VMware Cloud Foundation Site Protection and Disaster Recovery Guide

VMware Cloud Foundation 3.7

vmware®

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

https://docs.vmware.com/

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

docfeedback@vmware.com

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

Contents

About Site Protection and Recovery for VMware Cloud Foundation

Site Protection and Recovery for VMware Cloud Foundation provides step-by-step instructions about adapting a dual-region software-defined data center (SDDC) on top of VMware Cloud Foundation for disaster recovery of VMware management components.

You use VMware Site Recovery Manager and VMware vSphere Replication to perform site protection and recovery of the Cloud Management Platform that consists of vRealize Automation with embedded vRealize Orchestrator, and of the vRealize Operations Manager analytics cluster.

While not directly documented, this document can be used to protect workload domains across regions as well.

The documentation covers both failover to the recovery region and failback to the protected region.

Intended Audience

The *Site Protection and Recovery for VMware Cloud Foundation* documentation is intended for cloud architects, infrastructure administrators, cloud administrators and cloud operators 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 disaster recovery.

Required VMware Software

The *Site Protection and Recovery for VMware Cloud Foundation* documentation is compliant and validated with VMware Cloud Foundation 3.5.x.

Performing SDDC Failover and Failback

After you configure the SDDC for disaster recovery, for information about failover or failback of the components of the Cloud Management Platform or vRealize Operations Manager, see the *Site Protection and Recovery* documentation in VMware Validated Design for Software-Defined Data Center 4.2.

Prerequisites for Implementing Disaster Recovery on VMware Cloud Foundation

1

Before you implement disaster recovery in VMware Cloud Foundation, your environment must support certain prerequisites for deployment and networking.

You implement disaster recovery on vRealize Automation and the vRealize Operations Manager analytics cluster. You can apply the guidance for protecting workloads in Cloud Foundation workload domains. Both scenarios, management stack disaster recovery and workload disaster recovery, are validated and require the following prerequisites.

Disaster Recovery Considerations

When you prepare for disaster recovery, you must determine which of your two Cloud Foundation instances will function as the protected site and which one as the recovery site.

The protected site hosts the business-critical SDDC services. In the context of Cloud Foundation, the protected site contains the vRealize products, including vRealize Operations Manager and vRealize Automation, and tenant workloads with failover that is enabled in the event of a disaster.

The recovery site is an alternative location to which these vRealize applications and tenant workloads, if the latter is configured, are migrated and hosted in the event of a disaster.

In this guide, the protected site is referred to as Region A and the recovery site is referred to as Region B.

Disaster Recovery Prerequisites

Before you implement disaster recovery, verify that your environment satisfies the following prerequisites:

- In each region, provide the Windows virtual machine and environment configuration for Site Recovery Manager deployment.

Attribute	Site Recovery Manager
Guest OS	Windows Server 2012 R2 (64-bit)
Cluster	vRack-Cluster
Datastore	vsanDatastore
Number of CPUs	2
Memory (GB)	4
Disk space (GB)	40

Attribute	Site Recovery Manager
SCSI Controller	LSI Logic SAS
Virtual machine network adapter	VMXNET3
Virtual machine network	vRack-DPortGroup-Mgmt
Active Directory domain	*Subdomain of the Cloud Foundation instance*
Service account	Windows administrator
VMware Tools	Latest version

Download Site Recovery Manager 6.5.1 installer to both VMs.

- In each region, provide the environment configuration for deploying the vSphere Replication virtual appliance.

Attribute	Site Recovery Manager
Cluster	vRack-Cluster
Datastore	vsanDatastore
Number of CPUs	2
Memory (GB)	4
Disk space (GB)	18
SCSI Controller	LSI Logic SAS
Virtual machine network adapter	VMXNET3
Virtual machine network	vRack-DPortGroup-Mgmt

Download the vSphere Replication 6.5.1 `.iso` image and mount it on the machine that you use to access the vSphere Web Client.

- Obtain a license for Site Recovery Manager.

Cloud Foundation Prerequisites

- Verify that VMware Cloud Foundation is version 2.3.1 or later.
- Verify that you have obtained a Cloud Foundation license that covers the use of cross-vCenter NSX objects.
- Deploy vRealize Automation and vRealize Operations Manager after you deploy or upgrade Cloud Foundation to 2.3.1. vRealize Automation and vRealize Operations Manager are deployed in Region A.
- Temporarily migrate all virtual machines on NSX logical switches to VLAN-backed distributed port groups to keep their connectivity and disconnect the virtual machines from the logical switches. You can reconnect these virtual machines to the logical switches after NSX is configured for cross vCenter Server operations.

Networking Prerequisites

- The regions must be connected to each other and the connection must support jumbo frames and Layer 3 routing between the regions.
- All uplinks, port channels, and VLANs that carry VXLAN and vSphere Replication traffic must be configured for jumbo frames.
- The maximum supported latency between regions must be 150 ms.
- Sufficient bandwidth must be available for replication traffic. See VMware Knowledge Base article 2037268 to determine the required bandwidth for your workloads.
- BGP must be licensed and available for use on the Layer 3 devices in both regions.
- Nexus switches must be updated to a Nexus OS release that supports routing protocol adjacencies over virtual port channels. See https://www.cisco.com/c/en/us/support/docs/ip/ip-routing/118997-technote-nexus-00.html for the minimum required Nexus OS release and additional configuration required.

Prepare NSX for Cross-Region Support

2

The first step in configuring disaster recovery is to configure cross-region NSX to enable workload mobility.

Configure NSX for cross-region support of universal objects. Due to the default configuration of NSX within VMware Cloud Foundation, NSX must be reconfigured to support universal objects. If you select to use default networks during VMware Cloud Foundation bring-up, you must remove NSX objects that were deployed and you must update the hosts VTEPs to use unique routable IP addresses.

Note NSX cross-site on the management domain is not supported within a rack.

Procedure

1 Assign the Primary Role to NSX Manager in Region A

   Assign NSX Manager the primary role to enable universal networking objects that are used across all primary and secondary NSX instances in the protected and recovery regions. Set a universal Segment ID pool to define the range of VXLANs that are available to cross-region logical segments.

2 Create a Universal Transport Zone in Region A

   A transport zones controls to which hosts a logical switch can reach. Create a universal transport zone so that logical switches can connect to all hosts for disaster recover.

3 Delete the NSX Controllers in Region B

   For a dual-region setup, cross-vCenter NSX controllers are deployed only in the region that contains the primary NSX Manager. You must remove the NSX controller cluster in the recovery region.

4 Assign the Secondary Role to NSX Manager in Region B

   To enable cross-vCenter NSX networking, configure the NSX Manager in Region B as a secondary. You perform this operation from the primary NSX Manager which is in Region A. You join the management cluster in Region B to the universal transport zone from the local vCenter Server.

Assign the Primary Role to NSX Manager in Region A

Assign NSX Manager the primary role to enable universal networking objects that are used across all primary and secondary NSX instances in the protected and recovery regions. Set a universal Segment ID pool to define the range of VXLANs that are available to cross-region logical segments.

Procedure

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

   a Open a Web browser and go to `https://vcenter_server_address_region_A/vsphere-client`.

   b Log in using the following credentials.

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

2 Assign the primary role to the management NSX Manager.

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

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

   c On the **Management** tab, select the management NSX Manager and select **Actions > Assign Primary Role**.

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

3 Right-click **Mgmt Universal Transport Zone** and select **Enable CDO Mode**.

4 Create a universal Segment ID pool.

   a On the **Installation and Upgrade** tab, click the **Logical Network Settings** tab and click **Segment ID**.

   b Select the management NSX Manager from the drop-down menu.

   c Under the **Universal Segment ID pool and Multicast range** section, click **Edit**, enter `12000-12999` for the **Universal Segment ID Pool**, and click **OK**.

