VMware Cloud Foundation 2.3.2.5 to 3.5.1 Upgrade Guide

VMware Cloud Foundation 3.5

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

Upgrading VMware Cloud Foundation 2.3.2.5 to 3.5.1

1

Upgrading from 2.3.2.5 to 3.5.1 utilizes VMware Cloud Foundation Lifecycle Management (LCM). The process involves sequentially applying the Network and Data and Services LCM bundles from within the 2.3.2.5 SDDC Manager Dashboard and then the Configuration Drift Remediation and VMware Software BOM upgrade bundles from within the 3.5.1 SDDC Manager Dashboard.

You can only upgrade from VMware Cloud Foundation 2.3.2.5. If you have another version of VMware Cloud Foundation, you must first upgrade it to 2.3.2.5 before you can upgrade to 3.5.1.

The following bundles are required to upgrade from 2.3.2.5 to 3.5.1:

- Network migration bundle
- Data and services migration bundle
- Configuration drift remediation bundle
- VMware Software BOM upgrade bundle

Note vRealize components are not upgraded through LCM and must be manually upgraded before you upgrade to VMware Cloud Foundation 3.5.1. See Chapter 3 Upgrading vRealize Components.

The bundles address changes to the product that were introduced between the 2.3.2.5 release and the 3.5.1 release.

During the migration process, you cannot perform SDDC Manager operations, for example domain creation or expansion, network configuration changes, upgrades, certificate management, password management, and so on.

Network Migration

Some of the biggest changes between Cloud Foundation 2.3.2.5 and 3.5.1 are in the area of networking. Once you meet the upgrade prerequisites, the network migration bundle takes care of the rest.

Table 1-1. Networking differences between 2.3.2.5 and 3.5.1

Cloud Foundation 2.3.2.5	Cloud Foundation 3.5.1
DNS and NTP services are provided by the SDDC Manager Utility VM.	DNS and NTP services are externalized and you must set up a DNS server and NTP server before upgrading. See Upgrade Prerequisites.
Static IP pools for VXLAN tunnel endpoints (VTEPs).	DHCP-based IP pools for VTEPs. You must set up an external DHCP server before upgrading. See Upgrade Prerequisites.
Uplink ports on the vSphere Distributed Switch use a link aggregation group (LAG) port group.	Use a standard uplink port group. For VLAN, port groups use **Route based on physical NIC load** (load-based teaming) and for VXLAN, port groups use **Route based on SRC-ID**.

Data and Services Migration

As part of data and services migration, a new 3.5.1 SDDC Manager is deployed and data gets migrated from the old SDDC Manager to the new SDDC Manager. Control of the system is handed off to the 3.5.1 SDDC Manager.

Cloud Foundation 2.3.2.5 had two SDDC Manager VMs; the SDDC Manager Utility VM and the SDDC Manager Controller VM. Cloud Foundation 3.5.1 has only a single SDDC Manager VM.

Configuration Drift Remediation

Configuration drift applies new configurations to the VMware Software and Cloud Foundation components to make them compatible with 3.5.1 features. You initiate the Configuration Drift Remediation bundle from the 3.5.1 SDDC Manager Dashboard.

VMware Software BOM Upgrade

After applying the first three migration bundles, you must apply multiple BOM upgrade bundles to upgrade individual products. You initiate the VMware Software BOM upgrades from the 3.5.1 SDDC Manager Dashboard.

Use Cases Not Supported for Upgrade

2

You cannot upgrade to Cloud Foundation 3.5.1 in the following cases.

- You have VDI workload domains in your environment and you require the VDI workload domains to be migrated to 3.5.1.
- You have a stretched cluster or a manual multi-cluster deployment.
- You implemented cross-site NSX.
- You implemented disaster recovery.

If you have implemented disaster recovery, DR would have to be disabled or set to passive mode during upgrade since connectivity loss is experienced for brief periods of time during the upgrade process.

Upgrading vRealize Components

3

The Cloud Foundation vRealize components, with the exception of vRealize Suite Lifecycle Manager, are not upgraded through VMware Cloud Foundation Lifecycle Management and must be manually upgraded before you upgrade to VMware Cloud Foundation 3.5.1.

You only need to upgrade the vRealize components that you deployed as part of VMware Cloud Foundation 2.3.2.5. A vRealize Log Insight instance is automatically deployed as part of the management domain, so you must upgrade vRealize Log Insight.

If you plan to upgrade vRealize Operations or , make sure to Verify the vRealize Edge Load Balancer IP Address first.

After you upgrade Cloud Foundation to 3.5.1, you can upgrade vRealize Suite Lifecycle Manager through the SDDC Manager Dashboard. See Upgrade vRealize Suite Lifecycle Manager.

This chapter includes the following topics:

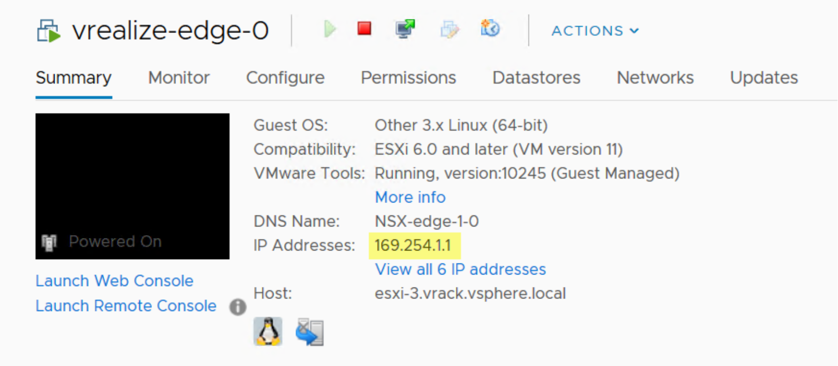
Verify the vRealize Edge Load Balancer IP Address

Before you upgrade vRealize Operations or vRealize Automation, you must verify that the vRealize Edge load balancers deployed in Cloud Foundation 2.3.2.5 have a primary IP address.

A failed deployment of vRealize Operations or vRealize Automation in Cloud Foundation 2.3.2.5 can leave the system in a state that prevents upgrade to 3.5.1.

Procedure

1. Log in to vCenter Server by using the vSphere Web Client.
2. Locate the `vrealize-edge` VMs and verify that a primary IP address is available.



Guest OS: Other 3.x Linux (64-bit)
Compatibility: ESXi 6.0 and later (VM version 11)
VMware Tools: Running, version:10245 (Guest Managed)
DNS Name: NSX-edge-1-0
IP Addresses: 169.254.1.1
Host: esxi-3.vrack.vsphere.local

If a primary IP address is available, you are ready to upgrade. If not, proceed to step 3.

3 Using the root credentials, SSH in to the SDDC Manager Controller VM.

4 Navigate to the `/etc/unbound/` directory.

5 Download the `unbound.conf` file to your local computer.

6 Open `unbound.conf`, look for the records containing information for `vrealize-edge.<your-domain>`, and gather their IP addresses.

7 In the vSphere Client, edit the `vrealize-edge` VMs to add the IP addresses you retrieved from `unbound.conf`.

Upgrade vRealize Automation from 7.3 to 7.5

In order to use vRealize Automation with VMware Cloud Foundation 3.5.1, you must manually upgrade to vRealize Automation 7.5.

You only need to perform the upgrade if you deployed vRealize Automation as part of VMware Cloud Foundation 2.3.2.5.

