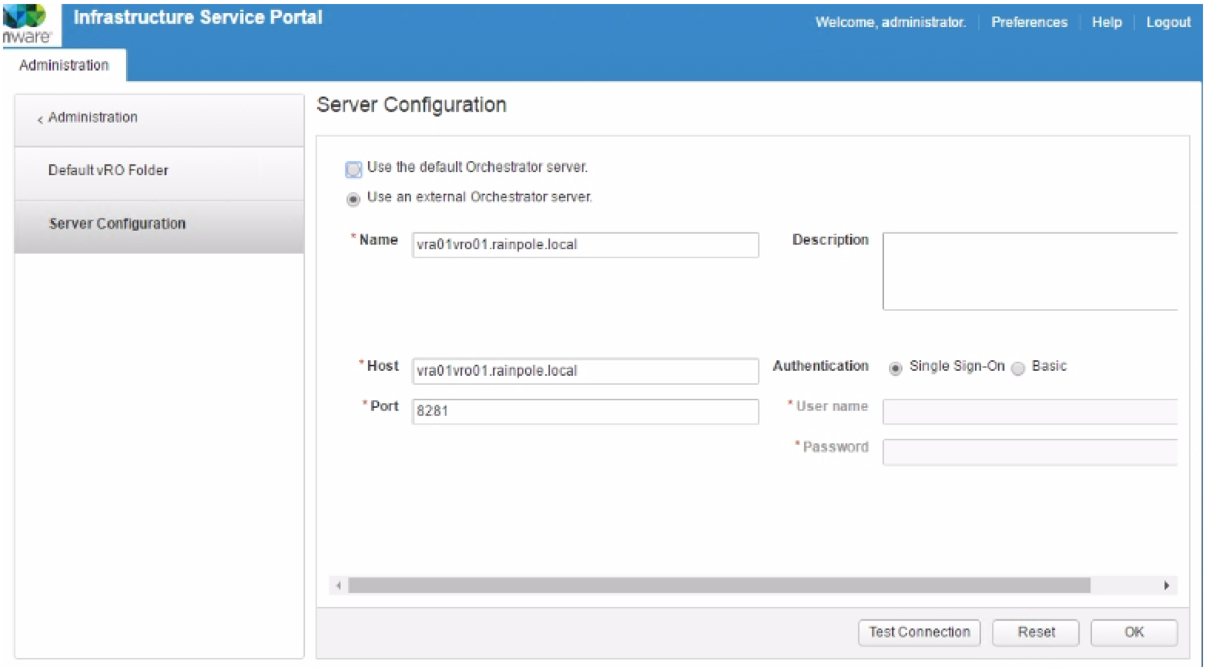
   b Log in using the following credentials.

Setting	Value
User name	administrator
Password	*vra_administrator_password*

2 Click **Advanced Services > vRO Configuration**.

3 On the **Server Configuration** page, select the **Use an external Orchestrator server** radio button, enter the following settings, and click **Test Connection**.

Setting	Value
Name	vra01vro01.rainpole.local
Host	vra01vro01.rainpole.local
Port	8281
Authentication	Single Sign-On



Server Configuration

○ Use the default Orchestrator server.

● Use an external Orchestrator server.

* Name	vra01vro01.rainpole.local	Description	
* Host	vra01vro01.rainpole.local	Authentication	● Single Sign-On ○ Basic
* Port	8281	* User name	
		* Password	

4 Click **OK** to save the settings and click **OK** to accept the warning message that appears.

A confirmation message will confirm the successful configuration of vRealize Orchestrator as an endpoint.

Create a vRealize Orchestrator Endpoint in Region A

IaaS administrators are responsible for creating the endpoints that allow vRealize Automation to communicate with your infrastructure. You create a vRealize Orchestrator endpoint for use by Realize Automation to communicate workflows.

Procedure

1 Log in to the Rainpole Infrastructure Service Portal.

   a Open a Web browser and go to `https://vra01svr01.rainpole.local/vcac/org/rainpole`.

   b From the **Select your domain** drop-down menu select **Rainpole.local** and click **Next**

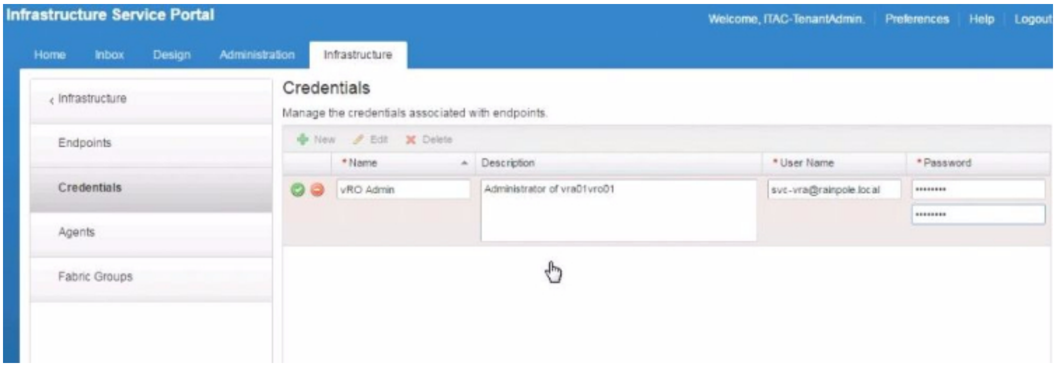
   c Log in using the following credentials.

Setting	Value
User name	itac-tenantadmin
Password	*itac_tenantadmin_password*
Domain	rainpole.local

2 Select **Infrastructure > Endpoints > Credentials**.

3 Click **New** to create a credential for the vRealize Orchestrator administrator, configure the following values, and click **Save**.

Setting	Value
Name	vRO Admin
Description	Administrator of vra01vro01
User Name	svc-vra@rainpole.local
Password	*svc-vra_password*



Credentials

Manage the credentials associated with endpoints.

*Name	Description	*User Name	*Password
vRO Admin	Administrator of vra01vro01	svc-vra@rainpole.local	•••••••• ••••••••

4 Create a new endpoint for vRealize Orchestrator.

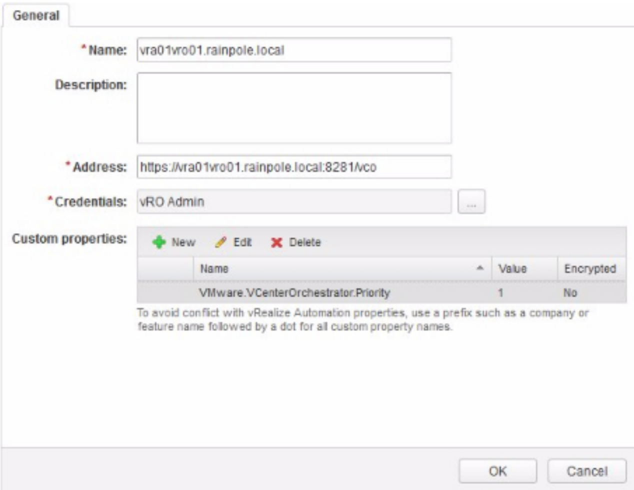
a Select **Infrastructure > Endpoints > Endpoints**.

b Click **New > Orchestration > vRealize Orchestrator**, configure the following values, and click **New** to add a custom property.

Setting	Value
Name	vra01vro01.rainpole.local
Address	https://vra01vro01.rainpole.local:8281/vco
Credentials	vRO Admin

c Configure the following values for the custom property, click **Save**, and click **OK**.

Setting	Value
Name	VMware.VCenterOrchestrator.Priority
Valure	1
Encrypted	Deselected



*Name: vra01vro01.rainpole.local

Description:

*Address: https://vra01vro01.rainpole.local:8281/vco

*Credentials: vRO Admin

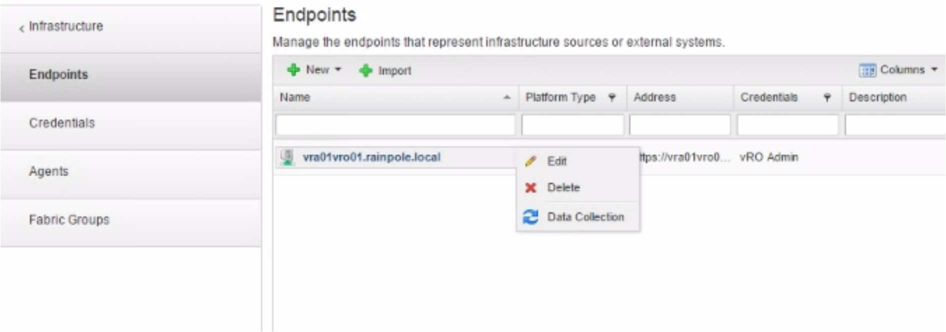
Custom properties:

Name	Value	Encrypted
VMware.VCenterOrchestrator.Priority	1	No

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.

5 Start the data collection for the newly created endpoint.

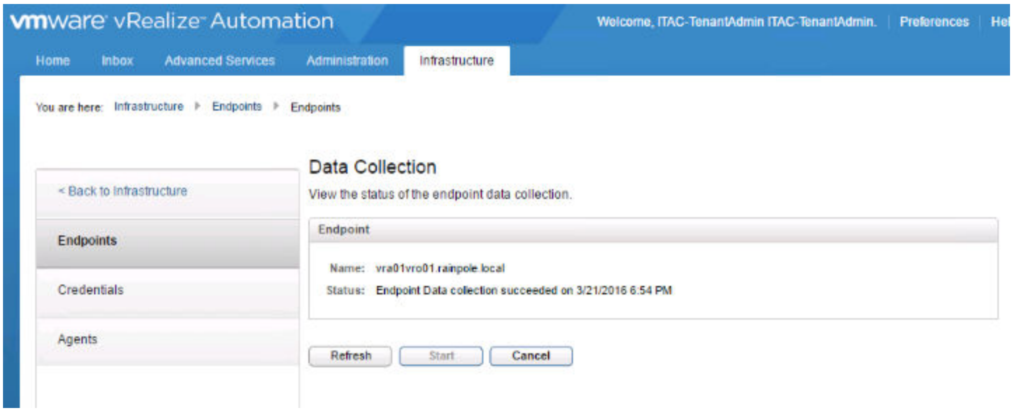
a Hover the vRealize Orchestrator endpoint in the Endpoints list and click **Data Collection**.



b Click **Start** to begin the vRealize Orchestrator data collection process. Wait several minutes for the data collection process to complete.

c Click **Refresh** to verify that the data collection successfully complete.

When a data collection success status message appears, the configuration process is complete.



Data Collection

View the status of the endpoint data collection.

Endpoint

Name: vra01vro01.rainpole.local

Status: Endpoint Data collection succeeded on 3/21/2016 6:54 PM

Add vRealize Automation Host in vRealize Orchestrator in Region A

To call vRealize Automation Plugin workflows, you configure the vRealize Automation host in vRealize Orachestrator.

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 vRealize Orchestrator Host A using the following hostname 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 > vRealize Automation > Configuration**.

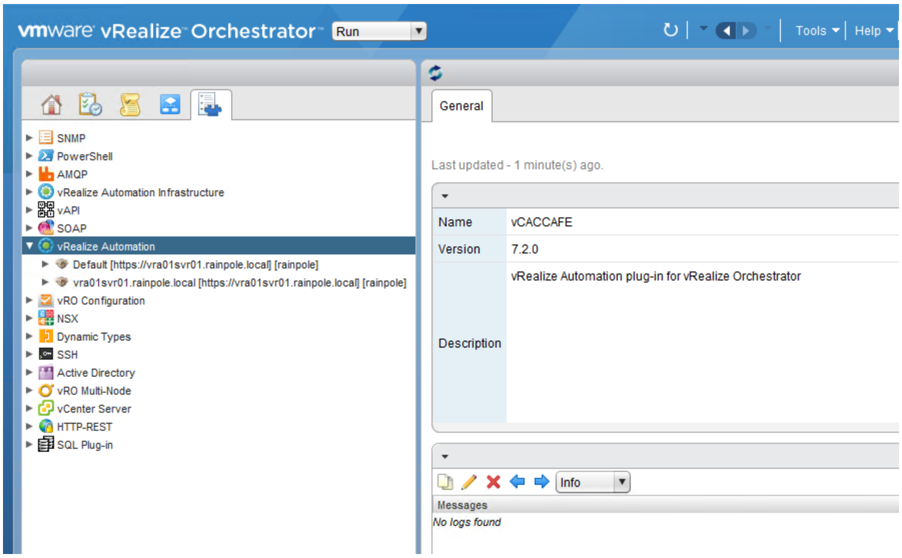
3 Right-click the **Add a vRA host using component registry** workflow and click **Start Workflow**.

a On the **Common parameters** page, configure the following settings, and click **Submit**.

Setting	Value
Name of the vCAC host	vra01svr01.rainpole.local
Connection timeout	30.0
Operation timeout	60.0

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

The vRealize Automation Server instance that you just added is visible in the inventory.


vmware vRealize Orchestrator
Run
Tools
Help
SNMP
PowerShell
AMQP
vRealize Automation Infrastructure
vAPI
SOAP
vRealize Automation
Default [https://vra01svr01.rainpole.local] [rainpole]
vra01svr01.rainpole.local [https://vra01svr01.rainpole.local] [rainpole]
vRO Configuration
NSX
Dynamic Types
SSH
Active Directory
vRO Multi-Node
vCenter Server
HTTP-REST
SQL Plug-in
General
Info
Messages

Last updated - 1 minute(s) ago.

Name	vCACCAFE
Version	7.2.0
Description	vRealize Automation plug-in for vRealize Orchestrator

No logs found

5 In the left pane, click **Workflows**, and navigate to **Library > vRealize Automation > Configuration**.

6 Right-click the **Add the IaaS host of a vRA host** workflow and click **Start Workflow**.

   a On the **Common parameters** page, select **vra01svr01.rainpole.local [https://vra01svr01.rainpole.local] [rainpole]** for **vCAC host**, and click **Next**.

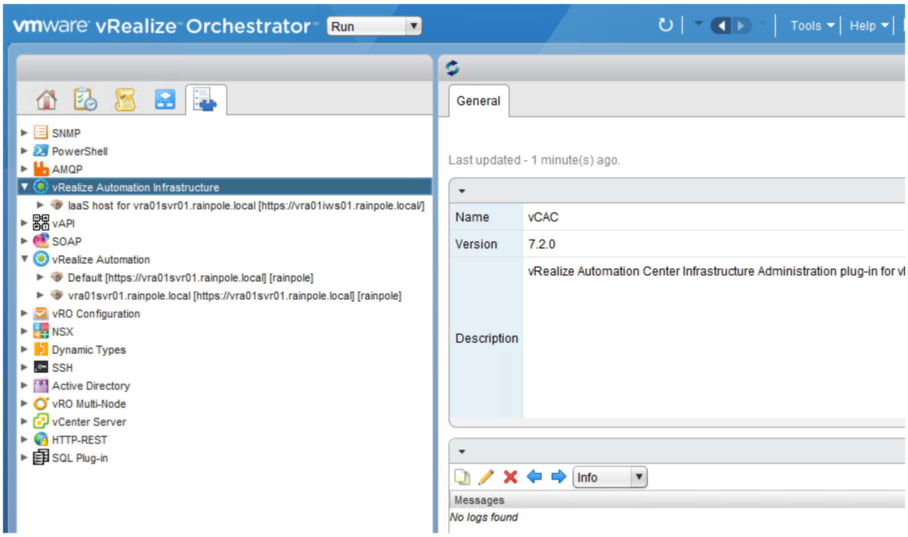
   b On the **Add an IaaS host** page, keep the default settings for **Host Properties** and click **Next**.

   c On the **Add an IaaS host** page, keep the default settings for the **Proxy Settings** and click **Next**.

   d On the **Host Authentication** page, select **SSO** for **Host's authentication type**, and click **Submit**.

7 To verify that the workflow completed successfully, click the **Inventory** tab and expand the **vRealize Automation Infrastructure** tree control.

   The vRealize Automation IaaS Server instance you added is visible in the inventory.


vmware vRealize Orchestrator
Run
Tools
Help
SNMP
PowerShell
AMQP
vRealize Automation Infrastructure
IaaS host for vra01svr01.rainpole.local [https://vra01iws01.rainpole.local/]
vAPI
SOAP
vRealize Automation
Default [https://vra01svr01.rainpole.local] [rainpole]
vra01svr01.rainpole.local [https://vra01svr01.rainpole.local] [rainpole]
vRO Configuration
NSX
Dynamic Types
SSH
Active Directory
vRO Multi-Node
vCenter Server
HTTP-REST
SQL Plug-in
General
Info

Last updated - 1 minute(s) ago.

Name	vCAC
Version	7.2.0
Description	vRealize Automation Center Infrastructure Administration plug-in for vl

Messages

No logs found

vRealize Business Installation in Region A

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 their data center.

Deploy the vRealize Business Virtual Appliances in Region A

VMware vRealize Business provides capabilities that allow users to gain greater visibility into financial aspects of their cloud infrastructure and let them optimize and improve these operations.

You deploy two instances of vRealize Business, a Server and a Data Collector. Repeat this procedure twice to deploy the two appliances.

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 Click **Hosts and Clusters** and navigate to the **mgmt01vc01.sfo01.rainpole.local** vCenter Server object.

3 Right-click the **mgmt01vc01.sfo01.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 for the respective appliance that you deploy and click **Next**.

Setting	Value for Server	Value for Data Collector
Name	vra01bus01.rainpole.local	vra01buc01.sfo01.rainpole.local
Select a datacenter or folder	vRA01	vRA01IAS

6 On the **Select a resource** page, select the **SFO01-Mgmt01** cluster and click **Next**.

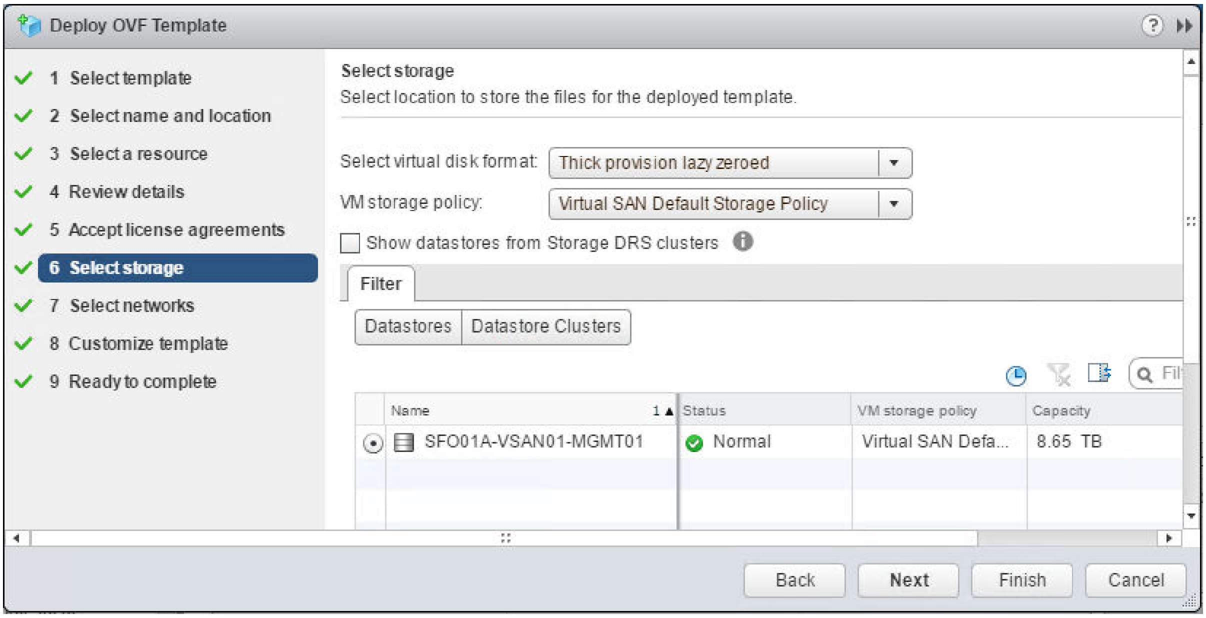
7 On the **Review details** page, examine the virtual appliance details, such as product, version, download and disk size, and click **Next**.

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 **vSAN Default Storage Policy** from the **VM storage policy** drop-down menu.

b From the datastore table, select the **SFO01A-VSAN01-MGMT01** vSAN datastore and click **Next**.



Select storage

Select location to store the files for the deployed template.

Select virtual disk format: Thick provision lazy zeroed

VM storage policy: Virtual SAN Default Storage Policy

□ Show datastores from Storage DRS clusters

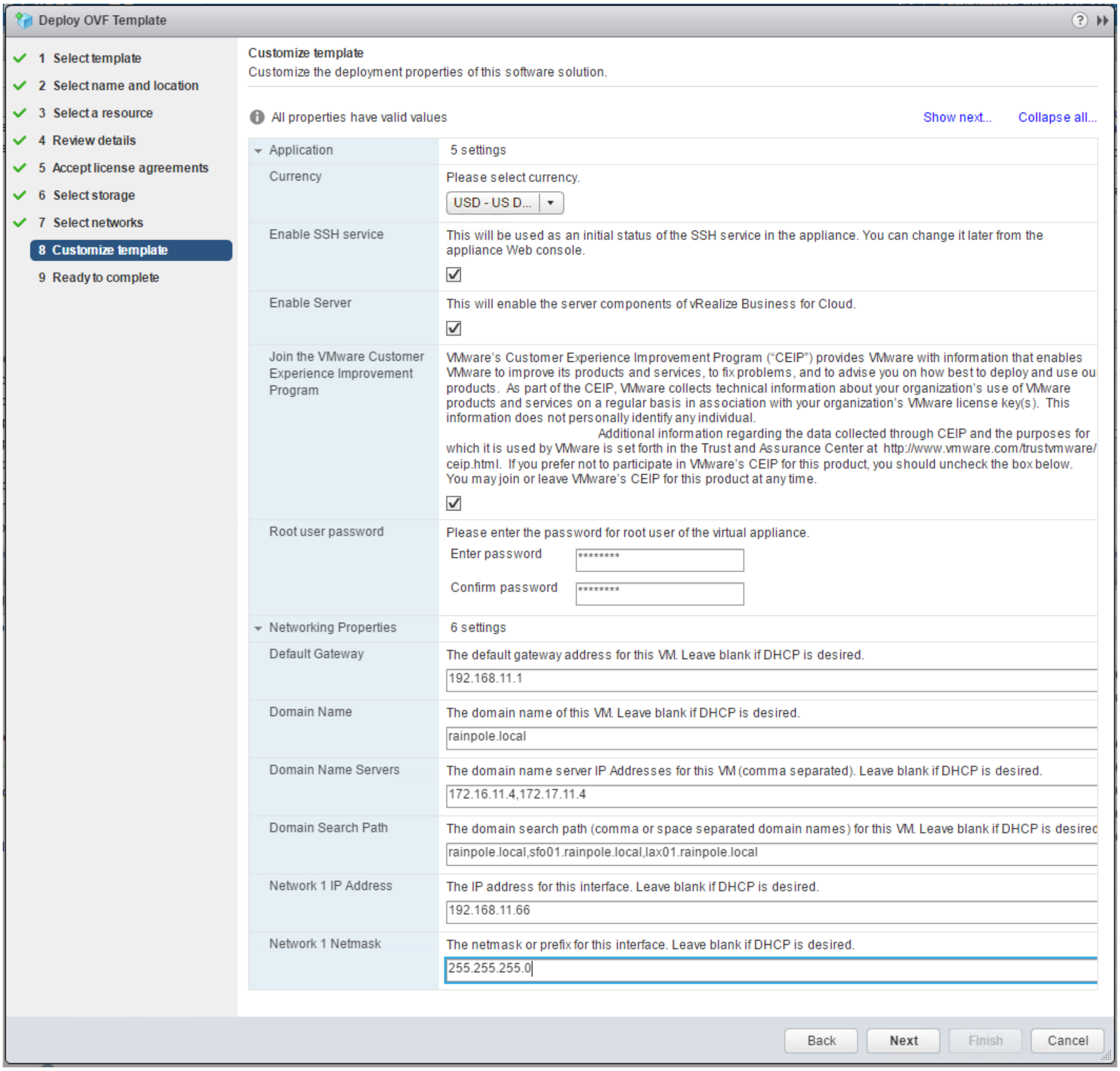
	Name	Status	VM storage policy	Capacity
●	SFO01A-VSAN01-MGMT01	Normal	Virtual SAN Defa...	8.65 TB

10 On the **Select networks** page, select the appropriate network from the **Destination** drop-down menu, and click **Next**.

Setting	Value for Server	Value for Data Collector
Network 1	Ends with Mgmt-xRegion01-VXLAN	Ends with Mgmt-RegionA01-VXLAN

11 On the **Customize template** page, configure the following values and click **Next**.

Setting	Values for Server	Values for Data Collector
Currency	USD	USD
Enable SSH service	Selected	Selected
Enable Server	Selected	Deselected
Join the VMware Customer Experience Improvement Program	Selected	Selected
Root user password	*vrb_server_root_password*	*vrb_collector_root_password*
Default Gateway	192.168.11.1	192.168.13.1
Domain Name	rainpole.local	sfo01.rainpole.local
Domain Name Servers	172.16.11.4,172.17.11.4	172.16.11.5,172.16.11.4
Domain Search Path	rainpole.local,sfo01.rainpole.local,lax01.rainpole.local	sfo01.rainpole.local
Network 1 IP Address	192.168.11.66	192.168.31.54
Network 1 Netmask	255.255.255.0	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

Application	5 settings
Currency	Please select currency. USD - US D... ▾
Enable SSH service	This will be used as an initial status of the SSH service in the appliance. You can change it later from the appliance Web console. ☑
Enable Server	This will enable the server components of vRealize Business for Cloud. ☑
Join the VMware Customer Experience Improvement Program	VMware's Customer Experience Improvement Program ("CEIP") provides VMware with information that enables VMware to improve its products and services, to fix problems, and to advise you on how best to deploy and use ou products. As part of the CEIP, VMware collects technical information about your organization's use of VMware products and services on a regular basis in association with your organization's VMware license key(s). This information does not personally identify any individual. Additional information regarding the data collected through CEIP and the purposes for which it is used by VMware is set forth in the Trust and Assurance Center at http://www.vmware.com/trustvmware/ceip.html. If you prefer not to participate in VMware's CEIP for this product, you should uncheck the box below. You may join or leave VMware's CEIP for this product at any time. ☑
Root user password	Please enter the password for root user of the virtual appliance. Enter password ******** Confirm password ********
Networking Properties	6 settings
Default Gateway	The default gateway address for this VM. Leave blank if DHCP is desired. 192.168.11.1
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. 172.16.11.4,172.17.11.4
Domain Search Path	The domain search path (comma or space separated domain names) for this VM. Leave blank if DHCP is desirec rainpole.local,sfo01.rainpole.local,lax01.rainpole.local
Network 1 IP Address	The IP address for this interface. Leave blank if DHCP is desired. 192.168.11.66
Network 1 Netmask	The netmask or prefix for this interface. Leave blank if DHCP is desired. 255.255.255.0

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

13 Change the vRealize Business virtual appliance memory size.

a Right-click the **vra01bus01.rainpole.local** virtual machine and select **Edit Settings**.

b Click **Virtual Hardware**, enter `8GB` for **Memory**, and click **OK**.

c Right-click the **vra01buc01.sfo01.rainpole.local** virtual machine and select **Edit Settings**.

d Click **Virtual Hardware**, enter `2GB` for **Memory**, and click **OK**.

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

15 Repeat this procedure to deploy the vRealize Business Data Collector vra01buc01.sfo01.rainpole.local.

Configure SSL Certificate for vRealize Business Server in Region A

Import the previously generated certificates for vRealize Business from the vRealize Business appliance management console.

Prerequisites

Verify that you have access to the vRealize Business certificates. For more information, see "Use the Certificate Generation Utility to Generate CA-Signed Certificates for the SDDC Management Components" in the *VMware Validated Design Planning and Preparation* document.

Procedure

1 Log in to the vRealize Business Server appliance management console.

   a Open a Web browser and go to **`https://vra01bus01.rainpole.local:5480`**.

   b Log in using the following credentials.

Setting	Value
User name	root
Password	*vrb_server_root_password*

2 Click the **Administration** tab and click **SSL**.

3 On the **Replace SSL Certificate** page, select **Import PEM encoded Certificate** from the **Choose mode** drop down menu.

4 Enter the values from the previously-generated certificate for vRealize Business and click **Replace Certificate**.

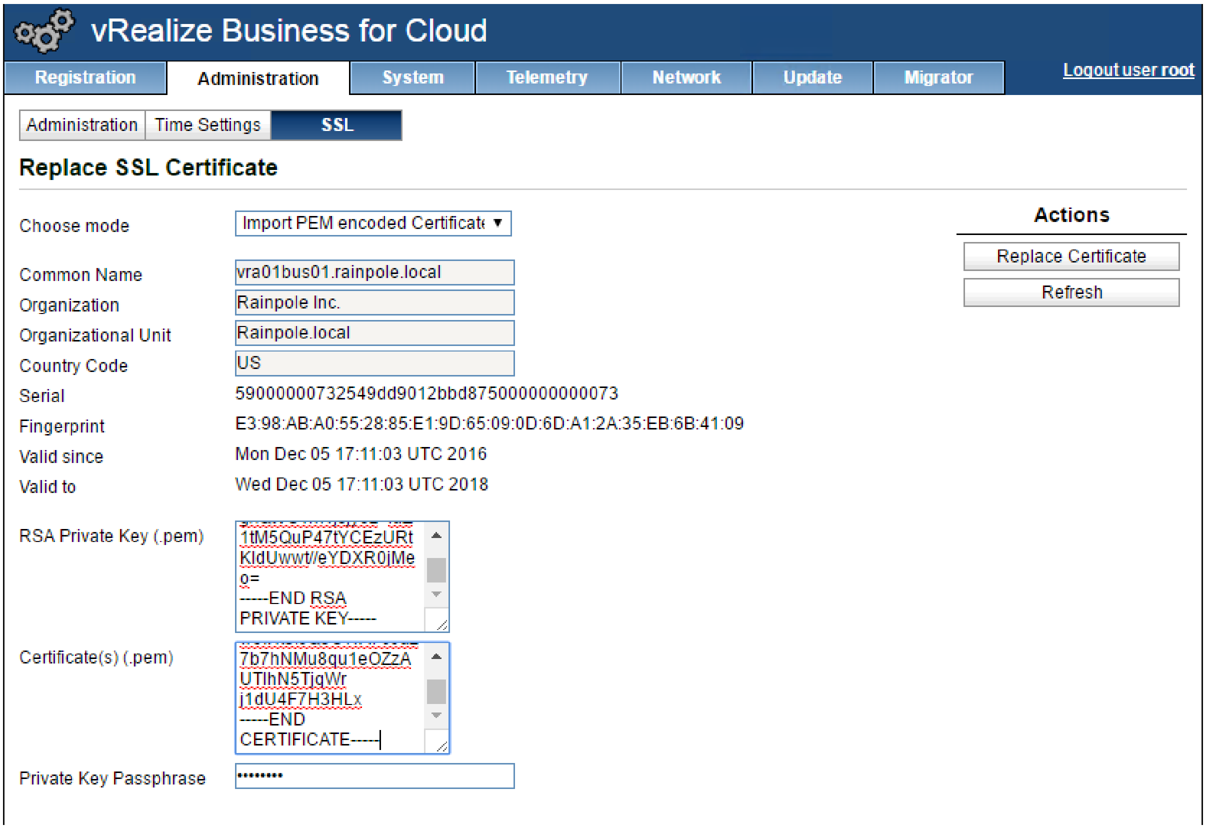
   Use the `vrb.key` file as the **RSA Private Key (.key)** and the `vrb.3.pem` file for the **Certificate(s) (.pem)** entry. These files are in the `vrb` folder that you created during certificate generation.

Setting	Value
Choose mode	Import PEM encoded Certificate

RSA Private Key (.key)	`------BEGIN RSA PRIVATE KEY-----`
	`private_key_value`
	`-----END RSA PRIVATE KEY-----`

Certificate(s) (.pem)	`-----BEGIN CERTIFICATE-----`
	`Server_certificate_value`
	`-----END CERTIFICATE-----`
	`-----BEGIN CERTIFICATE-----`
	`Intermediate_CA`
	`-----END CERTIFICATE-----`
	`-----BEGIN CERTIFICATE-----`
	`Root_CA_certificate_value`
	`-----END CERTIFICATE-----`

Private Key Passphrase	*vrb_cert_passphrase*



Replace SSL Certificate

Choose mode	Import PEM encoded Certificate ▾
Common Name	vra01bus01.rainpole.local
Organization	Rainpole Inc.
Organizational Unit	Rainpole.local
Country Code	US
Serial	59000000732549dd9012bbd875000000000073
Fingerprint	E3:98:AB:A0:55:28:85:E1:9D:65:09:0D:6D:A1:2A:35:EB:6B:41:09
Valid since	Mon Dec 05 17:11:03 UTC 2016
Valid to	Wed Dec 05 17:11:03 UTC 2018
RSA Private Key (.pem)	1tM5QuP47tYCEzURt KldUwwt/eYDXR0jMe o= -----END RSA PRIVATE KEY-----
Certificate(s) (.pem)	7b7hNMu8qu1eOZzA UTlhN5TjqWr j1dU4F7H3HLx -----END CERTIFICATE-----
Private Key Passphrase	••••••••

5 Verify that the certificate changed successfully.

A message appears that informs you that the SSL certificate was successfully configured.

6 Click the **System** tab and click **Reboot** for the changes to take effect.

Configure NTP for vRealize Business in Region A

Configure the network time protocol (NTP) on both vRealize business appliances from the virtual appliance management interface (VAMI).

Perform the procedure on both vRealize Business Server and vRealize Business Data Collector virtual appliances.

Host	VAMI URL
Server	https://vra01bus01.rainpole.local:5480
Data Collector	https://vra01buc01.sfo01.rainpole.local:5480

Procedure

1 Log in to the vRealize Business Server appliance management console.

   a Open a Web browser and go to **`https://vra01bus01.rainpole.local:5480`**.

   b Log in using the following credentials.

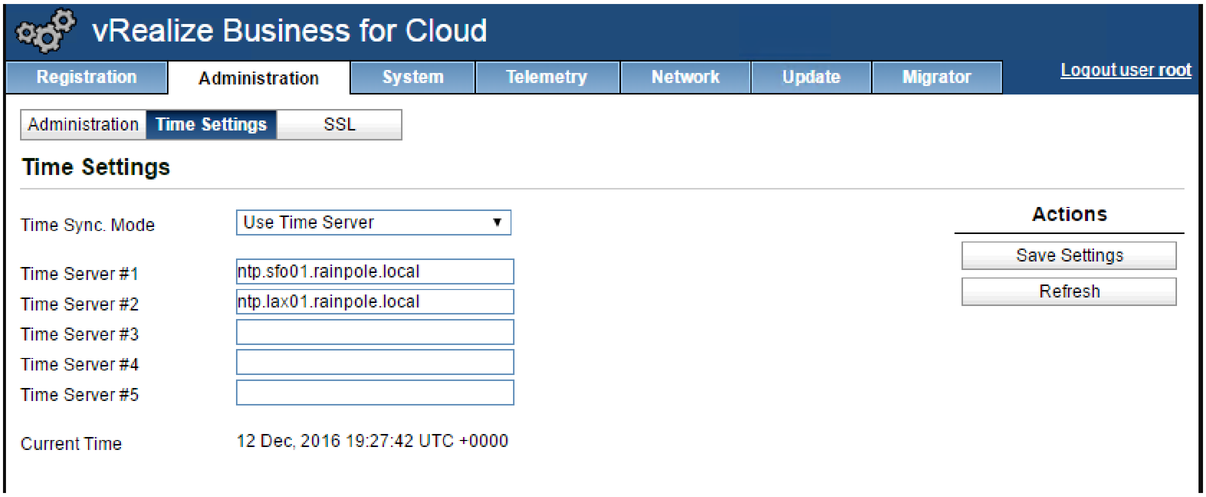
Setting	Value
User name	root
Password	*vrb_server_root_password*

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	Value
Time Sync. Mode	Use Time Server
Time Server #1	ntp.sfo01.rainpole.local
Time Server #2	ntp.lax01.rainpole.local



Time Settings

Time Sync. Mode	Use Time Server ▾
Time Server #1	ntp.sfo01.rainpole.local
Time Server #2	ntp.lax01.rainpole.local
Time Server #3	
Time Server #4	
Time Server #5	
Current Time	12 Dec, 2016 19:27:42 UTC +0000

3 Repeat the procedure on the vRealize Business Data Collector virtual appliance vra01buc01.sfo01.rainpole.local.

Integrate vRealize Business with vRealize Automation in Region A

To prepare vRealize Business for use, you must register the vRealize Business Server to vRealize Automation by using the management interface.

Procedure

1 Log in to the vRealize Business Server appliance management console.

a Open a Web browser and go to **`https://vra01bus01.rainpole.local:5480`**.

b Log in using the following credentials.

Setting	Value
User name	root
Password	*vrb_server_root_password*

2 On the **vRealize Automation** tab, enter the following credentials to register with the vRealize Automation server.

Setting	Value
Hostname	vra01svr01.rainpole.local
SSO Default Tenant	rainpole
SSO Admin User	administrator
SSO Admin Password	*vra_administrator_password*
Accept "vRealize Automation" certificate	Deselected

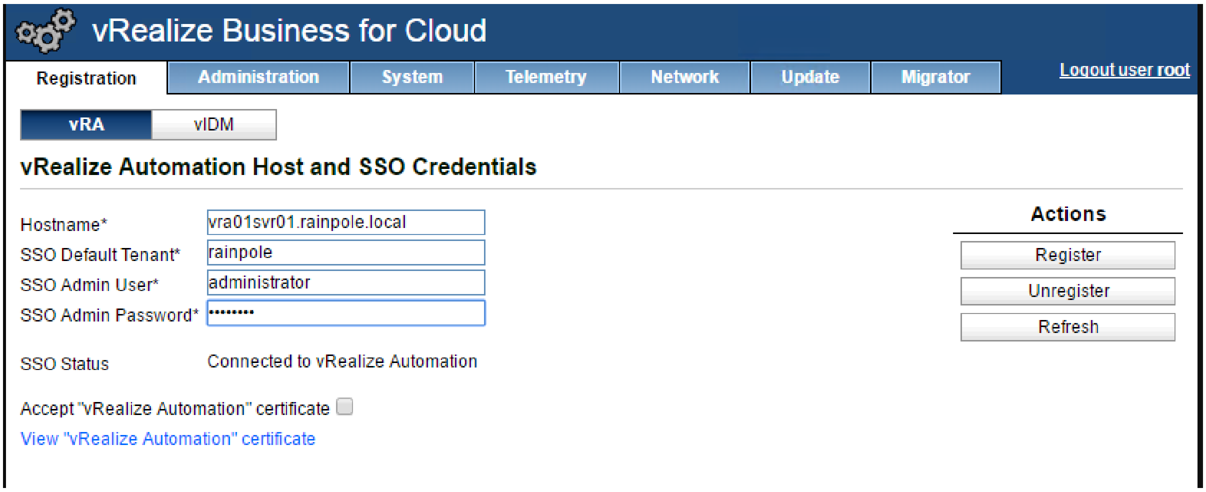
3 Click **Register** to connect to vRealize Automation and get its certificate.

A failure message appears at the top of the page. Wait until the SSO Status changes to `The certificate of "vRealize Automation" is not trusted. Please view and accept to register.`

4 Click the **View "vRealize Automation" certificate** link to download the vRealize Automation certificate.

5 Select the **Accept "vRealize Automation" certificate** check box and click **Register**.

SSO Status changes to `Connected to vRealize Automation`.



vRealize Automation Host and SSO Credentials

Hostname*	vra01svr01.rainpole.local
SSO Default Tenant*	rainpole
SSO Admin User*	administrator
SSO Admin Password*	••••••••
SSO Status	Connected to vRealize Automation
Accept "vRealize Automation" certificate	□

Register the vRealize Business Data Collector with the Server in Region A

After you integrate vRealize Business with vRealize Automation, you connect the two vRealize Business appliances.

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.

- Grant an added role to the tenant admin, enter product license key, and 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.

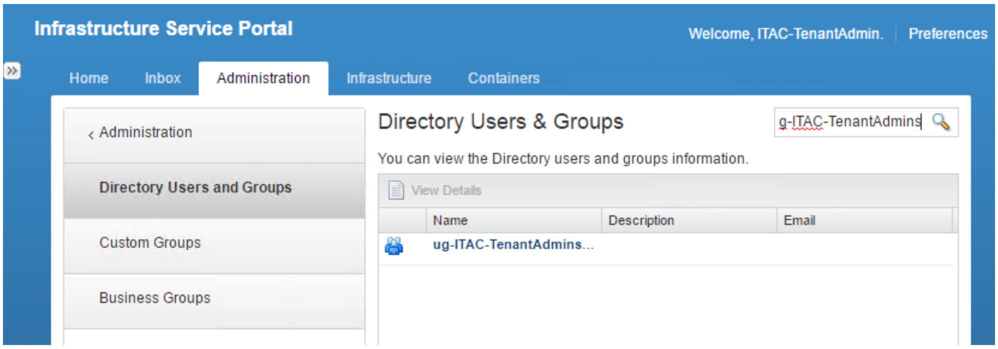
   a Open a Web browser and go to **`https://vra01svr01.rainpole.local/vcac/org/rainpole`**.

   b Log in using the following credentials.

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

2 Navigate to **Administration > Users & Groups > Directory Users & Groups**.

3 In the search text box, enter **`ug-ITAC-TenantAdmins`**.



Directory Users & Groups

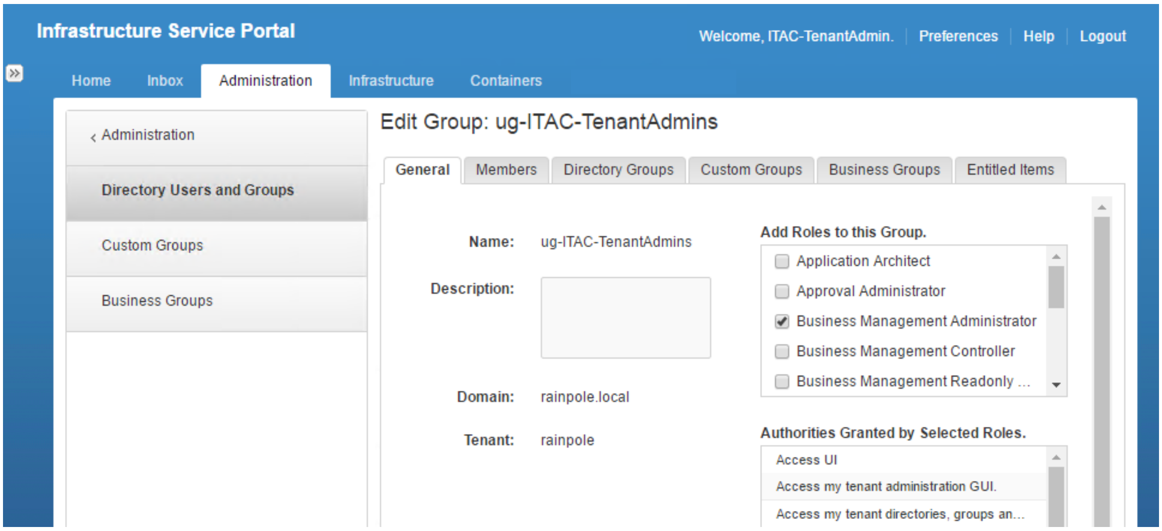
g-ITAC-TenantAdmins

You can view the Directory users and groups information.

Name	Description	Email
ug-ITAC-TenantAdmins...		

4 Click the **ug-ITAC-TenantAdmins** group to edit its settings.

5 On the **Edit Group** page, in the **Add Roles to this Group** list, select the **Business Management Administrator** role to add the role and click **Finish**.



Edit Group: ug-ITAC-TenantAdmins

Name: ug-ITAC-TenantAdmins

Description:

Domain: rainpole.local

Tenant: rainpole

Add Roles to this Group.

□ Application Architect
□ Approval Administrator
☑ Business Management Administrator
□ Business Management Controller
□ Business Management Readonly ...

Authorities Granted by Selected Roles.

Access UI
Access my tenant administration GUI.
Access my tenant directories, groups an...

6 Log out, and log in again by using the same credentials.

7 Assign a license to the vRealize Business solution.

  a Click the **Business Management** tab.

  b Under **License**, enter your serial number for vRealize Business and click **Save**.

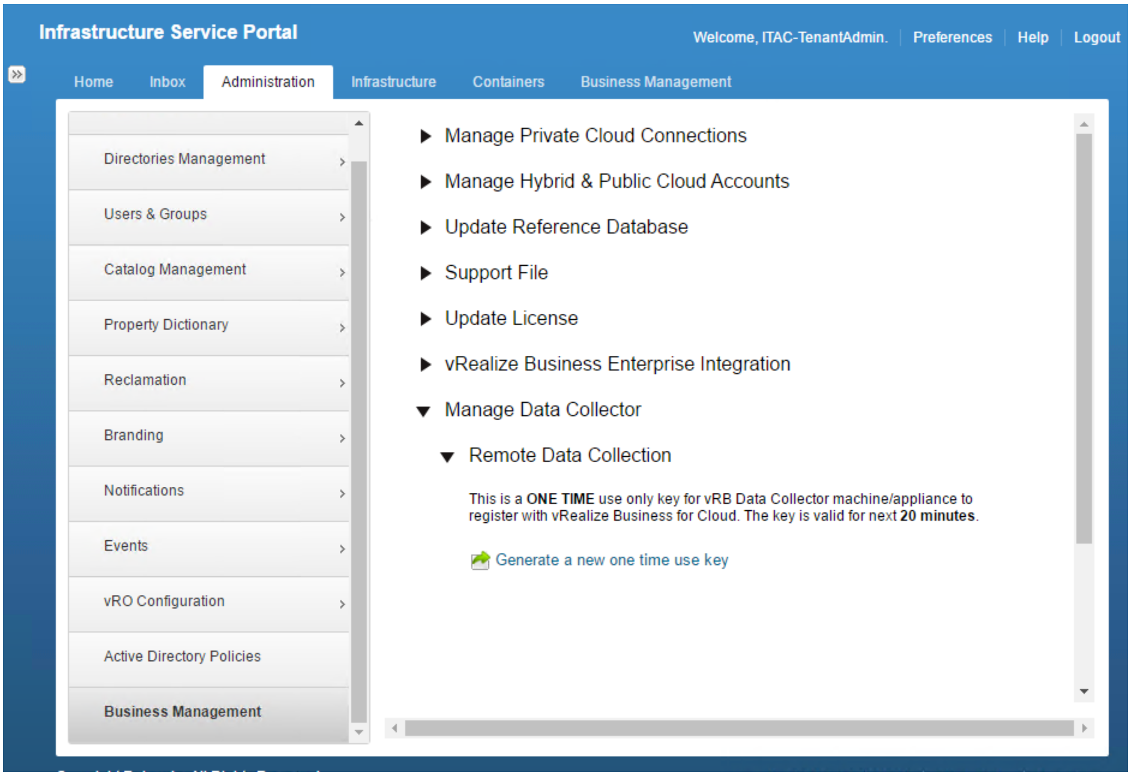
8 Generate a one-time use key for connecting the two vRealize Business appliances.

  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 at a later stage in the implementation sequence.



This is a **ONE TIME** use only key for vRB Data Collector machine/appliance to register with vRealize Business for Cloud. The key is valid for next **20 minutes**.