5 Repeat Step 2 and Step 4 for any workload domains you want to configure for disaster recovery.

   Use a different Segment ID pool range for each workload domain.

Create a Universal Transport Zone in Region A

A transport zones controls to which hosts a logical switch can reach. Create a universal transport zone so that logical switches can connect to all hosts for disaster recover.

Procedure

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

   a Open a Web browser and go to `https://vcenter_server_address_region_A/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 In the **Navigator**, click **Installation and Upgrade**.

4 On the **Logical Network Settings** tab, click **Transport Zones**.

5 From the **NSX Manager** drop down menu, select the IP address of the management NSX Manager.

6 Click the **New Transport Zone** icon.

7 In the **New Transport Zone** dialog box, enter the following settings.

Setting	Value
Mark this object for Universal Synchronization	Selected
Name	Mgmt Universal Transport Zone
Replication mode	Hybrid

8 Select the clusters to be a part of the transport zone and click **OK**.

9 (Optional) Repeat the procedure for workload domains that you want to configure for disaster recovery.

Delete the NSX Controllers in Region B

For a dual-region setup, cross-vCenter NSX controllers are deployed only in the region that contains the primary NSX Manager. You must remove the NSX controller cluster in the recovery region.

Procedure

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

   a Open a Web browser and go to `https://vcenter_server_address_region_B/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 In the **Navigator**, click **Installation and Upgrade**.

4 On the **Management** tab, under **NSX Controller nodes** select an NSX Controller and click the **Delete** icon.

5 Delete the remaining two controllers.

When you delete the last controller, select the **Forcefully Delete** option.

6 (Optional) Repeat the procedure for workload domains that you want to configure for disaster recovery.

Assign the Secondary Role to NSX Manager in Region B

To enable cross-vCenter NSX networking, configure the NSX Manager in Region B as a secondary. You perform this operation from the primary NSX Manager which is in Region A. You join the management cluster in Region B to the universal transport zone from the local vCenter Server.

Procedure

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

a Open a Web browser and go to `https://vcenter_server_address_region_A/vsphere-client`.

b Log in using the following credentials.

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

2 Assign the secondary role to the Management NSX Manager in Region B.

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

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

c On the **Management** tab, select the management NSX instance.

d Select **Actions > Add Secondary NSX Manager**.

e In the **Add Secondary NSX Manager** dialog box, enter the following settings and click **OK**.

Setting	Value
NSX Manager	*IP address of management NSX Manager in Region B*
User name	admin
Password	*mgmtnsx_admin_password*
Confirm Password	*mgmtnsx_admin_password*

f In the **Trust Certificate** confirmation dialog box, click **Yes**.

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

   a Open a Web browser and go to `https://vcenter_server_address_region_B/vsphere-client`.

   b Log in using the following credentials.

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

4 Change the Segment ID allocation.

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

   b Click **Installation and Upgrade** and select the NSX Manager in Region B from the **NSX Manager** drop-down menu.

   c click the **Logical Network Settings** and navigate to **VXLAN Settings > Segment IDs**.

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

Setting	Value
Segment ID pool	6000-6200
Enable Multicast addressing	Selected
Multicast addresses	239.5.0.0-239.5.255.255

5 In vCenter Server in Region B, add the management cluster in Region B to the Mgmt Universal Transport Zone.

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

   b Select the NSX Manager in Region B from the **NSX Manager** drop-down menu.

   c Select **Mgmt Universal Transport Zone** and click the **Connect Clusters** icon.

   d In the **Connect Clusters** dialog box, select the management cluster in Region B and click **OK**.

6 Repeat the procedure for workload domains that you want to configure for disaster recovery.

Configure Dynamic Routing

3

Dynamic routing enables the dynamic discovery of the IP subnets configured on NSX virtual wires by the physical network and vice versa.

Procedure

1 Configure dynamic routing for the management cluster in Region A.

See Configure NSX Dynamic Routing in the Management Cluster in Region A in VMware Validated Design for Software-Defined Data Center.

Note When you follow the instructions for enabling and configuring routing in Region A, add static routes to vRealize network SVI on the 172.x.x.x network instead of the 192.168.x.x network. This is because the vRealize network in Cloud Foundation is on the 172.x.x.x network.

2 Configure dynamic routing for the management cluster in Region B.

See Configure NSX Dynamic Routing in the Management Cluster in Region B in VMware Validated Design for Software-Defined Data Center.

3 (Optional) Configure dynamic routing for a workload domain in Region A.

See Configure NSX Dynamic Routing in the Shared Edge and Compute Cluster in Region A in VMware Validated Design for Software-Defined Data Center.

4 (Optional) Configure dynamic routing for a workload domain in Region B.

See Configure NSX Dynamic Routing in the Shared Edge and Compute Cluster in Region B in VMware Validated Design for Software-Defined Data Center.

Update the NTP Sources on vRealize Operations Manager in Region A

4

Before you fail over vRealize Operations Manager between regions, update the NTP synchronization settings with an NTP server in each region.

Procedure

1. Log in to the master node of vRealize Operations Manager by using a Secure Shell (SSH) client in Region A.
   a. Open an SSH session to the vrops-master.*domain.local* virtual machine.
   b. Log in using the following credentials.

Setting	Value
User name	root
Password	*vrops_root_password*

2. Open the `/etc/ntp.conf` file in edit mode.

```
vi /etc/ntp.conf
```

3. Locate the `## CaSA Section Start #` section of the file.
4. Under the `server` *`ip-address`* `iburst prefer` line, add the following new line.

```
server ip-address-NTP-server-RegionB iburst prefer
```

   where *ip-address-NTP-server-RegionB* is the IP address of the designated NTP server in Region B.

5. Save the file.

```
!wq
```

6. Restart the NTP daemon.

```
service ntp restart
```

7. Repeat the procedure for the master replica and all data nodes.

Place the Virtual Machines of a Management Solution in a Dedicated Folder

5

Virtual machine folders provide a logical grouping of virtual machines. You use place the virtual machines of vRealize Automation and of vRealize Operations Manager in own folder. You later create a mapping between these folders in Site Recovery Manager as a part of the failover setup.

This chapter includes the following topics:

Move the Virtual Machines of vRealize Automation and vRealize Operations Manager to Dedicated Folders in Region A

Create folders to group the virtual machines of vRealize Automation and vRealize Operations Manager, and move the virtual machines there. You use the folders for easier configuration of virtual machine replication.

Procedure

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

   a Open a Web browser and go to `https://vcenter_server_address_region_A/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 vRealize Automation and vRealize Operations Manager virtual machines.
   a In the **Navigator**, click **VMs and Templates** and expand the vCenter Server tree.
   b Right-click the **vRack-Datacenter** data center object and select **New Folder > New VM and Template Folder**.
   c In the **New Folder** dialog box, enter ***regiona*–m01fd–vra** as the folder name and click **OK**.

      where *regiona* is the subdomain of this Cloud Foundation instance, for example, `sfo01`.
   d Create another folder named ***regiona*–m01fd–vrops**.
3 Move the vRealize Automation virtual machines to the *regiona*–m01fd–vra folder.
   a In the **Navigator**, click **VMs and Templates** and expand the vCenter Server tree.
   b Click the vCenter Server object and click the **VMs** tab.
   c Select all vRealize Automation virtual machines and drag them to the ***regiona*-m01fd-vra** folder.
4 Move the vRealize Operations Manager virtual machines to the *regiona*–m01fd–vrops folder.
   a In the **Navigator**, click **VMs and Templates** and expand the vCenter Server tree.
   b Click the vCenter Server object and click the **VMs** tab.
   c Select all vRealize Operations Manger virtual machines and drag them to the ***regiona*-m01fd-vrops** folder.

Create Virtual Machine Folders for vRealize Automation and vRealize Operations Manager in Region B

Create folders to group the virtual machines of vRealize Automation and vRealize Operations Manager, and move the virtual machines there. You use the folders in folder mapping when a failover between the regions occurs.