Prerequisites

Download the VMware vRealize Automation 7.5.0 Update Repository ISO (`VMware-vR-Appliance-7.5.0.458-10053539-updaterepo.iso`) from my.vmware.com.

Upgrade vRealize Automation Virtual Appliances and the Infrastructure-as-a-Service Components

You begin upgrading the Cloud Foundation vRealize components from the previous version by upgrading the cloud management layer. You start by upgrading vRealize Automation.

Prerequisites

Verify that all vRealize Automation components have the required compute and storage resources to perform the upgrade, including space for temporary objects created during the process.

Table 3-1. Hardware Requirements for UpgradingvRealize Automation

Node	Hardware Requirement for Each Node	Description
vRealize Automation Appliances	Available disk space	■ Disk1 with 50 GB ■ Disk3 with 25 GB ■ Disk4 with 50 GB ■ At least 4.5 GB of free disk space on the root partition to download and run the upgrade. ■ At least 4.5 GB of free space on the `/storage/db` ■ `/storage/log` subfolder cleaned of older archived ZIP files to free up disk space.
	Memory	18 GB
	vCPU	4
vRealize Automation IaaS Windows virtual machines and Microsoft SQL Server database	Available disk space	5 GB

Verify that third-party software components required for the upgrade are available on the vRealize Automation nodes.

Table 3-2. Software Requirements for Upgrading vRealize Automation

Node	Software Requirement	Description
Primary vRealize Automation IaaS Model Manager Server	Java	■ Java SE Runtime Environment 8 64-bit Update 161 or later installed. Remove versions prior to Update 161. ■ After you install Java, set the `JAVA_HOME` environment variable to the directory path of the new version.

Download the required software for the upgrade is available on the vRealize Automation nodes and verify the current condition of vRealize Automation .

Table 3-3. Configuration Prerequisites for Upgrading vRealize Automation

Prerequisite Category	Description
Compatibility	Verify all third-party integrations that might have been configured for use with vRealize Automation are compatible with vRealize Automation version 7.5. Contact the third-party integration vendor or developer to ensure compatibility.
Backup	■ Verify that current backups of the vRealize Automation virtual appliances and the Infrastructure-as-a-Service (IaaS) virtual machines exist. ■ Verify that a current backup of the external vRealize Automation database exists.
Downloads	Download the VMware vRealize Automation 7.5.0 Update Repository package (`VMware-vR-Appliance-7.5.0.458-10053539-updaterepo.iso`) from my.vmware.com.

Prerequisite Category	Description
Cluster Integrity and Health	■ Examine the health of vRealize Automation by using the vRealize Production Test Tool to ensure that it is in good health. Remediate any issues prior to beginning the upgrade. See the product download page version 1.7.1. ■ Open a Web browser and log in to the VAMI management interface for each vRealize Automation appliance by navigating to **`https://<vRA Appliance FQDN>:5480`**. Select **Cluster** and verify that all vRealize Automation IaaS Windows Server nodes meet the following requirements: ■ Have a `Last Connected` status of less than 30 seconds. ■ Have a `Time Offset` status of less than 1 second. ■ Open a web browser and log in to the VAMI management interface for each vRealize Automation appliance by navigating to **`https://<vRA Appliance FQDN>:5480`**. Select **Cluster** and verify that all vRealize Automation virtual appliances meet the following requirements: ■ Have a `Last Connected` status of less than 10 minutes. ■ The PostgreSQL database is connected and reporting a `Status` state of `Up`, indicating that the master and replica nodes are running. ■ The PostgreSQL database is connected and reporting a `Valid` state of `Yes`, indicating synchronization between the master and replica nodes. ■ Open a web browser and log in to the VAMI management interface for each vRealize Automation appliance by navigating to **`https://<vRA Appliance FQDN>:5480`**. Select **Services** and verify that all Services are reporting a status of `REGISTERED`.
Preparing the vRealize Automation Environment	■ Make the vRealize Automation environment unavailable to end users and any automated integrations during the upgrade maintenance window. ■ Verify that the vRealize Automation environment has been quiesced for all activities, including but not limited to, users ordering new virtual machines and third-party integrations that may automate the ordering of new virtual machines. Without quiescing the environment, rollback operations may be disruptive, generating orphaned objects after snapshots have been created. Remediating such situation might require extending the maintenance window. ■ Verify that you have access to all databases and load balancers that are impacted by, or participate in, the vRealize Automation upgrade.

Direct Traffic to the Primary Node and Disable Health Monitoring for vRealize Automation on the Load Balancer

Direct all traffic to the primary node and disable the health check on the NSX load balancer for vRealize Suite applications.

The configuration change disables the additional pool members for the vRealize Automation VIPs. During an upgrade, the services inside the additional nodes might not be upgraded or initialized because of installation or power cycle operations. If the load balancer passes a request to one of the additional nodes, the request fails. If an additional pool member remains enabled, you might experience failures during vRealize Automation upgrade, and service initialization or registration failures during a vRealize Automation appliance power cycle operations.

On the NSX load balancer, you disable the additional vRealize Automation nodes and deselect the monitor for the associated traffic in the pools.

Procedure

1. Log in to the first vRealize Automation appliance via the VAMI interface (`https://<vRA Appliance FQDN>:5480`).
2. On the **Cluster** tab, check which nodes have the `REPLICA` label. The `REPLICA` label indicates which vRealize Appliances are the secondary.
3. Log in to vCenter Server by using the vSphere Web Client.
4. From the **Home** menu of the vSphere Web Client, select **Networking & Security**.
5. In the **Navigator**, click **NSX Edges**.
6. From the NSX Manager drop-down menu, select the NSX Manager IP Address corresponding to the NSX Manager for the management workload domain and double-click the NSX edge device for vRealize Suite to open its network settings.
7. On the **Manage** tab, click the **Load Balancer** tab and click **Pools**.
8. Select the **vra-svr-443** pool that contains the vRealize Automation appliances and click **Edit**.
9. In the **Edit Pool** dialog box, select the secondary node, click **Edit**, select **Disable** from the **State** drop-down menu, and click **OK**.
10. In the **Edit Pool** dialog box, select **NONE** from the **Monitors** drop-down menu and click **OK**.
11. Repeat the procedure on the remaining load balancer pools.
12. To verify that the load balancer redirects the traffic to the primary node of vRealize Automation, open a Web browser and go to `https://<vRA primary appliance FQDN>/vcac` to verify that the login page of the vRealize Automation administration portal appears.

Take Snapshots of the vRealize Automation Virtual Machines

Shut down the virtual machines in the correct order and take a snapshot of each virtual machine in the environment. If you must do a rollback of vRealize Automation to the previous state, use these snapshots to perform the rollback operation.

Procedure

1. Log in to the Management vCenter Server by using the vSphere Web Client.
2. From the **Home** menu, select **VMs and Templates**.
3. Shut down the vRealize Automation virtual machines in the environment according following the guidance in Shut Down vRealize Automation.
   a. Shut down the Distributed Execution Manager Orchestrator and Workers and all vRealize Automation agents in any order and wait for all components to finish shutting down.
   b. Shut down virtual machines that are running the Manager Service and wait for the shutdown to finish.
   c. Shut down the secondary Web node and wait for the shutdown to finish.

d Shut down the primary Web node, and wait for the shutdown to finish.

e Shut down all secondary vRealize Automation appliance instances and wait for the shutdown to finish.

f Shut down the primary vRealize Automation appliance and wait for the shutdown to finish.