9 Log in to the vRealize Business Data Collector console.

a Open a Web browser and go to `https://vra01buc01.sfo01.rainpole.local:9443/dc-ui`.

b Log in using the following credentials.

Setting	Value
User name	root
Password	*vrb_collector_root_password*

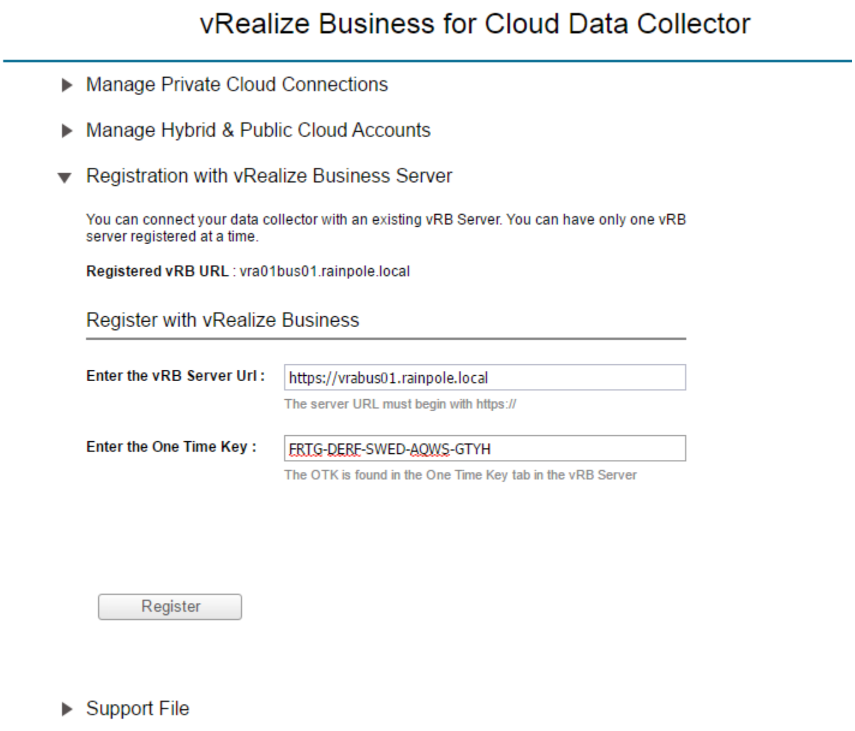
10 Register the Data Collector with the vRealize Business Server.

a Expand the **Registration with the vRealize Business Server** section.

b Enter the following values and click **Register**.

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

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



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 : vra01bus01.rainpole.local

Register with vRealize Business

Enter the vRB Server Url : https://vrabus01.rainpole.local

The server URL must begin with https://

Enter the One Time Key : FRTG-DERF-SWED-AQWS-GTYH

The OTK is found in the One Time Key tab in the vRB Server

▶ Support File

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

The vRealize Business appliances are now connected.

Connect vRealize Business with the Compute vCenter Server in Region A

vRealize Business requires communication with the Compute 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://vra01buc01.sfo01.rainpole.local:9443/dc-ui`**.

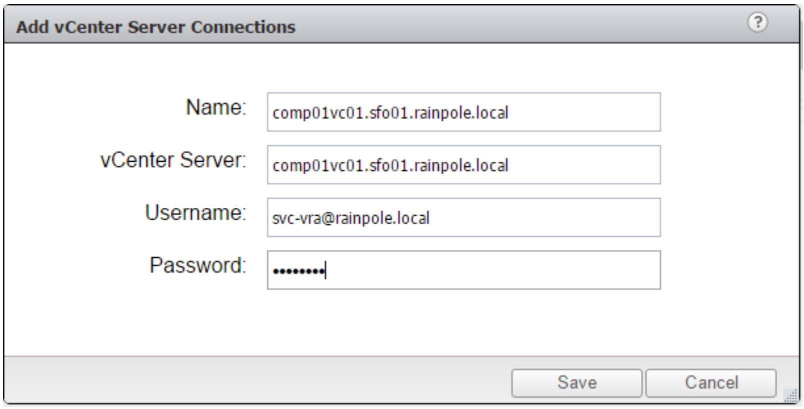
   b Log in using the following credentials.

Setting	Value
User name	root
Password	*vrb_collector_root_password*

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	comp01vc01.sfo01.rainpole.local
vCenter Server	comp01vc01.sfo01.rainpole.local
Username	svc-vra@rainpole.local
Password	*svc_vra_password*



Add vCenter Server Connections

Name: comp01vc01.sfo01.rainpole.local

vCenter Server: comp01vc01.sfo01.rainpole.local

Username: svc-vra@rainpole.local

Password: ••••••••

4 In the **SSL Certificate warning** dialog box, click **Install**.

5 In the **Success** dialog box, click **OK**.

Cloud Management Platform Post-Installation Tasks in Region A

After vRealize Automation and vRealize Orchestrator have been deployed, anti-affinity rules must be created to enable HA protection for both services. Health monitors must be enabled to monitor the health status of individual servers. The snapshots created during the vRealize Automation installation must also be deleted.

Create Anti-Affinity Rules for vRealize Automation and vRealize Orchestrator Virtual Machines in Region A

After deploying the vRealize Automation and vRealize Orchestrator appliances, 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.

Perform the procedure six times to create six unique anti-affinity rules.

Table 3-4. Anti-affinity Rules for the Cloud Management Platform

Name	Type	Members
anti-affinity-rule-vra-svr	Separate Virtual Machines	vra01svr01a.rainpole.local, vra01svr01b.rainpole.local
anti-affinity-rule-vra-iws	Separate Virtual Machines	vra01iws01a.rainpole.local, vra01iws01b.rainpole.local
anti-affinity-rule-vra-ims	Separate Virtual Machines	vra01ims01a.rainpole.local, vra01ims01b.rainpole.local
anti-affinity-rule-vra-dem	Separate Virtual Machines	vra01dem01.rainpole.local, vra01dem02.rainpole.local
anti-affinity-rule-vra-ias	Separate Virtual Machines	vra01ias01.sfo01.rainpole.local, vra01ias02.sfo01.rainpole.local
anti-affinity-rule-vro	Separate Virtual Machines	vra01vro01a.rainpole.local, vra01vro01b.rainpole.local

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 From the **Home** page, click **Hosts and Clusters**.

3 Under **mgmt01vc01.sfo01.rainpole.local**, click **SFO01**, and click **SFO01-Mgmt01**.

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-svr`.

b Select the **Enable rule** check box.

c Select **Separate Virtual Machines** from the **Type** drop-down menu.

d Click **Add**, select the **vra01svr01a.rainpole.local** and **vra01svr01b.rainpole.local** virtual machines, click **OK**, and click **OK**.

7 Repeat the procedure to configure the remaining anti-affinity rules.

Create VM Groups to Define the Startup Order of the Cloud Management Platform in Region A

VM Groups allow you to define the startup order of virtual machines. The startup order you define ensures that vSphere HA powers on virtual machines in the correct order.

Procedure

1 Log in to the Management 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 In the **Navigator**, select **Host and Clusters** and expand the **mgmt01vc01.sfo01.rainpole.local** tree.

3 Create a VM Group for the vRealize Automation IaaS Database.

a Select the **SFO01-Mgmt01** cluster and click the **Configure** tab.

b On the **Configure** page, click VM/Host Groups.

c On the **VM/Host Groups** page, click the **Add** button.

d In the **Create VM/Host Group** dialog, enter `vRealize Automation IaaS Database` in the **Name** field, select **VM Group** from the **Type** drop down, and click the **Add** button.

e In the **Add VM/Host Group Member** dialog, select **vra01mssql01.rainpole.local** and click **OK**.

f Click **OK** to save the VM/Host Group.

4 Repeat step 3 to create the following VM/Host Groups.

VM/Host Group Name	VM/Host Group Member
vRealize Automation Virtual Appliances	vra01svr01a.rainpole.local vra01svr01b.rainpole.local
vRealize Automation IaaS Web Servers	vra01iws01a.rainpole.local vra01iws01b.rainpole.local
vRealize Automation IaaS Managers	vra01ims01a.rainpole.local vra01ims01b.rainpole.local

VM/Host Group Name	VM/Host Group Member
vRealize Automation IaaS DEM Workers	vra01dem01.rainpole.local vra01dem02.rainpole.local
vRealize Automation IaaS Proxy Agents	vra01ias01.sfo01.rainpole.local vra01ias02.sfo01.rainpole.local
vRealize Orchestrators	vra01vro01a.rainpole.local vra01vro01b.rainpole.local
vRealize Business Servers	vra01bus01.rainpole.local
vRealize Business Remote Collectors	vra01buc01.sfo01.rainpole.local

5 Create a rule to power on the vRealize Automation Database before the vRealize Automation Virtual Appliances.

  a Select the **SFO01-Mgmt01** cluster and click the **Configure** tab.

  b On the **Configure** page, click **VM/Host Rules**.

  c On the **VM/Host Rules** page, click the **Add** button.

  d In the **Create VM/Host Rule** dialog, enter `SDDC Cloud Management Platform 01` in the **Name** field, ensure that the **Enable Rule** check box is selected, select **Virtual Machines to Virtual Machines** from the **Type** drop down.

  e Select **vRealize Automation Database** for the **First restart VMs in VM group** drop down list.

  f Select **vRealize Orchestrators** for the **Then restart VMs in VM group** drop down list

  g Click **OK** to save the rule.

6 Repeat step 5 to create the following VM/Host Rules to ensure the correct restart order for your Cloud Management Platform.

VM/Host Rule Name	First restart VMs in VM group	Then restart VMs in VM group
SDDC Cloud Management Platform 02	vRealize Orchestrators	vRealize Automation Virtual Appliances
SDDC Cloud Management Platform 03	vRealize Automation Virtual Appliances	vRealize Automation IaaS Web Servers
SDDC Cloud Management Platform 04	vRealize Automation IaaS Web Servers	vRealize Automation IaaS Managers
SDDC Cloud Management Platform 05	vRealize Automation IaaS Managers	vRealize Automation IaaS DEM Workers
SDDC Cloud Management Platform 06	vRealize Automation IaaS Managers	vRealize Automation IaaS Proxy Agents
SDDC Cloud Management Platform 07	vRealize Automation IaaS Managers	vRealize Business Servers
SDDC Cloud Management Platform 08	vRealize Business Servers	vRealize Business Remote Collectors

Enable Load Balancer Health Monitoring in Region A

Previously you disabled health monitoring for the SFOMGMT-LB01 load balancer to complete configuration of vRealize Automation. You may now re-enable health monitoring for the SFOMGMT-LB01 load balancer.

you perform this procedure multiple times to configure the health monitor, and to enable the second member for the server pools as described in the following table.

Pool Name	Monitor	Enable Pool Member
vra-svr-443	vra-svr-443-monitor	vra01svr01b
vra-svr-8444	vra-svr-443-monitor	-
vra-iaas-web-443	vra-iaas-web-443-monitor	vra01iws01b
vra-iaas-mgr-443	vra-iaas-mgr-443-monitor	vra01ims01b
vra-vro-8281	vra-vro-8281-monitor	vra01vro01b

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. In the **Navigator**, click **Networking & Security**, and select **NSX Edges**.

3. Select **172.16.11.65** from the **NSX Manager** drop-down menu, and double-click **SFOMGMT-LB01** to edit its settings.

4. Click the **Manage** tab, click **Load Balancer**, and select **Pools**.

5. From the pools table, select the **vra-svr-443** server pool, and click **Edit** icon.

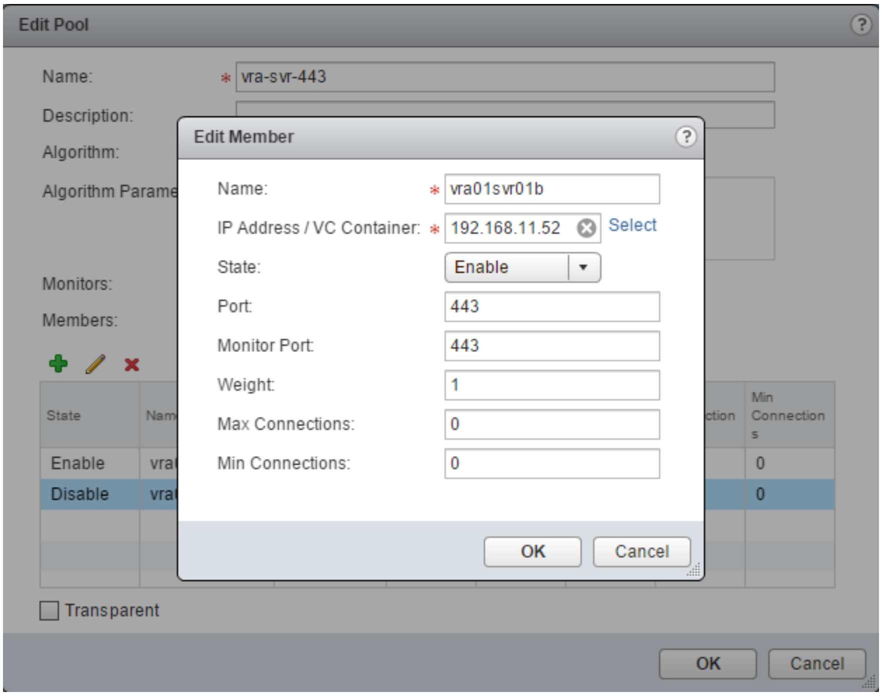
6. In the **Edit Pool** dialog box, configure the monitor, and enable the member that is not enabled.

   a. From the **Monitors** drop-down menu, select **vra-svr-443-monitor**.

   b. From the **Members** table, select **vra01svr01b** and click **Edit** icon.

c In the **Edit Member** dialog box, select the **Enable** for **State** and click **OK**.

d Click **OK** to close the **Edit Pool** dialog box.



Edit Pool

Name: * vra-svr-443

Description:

Algorithm:

Algorithm Parame

Monitors:

Members:

State	Nam	ction	Min Connections
Enable	vra		0
Disable	vra		0

□ Transparent

Edit Member

Name: * vra01svr01b

IP Address / VC Container: * 192.168.11.52

State: Enable

Port: 443

Monitor Port: 443

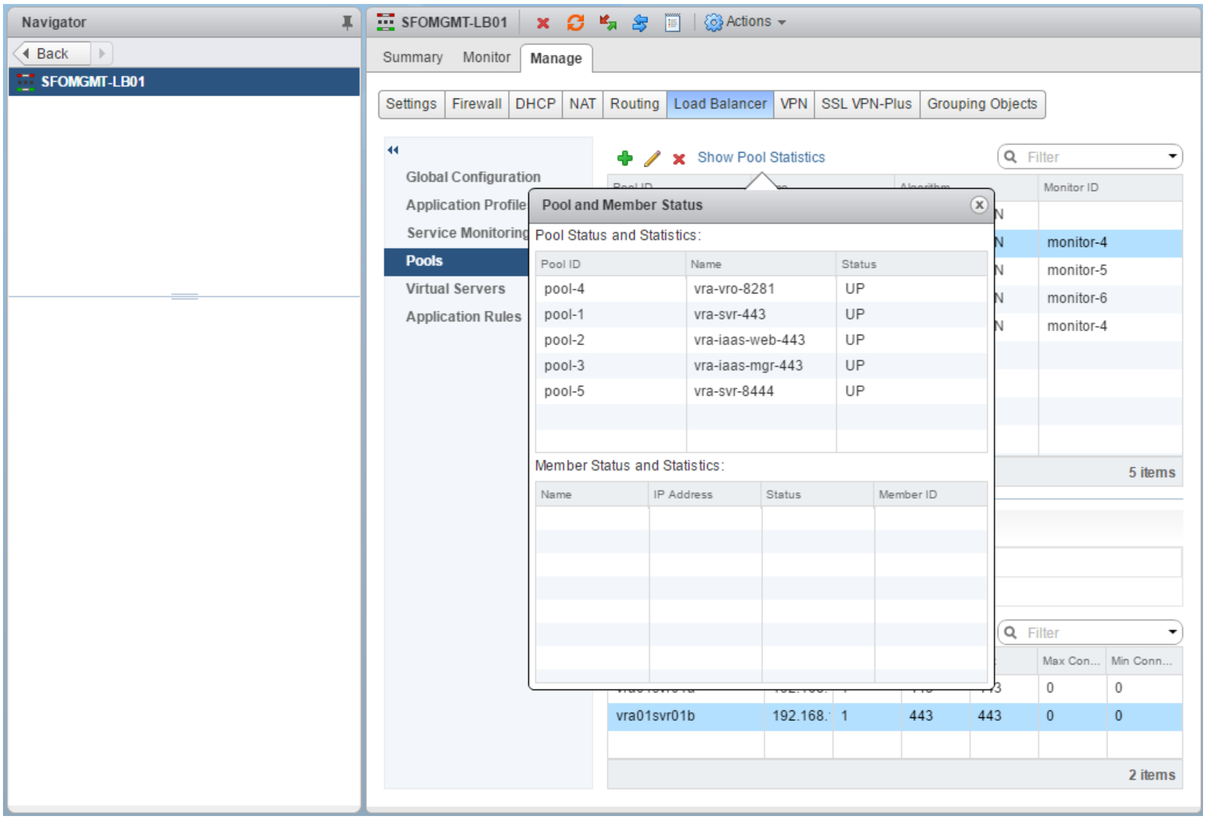
Weight: 1

Max Connections: 0

Min Connections: 0

7 Repeat the procedure to configure the health monitor and enable the second member for the remaining server pools.

8 Click **Show Pool Statistics** and make sure all the server pools **Status** show as **UP**.



Pool and Member Status

Pool Status and Statistics:

Pool ID	Name	Status
pool-4	vra-vro-8281	UP
pool-1	vra-svr-443	UP
pool-2	vra-iaas-web-443	UP
pool-3	vra-iaas-mgr-443	UP
pool-5	vra-svr-8444	UP

Member Status and Statistics:

Name	IP Address	Status	Member ID

Clean Up the vRealize Automation VM Snapshots in Region A

You made snapshots of each vRealize virtual machine during the vRealize Automation installation process. After you successfully complete the installation, you can delete these snapshots.

you repeat this procedure to remove all of the vRealize Automation virtual machine snapshots you created during the implementation. The virtual machine names and their respective folders are listed in the following table.

Virtual Machines	vCenter Folder
vra01svr01a.rainpole.local	VRA01
vra01svr01b.rainpole.local	VRA01
vra01mssql01.rainpole.local	VRA01
vra01iws01a.rainpole.local	VRA01
vra01iws01b.rainpole.local	VRA01
vra01ims01a.rainpole.local	VRA01
vra01ims01b.rainpole.local	VRA01
vra01dem01.rainpole.local	VRA01
vra01dem02.rainpole.local	VRA01
vra01ias01.sfo01.rainpole.local	VRA01IAS
vra01ias02.sfo01.rainpole.local	VRA01IAS

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 From the **Home** page, click **VMs and Templates**.

3 In the **Navigator**, expand the **mgmt01vc01.sfo01.rainpole.local > SFO01 > VRA01** folder.

4 Right-click the **vra01dem01.rainpole.local** VM and select **Snapshots > Manage Snapshots**.

5 Select the **Prior to vRA IaaS Component Installation** snapshot and click **Delete** icon.

6 Repeat this procedure to remove all of the remaining vRealize Automation virtual machine snapshots.

Content Library Configuration in Region A

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 with other vCenter Server instances if HTTP(S) traffic is allowed between them.

Configure a Content Library in the First Compute vCenter Server Instance in Region A

Create a content library and populate it with templates that you can use to deploy virtual machines in your environment. Content libraries let you synchronize templates among different vCenter Server instances so that all of the templates in your environment are consistent.

There is only one Compute vCenter Server in this VMware Validated Design, but if you deploy more instances for use by the compute cluster they can also use this content library.

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 From the **Home** page, click **Content Libraries** and click the **Create a new content library** icon.

   The **New Content Library** wizard opens.

3 On the **Name** page, specify the following settings and click **Next**.

Setting	Value
Name	SFO01-ContentLib01
vCenter Server	comp01vc01.sfo01.rainpole.local

4 On the **Configure content library** page, specify the following settings, and click **Next**.

Setting	Value
Local content library	Selected
Publish externally	Selected
Enable authentication	Selected
Password	*SFO01-ContentLib01_password*

5 On the **Add storage** page, click the **Select a datastore** radio button, select the **SFO01A-NFS01-VRALIB01** datastore to store the content library, and click **Next**.

6 On the **Ready to complete** page, click **Finish**.

Import the Virtual Machine Template OVF Files in Region A

You can import OVF packages that you previously prepared to use as a template for deploying virtual machines. The virtual machine templates that you add to the content library are used as vRealize Automation blueprints.

You repeat this procedure three times to import the virtual machine templates listed in *VM Templates to Import*Table 3-5.

Table 3-5. VM Templates to Import

VM Template Name	Description
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)

Prerequisites

Verify that you have prepared the OVF templates, as specified in the *Virtual Machine Template Specifications* section.

Procedure

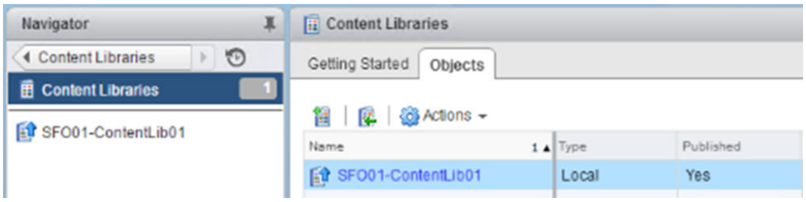
1 Log in to vCenter Server by using the vSphere Web Client.

  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 From the **Home** page, click **Content Libraries** and click the **Objects** tab.



3 Right-click the content library **SFO01-ContentLib01** and select **Import Item**.

4 In the **Import Library Item** dialog box, specify the settings for the first template and click **OK**.

Setting	Value
Source file	\redhat6-enterprise-64.ovf
Item name	redhat6-enterprise-64
Notes	Red Hat Enterprise Server 6 (64-bit)

5 Repeat the procedure to import the remaining virtual machine templates.

Tenant Content Creation in Region A

In order to provision virtual machines in the Compute vCenter, the tenant must be configured to utilize compute resources within vCenter Server.

Prerequisites

- Verify that a vCenter Server compute cluster has been deployed and configured. See Deploy and Configure the Shared Edge and Compute Cluster Components in Region A.
- Verify that an NSX instance has been configured for use by the vCenter Server compute cluster. See Deploy and Configure the Shared Edge and Compute Cluster NSX Instance in Region A.
- Proxy agents have been deployed.

Create Logical Switches for Business Groups in Region A

For each vCenter Server compute instance, 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 3-6. Logical Switch Names and Descriptions

Logical Switch Name	Description
Production-Web-VXLAN	Logical switch for Web tier of Production Business Group
Production-DB-VXLAN	Logical switch for Database tier of Production Business Group
Production-App-VXLAN	Logical switch for Application tier of Production Business Group
Development-Web-VXLAN	Logical switch for Web tier of Development Business Group
Development-DB-VXLAN	Logical switch for Database tier of Development Business Group
Development-App-VXLAN	Logical switch for Application tier of Development Business Group

Procedure

1 Log in to the Compute 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 Create a logical switch.

 a Click **Networking & Security**.

 b In the Navigator, select **Logical Switches**.

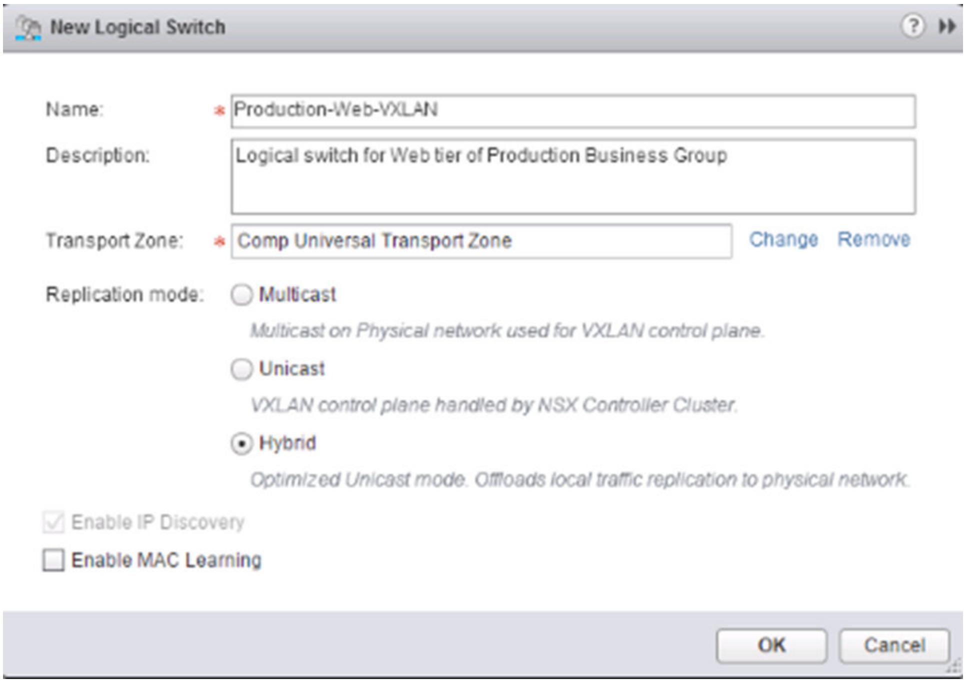
 c From the **NSX Manager** drop-down menu, select **172.16.11.66** as the NSX Manager.

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	Comp Universal Transport Zone
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: * Comp Universal Transport Zone

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

3 Repeat this procedure to create the remaining logical switches.

Configure User Roles in vRealize Automation in Region A

Roles are sets pf privileges that you associate with users to determine what tasks they can perform. Based on their responsibilities, individuals might have one or more roles associated with their user account. All user roles are assigned within the context of a specific tenant. However, some roles in the default tenant can manage system-wide configuration settings that apply to multiple tenants.

This procedure steps you through assigning roles to the ug-ITAC-TenantAdmins and ug-ITAC-TenantArchitects users and groups.

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-LocalRainpoleAdmin
Password	*itac-localrainpoleadmin_password*
Domain	vsphere.local

2 Click the **Administration** tab.

3 Navigate to **Users & Groups > Directory Users and Groups**.

4 Enter `ug-ITAC-TenantAdmins` in the search box and press **Enter**.

   The **ug-ITAC-TenantAdmins (ug-ITAC-TenantAdmins@rainpole.local)** group name displays in the**Name** text box.

5 Click the user group name **ug-ITAC-TenantAdmins (ug-ITAC-TenantAdmins@rainpole.local)**.

6 In the **Add Roles to this Group** list, select the **Application Architect**, **Approval Administrator**, **Container Administrator**, **Container Architect**, **Infrastructure Architect**, **Software Architect**, **Tenant Administrator**, and **XaaS Architect** check boxes, and click **Finish**.

7 Enter `ug-ITAC-TenantArchitects` in the **Tenant Administrators** search box and press **Enter**.

   The **ug-ITAC-TenantArchitects (ug-ITAC-TenantArchitects@rainpole.local)** group name displays in the **Name** text box.

8 Click the user group name **ug-ITAC-TenantArchitects (ug-ITAC-TenantArchitects@rainpole.local)**.

9 In the **Add Roles to this Group** list, select the **Application Architect**, **Container Architect**, **Infrastructure Architect**, **Software Architect**, **XaaS Architect** check box, and click **Finish**.

Create Fabric Groups in Region A

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 resources 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	*itac-tenantadmin_password*
Domain	rainpole.local

2 Select **Infrastructure > Endpoints > Fabric Groups**.

3 Click **New Fabric Group**, enter the following settings and click **OK**.

Setting	Value
Name	SFO Fabric Group
Fabric administrators	ug-ITAC-TenantAdmins@rainpole.local

Note You have not yet configured a vCenter Endpoint, so no compute resource is currently available for you to select. You will configure the vCenter Endpoint later.

4 Log out of the vRealize Automation portal.

Create Machine Prefixes in Region A

As a fabric administrator, you create machine prefixes that are used to create names for machines provisioned through vRealize Automation. Tenant administrators and business group managers select these machine prefixes and assign them to provisioned machines through blueprints and business group defaults.

Machine prefixes are shared across all tenants. Every business group has a default machine prefix. Every blueprint must have a machine prefix or use the group default prefix. Fabric administrators are responsible for managing machine prefixes. A prefix consists of a base name to be followed by a counter of a specified number of digits. When the digits are all used, vRealize Automation rolls back to the first number.

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 **Infrastructure > Administration** > **Machine Prefixes**.

3 Click the **New** icon to create a default machine prefix for the Production group using the following settings, and click the **Save** icon.

Setting	Value
Machine Prefix	Prod-
Number of Digits	5
Next Number	1

4 Click the **New** icon to create a default machine prefix for the Development group using the following settings, and click the **Save** icon.

Setting	Value
Machine Prefix	Dev-
Number of Digits	5
Next Number	1

Create Business Groups in Region A

Tenant administrators create business groups to associate a set of services and resources to a set of users, that often correspond to a line of business, department, or other organizational unit. Users must belong to a business group to request machines.

For this implementation create two business groups, the Production business group and the Development business group.

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 **Administration > Users and Groups > Business Groups**.

3 Click the **New** icon.

4 On the **General** tab, enter the following values and click **Next**.

Setting	Value
Name	Production
Send Manager emails to	ITAC-TenantAdmin@rainpole.local

5 On the **Members** tab, enter **`ug-ITAC-TenantAdmins@rainpole.local`** in the **Group manager role** text box, and click **Next**.

6 On the **Infrastructure** tab, select **Prod-** from the **Default machine prefix** drop-down menu and click **Finish**.

7 Click the **New** icon.

8 On the **General** tab, configure the following values, and click **Next**.

Setting	Value
Name	Development
Send Manager emails to	ITAC-TenantAdmin@rainpole.local

9 On the **Members** tab, enter **`ug-ITAC-TenantAdmins@rainpole.local`** in the **Group manager role** text box and click **Next**.

10 On the **Infrastructure** tab, select **Dev-** from the **Default machine prefix** drop-down menu, and click **Finish**.

Create Reservation Policies

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	*itac-tenantadmin_password*
Domain	rainpole.local

2 Navigate to **Infrastructure > Reservation > Reservation Polices**.

3 Click the **New** icon, configure the following settings, and click the **Save** icon.

Setting	Value
Name	SFO-Production-Policy
Description	Reservation policy for Production Business Group in SFO

4 Click the **New** icon, configure the following settings, and click the **Save** icon.

Setting	Value
Name	SFO-Development-Policy
Description	Reservation policy for Development Business Group in SFO

5 Click the **New** icon, configure the following settings, and click the **Save** icon.

Setting	Value
Name	SFO-Edge-Policy
Description	Reservation policy for Tenant Edge resources in SFO

Create a vSphere Endpoint in vRealize Automation in Region A

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	*itac-tenantadmin_password*
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 comp01vc01.sfo01.rainpole.local with the following settings, and click **Save**.

Setting	Value
Name	comp01vc01sfo01 admin
Description	Administrator of comp01vc01.sfo01.rainpole.local
User Name	svc-vra@rainpole.local
Password	*svc_vra_password*

4 Remain on the **Credentials** page and click **New** again.

5 Configure the NSX administrator credentials of comp01nsxm01.sfo01.rainpole.local with the following settings, and click **Save**.

Setting	Value
Name	comp01nsxm01sfo01 admin
Description	Administrator of NSX Manager comp01nsxm01.sfo01.rainpole.local
User Name	svc-vra@rainpole.local
Password	*svc_vra_password*

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**.

Setting	Value
Name	comp01vc01.sfo01.rainpole.local
Address	https://comp01vc01.sfo01.rainpole.local/sdk
Credentials	comp01vc01sfo01 admin
Specify manager for network and security platform	Selected
Address	https://comp01nsxm01.sfo01.rainpole.local
Credentials	comp01nsxm01sfo01 admin

Note The vSphere Endpoint Name must be identical to the name that you used to install the proxy agent. See "Install IaaS vSphere Proxy Agents."

Add Compute Resources to a Fabric Group in Region A

You allocate compute resources to fabric groups so that vRealize Automation can use the resources in that compute resource for that fabric group when provisioning virtual machines.

Procedure

1 Log in to the vRealize Automation Rainpole portal.

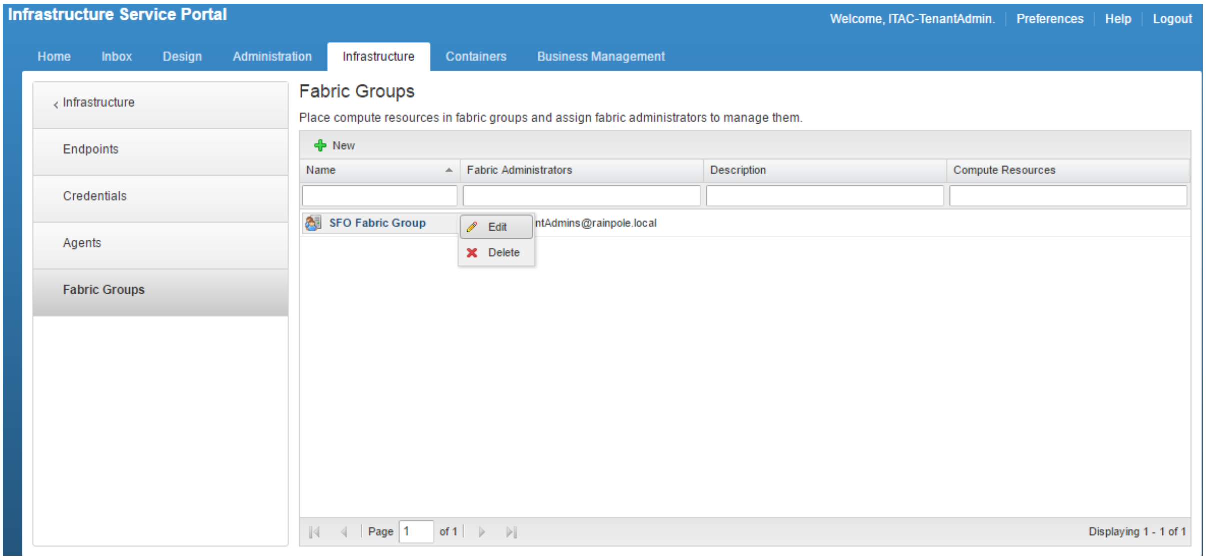
a Open a Web browser and go to `https://vra01svr01.rainpole.local/vcac/org/rainpole`.

b Log in using the following credentials.

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

2 Navigate to **Infrastructure > End Points > Fabric Groups**.

3 In the **Name** column, hover the mouse pointer over the fabric group name **SFO Fabric Group**, and click **Edit**.



Fabric Groups

Place compute resources in fabric groups and assign fabric administrators to manage them.

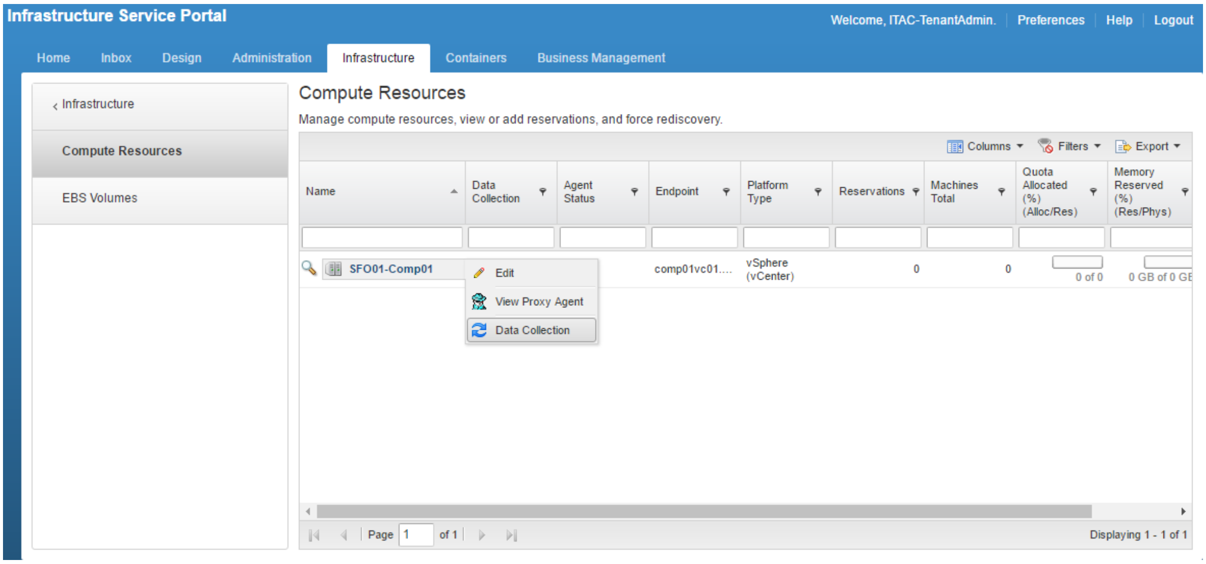
Name	Fabric Administrators	Description	Compute Resources
SFO Fabric Group	ntAdmins@rainpole.local		

4 On the **Edit Fabric Group** page, select **SFO01-Comp01** from the **Compute resources** table, and click **OK**.

Note It might take several minutes for vRealize Automation to connect to the Compute 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 vra01ias01.sfo01.rainpole.local and vra01ias02.sfo01.rainpole.local.

5 Navigate to **Infrastructure > Compute Resources > Compute Resources**.

6 In the **Compute Resource** column, hover the mouse pointer over the compute cluster **SFO01-Comp01**, and click **Data Collection**.



Compute Resources

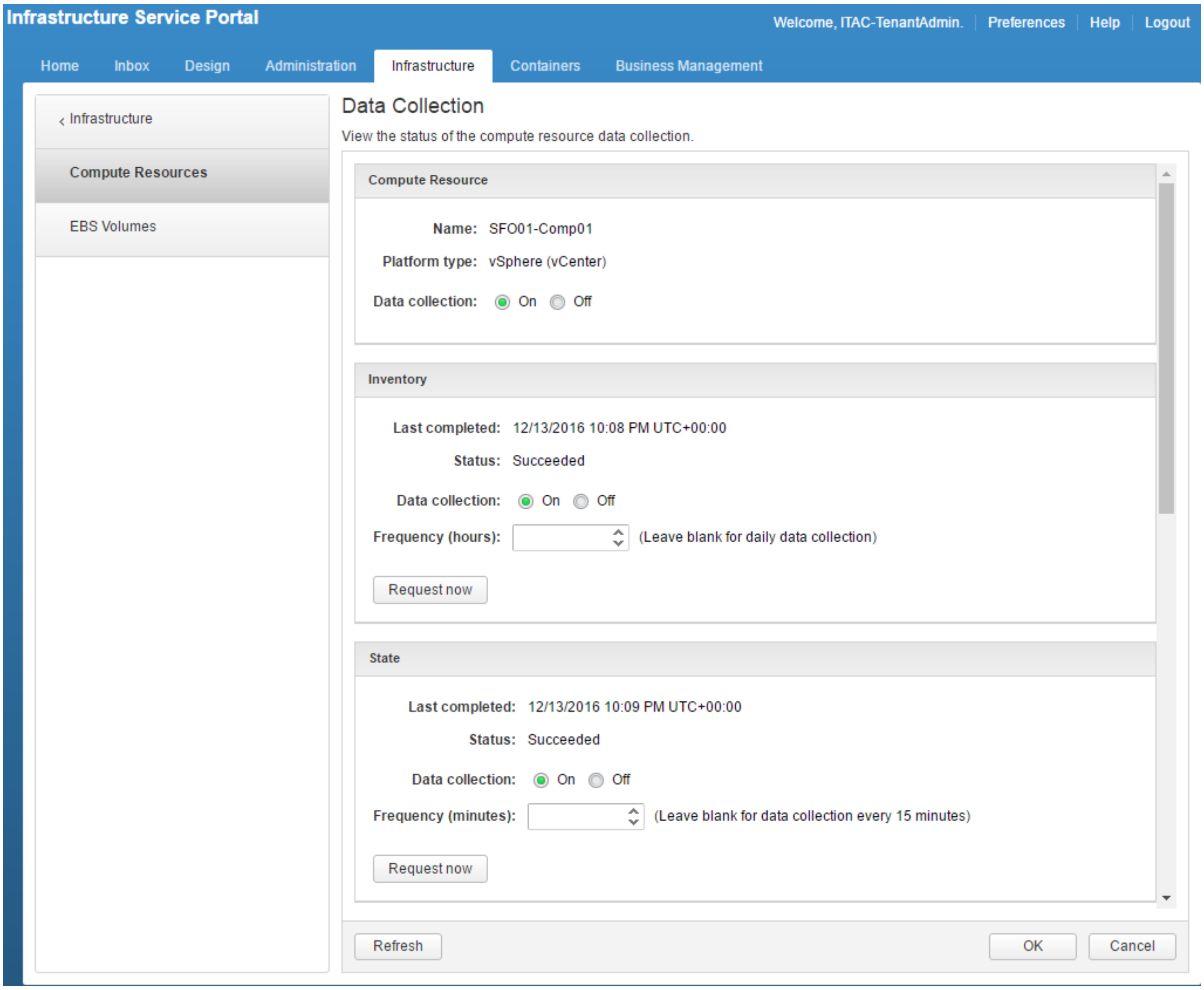
Manage compute resources, view or add reservations, and force rediscovery.

Name	Data Collection	Agent Status	Endpoint	Platform Type	Reservations	Machines Total	Quota Allocated (%) (Alloc/Res)	Memory Reserved (%) (Res/Phys)
SFO01-Comp01			comp01vc01....	vSphere (vCenter)	0	0	0 of 0	0 GB of 0 GE

7 Click on the **Request now** buttons in each field on the page.

Wait a few seconds for the data collection process to complete.

8 Click **Refresh**, and verify that **Status** for both **Inventory** and **Network and Security Inventory** shows **Succeeded**.



Data Collection

View the status of the compute resource data collection.

Compute Resource

Name: SFO01-Comp01

Platform type: vSphere (vCenter)

Data collection: ● On ○ Off

Inventory

Last completed: 12/13/2016 10:08 PM UTC+00:00

Status: Succeeded

Data collection: ● On ○ Off

Frequency (hours): (Leave blank for daily data collection)

State

Last completed: 12/13/2016 10:09 PM UTC+00:00

Status: Succeeded

Data collection: ● On ○ Off

Frequency (minutes): (Leave blank for data collection every 15 minutes)

Create External Network Profiles

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 and specifies the IP address and routing configuration for virtual machines that are provisioned to that network.

Prerequisites

Verify that the Create Logical Switches for Business Groups has been created.

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 > 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 Value
Name	Ext-Net-Profile-Production
Description	External Network profile for Production Business Group
IPAM endpoint	VMware
Subnet mask	255.255.255.0
Gateway	192.168.51.1

4 Click the **DNS** tab and enter the following values.

Setting	Value
Primary DNS	172.16.11.4
Secondary DNS	172.16.11.5
DNS Suffix	rainpole.local
DNS search suffixes	rainpole.local

5 Click the **Network Ranges** tab and follow these steps.

  a Click the **New** button.

  b Enter the following values for the Production Business IP Range profile.

  c Click **OK**.

Setting	Production Value
Name	Production
Description	Static IP range for Production Group
Starting IP address	192.168.51.20
Ending IP address	192.168.51.250

6 Verify that all the static IP addresses are added to the profile and click **OK**.

Create Reservations for the Compute Cluster in Region A

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 reservations for both the Production and Development business groups.

Group	Name
Production	SFO01-Comp01-Prod-Res01
Development	SFO01-Comp01-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	*itac-tenantadmin_password*
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 Group Value	Development Group Value
Name	SFO01-Comp01-Prod-Res01	SFO01-Comp01-Dev-Res01
Tenant	rainpole	rainpole
Business Group	Production	Development
Reservation Policy	SFO-Production-Policy	SFO-Development-Policy
Priority	100	100
Enable This Reservation	Selected	Selected

4 On the **New Reservation - vSphere (vCenter)** page, click the **Resources** tab.

   a Select **SFO01-Comp01(comp01vc01.sfo01.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 **DS-NFS-Primary-HIGH**, and enter `2000` in the **This Reservation Reserved** text box, enter `1` in the **Priority** text box, and click **OK**.

d In the **Storage (GB)** table, select the check box for datastore **DS-NFS-Primary-MED**, and enter `2000` in the **This Reservation Reserved** text box, enter `2` in the **Priority** text box, and click **OK**.

e In the **Storage (GB)** table, select the check box for datastore **DS-NFS-Primary-LOW**, and enter `2000` in the **This Reservation Reserved** text box, enter `3` in the **Priority** text box, and click **OK**.

f Select **User-VMRP01** 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.

a Configure the Production Business Group with the following values.

Production Network Path	Production Group Network Profile
vxw-dvs-xxxxx-Production-VXLAN	Ext-Net-Profile-Production

7 Click **OK** to save the reservation.

Create Reservations for the User Edge Resources in Region A

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.

Group	Name
Production	SFO01-Edge01-Prod-Res01
Development	SFO01-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	*itac-tenantadmin_password*
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	SFO01-Edge01-Prod-Res01	SFO01-Edge01-Dev-Res01
Tenant	rainpole	rainpole
Business Group	Production	Development
Reservation Policy	SFO-Edge-Policy	SFO-Edge-Policy
Priority	100	100
Enable This Reservation	Selected	Selected

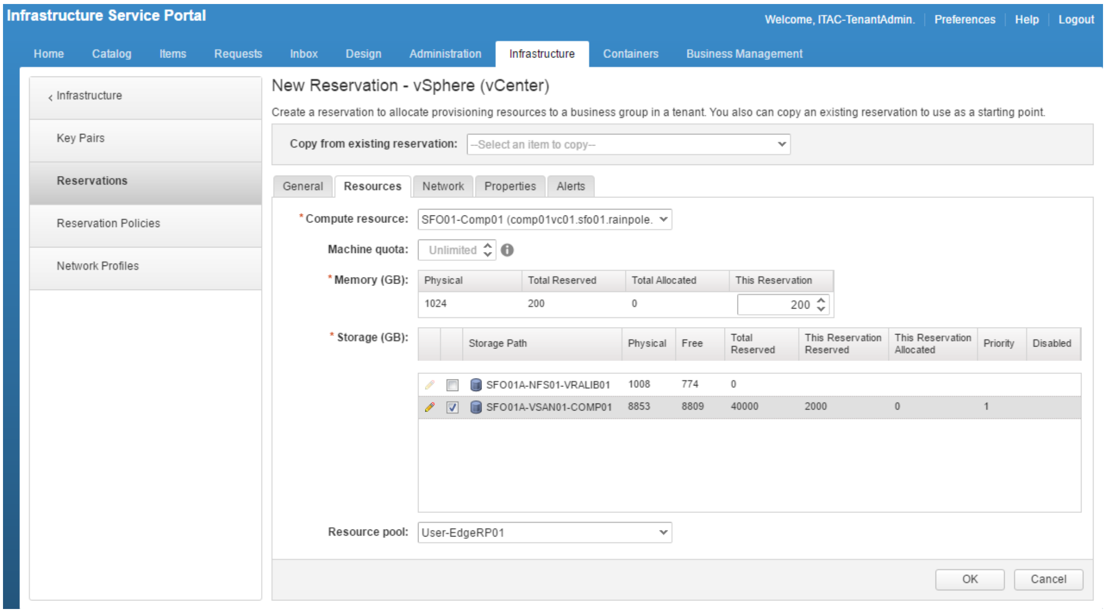
4 On the **New Reservation - vSphere (vCenter)** page, click the **Resources** tab.

a Select **SFO01-Comp01(comp01vc01.sfo01.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 **SFO01A-VSAN01-COMP01**, enter **`2000`** in the **This Reservation Reserved** text box, enter **`1`** in the **Priority** text box, and click **OK**.

d Select **User-EdgeRP01** 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.