Procedure

1 Log in to Management vCenter Server by using the vSphere Web Client.
   a Open a Web browser and go to **https://*vcenter_server_address_region_B*/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 vRealize Automation and vRealize Operations Manager virtual machines.

   a In the **Navigator**, click **VMs and Templates** and expand the vCenter Server tree.

   b Right-click the **vRack-Datacenter** data center object and select **New Folder > New VM and Template Folder**.

   c In the **New Folder** dialog box, enter ***regionb*-m01fd-vra** as the folder name and click **OK**.

   where *regionb* is the subdomain of this Cloud Foundation instance, for example, `lax01`.

   d Create another folder named ***regionb*-m01fd-vrops**.

Install Site Recovery Manager

6

You deploy Site Recovery Manager in each region for failover of critical applications from Region A to Region B in the cases of disaster or planned migration.

Procedure

1 Install Site Recovery Manger in Region A.

  See Install Site Recovery Manager in Region A in VMware Validated Design for Software-Defined Data Center.

2 Install Site Recovery Manger in Region B.

  See Install Site Recovery Manager in Region B in VMware Validated Design for Software-Defined Data Center.

3 Configure site pairing in Site Recovery Manager. follow the procedures in the VMware Validated Design: Configure the Site Recovery Manager Instances

  See Configure the Site Recovery Manager Instances in VMware Validated Design for Software-Defined Data Center.

  Note Because Cloud Foundation installs both regions with the same host names, the Platform Services Controller instances in the two regions cannot be joined to your Active Directory domain. When you follow the procedures in VMware Validated Design or Software-Defined Data Center, replace the Active Directory service accounts with a local vCenter Single Sign-On account such as **administrator@vsphere.local**.

4 Repeat this process for any workload domains that you want to protect. Site Recovery Manager has a one-to-one relationship with vCenter Server.

Deploy vSphere Replication

7

You deploy and configure vSphere Replication to enable replication of critical virtual machine data from Region A to Region B for failover by using Site Recovery Manager in the cases of disaster or planned migration.

Procedure

1 Deploy vSphere Replication in Region A.

Perform the procedures in Deploy vSphere Replication in Region A in VMware Validated Design for Software-Defined Data Center providing the following settings.

Setting	Value
Folder	Management VMs
Resource	SDDC-Management-ResourcePool
Management network destination	vRack-DPortGroup-Mgmt

2 Deploy vSphere Replication in Region B.

Perform the procedures in Deploy vSphere Replication in Region B in VMware Validated Design for Software-Defined Data Center providing the following settings.

Setting	Value
Folder	Management VMs
Resource	SDDC-Management-ResourcePool
Management network destination	vRack-DPortGroup-Mgmt

3 Connect the vSphere Replication instances.

Perform the procedures in Connect the vSphere Replication Instances in VMware Validated Design for Software-Defined Data Center.

4 (Optional) Repeat this process for workload domains that you want to protect.

Prepare the Environment for vSphere Replication Traffic

8

You replicate virtual machine data from the protected region to the recovery region by using vSphere Replication. vSphere Replication traffic must be route-able between regions. Configure data center networks and VMkernel adapters on the management hosts to enable vSphere Replication data transfer between regions.

Prerequisites

vSphere Replication traffic must be route-able between both regions. Create a data center network for routing vSphere Replication traffic outside of the Cloud Foundation instance in both regions.

Procedure

1 Create a VMkernel Adapter for vSphere Replication in Region A

   Create VMkernel adapters to isolate the incoming replication traffic on target ESXi hosts and connect the adapters to the data center network that is allocated for replication traffic.

2 Create a VMkernel Adapter for vSphere Replication in Region B

   Create VMkernel adapters to isolate the incoming replication traffic on target ESXi hosts and connect the adapters to the data center network that is allocated for replication traffic.

3 Isolate the Network Traffic of vSphere Replication

   vSphere Replication consumes a lot of bandwidth during initial replication, and when virtual machines are added or destroyed. To avoid network problems in the data center, isolate replication traffic from other network traffic.

Create a VMkernel Adapter for vSphere Replication in Region A

Create VMkernel adapters to isolate the incoming replication traffic on target ESXi hosts and connect the adapters to the data center network that is allocated for replication traffic.

Procedure

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

   a Open a Web browser and go to `https://vcenter_server_address_region_A/vsphere-client`.

   b Log in using the following credentials.

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

2 Create a VMkernel adapter for vSphere Replication on each host.

   a Select **Home > Hosts and Clusters**.

   b Expand the vCenter Server tree and select a management host in the **vRack-Cluster** cluster.

   c Click the **Configure** tab and under **Networking** select **VMkernel adapters**.

   d Click the **Add host networking** icon.

   e On the **Select connection type** page of the **Add Networking** wizard, select **VMkernel Network Adapter** and click **Next**.

   f On the **Select Target Device** page, click **Browse** next to **Select an existing network**, select the data center network previously allocated for vSphere Replication, click **OK**, and click **Next**.

   g On the **Port Properties** dialog box, select the **vSphere Replication** and **vSphere Replication NFC** check boxes, and click **Next**.

   h On the **IPv4 setting** page, select **Use static IPv4 settings**, enter the IPv4 settings for routing of replication traffic between the regions, and click **Next**.

   i On the **Ready to complete** page, verify the settings and click **Finish**.

3 Configure the MTU on the vSphere Replication VMkernel adapter.

   a On the **VMkernel adapters** page, select the newly-created VMkernel port and click the **Edit settings** icon.

   b In the **Edit Settings** dialog box, click **NIC settings**.

   c On the **NIC settings** page, change the **MTU** to `9000` and click **OK**.

4 Repeat Step 2 and Step 3 for all hosts in the management cluster.

5 Repeat the procedure for workload domains that you want to configure for disaster recovery.

Create a VMkernel Adapter for vSphere Replication in Region B

Create VMkernel adapters to isolate the incoming replication traffic on target ESXi hosts and connect the adapters to the data center network that is allocated for replication traffic.

Procedure

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

   a Open a Web browser and go to `https://vcenter_server_address_region_B/vsphere-client`.

   b Log in using the following credentials.

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

2 Create a VMkernel adapter for vSphere Replication on each host.

   a Select **Home > Hosts and Clusters**.

   b Expand the vCenter Server tree and select a management host in the **vRack-Cluster** cluster.

   c Click the **Configure** tab and under **Networking** select **VMkernel adapters**.

   d Click the **Add host networking** icon.

   e On the **Select connection type** page of the **Add Networking** wizard, select **VMkernel Network Adapter** and click **Next**.

   f On the **Select Target Device** page, click **Browse** next to **Select an existing network**, select the data center network previously allocated for vSphere Replication, click **OK**, and click **Next**.

   g On the **Port Properties** dialog box, select the **vSphere Replication** and **vSphere Replication NFC** check boxes, and click **Next**.

   h On the **IPv4 setting** page, select **Use static IPv4 settings**, enter the IPv4 settings for routing of replication traffic between the regions, and click **Next**.

   i On the **Ready to complete** page, verify the settings and click **Finish**.

3 Configure the MTU on the vSphere Replication VMkernel adapter.

   a On the **VMkernel adapters** page, select the newly-created VMkernel port and click the **Edit settings** icon.

   b In the **Edit Settings** dialog box, click **NIC settings**.

   c On the **NIC settings** page, change the **MTU** to `9000` and click **OK**.

4 Repeat Step 2 and Step 3 for all hosts in the management cluster.

5 Repeat the procedure for workload domains that you want to configure for disaster recovery.

Isolate the Network Traffic of vSphere Replication

vSphere Replication consumes a lot of bandwidth during initial replication, and when virtual machines are added or destroyed. To avoid network problems in the data center, isolate replication traffic from other network traffic.

Isolating the vSphere Replication traffic also enhances network performance in the data center by reducing the impact of this traffic on other traffic types.