The primary vRealize Automation appliance is the one that contains the master, or writeable, appliance database. Make a note of the name of the primary vRealize Automation appliance. You use this information when you restart vRealize Automation.

g Shut down the MSSQL virtual machine(s) in any order and wait for the shutdown to finish.

4 Take a snapshot of the vRealize Automation virtual machines in the environment.

5 Verify that the snapshots for each vRealize Automation virtual machine are successfully created.

6 Power on the vRealize Automation virtual machines in the environment according to Start Up vRealize Automation.

a Start the MS SQL database virtual machine(s).

b In vSphere, disable the NSX Manager health checks before you start the vRealize Automation appliance. Only ping health check should be enabled.

c In vSphere, start the master vRealize Automation appliance.

d Wait until the licensing service is running and `REGISTERED` in the master appliance management interface.

e Start the remaining vRealize Automation appliances at the same time.

f Wait for the appliances to start, and verify that services are running and listed as `REGISTERED` in the appliance management interface. It might take 15 or more minutes for appliances to start.

g Start the primary Web node and wait for the startup to finish.

h Start the secondary Web node and wait 5 minutes.

i Start the primary Manager Service machine and wait for 2 to 5 minutes.

j Start secondary Manager Service machine and wait 2 to 5 minutes.

k Start the Distributed Execution Manager Orchestrator and Workers and all vRealize Automation proxy agents. You can start these components in any order and you do not need to wait for one startup to finish before you start another.

l In vSphere, enable the NSX Manager health checks that were disabled in Step 4b.

7 Verify that the startup succeeded.

a Open a Web browser to the vRealize Automation appliance management interface URL.

b Click the **Services** tab.

c Click **Refresh** to monitor the progress of service startup. When all services are listed as registered, the system is ready to use.

Set the vRealize Automation PostgreSQL Replication Mode to Asynchronous

Before you upgrade vRealize Automation, make sure that the PostgreSQL replication mode is set to asynchronous.

Procedure

1. Log in to the first vRealize Automation appliance via the VAMI interface (`https://<vRA Appliance FQDN>:5480`).
2. Click **Cluster**.
3. Click **Async Mode** and wait until the action completes.
4. Verify that all nodes in the **Sync State** column display `Async` status.

Configure the Authentication Provider of vRealize Orchestrator with the Default Tenant

Before you perform the upgrade of vRealize Automation, you reconfigure the vRealize Orchestrator authentication provider to the default tenant and admin group to ensure the vRealize Orchestrator services come online post-upgrade.

Make a note of the currently configured tenant and group as they will be used after the upgrade to restore the configuration to its pre-upgrade state.

Procedure

1. Log in to vRealize Orchestrator Control Center
2. Under the **Manage** group of settings, click **Configure Authentication Provider**.
3. On the **Configure Autenthication Provider** page, click **Change** next to **Default tenant**, enter **`vsphere.local`** (or the name of the default tenant if different), and click **Apply**.
4. Click **Change** next to **Admin group**, enter **`vsphere.local`** (or the name of the default tenant if different), select the `vcoadmins` group, and click **Apply**.
5. Click **Save Changes**.

Upgrade the vRealize Automation Appliances and IaaS Components

When you upgrade the vRealize Automation in the cloud management layer, start the procedure from the primary vRealize Automation virtual appliance using the upgrade .iso file. The upgrade process supports automatic upgrade of both the vRealize Automation virtual appliance and the vRealize Automation IaaS components.

Prerequisites

- Verify that the primary IaaS Web Server virtual machine satisfies the following requirements:
  - Java SE Runtime Environment 8 64-bit update 161 or later is installed.
  - JAVA_HOME environment variable is set to the Java directory path.

- Mount the upgrade .iso file, `VMware-vR-Appliance-7.5.0.458-10053539-updaterepo.iso`, on the primary vRealize Automation virtual appliance.

Procedure

1 Log in to the first vRealize Automation appliance via the VAMI interface (`https://<vRA Appliance FQDN>:5480`).

2 Click the **Update** tab and click the **Settings** button.

3 Under the **Update Repository** section, select **Use CD-ROM Updates** and click **Save Settings**.

4 Click the **Status** tab and click **Check Updates** to load the update from the upgrade .iso file.

5 Verify that the update listed in **Available Updates** is 7.5, click Install Updates and click **OK** in the **Install Updates** dialog box.

You can monitor the upgrade process within the logs on the vRealize Automation virtual appliance: `/opt/vmware/var/log/vami/vami.log` - Logs the initial unpacking and staging of the upgrade bundle to the primary vRealize Automation virtual appliance. Once completed, additional logging is available in the updatecli.log: `/opt/vmware/var/log/vami/updatecli.log` - Logs the additional vRealize Automation upgrade processes, such as, the upgrade script execution.

6 On the **Status** page, monitor the **Update Status**.

After the upgrade completes, the system reboot is required to complete the update message appears on the **Status** page.

7 On the **System** tab, click **Reboot** and click **Reboot** in the confirmation dialog box to restart the primary vRealize Automation appliance.

Additional vRealize Automation virtual appliances restart automatically.

8 Log in to the first vRealize Automation appliance via the VAMI interface (`https://<vRA Appliance FQDN>:5480`).

9 On the **Update** tab, click the **Status** button, and monitor the vRealize Automation IaaS upgrade for each Windows Server-based component.

10 After the upgrade completes for the vRealize Automation IaaS components, use the **Cluster** tab to verify that each vRealize Automation IaaS nodes and components are version 7.5.0.xxxxx.

11 On the **vRA > Licensing** tab, verify that the vRealize Automation product license information remains and a valid license is still available.

12 If the upgrade process has removed the license, re-enter the license key.

a Enter the license key in the **New License Key** text box and click **Submit Key**.

b Verify that the license has been applied.

c Repeat this step on other vRA virtual appliances.

Restore the Configuration of the vRealize Orchestrator Authentication Provider

After you perform the upgrade of vRealize Automation, you configure the default tenant and admin group of the vRealize Orchestrator authentication provider with the configuration before the upgrade, that is, with the Rainpole tenant.

Procedure

1 Log in to the vRealize Automation appliance by using Secure Shell (SSH) client to configure the embedded vRealize Orchestrator.

2 Verify that the vRealize Orchestrator user interface service is running.

   a Run the following command to verify that the service is set to automatically start: `chkconfig vco–configurator`.

   b If the service reports `Off`, run the following command to enable an automatic restart of the Orchestrator user interface service upon subsequent reboots of the vRealize Automation appliance: `chkconfig vco–configurator on`.

   c Verify the status of Orchestrator User Interface by running the following command: `service vco–configurator status`.

   d Repeat the procedure to configure vRealize Orchestrator for the other vRA appliances.

3 Log in to vRealize Orchestrator Control Center to change the default tenant and admin group for the authentication provider.

4 Associate the default tenant and admin group for the vRealize Orchestrator authentication provider with the tenant configured prior to the upgrade.

5 Under the **Manage** group of settings, select **Configure Authentication Provider**.

6 On the **Configure Authentication Provider** page, click **Change** next to **Default tenant**, enter the name of the tenant configured prior to the upgrade, and click **Apply**.

7 Click **Change** next to **Admin group**, enter the name of the group used/configured prior to the upgrade, and click **Search**.