Copy from existing reservation: --Select an item to copy--

*Compute resource: SFO01-Comp01 (comp01vc01.sfo01.rainpole.

Machine quota: Unlimited

*Memory (GB):

Physical	Total Reserved	Total Allocated	This Reservation
1024	200	0	200

*Storage (GB):

		Storage Path	Physical	Free	Total Reserved	This Reservation Reserved	This Reservation Allocated	Priority	Disabled
	□	SFO01A-NFS01-VRALIB01	1008	774	0				
	☑	SFO01A-VSAN01-COMP01	8853	8809	40000	2000	0	1	

Resource pool: User-EdgeRP01

5 On the **New Reservation - vSphere (vCenter)** page, click the **Network** tab.

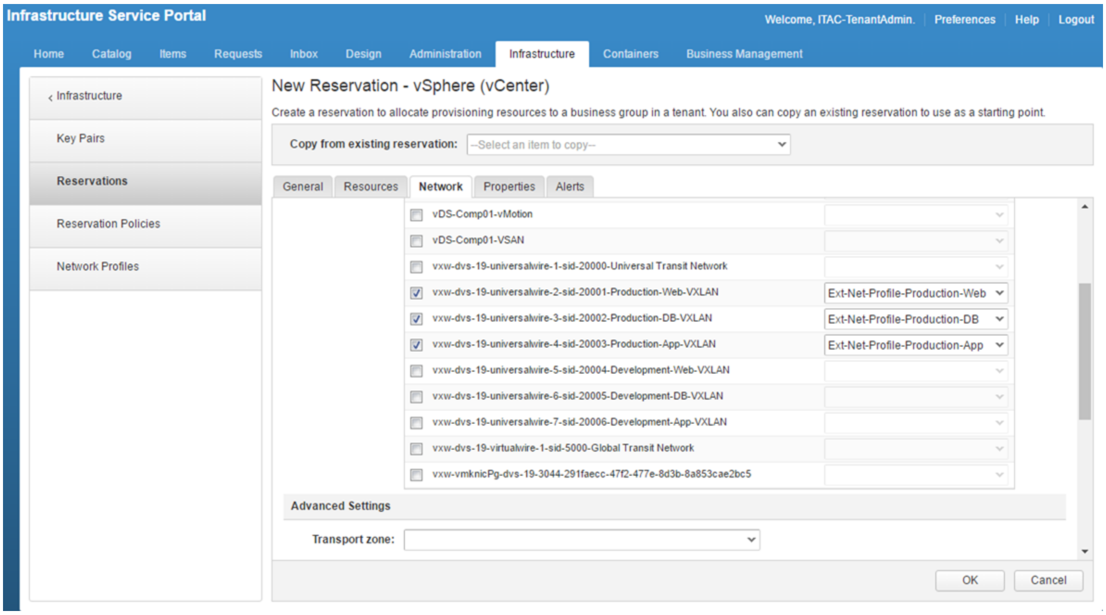
6 On the **Network** tab, select the network path check boxes listed in the table below from the Network Paths list, and select the corresponding network profile from the **Network Profile** drop-down menu for the business group whose reservation you are configuring.

Production Business Group

Production Port Group	Production Network Profile
vxw-dvs-xxxxx-Production-Web-VXLAN	Ext-Net-Profile-Production-Web
vxw-dvs-xxxxx-Production-DB-VXLAN	Ext-Net-Profile-Production-DB
vxw-dvs-xxxxx-Production-App-VXLAN	Ext-Net-Profile-Production-App

Development Business Group

Development Port Group	Development Network Profile
vxw-dvs-xxxxx-Development-Web-VXLAN	Ext-Net-Profile-Development-Web
vxw-dvs-xxxxx-Development-DB-VXLAN	Ext-Net-Profile-Development-DB
vxw-dvs-xxxxx-Development-App-VXLAN	Ext-Net-Profile-Development-App



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--

□ vDS-Comp01-vMotion	
□ vDS-Comp01-VSAN	
□ vxw-dvs-19-universalwire-1-sid-20000-Universal Transit Network	
☑ vxw-dvs-19-universalwire-2-sid-20001-Production-Web-VXLAN	Ext-Net-Profile-Production-Web
☑ vxw-dvs-19-universalwire-3-sid-20002-Production-DB-VXLAN	Ext-Net-Profile-Production-DB
☑ vxw-dvs-19-universalwire-4-sid-20003-Production-App-VXLAN	Ext-Net-Profile-Production-App
□ vxw-dvs-19-universalwire-5-sid-20004-Development-Web-VXLAN	
□ vxw-dvs-19-universalwire-6-sid-20005-Development-DB-VXLAN	
□ vxw-dvs-19-universalwire-7-sid-20006-Development-App-VXLAN	
□ vxw-dvs-19-virtualwire-1-sid-5000-Global Transit Network	
□ vxw-vmknicPg-dvs-19-3044-291faecc-47f2-477e-8d3b-8a853cae2bc5	

Advanced Settings

Transport zone:

7 Click **OK** to save the reservation.

8 Repeat the procedure to create a Edge reservation for the Development Business Group.

Create Customization Specifications in Compute vCenter Server in Region A

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 you create when you create blueprints for use with vRealize Automation.

Create a Customization Specification for Linux in Region A

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://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 Navigate to **Home > Operations and Policies > Customization Specification Manager**.

3 Select the vCenter Server **comp01vc01.sfo01.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 `sfo01.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	Los Angeles
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 Region A

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://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 Navigate to **Home > Operations and Policies > Customization Specification Manager**.

3 Select the vCenter Server **comp01vc01.sfo01.rainpole.local** from the drop-down menu.

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

The **New VM Guest Customization** 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***, 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-08:00) Pacific 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	sfo01.rainpole.local
User name	SFO01\administrator
Password	*admin_pwd*

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 Region A

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 all vCenter Server compute clusters that you add to vRealize Automation, including the first vCenter Server compute instance.

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.

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 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 Navigate to **Home > VMs and Templates**.

3 Expand the **comp01vc01.sfo01.rainpole.local** vCenter Server.

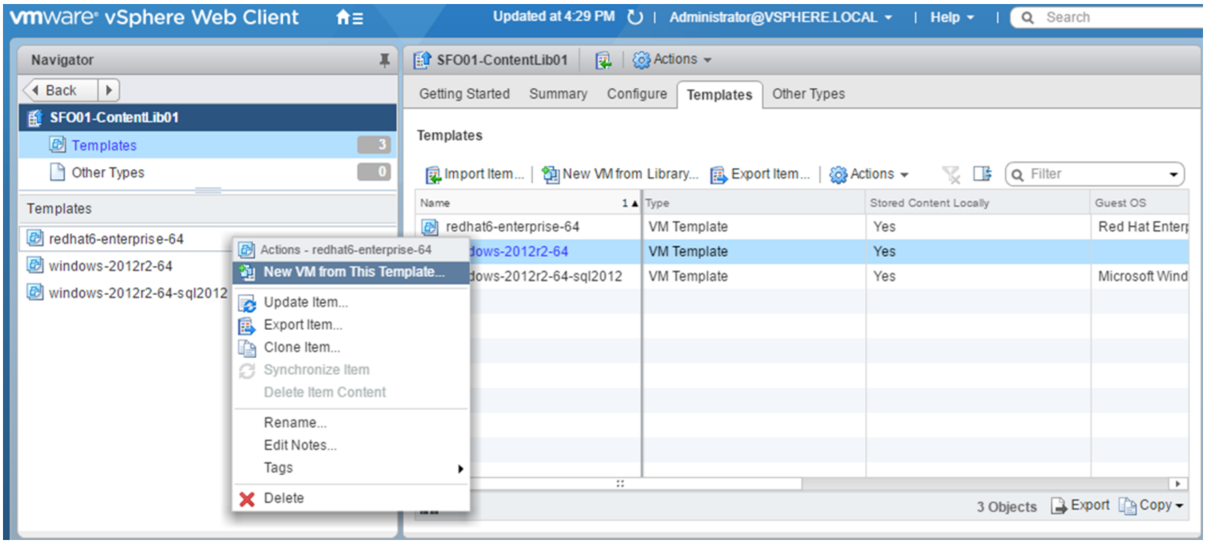
4 Right-click the **SFO01** data center and select **New Folder > New VM and Template Folder**.

5 Create a new folder and label it **`VM Templates`**.

6 Navigate to **Home > Content Libraries**.

7 Click **SFO01-ContentLib01 > Templates**.

8 Right-click the VM Template **redhat6-enterprice-64** and click **New VM from This Template**.



Name	Type	Stored Content Locally	Guest OS
redhat6-enterprise-64	VM Template	Yes	Red Hat Enterp
dows-2012r2-64	VM Template	Yes	
dows-2012r2-64-sql2012	VM Template	Yes	Microsoft Wind

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 **SFO01-Comp01** and select resouce pool **User-VMRP01**.

12 On the **Review details** page, verify the template details and click **Next**.

13 On the **Select storage** page, select the **SFO01A-NFS01-VRALIB01** datastore and select **Thin Provision** from the **Select virtual disk format** drop-down menu.

14 On the **Select networks** page, select **vDS-Comp01-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 that 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 Machine to a VM Template in Region A

You can convert a virtual machine directly to a template instead of making a copy by cloning.

Repeat this procedure for each of the VM Templates in the content library. The table below lists the VM Templates and the guest OS that each template uses to create a virtual machine.

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 Compute 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 Navigate to **Home > VMs and Templates**.

3 In the **Navigator** pane, expand **comp01vc01.sfo01.rainpole.local > SFO01 > 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.

6 Repeat this procedure for all of the VM Templates in the content library, verifying that each VM Template appears in the `VM Templates` folder.

Configure Single Machine Blueprints in Region A

Virtual machine blueprints determine a machine's attributes, the manner in which it is provisioned, and its policy and management settings.

Create a Service Catalog in Region A

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	*itac-tenantadmin_password*
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	SFO 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 Entitlements for Business Groups in Region A

You add a service, catalog item, or action to an entitlement, allowing the users and groups identified in the entitlement to request provisionable items in the service catalog. The entitlement allows members of a particular business group (for example, the Production business group) to use the blueprint. Without the entitlement, users cannot use the blueprint.

Perform this procedure twice to create entitlements for both the Production and Development business groups.

Entitlement Name	Status	Business Group	User & Groups
Prod-SingleVM-Entitlement	Active	Production	ug-ITAC-TenantAdmins
Dev-SingleVM-Entitlement	Active	Development	ug-ITAC-TenantAdmins

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 Click the **Administration** tab, and click **Catalog Management > Entitlements**.

3 Click **New**.

   The **New Entitlement** page appears.

4 On the **New Entitlement** page, select the **Details** tab, configure the following values, and click **Next**.

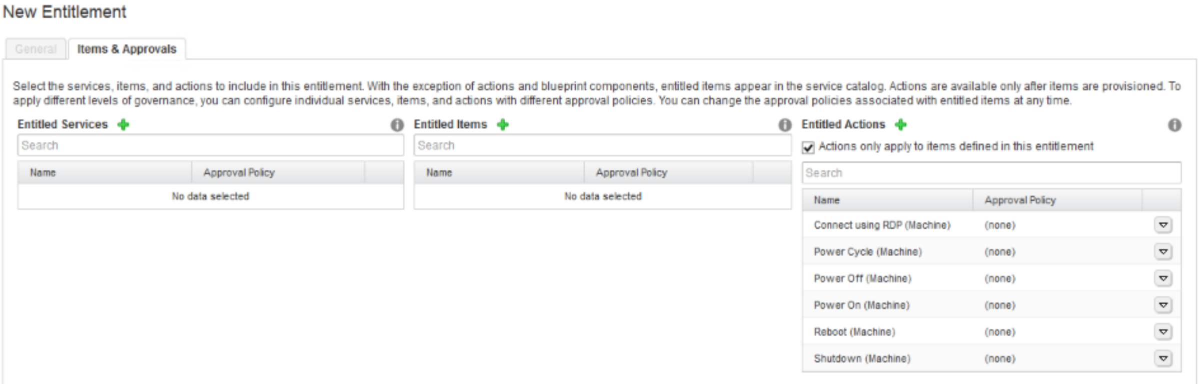
Setting	Production Value	Development Value
Name	Prod-SingleVM-Entitlement	Dev-SingleVM-Entitlement
Description	Default setting (blank)	Default setting (blank)
Expiration Date	Default setting (blank)	Default setting (blank)
Status	Active	Active
Business Group	Production	Development
All Users and Groups	Unselected	Unselected
Users & Groups	ug-ITAC-TenantAdmins	ug-ITAC-TenantAdmins

5 Click the **Items & Approvals** tab.

   a On the **Entitlement Actions** page, click the **Add Action** icon and add the following actions.

      - Connect using RDP (Machine)
      - Power Cycle (Machine)
      - Power Off (Machine)
      - Power On (Machine)
      - Reboot (Machine)
      - Shutdown (Machine)

   b Click **Finish**.



New Entitlement

General | Items & Approvals

Select the services, items, and actions to include in this entitlement. With the exception of actions and blueprint components, entitled items appear in the service catalog. Actions are available only after items are provisioned. To apply different levels of governance, you can configure individual services, items, and actions with different approval policies. You can change the approval policies associated with entitled items at any time.

Entitled Services

Search

Name	Approval Policy
No data selected	

Entitled Items

Search

Name	Approval Policy
No data selected	

Entitled Actions

☑ Actions only apply to items defined in this entitlement

Search

Name	Approval Policy
Connect using RDP (Machine)	(none)
Power Cycle (Machine)	(none)
Power Off (Machine)	(none)
Power On (Machine)	(none)
Reboot (Machine)	(none)
Shutdown (Machine)	(none)

6 Repeat this procedure to create an entitlement for the Development business group.

   Use the same Entitled Actions as for the Production business group.

Create a Single Machine Blueprint in Region A

Create a blueprint for cloning the `windows-2012r2-64` virtual machine using the specified resources on the Compute 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 the following six blueprints.

Blueprint Name	VM Template	Reservation Policy	Service Catalog	Add to Entitlement
Windows Server 2012 R2 - SFO Prod	windows-2012r2-64 (comp01vc01.sfo01.rainpole.local)	SFO-Production-Policy	SFO Service Catalog	Prod-SingleVM-Entitlement
Windows Server 2012 R2 - SFO Dev	windows-2012r2-64 (comp01vc01.sfo01.rainpole.local)	SFO-Development-Policy	SFO Service Catalog	Dev-SingleVM-Entitlement

Blueprint Name	VM Template	Reservation Policy	Service Catalog	Add to Entitlement
Windows Server 2012 R2 With SQL2012 - SFO Prod	windows-2012r2-64-sql2012(comp01vc01.sfo01.rainpole.local)	SFO-Production-Policy	SFO Service Catalog	Prod-SingleVM-Entitlement
Windows Server 2012 R2 With SQL2012 - SFO Dev	windows-2012r2-64-sql2012(comp01vc01.sfo01.rainpole.local)	SFO-Development-Policy	SFO Service Catalog	Dev-SingleVM-Entitlement
Redhat Enterprise Linux 6 - SFO Prod	redhat6-enterprise-64(comp01vc01.sfo01.rainpole.local)	SFO-Production-Policy	SFO Service Catalog	Prod-SingleVM-Entitlement
Redhat Enterprise Linux 6 - SFO Dev	redhat6-enterprise-64(comp01vc01.sfo01.rainpole.local)	SFO-Development-Policy	SFO 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	*itac-tenantadmin_password*
Domain	rainpole.local

2 Navigate to **Design > Blueprints**.

3 Click **New**.

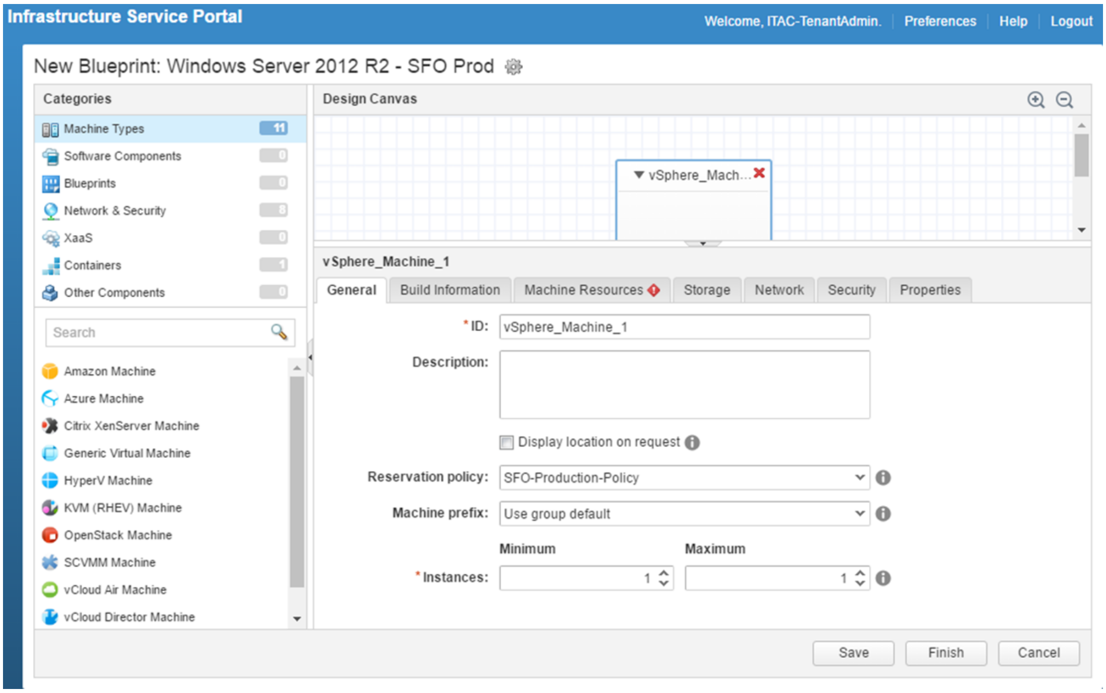
4 In the **New Blueprint** dialog box, configure the following settings on the **General** tab. Click **OK**.

Setting	Value
Name	Windows Server 2012 R2 - SFO Prod
Archive (days)	15
Deployment limit	Default setting (blank)
Minimum	30
Maximum	270

5 Select and drag the **vSphere Machine** icon to **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	SFO-Production-Policy
Machine prefix	Use group default
Minimum	Default setting (blank)
Maximum	Default setting (blank)



New Blueprint: Windows Server 2012 R2 - SFO Prod

vSphere_Machine_1

*ID: vSphere_Machine_1

Description:

□ Display location on request

Reservation policy: SFO-Production-Policy

Machine prefix: Use group default

*Instances: Minimum 1 Maximum 1

7 Click the **Build Information** tab, configure the following settings, and click **Save**.

Setting	Value
Blueprint type	Server
Action	Clone
Provisioning workflow	CloneWorkflow
Clone from	windows-2012r2-64 template
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.

a Select **Network & Security** in the **Categories** section to display the list of available network and security components.

b Select the **Existing Network** component and drag it onto the design canvas.

c Click in the **Existing network** text box and select the **Ext-Net-Profile-Production-Web** network profile.

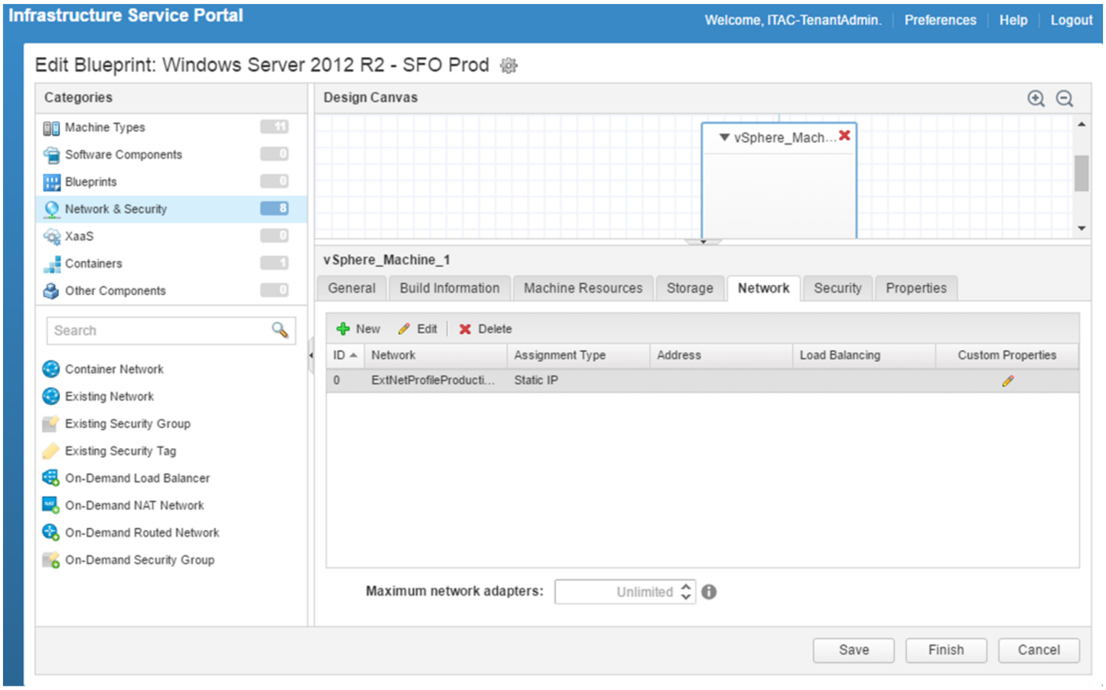
Blueprint Name	Existing network
Windows Server 2012 R2 - SFO Prod	Ext-Net-Profile-Production-Web
Windows Server 2012 R2 - SFO Dev	Ext-Net-Profile-Development-Web
Windows Server 2012 R2 With SQL2012 - SFO Prod	Ext-Net-Profile-Production-DB
Windows Server 2012 R2 With SQL2012 - SFO Dev	Ext-Net-Profile-Development-DB
Redhat Enterprise Linux 6 - SFO Prod	Ext-Net-Profile-Production-App
Redhat Enterprise Linux 6 - SFO Dev	Ext-Net-Profile-Development-App

d Click **Save**.

e Select **vSphere_Machine** properties from the design canvas.

f Select the **Network** tab, click **New**, and configure the following settings. Click **OK**.

Network	Assignment Type	Address
ExtNetProfileProductionWeb	Static IP	Default setting (blank)
ExtNetProfileDevelopmentWeb	Static IP	Default setting (blank)
ExtNetProfileProductionDB	Static IP	Default setting (blank)
ExtNetProfileDevelopmentDB	Static IP	Default setting (blank)
ExtNetProfileProductionApp	Static IP	Default setting (blank)
ExtNetProfileDevelopmentApp	Static IP	Default setting (blank)



ID	Network	Assignment Type	Address	Load Balancing	Custom Properties
0	ExtNetProfileProducti...	Static IP			

Maximum network adapters: Unlimited

g Click **Finish** to save the blueprint.

10 Select the blueprint **Windows Server 2012 R2 - SFO Prod** and click **Publish**.

11 Repeat this procedure to create additional blueprints.

Configure Entitlements for Blueprints in Region A

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 blueprints with their entitlement.

Blueprint Name	VM Template	Reservation Policy	Service Catalog	Add to Entitlement
Windows Server 2012 R2 - SFO Prod	windows-2012r2-64 (comp01vc01.sfo01.rainpole.local)	SFO-Production-Policy	SFO Service Catalog	Prod-SingleVM-Entitlement
Redhat Enterprise Linux 6 - SFO Prod	redhat6-enterprise-64(comp01vc01.sfo01.rainpole.local)	SFO-Production-Policy	SFO Service Catalog	Prod-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`**.

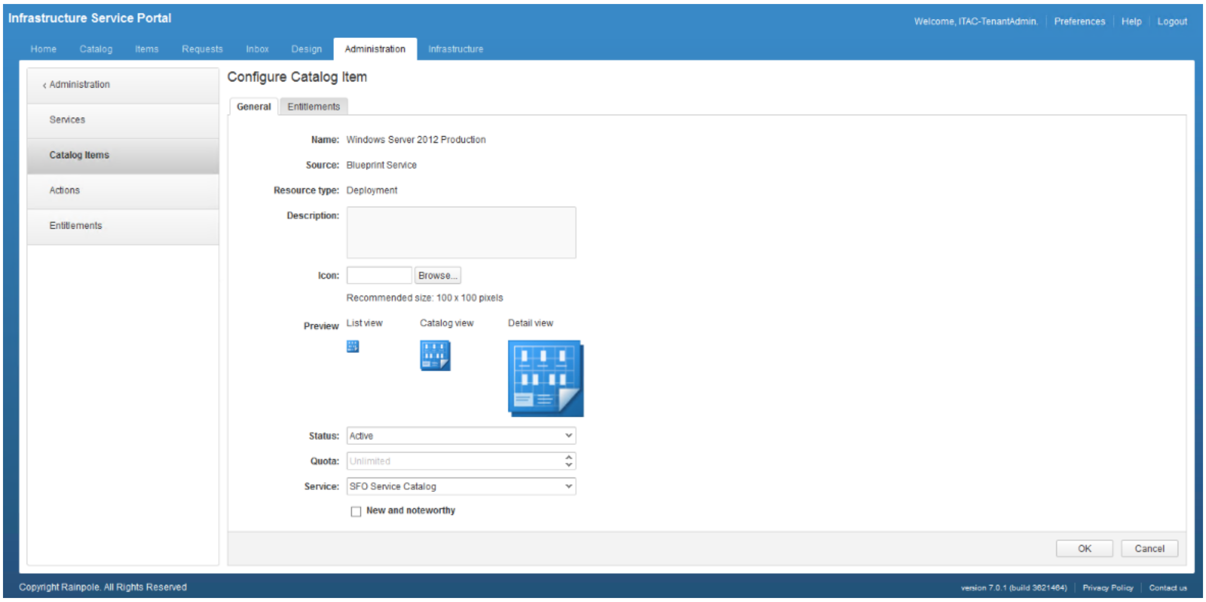
   b Log in using the following credentials.

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

2 Select the **Administration** tab and navigate to **Catalog Management > Catalog Items**.

3 On the **Catalog Items** pane, select the **Windows Server 2012 R2 - SFO Prod** blueprint in the **Catalog Items** list and click **Configure**.

4 On the **General** tab of the **Configure Catalog Item** dialog box, select **SFO Service Catalog** from the **Service** drop-down menu, and click **OK**.



Configure Catalog Item

Name: Windows Server 2012 Production

Source: Blueprint Service

Resource type: Deployment

Description:

Icon:

Recommended size: 100 x 100 pixels

Status: Active

Quota: Unlimited

Service: SFO Service Catalog

□ New and noteworthy

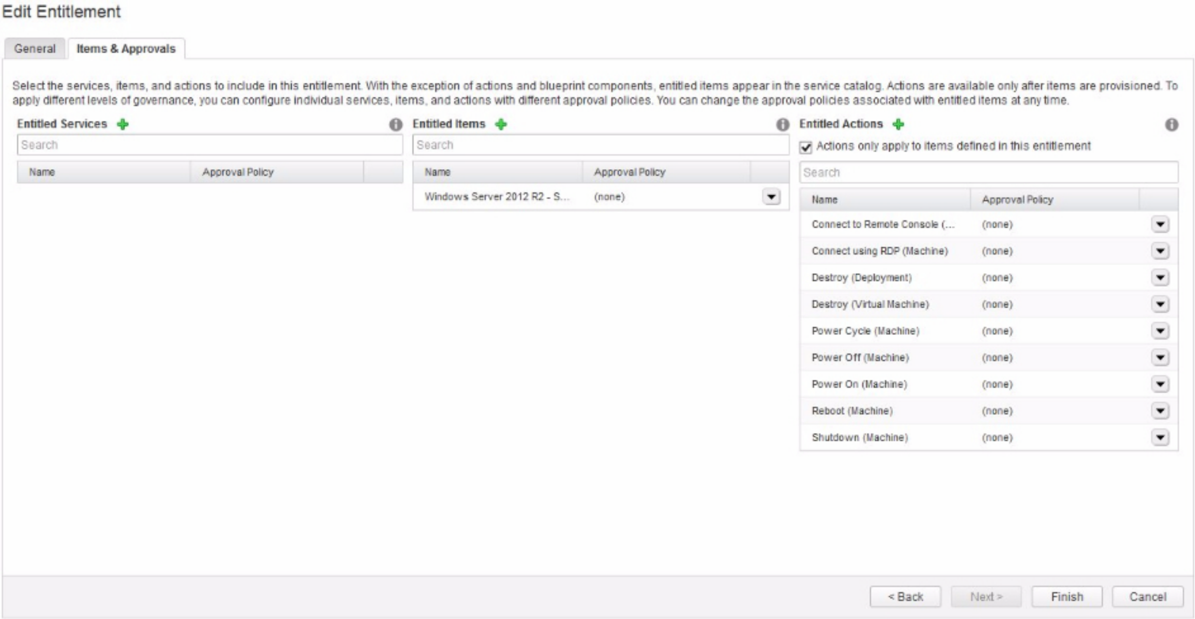
5 Associate the blueprint with the **Prod-SingleVM-Entitlement** entitlement.

   a Click **Entitlements** and select **Prod-SingleVM-Entitlement**.

     The **Edit Entitlement** pane appears.

   b Select the **Items & Approvals** tab and add the **Windows Server 2012 R2 - SFO Prod** blueprint to the **Entitled Items** list.

   c Click **Finish**.



Edit Entitlement

Select the services, items, and actions to include in this entitlement. With the exception of actions and blueprint components, entitled items appear in the service catalog. Actions are available only after items are provisioned. To apply different levels of governance, you can configure individual services, items, and actions with different approval policies. You can change the approval policies associated with entitled items at any time.

Entitled Services

Name	Approval Policy

Entitled Items

Name	Approval Policy
Windows Server 2012 R2 - S...	(none)

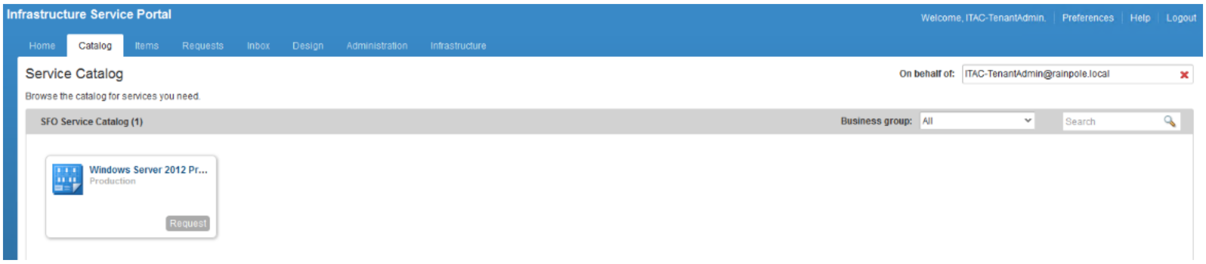
Entitled Actions

☑ Actions only apply to items defined in this entitlement

Name	Approval Policy
Connect to Remote Console (...	(none)
Connect using RDP (Machine)	(none)
Destroy (Deployment)	(none)
Destroy (Virtual Machine)	(none)
Power Cycle (Machine)	(none)
Power Off (Machine)	(none)
Power On (Machine)	(none)
Reboot (Machine)	(none)
Shutdown (Machine)	(none)

6 Repeat the steps above for blueprint "Redhat Enterprise Linux 6 - SFO Prod "

7 Select the **Catalog** tab and verify that the blueprints are listed in the Service Catalog.



Service Catalog

Browse the catalog for services you need.

On behalf of: ITAC-TenantAdmin@rainpole.local

SFO Service Catalog (1)

Business group: All

Region A Operations Implementation

4

Deploy vRealize Operations Manager and vRealize Log Insight in Region A to add monitoring capabilities to your SDDC.

- Region A vRealize Operations Manager Implementation

  Deploy the vRealize Operations Manager analytics cluster to monitor the resources in your SDDC. Deploy also remote collectors to collect data from the vCenter Server instances in Region A.

- Region A vRealize Log Insight Implementation

  Deploy vRealize Log Insight in a cluster configuration of three nodes with an integrated load balancer: one master and two worker nodes.

- Region A vSphere Update Manager Download Service Implementation

  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 Region A.

Region A vRealize Operations Manager Implementation

Deploy the vRealize Operations Manager analytics cluster to monitor the resources in your SDDC. Deploy also remote collectors to collect data from the vCenter Server instances in Region A.

Procedure

1. Deploy vRealize Operations Manager in Region A

   Start the deployment of vRealize Operations Manager in Region A by deploying the nodes of the analytics cluster and the remote collector nodes.

2. Configure the Load Balancer for vRealize Operations Manager in Region A

   Configure load balancing for the analytics cluster on the dedicated SFOMGMT-LB01 NSX Edge service gateway for Region A. Remote collector cluster for Region A does not require load balancing.

3. Add an Authentication Source for the Active Directory

   Connect vRealize Operations Manager to the Active Directory of the SDDC for central user management and access control.

4 Configure User Access in vSphere for Integration with vRealize Operations Manager in Region A

Configure operations services accounts with permissions that are required to enable vRealize Operations Manager access to monitoring data on the Management vCenter Server and Compute vCenter Server in Region A.

5 Add vCenter Adapter Instances to vRealize Operations Manager for Region A

After you deploy the analytics cluster and the remote collector nodes of vRealize Operations Manager in Region A and start vRealize Operations Manager, add vCenter Adapter instances for the Management and Compute vCenter Server instances in Region A.

6 Connect vRealize Operations Manager to the NSX Managers in Region A

Install and configure the vRealize Operations Management Pack for NSX for vSphere to monitor the NSX networking services deployed in each vSphere cluster 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.

7 Connect vRealize Operations Manager to vRealize Automation in Region A

Install and configure the vRealize Operations Manager Management Pack for vRealize Automation to monitor the health and capacity risk of your cloud infrastructure in the context of the tenant's business groups.

8 Enable Storage Device Monitoring in vRealize Operations Manager in Region A

Install and configure the vRealize Operations Management Pack for Storage Devices to view the storage topology, and to monitor the capacity and problems on storage components.

9 Configure E-Mail Alerts in vRealize Operations Manager

You configure e-mail notifications in vRealize Operations Manager so that users and applications receive the administrative alerts from vRealize Operations Manager about certain situations in the data center.

Deploy vRealize Operations Manager in Region A

Start the deployment of vRealize Operations Manager in Region A by deploying the nodes of the analytics cluster and the remote collector nodes.

Procedure

1 Prerequisites for Deploying vRealize Operations Manager in Region A

Before you deploy vRealize Operations Manager, verify that your environment satisfies the requirements for this deployment.

2 Deploy the Virtual Appliance for Each Node of the Analytics Cluster in Region A

Use the vSphere Web Client to deploy each vRealize Operations Manager node as a virtual appliance on the management cluster in Region A.

3 Configure the Master Node in the Analytics Cluster

   After you deploy the virtual appliance for the master node of the vRealize Operations Manager analytics cluster, enable its administration role in the cluster.

4 Configure the Master Replica Node in the Analytics Cluster

   After you deploy a virtual appliance instance for the master replica node and configure a master node in the cluster, enable the cluster node functionality of the master replica node and join it to the analytics cluster.

5 Configure the Data Node in the Analytics Cluster

   After you deploy the virtual appliance for a data node of the vRealize Operations Manager analytics cluster, enable its role in the cluster.

6 Deploy the Remote Collector Virtual Appliances

   After you deploy and enable the roles of the analytics cluster nodes, use the vSphere Web Client to deploy each of the two virtual appliances for the remote collectors in Region A. In a multi-region environment, you deploy remote collectors to forward data from the vCenter Server instances in Region A to the analytics cluster also to support failover of the analytics cluster.

7 Connect the Remote Collector Nodes to the Analytics Cluster

   After you deploy the virtual appliances for the remote collector nodes on the Management vCenter Server, configure the settings of the remote collectors and connect them to the analytics cluster.

8 Configure a DRS Anti-Affinity Rule for vRealize Operations Manager in Region A

   To protect the vRealize Operations Manager virtual machines from a host-level failure, configure vSphere DRS to run both the virtual machines of the analytics cluster and of the remote collectors on different hosts in the management cluster.

9 Enable High Availability and Start vRealize Operations Manager

   After you deploy the virtual appliances for the analytics cluster nodes and remote collector nodes, enable high availability in the analytics cluster by assigning the replica role to the vrops-repln-02 node, and start the analytics cluster.

10 Assign a License to vRealize Operations Manager

   After you deploy and start vRealize Operations Manager in Region A, you assign a valid license.

11 Group Remote Collector Nodes in Region A

   After you start vRealize Operations Manager and assign it a license, 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 vRealize Operations Manager in Region A

Before you deploy vRealize Operations Manager, verify that your environment satisfies the requirements for this deployment.

IP Addresses and Host Names

Verify that static IP address and FQDNs for the vRealize Operations Manager application virtual network are available for the first region of the SDDC deployment.

For the analytics cluster application virtual network, allocate 3 static IP addresses and FQDNs for the nodes and one for the load balancer, and map host names to the IP addresses. For the remote collector cluster, allocate 2 static IP addresses and FQDNs.

Table 4‑1. IP Addresses and Host Names for the Analytics Cluster in Region A

Role	IP Address	FQDN
External load balancer VIP address	192.168.11.35	vrops-cluster-01.rainpole.local
Master node	192.168.11.31	vrops-mstrn-01.rainpole.local
Master replica node	192.168.11.32	vrops-repln-02.rainpole.local
Data node 1	192.168.11.33	vrops-datan-03.rainpole.local
Default gateway	192.168.11.1	-
DNS server	■ 172.16.11.4 ■ 172.17.11.4	-
Subnet mask	255.255.255.0	-
NTP servers	■ 172.16.11.251 ■ 172.16.11.252 ■ 172.17.11.251 ■ 172.17.11.252	■ ntp.sfo01.rainpole.local ■ ntp.lax01.rainpole.local

Table 4‑2. IP Addresses and Host Names for the Remote Collectors in Region A

Role	IP Address	FQDN
Remote collector node 1	192.168.31.31	vrops-rmtcol-01.sfo01.rainpole.local
Remote collector node 2	192.168.31.32	vrops-rmtcol-02.sfo01.rainpole.local
Default gateway	192.168.31.1	-
DNS server	172.16.11.5	-
Subnet mask	255.255.255.0	-

Deployment Prerequisites

Verify that your environment satisfies the following prerequisites to deployment vRealize Operations Manager.

Prerequisite	Value
Storage	■ Virtual disk provisioning. ■ Thin ■ Required storage per node ■ Initial storage for node deployment: 1.6 GB ■ Storage for monitoring data for analytics cluster nodes: 1 TB
Software Features	■ vSphere ■ Management vCenter Server ■ Client Integration Plugin on the machine where you use the vSphere Web Client ■ Management cluster with enabled DRS and HA. ■ NSX for vSphere ■ Application virtual network for the 3-node analytics cluster. ■ Application virtual network for the 2 remote collector nodes.
Installation Package	Download the `.ova` file of the vRealize Operations Manager virtual appliance on the machine where you use the vSphere Web Client.
License	Verify that you have obtained a license that covers the use of vRealize Operations Manager.
Active Directory	Verify that you have a parent active directory with the SDDC user roles configured for the rainpole.local domain.
Certification Authority	Configure the root Active Directory domain controller as a certificate authority for the environment.

Deploy the Virtual Appliance for Each Node of the Analytics Cluster in Region A

Use the vSphere Web Client to deploy each vRealize Operations Manager node as a virtual appliance on the management cluster in Region A.

You repeat the deployment for each of the three analytics nodes: master, master replica, and data.

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.

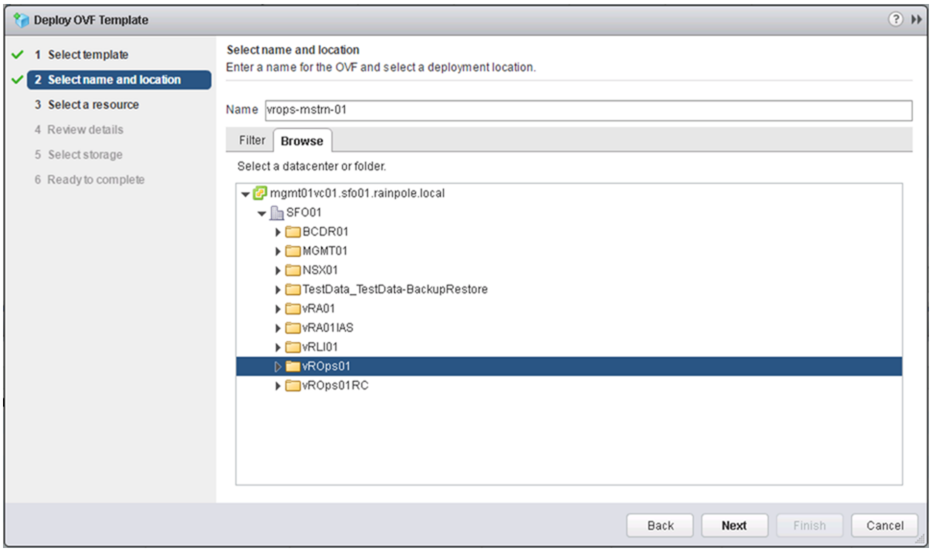
Setting	Value
User name	administrator@vsphere.local
Password	*vsphere_admin_password*

2 Navigate to the mgmt01vc01.sfo01.rainpole.local vCenter Server object.

3 Right-click the **mgmt01vc01.sfo01.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**.



Select name and location

Enter a name for the OVF and select a deployment location.

Name vrops-mstrn-01

Select a datacenter or folder.

- mgmt01vc01.sfo01.rainpole.local
  - SFO01
    - BCDR01
    - MGMT01
    - NSX01
    - TestData_TestData-BackupRestore
    - vRA01
    - vRA01IAS
    - vRLI01
    - vROps01
    - vROps01RC

a Enter a name for the node according to its role.

Name	Role
vrops-mstrn-01	Master node
vrops-repln-02	Master replica node
vrops-datan-03	Data node 1

b Select the inventory folder for the virtual appliance.

Setting	Value
vCenter Server	mgmt01vc01.sfo01.rainpole.local
Datacenter	SFO01
Folder	vROps01

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

Setting	Value
Datacenter	SFO01
Cluster	SFO01-Mgmt01

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 the **Medium** deployment configuration of the virtual appliance, and click **Next**.

10. On the **Select storage** page, select the following datastore and configure its settings, and click **Next**.

Setting	Value
Select virtual disk format	Thin provision
VM Storage Policy	Virtual SAN Default Storage Policy
Datastore	SFO01A-VSAN01-MGMT01

11. On the **Select networks** page, select the distributed port group on the vDS-Mgmt distributed switch that ends with `Mgmt-xRegion01-VXLAN`, and click **Next**.

12. On the **Customize template** page, set 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	172.16.11.4, 172.17.11.4
Default gateway	192.168.11.1
Static IPv4 address	■ 192.168.11.31 for vrops-mstrn-01 ■ 192.168.11.32 for vrops-repln-02 ■ 192.168.11.33 for vrops-datan-03
Subnet mask	255.255.255.0

    b. From the **Timezone setting** drop-down menu, select the **Etc/UTC** time zone.

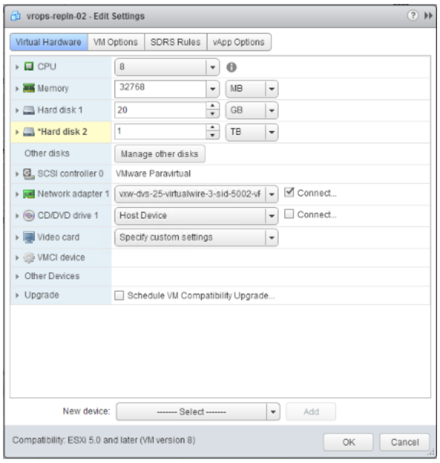
13. On the **Ready to complete** page,verify that the settings for deployment are correct, and click **Finish**.

14. After the virtual appliance is deployed, expand the data disk of the virtual appliance to collect and store data from a large number of virtual machines.

    a. In the vSphere Web Client, navigate to the virtual appliance object.

    b. Right-click the virtual appliance and select **Edit Settings**.

    c. In the **Edit Settings** dialog box, locate **Hard disk 2**, increase the size of the virtual appliance disk from 250 GB to 1 TB, and click **OK**.



vrops-repln-02 - Edit Settings

CPU	8		
Memory	32768	MB	
Hard disk 1	20	GB	
*Hard disk 2	1	TB	
Other disks	Manage other disks		
SCSI controller 0	VMware Paravirtual		
Network adapter 1	vxw-dvs-25-virtualwire-3-sid-5002-vl	☑ Connect...	
CD/DVD drive 1	Host Device	□ Connect...	
Video card	Specify custom settings		
VMCI device			
Other Devices			
Upgrade	□ Schedule VM Compatibility Upgrade...		

New device: ------- Select -------

Compatibility: ESXi 5.0 and later (VM version 8)

15 After the virtual appliance is deployed, right-click the virtual appliance object and select **Power > Power On**.

During the power-on process, the virtual appliance expands the vRealize Operations Manager data partition as well.

16 Change the default empty password for the root user.

a In the vSphere Web Client, right-click the analytics virtual appliance and select **Open Console** to open the remote console to the appliance.

Name	Role
vrops-mstrn-01	Master node
vrops-repln-02	Master replica node
vrops-datan-03	Data node 1

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.

17 Repeat this procedure to deploy the vRealize Operations Manager virtual appliance for the next node in the analytics cluster.

Configure the Master Node in the Analytics Cluster

After you deploy the virtual appliance for the master node of the vRealize Operations Manager analytics cluster, enable its administration role in the cluster.

Prerequisites

Generate the PEM file for vRealize Operations Manager by using the `CertGenVVD` tool and download it to your computer. See the *VMware Validated Design Planning and Preparation* documentation or VMware Knowledge Base article 2146215.

Procedure

1 Open a Web browser and go to **`https://vrops-mstrn-01.rainpole.local`**.

2 On the initial setup page, click **New Installation**.

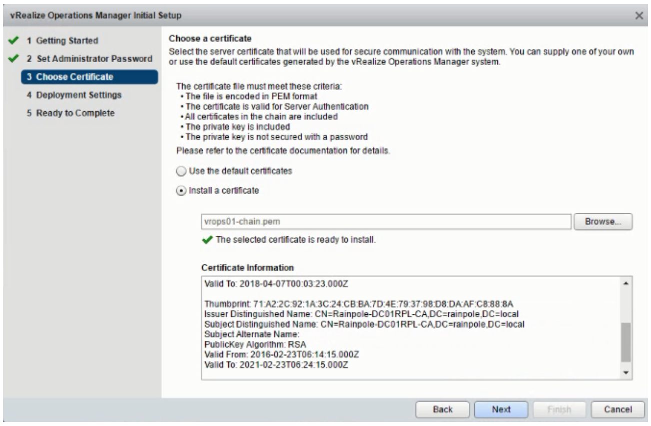
3 On the **Getting Started** page, review the steps for creating a cluster, and click **Next**.