You isolate the network traffic to the vSphere Replication Server by dedicating a VMkernel network adapter on each management ESXi host that sends data to the vSphere Replication Server and using a dedicated network adapter on the vSphere Replication Server VM.

Procedure

- Perform Isolate the Network Traffic of vSphere Replication in VMware Validated Design for Software-Defined Data Center.

Migrate vRealize Automation and vRealize Operations Manager to the Cross-Region Application Virtual Network

9

To enable disaster recovery and workload mobility you must migrate the virtual machines from the vRealize VLAN backed network to the Mgmt-xRegion01-VXLAN VXLAN backed network.

Procedure

1 Create the Cross-Region Application Virtual Network

The cross-region application virtual network is an NSX universal logical switch that is available in both regions. Its configuration supports failover and workload migration while keeping the workload IP addresses the same.

2 Power Off the Virtual Machines of vRealize Automation and vRealize Operations Manager

Power off the vRealize Automation and vRealize Operations virtual machines to prepare them for migration to the cross-region application virtual network. The virtual machines must be powered off before migration as IP connectivity to or from the application virtual network is not available at this stage.

3 Migrate vRealize Automation and vRealize Operations Manager to the Cross-Region Application Virtual Network

Migrate the powered-off virtual machines of vRealize Automation and vRealize Operations Manager from the vRealize port group that is VLAN-backed to the cross-region application virtual network that is VXLAN-backed.

4 Shut Down and Remove the vRealize VLAN from the Physical Network

Before you bring up the IP subnet for vRealize Automation and vRealize Operations Manager, remove the deprecated vRealize VLAN from the physical network.

5 Connect the Cross-Region Application Virtual Network to the Universal Distributed Logical Router

Create an internal interface to the logical switch on the universal distributed logical router. Internal interfaces are generally for East-West traffic.

6 Power On the Virtual Machines of vRealize Automation and vRealize Operations Manager

Now that IP connectivity has been established to the vRealize Application Virtual Network you can power on the virtual machines.

7 Install the vcfvrdrhelper script in Region A

Install the `vcfvrdrhelper` script on SDDC Manager in Region A to update the vRealize port group information in SDDC Manager database in Region A.

8 Configure the Environment After the Migration to the Cross-Region Network

After migrating and powering on the virtual machines of vRealize Automation and vRealize Operations Manager, remove the vRealize port group, enable SSL passthrough and HTTP redirects for vRealize Operations Manager the vRealize edge device.

What to do next

Create the Cross-Region Application Virtual Network

The cross-region application virtual network is an NSX universal logical switch that is available in both regions. Its configuration supports failover and workload migration while keeping the workload IP addresses the same.

Procedure

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

a Open a Web browser and go to `https://vcenter_server_address_region_A/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 **Navigator**.

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

4 From the **NSX Manager** drop-down menu, select the IP address of the Management NSX Manager.

5 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

6 Repeat the procedure for workload domains that you want to configure for disaster recovery.

Power Off the Virtual Machines of vRealize Automation and vRealize Operations Manager

Power off the vRealize Automation and vRealize Operations virtual machines to prepare them for migration to the cross-region application virtual network. The virtual machines must be powered off before migration as IP connectivity to or from the application virtual network is not available at this stage.

Procedure

1. Log in to Management vCenter Server by using the vSphere Web Client.
   a. Open a Web browser and go to `https://vcenter_server_address_region_A/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 **VMs and Templates**.
3. Select the *regiona*-m01fd-vrops folder and click the **VMs** tab.
4. Power off the vRealize Operations Manager virtual machines in the following order.
   - vRealize Operations Manager Data Nodes
   - vRealize Operations Manager Replica
   - vRealize Operations Manager Master
5. Select the *regiona*-m01fd-vra folder and click the **VMs** tab.
6. Power off the vRealize Automation virtual machines in the following order.
   - vRealize Automation Distributed Execution Manager (DEM) Workers
   - vRealize Automation DEM Orchestrator
   - vRealize Automation Infrastructure Manager Service
   - vRealize Automation Infrastructure Web Servers
   - vRealize Automation Appliances
   - Microsoft SQL Server

Migrate vRealize Automation and vRealize Operations Manager to the Cross-Region Application Virtual Network

Migrate the powered-off virtual machines of vRealize Automation and vRealize Operations Manager from the vRealize port group that is VLAN-backed to the cross-region application virtual network that is VXLAN-backed.

Procedure

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

   a Open a Web browser and go to `https://vcenter_server_address_region_A/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**.

3 Expand the Management vCenter Servers tree.

4 Right-click the **vRack-DSwitch** distributed switch and select **Migrate VMs to Another Network**.

5 On the **Select source and destination networks** page of the **Migrate VMs to Another Network** wizard, configure the following networks and click **Next**.

   a Under **Source network**, click **Browse** for the **Specific network**, select the **vRack-DPortGroup-vRealize** port group and click **OK**

   b Next to **Destination Network**, click **Browse**, select the port group that ends with `Mgmt-xRegion01-VXLAN` and click **OK**.

   This port group represents the cross-region application virtual network.

6 On the **Select VMs to Migrate** page, select all vRealize virtual machines, including the load balancers (**vRealize-Edge-0** and **vRealize-Edge-1**), and click **Next**.

7 On the **Ready to complete** page, verify the changes and click **Finish**.

Shut Down and Remove the vRealize VLAN from the Physical Network

Before you bring up the IP subnet for vRealize Automation and vRealize Operations Manager, remove the deprecated vRealize VLAN from the physical network.

You remove the vRealize VLAN from the physical network according to the physical network topology and vendors used. As a result, you must perform a procedure according your network setup.

Consider the following high-level process:

- Log in to the switch that contains the SVI (default gateway) for the vRealize VLAN and delete the SVI and VLAN.
- Delete the VLAN from all switches in the environment.
- Delete the VLAN from the trunk ports on the ESXi hosts.

Connect the Cross-Region Application Virtual Network to the Universal Distributed Logical Router

Create an internal interface to the logical switch on the universal distributed logical router. Internal interfaces are generally for East-West traffic.

Procedure

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

   a Open a Web browser and go to `https://vcenter_server_address_region_A/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 In the **Navigator**, click **NSX Edges** and select the IP address of the management NSX Manager from the **NSX Manager** drop-down box.

4 Double-click the universal distributed logical router to open its settings.

5 On the **Manage** tab, click the **Settings** tab and select **Interfaces**.

6 Click the **Add** icon, in the **Add Logical Router Interface** dialog box, enter the following values, and click **OK**.

Setting	Value
Name	`Mgmt-xRegion01-VXLAN`
Type	Internal
Connected To	Mgmt-xRegion01-VXLAN
Primary IP Address / Subnet Prefix Lengh	*IP address and subnet prefix lengh from deleted vRealize SVI*
MTU	9000

Power On the Virtual Machines of vRealize Automation and vRealize Operations Manager

Now that IP connectivity has been established to the vRealize Application Virtual Network you can power on the virtual machines.

Prerequisites

If the Microsoft SQL Server was not on the vRealize VLAN it must be brought up first and have its IP changed. After changing the SQL servers IP address verify the updated IP address is resolvable via DNS.

Procedure

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

   a Open a Web browser and go to `https://vcenter_server_address_region_A/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 **VMs and Templates**.

3 Select the *regiona*-m01fd-vrops folder and click the **VMs** tab.

4 Power on the vRealize Operations Manager virtual machines in the following order.

   - vRealize Operations Manager Master
   - vRealize Operations Manager Replica
   - vRealize Operations Manager Data Nodes

5 Select the *regiona*-m01fd-vra folder and click the **VMs** tab.

6 Power on the vRealize Automation virtual machines in the following order.

   - Microsoft SQL Server
   - vRealize Automation Appliances
   - vRealize Automation Infrastructure Web Servers
   - vRealize Automation Infrastructure Manager Service
   - DEM Orchestrators and DEM workers
   - vRealize Automation Distributed Execution Managers

Install the vcfvrdrhelper script in Region A

Install the `vcfvrdrhelper` script on SDDC Manager in Region A to update the vRealize port group information in SDDC Manager database in Region A.