8 From the drop-down menu, select the name of the group used/configured prior to the upgrade, and click **Apply**.

9 Click **Save Changes**.

Re-Enable Traffic to the Secondary Nodes and Health Monitoring for vRealize Automation on the Load Balancer

After you complete the upgrade of vRealize Automation, restore traffic distribution and health checks on the NSX load balancer, across the primary and secondary components of the vRealize Automation platform.

On the NSX load balancer, you re-enable the secondary vRealize Automation nodes and select the monitor for the associated traffic in the pools.

Procedure

1. Log in to vCenter Server by using the vSphere Web Client.
2. From the **Home** menu of the vSphere Web Client, select **Networking & Security**.
3. In the **Navigator**, click **NSX Edges**.
4. From the **NSX Manager** drop-down menu, select the NSX Manager IP Address corresponding to the NSX Manager for the management workload domain and double-click the vRA edge device to open its network settings.
5. On the **Load Balancer** tab, click **Pools**.
6. Select the pool that contains the vRealize Automation appliances and click **Edit**.
7. In the **Edit Pool** dialog box, select the secondary node that you disabled before the upgrade, click **Edit**, select **Enable** from the **State** drop-down menu, and click **OK**.
8. In the **Edit Pool** dialog box, select **NONE** from the **Monitors** drop-down menu and click **OK**.
9. Repeat this procedure for the remaining load balancer pools.

Delete the Snapshots of the vRealize Automation Virtual Machines

After you determine that vRealize Automation is functioning correctly and there is no need for rollback, you can delete the virtual machine snapshots.

Procedure

1. Log in to vCenter Server by using the vSphere Web Client.
2. From the **Home** menu, select **VMs and Templates**.
3. Navigate to the first vRealize Automation virtual machine, right-click it, and select **Snapshots > Manage Snapshots**.
4. Click the snapshot that you created before the vRealize Automation upgrade, click the **Delete a VM Snapshot** icon and click **Yes**.
5. In the **Confirm Delete** dialog box, click **Yes**.
6. Repeat this procedure for the remaining vRealize Automation virtual machines.

Expand vRealize Automation to a Three-Node Appliance Architecture Post-Upgrade

Perform the post-upgrade operation of expanding your vRealize Automation cluster to include a third appliance.

Cloud Foundation 2.3.2.5 used a two-node architecture, but Cloud Foundation 3.5.1 uses a three-node architecture. By adding a node to the vRealize Automation cluster and operating with the synchronous replication mode enabled, the embedded PostgreSQL database can automate failover between nodes. Failover support improves resilience of the cloud management layer stack to failures and reduces the number of manual failover procedures.

Prerequisites

- Virtual disk provisioning
  - Thin
  - Required storage: 140 GB
- Root Active Directory domain controller as a certificate authority for the environment

Replace the vRealize Automation Certificate

Before you expand the vRealize Automation cluster with a third vRealize Automation virtual appliance, you must install a certificate that includes the host name of the third appliance on the vRealize Automation virtual appliances and vRealize Automation IaaS components.

You add the third vRealize Automation virtual appliance as an additional subject alternative name (SAN) in the certificate. You must also update the trusted vRealize Automation certificate on the vRealize Business for Cloud (if vRealize Business is deployed and vRealize Automation is registered with it) and vRealize Operations Manager deployments in the environment.

Add a Third vRealize Automation Appliance to the Cluster

Cloud Foundation 2.3.2.5 used a two-node architecture, but Cloud Foundation 3.5.1 uses a three-node architecture. Add a third vRealize Automation appliance to the cluster to use vRealize Automation with Cloud Foundation 3.5.1.

Prerequisites

Download the VMware vRealize Automation 7.5.0 OVA file (`VMware-vR-Appliance-7.5.0.458-10053539_OVF10.ova`) from my.vmware.com.

Take Snapshots of the vRealize Automation Virtual Machines

Shut down the virtual machines in the correct order and take a snapshot of each virtual machine in the environment. If you must do a rollback of vRealize Automation to the previous state, use these snapshots to perform the rollback operation.

Procedure

1. Log in to the Management vCenter Server by using the vSphere Web Client.
2. From the **Home** menu, select **VMs and Templates**.
3. Shut down the vRealize Automation virtual machines in the environment according following the guidance in Shut Down vRealize Automation.
   a. Shut down the Distributed Execution Manager Orchestrator and Workers and all vRealize Automation agents in any order and wait for all components to finish shutting down.
   b. Shut down virtual machines that are running the Manager Service and wait for the shutdown to finish.
   c. Shut down the secondary Web node and wait for the shutdown to finish.

   d Shut down the primary Web node, and wait for the shutdown to finish.

   e Shut down all secondary vRealize Automation appliance instances and wait for the shutdown to finish.

   f Shut down the primary vRealize Automation appliance and wait for the shutdown to finish.

     The primary vRealize Automation appliance is the one that contains the master, or writeable, appliance database. Make a note of the name of the primary vRealize Automation appliance. You use this information when you restart vRealize Automation.

   g Shut down the MSSQL virtual machine(s) in any order and wait for the shutdown to finish.

4. Take a snapshot of the vRealize Automation virtual machines in the environment.

5. Verify that the snapshots for each vRealize Automation virtual machine are successfully created.

6. Power on the vRealize Automation virtual machines in the environment according to Start Up vRealize Automation.

   a Start the MS SQL database virtual machine(s).

   b In vSphere, disable the NSX Manager health checks before you start the vRealize Automation appliance. Only ping health check should be enabled.

   c In vSphere, start the master vRealize Automation appliance.

   d Wait until the licensing service is running and `REGISTERED` in the master appliance management interface.

   e Start the remaining vRealize Automation appliances at the same time.

   f Wait for the appliances to start, and verify that services are running and listed as `REGISTERED` in the appliance management interface. It might take 15 or more minutes for appliances to start.

   g Start the primary Web node and wait for the startup to finish.

   h Start the secondary Web node and wait 5 minutes.

   i Start the primary Manager Service machine and wait for 2 to 5 minutes.

   j Start secondary Manager Service machine and wait 2 to 5 minutes.

   k Start the Distributed Execution Manager Orchestrator and Workers and all vRealize Automation proxy agents. You can start these components in any order and you do not need to wait for one startup to finish before you start another.

   l In vSphere, enable the NSX Manager health checks that were disabled in Step 4b.

7. Verify that the startup succeeded.

   a Open a Web browser to the vRealize Automation appliance management interface URL.

   b Click the **Services** tab.

   c Click **Refresh** to monitor the progress of service startup. When all services are listed as registered, the system is ready to use.

Direct Traffic to the Primary Node and Disable Health Monitoring for vRealize Automation on the Load Balancer

Direct all traffic to the primary node and disable the health check on the NSX load balancer for vRealize Suite applications.

The configuration change disables the additional pool members for the vRealize Automation VIPs. During an upgrade, the services inside the additional nodes might not be upgraded or initialized because of installation or power cycle operations. If the load balancer passes a request to one of the additional nodes, the request fails. If an additional pool member remains enabled, you might experience failures during vRealize Automation upgrade, and service initialization or registration failures during a vRealize Automation appliance power cycle operations.

On the NSX load balancer, you disable the additional vRealize Automation nodes and deselect the monitor for the associated traffic in the pools.