4 On the **Set Administrator Password** page, type and confirm the password for admin user account.

5 On the **Choose Certificate** page, select the **Install a certificate** button, click **Browse**, select the certificate chain `.pem` file that contains the own private key and the issuer and own certificate files, and click **Next**.

You generate a PEM file `vrops.2.chain.pem` by using the `CertGenVVD` tool.

After the setup imports and validates the certificate, notice that the certificate has a common name, `vrops-cluster-01.rainpole.local`, and a subject alternative name that contains `vrops-mstrn-01.rainpole.local` for the master node.



Choose a certificate

Select the server certificate that will be used for secure communication with the system. You can supply one of your own or use the default certificates generated by the vRealize Operations Manager system.

The certificate file must meet these criteria:
- The file is encoded in PEM format
- The certificate is valid for Server Authentication
- All certificates in the chain are included
- The private key is included
- The private key is not secured with a password

Please refer to the certificate documentation for details.

○ Use the default certificates

● Install a certificate

vrops01-chain.pem

✓ The selected certificate is ready to install.

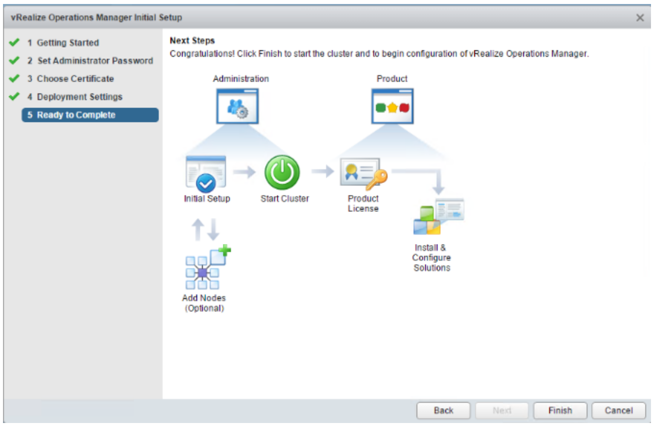
Certificate Information

```
Valid To: 2018-04-07T00:03:23.000Z

Thumbprint: 71:A2:2C:92:1A:3C:24:CB:BA:7D:4E:79:37:98:D8:DA:AF:C8:88:8A
Issuer Distinguished Name: CN=Rainpole-DC01RPL-CA,DC=rainpole,DC=local
Subject Distinguished Name: CN=Rainpole-DC01RPL-CA,DC=rainpole,DC=local
Subject Alternate Name:
PublicKey Algorithm: RSA
Valid From: 2016-02-23T06:14:15.000Z
Valid To: 2021-02-23T06:24:15.000Z
```

6 On the **Deployment Settings** page, configure the following settings, and click **Next**.

Setting	Value
Cluster Master Node Name	vrops-mstrn-01
NTP Server Address	■ ntp.sfo01.rainpole.local ■ ntp.lax01.rainpole.local

7 On the **Ready to Complete** page, click **Finish**.



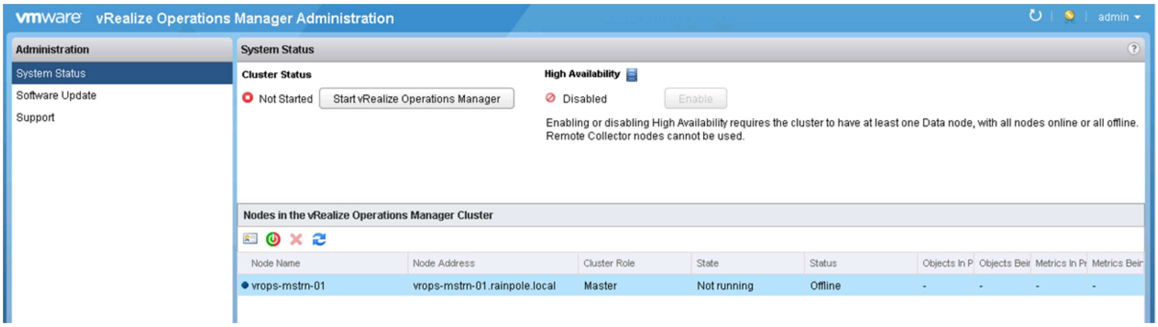
Next Steps

Congratulations! Click Finish to start the cluster and to begin configuration of vRealize Operations Manager.

When the configuration process completes, the vRealize Operations Manager Administration console opens.

8. Click **System Status** in the **Administration** panel to verify that you have a vRealize Operations Manager instance created.

   The virtual appliance instance acting as the master node appears in the **Nodes in the vRealize Operations Manager Cluster** list.



Cluster Status: Not Started

High Availability: Disabled

Enabling or disabling High Availability requires the cluster to have at least one Data node, with all nodes online or all offline. Remote Collector nodes cannot be used.

Nodes in the vRealize Operations Manager Cluster

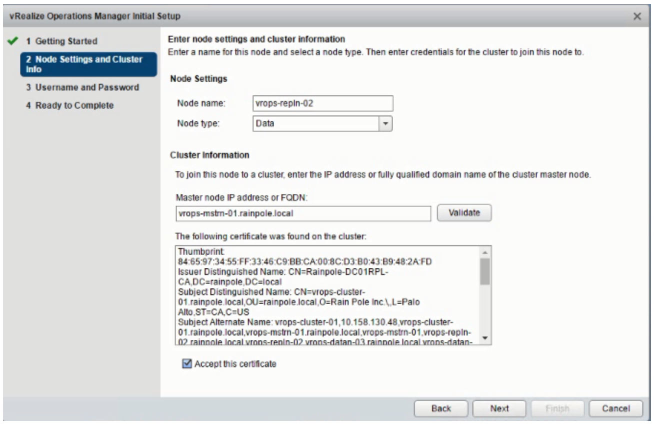
Node Name	Node Address	Cluster Role	State	Status	Objects In P	Objects Beir	Metrics In Pr	Metrics Beir
● vrops-mstrn-01	vrops-mstrn-01.rainpole.local	Master	Not running	Offline	-	-	-	-

Configure the Master Replica Node in the Analytics Cluster

After you deploy a virtual appliance instance for the master replica node and configure a master node in the cluster, enable the cluster node functionality of the master replica node and join it to the analytics cluster.

Procedure

1. Open a Web browser and go to **`https://vrops-repln-02.rainpole.local`**.
2. In 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.



Enter node settings and cluster information

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: vrops-repln-02

Node type: Data

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: vrops-mstrn-01.rainpole.local

The following certificate was found on the cluster:

```
Thumbprint:
84:65:97:34:55:FF:33:46:C9:BB:CA:00:8C:D3:B0:43:B9:48:2A:FD
Issuer Distinguished Name: CN=Rainpole-DC01RPL-
CA,DC=rainpole,DC=local
Subject Distinguished Name: CN=vrops-cluster-
01.rainpole.local,OU=rainpole.local,O=Rain Pole Inc.\,L=Palo
Alto,ST=CA,C=US
Subject Alternate Name: vrops-cluster-01,10.158.130.48,vrops-cluster-
01.rainpole.local,vrops-mstrn-01.rainpole.local,vrops-mstrn-01,vrops-repln-
02.rainpole.local,vrops-repln-02,vrops-datan-03.rainpole.local,vrops-datan-
```

☑ Accept this certificate

a Configure the name, type and master address of the node.

Setting	Value
Node name	vrops-repln-02
Node type	Data
Master node IP address or FQDN	vrops-mstrn-01.rainpole.local

b Next to the **Master node IP address or FQDN** text box, click **Validate**.

The certificate of the master node displays in the text box.

c Verify that the master certificate is correct, and click **Accept this certificate**.

d Click **Next**.

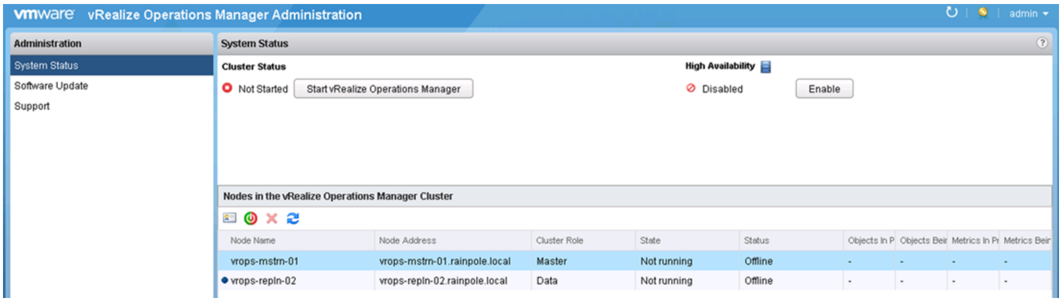
5 On the **Username and Password** page, select **Use cluster administrator user name and password**, enter the ***vrops_admin_password*** password for the admin user, and click **Next**.

6 On the **Ready to Complete** page, click **Finish**.

When the configuration process completes, the vRealize Operations Manager Administration console opens.

7 Click **System Status** in the Administration panel to verify that the node is added to the analytics cluster.

The virtual appliance instance acting as the data node appears in the **Nodes in the vRealize Operations Manager Cluster** list.


vmware vRealize Operations Manager Administration
admin
Administration
System Status
Software Update
Support
System Status
Cluster Status
Not Started
Start vRealize Operations Manager
High Availability
Disabled
Enable
Nodes in the vRealize Operations Manager Cluster

Node Name	Node Address	Cluster Role	State	Status	Objects In P	Objects Beir	Metrics In Pr	Metrics Beir
vrops-mstrn-01	vrops-mstrn-01.rainpole.local	Master	Not running	Offline	-	-	-	-
● vrops-repln-02	vrops-repln-02.rainpole.local	Data	Not running	Offline	-	-	-	-

Configure the Data Node in the Analytics Cluster

After you deploy the virtual appliance for a data node of the vRealize Operations Manager analytics cluster, enable its role in the cluster.

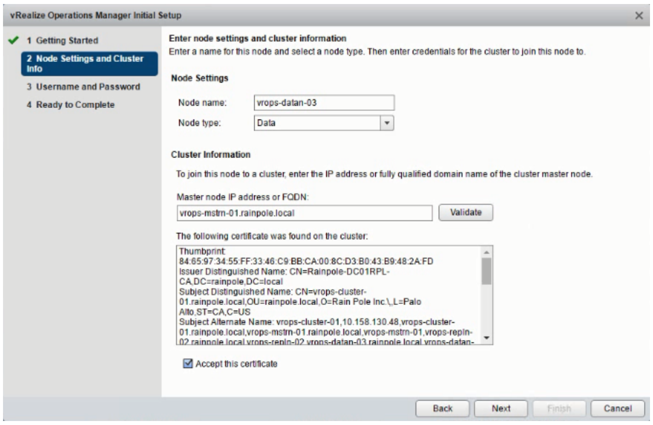
Procedure

1 Open a Web browser and go to `https://vrops-datan-03.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.



Enter node settings and cluster information

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: vrops-datan-03

Node type: Data

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: vrops-mstrn-01.rainpole.local

The following certificate was found on the cluster:

```
Thumbprint:
84:65:97:34:55:FF:33:46:C9:BB:CA:00:8C:D3:B0:43:B9:48:2A:FD
Issuer Distinguished Name: CN=Rainpole-DC01RPL-
CA,DC=rainpole,DC=local
Subject Distinguished Name: CN=vrops-cluster-
01.rainpole.local,OU=rainpole.local,O=Rain Pole Inc.\,,L=Palo
Alto,ST=CA,C=US
Subject Alternate Name: vrops-cluster-01,10.158.130.48,vrops-cluster-
01.rainpole.local,vrops-mstrn-01.rainpole.local,vrops-mstrn-01,vrops-repln-
02.rainpole.local,vrops-repln-02,vrops-datan-03.rainpole.local,vrops-datan-
```

☑ Accept this certificate

a Configure the name, type and master address of the data node.

Setting	Value
Node name	vrops-datan-03
Node type	Data
Master node IP address or FQDN	vrops-mstrn-01.rainpole.local

b Click **Validate** next to the **Master node IP address or FQDN**.

The certificate of the master node certificate appears in the text box.

c Verify that the master certificate is correct, and click **Accept this certificate**.

d Click **Next**.

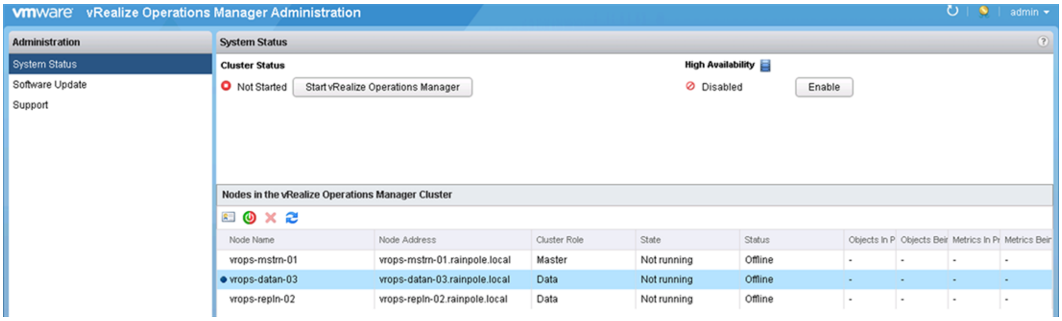
5 On the **Username and password** page, select **Use cluster administrator user name and password**, enter the `vrops_admin_password` password for the admin user, and click **Next**.

6 On the **Ready to Complete** page, click **Finish**.

When the configuration process completes, the vRealize Operations Manager Administration console opens.

7 Click **System Status** in the **Administration** panel to verify that the node is added to the cluster.

The virtual appliance instance acting as the data node appears in the **Nodes in the vRealize Operations Manager Cluster** list.



Node Name	Node Address	Cluster Role	State	Status	Objects In P	Objects Beir	Metrics In Pr	Metrics Beir
vrops-mstrn-01	vrops-mstrn-01.rainpole.local	Master	Not running	Offline	-	-	-	-
● vrops-datan-03	vrops-datan-03.rainpole.local	Data	Not running	Offline	-	-	-	-
vrops-repln-02	vrops-repln-02.rainpole.local	Data	Not running	Offline	-	-	-	-

Deploy the Remote Collector Virtual Appliances

After you deploy and enable the roles of the analytics cluster nodes, use the vSphere Web Client to deploy each of the two virtual appliances for the remote collectors in Region A. In a multi-region environment, you deploy remote collectors to forward data from the vCenter Server instances in Region A to the analytics cluster also to support failover of the analytics cluster.

Repeat this procedure two times to deploy two remote collector appliances.

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 Navigate to the mgmt01vc01.sfo01.rainpole.local vCenter Server object.

3 Right-click the **mgmt01vc01.sfo01.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
Name	■ vrops-rmtcol-01 for remote collector 1 ■ vrops-rmtcol-02 for remote collector 2
vCenter Server	mgmt01vc01.sfo01.rainpole.local
Data center	SFO01
Folder	vROps01RC

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

Setting	Value
Datacenter	SFO01
Cluster	SFO01-Mgmt01

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 the **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	SFO01A-VSAN01-MGMT01

11 On the **Select networks** page, select the distributed port group on the vDS-Mgmt distributed switch that ends with `Mgmt–RegionA01–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.

Option	Description
DNS server	172.16.11.5
Default gateway	192.168.31.1
Static IPv4 address	■ 192.168.31.31 for remote collector 1 ■ 192.168.31.32 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
vrops-rmtcol-01	Remote collector 1
vrops-rmtcol-02	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 procedure to deploy the second remote collector appliance.

Connect the Remote Collector Nodes to the Analytics Cluster

After you deploy the virtual appliances for the remote collector nodes on the Management vCenter Server, configure the settings of the remote collectors and connect them to the analytics cluster.

Procedure

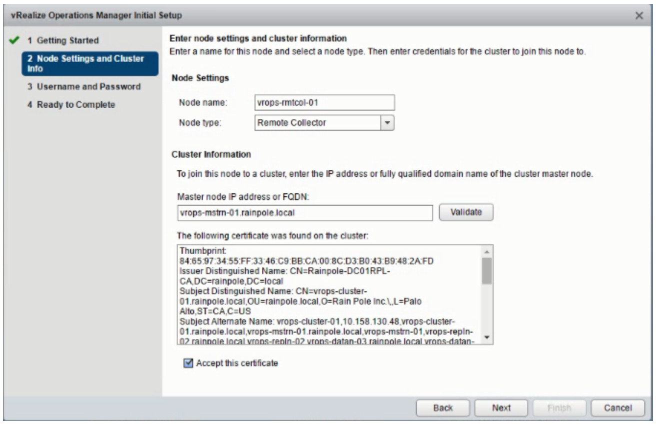
1 Open a Web browser, and go to the initial setup user interface of each remote collector node virtual appliance.

Remote Collector Node	URL for Setup Interface
Remote collector 1	https://vrops-rmtcol-01.sfo01.rainpole.local
Remote collector 2	https://vrops-rmtcol-02.sfo01.rainpole.local

2 In 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.



vRealize Operations Manager Initial Setup

Enter node settings and cluster information

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: vrops-rmtcol-01

Node type: Remote Collector

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: vrops-mstrn-01.rainpole.local

The following certificate was found on the cluster:

```
Thumbprint:
84:65:97:34:55:FF:33:46:C9:BB:CA:00:8C:D3:B0:43:B9:48:2A:FD
Issuer Distinguished Name: CN=Rainpole-DC01RPL-
CA,DC=rainpole,DC=local
Subject Distinguished Name: CN=vrops-cluster-
01.rainpole.local,OU=rainpole.local,O=Rain Pole Inc.\,L=Palo
Alto,ST=CA,C=US
Subject Alternate Name: vrops-cluster-01,10.158.130.48,vrops-cluster-
01.rainpole.local,vrops-mstrn-01.rainpole.local,vrops-mstrn-01,vrops-repln-
02.rainpole.local,vrops-repln-02,vrops-datan-03.rainpole.local,vrops-datan-
```

☑ Accept this certificate

a Configure the name, type and master address of the node.

Setting	Value
Node name	■ vrops-rmtcol-01 for remote collector 1 ■ vrops-rmtcol-02 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.

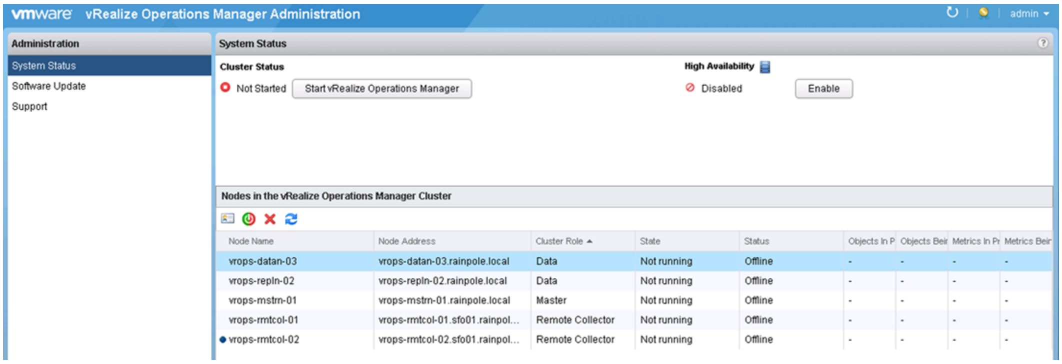
c Validate that the master certificate is correct, and click **Accept this certificate**.

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**.

After configuration of the second remote collector 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, and the remote collectors vrops-rmtcol-01 and vrops-rmtcol-02.



vmware vRealize Operations Manager Administration
admin
Administration
System Status
Software Update
Support

System Status

Cluster Status: Not Started

Start vRealize Operations Manager

High Availability: Disabled

Nodes in the vRealize Operations Manager Cluster

Node Name	Node Address	Cluster Role	State	Status	Objects In P	Objects Beir	Metrics In Pr	Metrics Beir
vrops-datan-03	vrops-datan-03.rainpole.local	Data	Not running	Offline	-	-	-	-
vrops-repln-02	vrops-repln-02.rainpole.local	Data	Not running	Offline	-	-	-	-
vrops-mstrn-01	vrops-mstrn-01.rainpole.local	Master	Not running	Offline	-	-	-	-
vrops-rmtcol-01	vrops-rmtcol-01.sfo01.rainpol...	Remote Collector	Not running	Offline	-	-	-	-
● vrops-rmtcol-02	vrops-rmtcol-02.sfo01.rainpol...	Remote Collector	Not running	Offline	-	-	-	-

Configure a DRS Anti-Affinity Rule for vRealize Operations Manager in Region A

To protect the vRealize Operations Manager virtual machines from a host-level failure, configure vSphere DRS to run both the virtual machines of the analytics cluster and of the remote collectors on different hosts in the management cluster.

You use two anti-affinity rules for the analytics virtual machines: one for the analytics nodes and one for the remote collector nodes. This rule configuration also accommodates the case when you place a host from the management cluster in maintenance mode.

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 Navigate to the mgmt01vc01.sfo01.rainpole.local vCenter Server object, and under the **SFO01** data center object select the **SFO01-Mgmt01** cluster.

3 Click **Configure** tab.

4 Under the **Configuration** group of settings, select **VM/Host Rules**.

5 In the **VM/Host Rules** list, click **Add** 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 vRealize Operations Manager analytics cluster, and click **OK**.

Setting	Value
Name	anti-affinity-rule-vropsm
Enable rule	Selected
Type	Separate Virtual Machines
Members	■ vrops-mstrn-01 ■ vrops-repln-02 ■ vrops-datan-03

7 In the **VM/Host Rules** list, click **Add** above the rules list, add a new anti-affinity rule for the virtual machines of the two remote collectors, and click **OK**.

Setting	Value
Name	anti-affinity-rule-vropsr
Enable rule	Selected
Type	Separate Virtual Machines
Members	■ vrops-rmtcol-01 ■ vrops-rmtcol-02

Enable High Availability and Start vRealize Operations Manager

After you deploy the virtual appliances for the analytics cluster nodes and remote collector nodes, enable high availability in the analytics cluster by assigning the replica role to the vrops-repln-02 node, and start the analytics cluster.

Procedure

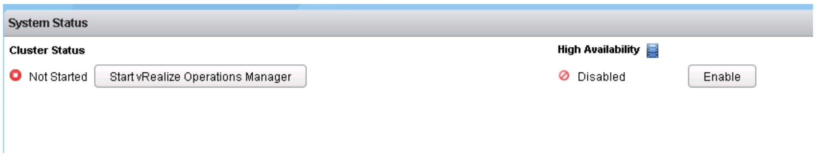
1 Log in to vRealize Operations Manager by using the administration console.

   a Open a Web browser and go to **`https://vrops-mstrn-01.rainpole.local`** .

   b Log in using the following credentials.

Setting	Value
User name	admin
Password	*vrops_admin_password*

   On the **System Status** page, the cluster status is `Not Started`, and the high availability of the cluster is `Disabled`.

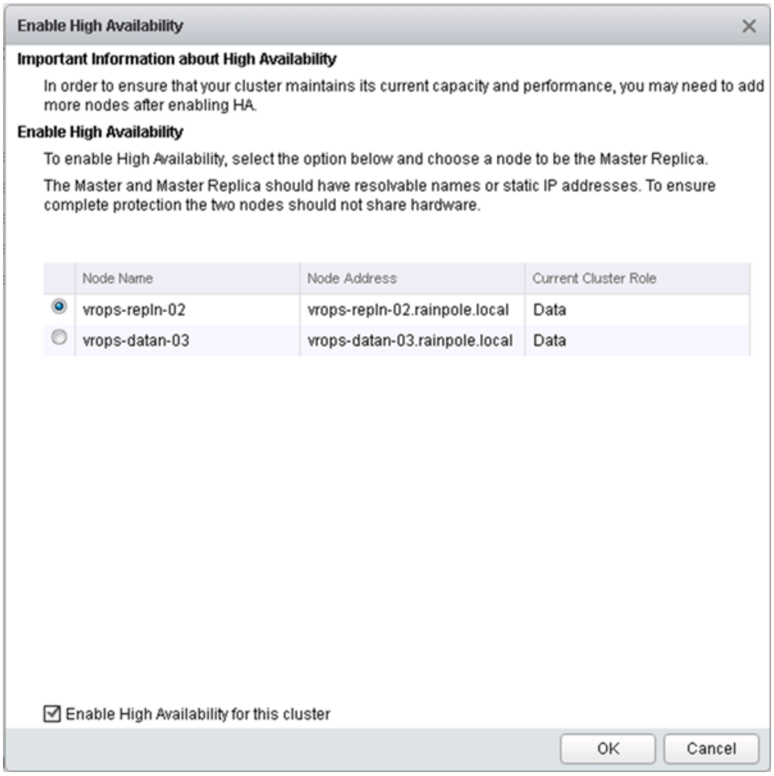


2 On the **System Status** page, click **Enable** under **High Availability**.

   A list of all nodes that have the data node role appears.

3 In the **Enable High Availability** dialog box, configure the following values, and click **OK**.

Setting	Value
vrops-repln-02	Selected
Enable High Availability for this cluster	Selected



Enable High Availability

Important Information about High Availability

In order to ensure that your cluster maintains its current capacity and performance, you may need to add more nodes after enabling HA.

Enable High Availability

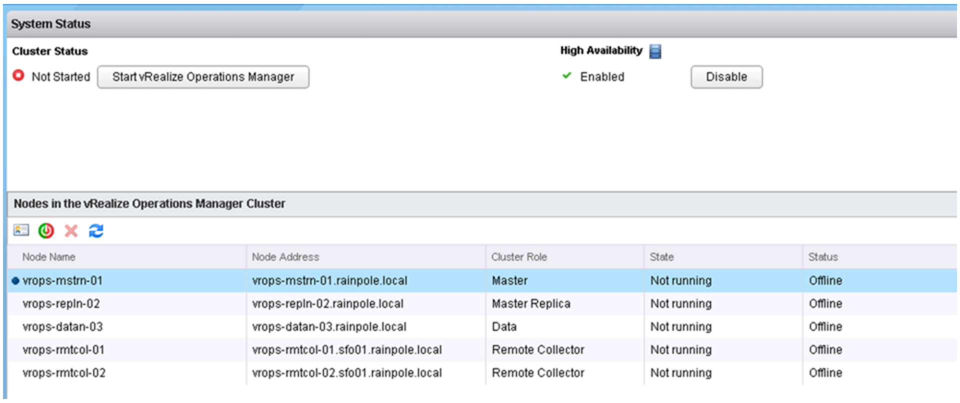
To enable High Availability, select the option below and choose a node to be the Master Replica.

The Master and Master Replica should have resolvable names or static IP addresses. To ensure complete protection the two nodes should not share hardware.

	Node Name	Node Address	Current Cluster Role
●	vrops-repln-02	vrops-repln-02.rainpole.local	Data
○	vrops-datan-03	vrops-datan-03.rainpole.local	Data

☑ Enable High Availability for this cluster

High availability becomes enabled after several minutes. The vrops-mstrn-01 is the master node, vrops-repln-02 is the master replica node, and the remaining nodes are data and remote collectors nodes.



System Status

Cluster Status: Not Started

High Availability: ✓ Enabled

Nodes in the vRealize Operations Manager Cluster

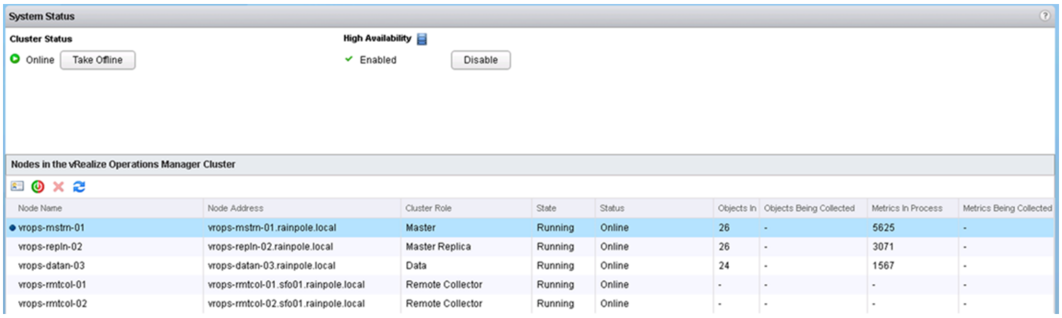
Node Name	Node Address	Cluster Role	State	Status
vrops-mstrn-01	vrops-mstrn-01.rainpole.local	Master	Not running	Offline
vrops-repln-02	vrops-repln-02.rainpole.local	Master Replica	Not running	Offline
vrops-datan-03	vrops-datan-03.rainpole.local	Data	Not running	Offline
vrops-rmtcol-01	vrops-rmtcol-01.sfo01.rainpole.local	Remote Collector	Not running	Offline
vrops-rmtcol-02	vrops-rmtcol-02.sfo01.rainpole.local	Remote Collector	Not running	Offline

4 Click **Start vRealize Operations Manager**.

A confirmation dialog about initial startup appears.

5 Click **Yes** to confirm the startup of vRealize Operations Manager.

After several minutes the nodes of the cluster start, and the analytics cluster and remote collectors for Region A are online.



Node Name	Node Address	Cluster Role	State	Status	Objects In	Objects Being Collected	Metrics In Process	Metrics Being Collected
● vrops-mstrn-01	vrops-mstrn-01.rainpole.local	Master	Running	Online	26	-	5625	-
vrops-repln-02	vrops-repln-02.rainpole.local	Master Replica	Running	Online	26	-	3071	-
vrops-datan-03	vrops-datan-03.rainpole.local	Data	Running	Online	24	-	1567	-
vrops-rmtcol-01	vrops-rmtcol-01.sfo01.rainpole.local	Remote Collector	Running	Online	-	-	-	-
vrops-rmtcol-02	vrops-rmtcol-02.sfo01.rainpole.local	Remote Collector	Running	Online	-	-	-	-

Assign a License to vRealize Operations Manager

After you deploy and start vRealize Operations Manager in Region A, you assign a valid license.

Procedure

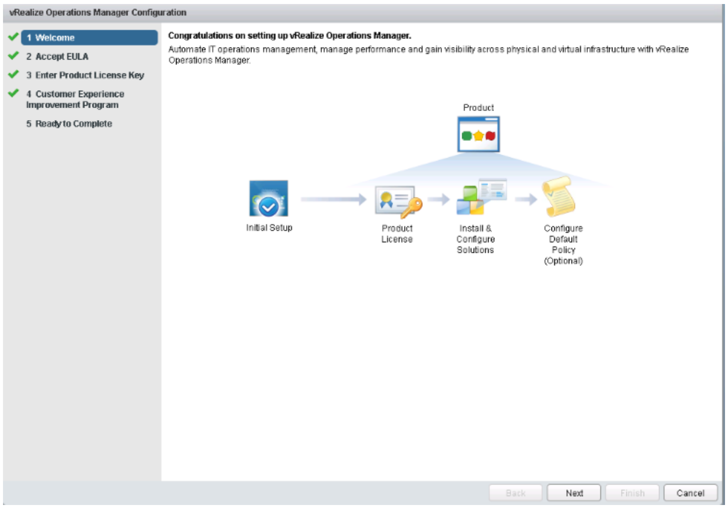
1 Log in to the **vRealize Operations Manager Configuration** wizard.

  a Open a Web browser and go to **`https://vrops-mstrn-01.rainpole.local`** .

  b Log in using the following credentials.

Setting	Value
User name	admin
Password	*vrops_admin_password*

2 On the **Welcome** page of the **vRealize Operations Manager Configuration** wizard, examine the process overview, and click **Next**.



vRealize Operations Manager Configuration
✓ 1 Welcome
✓ 2 Accept EULA
✓ 3 Enter Product License Key
✓ 4 Customer Experience Improvement Program
5 Ready to Complete
Product
Initial Setup
Product License
Install & Configure Solutions
Configure Default Policy (Optional)
Back
Next
Finish
Cancel

Congratulations on setting up vRealize Operations Manager.

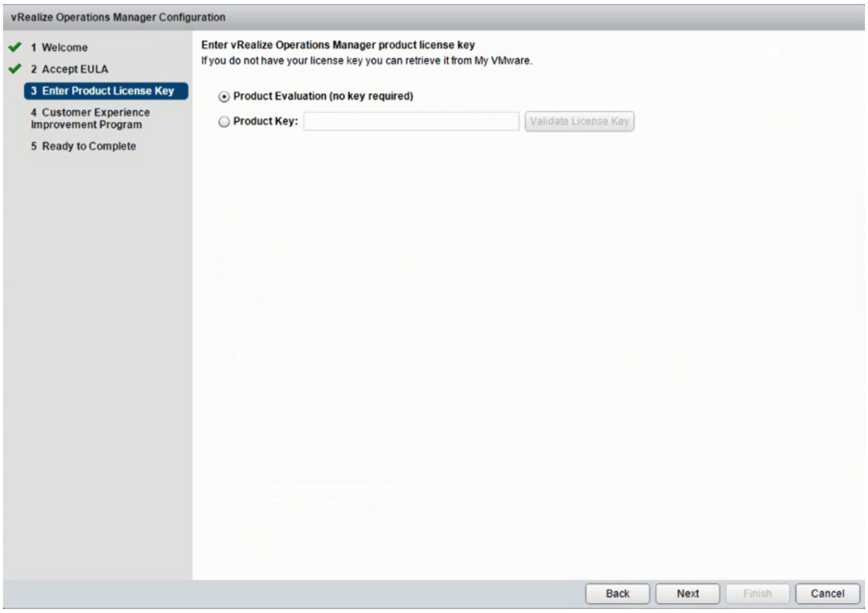
Automate IT operations management, manage performance and gain visibility across physical and virtual infrastructure with vRealize Operations Manager.

3 On the **Accept EULA** page, accept the end user license agreement, and click **Next**.

4. On the **Enter Product License Key** page, enter the vRealize Operations manager product license key.

   a. Select **Product Key** and enter the license key.

   b. Click **Validate License Key**, and click **Next**.



vRealize Operations Manager Configuration

Enter vRealize Operations Manager product license key

If you do not have your license key you can retrieve it from My VMware.

● Product Evaluation (no key required)

○ Product Key:

5. (Optional) On the **Customer Experience Improvement Program** page, to send technical information for product improvement, select **Join the VMware Customer Experience Impovement Program** and click **Next**.

6. On the **Ready to Complete** page, click **Finish**.

The vRealize Operations Manager user interface opens.

Group Remote Collector Nodes in Region A

After you start vRealize Operations Manager and assign it a license, 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 the vRealize Operations Manager administration console.

   a. Open a Web browser and go to `https://vrops-mstrn-01.rainpole.local`.

   b. Log in using the following credentials.

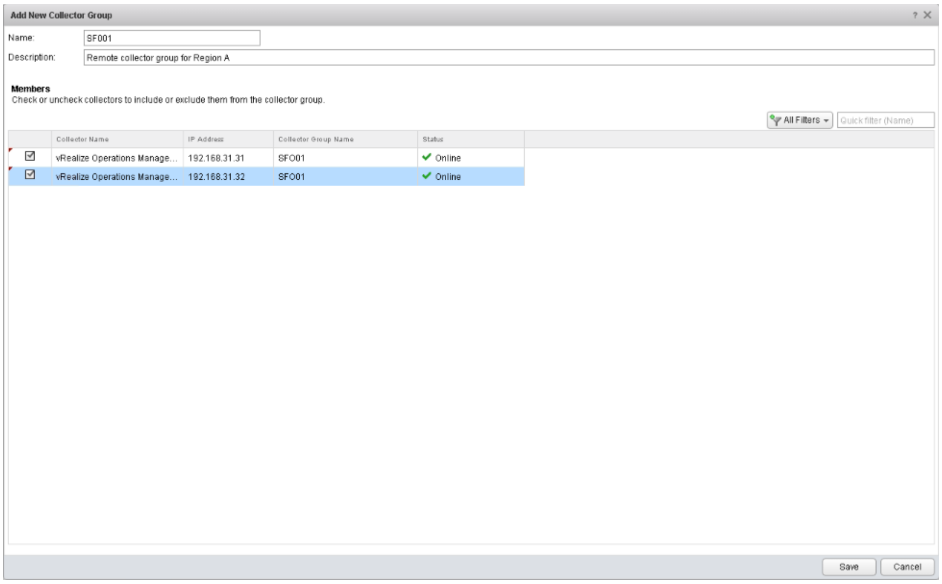
Setting	Value
User name	admin
Password	*vrops_admin_password*

2 On the **Home** page, click **Administration** and click **Collector Groups**.

3 Click **Add**.

4 In the **Add New Collector Group** dialog box, configure the following settings, and click **Save**.

Setting	Value
Name	SFO01
Description	Remote collector group for Region A
vrops-rmtcol-01	Selected
vrops-rmtcol-02	Selected



Add New Collector Group

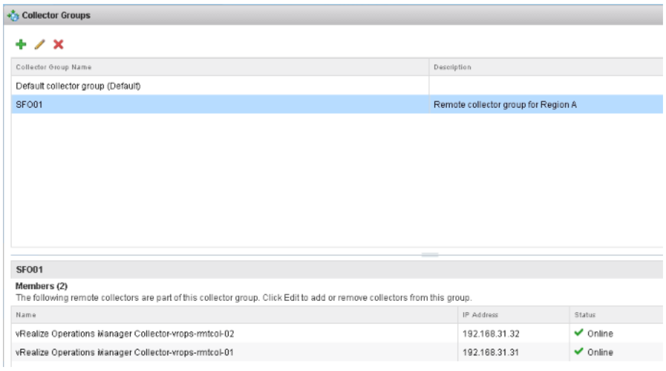
Name: SF001

Description: Remote collector group for Region A

Members
Check or uncheck collectors to include or exclude them from the collector group.

	Collector Name	IP Address	Collector Group Name	Status
☑	vRealize Operations Manage...	192.168.31.31	SFO01	✓ Online
☑	vRealize Operations Manage...	192.168.31.32	SFO01	✓ Online

The SFO01 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)	
SFO01	Remote collector group for Region A

SFO01

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
vRealize Operations Manager Collector-vrops-rmtcol-02	192.168.31.32	✓ Online
vRealize Operations Manager Collector-vrops-rmtcol-01	192.168.31.31	✓ Online

Configure the Load Balancer for vRealize Operations Manager in Region A

Configure load balancing for the analytics cluster on the dedicated SFOMGMT-LB01 NSX Edge service gateway for Region A. Remote collector cluster for Region A does not require load balancing.

Prerequisites

- Verify that the NSX Manager for the management cluster has the management virtual application network for the analytics cluster configured.
- Verify that the Load Balancer service is enabled on the NSX Edge service gateway.

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 From the **Home** menu, select **Networking & Security**.

   The vSphere Web Client displays the **NSX Home** page.

3 On the **NSX Home** page, click **NSX Edges** and select **172.16.11.65** from the **NSX Manager** drop-down menu at the top of the **NSX Edges** page.

4 On the **NSX Edges** page, double-click the **SFOMGMT-LB01** NSX edge.

5 Configure the load balancing VIP address for analytics cluster.

   a On the **Manage** tab, click the **Settings** tab and click **Interfaces**.

   b Select the **OneArmLB** interface and click the **Edit** icon.

   c In the **Edit NSX Edge Interface** dialog box, click the **Edit** icon and in the **Secondary IP Addresses** text box enter the `192.168.11.35` VIP address.

   d Click **OK** to save the configuration.

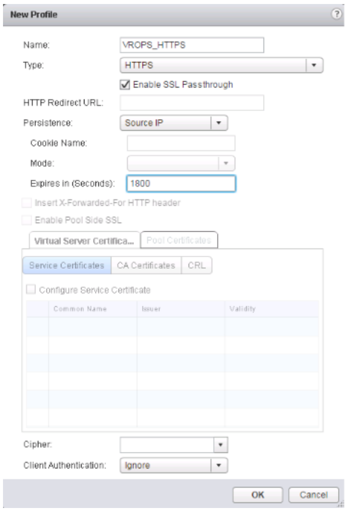
6 Create an application profile.

a On the **Manage** tab for the SFOMGMT-LB01 device, click the **Load Balancer** tab.

b Click **Application Profiles**, and click the **Add** icon.

c In the **New Profile** dialog box, configure the profile using the following configuration settings, and click **OK**.

Setting	Value
Name	VROPS_HTTPS
Type	HTTPS
Enable SSL Passthrough	Selected
Persistence	Source IP
Expires in (Seconds)	1800
Client Authentication	Ignore



New Profile

Name: VROPS_HTTPS

Type: HTTPS

☑ Enable SSL Passthrough

HTTP Redirect URL:

Persistence: Source IP

Cookie Name:

Mode:

Expires in (Seconds): 1800

□ Insert X-Forwarded-For HTTP header

□ Enable Pool Side SSL

□ Configure Service Certificate

Common Name	Issuer	Validity

Cipher:

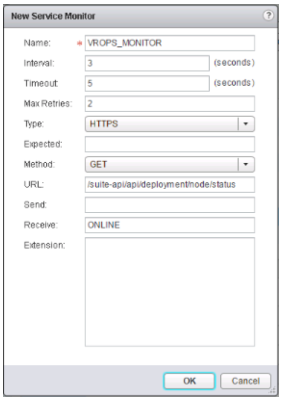
Client Authentication: Ignore

7 Create a service monitoring entry.

a On the **Load Balancer** tab for the of the SFOMGMT-LB01 device, click **Service Monitoring** and click the **Add** icon.

b In the **New Service Monitor** dialog box, configure the health check parameters using the following configuration settings, and click **OK**.

Setting	Value
Name	VROPS_MONITOR
Interval	3
Timeout	5
Max Retries	2
Type	HTTPS
Method	GET
URL	/suite-api/api/deployment/node/status
Receive	ONLINE (must be upper case)



New Service Monitor

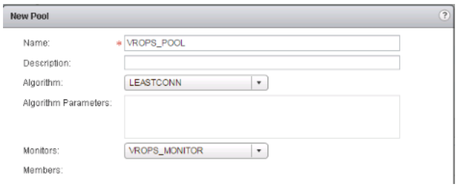
Name: * VROPS_MONITOR
Interval: 3 (seconds)
Timeout: 5 (seconds)
Max Retries: 2
Type: HTTPS
Expected:
Method: GET
URL: /suite-api/api/deployment/node/status
Send:
Receive: ONLINE
Extension:

8 Add a server pool.

a On the **Load Balancer** tab of the SFOMGMT-LB01 device, select **Pools**, and click the **Add** icon.

b In the **New Pool** dialog box, configure the load balancing profile using the following configuration settings.

Setting	Value
Name	VROPS_POOL
Algorithm	LEASTCONN
Monitors	VROPS_MONITOR



New Pool

Name: * VROPS_POOL
Description:
Algorithm: LEASTCONN
Algorithm Parameters:
Monitors: VROPS_MONITOR
Members:

c Under **Members**, click the **Add** icon to add the pool members.

d In the **New Member** dialog box, add one member for each node of the analytics cluster and click **OK**.

Setting	Value
Name	■ vrops-mstrn-01 ■ vrops-repln-02 ■ vrops-datan-03
IP Address	■ 192.168.11.31 ■ 192.168.11.32 ■ 192.168.11.33
State	Enable
Port	443
Monitor Port	443
Weight	1
Max Connections	8
Min Connections	8

e In the **New Pool** dialog box, click **OK**.

9 Add a virtual server.

a On the **Load Balancer** tab of the SFOMGMT-LB01 device, select **Virtual Servers** and click the **Add** icon.

b In the **New Virtual Server** dialog box, configure the settings of the virtual server for the analytics cluster and click **OK**.

Setting	Value
Enable Virtual Server	Selected
Application Profile	VROPS_HTTPS
Name	VROPS_VIRTUAL_SERVER
IP Address	192.168.11.35 Click **Select IP Address**, select **OneArmLB** from the drop-down menu and select **192.168.11.35** IP for the virtual NIC.
Protocol	HTTPS
Port	443
Default Pool	VROPS_POOL
Connection Limit	0
Connection Rate Limit	0

You can connect to the analytics cluster at the public Virtual Server IP address over HTTPS at the `https://vrops-cluster-01.rainpole.local` address.

10 Configure auto-redirect from HTTP to HTTPS requests.

The NSX Edge can redirect users from HTTP to HTTPS without entering another URL in the browser.

a On the **Load Balancer** tab of the SFOMGMT-LB01 device, select **Application Profiles** and click the **Add** icon.

b In the **New Profile** dialog box, configure the application profile settings and click **OK**.

Setting	Value
Name	VROPS_REDIRECT
Type	HTTP
HTTP Redirect URL	https://vrops-cluster-01.rainpole.local/vcops-web-ent/login.action
Persistence	Source IP
Expires in (Seconds)	1800

c On the **Load Balancer** tab of the SFOMGMT-LB01 device, select **Virtual Servers** and click the **Add** icon.

d Configure the settings of the virtual server for HTTP redirects.

Setting	Value
Enable Virtual Server	Selected
Application Profile	VROPS_REDIRECT
Name	VROPS_REDIRECT
IP Address	192.168.11.35
Protocol	HTTP
Port	80
Default Pool	NONE
Connection Limit	0
Connection Rate Limit	0

You can connect to the analytics cluster at the public Virtual Server IP address over HTTP at the `http://vrops-cluster-01.rainpole.local` address.

11 Verify the pool configuration by examining the pool statistics that reflect the status of the components behind the load balancer.

a Log out and log in again to the vSphere Web Client.

b From the **Home** menu, select **Networking & Security**.

c On the **NSX Home** page, click **NSX Edges** and select **172.16.11.65** from the **NSX Manager** drop-down menu at the top of the **NSX Edges** page.

d On the **NSX Edges** page, double-click the **SFOMGMT-LB01** NSX edge.

e On the **Manage** tab, click the **Load Balancer** tab.

f Select **Pools** and click **Show Pool Statistics**.

g In the **Pool and Member Status** dialog box, select the **VROPS_POOL** pool.

Verify that the load balancer pool is up.

Add an Authentication Source for the Active Directory

Connect vRealize Operations Manager to the Active Directory of the SDDC for central user management and access control.

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`.

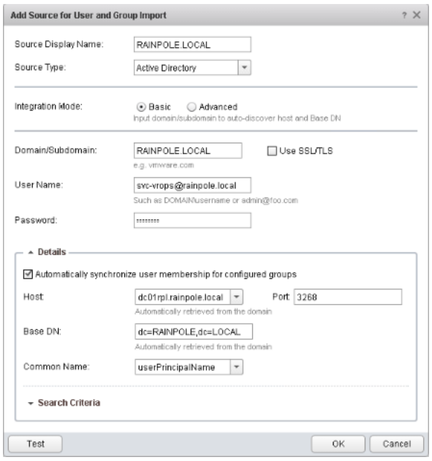
b Log in using the following credentials.

Setting	Value
User name	admin
Password	*vrops_admin_password*

2 In the left pane of vRealize Operations Manager, click **Administration** and click **Authentication Sources**.

3 On the **Authentication Sources** page, click the **Add** button.

4 In the **Add Source for User and Group Import** dialog box, enter the settings for the rainpole.local and sfo01.rainpole.local Active Directories, and click **OK**.