Because the port group for the vRealize is different as a result from configuring the environment for disaster recovery, this value must be updated in the SDDC Manager database so that future vRealize deployments are in the correct port group.

Procedure

- Perform the steps in VMware Knowledge Base article 59203 to update the vRealize port group and enable DNS record replication from SDDC Manager in Region A to SDDC Manager in Region B.

Configure the Environment After the Migration to the Cross-Region Network

After migrating and powering on the virtual machines of vRealize Automation and vRealize Operations Manager, remove the vRealize port group, enable SSL passthrough and HTTP redirects for vRealize Operations Manager the vRealize edge device.

Procedure

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

   a Open a Web browser and go to `https://vcenter_server_address_region_A/vsphere-client`.

   b Log in using the following credentials.

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

2 Delete the vRealize port group from the vSphere Distributed Switch.

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

   b Expand the Management vCenter Server tree.

   c Right-click the **vRack-DPortGroup-vRealize** port group of the **vRack-DSwitch** switch and select **Delete** and confirm.

3 Enable SSL Passthrough on the VROPS_HTTPS Application Profile on the vRealize-Edge.

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

   b Click **NSX Edges** and select the IP address of the Management Manager from the **NSX Manager** drop-down box.

   c Double-click **vRealize-Edge** to open its settings.

   d On the **Manage** tab, click the **Load Balancer** tab.

   e Select **Application Profiles**, select **VROPS_HTTPS**, and click the **Edit** icon.

   f In the **Edit Profile** dialog box, deselect the **Configure Service Certificate**, select the **Enable SSL Passthrough** check box, and click **OK**.

4 Reconfigure for HTTP on the VROPS_REDIRECT Application Profile on the vRealize-Edge.

   a On the Load Balancer page for the **vRealize-Edge**, select **Application Profiles**, select **VROPS_REDIRECT**, and click the **Edit** icon.

   b In the **Edit Profile** dialog box, select **HTTP** from the **Type** drop-down menu, and click **OK**.

Create the NSX Load Balancer for vRealize Automation and vRealize Operations Manager in Region B

10

The NSX load balancer used for vRealize virtual machines can not be failed over, as such one must be configured in Region B to support the load balancing requirements of these applications.

Procedure

1 Deploy the NSX Edge for Load Balancing vRealize Automation and vRealize Operations Manager in Region B

Deploy a load balancer for use by management applications connected to the application virtual network Mgmt-xRegion01-VXLAN after their failover to Region B.

2 Disable the Interface on the vRealize NSX Edge Load Balancer in Region B

Because the load balancers in Region A and Region B have the same IP addresses, the load balancer in Region B must have its interface disconnected until a disaster recovery event occurs.

3 Configure the NSX Load Balancer for vRealize Automation and vRealize Operations Manager in Region B

Configure the NSX Edge to perform load balancing for vRealize Automation and vRealize Operations Manager when those applications are running in Region B.

Deploy the NSX Edge for Load Balancing vRealize Automation and vRealize Operations Manager in Region B

Deploy a load balancer for use by management applications connected to the application virtual network Mgmt-xRegion01-VXLAN after their failover to Region B.

Procedure

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

   a Open a Web browser and go to `https://vcenter_server_address_region_B/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 Edges** and select the IP address of the management NSX Manager from the **NSX Manager** drop-down box.

4 Click the **Add** icon to create a new NSX Edge.

5 On the **Name and Description** page, enter the following settings, and click **Next**.

Setting	Value
Install Type	Edge Services Gateway
Name	vRealize-Edge
Deploy NSX Edge	Selected
Enable High Availability	Selected

6 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

7 On the **Configure Deployment** page, perform the following configuration steps, and click **Next**.

a Select **vRack-Datacenter** from the **Datacenter** drop-down menu.

b Select the **Large** radio button to specify the **Appliance Size**.

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

Perform twice to add two NSX Edge appliances with the same settings.

Setting	Value
Resource pool	Network-ResourcePool
Datastore	vsanDatastore
Folder	Networking VMs
Resource Reservation	System Managed

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

Setting	Value
Name	mgmt-vnic-vrealize-edge
Type	Internal
Connected To	Mgmt-xRegion01-VXLAN
Connectivity Status	Connected
Primary IP Address	Same as vRealize-Edge in Region A
Secondary IP Addresses	Same as vRealize-Edge in Region A
Subnet Prefix Length	Same as vRealize-Edge in Region A
MTU	9000
Send ICMP Redirect	Selected

9 On the **Configure Default Gateway** page, enter the default gateway for the vRealize network and enter `9000` for the **MTU** and click **Next**.

10 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

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

12 Enable HA logging.

   a On the **NSX Edges** page, double-click **vRealize-Edge** to open its settings.

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

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

   d Select the **Enable Logging** check box and click **OK**.

Disable the Interface on the vRealize NSX Edge Load Balancer in Region B

Because the load balancers in Region A and Region B have the same IP addresses, the load balancer in Region B must have its interface disconnected until a disaster recovery event occurs.

Procedure

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

   a Open a Web browser and go to `https://vcenter_server_address_region_B/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 Edges** and select the IP address of the Management NSX Manager from the **NSX Manager** drop-down box.

4 Double-click **vRealize-Edge**.

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

6 Click **Interfaces**, select the **mgmt-vnic-vrealize-edge** vNIC, and click **Edit**.

7 In the **Edit NSX Edge Interface** dialog box, set **Connectivity Status** to **Disconnected** and click **OK**.

Configure the NSX Load Balancer for vRealize Automation and vRealize Operations Manager in Region B

Configure the NSX Edge to perform load balancing for vRealize Automation and vRealize Operations Manager when those applications are running in Region B.

Procedure

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

   a Open a Web browser and go to `https://vcenter_server_address_region_B/vsphere-client`.

   b Log in using the following credentials.

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

2 Get the edge-id for the vRealize-Edge load balancer.

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

   b Click **NSX Edges** and select the IP address of the Management NSX Manager from the **NSX Manager** drop-down box.

   c Write down the ID listed in the **Id** field for the **vRealize-Edge**.

3 Use a REST client to retrieve the load balancer configuration from the vRealize-Edge load balancer in Region A.

a Using a REST client, send a `GET https://Region-A-NSX-Manager/api/4.0/edges/edge-id/loadbalancer/config`.

Where *Region-A-NSX-Manager* is the IP address of the Management NSX Manager in Region A and *edge-id* is the ID that you have written down.