Procedure

1. Log in to the first vRealize Automation appliance via the VAMI interface (`https://<vRA Appliance FQDN>:5480`).
2. On the **Cluster** tab, check which nodes have the `REPLICA` label. The `REPLICA` label indicates which vRealize Appliances are the secondary.
3. Log in to vCenter Server by using the vSphere Web Client.
4. From the **Home** menu of the vSphere Web Client, select **Networking & Security**.
5. In the **Navigator**, click **NSX Edges**.
6. From the NSX Manager drop-down menu, select the NSX Manager IP Address corresponding to the NSX Manager for the management workload domain and double-click the NSX edge device for vRealize Suite to open its network settings.
7. On the **Manage** tab, click the **Load Balancer** tab and click **Pools**.
8. Select the **vra-svr-443** pool that contains the vRealize Automation appliances and click **Edit**.
9. In the **Edit Pool** dialog box, select the secondary node, click **Edit**, select **Disable** from the **State** drop-down menu, and click **OK**.
10. In the **Edit Pool** dialog box, select **NONE** from the **Monitors** drop-down menu and click **OK**.
11. Repeat the procedure on the remaining load balancer pools.
12. To verify that the load balancer redirects the traffic to the primary node of vRealize Automation, open a Web browser and go to `https://<vRA primary appliance FQDN>/vcac` to verify that the login page of the vRealize Automation administration portal appears.

Add the Third vRealize Automation Appliance as a Disabled Member to the Load Balancer

Before you expand the vRealize Automation cluster, add the host name and IP address of the third vRealize Automation virtual appliance as a disabled member of the server pools on the load balancer.

On the load balancer, perform the following procedure to update the server pools related to the traffic to the vRealize Automation appliance with the settings for the third vRealize Automation virtual appliance.

Procedure

1. Log in to vCenter Server by using the vSphere Web Client.
2. From the **Home** menu of the vSphere Web Client, select **Networking & Security**.
3. In the **Navigator**, click **NSX Edges**.
4. From the **NSX Manager** drop-down menu, select the NSX Edge Load Balancer and double-click the NSX Edge to open its network settings.
5. Click the **Manage** tab, click **Load Balancer**, and select **Pools**.
6. Select the first pool and click the **Edit** icon.
7. Under **Members**, click the **Add** icon to add a third pool member.
8. In the **New Member** dialog box, enter the settings for the new member and click **OK**.

Setting	Value
Name	Hostname of the third vRealize Automation appliance, for example, `vra01svr01c`.
IP Address/VC Container	IP address of the third vRealize Automation appliance, for example, `172.16.11.83`.
State	Disabled
Port	Match the port used by the other vRealize Automation appliances in the pool. For example, 443.
Monitor Port	Match the monitor port used by the other vRealize Automation appliances in the pool. For example, 443.
Weight	1

9. Repeat the procedure to update any remaining server pools with the details about the third vRealize Automation virtual appliance in a disabled state.

Deploy the Third vRealize Automation Virtual Appliance

Deploy a third vRealize Automation virtual appliance to the management cluster using the downloaded `.ova` file. Then, you can expand the vRealize Automation cluster.

Prerequisites

Download the `.ova` file, `VMware-vR-Appliance-7.5.0.458-10053539_OVF10.ova`, for vRealize Automation 7.5 to the system from which you are performing the upgrade.

Procedure

1. Log in to the Management vCenter Server by using the vSphere Web Client.
2. In the vSphere Web Client, select **Home > Hosts and Clusters**.

3 Right-click the management cluster and select **Deploy OVF Template**.

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

5 On the **Select name and folder** page, enter a name (for example, `vra01svr01c`) and folder, and click **Next**.

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

7 On the **Accept license agreements** page, accept the end user license agreements and click **Next**.

8 On the **Select storage** page, set the following datastore configuration and click **Next**.

Setting	Value
Select virtual disk format	Thin Provision
VM storage policy	vSAN Default Storage Policy
Datastore	For example, `sfo01-m01-vsan`.

9 On the **Setup Networks** page, select the **vRack-DPortGroup-vRealize** distributed port group from the **Destination Network** drop-down menu and click **Next.**

10 On the **Customize template** page, configure the following values, and click **Next**.

Option	Description
Enable SSH service in the appliance	Selected
Hostname	Host name of the third vRealize Automation appliance. For example, *vra01svr01c.rainpole.local*.
Initial Root Password	*vra_appC_root_password*
Default Gateway	For example, 192.168.11.1.
Domain Name	For example, rainpole.local.
Domain Names Servers	For example, 172.16.11.4,172.17.11.4.
Domain Search Path	For example, rainpole.local,sfo01.rainpole.local.
Network 1 IP Address	For example, 192.168.11.50.
Network 1 Netmask	For example, 255.255.255.0.

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

12 In the search text box type the name of you provided for the third vRealize Automation appliance, for example `vra01svr01c`.

13 Click the virtual machine name (**vra01svr01c**), click the **Power On** icon, and wait until the power-on procedure is completed.

14 In the virtual machine console, verify that the VM uses the configuration settings you specified.

   a In the vSphere Web Client, right-click the appliance and select **Open Console** to open the remote console to the appliance.

   b Examine the welcome screen of the appliance console.

   c Close the virtual appliance console.

Join the Third vRealize Automation Appliance to the Cluster

After you deploy the third vRealize Automation appliance, join it to the vRealize Automation cluster. After you join the appliance, the vRealize Automation services start, and the appliance inherits the settings from the cluster, such as, certificate and licensing.

Procedure

1 Log in to the first vRealize Automation appliance via the VAMI interface (`https://<vRA Appliance FQDN>:5480`).

2 On the **Cluster** tab, check which node has the `MASTER` label.

3 Log in to the management console of the newly deployed vRealize Automation appliance.

4 If the **Installation Wizard** appears, click **Cancel** to go directly to the management interface.

5 On the **Admin** tab, click **Time Settings** and verify that the time source is the same as on the `MASTER`.

6 On the **Cluster** tab, enter the following settings and click **Join Cluster**.

Setting	Value
Leading Cluster Node	*FQDN of the master vRealize Automation appliance*
Admin User	root
Password	password of the MASTER vRealize Automation appliance

7 If certificate warnings are displayed, ignore them.

8 Monitor the status of the services as they are restarted on the appliance.

   a Click the **Services** tab and click the **Refresh** button to monitor the progress of services startup.

9 Start the embedded vRealize Orchestrator services.

   a On the **vRA > Orchestrator** tab, select **Orchestrator user interface**.

   b If the service is stopped, in the **Actions** area, click **Start**.

   c Repeat this step for **Orchestrator Server**.

10 Configure the Orchestrator user interface service to start automatically after upgrade.

   a Open an SSH connection to the appliance and log in.

   b Run the following command to verify that the service is set to automatically start.

```
chkconfig vco-configurator
```

c If the service reports `Off`, run the following command to enable an automatic restart of the Orchestrator user interface service upon subsequent reboots of the vRealize Automation appliance.

```
chkconfig vco–configurator on
```

d Verify the status of Orchestrator User Interface by running the following command.

```
service vco–configurator status
```

Enable Synchronous Mode for vRealize Automation Database Replication

After you expand vRealize Automation to include the third vRealize Automation virtual appliance, change the replication method of the PostgreSQL database to synchronous mode for automatic failover with improved data loss protection.

Procedure

1 Log in to the first vRealize Automation appliance via the VAMI interface (`https://<vRA Appliance FQDN>:5480`).

2 On the **Cluster** tab, review the current **Replication Mode**.

3 Verify the following database settings.

Setting	Expected Value
Replication Mode	Database is in Asynchronous Mode
Connection Status	Connected

4 Verify that all three hosts appear in the list of database nodes.

Example Database Node Hosts	Status
vra01svr01a.rainpole.local	Up
vra01svr01b.rainpole.local	Up
vra01svr01c.rainpole.local	Up

5 Verify that each of the two replica hosts has the following configuration.

Setting	Expected Value
Sync State	Async
Valid	Yes

6 Click the **Sync Mode** button to enable the synchronous replication mode of the PostgreSQL database.

Wait until the **Replication Mode** updates.