Add Source for User and Group Import

Source Display Name: RAINPOLE.LOCAL

Source Type: Active Directory

Integration Mode: ● Basic ○ Advanced

Input domain/subdomain to auto-discover host and Base DN

Domain/Subdomain: RAINPOLE.LOCAL □ Use SSL/TLS

e.g. vmware.com

User Name: svc-vrops@rainpole.local

Such as DOMAIN\username or admin@foo.com

Password: ••••••••

Details

☑ Automatically synchronize user membership for configured groups

Host: dc01rpl.rainpole.local Port: 3268

Automatically retrieved from the domain

Base DN: dc=RAINPOLE,dc=LOCAL

Automatically retrieved from the domain

Common Name: userPrincipalName

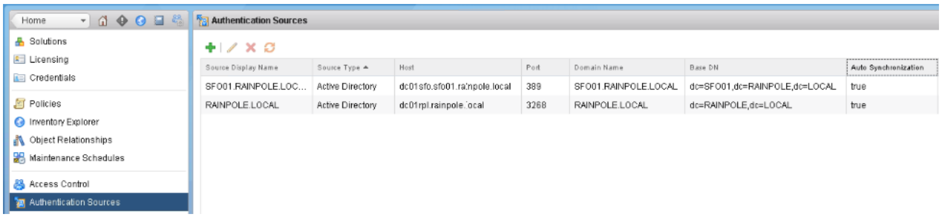
Active Directory Settings	rainpole.local Value	sfo01.rainpole.local Value
Source Display Name	RAINPOLE.LOCAL	SFO01.RAINPOLE.LOCAL
Source Type	Active Directory	Active Directory
Integration Mode	Basic	Basic

Active Directory Settings	rainpole.local Value	sfo01.rainpole.local Value
Domain/Subdomain	RAINPOLE.LOCAL	SFO01.RAINPOLE.LOCAL
Use SSL/TLS	Deselected	Deselected
User Name	svc-vrops@rainpole.local	svc-vrops@rainpole.local
Password	*svc-vrops_password*	*svc-vrops_password*
Settings under the **Details** section		
Automatically synchronize user membership for configured groups	Selected	Selected
Host	dc01rpl.rainpole.local	dc01sfo.sfo01.rainpole.local
Port	3268	389
Base DN	dc=RAINPOLE,dc=LOCAL	dc=SFO01,dc=RAINPOLE,dc=LOCAL
Common Name	userPrincipalName	userPrincipalName

5 Click the **Test** button to test the connection to the domain controller and in the **Info** success message click **OK**.

6 In the **Add Source for User and Group Import** dialog box, click **OK**.

The two Active Directories are added to vReliaze Operations Manager.



Authentication Sources

Source Display Name	Source Type	Host	Port	Domain Name	Base DN	Auto Synchronization
SFO01.RAINPOLE.LOC...	Active Directory	dc01sfo.sfo01.rainpole.local	389	SFO01.RAINPOLE.LOCAL	dc=SFO01,dc=RAINPOLE,dc=LOCAL	true
RAINPOLE.LOCAL	Active Directory	dc01rpl.rainpole.local	3268	RAINPOLE.LOCAL	dc=RAINPOLE,dc=LOCAL	true

Configure User Access in vSphere for Integration with vRealize Operations Manager in Region A

Configure operations services accounts with permissions that are required to enable vRealize Operations Manager access to monitoring data on the Management vCenter Server and Compute vCenter Server in Region A.

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 instanced in the inventory.

Procedure

1 Define a User Role in vSphere for Storage Devices Adapters in vRealize Operations Manager for Region A

In vSphere, 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 Region A

Assign global permissions in Region A to the operations service accounts svc-vrops and svc-mpsd-vrops in order to access monitoring data from the Management vCenter Server and Compute vCenter Server in Region A with vRealize Operations Manager.

Define a User Role in vSphere for Storage Devices Adapters in vRealize Operations Manager for Region A

In vSphere, 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://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, 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	■ **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.

4 The Management vCenter Server for Region A propagates the role to the other linked vCenter Server instances.

Configure User Privileges in vSphere for Integration with vRealize Operations Manager for Region A

Assign global permissions in Region A to the operations service accounts svc-vrops and svc-mpsd-vrops in order to access monitoring data from the Management vCenter Server and Compute vCenter Server in Region A with 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 Management vCenter Server and Compute vCenter Server for Region A are connected to the Active Directory domain.
- Verify that the users and groups from the rainpole.local domain are available in the Management vCenter Server and in the Compute vCenter Server for Region A.

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*

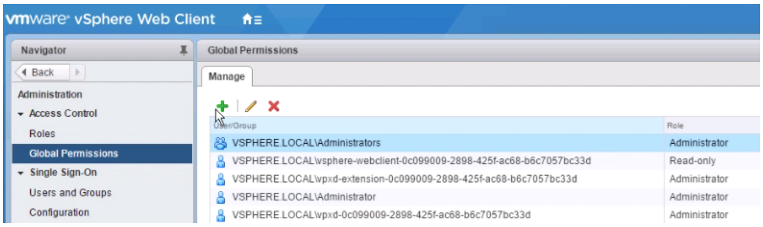
2 From the **Home** menu, select **Administration**.

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 **Administration** and click **Global Permissions**.

   b Click **Add Permission**.

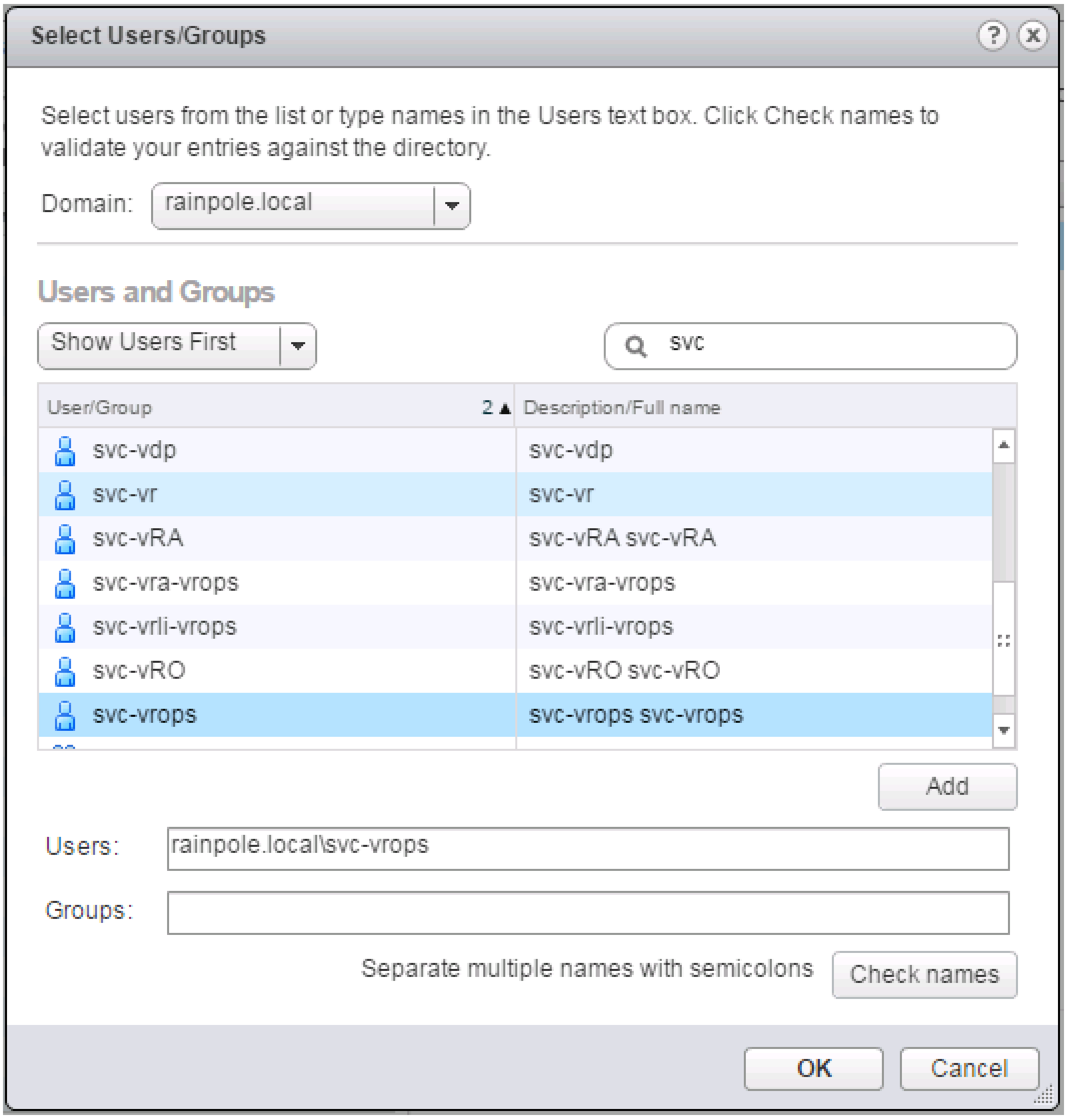


User/Group	Role
VSPHERE.LOCAL\Administrators	Administrator
VSPHERE.LOCAL\vsphere-webclient-0c099009-2898-425f-ac68-b6c7057bc33d	Read-only
VSPHERE.LOCAL\vpxd-extension-0c099009-2898-425f-ac68-b6c7057bc33d	Administrator
VSPHERE.LOCAL\Administrator	Administrator
VSPHERE.LOCAL\vpxd-0c099009-2898-425f-ac68-b6c7057bc33d	Administrator

   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**.



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

svc

User/Group 2 ▲	Description/Full name
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
svc-vrops	svc-vrops svc-vrops

Users: rainpole.local\svc-vrops

Groups:

Separate multiple names with semicolons

f In the **Global Permissions Root - Add Permission** dialog box, from the **Assigned Role** drop-down menu, select **Read-only**, ensure that **Propogate to children** is selected, and click **OK**.

g Repeat the steps to assign the `MPSD Metrics User` role to the svc-mpsd-vrops user.

The global permissions of svc-vrops and svc-mpsd-vrops propagate to all linked vCenter Server instances.

Add vCenter Adapter Instances to vRealize Operations Manager for Region A

After you deploy the analytics cluster and the remote collector nodes of vRealize Operations Manager in Region A and start vRealize Operations Manager, add vCenter Adapter instances for the Management and Compute vCenter Server instances in Region A.

Prerequisites

- Verify that the Management vCenter Server and Compute vCenter Server are running.
- Verify that the Management vCenter Server and Compute vCenter Server are configured with the rainpole.local Active Directory domain.

Procedure

1 Log in to vRealize Operations Manager by using the administration console.

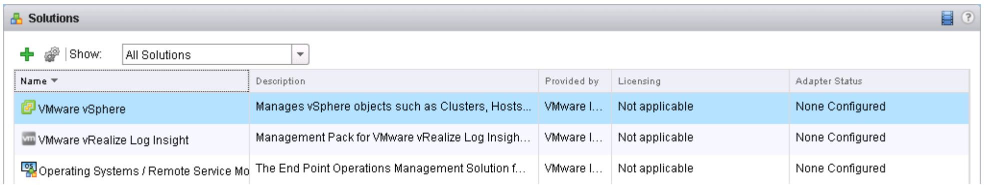
   a Open a Web browser and go to **`https://vrops-cluster-01.rainpole.local`**.

   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.



Solutions

Show: All Solutions

Name	Description	Provided by	Licensing	Adapter Status
VMware vSphere	Manages vSphere objects such as Clusters, Hosts...	VMware I...	Not applicable	None Configured
VMware vRealize Log Insight	Management Pack for VMware vRealize Log Insigh...	VMware I...	Not applicable	None Configured
Operating Systems / Remote Service Mo	The End Point Operations Management Solution f...	VMware I...	Not applicable	None Configured

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**.

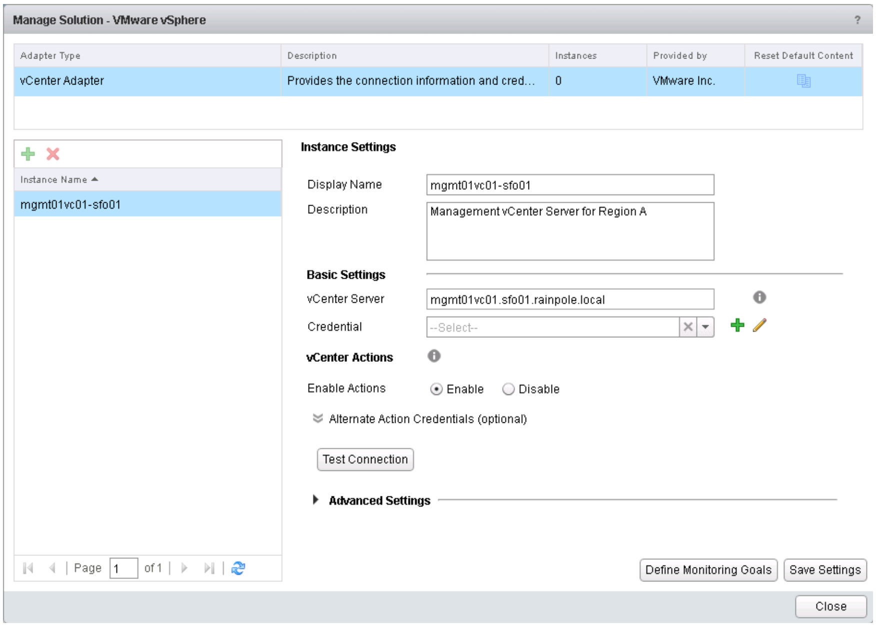
Empty settings for the vCenter Adapter default instance appear under **Instance Settings** if vRealize Operations Manager does not have vCenter Adapters configured.

5 Under **Instance Settings**, enter the settings for connection to vCenter Server.

a If you already have added another vCenter Adapter, 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 for Management vCenter Server	Value for Compute vCenter Server
Name	mgmt01vc01-sfo01	comp01vc01-sfo01
Description	Management vCenter Server for Region A	Compute vCenter Server for Region A
vCenter Server	mgmt01vc01.sfo01.rainpole.local	comp01vc01.sfo01.rainpole.local



Manage Solution - VMware vSphere

Adapter Type	Description	Instances	Provided by	Reset Default Content
vCenter Adapter	Provides the connection information and cred...	0	VMware Inc.	

Instance Name ▲
mgmt01vc01-sfo01

Instance Settings

Display Name: mgmt01vc01-sfo01

Description: Management vCenter Server for Region A

Basic Settings

vCenter Server: mgmt01vc01.sfo01.rainpole.local

Credential: --Select--

vCenter Actions

Enable Actions: ● Enable ○ Disable

Alternate Action Credentials (optional)

c Click the **Add** icon on the right side, configure the collection credentials for connection to the vCenter Server instances, and click **OK**.

Management vCenter Server Credentials Attribute	Value
Credential name	■ mgmt01vc01-sfo01-credentials (for Management vCenter Server) ■ comp01vc01-sfo01-credentials (for Compute 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.

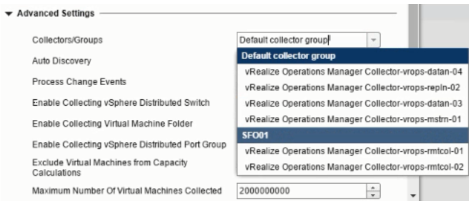
The vCenter Server certificate appears.

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 **SFO01** group.



Advanced Settings

Collectors/Groups: Default collector group

Auto Discovery

Process Change Events

Enable Collecting vSphere Distributed Switch

Enable Collecting Virtual Machine Folder

Enable Collecting vSphere Distributed Port Group

Exclude Virtual Machines from Capacity Calculations

Maximum Number Of Virtual Machines Collected: 2000000000

Default collector group
vRealize Operations Manager Collector-vrops-datan-04
vRealize Operations Manager Collector-vrops-repln-02
vRealize Operations Manager Collector-vrops-datan-03
vRealize Operations Manager Collector-vrops-mstrn-01
SFO01
vRealize Operations Manager Collector-vrops-rmtcol-01
vRealize Operations Manager Collector-vrops-rmtcol-02

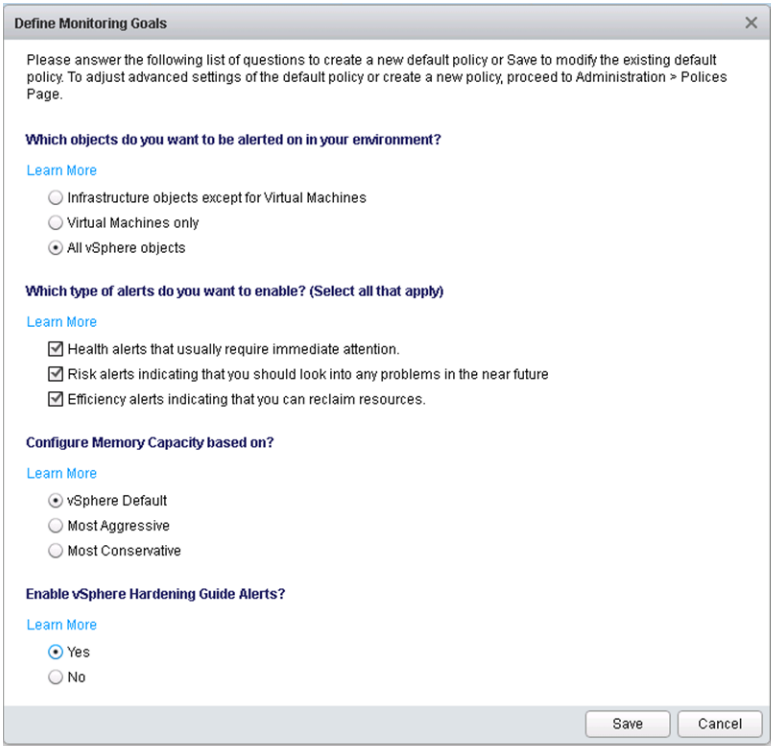
j Specify a user account with administrator privileges to register vRealize Operations Manager with the vCenter Server instance.

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.

Setting	Value
Registration user	administrator@vsphere.local
Registration password	*vsphere_admin_password*

6 Click **Define Monitoring Goals**

7 On 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 > Polices 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?

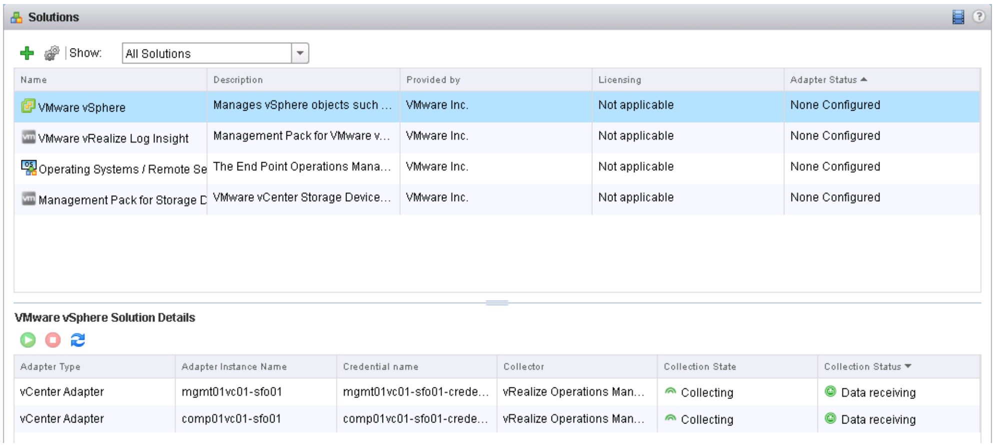
Learn More

● Yes
○ No

8. Click **OK** in the **Default Policy Information** 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. Repeat Step 5 to Step 11 for the Compute vCenter Server.
13. In the **Manage Solution - VMware vSphere** dialog box, click **Close.**
14. On the **Solutions** page, select **VMware vSphere** from the solution table to view the collection state and collection status of the adapters.

    The collection state indicates whether the adapter should be collecting data. The collection status value indicates whether vRealize Operations Manager is receiving data about a certain object type. An adapter instance has a status value only if its collection state is `Collecting`.

    The **Collection State** column for the vCenter Adapters displays `Collecting`, and the **Collection Status** column displays `Data receiving`.



Name	Description	Provided by	Licensing	Adapter Status ▲
VMware vSphere	Manages vSphere objects such ...	VMware Inc.	Not applicable	None Configured
VMware vRealize Log Insight	Management Pack for VMware v...	VMware Inc.	Not applicable	None Configured
Operating Systems / Remote Se	The End Point Operations Mana...	VMware Inc.	Not applicable	None Configured
Management Pack for Storage D	VMware vCenter Storage Device...	VMware Inc.	Not applicable	None Configured

VMware vSphere Solution Details

Adapter Type	Adapter Instance Name	Credential name	Collector	Collection State	Collection Status ▼
vCenter Adapter	mgmt01vc01-sfo01	mgmt01vc01-sfo01-crede...	vRealize Operations Man...	Collecting	Data receiving
vCenter Adapter	comp01vc01-sfo01	comp01vc01-sfo01-crede...	vRealize Operations Man...	Collecting	Data receiving

Connect vRealize Operations Manager to the NSX Managers in Region A

Install and configure the vRealize Operations Management Pack for NSX for vSphere to monitor the NSX networking services deployed in each vSphere cluster 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.

Prerequisites

- Download the `.pak` file for the vRealize Operations Manager Management Pack for NSX for vSphere from *VMware Solutions Exchange*.
- Verify that the vCenter Server instances for Region A are deployed.

- Verify that the NSX Manager is installed and configured for the management cluster, and for the shared edge and compute cluster.
- Verify that vRealize Operations Manager is deployed and its analytics cluster is started.
- Verify that the remote collector nodes for Region A are deployed and grouped.
- Verify that vRealize Log Insight is deployed.

Procedure

1 Install the vRealize Operations Manager Management Pack for NSX for vSphere in Region A

Install the `.pak` file for the management pack for NSX for vSphere to add the solution entry and adapters to vRealize Operations Manager.

2 Configure User Privileges in NSX Manager for Integration with vRealize Operations Manager for Region A

Assign the permissions that are required to access monitoring data from the Management NSX Manager and Compute Manager in Region A in vRealize Operations Manager to the operations local service account svc-vrops-nsx.

3 Add NSX-vSphere Adapter Instances to vRealize Operations Manager for Region A

After you install the management pack, configure NSX-vSphere Adapters: one for the NSX Manager for the management cluster and one for the NSX Manager for the shared edge and compute cluster.

4 Add Network Devices Adapter to vRealize Operations Manager for Region A

Configure a Network Devices Adapter to monitor the switches and routers in your environment, and view related alerts, metrics and object capacity.

Install the vRealize Operations Manager Management Pack for NSX for vSphere in Region A

Install the `.pak` file for the management pack for NSX for vSphere to add the solution entry and adapters to vRealize Operations Manager.

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`**.

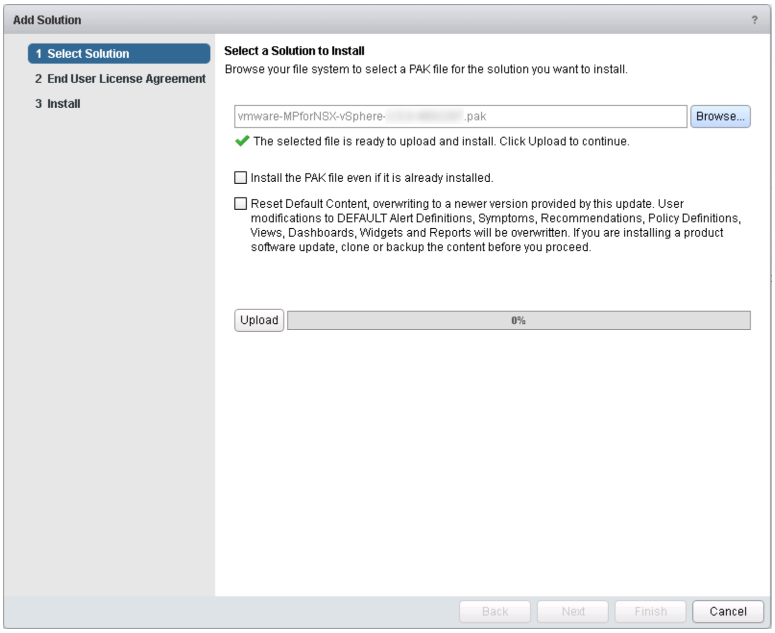
b Log in using the following credentials.

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, click the **Add** icon.

4 On the **Select Solution** page from the **Add Solution** wizard, browse to the `.pak` file of the vRealize Operations Manager Management Pack for NSX for vSphere and click **Upload**.



Select a Solution to Install

Browse your file system to select a PAK file for the solution you want to install.

vmware-MPforNSX-vSphere-[redacted].pak

✓ The selected file is ready to upload and install. Click Upload to continue.

□ Install the PAK file even if it is already installed.

□ Reset Default Content, overwriting to a newer version provided by this update. User modifications to DEFAULT Alert Definitions, Symptoms, Recommendations, Policy Definitions, Views, Dashboards, Widgets and Reports will be overwritten. If you are installing a product software update, clone or backup the content before you proceed.

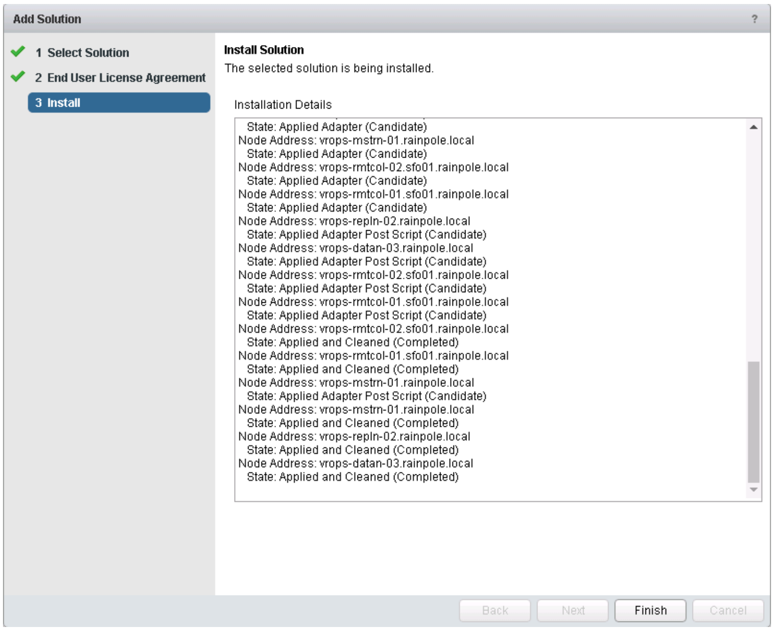
After the NSX management pack file has been uploaded, you see details about the management pack.

5 After the upload is complete, click **Next**.

6 On the **End User License Agreement** page, accept the license agreement and click **Next**.

The installation of the management pack starts. You see its progress on the **Install** page.

7 After the installation is complete, click **Finish** on the **Install** page.



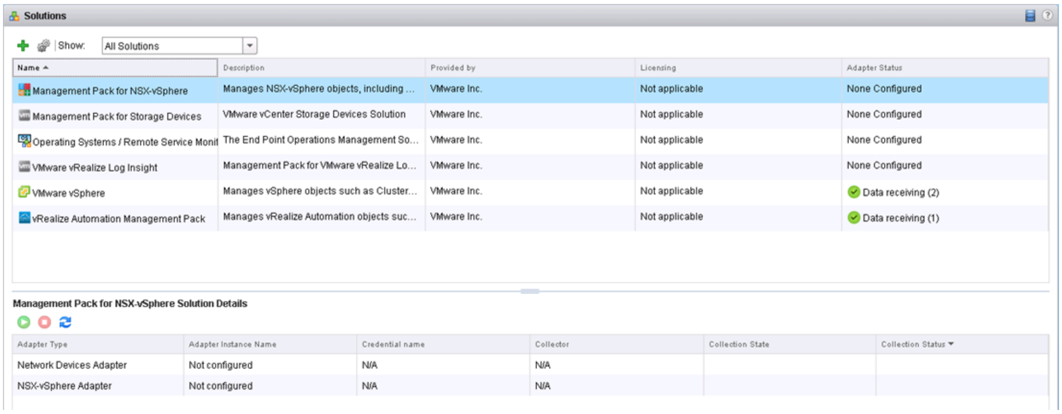
Install Solution

The selected solution is being installed.

Installation Details

```
  State: Applied Adapter (Candidate)
Node Address: vrops-mstrn-01.rainpole.local
  State: Applied Adapter (Candidate)
Node Address: vrops-rmtcol-02.sfo01.rainpole.local
  State: Applied Adapter (Candidate)
Node Address: vrops-rmtcol-01.sfo01.rainpole.local
  State: Applied Adapter (Candidate)
Node Address: vrops-repln-02.rainpole.local
  State: Applied Adapter Post Script (Candidate)
Node Address: vrops-datan-03.rainpole.local
  State: Applied Adapter Post Script (Candidate)
Node Address: vrops-rmtcol-02.sfo01.rainpole.local
  State: Applied Adapter Post Script (Candidate)
Node Address: vrops-rmtcol-01.sfo01.rainpole.local
  State: Applied Adapter Post Script (Candidate)
Node Address: vrops-rmtcol-02.sfo01.rainpole.local
  State: Applied and Cleaned (Completed)
Node Address: vrops-rmtcol-01.sfo01.rainpole.local
  State: Applied and Cleaned (Completed)
Node Address: vrops-mstrn-01.rainpole.local
  State: Applied Adapter Post Script (Candidate)
Node Address: vrops-mstrn-01.rainpole.local
  State: Applied and Cleaned (Completed)
Node Address: vrops-repln-02.rainpole.local
  State: Applied and Cleaned (Completed)
Node Address: vrops-datan-03.rainpole.local
  State: Applied and Cleaned (Completed)
```

The Management Pack for NSX-vSphere solution appears on the **Solutions** page of the vRealize Operations Manager user interface.



Name	Description	Provided by	Licensing	Adapter Status
Management Pack for NSX-vSphere	Manages NSX-vSphere objects, including ...	VMware Inc.	Not applicable	None Configured
Management Pack for Storage Devices	VMware vCenter Storage Devices Solution	VMware Inc.	Not applicable	None Configured
Operating Systems / Remote Service Monit	The End Point Operations Management So...	VMware Inc.	Not applicable	None Configured
VMware vRealize Log Insight	Management Pack for VMware vRealize Lo...	VMware Inc.	Not applicable	None Configured
VMware vSphere	Manages vSphere objects such as Cluster...	VMware Inc.	Not applicable	✓ Data receiving (2)
vRealize Automation Management Pack	Manages vRealize Automation objects suc...	VMware Inc.	Not applicable	✓ Data receiving (1)

Management Pack for NSX-vSphere Solution Details

Adapter Type	Adapter Instance Name	Credential name	Collector	Collection State	Collection Status
Network Devices Adapter	Not configured	N/A	N/A		
NSX-vSphere Adapter	Not configured	N/A	N/A		

Configure User Privileges in NSX Manager for Integration with vRealize Operations Manager for Region A

Assign the permissions that are required to access monitoring data from the Management NSX Manager and Compute Manager in Region A in vRealize Operations Manager to the operations local service account svc-vrops-nsx.

Prerequisites

- Ensure that SSH has been enabled on the Management NSX Manager and Compute NSX Manager in Region A.
- On a Windows host that has access to you data center, install a REST client, such as the RESTClient add-on for Firefox.

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.

NSX Manager	Host name
NSX Manager for the management cluster	mgmt01nsxm01.sfo01.rainpole.local
NSX Manager for the shared compute and edge cluster	comp01nsxm01.sfo01.rainpole.local

b Log in using the following credentials.

Setting	Value
User name	admin
Password	■ *mngnsx_admin_password* ■ *compnsx_admin_password*

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	■ *mngnsx_admin_password* ■ *compnsx_admin_password*

The Authorization: Basic XXX header appears in the Headers pane.

e In the **Request** pane, enter the following header details and click Okay.

Request Header Attribute	Value
Name	Content-Type
Value	Application/xml

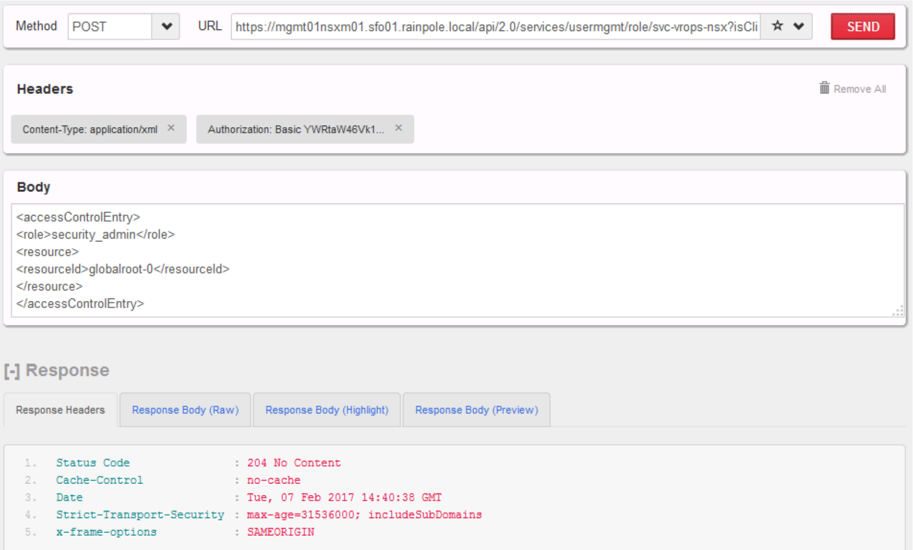
The Content-Type:application/xml header appears in the **Headers** pane.

f 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 management cluster	https://mgmt01nsxm01.sfo01.rainpole.local/api/2.0/services/usermgmt/role/svc-vrops-nsx?isCli=true
NSX Manager for the shared edge and compute cluster	https://comp01nsxm01.sfo01.rainpole.local/api/2.0/services/usermgmt/role/svc-vrops-nsx?isCli=true

g 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>
```



Method: POST

URL: https://mgmt01nsxm01.sfo01.rainpole.local/api/2.0/services/usermgmt/role/svc-vrops-nsx?isCli

Headers

Content-Type: application/xml

Authorization: Basic YWRtaW46Vk1...

Body

```
<accessControlEntry>
<role>security_admin</role>
<resource>
<resourceId>globalroot-0</resourceId>
</resource>
</accessControlEntry>
```