For example, the output could be as follows:

```
<?xml version="1.0" encoding="UTF-8"?>
<loadBalancer>
    <version>55</version>
    <enabled>true</enabled>
    <enableServiceInsertion>false</enableServiceInsertion>
    <accelerationEnabled>true</accelerationEnabled>
    <virtualServer>
        <virtualServerId>virtualServer-4</virtualServerId>
        <name>vs_iaas-manager_443</name>
        <enabled>true</enabled>
        <ipAddress>20.1.8.10</ipAddress>
        <protocol>https</protocol>
        <port>443</port>
        <connectionLimit>0</connectionLimit>
        <defaultPoolId>pool-4</defaultPoolId>
        <applicationProfileId>applicationProfile-4</applicationProfileId>
        <enableServiceInsertion>false</enableServiceInsertion>
        <accelerationEnabled>false</accelerationEnabled>
    </virtualServer>
    <virtualServer>
        <virtualServerId>virtualServer-5</virtualServerId>
        <name>vs_iaas-web_443</name>
        <enabled>true</enabled>
        <ipAddress>20.1.8.12</ipAddress>
        <protocol>https</protocol>
        <port>443</port>
        <connectionLimit>0</connectionLimit>
        <defaultPoolId>pool-5</defaultPoolId>
        <applicationProfileId>applicationProfile-5</applicationProfileId>
        <enableServiceInsertion>false</enableServiceInsertion>
        <accelerationEnabled>false</accelerationEnabled>
    </virtualServer>
    <virtualServer>
        <virtualServerId>virtualServer-6</virtualServerId>
        <name>vs_vra-va-web_443</name>
        <enabled>true</enabled>
        <ipAddress>20.1.8.11</ipAddress>
        <protocol>https</protocol>
        <port>443</port>
        <connectionLimit>0</connectionLimit>
        <defaultPoolId>pool-6</defaultPoolId>
        <applicationProfileId>applicationProfile-6</applicationProfileId>
        <enableServiceInsertion>false</enableServiceInsertion>
        <accelerationEnabled>false</accelerationEnabled>
```

```
    </virtualServer>
    <virtualServer>
        <virtualServerId>virtualServer-7</virtualServerId>
        <name>VROPS_VIRTUAL_SERVER</name>
        <enabled>true</enabled>
        <ipAddress>20.1.8.13</ipAddress>
        <protocol>https</protocol>
        <port>443</port>
        <connectionLimit>0</connectionLimit>
        <defaultPoolId>pool-7</defaultPoolId>
        <applicationProfileId>applicationProfile-7</applicationProfileId>
        <enableServiceInsertion>false</enableServiceInsertion>
        <accelerationEnabled>false</accelerationEnabled>
    </virtualServer>
    <virtualServer>
        <virtualServerId>virtualServer-8</virtualServerId>
        <name>VROPS_REDIRECT</name>
        <enabled>true</enabled>
        <ipAddress>20.1.8.13</ipAddress>
        <protocol>http</protocol>
        <port>80</port>
        <connectionLimit>0</connectionLimit>
        <applicationProfileId>applicationProfile-8</applicationProfileId>
        <enableServiceInsertion>false</enableServiceInsertion>
        <accelerationEnabled>false</accelerationEnabled>
    </virtualServer>
    <pool>
        <poolId>pool-4</poolId>
        <name>pool_iaas-manager_443</name>
        <algorithm>round-robin</algorithm>
        <transparent>false</transparent>
        <monitorId>monitor-7</monitorId>
        <member>
            <memberId>member-13</memberId>
            <ipAddress>20.1.8.6</ipAddress>
            <weight>1</weight>
            <monitorPort>443</monitorPort>
            <port>443</port>
            <maxConn>0</maxConn>
            <minConn>0</minConn>
            <condition>enabled</condition>
            <name>IaaS_Man1</name>
        </member>
        <member>
            <memberId>member-14</memberId>
            <ipAddress>20.1.8.7</ipAddress>
            <weight>1</weight>
            <monitorPort>443</monitorPort>
            <port>443</port>
            <maxConn>0</maxConn>
            <minConn>0</minConn>
            <condition>disabled</condition>
            <name>IaaS_Man2</name>
        </member>
    </pool>
```

```
    <pool>
        <poolId>pool-5</poolId>
        <name>pool_iaas-web_443</name>
        <algorithm>round-robin</algorithm>
        <transparent>false</transparent>
        <monitorId>monitor-8</monitorId>
        <member>
            <memberId>member-15</memberId>
            <ipAddress>20.1.8.4</ipAddress>
            <weight>1</weight>
            <monitorPort>443</monitorPort>
            <port>443</port>
            <maxConn>0</maxConn>
            <minConn>0</minConn>
            <condition>enabled</condition>
            <name>IaaS_Web1</name>
        </member>
        <member>
            <memberId>member-16</memberId>
            <ipAddress>20.1.8.5</ipAddress>
            <weight>1</weight>
            <monitorPort>443</monitorPort>
            <port>443</port>
            <maxConn>0</maxConn>
            <minConn>0</minConn>
            <condition>enabled</condition>
            <name>IaaS_Web2</name>
        </member>
    </pool>
    <pool>
        <poolId>pool-6</poolId>
        <name>pool_vra-va-web_443</name>
        <algorithm>round-robin</algorithm>
        <transparent>false</transparent>
        <monitorId>monitor-9</monitorId>
        <member>
            <memberId>member-17</memberId>
            <ipAddress>20.1.8.2</ipAddress>
            <weight>1</weight>
            <monitorPort>443</monitorPort>
            <port>443</port>
            <maxConn>0</maxConn>
            <minConn>0</minConn>
            <condition>enabled</condition>
            <name>vRA_VA1</name>
        </member>
        <member>
            <memberId>member-18</memberId>
            <ipAddress>20.1.8.3</ipAddress>
            <weight>1</weight>
            <monitorPort>443</monitorPort>
            <port>443</port>
            <maxConn>0</maxConn>
            <minConn>0</minConn>
            <condition>enabled</condition>
```

```
            <name>vRA_VA2</name>
        </member>
    </pool>
    <pool>
        <poolId>pool-7</poolId>
        <name>VROPS_POOL</name>
        <algorithm>leastconn</algorithm>
        <transparent>false</transparent>
        <monitorId>monitor-10</monitorId>
        <member>
            <memberId>member-38</memberId>
            <ipAddress>20.1.8.17</ipAddress>
            <weight>1</weight>
            <monitorPort>443</monitorPort>
            <port>443</port>
            <maxConn>0</maxConn>
            <minConn>0</minConn>
            <condition>enabled</condition>
            <name>vrops-data-node-2</name>
        </member>
        <member>
            <memberId>member-39</memberId>
            <ipAddress>20.1.8.16</ipAddress>
            <weight>1</weight>
            <monitorPort>443</monitorPort>
            <port>443</port>
            <maxConn>0</maxConn>
            <minConn>0</minConn>
            <condition>enabled</condition>
            <name>vrops-data-node-1</name>
        </member>
        <member>
            <memberId>member-40</memberId>
            <ipAddress>20.1.8.15</ipAddress>
            <weight>1</weight>
            <monitorPort>443</monitorPort>
            <port>443</port>
            <maxConn>0</maxConn>
            <minConn>0</minConn>
            <condition>enabled</condition>
            <name>vrops-replica</name>
        </member>
        <member>
            <memberId>member-41</memberId>
            <ipAddress>20.1.8.14</ipAddress>
            <weight>1</weight>
            <monitorPort>443</monitorPort>
            <port>443</port>
            <maxConn>0</maxConn>
            <minConn>0</minConn>
            <condition>enabled</condition>
            <name>vrops-master</name>
        </member>
    </pool>
    <applicationProfile>
```

```
        <applicationProfileId>applicationProfile-4</applicationProfileId>
        <name>IaaS Manager</name>
        <insertXForwardedFor>false</insertXForwardedFor>
        <sslPassthrough>true</sslPassthrough>
        <template>HTTPS</template>
        <serverSslEnabled>false</serverSslEnabled>
    </applicationProfile>
    <applicationProfile>
        <applicationProfileId>applicationProfile-5</applicationProfileId>
        <persistence>
            <method>sourceip</method>
            <expire>1800</expire>
        </persistence>
        <name>IaaS Web</name>
        <insertXForwardedFor>false</insertXForwardedFor>
        <sslPassthrough>true</sslPassthrough>
        <template>HTTPS</template>
        <serverSslEnabled>false</serverSslEnabled>
    </applicationProfile>
    <applicationProfile>
        <applicationProfileId>applicationProfile-6</applicationProfileId>
        <persistence>
            <method>sourceip</method>
            <expire>1800</expire>
        </persistence>
        <name>vRealize Automation VA Web</name>
        <insertXForwardedFor>false</insertXForwardedFor>
        <sslPassthrough>true</sslPassthrough>
        <template>HTTPS</template>
        <serverSslEnabled>false</serverSslEnabled>
    </applicationProfile>
    <applicationProfile>
        <applicationProfileId>applicationProfile-8</applicationProfileId>
        <persistence>
            <method>sourceip</method>
            <expire>1800</expire>
        </persistence>
        <name>VROPS_REDIRECT</name>
        <insertXForwardedFor>false</insertXForwardedFor>
        <sslPassthrough>false</sslPassthrough>
        <template>HTTPS</template>
        <serverSslEnabled>false</serverSslEnabled>
        <httpRedirect>
            <to>https://vrops-cluster.sfo01.vmw.corp/vcops-web-ent/login.action</to>
        </httpRedirect>
    </applicationProfile>
    <applicationProfile>
        <applicationProfileId>applicationProfile-7</applicationProfileId>
        <persistence>
            <method>sourceip</method>
            <expire>1800</expire>
        </persistence>
        <name>VROPS_HTTPS</name>
        <insertXForwardedFor>false</insertXForwardedFor>
        <sslPassthrough>true</sslPassthrough>
```

```
        <template>HTTPS</template>
        <serverSslEnabled>false</serverSslEnabled>
    </applicationProfile>
    <monitor>
        <monitorId>monitor-1</monitorId>
        <type>tcp</type>
        <interval>5</interval>
        <timeout>15</timeout>
        <maxRetries>3</maxRetries>
        <name>default_tcp_monitor</name>
    </monitor>
    <monitor>
        <monitorId>monitor-2</monitorId>
        <type>http</type>
        <interval>5</interval>
        <timeout>15</timeout>
        <maxRetries>3</maxRetries>
        <method>GET</method>
        <url>/</url>
        <name>default_http_monitor</name>
    </monitor>
    <monitor>
        <monitorId>monitor-3</monitorId>
        <type>https</type>
        <interval>5</interval>
        <timeout>15</timeout>
        <maxRetries>3</maxRetries>
        <method>GET</method>
        <url>/</url>
        <name>default_https_monitor</name>
    </monitor>
    <monitor>
        <monitorId>monitor-7</monitorId>
        <type>https</type>
        <interval>3</interval>
        <timeout>10</timeout>
        <maxRetries>3</maxRetries>
        <method>GET</method>
        <url>/VMPSProvision</url>
        <name>Iaas Manager</name>
        <receive>ProvisionService</receive>
    </monitor>
    <monitor>
        <monitorId>monitor-8</monitorId>
        <type>https</type>
        <interval>3</interval>
        <timeout>10</timeout>
        <maxRetries>3</maxRetries>
        <method>GET</method>
        <url>/wapi/api/status/web</url>
        <name>Iaas Web</name>
        <receive>REGISTERED</receive>
    </monitor>
    <monitor>
        <monitorId>monitor-9</monitorId>
```

```
        <type>https</type>
        <interval>3</interval>
        <timeout>10</timeout>
        <maxRetries>3</maxRetries>
        <method>GET</method>
        <url>/vcac/services/api/health</url>
        <expected>204</expected>
        <name>vRealize Automation VA Web</name>
    </monitor>
    <monitor>
        <monitorId>monitor-10</monitorId>
        <type>https</type>
        <interval>3</interval>
        <timeout>5</timeout>
        <maxRetries>2</maxRetries>
        <method>GET</method>
        <url>/suite-api/api/deployment/node/status</url>
        <name>VROPS_MONITOR</name>
        <receive>ONLINE</receive>
    </monitor>
    <logging>
        <enable>true</enable>
        <logLevel>info</logLevel>
    </logging>
</loadBalancer>
```