7 Verify the following database settings.

Setting	Expected Value
Replication Mode	Database is in Synchronous Mode. Automatic failover is now turned on!
Connection Status	Connected

8 Verify that you see the hosts in step 4.

9 Verify that each of the two replica hosts has the following configuration.

Setting	Expected Value
Sync State	Sync
Valid	Yes

Enable the State and Health Monitoring for the New vRealize Automation Appliance on the Load Balancer

After you complete expansion of the vRealize Automation cluster, update traffic distribution and health checks on the NSX load balancer to cover the new configuration of primary and secondary components of vRealize Automation platform.

Procedure

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

2 From the **Home** menu of the vSphere Web Client, select **Networking & Security**.

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

4 From the **NSX Manager** drop-down menu, select the NSX Manager IP Address corresponding to the NSX Manager for the management workload domain and double-click the vRealize Automation edge device to open its network settings.

5 On the **Manage** tab, click the **Load Balancer** tab, click **Pools**.

6 Select the pool that contains the vRealize Automation appliances and click **Edit**.

7 In the **Edit Pool** dialog box, select the new vRealize Automation appliance, click **Edit**, select **Enable** from the **State** drop-down menu, and click **OK**.

8 In the **Edit Pool** dialog box, select the vRealize Automation monitor from the **Monitors** drop-down menu and click **OK**.

9 Repeat the procedure on any remaining load balancer pools.

Delete the Snapshots of the vRealize Automation Virtual Machines

After you determine that vRealize Automation is functioning correctly and there is no need for rollback, you can delete the virtual machine snapshots.

Procedure

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

2 From the **Home** menu, select **VMs and Templates**.

3 Navigate to the first vRealize Automation virtual machine, right-click it, and select **Snapshots > Manage Snapshots**.

4 Click the snapshot that you created before the vRealize Automation upgrade, click the **Delete a VM Snapshot** icon and click **Yes**.

5 In the **Confirm Delete** dialog box, click **Yes**.

6 Repeat this procedure for the remaining vRealize Automation virtual machines.

Configure the Environment for the Third vRealize Automation Appliance

After you complete the expansion of vRealize Automation, update the anti-affinity rules in the environment and configure log forwarding.

Update the Anti-Affinity Rules for vRealize Automation Virtual Machines

After you complete the expansion of the vRealize Automation cluster, update the VM/Host anti-affinity to ensure that each of the vRealize Automation virtual appliances are maintained on different hosts.

Procedure

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

2 From the **Home** page, click **Hosts and Clusters**.

3 In the **Navigator**, select the management cluster.

4 Click the **Configure** tab, and under **Configuration**, select **VM/Host Rules**.

5 Under **VM/Host Rules**, select the existing anti-affinity for vRealize Automation rule and click **Edit**.

6 In the **Edit VM/Host Rule** dialog box, click **Add**, select the the host name of the third vRealize Automation appliance (for example, `vra01svr01c`), and click **OK**.

   The rule includes the virtual machines of the three vRealize Automation appliances.

Configure Log Forwarding for the Third vRealize Automation Appliance

Log in to the primary management console interface of the newly added vRealize Automation appliance and update the Log Insight Agent configuration.

Agent configuration for the vRealize Automation virtual appliances includes the following tasks:

- Verify that the log forwarding configuration has been inherited and configured on the new vRealize Automation virtual appliance to send logs to the vRealize Log Insight cluster.
- Update the agent group for configuring log forwarding from the vRealize Automation modules to include the new vRealize Automation virtual appliance.

- Update the agent group for configuring log forwarding from the operating system to include the new vRealize Automation virtual appliance.

Procedure

1 Log in to the third vRealize Automation appliance via the VAMI interface (`https://<vRA Appliance FQDN>:5480`).

2 Configure log forwarding to vRealize Log Insight.

a On the **vRA** tab, click the **Logs** tab.

b Scroll down to the **Log Insight Agent Configuration** section.

c Verify that the following values are replicated from the primary vRealize Automation appliance to the third vRealize Automation appliance, and click **Save Settings**.

Setting	Value
Host	vRealize Log Insight load balancer
Port	9000
Protocol	CFAPI
SSL Enabled	Deselected

d Scroll down to the **Agent Behavior Configuration** section.

Setting	Value
Reconnect	30
Max Buffer Size	2000
Debug Level	No Debug Messages

3 Log in to the vRealize Log Insight user interface.

4 Click the configuration drop-down menu icon ☰ and select **Administration**.

5 Under **Management**, click **Agents**.

6 Add the new appliance to the agent group for the vRealize Automation appliances.

You use this agent group to configure centrally the collection of logs that appear in the vRealize Automation dashboards.

a From the **All Agents** drop-down menu, select the agent group for the vRealize Automation appliances.

b In the agent filter text boxes, add the host name of the new vRealize Automation appliance and press Enter.

Filter	Operator	Values
Hostname	Matches	■ Host name of the third vRealize Automation appliance

  c Click **Refresh** and verify that all the agents in the filter appear in the **Agents** list.

  d Click **Save Agent Group** at the bottom of the page.

7 Repeat the steps to add the new vRealize Automation appliance to the Linux agent group that stores central configuration for the agents on the management virtual appliances.

Filter	Operator	Values
Hostname	Matches	■ Host name of the third vRealize Automation appliance

Upgrade vRealize Operations from 6.6.1 to 7.0

In order to use vRealize Operations with VMware Cloud Foundation 3.5.1, you must upgrade to vRealize Operations 7.0.

You only need to perform the upgrade if you deployed vRealize Operations Manager as part of VMware Cloud Foundation 2.3.2.5.

Prerequisites

- Take snapshots of all vRealize Operations Manager VMs.
- Download the vRealize Operations Manager - Virtual Appliance Security Patch (`vRealize_Operations_Manager-VA-7.0.0.11287810.pak`) from my.vmware.com.
- Download the vRealize Operations Manager - Virtual Appliance upgrade (`vRealize_Operations_Manager-VA-7.0.0.10098132.pak`) from my.vmware.com.
- Download the vRealize Operations Manager - Virtual Appliance Operating System upgrade (`vRealize_Operations_Manager-VA-OS-7.0.0.10098132.pak`) from my.vmware.com.
- Examine the health of vRealize Operations Manager cluster by using the Upgrade Assessment Tool. Remediate any issues before you begin the upgrade. See VMware Knowledge Base article 57283 and the product download page version 7.0.
- Preserve any customized content by cloning the content. Customized content includes alert definitions, symptom definitions, recommendations, and views.
- On all vRealize Operations Manager virtual appliances, verify that the vRealize Log Insight agent configuration, located in the `/var/lib/loginsight-agent/liagent.ini` file, contains `ssl=no`.

Procedure

1 Take the vRealize Operations Manager Nodes Offline and Take Snapshots

  Before you perform the upgrade of vRealize Operations Manager, take the nodes in the cluster offline and take a snapshot of each node. If you must perform a rollback of vRealize Operations Manager to the previous state, these snapshots accelerate the rollback operation.