```
Status Code               : 204 No Content
Cache-Control             : no-cache
Date                      : Tue, 07 Feb 2017 14:40:38 GMT
Strict-Transport-Security : max-age=31536000; includeSubDomains
x-frame-options           : SAMEORIGIN
```

The Status changes to `204 No Content`.

h Repeat the step for the other NSX Manager.

Add NSX-vSphere Adapter Instances to vRealize Operations Manager for Region A

After you install the management pack, configure NSX-vSphere Adapters: one for the NSX Manager for the management cluster and one for the NSX Manager for the shared edge and compute cluster.

Procedure

1 Log in to vRealize Operations Manager by using the administration console.

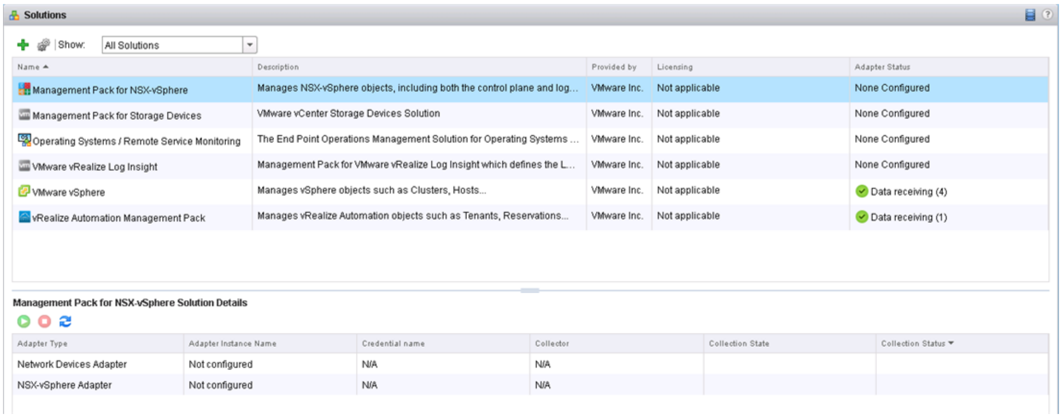
a Open a Web browser and go to **`https://vrops-cluster-01.rainpole.local`**.

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 **Management Pack for NSX-vSphere** from the solution table, and click **Configure**.



Solutions

Show: All Solutions

Name ▲	Description	Provided by	Licensing	Adapter Status
Management Pack for NSX-vSphere	Manages NSX-vSphere objects, including both the control plane and log...	VMware Inc.	Not applicable	None Configured
Management Pack for Storage Devices	VMware vCenter Storage Devices Solution	VMware Inc.	Not applicable	None Configured
Operating Systems / Remote Service Monitoring	The End Point Operations Management Solution for Operating Systems ...	VMware Inc.	Not applicable	None Configured
VMware vRealize Log Insight	Management Pack for VMware vRealize Log Insight which defines the L...	VMware Inc.	Not applicable	None Configured
VMware vSphere	Manages vSphere objects such as Clusters, Hosts...	VMware Inc.	Not applicable	✓ Data receiving (4)
vRealize Automation Management Pack	Manages vRealize Automation objects such as Tenants, Reservations...	VMware Inc.	Not applicable	✓ Data receiving (1)

Management Pack for NSX-vSphere Solution Details

Adapter Type	Adapter Instance Name	Credential name	Collector	Collection State	Collection Status ▼
Network Devices Adapter	Not configured	N/A	N/A		
NSX-vSphere Adapter	Not configured	N/A	N/A		

4 In the **Manage Solution - Management Pack for NSX-vSphere** dialog box, from the **Adapter Type** table at the top, select **NSX-vSphere Adapter**.

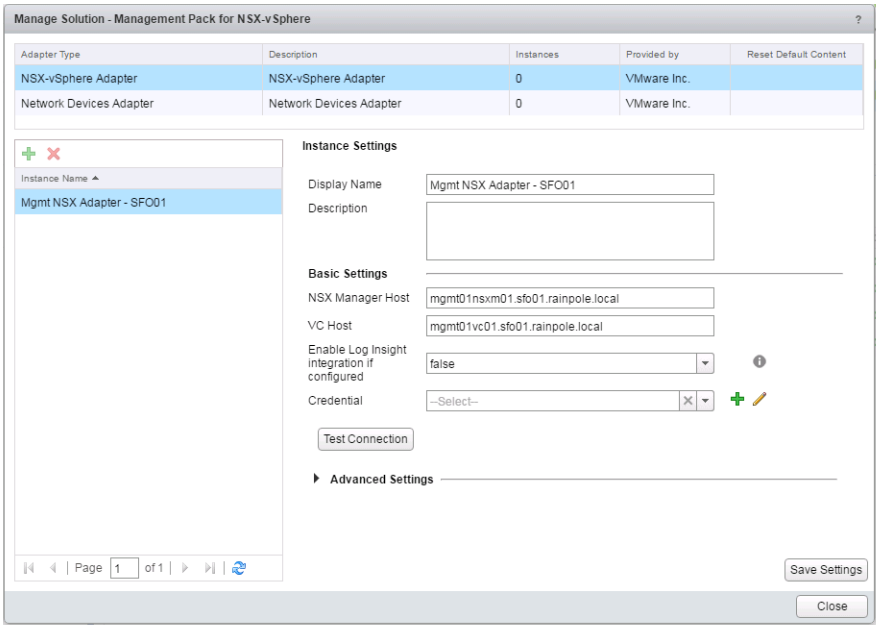
Empty settings for the NSX-vSphere Adapter appear under **Instance Settings** if vRealize Operations Manager does not have NSX-vSphere Adapters configured.

5 Under **Instance Settings**, enter the settings for connection to the NSX Manager for the management cluster or to the NSX Manager for the shared edge and compute cluster.

   a If you already have added another NSX-vSphere Adapter, click the **Add** icon to add an adapter settings.

   b Enter the name, the FQDN of NSX Manager and the FQDN of the vCenter Server instance that is connected to NSX Manager, and enable log forwarding of NSX-related data to vRealize Log Insight.

Setting	Value for the NSX Manager for the Management Cluster	Value for the NSX Manager for the Shared Edge and Compute Cluster
Display Name	Mgmt NSX Adapter - SFO01	Comp NSX Adapter - SFO01
Description	-	-
NSX Manager Host	mgmt01nsxm01.sfo01.rainpole.local	comp01nsxm01.sfo01.rainpole.local
VC Host	mgmt01vc01.sfo01.rainpole.local	comp01vc01.sfo01.rainpole.local
Enable Log Insight integration if configured	false	false



Manage Solution - Management Pack for NSX-vSphere

Adapter Type	Description	Instances	Provided by	Reset Default Content
NSX-vSphere Adapter	NSX-vSphere Adapter	0	VMware Inc.	
Network Devices Adapter	Network Devices Adapter	0	VMware Inc.	

Instance Name

Mgmt NSX Adapter - SFO01

Instance Settings

Display Name: Mgmt NSX Adapter - SFO01

Description:

Basic Settings

NSX Manager Host: mgmt01nsxm01.sfo01.rainpole.local

VC Host: mgmt01vc01.sfo01.rainpole.local

Enable Log Insight integration if configured: false

Credential: --Select--

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 Management Cluster	Value for the NSX Manager for the Shared Edge and Compute Cluster
Credential name	Credentials to Mgmt vCenter Server and NSX Manager	Credentials to Compute/Edge VC and NSX Manager
NSX User Name	svc-vrops-nsx	svc-vrops-nsx
NSX Manager Password	*svc-vrops-nsx_password*	*svc-vrops-nsx_password*
vCenter User Name	svc-vrops@rainpole.local	svc-vrops@rainpole.local
vCenter Password	*svc-vrops-password*	*svc-vrops-password*

d Expand the **Advanced Settings** pane, click the **Collectors/Groups** drop-down menu and select **SFO01**.

e Click **Test Connection** to validate the connection to the Management NSX Manager or Compute NSX Manager.

The NSX Manager certificate appears.

f Click **Save Settings**.

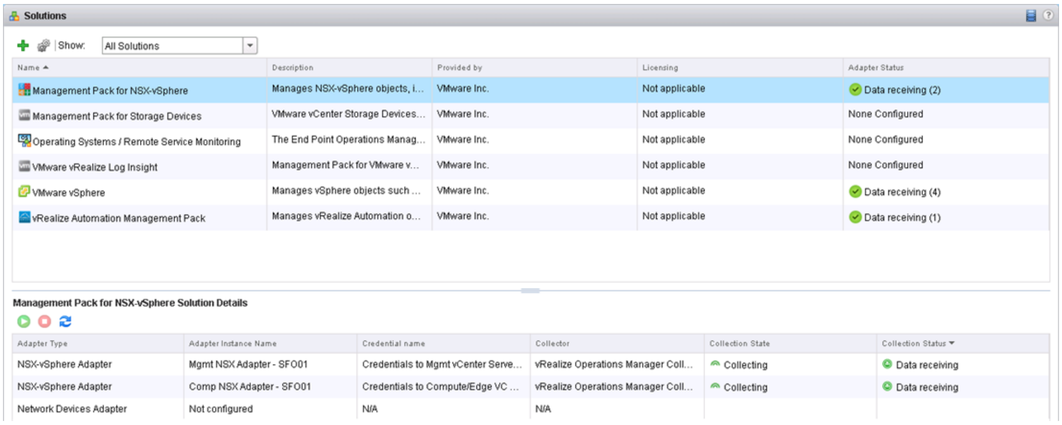
g In the **Review and Accept Certificate** dialog box, verify the certificate information and click **OK.**

h Click **OK** in the **Adapter Instance Info** box.

i Repeat these steps to create an NSX-vSphere Adapter for the NSX Manager for the shared edge and compute cluster.

6 In the **Manage Solution - Management Pack for NSX-vSphere** dialog box, click **Close**.

The two NSX-vSphere Adapters are 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, i...	VMware Inc.	Not applicable	Data receiving (2)
Management Pack for Storage Devices	VMware vCenter Storage Devices...	VMware Inc.	Not applicable	None Configured
Operating Systems / Remote Service Monitoring	The End Point Operations Manag...	VMware Inc.	Not applicable	None Configured
VMware vRealize Log Insight	Management Pack for VMware v...	VMware Inc.	Not applicable	None Configured
VMware vSphere	Manages vSphere objects such ...	VMware Inc.	Not applicable	Data receiving (4)
vRealize Automation Management Pack	Manages vRealize Automation o...	VMware Inc.	Not applicable	Data receiving (1)

Management Pack for NSX-vSphere Solution Details

Adapter Type	Adapter Instance Name	Credential name	Collector	Collection State	Collection Status
NSX-vSphere Adapter	Mgmt NSX Adapter - SFO01	Credentials to Mgmt vCenter Serve...	vRealize Operations Manager Coll...	Collecting	Data receiving
NSX-vSphere Adapter	Comp NSX Adapter - SFO01	Credentials to Compute/Edge VC ...	vRealize Operations Manager Coll...	Collecting	Data receiving
Network Devices Adapter	Not configured	N/A	N/A		

Add Network Devices Adapter to vRealize Operations Manager for Region A

Configure a Network Devices Adapter to monitor the switches and routers in your environment, and view related alerts, metrics and object capacity.

The Network Devices Adapter collects data across all vCenter Server instances that you monitor by using vRealize Operations Manager. In a multi-region environment, you use a single adapter instance to access data for all regions.

Prerequisites

- To monitor network devices, SNMP must be enabled in your network environment.
- For complete monitoring of your environment, Link Layer Discovery Protocol (LLDP) or Cisco Discovery Protocol (CDP) must also be enabled on each network device.

Procedure

1 Log in to vRealize Operations Manager by using the administration console.

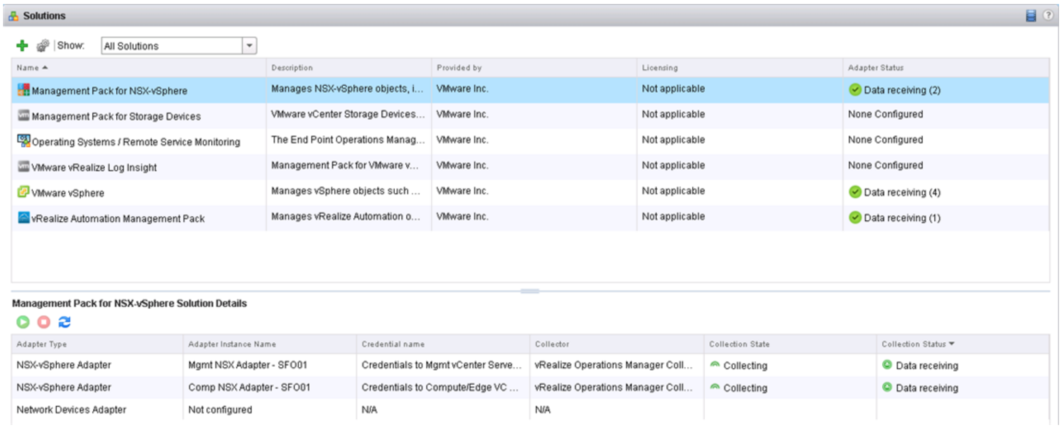
   a Open a Web browser and go to **`https://vrops-cluster-01.rainpole.local`**.

   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**.



Name	Description	Provided by	Licensing	Adapter Status
Management Pack for NSX-vSphere	Manages NSX-vSphere objects, i...	VMware Inc.	Not applicable	✓ Data receiving (2)
Management Pack for Storage Devices	VMware vCenter Storage Devices...	VMware Inc.	Not applicable	None Configured
Operating Systems / Remote Service Monitoring	The End Point Operations Manag...	VMware Inc.	Not applicable	None Configured
VMware vRealize Log Insight	Management Pack for VMware v...	VMware Inc.	Not applicable	None Configured
VMware vSphere	Manages vSphere objects such ...	VMware Inc.	Not applicable	✓ Data receiving (4)
vRealize Automation Management Pack	Manages vRealize Automation o...	VMware Inc.	Not applicable	✓ Data receiving (1)

Management Pack for NSX-vSphere Solution Details

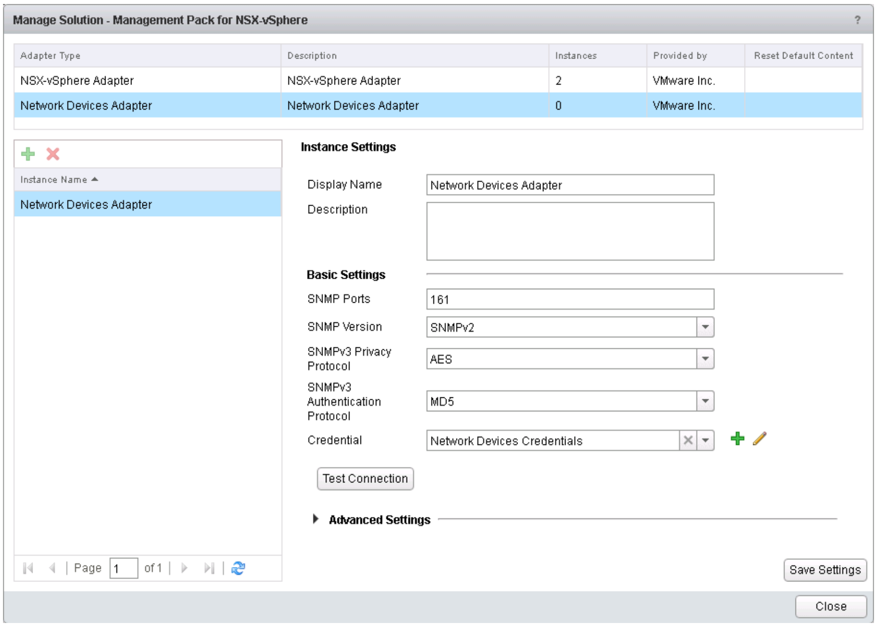
Adapter Type	Adapter Instance Name	Credential name	Collector	Collection State	Collection Status
NSX-vSphere Adapter	Mgmt NSX Adapter - SFO01	Credentials to Mgmt vCenter Serve...	vRealize Operations Manager Coll...	Collecting	Data receiving
NSX-vSphere Adapter	Comp NSX Adapter - SFO01	Credentials to Compute/Edge VC ...	vRealize Operations Manager Coll...	Collecting	Data receiving
Network Devices Adapter	Not configured	N/A	N/A		

4 In **Manage Solution - Management Pack for NSX-vSphere** dialog box, from the **Adapter Type** table at the top, select **Network Devices Adapter**.

5 Under **Instance Settings**, enter the settings for SNMP connection to the network devices for the management cluster.

a Enter the name, SNMP version and credentials.

Setting	Value
Display Name	Network Devices Adapter
Description	-
SNMP Ports	161
SNMP Version	SNMPv2
SNMPv3 Privacy Protocol	AES
SNMPv3 Authentication Protocol	MD5



Manage Solution - Management Pack for NSX-vSphere

Adapter Type	Description	Instances	Provided by	Reset Default Content
NSX-vSphere Adapter	NSX-vSphere Adapter	2	VMware Inc.	
Network Devices Adapter	Network Devices Adapter	0	VMware Inc.	

Instance Name

Network Devices Adapter

Instance Settings

Display Name: Network Devices Adapter

Description:

Basic Settings

SNMP Ports: 161

SNMP Version: SNMPv2

SNMPv3 Privacy Protocol: AES

SNMPv3 Authentication Protocol: MD5

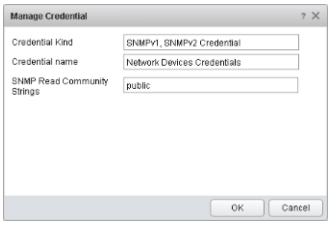
Credential: Network Devices Credentials

b Click the **Add** icon, and configure the credentials for connecting the Network Devices Adapter to the network devices, and click **OK**.

Credential	Value
Credential Kind	SNMPv1, SNMPv2 Credential
Credential Name	Network Devices Credentials
SNMP Read Community Strings	public

For SNMPv1 and SNMPv2 devices, enter a comma-separated list of community names (default is public).

For SNMPv3 devices, provide SNMPv3 credentials in addition to the settings for SNMPv1 and SNMPv2.



Manage Credential

Credential Kind	SNMPv1, SNMPv2 Credential
Credential name	Network Devices Credentials
SNMP Read Community Strings	public

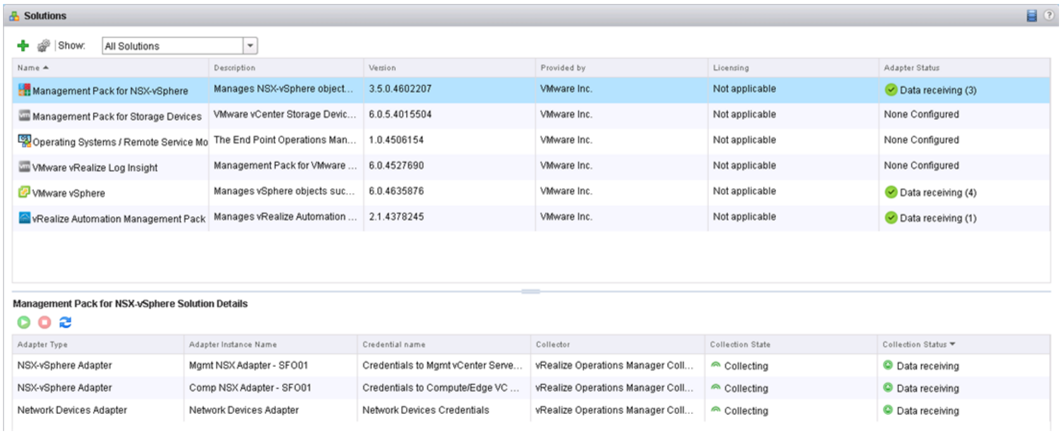
c Click **Test Connection** to verify the settings, and if the test is successful click the **OK** button.

d Expand the **Advanced Settings** section of settings, and verify that the **Collectors/Groups** option is set to **Default collector group**.

e Click **Save Settings** and click **OK** in the information box that appears.

6 In the **Manage Solution - Management Pack for NSX-vSphere** dialog box, click **Close**.

The Network Devices Adapter appears on the **Solutions** page of the vRealize Operations Manager user interface. The adapter is collecting data about the network devices in Region A of the SDDC.
The **Collection State** of the adapter is `Collecting` and the **Collection Status** is `Data receiving`.



Solutions

Show: All Solutions

Name	Description	Version	Provided by	Licensing	Adapter Status
Management Pack for NSX-vSphere	Manages NSX-vSphere object...	3.5.0.4602207	VMware Inc.	Not applicable	✓ Data receiving (3)
Management Pack for Storage Devices	VMware vCenter Storage Devic...	6.0.5.4015504	VMware Inc.	Not applicable	None Configured
Operating Systems / Remote Service Mo	The End Point Operations Man...	1.0.4506154	VMware Inc.	Not applicable	None Configured
VMware vRealize Log Insight	Management Pack for VMware ...	6.0.4527690	VMware Inc.	Not applicable	None Configured
VMware vSphere	Manages vSphere objects suc...	6.0.4635876	VMware Inc.	Not applicable	✓ Data receiving (4)
vRealize Automation Management Pack	Manages vRealize Automation ...	2.1.4378245	VMware Inc.	Not applicable	✓ Data receiving (1)

Management Pack for NSX-vSphere Solution Details

Adapter Type	Adapter Instance Name	Credential name	Collector	Collection State	Collection Status
NSX-vSphere Adapter	Mgmt NSX Adapter - SFO01	Credentials to Mgmt vCenter Serve...	vRealize Operations Manager Coll...	Collecting	Data receiving
NSX-vSphere Adapter	Comp NSX Adapter - SFO01	Credentials to Compute/Edge VC ...	vRealize Operations Manager Coll...	Collecting	Data receiving
Network Devices Adapter	Network Devices Adapter	Network Devices Credentials	vRealize Operations Manager Coll...	Collecting	Data receiving

Connect vRealize Operations Manager to vRealize Automation in Region A

Install and configure the vRealize Operations Manager Management Pack for vRealize Automation to monitor the health and capacity risk of your cloud infrastructure in the context of the tenant's business groups.

Prerequisites

- Download the `.pak` file for the vRealize Operations Manager Management Pack for vRealize Automation from *VMware Solutions Exchange*.
- Verify that vRealize Operations Manager is deployed and its analytics cluster is started.
- Verify that vRealize Automation is deployed.

Procedure

1. Configure Collection of Metrics from vRealize Automation in vRealize Operations Manager in Region A

   Connect vRealize Automation to vRealize Operations Manager for collecting statistics about the tenant workloads that are provisioned by using vRealize Automation.

2. Configure Integration of vRealize Operations Manager with vRealize Automation for Workload Reclamation in Region A

   Connect vRealize Automation with vRealize Operations Manager to collect metrics that vRealize Automation can use to identify tenant workloads for reclamation in Region A. Such workloads have low use of CPU, memory use, or disk space.

Configure Collection of Metrics from vRealize Automation in vRealize Operations Manager in Region A

Connect vRealize Automation to vRealize Operations Manager for collecting statistics about the tenant workloads that are provisioned by using vRealize Automation.

Procedure

1. Configure User Privileges on vRealize Automation for Integration with vRealize Operations Manager in Region A

   Assign the permissions that are required to access monitoring data from the vRealize Automation in vRealize Operations Manager to the svc-vrops-vra operations service account. The svc-vrops-vra user has rights that are specifically required for access to vRealize Automation in vRealize Operations Manager.

2. Install the vRealize Operations Manager Management Pack for vRealize Automation in Region A

   Install the `.pak` file for vRealize Operations Manager Management Pack for vRealize Automation to monitor the state of objects related about tenants, business groups, reservations groups, and blueprints.

3. Add vRealize Automation Adapter to vRealize Operations Manager for Region A

   After you install the management pack, configure a vRealize Automation adapter to collect monitoring data from vRealize Automation.

Configure User Privileges on vRealize Automation for Integration with vRealize Operations Manager in Region A

Assign the permissions that are required to access monitoring data from the vRealize Automation in vRealize Operations Manager to the svc-vrops-vra operations service account. The svc-vrops-vra user has rights that are specifically required for access to vRealize Automation in vRealize Operations Manager.

Procedure

1 Log in to the vRealize Automation portal.

   a Open a Web browser and go to `https://vra01svr01.rainpole.local/vcac`.

   b Log in using the following credentials.

Setting	Value
User name	administrator
Password	*vra_administrator_password*
Domain	vsphere.local

2 On the **Tenants** tab, click the **Rainpole** tenant.

3 Click the **Administrators** tab to assign tenant administrator and IaaS administrator roles to the svc-vrops-vra service account.

   a Enter `svc-vrops-vra` in the **Tenant administrators** search text box, click the **Search** icon, and click **svc-vrops-vra (svc-vrops-vra@rainpole.local)** that shows in the search result list to assign the role to the account.

   b Enter `svc-vrops-vra` in the **IaaS administrators** search text box, click **Search** icon, and click **svc-vrops-vra (svc-vrops-vra@rainpole.local)** that shows in the search result list to assign the role to the account.

   c Click **Finish**.

4 Log out of the vRealize Automation Default tenant portal.

5 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

6 Navigate to **Administration > Users & Groups > Directory Users and Groups** to assign the software architect role to the svc-vrops-vra service account.

   a Enter `svc-vrops-vra` in the search box, click the **Search** icon and click **svc-vrops-vra (svc-vrops-vra@rainpole.local)** user.

   b The setting of the svc-vrops-vra account appear.

   c On the **General** tab, select **Software Architect** under **Add roles to this User**, and click **Finish**.

7 Navigate to **Infrastructure > Endpoints > Fabric Groups** to assign the fabric administrator role to the svc-vrops-vra service account.

   a On the **Fabric Groups** page, click **SFO 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**.

Install the vRealize Operations Manager Management Pack for vRealize Automation in Region A

Install the `.pak` file for vRealize Operations Manager Management Pack for vRealize Automation to monitor the state of objects related about tenants, business groups, reservations groups, and blueprints.

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`.

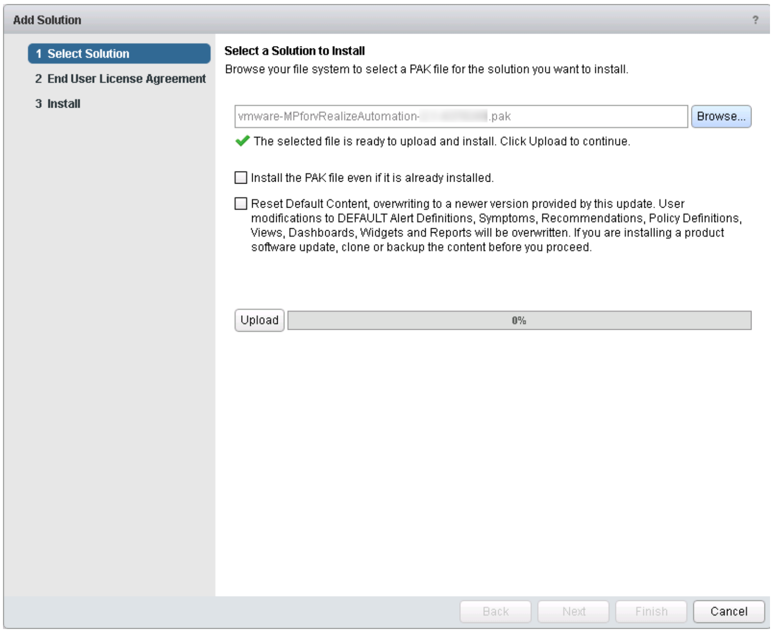
   b Log in using the following credentials.

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, click the **Add** icon.

4 On the **Select Solution** page of the **Add Solution** wizard, browse to the `.pak` file of the vRealize Operations Manager Management Pack for vRealize Automation, and click **Upload**.



Select a Solution to Install

Browse your file system to select a PAK file for the solution you want to install.

vmware-MPforvRealizeAutomation-[redacted].pak

✓ The selected file is ready to upload and install. Click Upload to continue.

□ Install the PAK file even if it is already installed.

□ Reset Default Content, overwriting to a newer version provided by this update. User modifications to DEFAULT Alert Definitions, Symptoms, Recommendations, Policy Definitions, Views, Dashboards, Widgets and Reports will be overwritten. If you are installing a product software update, clone or backup the content before you proceed.

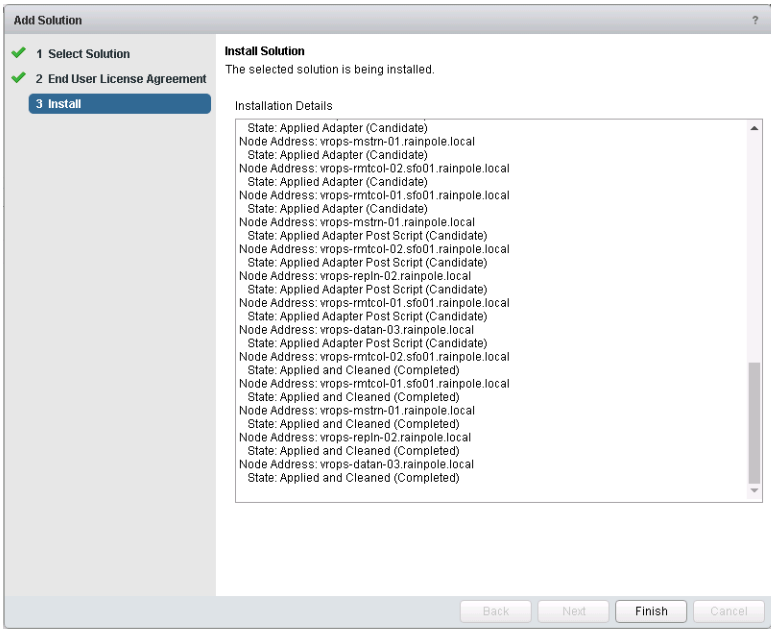
After the vRealize Automation management pack file has been uploaded, you see details about the management pack.

5 After the upload is complete, click **Next**.

6 On the **End User License Agreement** page, accept the license agreement and click **Next**.

The installation of the management pack starts. You see its progress on the **Install** page.

7 After the installation is complete, click **Finish** on the **Install** page.



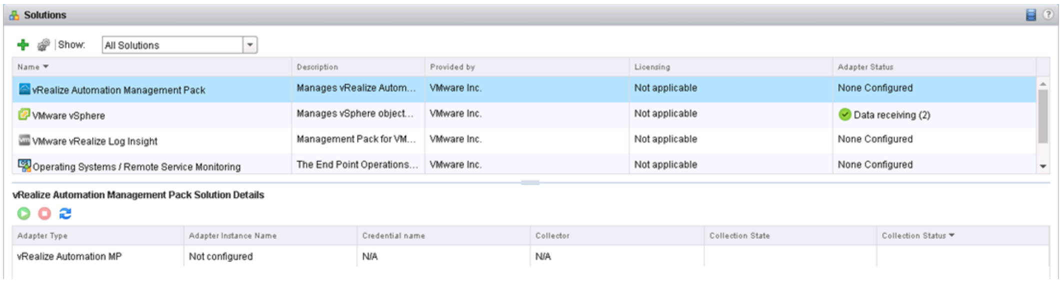
Install Solution

The selected solution is being installed.

Installation Details

```
  State: Applied Adapter (Candidate)
Node Address: vrops-mstrn-01.rainpole.local
  State: Applied Adapter (Candidate)
Node Address: vrops-rmtcol-02.sfo01.rainpole.local
  State: Applied Adapter (Candidate)
Node Address: vrops-rmtcol-01.sfo01.rainpole.local
  State: Applied Adapter (Candidate)
Node Address: vrops-mstrn-01.rainpole.local
  State: Applied Adapter Post Script (Candidate)
Node Address: vrops-rmtcol-02.sfo01.rainpole.local
  State: Applied Adapter Post Script (Candidate)
Node Address: vrops-repln-02.rainpole.local
  State: Applied Adapter Post Script (Candidate)
Node Address: vrops-rmtcol-01.sfo01.rainpole.local
  State: Applied Adapter Post Script (Candidate)
Node Address: vrops-datan-03.rainpole.local
  State: Applied Adapter Post Script (Candidate)
Node Address: vrops-rmtcol-02.sfo01.rainpole.local
  State: Applied and Cleaned (Completed)
Node Address: vrops-rmtcol-01.sfo01.rainpole.local
  State: Applied and Cleaned (Completed)
Node Address: vrops-mstrn-01.rainpole.local
  State: Applied and Cleaned (Completed)
Node Address: vrops-repln-02.rainpole.local
  State: Applied and Cleaned (Completed)
Node Address: vrops-datan-03.rainpole.local
  State: Applied and Cleaned (Completed)
```

The vRealize Automation Management Pack solution appears on the **Solutions** page of the vRealize Operations Manager user interface.



Solutions

Name	Description	Provided by	Licensing	Adapter Status
vRealize Automation Management Pack	Manages vRealize Autom...	VMware Inc.	Not applicable	None Configured
VMware vSphere	Manages vSphere object...	VMware Inc.	Not applicable	✓ Data receiving (2)
VMware vRealize Log Insight	Management Pack for VM...	VMware Inc.	Not applicable	None Configured
Operating Systems / Remote Service Monitoring	The End Point Operations...	VMware Inc.	Not applicable	None Configured

vRealize Automation Management Pack Solution Details

Adapter Type	Adapter Instance Name	Credential name	Collector	Collection State	Collection Status
vRealize Automation MP	Not configured	N/A	N/A		

Add vRealize Automation Adapter to vRealize Operations Manager for Region A

After you install the management pack, configure a vRealize Automation adapter to collect monitoring data from vRealize Automation.

Procedure

1 Log in to vRealize Operations Manager by using the administration console.

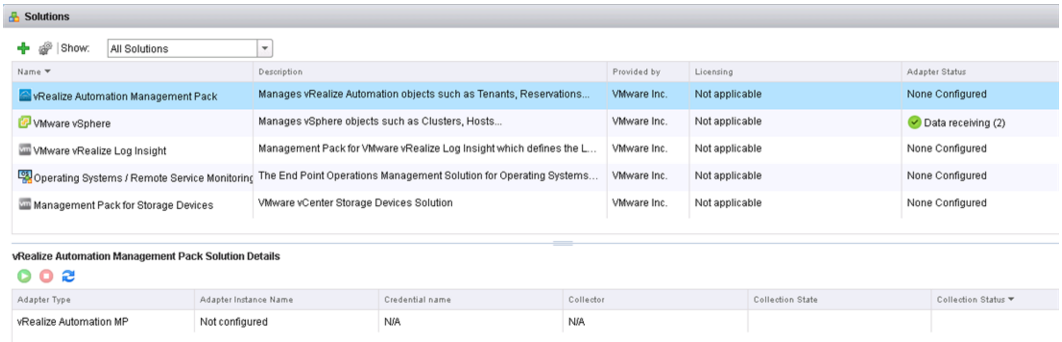
   a Open a Web browser and go to **`https://vrops-cluster-01.rainpole.local`**.

   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 **vRealize Automation Management Pack** and click **Configure**.



Solutions

Name	Description	Provided by	Licensing	Adapter Status
vRealize Automation Management Pack	Manages vRealize Automation objects such as Tenants, Reservations...	VMware Inc.	Not applicable	None Configured
VMware vSphere	Manages vSphere objects such as Clusters, Hosts...	VMware Inc.	Not applicable	✓ Data receiving (2)
VMware vRealize Log Insight	Management Pack for VMware vRealize Log Insight which defines the L...	VMware Inc.	Not applicable	None Configured
Operating Systems / Remote Service Monitoring	The End Point Operations Management Solution for Operating Systems...	VMware Inc.	Not applicable	None Configured
Management Pack for Storage Devices	VMware vCenter Storage Devices Solution	VMware Inc.	Not applicable	None Configured

vRealize Automation Management Pack Solution Details

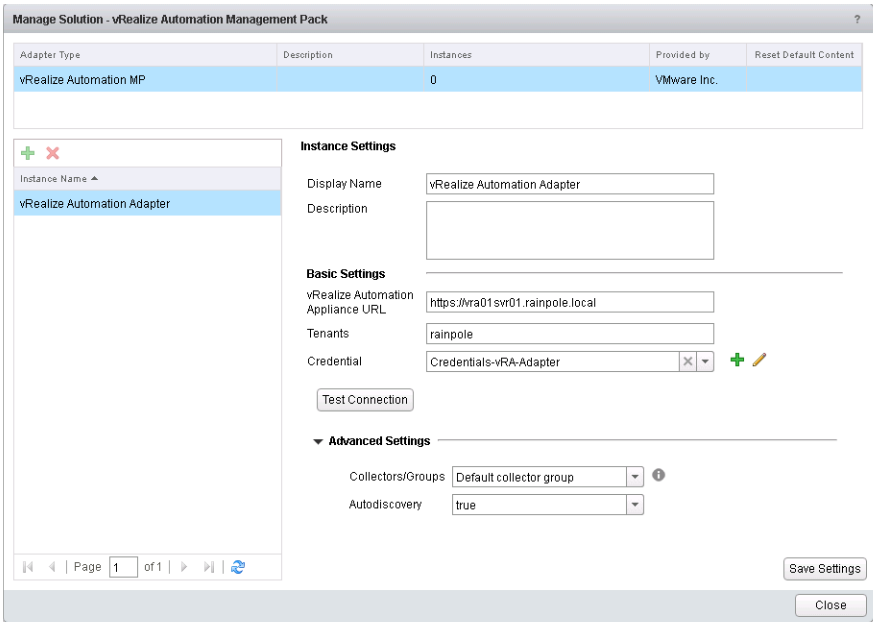
Adapter Type	Adapter Instance Name	Credential name	Collector	Collection State	Collection Status
vRealize Automation MP	Not configured	N/A	N/A		

4 In the **Manage Solution - vRealize Automation Management Pack** dialog box, from the **Adapter Type** table at the top, select **vRealize Automation MP**.

5 Under **Instance Settings**, enter the settings for connection to vRealize Automation.

a Enter the name and the FQDN of vRealize Automation front-end portal, and turn data collection on for the Rainpole tenant.

Setting	Value
Name	vRealize Automation Adapter
Description	-
vRealize Automation Appliance URL	https://vra01svr01.rainpole.local
Tenants	rainpole



Manage Solution - vRealize Automation Management Pack

Adapter Type	Description	Instances	Provided by	Reset Default Content
vRealize Automation MP		0	VMware Inc.	

Instance Name
vRealize Automation Adapter

Instance Settings

Display Name: vRealize Automation Adapter
Description:

Basic Settings
vRealize Automation Appliance URL: https://vra01svr01.rainpole.local
Tenants: rainpole
Credential: Credentials-vRA-Adapter

Advanced Settings
Collectors/Groups: Default collector group
Autodiscovery: true

b Click the **Add** icon, configure the credentials for connection to vRealize Automation, and click **OK**.

Credential	Value
Credential name	Credentials-vRA-Adapter
SysAdmin Username	administrator@vsphere.local
SysAdmin Password	*vra_administrator_password*
SuperUser Username	svc-vrops-vra@rainpole.local
SuperUser Password	*svc_vrops_vra_password*

c Click **Test Connection** to validate the connection to vRealize Automation.

d In the **Review and Accept Certificate** dialog box, verify the vRealize Automation certificate information and click **OK**.

e Click **OK** in the **Test Connection Info** dialog box.

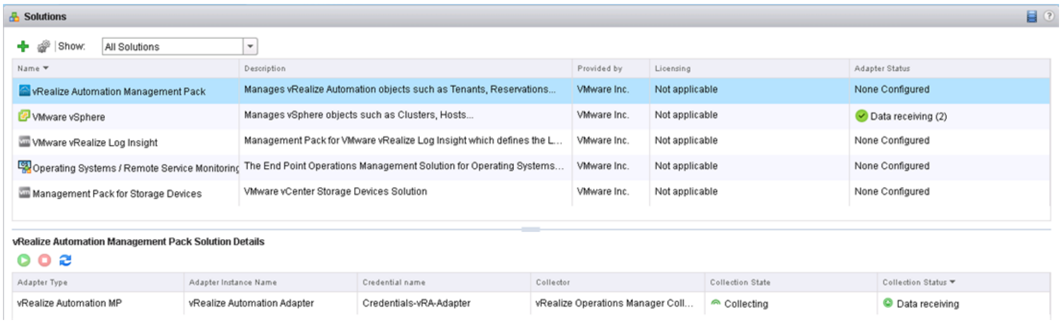
f Expand the **Advanced Settings** section of settings, and verify the following configuraton.

Advanced Setting	Value
Collectors/Groups	Default Collector Group
Autodiscovery	True

g Click **Save Settings** and click **OK** in the information box that appears.

6 In the **Manage Solution - vRealize Automation Management Pack** dialog box, click **Close**.

The **vRealize Automation MP** adapter appears on the Solutions page of the vRealize Operations Manager user interface. The **Collection State** of the adapter is `Collecting` and the **Collection Status** is `Data receiving`.



Name	Description	Provided by	Licensing	Adapter Status
vRealize Automation Management Pack	Manages vRealize Automation objects such as Tenants, Reservations...	VMware Inc.	Not applicable	None Configured
VMware vSphere	Manages vSphere objects such as Clusters, Hosts...	VMware Inc.	Not applicable	✓ Data receiving (2)
VMware vRealize Log Insight	Management Pack for VMware vRealize Log Insight which defines the L...	VMware Inc.	Not applicable	None Configured
Operating Systems / Remote Service Monitoring	The End Point Operations Management Solution for Operating Systems...	VMware Inc.	Not applicable	None Configured
Management Pack for Storage Devices	VMware vCenter Storage Devices Solution	VMware Inc.	Not applicable	None Configured

vRealize Automation Management Pack Solution Details

Adapter Type	Adapter Instance Name	Credential name	Collector	Collection State	Collection Status
vRealize Automation MP	vRealize Automation Adapter	Credentials-vRA-Adapter	vRealize Operations Manager Coll...	Collecting	Data receiving

Configure Integration of vRealize Operations Manager with vRealize Automation for Workload Reclamation in Region A

Connect vRealize Automation with vRealize Operations Manager to collect metrics that vRealize Automation can use to identify tenant workloads for reclamation in Region A. Such workloads have low use of CPU, memory use, or disk space.

Procedure

1 Configure User Privileges on vRealize Operations Manager for Tenant Workload Reclamation in Region A

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 Region A.

2 Add vRealize Operations Manager as a Metrics Provider in vRealize Automation

Integrate vRealize Automation with vRealize Operations Manager to pull metrics for reclamation of tenant workloads.

Configure User Privileges on vRealize Operations Manager for Tenant Workload Reclamation in Region A

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 Region A.

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 **Access Control**.

3 On the **Access Control** page, click the **User Accounts** tab and click the **Import Users** icon.

4 On the **Import Users** page, import the svc-vra-vrops@rainpole.local service account.

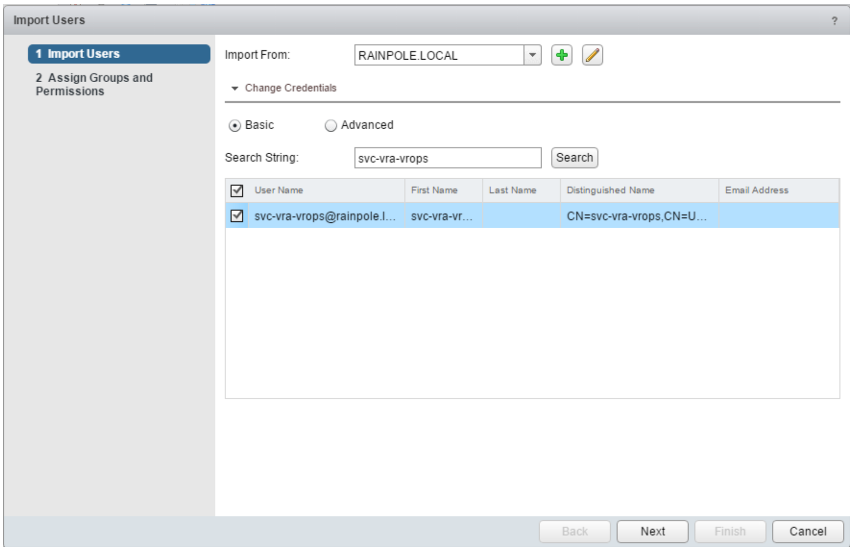
   a From the **Import From** drop-down menu, select **RAINPOLE.LOCAL**.

   b Select the **Basic** option for the seach query.

   c In the **Search String** text box, enter **`svc-vra-vrops`** and click **Search**.

   The search results contain the svc-vra-vrops user account.

   d Select **svc-vra-vrops@rainpole.local** and click **Next**.



Import From: RAINPOLE.LOCAL

● Basic ○ Advanced

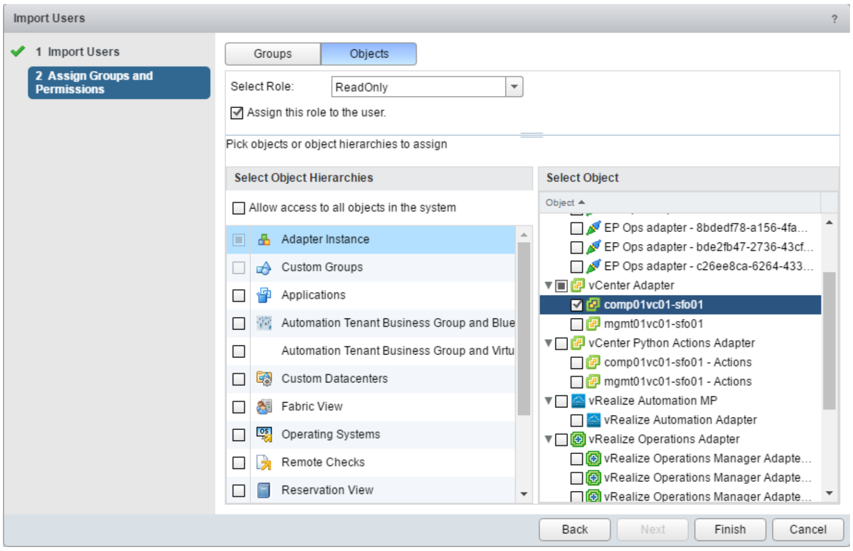
Search String: svc-vra-vrops

☑ User Name	First Name	Last Name	Distinguished Name	Email Address
☑ svc-vra-vrops@rainpole.l...	svc-vra-vr...		CN=svc-vra-vrops,CN=U...	

5 On the **Assign Groups and Permissions** page, to assign the `ReadOnly` role to the svc-vra-vrops@rainpole.local service account, click the **Objects** tab, configure the following settings and click **Finish**.

Setting	Value
Select Role	ReadOnly
Assign this role to the user	Selected

Setting	Value
Select Object	**vCenter Adapter > comp01vc01-sfo01**
Select Object Hierarchies	Adapter Instance This option is automatically selected after you select the adapter instance.



Import Users

✓ 1 Import Users

2 Assign Groups and Permissions

Select Role: ReadOnly

☑ Assign this role to the user.

Pick objects or object hierarchies to assign

?
Groups
Objects
Select Object Hierarchies
□ Allow access to all objects in the system
▣ Adapter Instance
□ Custom Groups
□ Applications
□ Automation Tenant Business Group and Blue
□ Automation Tenant Business Group and Virtu
□ Custom Datacenters
□ Fabric View
□ Operating Systems
□ Remote Checks
□ Reservation View
Select Object
Object
□ EP Ops adapter - 8bdedf78-a156-4fa...
□ EP Ops adapter - bde2fb47-2736-43cf...
□ EP Ops adapter - c26ee8ca-6264-433...
▣ vCenter Adapter
☑ comp01vc01-sfo01
□ mgmt01vc01-sfo01
□ vCenter Python Actions Adapter
□ comp01vc01-sfo01 - Actions
□ mgmt01vc01-sfo01 - Actions
□ vRealize Automation MP
□ vRealize Automation Adapter
□ vRealize Operations Adapter
□ vRealize Operations Manager Adapte...
□ vRealize Operations Manager Adapte...
□ vRealize Operations Manager Adapte...
Back
Next
Finish
Cancel

Add vRealize Operations Manager as a Metrics Provider in vRealize Automation

Integrate vRealize Automation with vRealize Operations Manager to pull metrics for reclamation of tenant workloads.

Procedure

1 Log in to the vRealize Automation Rainpole portal.

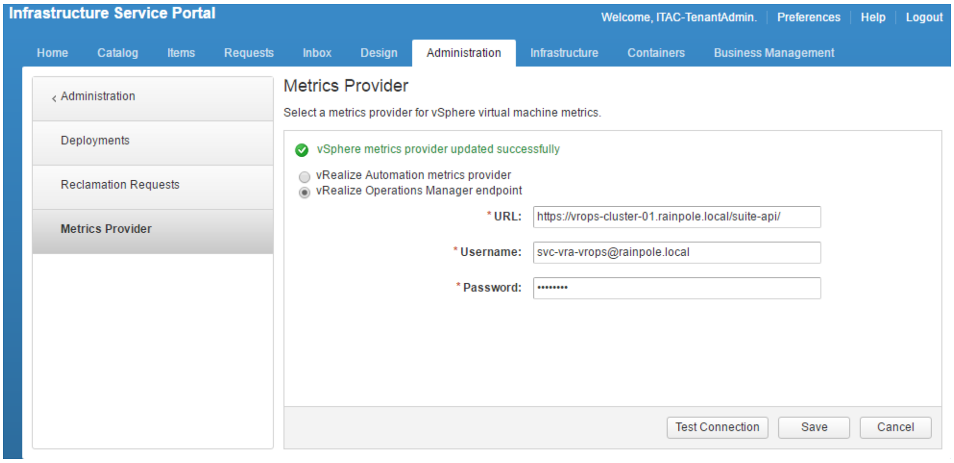
   a Open a Web browser and go to `https://vra01svr01.rainpole.local/vcac/org/rainpole`.

   b Log in using the following credentials.

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

2 Navigate to **Administration > Reclamation > Metrics Provider**.

3 On the **Metrics Provider** page, configure the vRealize Operations Manager settings.



Metrics Provider

Select a metrics provider for vSphere virtual machine metrics.

✓ vSphere metrics provider updated successfully

○ vRealize Automation metrics provider
● vRealize Operations Manager endpoint

* URL:	https://vrops-cluster-01.rainpole.local/suite-api/
* Username:	svc-vra-vrops@rainpole.local
* Password:	••••••••

a Select **vRealize Operations Manager endpoint**.

b Configure the following settings for vRealize Operations Manager.

Setting	Value
URL	https://vrops-cluster-01.rainpole.local/suite-api/
Username	svc-vra-vrops@rainpole.local
Password	*svc-vra-vrops_password*

c Click **Test Connection**, verify that the test connection is successful, and click **Save**.

d In the certificate warning message box, click **OK**.

The `vSphere metrics provider updated successfully` message appears.

Enable Storage Device Monitoring in vRealize Operations Manager in Region A

Install and configure the vRealize Operations Management Pack for Storage Devices to view the storage topology, and to monitor the capacity and problems on storage components.

Prerequisites

- Download the `.pak` file for the vRealize Operations Manager Management Pack for Storage Devices from *VMware Solutions Exchange*.
- Verify that vRealize Operations Manager is deployed and its analytics cluster is started.
- Verify that the remote collector nodes for Region A are deployed and grouped.

Procedure

1 Install the vRealize Operations Manager Management Pack for Storage Devices in Region A

Install the `.pak` file of the management pack for storage devices to add the management pack as a solution to vRealize Operations Manager.

2 Add Storage Devices Adapters in vRealize Operations Manager for Region A

After you install the management pack, configure Storage Devices adapter to collect monitoring data about the storage devices in the SDDC.

Install the vRealize Operations Manager Management Pack for Storage Devices in Region A

Install the `.pak` file of the management pack for storage devices to add the management pack as a solution to vRealize Operations Manager.

Prerequisites

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`**.

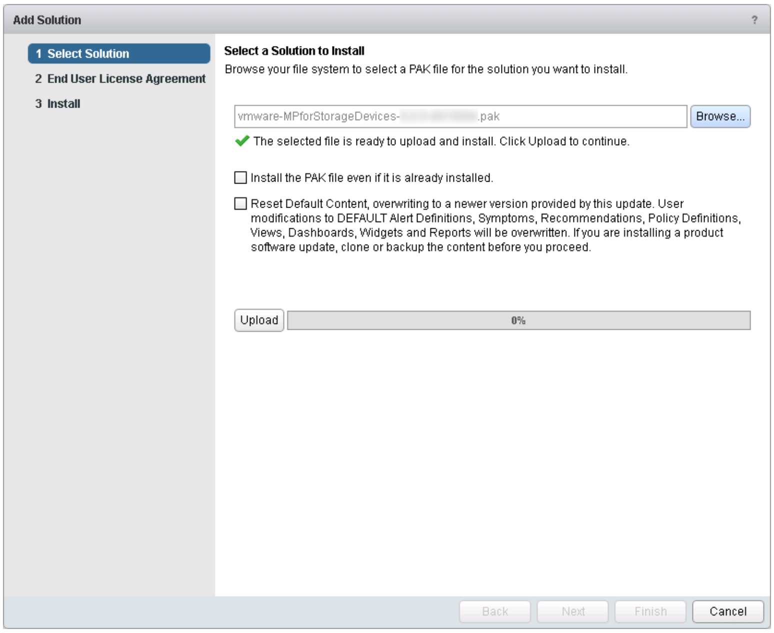
   b Log in using the following credentials.

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, click the **Add** icon.

4 On the **Select Solution** page from the **Add Solution** wizard, browse to the `.pak` file of the vRealize Operations Manager Management Pack for Storage Devices and click **Upload**.



Add Solution

1 Select Solution
2 End User License Agreement
3 Install

Select a Solution to Install

Browse your file system to select a PAK file for the solution you want to install.

vmware-MPforStorageDevices-[redacted].pak Browse...

✓ The selected file is ready to upload and install. Click Upload to continue.

□ Install the PAK file even if it is already installed.

□ Reset Default Content, overwriting to a newer version provided by this update. User modifications to DEFAULT Alert Definitions, Symptoms, Recommendations, Policy Definitions, Views, Dashboards, Widgets and Reports will be overwritten. If you are installing a product software update, clone or backup the content before you proceed.

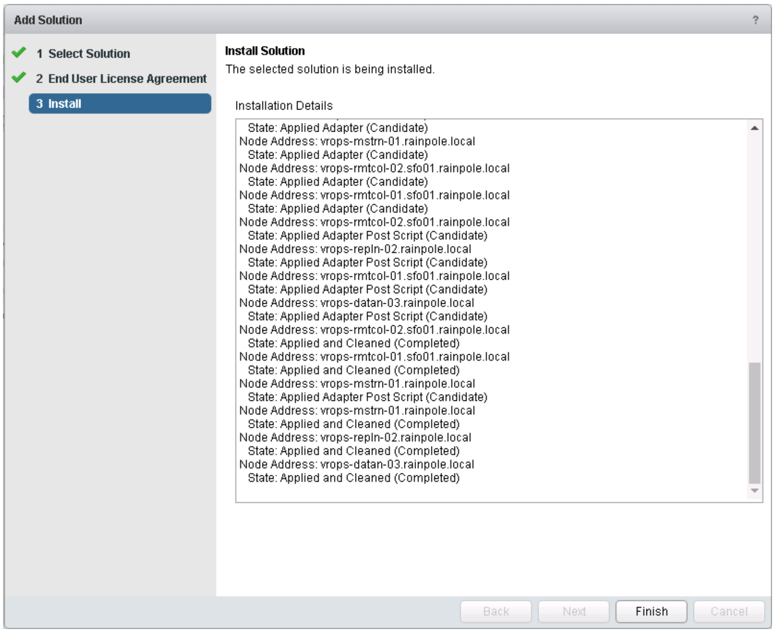
Upload 0%

5 After the upload is complete, click **Next**.

6 On the **End User License Agreement** page, accept the license agreement and click **Next**.

The installation of the management pack starts. You see its progress on the **Install** page.

7 After the installation is complete, click **Finish** on the **Install** page.



Add Solution

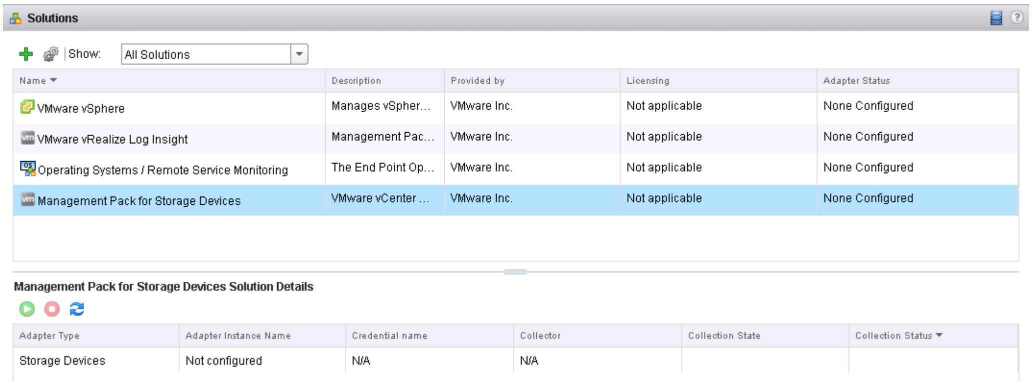
Install Solution

The selected solution is being installed.

Installation Details