4 Save the output to a file.

   a Edit the file and remove the line that begins with `<version>`.

   For example, *<version>55</version>* from Step 3.

   b Save the file.

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

   a Open a Web browser and go to **`https://`*`vcenter_server_address_region_B`*`/vsphere-client`**.

   b Log in using the following credentials.

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

6 Get the edge-id for the vRealize-Edge load balancer in Region B.

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

   b Click **NSX Edges** and select the IP address of the Management NSX Manager from the **NSX Manager** drop-down box.

   c Write down the ID listed in the **Id** field for the **vRealize-Edge**.

7 Use a REST client to configure the vRealize Edge load balancer in Region B.

   a Send a `PUT https://Region-B-NSX-Manager/api/4.0/edges/edge-id/loadbalancer/config` request.

   Where *Region-B-NSX-Manager* is the IP address of the Management NSX Manager in Region B and *edge-id* is the ID from Step 6.

   b Paste the response from Step 4 in to the body of the PUT request.

   You receive a status code of `204 No Conent` as confirmation the command was successful.

8 Enable the DNS resolver on the vRealize-Edge.

   a Back in the vSphere Web Client in Region B, double-click on **vRealize-Edge**.

   b On the **Manage** tab, click the **Settings** tab, select **Configuration** and click **Change**.

   c In the **DNS Configuration** dialog box, select the **Enable DNS Service** check box.

   d Enter the IP address of SDDC Manager for **DNS Server 1** and **DNS Server 2**, and click **OK**.

Fail Over and Fail Back the SDDC Management Applications

11

After you set up two Cloud Foundation instances for disaster recovery, you can fail over vRealize Automation, vRealize Operations Manager, and workload domain virtual machines protected by vSphere Replication and Site Recovery Manager.

Perform the instructions in the *VMware Validated Design Site Protection and Recovery* documentation according to the setup of your Cloud Foundation environment.

Procedure

1 Configure Failover of Management Applications

2 Test the Failover of Management Applications

3 Perform Planned Migration of Management Applications

4 Perform Disaster Recovery of Management Applications

5 Post-Failover Configuration of Management Applications

6 Failback of the SDDC Management Applications

7 Reprotect of the SDDC Management Applications

Upgrade NSX in a Cross-Site Configuration

12

This section explains how upgrade NSX components when they are manually configured in a cross-site deployment. Perform the steps in the order in which they are documented on each workload domain in your Cloud Foundation environment.

Procedure

1 Upgrade Primary NSX Manager

Upgrade NSX Manager on the primary site.

2 Upgrade Secondary NSX Manager

Upgrade NSX Manager on the secondary site.

3 Upgrade NSX Components on Primary Site

After the secondary NSX Manager is upgraded, upgrade the remaining NSX stack on the primary site.

4 Upgrade NSX Components on Secondary Site

After the complete NSX stack is upgraded on the primary site, upgrade the remaining NSX stack on the secondary site.

Upgrade Primary NSX Manager

Upgrade NSX Manager on the primary site.

Procedure

Procedure

1 Download the appropriate install bundle.

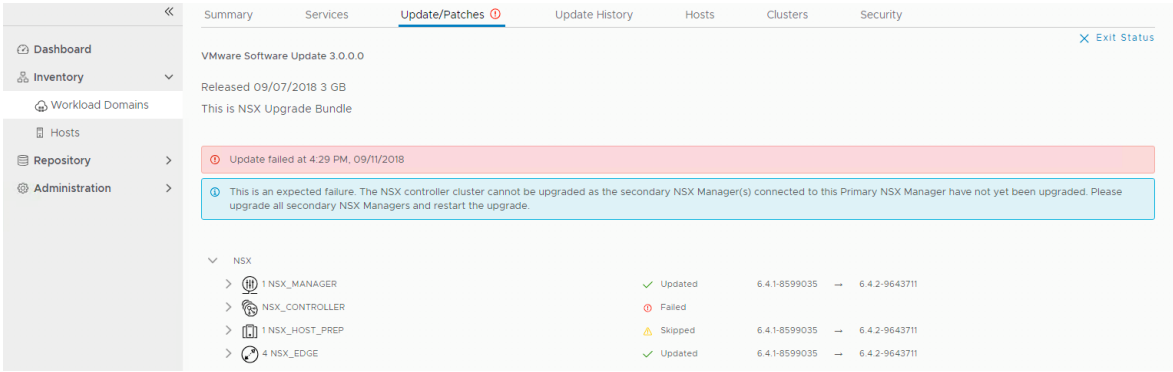
For more information, see Download LCM Bundles in the *VMware Cloud Foundation Operations and Administration Guide*.