2 Upgrade the Operating System on the vRealize Operations Manager Appliances

   When you upgrade the vRealize Operation Manager cluster, start the process by upgrading the operating system of the vRealize Operations Manager virtual appliances. You use the administration user interface on the vRealize Operations Manager master node to perform the operation.

3 Upgrade the vRealize Operations Manager Software

   After you upgrade the operating system on the vRealize Operations Manager virtual appliances, upgrade the software on the appliances.

4 Upgrade Non-Native vRealize Operations Manager Management Packs

   After you complete the upgrade of vRealize Operations Manager, upgrade the non-native management packs to ensure continuous interoperability.

5 Delete the Snapshots of the vRealize Operations Manager Nodes

   After completing the upgrade of vRealize Operations Manager and verifying operations and functionality, you delete the virtual machine snapshots.

Take the vRealize Operations Manager Nodes Offline and Take Snapshots

Before you perform the upgrade of vRealize Operations Manager, take the nodes in the cluster offline and take a snapshot of each node. If you must perform a rollback of vRealize Operations Manager to the previous state, these snapshots accelerate the rollback operation.

Procedure

1 Log in to the vRealize Operations Manager administrator interface on the master node.

2 Take all vRealize Operations Manager nodes in the cluster offline.

   a In the **Navigator**, click **System Status**.

   b On the **System Status** page, under **Cluster Status** click **Take Offline**.

   c In the **Take Cluster Offline** dialog, enter **`vRealize Operations Manager 7.0 Upgrade`** in the Reason text box and click OK.

3 Wait until all vRealize Operations Manager nodes in the cluster are offline and the Cluster Status becomes `Offline`.

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

5 Take a snapshot of each vRealize Operations Manager node (master node, master replica node, data nodes, and remote collector nodes).

Upgrade the Operating System on the vRealize Operations Manager Appliances

When you upgrade the vRealize Operation Manager cluster, start the process by upgrading the operating system of the vRealize Operations Manager virtual appliances. You use the administration user interface on the vRealize Operations Manager master node to perform the operation.

Procedure

1. Log in to the administrator user interface on the vRealize Operations Manager master node.
2. In the **Navigator**, click **Software Update**.
3. On the **Software Update** page, click **Install a Software Update**.
4. In the **Select Software Update** wizard, click **Browse** and locate `vRealize_Operations_Manager-VA-OS-7.0.0.10098132.pak` on the local file system.
5. Select **Install the PAK file even if it is already installed**, click **Upload** and click **Next**.
6. On the **End User License Agreement** page, select the **I accept the terms of this agreement** check box and click **Next**.
7. On the **Update Information** dialog, review the Important Update and Release Information and click **Next**.
8. On the **Install Software Update** page, click **Install**.

Wait until the operating system software update is completed. You are logged out from the administrator user interface of the master node while the software update process restarts each of the vRealize Operations Manager nodes included in the deployment. After the operating system update process is complete, log back in to the administrator user interface on the master node and verify that the cluster status is `ONLINE` on the **Cluster Status** page.

Upgrade the vRealize Operations Manager Software

After you upgrade the operating system on the vRealize Operations Manager virtual appliances, upgrade the software on the appliances.

Procedure

1. Log in to the administrator user interface on the vRealize Operations Manager master node.
2. Take all vRealize Operations Manager nodes in the cluster offline.
   a. In the **Navigator**, click **System Status**.
   b. On the **System Status** page, under **Cluster Status** click **Take Offline**.
   c. In the **Take Cluster Offline** dialog, enter **`vRealize Operations Manager 7.0 Upgrade`** in the **Reason** text box and click **OK**.
3. Wait until all vRealize Operations Manager nodes in the cluster are offline and the **Cluster Status** becomes `Offline`.
4. Perform the upgrade of vRealize Operations Manager software.
   a. In the **Navigator**, click **Software Update**.
   b. On the **Software Update** page , click **Install a Software Update**.
   c. On the **Select Software Update** page of the **Add Software Update** wizard, click **Browse** and locate `vRealize_Operations_Manager-VA-7.0.0.10098132.pak` on the local file system.

   d Select **Install the PAK file even if it is already installed**, click **Upload**, and click **Next**.

   e On the **End User License Agreement** page, select the **I accept the terms of this agreement** check box and click **Next**.

   f On the **Update Information** page, review the **Important Update and Release Information** and click **Next**.

   g On the **Install Software Update** page, click **Install**.

5 Wait until the update of the vRealize Operations Manager software is completed.

   You are logged out from the administrator user interface of the master node while the software update process restarts each of the vRealize Operations Manager nodes included in the deployment.

6 After the software update process is complete, log back in to the administrator user interface on the master node and verify that the cluster status is `Online` on the **Cluster Status** page.

7 Repeat steps 1-6 using `vRealize_Operations_Manager-VA-7.0.0.11287810.pak`.

8 Before you log in to the vRealize Operations Manager user interface, clear your browser cache to ensure that all objects in the vRealize Operations Manager user interface are displayed correctly.

Upgrade Non-Native vRealize Operations Manager Management Packs

After you complete the upgrade of vRealize Operations Manager, upgrade the non-native management packs to ensure continuous interoperability.

During the upgrade, vRealize Operations updates any in-product management packs and versions them alongside the vRealize Operations version and build. Validate the compatibility of any VMware add-on or third-party management packs that you have manually installed by reviewing the Tech Specs page for each management pack at https://marketplace.vmware.com. For example, the Management Pack for NSX-v, Management Pack for Storage Devices, and Management Pack for SDDC Health Management, and the Management Pack for Site Recovery Manager are not natively included with vRealize Operations 7.0 and Cloud Foundation.

Procedure

1 Download any needed management pack upgrades from https://marketplace.vmware.com.

2 Log in to vRealize Operations Manager by using the operations interface.

3 Upgrade the applicable management pack.

   a On the main navigation bar, click **Administration**.

   b In the left pane of vRealize Operations Manager, click **Solutions**.

   c On the **Solutions** page, click **Add**.

   d On the **Select a Solution** page, browse your file system and locate the .pak file of management pack to be upgraded.

   e Select **Install the PAK file even if it is already installed**, click **Upload**, and click **Next**.

   f On the **End User Agreement** page, select the **I accept the terms of this agreement** check box and click **Next**.

   g After the upgrade is complete, click **Finish**.

4 Verify that the adapters related to the upgraded management pack are collecting metrics.

   a On the **Solutions** page, select the relevant solution from the solution table.

   b Under **Configured Adapter Instances**, verify that the **Collection State** is `Collecting` and the **Collection Status** is `Data Receiving`.

5 Repeat Steps 3 and 4 for any other management packs that need to be upgraded.

What to do next

- Once you have completed and validated the upgrade, delete the snapshots you took of the vRealize Operations Manager nodes.
- Provide an updated vRealize Operations Manager license key. See vRealize Operations Manager License Keys.

Delete the Snapshots of the vRealize Operations Manager Nodes

After completing the upgrade of vRealize Operations Manager and verifying operations and functionality, you delete the virtual machine snapshots.

Procedure

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

2 From the **Home** menu, select **VMs and Templates**.

3 Navigate to the first vRealize Operations Manager virtual machine, right-click it, and select **Snapshots > Manage Snapshots**.

4 Click the snapshot that you created before the vRealize Operations Manager upgrade, click the **Delete a VM Snapshot** icon and click **Yes**.