```
  State: Applied Adapter (Candidate)
Node Address: vrops-mstrn-01.rainpole.local
  State: Applied Adapter (Candidate)
Node Address: vrops-rmtcol-02.sfo01.rainpole.local
  State: Applied Adapter (Candidate)
Node Address: vrops-rmtcol-01.sfo01.rainpole.local
  State: Applied Adapter (Candidate)
Node Address: vrops-rmtcol-02.sfo01.rainpole.local
  State: Applied Adapter Post Script (Candidate)
Node Address: vrops-repln-02.rainpole.local
  State: Applied Adapter Post Script (Candidate)
Node Address: vrops-rmtcol-01.sfo01.rainpole.local
  State: Applied Adapter Post Script (Candidate)
Node Address: vrops-datan-03.rainpole.local
  State: Applied Adapter Post Script (Candidate)
Node Address: vrops-rmtcol-02.sfo01.rainpole.local
  State: Applied and Cleaned (Completed)
Node Address: vrops-rmtcol-01.sfo01.rainpole.local
  State: Applied and Cleaned (Completed)
Node Address: vrops-mstrn-01.rainpole.local
  State: Applied Adapter Post Script (Candidate)
Node Address: vrops-mstrn-01.rainpole.local
  State: Applied and Cleaned (Completed)
Node Address: vrops-repln-02.rainpole.local
  State: Applied and Cleaned (Completed)
Node Address: vrops-datan-03.rainpole.local
  State: Applied and Cleaned (Completed)
```

The Management Pack for Storage Devices solution appears on the **Solutions** page of the vRealize Operations Manager user interface.



Solutions

Show: All Solutions

Name	Description	Provided by	Licensing	Adapter Status
VMware vSphere	Manages vSpher…	VMware Inc.	Not applicable	None Configured
VMware vRealize Log Insight	Management Pac…	VMware Inc.	Not applicable	None Configured
Operating Systems / Remote Service Monitoring	The End Point Op…	VMware Inc.	Not applicable	None Configured
Management Pack for Storage Devices	VMware vCenter …	VMware Inc.	Not applicable	None Configured

Management Pack for Storage Devices Solution Details

Adapter Type	Adapter Instance Name	Credential name	Collector	Collection State	Collection Status
Storage Devices	Not configured	N/A	N/A		

Add Storage Devices Adapters in vRealize Operations Manager for Region A

After you install the management pack, configure Storage Devices adapter to collect monitoring data about the storage devices in the SDDC.

Procedure

1 Log in to vRealize Operations Manager by using the administration console.

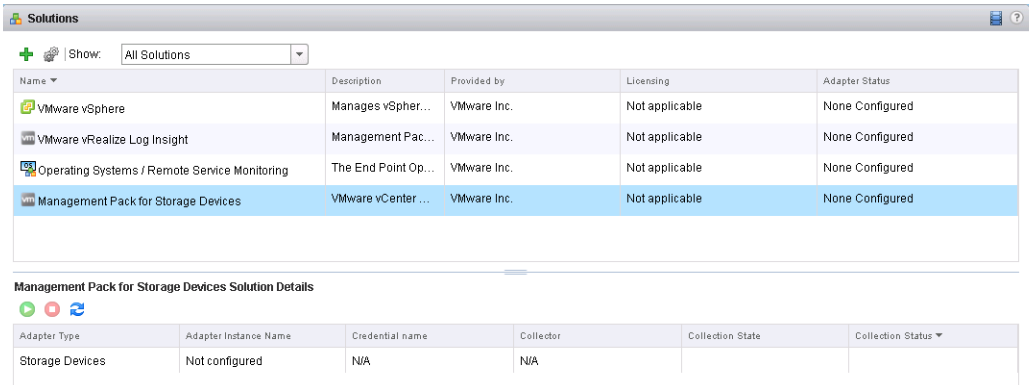
   a Open a Web browser and go to **`https://vrops-cluster-01.rainpole.local`**.

   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 the solution table and click **Configure**.



Solutions

Show: All Solutions

Name	Description	Provided by	Licensing	Adapter Status
VMware vSphere	Manages vSpher...	VMware Inc.	Not applicable	None Configured
VMware vRealize Log Insight	Management Pac...	VMware Inc.	Not applicable	None Configured
Operating Systems / Remote Service Monitoring	The End Point Op...	VMware Inc.	Not applicable	None Configured
Management Pack for Storage Devices	VMware vCenter ...	VMware Inc.	Not applicable	None Configured

Management Pack for Storage Devices Solution Details

Adapter Type	Adapter Instance Name	Credential name	Collector	Collection State	Collection Status
Storage Devices	Not configured	N/A	N/A		

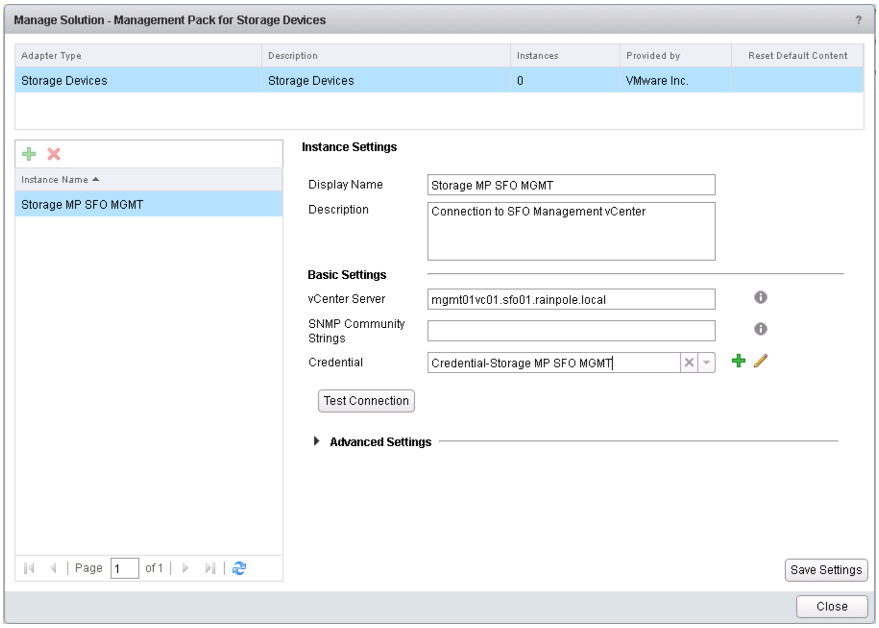
4 In the **Manage Solution - Management Pack for Storage Devices** dialog box, from the **Adapter Type** table at the top, select **Storage Devices**.

5 Under **Instance Settings**, enter the settings for connection to the Management vCenter Server or to the Compute vCenter Server.

a If you already have added another Storage Devices adapter, click the **Add** icon to add an adapter settings.

b Enter the name, description, and FQDN of the vCenter Server instance.

Setting	Value for the Management Cluster	Value for the Shared Edge and Compute Cluster
Name	Storage MP SFO MGMT	Storage MP SFO Compute
Description	Connection to SFO Management vCenter	Connection to SFO Compute vCenter
vCenter Server	mgmt01vc01.sfo01.rainpole.local	comp01vc01.sfo01.rainpole.local
SNMP Community Strings	-	-



Manage Solution - Management Pack for Storage Devices

Adapter Type	Description	Instances	Provided by	Reset Default Content
Storage Devices	Storage Devices	0	VMware Inc.	

Instance Name
Storage MP SFO MGMT

Instance Settings

Display Name	Storage MP SFO MGMT
Description	Connection to SFO Management vCenter

Basic Settings

vCenter Server	mgmt01vc01.sfo01.rainpole.local
SNMP Community Strings	
Credential	Credential-Storage MP SFO MGMT

c Click the **Add** icon, and configure the credentials for connection to the Management and Compute vCenter Server, and click **OK**.

Setting	Value for the Management Cluster	Value for the Shared Edge and Compute Cluster
Credential name	Credential-Storage MP SFO MGMT	Credential-Storage MP SFO Compute
User Name	svc-mpsd-vrops@rainpole.local	svc-mpsd-vrops@rainpole.local
Password	*svc-mpsd-vrops-password*	*svc-mpsd-vrops-password*

d Click **Test Connection** to validate the connection to the Management vCenter Server or the Compute vCenter Server.

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 Info** dialog box.
- g Expand the **Advanced Settings** section of settings, and from the **Collectors/Groups** drop-down menu, select the **SFO01** remote collector group.
- h Click **Save Settings** and click **OK** in the information box that appears.
- i Repeat the steps for the other vCenter Server instance.

6 In the **Manage Solution - Management Pack for Storage Devices** dialog box, click **Close**.

The Storage Devices adapters 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`.

Configure E-Mail Alerts in vRealize Operations Manager

You configure e-mail notifications in vRealize Operations Manager so that users and applications receive the administrative alerts from vRealize Operations Manager about certain situations in the data center.

Prerequisites

Verify that you have access to an SMTP 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*

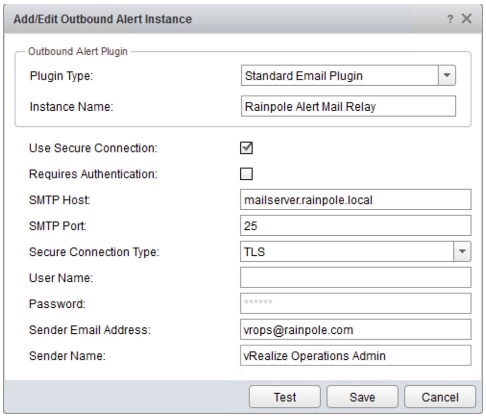
2 In the left pane of vRealize Operations Manager, click **Administration** and click **Outbound Settings**.

3 On the **Outbound Settings** page, click the **Add** icon to create an outbound alert instance.

4 In the **Add/Edit Outbound Alert Instance** dialog box, configure the settings for the Standard Email Plug-in, and click **OK**.

Alert Instance Setting	Value
Plugin Type	Standard Email Plugin
Instance Name	Rainpole Alert Mail Relay
Use Secure Connection	Selected
SMTP Host	*FQDN of the mail server*
SMTP Port	*Server port for SMTP requests* The SMTP service application usually listens on TCP port 25 for incoming requests.
Secure Connection Type	TLS

Alert Instance Setting	Value
Sender Email Address	vrops@rainpole.com
Sender Name	vRealize Operations Admin



Plugin Type: Standard Email Plugin
Instance Name: Rainpole Alert Mail Relay
Use Secure Connection: ☑
Requires Authentication: □
SMTP Host: mailserver.rainpole.local
SMTP Port: 25
Secure Connection Type: TLS
User Name:
Password: ******
Sender Email Address: vrops@rainpole.com
Sender Name: vRealize Operations Admin

5 Click **Test** to verify the connection with the SMTP server.

6 After the verification completes, click **Save**.

Region A vRealize Log Insight Implementation

Deploy vRealize Log Insight in a cluster configuration of three nodes with an integrated load balancer: one master and two worker nodes.

Procedure

1 Deploy vRealize Log Insight in Region A

Start the deployment of vRealize Log Insight in Region A by deploying the master and worker nodes and forming the vRealize Log Insight cluster.

2 Replace the Certificate of vRealize Log Insight in Region A

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.

3 Connect vRealize Log Insight to the vSphere Environment in Region A

Start collecting log information about the ESXi and vCenter Server instances in the SDDC.

4 Connect vRealize Log Insight to vRealize Operations Manager in Region A

Connect vRealize Log Insight to vRealize Operations Manager so that you can use the Launch in Context functionality between the two application, allowing for you to troubleshoot vRealize Operations Manager by using dashboards and alerts in the vRealize Log Insight user interface.

5 Connect vRealize Log Insight to the NSX Instances in Region A

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. 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 Region A

Connect the vRealize Log to vRealize Automation to receive log information from all components of vRealize Automation in the vRealize Log Insight UI.

7 Install the vRealize Log Insight Content Pack for vSAN in Region A

Install the content pack for VMware vSAN to add the dashboards for viewing log information in vRealize Log Insight.

8 Configure Log Retention and Archiving in Region A

Set log retention to one week and archive logs for 90 days according to the *VMware Validated Design Architecture and Design* documentation.

Deploy vRealize Log Insight in Region A

Start the deployment of vRealize Log Insight in Region A by deploying the master and worker nodes and forming the vRealize Log Insight cluster.

Procedure

1 Prerequisites for Deploying vRealize Log Insight in Region A

Before you deploy vRealize Log Insight, 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 Region A

Use the vSphere Web Client to deploy each vRealize Log Insight node as a virtual appliance on the management cluster in Region A.

3 Configure a DRS Anti-Affinity Rule for vRealize Log Insight in Region A

To protect the vRealize Log Insight cluster from a host-level failure, configure vSphere DRS to run the worker virtual appliances on different hosts in the management cluster.

4 Start the vRealize Log Insight Instance in Region A

Configure and start the vRealize Log Insight master node. Before you form a cluster by adding the worker nodes, vRealize Log Insight must be running.

5 Join the Worker Nodes to vRealize Log Insight in Region A

After you deploy the virtual appliances for vRealize Log Insight and start the vRealize Log Insight instance on the master node, join the two worker nodes to form a cluster.

6 Enable the Integrated Load Balancer of vRealize Log Insight in Region A

After you join the master and the worker nodes to create a vRealize Log Insight cluster, 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 Region A

To use user roles in vRealize Log Insight that are maintained centrally and are inline with the other solutions in the SDDC, enable Active Directory support.

Prerequisites for Deploying vRealize Log Insight in Region A

Before you deploy vRealize Log Insight, 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 Log Insight are available in the application virtual network for Region A.

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 Region A must be routable via the vSphere management network.

Table 4-3. IP Addresses and Host Names for the vRealize Log Insight Instance in Region A

Role	IP Address	FQDN
Integrated load balancer VIP address	192.168.31.10	vrli-cluster-01.sfo01.rainpole.local
Master node	192.168.31.11	vrli-mstr-01.sfo01.rainpole.local
Worker node 1	192.168.31.12	vrli-wrkr-01.sfo01.rainpole.local
Worker node 2	192.168.31.13	vrli-wrkr-02.sfo01.rainpole.local
Default gateway	192.168.31.1	-
DNS server	■ 172.16.11.5 ■ 172.16.11.4	-
Subnet mask	255.255.255.0	-
NTP servers	■ 172.16.11.251 ■ 172.16.11.252 ■ 172.17.11.251 ■ 172.17.11.252	■ ntp.sfo01.rainpole.local ■ ntp.lax01.rainpole.local

Deployment Prerequisites

Verify that your environment satisfies the following prerequisites to deploying vRealize Log Insight.

Prerequisite	Value
Storage	■ Virtual disk provisioning. ■ Thin ■ Required storage per node ■ Initial storage for node deployment: 510 GB
Software Features	■ vSphere ■ Management vCenter Server ■ Client Integration Plugin on the machine where you use the vSphere Web Client ■ Management cluster with DRS and HA enabled. ■ NSX for vSphere Application virtual network for the 3-node vRealize Log Insight cluster

Prerequisite	Value
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 Region A

Use the vSphere Web Client to deploy each vRealize Log Insight node as a virtual appliance on the management cluster in Region A.

You deploy three vRealize Log Insight nodes - one master node and two worker nodes.

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 Navigate to the mgmt01vc01.sfo01.rainpole.local vCenter Server object.

3 Right-click **mgmt01vc01.sfo01.rainpole.local** and select **Deploy OVF Template**.

4 On the **Select source** page, select **Local file**, click **Browse**, 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	Value
vrli-mstr-01	Master node
vrli-wrkr-01	Worker node 1
vrli-wrkr-02	Worker node 2

b Select the inventory folder for the virtual appliance.

Setting	Value
vCenter Server	mgmt01vc01.sfo01.rainpole.local
Data center	SFO01
Folder	vRLI01

6 On the **Select a resource** page, select the **SFO01-Mgmt01** management cluster as the resource to run the virtual appliance on, and click **Next**.

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 **Medium** deployment configuration, and click **Next**.

10 On the **Select storage** page, select the datastore.

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 **SFO01A-VSAN01-MGMT01** datastore and click **Next**.

11 On the **Setup networks** page, select the distributed port group on the `vDS-Mgmt` distributed switch that ends with `Mgmt-RegionA01-VXLAN`, and click **Next**.

12 On the **Customize template** page, set 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	▪ vrli-mstr-01.sfo01.rainpole.local for the master node ▪ vrli-wrkr-01.sfo01.rainpole.local for the worker node 1 ▪ vrli-wrkr-02.sfo01.rainpole.local for the worker node 2
Default gateway	192.168.31.1
DNS	172.16.11.5,172.16.11.4
DNS searchpath	sfo01.rainpole.local,rainpole.local
DNS domain	sfo01.rainpole.local
Static IPv4 address	▪ 192.168.31.11 for the master node ▪ 192.168.31.12 for the worker node 1 ▪ 192.168.31.13 for the worker node 2
Subnet mask	255.255.255.0

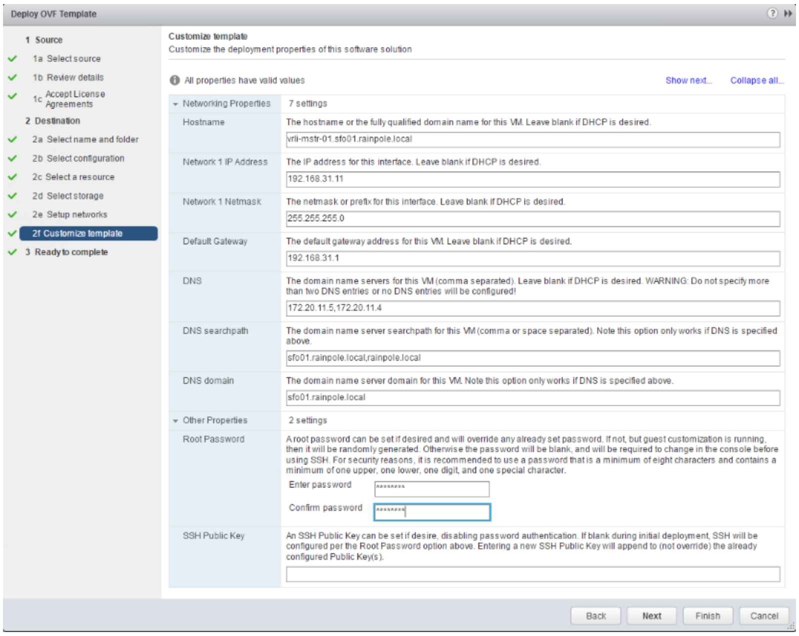
b In the **Other Properties** section, enter and confirm a password for the root user.

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 when you log in to the console of the vRealize Log Insight virtual appliance.

c Click **Next**.



Customize template

Customize the deployment properties of this software solution

All properties have valid values

Networking Properties — 7 settings

Hostname	The hostname or the fully qualified domain name for this VM. Leave blank if DHCP is desired. vrli-mstr-01.sfo01.rainpole.local
Network 1 IP Address	The IP address for this interface. Leave blank if DHCP is desired. 192.168.31.11
Network 1 Netmask	The netmask or prefix for this interface. Leave blank if DHCP is desired. 255.255.255.0
Default Gateway	The default gateway address for this VM. Leave blank if DHCP is desired. 192.168.31.1
DNS	The domain name servers for this VM (comma separated). Leave blank if DHCP is desired. WARNING: Do not specify more than two DNS entries or no DNS entries will be configured! 172.20.11.5,172.20.11.4
DNS searchpath	The domain name server searchpath for this VM (comma or space separated). Note this option only works if DNS is specified above. sfo01.rainpole.local,rainpole.local
DNS domain	The domain name server domain for this VM. Note this option only works if DNS is specified above. sfo01.rainpole.local

Other Properties — 2 settings

Root Password	A root password can be set if desired and will override any already set password. If not, but guest customization is running, then it will be randomly generated. Otherwise the password will be blank, and will be required to change in the console before using SSH. For security reasons, it is recommended to use a password that is a minimum of eight characters and contains a minimum of one upper, one lower, one digit, and one special character. Enter password ******** Confirm password ********
SSH Public Key	An SSH Public Key can be set if desire, disabling password authentication. If blank during initial deployment, SSH will be configured per the Root Password option above. Entering a new SSH Public Key will append to (not override) the already configured Public Key(s).

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 **Power > Power On**.

15 Repeat the procedure to deploy the vRealize Log Insight virtual appliance for the next node in the cluster.

Configure a DRS Anti-Affinity Rule for vRealize Log Insight in Region A

To protect the vRealize Log Insight cluster from a host-level failure, configure vSphere DRS to run the worker virtual appliances on different hosts in the management cluster.

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 Navigate to the mgmt01vc01.sfo01.rainpole.local vCenter Server object, and under the SFO01 data center object select the **SFO01-Mgmt01** cluster.

3 On the **Configure** tab, select **VM/Host Rules**.

4 In the **VM/Host Rules** list, click **Add** above the rules list and add a new anti-affinity rule called `vrli-antiaffinity-rule` for the vrli-mstr-01, vrli-wrkr-01, and vrli-wrkr-02 virtual machines, and click **OK**.

Rule Attribute	Value
Name	anti-affinity-rule-vrli
Enable rule	Yes
Type	Separate Virtual Machines
Members	■ vrli-mstr-01 ■ vrli-wrkr-01 ■ vrli-wrkr-02

Start the vRealize Log Insight Instance in Region A

Configure and start the vRealize Log Insight master node. Before you form a cluster by adding the worker nodes, vRealize Log Insight must be running.

Procedure

1 Open a Web browser and go to **`http://vrli-mstr-01.sfo01.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 be at least 8 characters long, and must 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	*email_address_to_receive_system_notifications*
Send HTTP Post System Notifications To	https://vrli-cluster-01.sfo01.rainpole.local

7 On the **Time Configuration** page, enter the following settings, click **Test** and then click **Save and Continue**.

Setting	Value
Sync Server Time With	NTP Server (recommended)
NTP Servers	ntp.sfo01.rainpole.local, ntp.lax01.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, type 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 Region A

After you deploy the virtual appliances for vRealize Log Insight and start the vRealize Log Insight instance on the master node, 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://vrli-wrkr-01.sfo01.rainpole.local
Worker node 2	https://vrli-wrkr-02.sfo01.rainpole.local

The initial configuration wizard opens.

2 Click **Next** 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 `vrli-mstr-01.sfo01.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 Region A

After you join the master and the worker nodes to create a vRealize Log Insight cluster, 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://vrli-mstr-01.sfo01.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 **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	192.168.31.10
FQDN	vrli-cluster-01.sfo01.rainpole.local

Join vRealize Log Insight to the Active Directory in Region A

To use user roles in vRealize Log Insight that are maintained centrally and are inline with the other solutions in the SDDC, enable Active Directory support.

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 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
User Name	svc-loginsight
Password	*svc_loginsight_password*
Connection Type	Standard
Require SSL	Yes or No according to the instructions from the IT administrator

  b Click **Test Connection** to verify the connection, and click **Save**.

Replace the Certificate of vRealize Log Insight in Region A

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.

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 **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 PEM file on your computer, and click **Save**.

Certificate Generation Option	Certificate File
Using the CertGenVVD tool	vrli.sfo01.2.chain.pem

The certificate is uploaded to vRealize Log Insight.

5 Import the certificate into the Java Keystore on each vRealize Log Insight node.

a Open an SSH session and go each of the vRealize Log Insight nodes.

Name	Role
vrli-mstr-01.sfo01.rainpole.local	Master node
vrli-wrkr-01.sfo01.rainpole.local	Worker node 1
vrli-wrkr-02.sfo01.rainpole.local	Worker node 2

b Log in using the following credentials.

Setting0	Value
User name	root
Password	*vrli_root_password*

c Convert the on-disk **`vrli.sfo01.2.chain.pem`** file into a **`vrli.sfo01.2.chain.crt`** file.

```
openssl x509 -in /root/vrli.sfo01.2.chain.pem -inform PEM -out /root/vrli.sfo01.2.chain.crt
```

d Import the vrli.sfo01.2.chain.crt into the Java Keystore:

```
cd /usr/java/default/lib/security/

../../bin/keytool -import -alias loginsight -file /root/vrli.sfo01.2.chain.crt -keystore
cacerts
```

e When prompted for a keystore password, type **`changeit`**.

f When prompted to accept the certificate, type **`yes`**.

g Repeat this operation on all vRealize Log Insight nodes until complete.

6 Open a Web browser and go to **`https://vrli-cluster-01.sfo01.rainpole.local`**

A warning message that the connection is not trusted appears.

7 To review the certificate, click the padlock 🔒 in the address bar of the browser, and verify that **Subject Alternative Name** contains the names of the vRealize Log Insight cluster nodes.

8 Import the certificate in your Web browser.

For example, in Google Chrome under the HTTPS/TLS settings click **Manage certificates**, and in the **Certificates** dialog box import `vrli-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 Region A

Start collecting log information about the ESXi and vCenter Server instances in the SDDC.

Procedure

1 Configure User Privileges in vSphere for Integration with vRealize Log Insight for Region A

Assign global permissions in Region A to the operations service account svc-loginsight in order to collect log information from the vCenter Server instances and ESXi hosts with vRealize Log Insight. The svc-loginsight user account is specifically dedicated to collecting log information from vCenter Server and ESXi.

2 Connect vRealize Log Insight to vSphere in Region A

After you configure the svc-loginsight Active Directory user with the vSphere privileges that are required for retrieving log information from the vCenter Server instances and ESXi hosts, connect vRealize Log Insight to vSphere.

3 Configure vCenter Server to Forward Log Events to vRealize Log Insight in Region A

You can configure each vCenter Server and Platform Services Controller 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 Region A

Assign global permissions in Region A to the operations service account svc-loginsight in order to collect log information from the vCenter Server instances and ESXi hosts with vRealize Log Insight. The svc-loginsight user account is specifically dedicated to collecting log information from vCenter Server and ESXi.

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 From the **Home** menu, select **Administration**.

3 Under **Access Control**, click **Roles**.

4 Create a role for vRealize Log Insight.

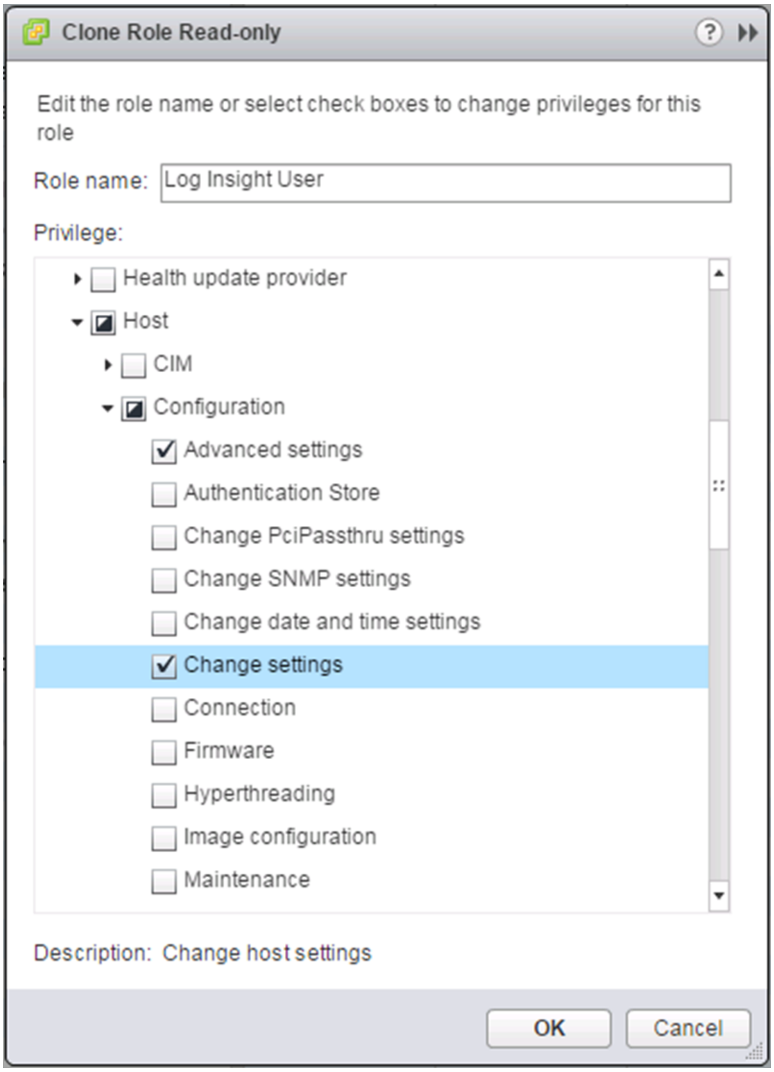
   a Select **Read-only** and click the **Clone** icon.

      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	■ **Host.Configuration.Advanced settings** ■ **Host.Configuration.Change settings** ■ **Host.Configuration.Network configuration** ■ **Host.Configuration.Security profile and firewall** The following privileges are inherited from the Read-only role. ■ **System.Anonymous** ■ **System.View** ■ **System.Read**

      These host privileges allow vRealize Log Insight to configure the syslog service on the ESXi hosts.



Clone Role Read-only

Edit the role name or select check boxes to change privileges for this role

Role name: Log Insight User

Privilege:

- □ Health update provider
- ▣ Host
  - □ CIM
  - ▣ Configuration
    - ☑ Advanced settings
    - □ Authentication Store
    - □ Change PciPassthru settings
    - □ Change SNMP settings
    - □ Change date and time settings
    - ☑ Change settings
    - □ Connection
    - □ Firmware
    - □ Hyperthreading
    - □ Image configuration
    - □ Maintenance

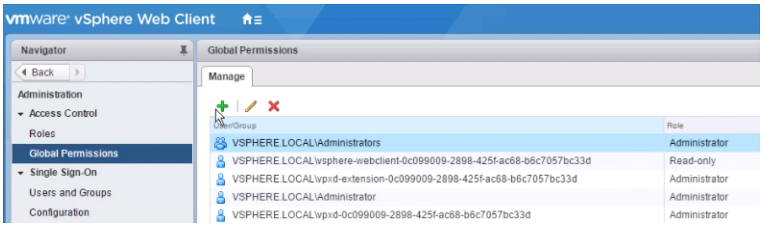
Description: Change host settings

The Log Insight User role is propagated to other linked vCenter Server instances.

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**.

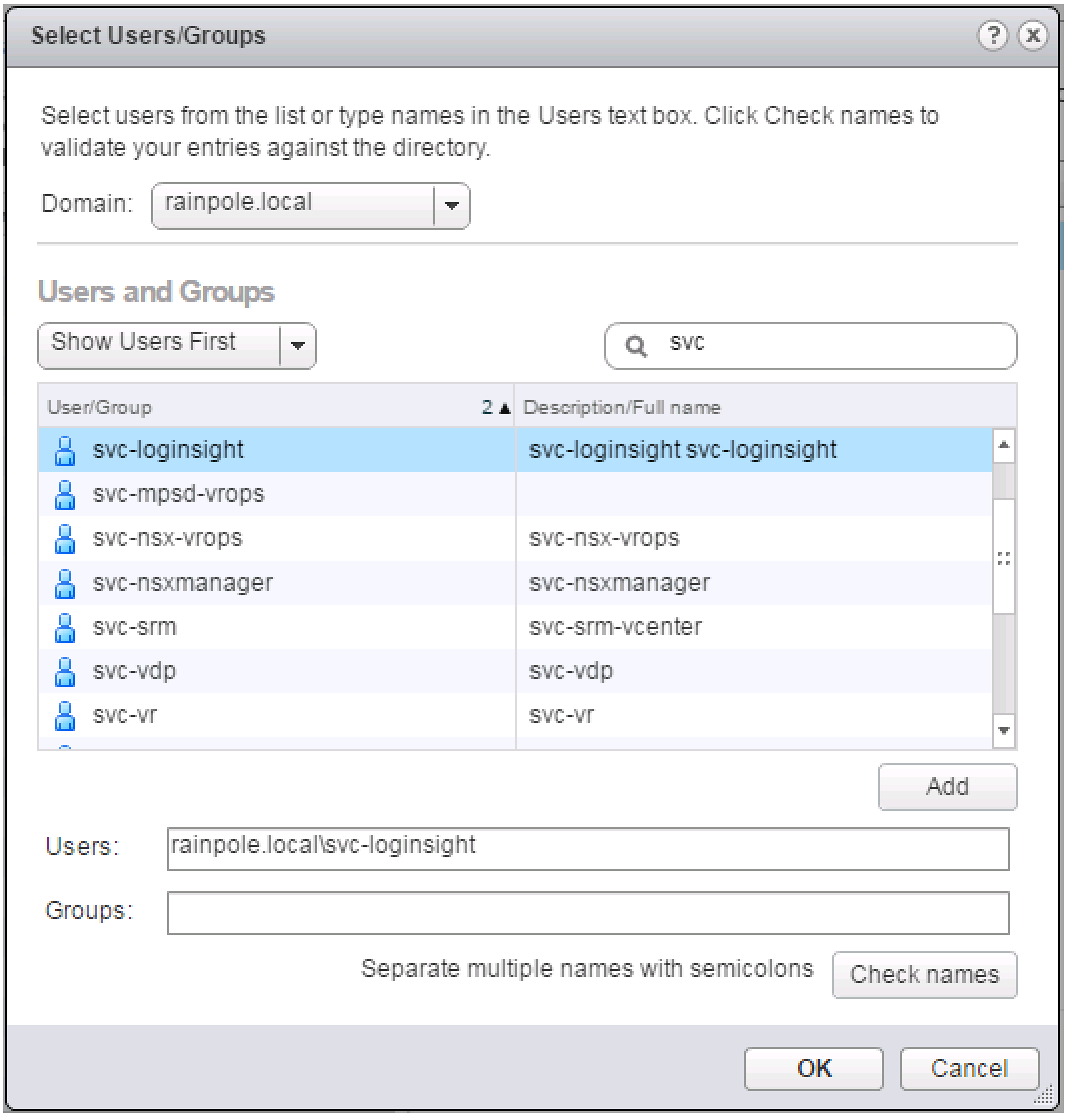


User/Group	Role
VSPHERE.LOCAL\Administrators	Administrator
VSPHERE.LOCAL\vsphere-webclient-0c099009-2898-425f-ac68-b6c7057bc33d	Read-only
VSPHERE.LOCAL\vpxd-extension-0c099009-2898-425f-ac68-b6c7057bc33d	Administrator
VSPHERE.LOCAL\Administrator	Administrator
VSPHERE.LOCAL\vpxd-0c099009-2898-425f-ac68-b6c7057bc33d	Administrator

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**.



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

svc

User/Group	Description/Full name
svc-loginsight	svc-loginsight svc-loginsight
svc-mpsd-vrops	
svc-nsx-vrops	svc-nsx-vrops
svc-nsxmanager	svc-nsxmanager
svc-srm	svc-srm-vcenter
svc-vdp	svc-vdp
svc-vr	svc-vr

Users: rainpole.local\svc-loginsight

Groups:

Separate multiple names with semicolons

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 all vCenter Server instances.

Connect vRealize Log Insight to vSphere in Region A

After you configure the svc-loginsight Active Directory user with the vSphere privileges that are required for retrieving log information from the vCenter Server instances and ESXi hosts, 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://vrli-cluster-01.sfo01.rainpole.local`**.

  b Log in using the following credentials.

Setting	Value
User name	admin
Password	*vrli_admin_password*

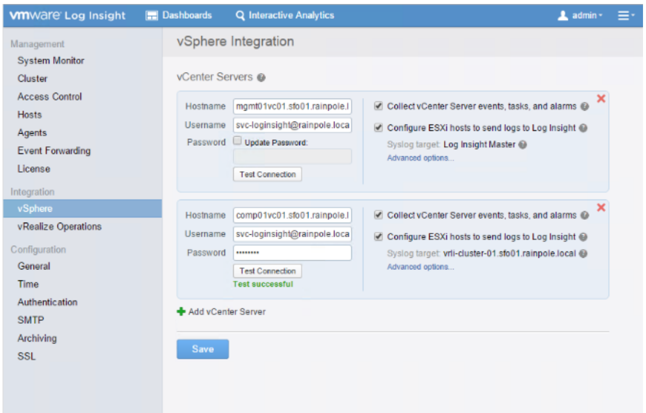
2 Click the configuration drop-down menu icon ☰ and select **Administration**.

3 Under **Integration**, click **vSphere**.

4 In the **vCenter Servers** pane, enter the connection settings for the Management vCenter Server and for the Compute 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	■ mgmt01vc01.sfo01.rainpole.local ■ comp01vc01.sfo01.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



vSphere Integration

vCenter Servers

Hostname mgmt01vc01.sfo01.rainpole.l
Username svc-loginsight@rainpole.loca
Password □ Update Password:
☑ Collect vCenter Server events, tasks, and alarms
☑ Configure ESXi hosts to send logs to Log Insight
Syslog target: Log Insight Master

Hostname comp01vc01.sfo01.rainpole.l
Username svc-loginsight@rainpole.loca
Password ••••••••
Test successful
☑ Collect vCenter Server events, tasks, and alarms
☑ Configure ESXi hosts to send logs to Log Insight
Syslog target: vrli-cluster-01.sfo01.rainpole.local

  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.

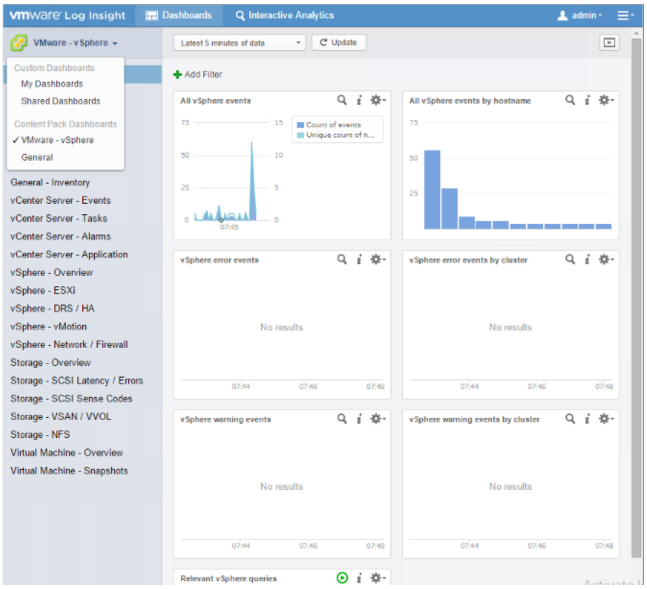
  c Click **Add vCenter Server** to add a new settings form and repeat the steps to add the settings for the second vCenter Server instance in Region A.

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 instances.

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 Region A

You can configure each vCenter Server and Platform Services Controller 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.

In Region A, you configure the following vCenter Server and Platform Services Controller instances:

Appliance Type	Appliance Management Interface URL
vCenter Server instances	■ https://mgmt01vc01.sfo01.rainpole.local:5480 ■ https://comp01vc01.sfo01.rainpole.local:5480
Platform Services Controller instances	■ https://mgmt01psc01.sfo01.rainpole.local:5480 ■ https://comp01psc01.sfo01.rainpole.local:5480

Procedure

1 Redirect the log events from the appliance to vRealize Log Insight.

a Open a Web browser and go to **`https://mgmt01vc01.sfo01.rainpole.local:5480`**.

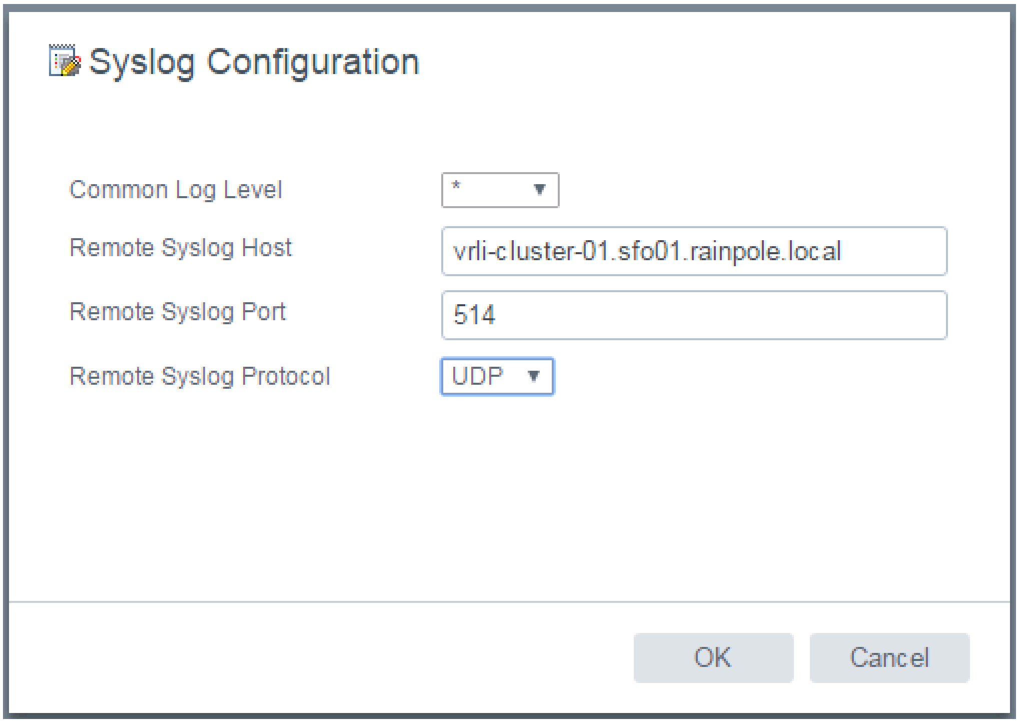
b Log in using the following credentials.

Setting	Value
User name	root
Password	*mgmtvc_root_password*

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	vrli-cluster-01.sfo01.rainpole.local
Remote Syslog Port	514
Remote Syslog Protocol	UDP



Syslog Configuration

Common Log Level: *

Remote Syslog Host: vrli-cluster-01.sfo01.rainpole.local

Remote Syslog Port: 514

Remote Syslog Protocol: UDP

e Repeat the steps for the other vCenter Server Appliance and Platform Services Controller Appliances.

2 Verify that the appliances are forwarding their syslog traffic to vRealize Log Insight.

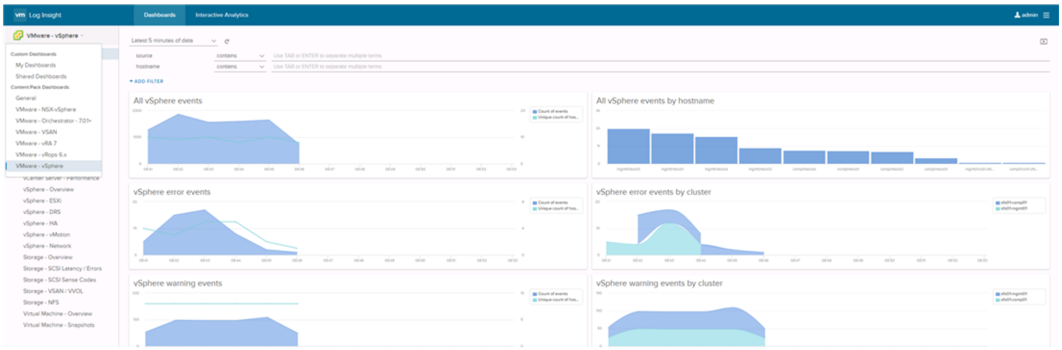
   a Open a Web browser and go to **`https://vrli-cluster-01.sfo01.rainpole.local`**.

   b Log in using the following credentials.

Setting	Value
User name	admin
Password	*vrli_admin_password*

   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 presented on the **All vSphere events by hostname** widget of the **General Overview** dashboard.



Connect vRealize Log Insight to vRealize Operations Manager in Region A

Connect vRealize Log Insight to vRealize Operations Manager so that you can use the Launch in Context functionality between the two application, allowing for you to troubleshoot vRealize Operations Manager by using dashboards and alerts in the vRealize Log Insight user interface.

Procedure

1 Configure User Privileges on vRealize Operations Manager for Integration with vRealize Log Insight in Region A

   Configure read-only privileges for the svc-vrli-vrops@rainpole.local service account on vRealize Operations Manager.

2 Enable the vRealize Log Insight Integration with vRealize Operations Manager for Region A

   Connect vRealize Log Insight in Region A with vRealize Operations Manager to launch vRealize Log Insight from within vRealize Operations Manager and to send alerts to vRealize Operations Manager.

3 Install the vRealize Log Insight Content Pack for vRealize Operations Manager in Region A

   Install the content pack for vRealize Operations Manager to add the dashboards for viewing log information in vRealize Log Insight.

4 Configure the Log Insight Agent on vRealize Operations Manager to Forward Log Events to vRealize Log Insight in Region A

After you install the content pack for vRealize Operations Manager, configure the Log Insight agent on vRealize Operations Manager to send audit logs and system events to vRealize Log Insight in Region A.

Configure User Privileges on vRealize Operations Manager for Integration with vRealize Log Insight in Region A

Configure read-only privileges for the svc-vrli-vrops@rainpole.local service account on vRealize Operations Manager.

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 **Access Control**.

3 On the **Access Control** page, click the **User Accounts** tab and click the **Import Users** icon.

4 On the **Import Users** page, import the svc-vrli-vrops@rainpole.local service account.

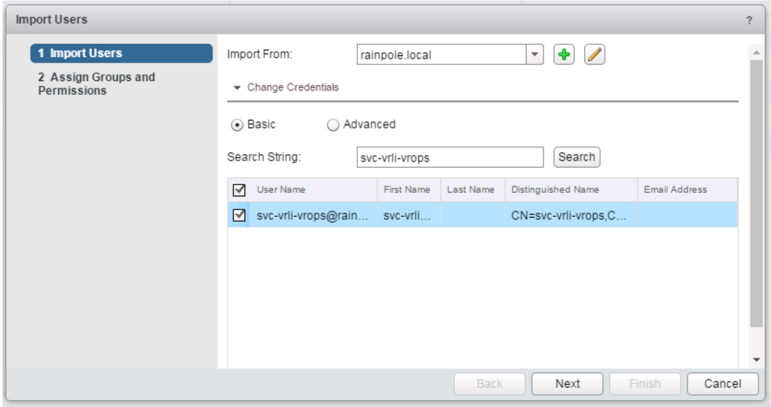
   a From the **Import From** drop-down menu, select **RAINPOLE.LOCAL**.

   b Select the **Basic** option for the seach query.

   c In the **Search String** text box, enter `svc-vrli-vrops` and click **Search**.

   The search results contain the svc-vrli-vrops user account.

   d Select **svc-vrli-vrops@rainpole.local** and click **Next**.



Import Users

1 Import Users

2 Assign Groups and Permissions

Import From: rainpole.local

Change Credentials

● Basic ○ Advanced

Search String: svc-vrli-vrops

☑	User Name	First Name	Last Name	Distinguished Name	Email Address
☑	svc-vrli-vrops@rain...	svc-vrli...		CN=svc-vrli-vrops,C...	

5 On the **Assign Groups and Permissions** page, to assign the `Administrator` role to the svc-vrli-vrops@rainpole.local service account, click the **Objects** tab, configure the following settings and click **Finish**.

Setting	Value
Select Role	Administrator
Assign this role to the user	Selected
Allow access to all objects in the system	Selected

6 When prompted with the warning for allowing access to all objects on the system, click **Yes**.

Enable the vRealize Log Insight Integration with vRealize Operations Manager for Region A

Connect vRealize Log Insight in Region A with vRealize Operations Manager to launch vRealize Log Insight from within vRealize Operations Manager and to send alerts to vRealize Operations Manager.

Prerequisites

- Verify that the vRealize Log Insight management pack is installed in vRealize Operations Manager
- Verify that you have connected vRealize Operations Manager to the mgmt01vc01.sfo01.rainpole.local or comp01vc01.sfo01.rainpole.local vCenter Server instances.
- Verify that you have connected vRealize Log Insight to the mgmt01vc01.sfo01.rainpole.local or comp01vc01.sfo01.rainpole.local vCenter Server instances.
- Verify that you have configured the svc-vrli-vrops@rainpole.local service account within vRealize Operations Manager.

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 **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.

   d Select the **Enable launch in context** check box.

5 Click **Save**.

   A progress dialog box appears.

Install the vRealize Log Insight Content Pack for vRealize Operations Manager in Region A

Install the content pack for vRealize Operations Manager to add the dashboards for viewing log information in vRealize Log Insight.

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 **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, click **Install**.

After the installation is complete, the VMware - vRops 6.x content pack appears in the **Installed Content Packs** list on the left.

Configure the Log Insight Agent on vRealize Operations Manager to Forward Log Events to vRealize Log Insight in Region A

After you install the content pack for vRealize Operations Manager, configure the Log Insight agent on vRealize Operations Manager to send audit logs and system events to vRealize Log Insight in Region A.

Procedure

1 On your computer, create a `liagent.ini` file for each of the 5 nodes of vRealize Operations Manager.

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|ANALYTICS-analytics]
tags = {"vmw_vr_ops_appname":"vROps",
"vmw_vr_ops_logtype":"ANALYTICS","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 = analytics*.log*
exclude_fields=hostname

[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|WEB-web]
directory = /data/vcops/log
tags = {"vmw_vr_ops_appname":"vROps",
"vmw_vr_ops_logtype":"WEB","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 = web*.log*
exclude_fields=hostname
event_marker=^\d{4}-\d{2}-\d{2}[\s]\d{2}:\d{2}:\d{2}\,\d{3}

[filelog|GEMFIRE-gemfire]
tags = {"vmw_vr_ops_appname":"vROps",
"vmw_vr_ops_logtype":"GEMFIRE","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 = gemfire*.log*
exclude_fields=hostname

[filelog|VIEW_BRIDGE-view_bridge]
tags =
{"vmw_vr_ops_appname":"vROps","vmw_vr_ops_logtype":"VIEW_BRIDGE","vmw_vr_ops_clustername":"<YOU
R 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 = view-bridge*.log*
exclude_fields=hostname
event_marker=^\d{4}-\d{2}-\d{2}[\s]\d{2}:\d{2}:\d{2}\,\d{3}

[filelog|VCOPS_BRIDGE-vcops_bridge]
tags =
{"vmw_vr_ops_appname":"vROps","vmw_vr_ops_logtype":"VCOPS_BRIDGE","vmw_vr_ops_clustername":"<YO
UR 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 = vcops-bridge*.log*
exclude_fields=hostname
event_marker=^\d{4}-\d{2}-\d{2}[\s]\d{2}:\d{2}:\d{2}\,\d{3}

[filelog|SUITEAPI-api]
directory = /data/vcops/log
tags = {"vmw_vr_ops_appname":"vROps",
"vmw_vr_ops_logtype":"SUITEAPI","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 = api.log*;http_api.log*;profiling_api.log*
exclude_fields=hostname
event_marker=^\d{4}-\d{2}-\d{2}[\s]\d{2}:\d{2}:\d{2}\,\d{3}

[filelog|SUITEAPI-suite_api]
directory = /data/vcops/log/suite-api
tags = {"vmw_vr_ops_appname":"vROps",
"vmw_vr_ops_logtype":"SUITEAPI","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 = *.log*
exclude_fields=hostname
event_marker=^\d{2}-\w{3}-\d{4}[\s]\d{2}:\d{2}:\d{2}\.\d{3}

[filelog|ADMIN_UI-admin_ui]
tags = {"vmw_vr_ops_appname":"vROps",
"vmw_vr_ops_logtype":"ADMIN_UI","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/casa
include = *.log*;*_log*
exclude_fields=hostname
```

```
[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 = analytics*.txt;collector*.txt
exclude_fields=hostname

[filelog|TOMCAT_WEBAPP-tomcat_webapp]
tags =
{"vmw_vr_ops_appname":"vROps","vmw_vr_ops_logtype":"TOMCAT_WEBAPP","vmw_vr_ops_clustername":"<Y
OUR 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/product-ui
include = *.log*;*_log*
exclude_fields=hostname

[filelog|OTHER-other1]
tags = {"vmw_vr_ops_appname":"vROps",
"vmw_vr_ops_logtype":"OTHER","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 =
aim*.log*;calltracer*.log*;casa.audit*.log*;distributed*.log*;hafailover*.log;his*.log*;install
er*.log*;locktrace*.log*;opsapi*.log*;query-service-
timer*.log*;queryprofile*.log*;vcopsConfigureRoles*.log*
exclude_fields=hostname
event_marker=^\d{4}-\d{2}-\d{2}[\s]\d{2}:\d{2}:\d{2}\,\d{3}

[filelog|OTHER-other2]
tags = {"vmw_vr_ops_appname":"vROps", "vmw_vr_ops_logtype":"OTHER",
"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 = env-checker.log*
exclude_fields=hostname
event_marker=^\d{2}\D{1}\d{2}\D{1}\d{4}\s\d{2}:\d{2}:\d{2}

[filelog|OTHER-other3]
tags = {"vmw_vr_ops_appname":"vROps", "vmw_vr_ops_logtype":"OTHER",
"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 = gfsh*.log*;HTTPPostAdapter*.log*;meta-gemfire*.log*;migration*.log*
exclude_fields=hostname

[filelog|OTHER-watchdog]
tags = {"vmw_vr_ops_appname":"vROps", "vmw_vr_ops_logtype":"OTHER",
"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/vcops-watchdog
include = vcops-watchdog.log*
exclude_fields=hostname
event_marker=^\d{4}-\d{2}-\d{2}[\s]\d{2}:\d{2}:\d{2}\,\d{3}

[filelog|ADAPTER-vmwareadapter]
tags = {"vmw_vr_ops_appname":"vROps", "vmw_vr_ops_logtype":"ADAPTER",
"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/adapters/VMwareAdapter
include = *.log*
exclude_fields=hostname
event_marker=^\d{4}-\d{2}-\d{2}[\s]\d{2}:\d{2}:\d{2}\,\d{3}

[filelog|ADAPTER-vcopsadapter]
tags = {"vmw_vr_ops_appname":"vROps", "vmw_vr_ops_logtype":"ADAPTER",
"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/adapters/VCOpsAdapter
include = *.log*
exclude_fields=hostname
event_marker=^\d{4}-\d{2}-\d{2}[\s]\d{2}:\d{2}:\d{2}\,\d{3}

[filelog|ADAPTER-openapiadapter]
tags = {"vmw_vr_ops_appname":"vROps", "vmw_vr_ops_logtype":"ADAPTER",
"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/adapters/OpenAPIAdapter
include = *.log*
exclude_fields=hostname
event_marker=^\d{4}-\d{2}-\d{2}[\s]\d{2}:\d{2}:\d{2}\,\d{3}
```

b In the node-specific `liagent.ini` file, change the following parameters and save the file.