2 Upgrade NSX Manager.

For more information, see Update Workload Domain in the *VMware Cloud Foundation Operations and Administration Guide*.

The upgrade fails during the controller upgrade. Here is a sample screenshot of what you may see.

Figure 12-1. Sample Screenshot of Failed Upgrade on Primary Site



3 Leave the upgrade on the primary site as is and proceed to the next step.

Upgrade Secondary NSX Manager

Upgrade NSX Manager on the secondary site.

Procedure

1 Download the appropriate install bundle.

For more information, see Download LCM Bundles in the *VMware Cloud Foundation Operations and Administration Guide*.

2 SSH in to the SDDC Manager VM with the vcf user name and password specified in the Deployment Parameter sheet.

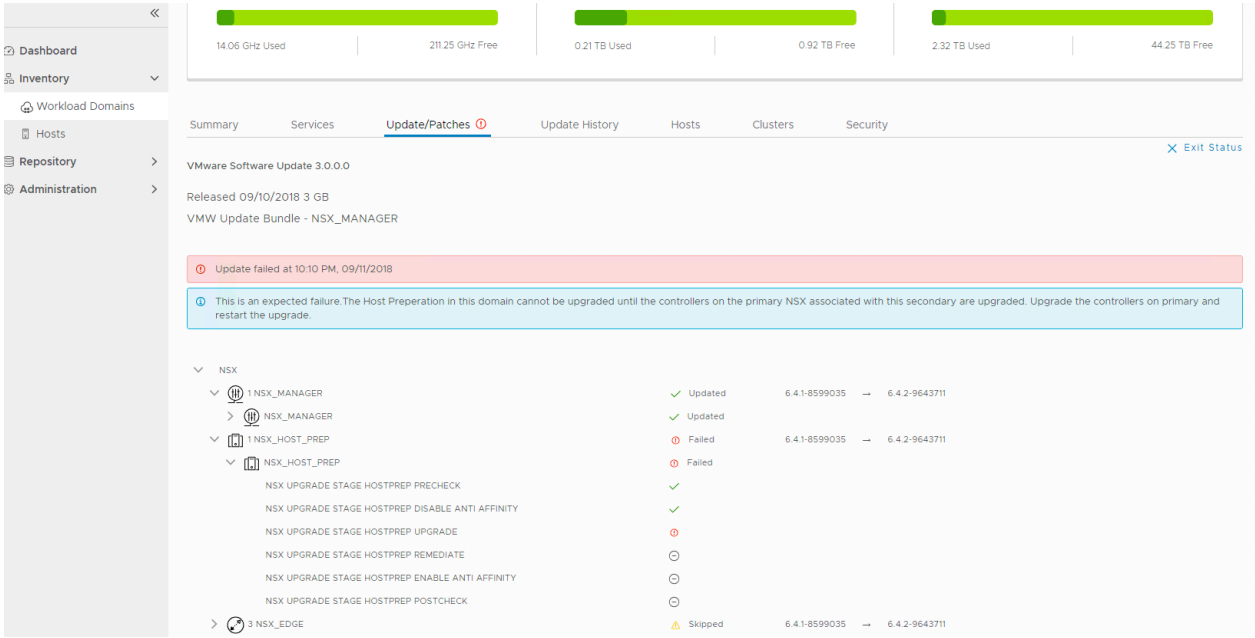
3 Run the following command.

`curl –k https://127.0.0.1/lcm/upgrades –u '`*user_name*`:`*password*`' –X POST –d '{"bundleType":"VMWARE_SOFTWARE", "bundleId":"`*bundle-id to be scheduled for update*`","scheduledTime":`*time when update should start*`,"expectedEndTime":0,"slaType":"SLOW", "vcenterIds":["`*vcenter-id for the vc where the update needs to be scheduled*`"]} ' –H 'Content–Type:application/json'`

4 Check the upgrade status on the Patches/Update tab of the workload domain on the SDDC Manager Dashboard.

NSX Manager is upgraded. Though the NSX controllers appear to be upgraded, they are skipped since there are no controllers present on the secondary site. The upgrade fails at stage `NSX upgrade stage hostprep upgrade`.

Figure 12-2. Sample Screenshot of Failed Upgrade on Secondary Site



5 Leave the upgrade on the secondary site as is and proceed to the next step.

Upgrade NSX Components on Primary Site

After the secondary NSX Manager is upgraded, upgrade the remaining NSX stack on the primary site.

Procedure

- On the Updates/Patches tab of the workload domain page on the primary site, apply the bundle or schedule it for an appropriate date and time.

  For more information, see Update Workload Domain in the *VMware Cloud Foundation Operations and Administration Guide*.

Upgrade NSX Components on Secondary Site

After the complete NSX stack is upgraded on the primary site, upgrade the remaining NSX stack on the secondary site.

Procedure

- From the SDDC Manager VM (you should be already logged in to the VM), run the following command.

  `curl –k https://127.0.0.1/lcm/upgrades –u '`*user_name*`:`*password*`' –X POST –d '{"bundleType":"VMWARE_SOFTWARE", "bundleId":"`*bundle-id to be scheduled for update*`","scheduledTime":`*time when update should start*`>,"expectedEndTime":0,"slaType":"SLOW", "vcenterIds":["`*vcenter-id for the vc where the update needs to be scheduled*`"]} ' –H 'Content–Type:application/json'`

  NSX is upgraded on both sites.

Cloud Foundation Glossary

13

Term	Description
availability zone	Collection of infrastructure components. Each availability zone is isolated from other availability zones to prevent the propagation of failure or outage across the data center.
bring-up	Initial configuration of a newly deployed Cloud Foundation system. During the bring-up process, the management domain is created and the Cloud Foundation software stack is deployed on the management domain.
commission host	Adding a host to Cloud Foundation inventory. The host remains in the free pool until it is assigned to a workload domain.
composability	Ability to dynamically configure servers to meet the needs of your workloads without physically moving any hardware components. You bind disaggregated hardware components (compute, network, storage, and offload components) together to create a logical system based on the needs of your applications.
dirty host	A host that has been removed from a cluster in a workload domain. A dirty host cannot be assigned to another workload domain until it is cleaned up.
decommission host	Remove an unassigned host from the Cloud Foundation inventory. SDDC Manager does not manage decommissioned hosts.
free pool	Hosts in the Cloud Foundation inventory that are not assigned to a workload domain
host	An imaged server.
inventory	Logical and physical entities managed by Cloud Foundation.
Lifecycle Manager (LCM)	Automates patching and upgrading of the software stack.
management domain	Cluster of physical hosts that contains the management component VMs
network pool	Automatically assigns static IP addresses to vSAN and vMotion vmkernel ports so that you don't need to enter IP addresses manually when creating a VI workload domain or adding a host or cluster to a workload domain.
patch update bundle	Contains bits to update the appropriate Cloud Foundation software components in your management or VI workload domain.
region	A Cloud Foundation instance.
SDDC Manager	Software component that provisions, manages, and monitors the logical and physical resources of a Cloud Foundation system.
SDDC Manager VM	Virtual machine (VM) that contains the SDDC Manager services and a shell from which command line tools can be run. This VM exposes the SDDC Manager UI.
server	Bare metal server in a physical rack. After imaging, it is referred to as a host.

Term	Description
unassigned host	Host in the free pool that does not belong to a workload domain.
workload domain	A policy based resource container with specific availability and performance attributes that combines vSphere, storage (vSAN or NFS) and networking (NSX for vSphere or NSX-T) into a single consumable entity. A workload domain can be created, expanded, and deleted as part of the SDDC lifecycle operations. It can contain cluster(s) of physical hosts with a corresponding vCenter to manage them. The vCenter for a workload domain physically lives in the management domain.