Parameter	Description	Location in liagent.ini	Configuration Instructions
hostname	IP address or FQDN of the Log Insight VIP	`[server]` section	Replace `<YOUR LOGINSIGHT HOSTNAME HERE>` with **`vrli-cluster-01.sfo01.rainpole.local`**.
proto	Protocol that the agent uses to send events to the Log Insight server.	`[server]` section	Remove the **;** comment in front of the parameter to set the log protocol to **`cfapi`**.
port	Communication port that the agent uses to send events to the vRealize Log Insight server.	`[server]` section	Remove the **;** comment in front of the parameter to set the port to **`9000`**.

Parameter	Description	Location in liagent.ini	Configuration Instructions
vmw_vr_ops_clustername	Name of the vRealize Operations Manager cluster	each [filelog| *section_name*] section	Replace each <YOUR CLUSTER NAME HERE> with **vrops-cluster-01**.
vmw_vr_ops_clusterrole	Role of the vRealize Operations Manager node	each [filelog| *section_name*] section	Set to **Master**, **Replica**, **Data** or **Remote Collector**.
vmw_vr_ops_hostname	IP address or FQDN of the vRealize Operations Manager node	each [filelog| *section_name*] section	Replace each <YOUR VROPS HOSTNAMEHERE> with the following FQDN: ■ **vrops-mstrn-01.rainpole.local** for the master node ■ **vrops-repln-02.rainpole.local** for the replica node ■ **vrops-datan-03.rainpole.local** for data node 1 ■ **vrops-rmtcol-01.sfo01.rainpole.local** for remote collector 1 ■ **vrops-rmtcol-02.sfo01.rainpole.local** for remote collector 2
vmw_vr_ops_nodename	Name of the vRealize Operations Manager node that is set during node initial configuration	each [filelog| *section_name*] section	Replace each <YOUR NODE NAME HERE> with the following name: ■ **vrops-mstrn-01** for the master node ■ **vrops-repln-02** for the replica node ■ **vrops-datan-03** for data node 1 ■ **vrops-rmtcol-01** for remote collector 1 ■ **vrops-rmtcol-02** 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=vrli-cluster-01.sfo01.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 master replica node 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":"ANALYTICS","vmw_vr_ops_clustername":"vrops-cluster-01",
"vmw_vr_ops_clusterrole":"Replica","vmw_vr_ops_nodename":"vrops-repln-02",
"vmw_vr_ops_hostname":"vrops-repln-02.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://mgmt01vc01.sfo01.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 mgmt01vc01.sfo01.rainpole.local vCenter Server, navigate to the virtual appliance for the node.

Virtual Appliance Name	Role
vrops-mstrn-01	Master node
vrops-repln-02	Master replica node
vrops-datan-03	Data node 1
vrops-rmtcol-01	Remote collector 1
vrops-rmtcol-02	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	*vrops_root_password*

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 Stop the SSH service on the virtual appliance by running the following command.

```
service
                        sshd stop
```

4 Repeat the steps for each of the remaining vRealize Operations Manager nodes.

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://vrli-cluster-01.sfo01.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 menu at the top, select **vRops 6.x - Sample** from the **Available Templates** section and click **Copy Template**.

f In the **Copy Agent Group** dialog box, enter **`vRops6 - Agent Group`** in the name text box and click **Copy**.

g In the **agent filter** fields, enter the following values pressing Enter after each host name.

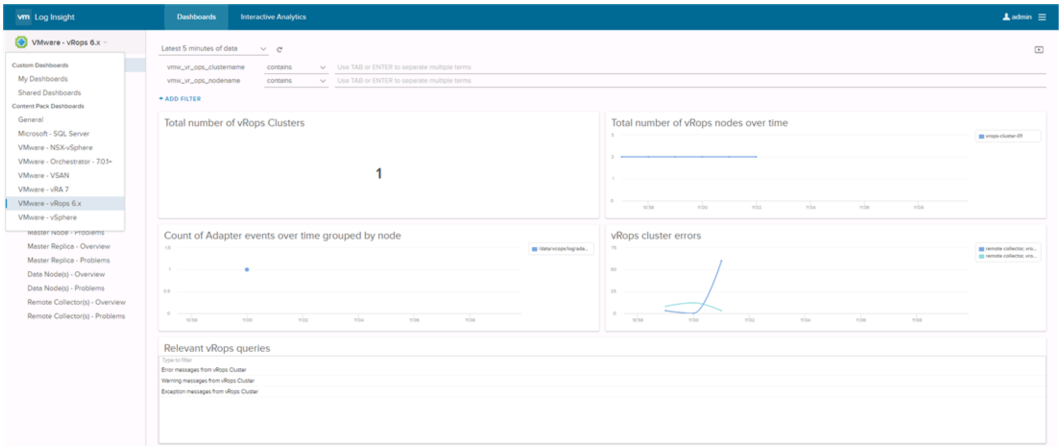
Filter	Operator	Values
Hostname	matches	■ vrops-mstrn-01.rainpole.local ■ vrops-repln-02.rainpole.local ■ vrops-datan-03.rainpole.local ■ vrops-rmtcol-01.sfo01.rainpole.local ■ vrops-rmtcol-02.sfo01.rainpole.local

h Click **Refresh** and verify that all the agents in the filter appear in the **Agents** list.

i Click **Save New Group** at the bottom of the page.

j Click the **Dashboard** tab and select the **VMware - vRops 6.x** dashboard from the drop-down menu on the left.

All VMware - vRops 6 dashboards become available on the vRealize Log Insight Home page.



Connect vRealize Log Insight to the NSX Instances in Region A

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. 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 Region A

Install the content pack for NSX for vSphere to add the dashboards for viewing log information in vRealize Log Insight.

2 Configure NSX Managers to Forward Log Events to vRealize Log Insight in Region A

Configure the NSX Manager for the management cluster and the NSX Manager for the compute and edge clusters to send audit logs and system events to vRealize Log Insight in Region A.

3. Configure the NSX Controllers to Forward Events to vRealize Log Insight in Region A

   Configure the NSX Controller instances for the management, compute and edge clusters to forward log information to vRealize Log Insight in Region A 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 Region A

   Redirect log information from the edge services gateways, universal distributed logical router and load balancer in Region A to vRealize Log Insight in Region A.

Install the vRealize Log Insight Content Pack for NSX for vSphere in Region A

Install the content pack for NSX for vSphere to add the dashboards for viewing log information in vRealize Log Insight.

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 **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, 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 Region A

Configure the NSX Manager for the management cluster and the NSX Manager for the compute and edge clusters to send audit logs and system events to vRealize Log Insight in Region A.

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.

NSX Manager	URL
NSX Manager for the management cluster	https://mgmt01nsxm01.sfo01.rainpole.local
NSX Manager for the shared compute and edge cluster	https://comp01nsxm01.sfo01.rainpole.local

b Log in using the following credentials.

Setting	Value
User name	admin
Password	*nsx_manager_admin_password*

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 vRealize Log Insight as a syslog server by specifying the following settings and click **OK**.

Syslog Server Setting	Value
Syslog Server	vrli-cluster-01.sfo01.rainpole.local
Port	514
Protocol	UDP

5 Repeat the steps for the other NSX Manager.

Configure the NSX Controllers to Forward Events to vRealize Log Insight in Region A

Configure the NSX Controller instances for the management, compute and edge clusters to forward log information to vRealize Log Insight in Region A 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.

Procedure

1 Log in to the Windows host that has access to your 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**.

Setting	Value
User name	admin
Password	*mngnsx_admin_password* *compnsx_admin_password*

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 management cluster	https://mgmt01nsxm01.sfo01.rainpole.local/api/2.0/vdn/controller
NSX Manager for the shared edge and compute cluster	https://comp01nsxm01.sfo01.rainpole.local/api/2.0/vdn/controller

The RESTClient sends a query to the NSX Manager about the installed NSX controllers.

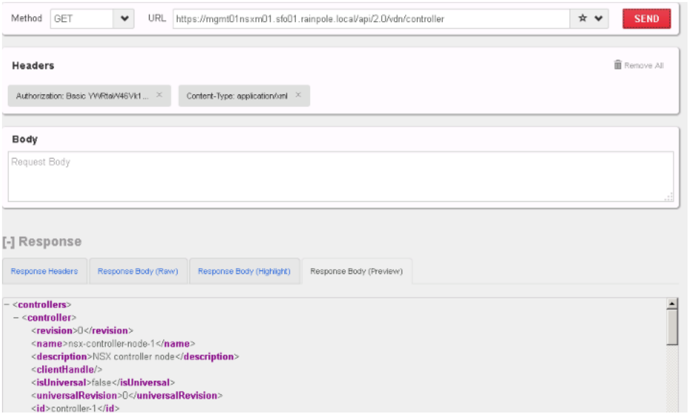
c After the NSX Manager sends a response back, click the **Response Body (Preview)** tab under **Response**.

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.

e Repeat the steps for the other NSX Manager.



Method GET URL https://mgmt01nsxm01.sfo01.rainpole.local/api/2.0/vdn/controller

Headers

Authorization: Basic YWRtaW46Vk1 ...

Content-Type: application/xml

Body

```
- <controllers>
  - <controller>
      <revision>0</revision>
      <name>nsx-controller-node-1</name>
      <description>NSX controller node</description>
      <clientHandle/>
      <isUniversal>false</isUniversal>
      <universalRevision>0</universalRevision>
      <id>controller-1</id>
```

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.

Table 4-4.

NSX Manager	NSX Controller in the Controller Cluster	POST URL
NSX Manager for the management cluster	NSX Controller 1	https://mgmt01nsxm01.sfo01.rainpole.local/api/2.0/vdn/controller/controller-1/syslog
	NSX Controller 2	https://mgmt01nsxm01.sfo01.rainpole.local/api/2.0/vdn/controller/controller-2/syslog
	NSX Controller 3	https://mgmt01nsxm01.sfo01.rainpole.local/api/2.0/vdn/controller/controller-3/syslog
NSX Manager for the shared edge and compute cluster	NSX Controller 1	https://comp01nsxm01.sfo01.rainpole.local/api/2.0/vdn/controller/controller-1/syslog
	NSX Controller 2	https://comp01nsxm01.sfo01.rainpole.local/api/2.0/vdn/controller/controller-2/syslog
	NSX Controller 3	https://comp01nsxm01.sfo01.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>vrli-cluster-01.sfo01.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**, in the **URL** text box, enter the controller-specific syslog URL from the previous step, and click the**SEND** button.

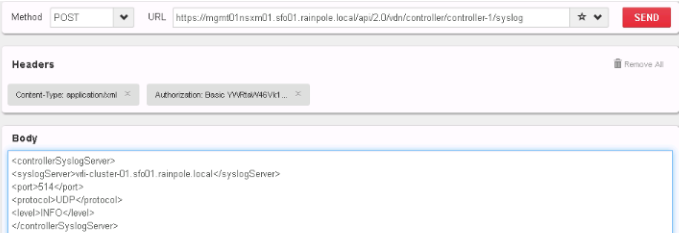
b After the NSX Manager sends a response back, click the **Response Body (Preview)** tab under **Response**.

The response body contains a root <controllerSyslogServer> element, which represents the settings for the remote syslog server on the NSX Controller.

   c. Verify that the value of the <syslogServer> element is vrli-cluster-01.sfo01.rainpole.local.

   d. Repeat the steps for the next NSX Controller.

7. Verify the syslog configuration on each NSX Controller.



Method: POST

URL: https://mgmt01nsxm01.sfo01.rainpole.local/api/2.0/vdn/controller/controller-1/syslog

Headers

Content-Type: application/xml

Authorization: Basic YWRtaW46Vk1 ...

Body

```
<controllerSyslogServer>
<syslogServer>vrli-cluster-01.sfo01.rainpole.local</syslogServer>
<port>514</port>
<protocol>UDP</protocol>
<level>INFO</level>
</controllerSyslogServer>
```

Configure the NSX Edge Instances to Forward Log Events to vRealize Log Insight in Region A

Redirect log information from the edge services gateways, universal distributed logical router and load balancer in Region A to vRealize Log Insight in Region A.

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. 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
Management NSX Manager	172.16.11.65
Compute NSX Manager	172.16.11.66

   The edge devices in the scope of the NSX Manager appear.

5 Configure the log forwarding on each edge service gateway of Management and Compute NSX Managers instances.

   a Double-click the edge device to open its user interface.

Traffic	Management NSX Edge Service Gateway	Compute NSX Edge Service Gateway
North-South Routing	SFOMGMT-ESG01	SFOCOMP-ESG01
North-South Routing	SFOMGMT-ESG02	SFOCOMP-ESG02
East-West Routing	UDLR01	UDLR01
Load Balancer	SFOMGMT-LB01	-

   b On the NSX Edge device page, click the **Manage** tab, click **Settings**, and click **Configuration**.

   c In the **Details** pane, 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	192.168.31.10
Protocol	udp

   e Click **OK**.

   f Repeat the steps for the remaining NSX Edge devices of Management and Compute NSX Manager instances.

The vRealize Log Insight user interface 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 Region A

Connect the vRealize Log to vRealize Automation to receive log information from all components of vRealize Automation in the vRealize Log Insight UI.

Procedure

1 Install the vRealize Log Insight Content Packs for the Cloud Management Platform in Region A

   Install the content packs for vRealize Automation, vRealize Orchestrator and Microsoft SQL Server to add the dashboards for viewing log information about the Cloud Management Platform in vRealize Log Insight.

2 Install and Configure vRealize Log Insight Windows Agents in Region A

   Install the vRealize Log Insight agent on the Windows virtual machines for the Distributed Execution Manager, IaaS Manager Service, IaaS Web Server, IaaS SQL Server and the vSphere proxy agents. Configure Log Insight Windows Agents from the vRealize Log Insight Web interface.

3. Configure vRealize Log Insight Linux Agents in the vRealize Automation Virtual Appliances in Region A

   vRealize Log Insight Agent comes pre-installed on the vRealize Automation virtual appliance. Configure the `liagent.ini` configuration file on each virtual appliance.

4. Configure vRealize Orchestrator to Forward Log Events to vRealize Log Insight in Region A

   You can configure each vRealize Orchestrator appliance to forward system logs and events to the vRealize Log Insight instance. All syslog information can then be viewed and analyzed from the vRealize Log Insight Web interface.

Install the vRealize Log Insight Content Packs for the Cloud Management Platform in Region A

Install the content packs for vRealize Automation, vRealize Orchestrator and Microsoft SQL Server to add the dashboards for viewing log information about the Cloud Management Platform in vRealize Log Insight.

You install the following content packs:

- VMware - vRA 7
- VMware - Orchestrator
- Microsoft - SQL Server

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 **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, click **Install**.

6. Repeat the procedure to install the **VMware - Orchestrator** and **Microsoft - SQL Server** content packs.

After the installation is complete, the VMware - vRA, VMware - Orchestrator and Microsoft - SQL Server content packs appear in the Installed Content Packs list on the left.

Install and Configure vRealize Log Insight Windows Agents in Region A

Install the vRealize Log Insight agent on the Windows virtual machines for the Distributed Execution Manager, IaaS Manager Service, IaaS Web Server, IaaS SQL Server and the vSphere proxy agents. Configure Log Insight Windows Agents from the vRealize Log Insight Web interface.

Procedure

1. Install the Log Insight Windows Agents on 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 or VM Name
IaaS Web Server	vra01iws01a.rainpole.local
IaaS Web Server	vra01iws01b.rainpole.local
IaaS Manager Service and DEM Orchestrator	vra01ims01a.rainpole.local
IaaS Manager Service and DEM Orchestrator	vra01ims01b.rainpole.local
IaaS DEM Worker	vra01dem01.rainpole.local
IaaS DEM Worker	vra01dem02.rainpole.local
vSphere Proxy Agent	vra01ias01.sfo01.rainpole.local
vSphere Proxy Agent	vra01ias02.sfo01.rainpole.local
Microsoft SQL Server	vra01mssql01.rainpole.local

   b. Log in using the following credentials.

Setting	Value
User name	Windows administrator user
Password	*windows_administrator_password*

   c. Open a Web browser and go to **`https://vrli-cluster-01.sfo01.rainpole.local`** .

   d. Log in using the following credentials.

Setting	Value
User name	admin
Password	*vrli_admin_password*

   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 `.msi` file on your computer.

   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 vrli-cluster-01.sfo01.rainpole.local shown in the **Host** text box, click **Install**.

l When the installation is complete, click **Finish**.

2 Configure the Log Insight Windows Agent Group for the vRealize Automation IaaS components from the vRealize Log Insight Web 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*

c Click the configuration drop-down menu icon ☰ and select **Administration**.

d Under **Management**, click **Agents**.

e From the drop-down at 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 In the agent filter fields, use the following selections.

Use ENTER to separate the host name values.

Filter	Operator	Values
Hostname	matches	vra01iws01a.rainpole.local vra01iws01b.rainpole.local vra01ims01a.rainpole.local vra01ims01b.rainpole.local vra01dem01.rainpole.local vra01dem02.rainpole.local vra01ias01.sfo01.rainpole.local vra01ias02.sfo01.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.

3 In the vRealize Log Insight Web user interface, configure the Log Insight Windows Agent Group for the Microsoft SQL Server component that is used by vRealize Automation.

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*

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 **Microsoft - SQL Server** from the **Available Templates** section..

f Click **Copy Template**.

g In the **Copy Agent Group** dialog box, enter **`vRA7 - Microsoft SQL Server Agent Group`** in the name text box and click **Copy.**

h In the agent filter fields, use the following selections.

Use ENTER to separate the host name values.

Filter	Operator	Values
Hostname	matches	vra01mssql01.rainpole.local

i Under **Agent Configuration**, click **Edit**

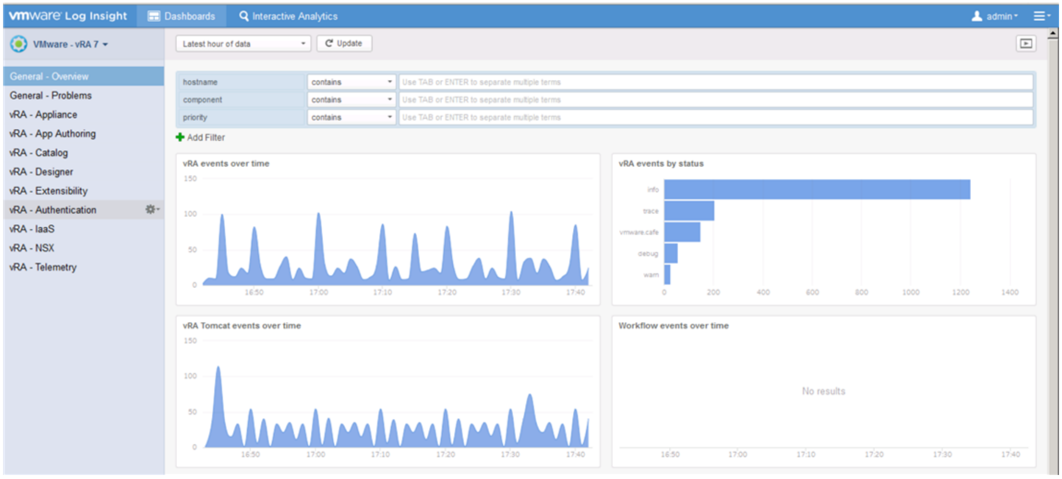
j Locate `directory=C:\Program Files\Microsoft SQL Server\MSSQL10.MSSQLSERVER\MSSQL\Log` and change it to `directory=C:\Program Files\Microsoft SQL Server\MSSQL11.MSSQLSERVER\MSSQL\Log`

Note In this VMware Validated Design, Microsoft SQL Server 2012 R2 has been installed in the default location on the Windows Server virtual machine.

k Click **Refresh** and verify that all the agents listed in the filter appear in the Agents list.

l Click **Save New Group** at the bottom of the page.

All VMware vRA 7 dashboards become available on the vRealize Log Insight Home page.



Configure vRealize Log Insight Linux Agents in the vRealize Automation Virtual Appliances in Region A

vRealize Log Insight Agent comes pre-installed on the vRealize Automation virtual appliance. Configure the `liagent.ini` configuration file on each virtual appliance.

Procedure

1 Edit the `liagent.ini` file on the first vRealize Automation virtual appliance.

   a Open an SSH connection to the virtual appliance by using the following settings.

Setting	Value
SSH sever	vra01svr01a.rainpole.local
User name	root
Password	*vra_applianceA_root_password*

   b Open the `/var/lib/loginsight-agent/liagent.ini` file in a text editor.

   c Update the following parameters in the `[server]` section and save your changes.

   ```
   [server]
   hostname=vrli-cluster-01.sfo01.rainpole.local
   proto=cfapi
   port=9000
   ```

d Restart the Log Insight agent by running the following command

```
/etc/init.d/liagentd restart
```

e Repeat the steps on the second vRealize Automation appliance vra01svr01b.rainpole.local by using the following settings.

Setting	Value
SSH Server	vra01svr01b.rainpole.local
User name	root
Password	*vra_applianceB_root_password*

2 Configure the Linux Agent Group on the Log Insight server.

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*

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 **vRealize Automation 7 - Linux** from the **Available Templates** section.

f Click **Copy Template**.

g In the **Copy Agent Group** dialog box, enter **`vRA7 - Linux 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.

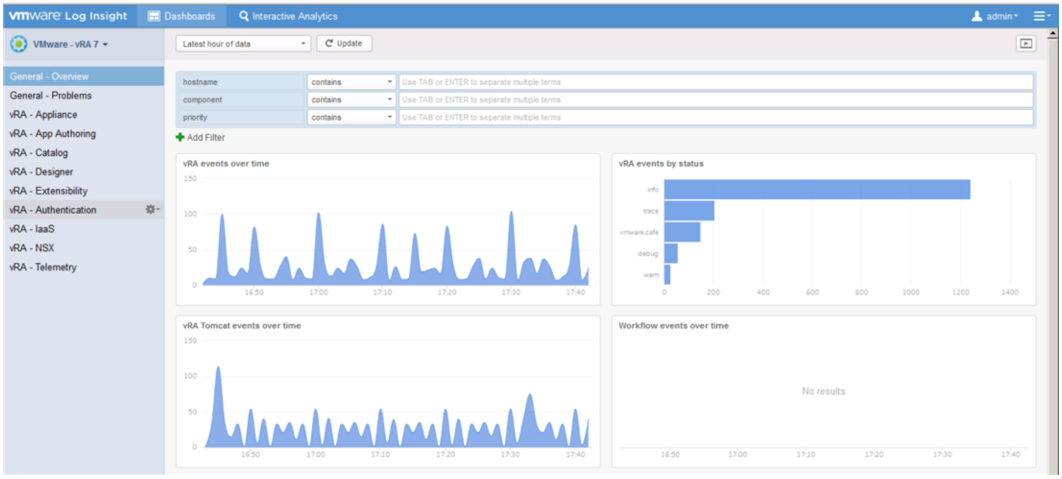
Filter	Operator	Values
Hostname	matches	vra01svr01a.rainpole.local vra01svr01b.rainpole.local

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 VR 7** dashboard from the drop-down menu on the left.

All VMware vRA 7 dashboards become available on the vRealize Log Insight Home page.



Configure vRealize Orchestrator to Forward Log Events to vRealize Log Insight in Region A

You can configure each vRealize Orchestrator appliance to forward system logs and events to the vRealize Log Insight instance. All syslog information can then be viewed and analyzed from the vRealize Log Insight Web interface.

In Region A, you configure the following vRealize Orchestrator instances.

Host	Control Center URL
Host A	https://vra01vro01a.rainpole.local:8283/vco-controlcenter
Host B	https://vra01vro01b.rainpole.local:8283/vco-controlcenter

Procedure

1 Log in to the vRealize Orchestrator Control Center.

   a Open a Web browser and go to `https://vra01vro01a.rainpole.local:8283/vco-controlcenter`.

   b Log in using the following credentials.

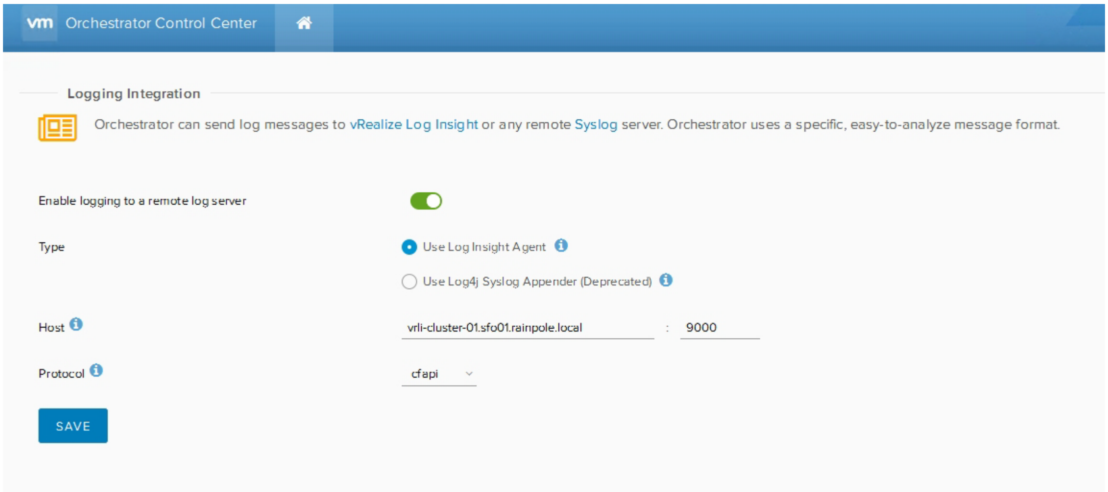
Setting	Value
User name	root
Password	*hostA_root_password*

2 From the **Home** page, under **Log**, click **Logging Integration**.

3 On the **Logging Integration** page, specify the following settings and click **Save**.

Setting	Value
Enable logging to a remote log server	Selected
Use Log Insight Agent	Selected
Host	vrli-cluster-01.sfo01.rainpole.local

Setting	Value
Port	9000
Protocol	cfapi



Logging Integration

Orchestrator can send log messages to vRealize Log Insight or any remote Syslog server. Orchestrator uses a specific, easy-to-analyze message format.

Enable logging to a remote log server	●
Type	● Use Log Insight Agent ○ Use Log4j Syslog Appender (Deprecated)
Host	vrli-cluster-01.sfo01.rainpole.local : 9000
Protocol	cfapi

4 Repeat the procedure for the second vRealize Orchestrator appliance vra01vro01b.rainpole.local.

5 Enable vRealize Log Insight agents for vRealize Orchestrator.

a Open a Web browser and go to **`https://vrli-cluster-01.sfo01.rainpole.local`**

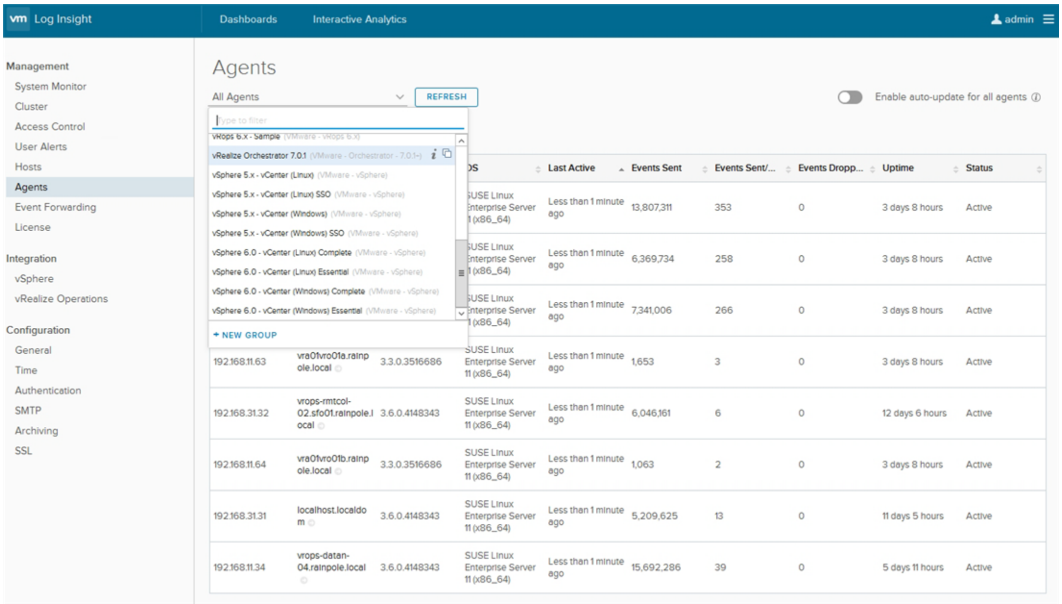
b Log in using the following credentials.

Setting	Value
User name	admin
Password	*vrli_admin_password*

c Click the configuration drop-down menu icon ☰ and select **Administration**.

d Under **Management**, click **Agents**.

e From the drop-down menu at the top, select **vRealize Orchestrator 7.0.1** from the **All Agents** section and click **Copy Template**.


vm Log Insight
Dashboards
Interactive Analytics
admin
Management
System Monitor
Cluster
Access Control
User Alerts
Hosts
Agents
Event Forwarding
License
Integration
vSphere
vRealize Operations
Configuration
General
Time
Authentication
SMTP
Archiving
SSL
Agents
All Agents
REFRESH
Enable auto-update for all agents
Type to filter
vRops 6.x - Sample (VMware - vRops 6.x)
vRealize Orchestrator 7.0.1 (VMware - Orchestrator - 7.0.1-)
vSphere 5.x - vCenter (Linux) (VMware - vSphere)
vSphere 5.x - vCenter (Linux) SSO (VMware - vSphere)
vSphere 5.x - vCenter (Windows) (VMware - vSphere)
vSphere 5.x - vCenter (Windows) SSO (VMware - vSphere)
vSphere 6.0 - vCenter (Linux) Complete (VMware - vSphere)
vSphere 6.0 - vCenter (Linux) Essential (VMware - vSphere)
vSphere 6.0 - vCenter (Windows) Complete (VMware - vSphere)
vSphere 6.0 - vCenter (Windows) Essential (VMware - vSphere)
+ NEW GROUP

			DS	Last Active	Events Sent	Events Sent/...	Events Dropp...	Uptime	Status
			SUSE Linux nterprise Server 1 (x86_64)	Less than 1 minute ago	13,807,311	353	0	3 days 8 hours	Active
			SUSE Linux nterprise Server 1 (x86_64)	Less than 1 minute ago	6,369,734	258	0	3 days 8 hours	Active
			SUSE Linux nterprise Server 1 (x86_64)	Less than 1 minute ago	7,341,006	266	0	3 days 8 hours	Active
192.168.11.63	vra01vro01a.rainpole.local	3.3.0.3516686	SUSE Linux Enterprise Server 11 (x86_64)	Less than 1 minute ago	1,653	3	0	3 days 8 hours	Active
192.168.31.32	vrops-rmtcol-02.sfo01.rainpole.local	3.6.0.4148343	SUSE Linux Enterprise Server 11 (x86_64)	Less than 1 minute ago	6,046,161	6	0	12 days 6 hours	Active
192.168.11.64	vra01vro01b.rainpole.local	3.3.0.3516686	SUSE Linux Enterprise Server 11 (x86_64)	Less than 1 minute ago	1,063	2	0	3 days 8 hours	Active
192.168.31.31	localhost.localdom	3.6.0.4148343	SUSE Linux Enterprise Server 11 (x86_64)	Less than 1 minute ago	5,209,625	13	0	11 days 5 hours	Active
192.168.11.34	vrops-datan-04.rainpole.local	3.6.0.4148343	SUSE Linux Enterprise Server 11 (x86_64)	Less than 1 minute ago	15,692,286	39	0	5 days 11 hours	Active

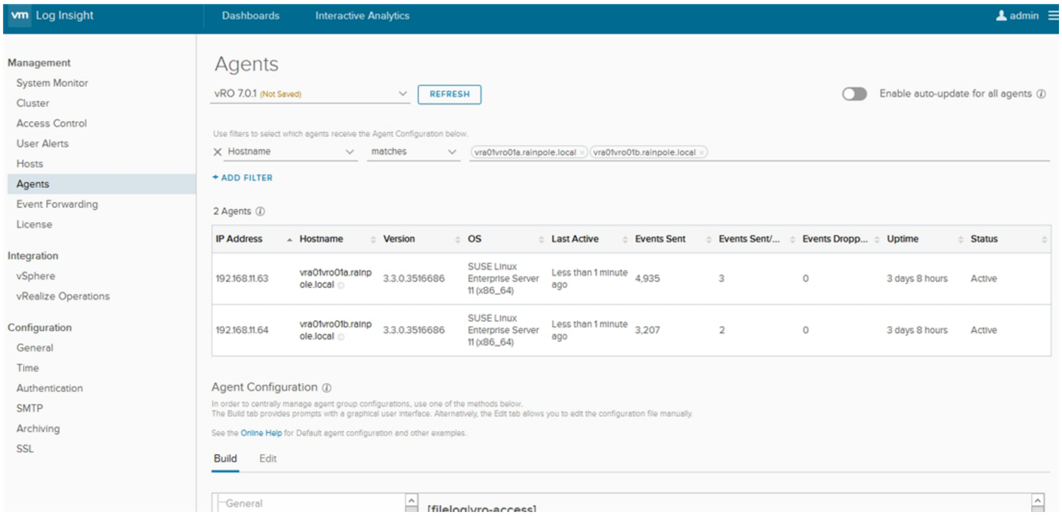
f In the **Copy Agent Group** dialog box, enter **`vRO 7.0.1`** in the name text box and click **Save New Group**.

g Under the **All Agents** drop-down menu, select **vRO 7.0.1**.

h In the **agent filter** fields, enter the following values pressing Enter after each host name to determine which agents receive the configuration.

Filter	Operator	Values
Hostname	matches	■ vra01vro01a.rainpole.local ■ vra01vro01b.rainpole.local

i Click **Refresh** and verify that in the **Agents** list vRealize Log Insight receives data from the two agents in the filter.



Agents

vRO 7.0.1 (Not Saved)

Enable auto-update for all agents

Use filters to select which agents receive the Agent Configuration below.

Hostname matches vra01vro01a.rainpole.local vra01vro01b.rainpole.local

2 Agents

IP Address	Hostname	Version	OS	Last Active	Events Sent	Events Sent/...	Events Dropp...	Uptime	Status
192.168.11.63	vra01vro01a.rainpole.local	3.3.0.3516686	SUSE Linux Enterprise Server 11 (x86_64)	Less than 1 minute ago	4,935	3	0	3 days 8 hours	Active
192.168.11.64	vra01vro01b.rainpole.local	3.3.0.3516686	SUSE Linux Enterprise Server 11 (x86_64)	Less than 1 minute ago	3,207	2	0	3 days 8 hours	Active

Agent Configuration

In order to centrally manage agent group configurations, use one of the methods below.
The Build tab provides prompts with a graphical user interface. Alternatively, the Edit tab allows you to edit the configuration file manually.

See the Online Help for Default agent configuration and other examples.

[filelog|vro-access]

j Click **Save Agent Group** at the bottom of the page.

6 Verify that the vRealize Log Insight server is receiving log events from the vRealize Orchestrator appliances.

a Open a Web browser and go to **`https://vrli-cluster-01.sfo01.rainpole.local`**.

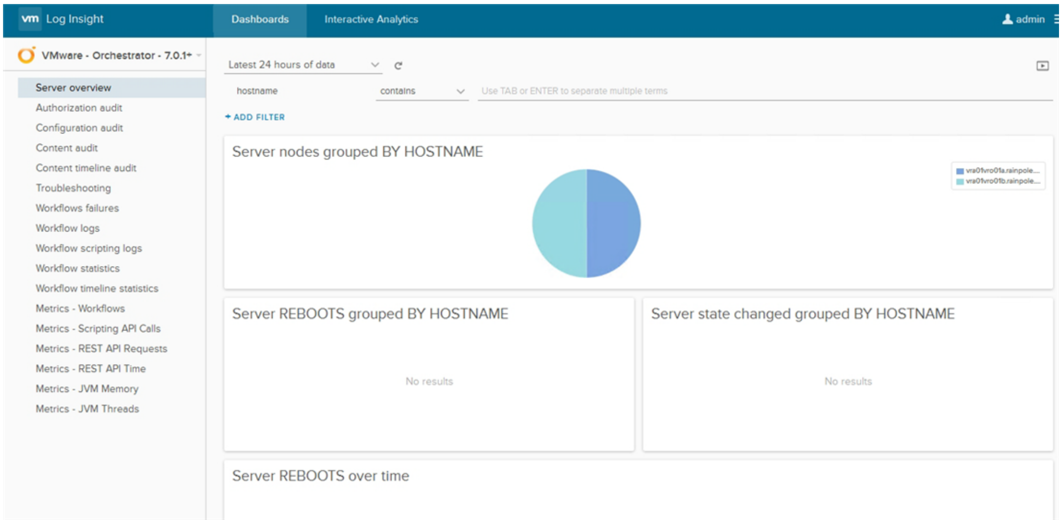
b Log in using the following credentials.

Setting	Value
User name	admin
Password	*vrli_admin_password*

c In the vRealize Log Insight user interface, select **VMware - Orchestrator - 7.0.1+** from the **Dashboards** drop-down menu.

d Verify that the **Server nodes grouped by hostname** widget on the **Server overview** dashboard shows the two vRealize Orchestrator hosts.

The other dashboards start showing data when they get the associated events.



Latest 24 hours of data

hostname contains

Install the vRealize Log Insight Content Pack for vSAN in Region A

Install the content pack for VMware vSAN to add the dashboards for viewing log information in vRealize Log Insight.

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 **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, 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 Log Retention and Archiving in Region A

Set log retention to one week and archive logs for 90 days according to the *VMware Validated Design Architecture and Design* documentation.

Prerequisites

- Create an NFS share of 1 TB in Region and export it as `/V2D_vRLI_MgmtA_1TB`.
- Verify that the NFS server supports NFS v3.
- Verify that the NFS partition allows read and write operations for guest accounts.
- Verify that the mount does not require authentication.
- Verify that the NFS share is directly accessible to vRealize Log Insight
- If using a Windows NFS server, allow unmapped user Unix access (by UID/GID).

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 Configure retention threshold notification.

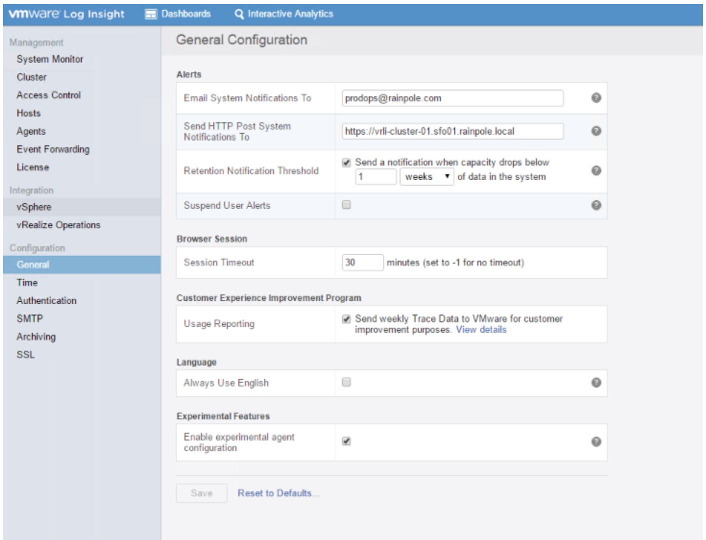
Log Insight continually estimates how long data can be retained with the currently available pool of storage.

If the estimation drops below the retention threshold of one week, Log Insight immediately notifies the administrator that the amount of searchable log data is likely to drop.

a Under **Configuration**, click **General**.

b On the **General Configuration** page, under the **Alerts** section, select the **Send a notification when capacity drops below** check box next to **Retention Notification Threshold**, and enter a 1-week period in the text box.

c Click **Save**.



General Configuration

Alerts

Email System Notifications To: prodops@rainpole.com

Send HTTP Post System Notifications To: https://vrli-cluster-01.sfo01.rainpole.local

Retention Notification Threshold: ☑ Send a notification when capacity drops below 1 weeks ▾ of data in the system

Suspend User Alerts: □

Browser Session

Session Timeout: 30 minutes (set to -1 for no timeout)

Customer Experience Improvement Program

Usage Reporting: ☑ Send weekly Trace Data to VMware for customer improvement purposes. View details

Language

Always Use English: □

Experimental Features

Enable experimental agent configuration: ☑

4 Configure data archiving.

a Under **Configuration**, click **Archiving**.

b Select the **Enable Data Archiving** check box.

c In the **Archive Location** text box, enter the path in the form of `nfs://`*`nfs-server-address`*`/V2D_vRLI_MgmtA_1TB` to an NFS partition where logs will be archived.

d Click **Test** next to the **Archive Location** text box to verify that the share is accessible.

e Click **Save**.

Region A vSphere Update Manager Download Service Implementation

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 Region A.

Procedure

1. Configure PostgreSQL Database Your Linux-Based Host Operating System for UMDS in Region A

   On a virtual machine with Ubuntu 14.04 Long Term Support (LTS) where you plan to install Update Manager Download Service (UMDS), configure a PostgreSQL database instance.

2. Install UMDS on Ubuntu OS in Region A

   After you install the PostgreSQL database on the UMDS virtual machine, install the UMDS software.

3. Set Up the Data to Download with UMDS in Region A

   By default UMDS downloads patch binaries, patch metadata, and notifications for hosts. Specify which patch binaries and patch metadata to download with UMDS in Region A.

4. Install and Configure the UMDS Web Server in Region A

   The UMDS server in Region A 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 Region A

   Configure Update Manager to use the UMDS shared repository as a source for downloading ESXi patches, extensions, and notifications.

Configure PostgreSQL Database Your Linux-Based Host Operating System for UMDS in Region A

On a virtual machine with Ubuntu 14.04 Long Term Support (LTS) where you plan to install Update Manager Download Service (UMDS), configure a PostgreSQL database instance.

Prerequisites

- Create a virtual machine for UMDS on the management cluster of Region A. See *Virtual Machine Specifications* from the *Planning and Preparation* documentation.
- Verify you have PostgreSQL database user credentials.

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. In the vSphere Web Client, right-click the mgmt01umds01.sfo01.rainpole.local 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 14.04	`/etc/postgresql/`*`postgres_version`*`/main`

```
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	*umds_db*	*umds_db_user*		md5

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 Region A

After you install the PostgreSQL database on the UMDS virtual machine, 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 mgmt01umds01.sfo01.rainpole.local.

   b Log in using the following credentials.

Setting	Value
User name	svc-umds
Password	*svc-umds_password*

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 -xzvf /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	UMDS_DSN
Provide the database username	*umds_db_user*
Provide the database password	*umds_db_user_password*

10 Type **yes** and press Enter to install UMDS.

Set Up the Data to Download with UMDS in Region A

By default UMDS downloads patch binaries, patch metadata, and notifications for hosts. Specify which patch binaries and patch metadata to download with UMDS in Region A.

Procedure

1. Log in to the UMDS virtual machine by using a Secure Shell (SSH) client.
   a. Open an SSH connection to mgmt01umds01.sfo01.rainpole.local.
   b. Log in using the following credentials.

Setting	Value
User name	svc-umds
Password	*svc-umds_password*

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 of 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 Region A

The UMDS server in Region A 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 VUM instances within the region using an 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 mgmt01umds01.sfo01.rainpole.local.

   b Log in using the following credentials.

Setting	Value
User name	svc-umds
Password	*svc-umds_password*

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 mgmt01umds01 mgmt01umds01.sfo01.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 you can browse the files on the UMDS Web server by opening a Web browser to **http://mgmt01umds01.sfo01.rainpole.local**.

Use the UMDS Shared Repository as the Download Source in Update Manager in Region A

Configure Update Manager to use the UMDS shared repository 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://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, click the **Update Manager** icon.

3 From the **Objects** tab, click the **mgmt01vc01.sfo01.rainpole.local** vCenter Server for Region A.

   The **Objects** tab also displays all the vCenter Server system to which an Update Manager instance is connected.

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://mgmt01umds01.sfo01.rainpole.local

The vSphere Web Client performs validation of the URL.

7 In the **Download sources** page, click **Download Now** to run the download patch definitions.

8 If you are deploying the management components in Region A, repeat the procedure to configure the http://mgmt01umds01.sfo01.rainpole.local repository for the comp01vc01.sfo01.rainpole.local vCenter Server.