5 In the **Confirm Delete** dialog box, click **Yes**.

6 Repeat this procedure for the remaining vRealize Operations Manager virtual machines.

Upgrade vRealize Log Insight from 4.3.0 to 4.7.0

In order to use vRealize Log Insight with Cloud Foundation 3.5.1, you must manually upgrade vRealize Log Insight to version 4.7.0.

vRealize Log Insight is automatically deployed as part of Cloud Foundation 2.3.2.5, so you must upgrade vRealize Log Insight to 4.7.0.

Prerequisites

- Take snapshots of all vRealize Log Insight VMs.

- Download the VMware vRealize Log Insight 4.5.1- Upgrade Package (`VMware-vRealize-Log-Insight-4.5.1-<build>.pak`) from my.vmware.com.
- Download the VMware vRealize Log Insight 4.6.2- Upgrade Package (`VMware-vRealize-Log-Insight-4.6.2-<build>.pak`) from my.vmware.com.
- Download the VMware vRealize Log Insight 4.7.0- Upgrade Package (`VMware-vRealize-Log-Insight-4.7.0-<build>.pak`) from my.vmware.com.

Procedure

1. Disable Pre-Upgrade Verification in vRealize Log Insight

   You must disable pre-upgrade verification before you apply the vRealize Log Insight upgrade packages.

2. Take Snapshots of the vRealize Log Insight Virtual Machines

   Before you perform the upgrade of vRealize Log Insight, take a snapshot of each node. If you must perform a rollback of vRealize Log Insight to the previous state, these snapshots accelerate the rollback operation.

3. Upgrade vRealize Log Insight

   To upgrade vRealize Log Insight from 4.3.0 to 4.7.0, you must apply three upgrade packages, in order.

4. Upgrade the Content Packs on vRealize Log Insight

   Content packs are plugins to vRealize Log Insight that provide pre-defined knowledge about specific types of events such as log messages. You must upgrade to the latest content packs for use with vRealize Log Insight 4.7.0.

5. Delete the Snapshots of the vRealize Log Insight Virtual Machines

   After completing the upgrade of vRealize Log Insight and verifying operations and functionality, you delete the virtual machine snapshots.

Disable Pre-Upgrade Verification in vRealize Log Insight

You must disable pre-upgrade verification before you apply the vRealize Log Insight upgrade packages.

Procedure

1. Log in to the vRealize Log Insight user interface on the Log Insight master node as the admin user.
2. Open a second tab in the same browser and connect to `https://<Log Insight master node>/internal/config`.
3. Add the following line inside the `<upgrade></upgrade>` stanza:

   ```
   <upgrade-prevalidation-enabled value="false" /> #
   ```

4. Click the **SAVE** button.

Take Snapshots of the vRealize Log Insight Virtual Machines

Before you perform the upgrade of vRealize Log Insight, take a snapshot of each node. If you must perform a rollback of vRealize Log Insight to the previous state, these snapshots accelerate the rollback operation.

Procedure

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

2 Take a snapshot of each vRealize Log Insight node (master node and worker nodes).

3 Verify that the snapshots for each vRealize Log Insight node are successfully created.

Upgrade vRealize Log Insight

To upgrade vRealize Log Insight from 4.3.0 to 4.7.0, you must apply three upgrade packages, in order.

Procedure

1 Log in to the vRealize Log Insight user interface as the admin user.

2 Click the configuration drop-down menu icon ☰ and select **Administration**.

3 Under **Management**, click **Cluster** and click **Upgrade Cluster**.

4 Browse to the location of the `VMware-vRealize-Log-Insight-4.5.1-<build>.pak` file on your local file system and click **Open**.

5 In the **Upgrade Log Insight** dialog box, click **Upgrade** and wait until the .pak file uploads to the master node.

6 On the **End User License Agreement** page, click **Accept**.

The Upgrade Log Insight progress dialog box opens.

7 After the upgrade of the master node completes, click **OK** in the Upgrade Successful dialog box.

The upgrade of the remaining nodes in the cluster starts automatically. After the upgrade process for the cluster completes, the Integrated Load Balancer comes online and displays as **Available**.

8 Repeat the steps above for the other upgrade packages:

- `VMware-vRealize-Log-Insight-4.6.2-<build>.pak`
- `VMware-vRealize-Log-Insight-4.7.0-<build>.pak`

Upgrade the Content Packs on vRealize Log Insight

Content packs are plugins to vRealize Log Insight that provide pre-defined knowledge about specific types of events such as log messages. You must upgrade to the latest content packs for use with vRealize Log Insight 4.7.0.

Procedure

1 Log in to the vRealize Log Insight user interface as the admin user.

2. Click the configuration drop-down menu icon ☰ and select **Content Pack**.
3. In the **Content Pack** pane, under **Content Pack Market Place**, click **Updates**.
4. In the **Log Insight Content Pack Marketplace** pane, click **Update All** to upgrade all content packs to the latest version.

What to do next

After you upgrade the content packs, click each of the items under **Installed Content Packs** and verify that the version number of each content pack matches the version in the VMware Cloud Foundation 3.5.1 Release Notes.

Delete the Snapshots of the vRealize Log Insight Virtual Machines

After completing the upgrade of vRealize Log Insight and verifying operations and functionality, you delete the virtual machine snapshots.

Procedure

1. Log in to vCenter Server by using the vSphere Web Client.
2. From the **Home** menu, select **VMs and Templates**.
3. Navigate to the first vRealize Log Insight virtual machine, right-click it, and select **Snapshots > Manage Snapshots**.
4. Click the snapshot that you created before the vRealize Log Insight upgrade, click the **Delete a VM Snapshot** icon and click **Yes**.
5. In the **Confirm Delete** dialog box, click **Yes**.
6. Repeat this procedure for the remaining vRealize Log Insight virtual machines.

Before You Start the Upgrade 4

Before you begin the upgrade to 3.5.1, it is important that you follow the instructions in this section carefully to avoid any issues.

This chapter includes the following topics:

Upgrade Prerequisites

Ensure that you meet the prerequisites described in this section before starting the upgrade process. Note that you cannot change or consolidate the VXLAN networks used when upgrading to 3.5.x.

- Read the VMware Cloud Foundation Planning and Preparation Guide to understand how to prepare your environment for Cloud Foundation 3.5.1.
- Your Cloud Foundation environment must be at version 2.3.2.5. If you are at an earlier version, you must upgrade to 2.3.2.5 before migrating to version 3.5.1. For information on how to upgrade, refer to the Release Notes for the version in your current environment.
- All assigned hosts must have ESXi 6.5.0-10719125 installed. See Verify the ESXi Version of the Cloud Foundation Hosts.
- Ensure that the SDDC Manager VM names are the default VM names as seen in vCenter Server:
  - SDDC Manager Utility
  - SDDC Manager Controller

  If they were renamed, revert to the default names. These names are used for powering down the VMs and the inventory will not recognize them if they have been renamed.
- Update the firmware in your environment.

The upgrade process upgrades vSphere 6.5EP11 to 6.7U1, which may require firmware updates in order to stay compliant with the VMware Hardware Compatibility List. Firmware updates must be made prior to beginning this upgrade. Ensure that any new firmware versions are supported with both the current (6.5 EP11) and new (6.7U1) releases.

- Ensure that all Cisco ToR and Inter Rack switches have a switch OS version of NX-OS 7.0(3)I7(1) and are supported by VCF 2.3.2. See the VMware Compatibility Guide.
- Make sure that no VMs are associated with non-routable or OOB port groups. During upgrade, non-routable and OOB port groups are deleted. If any VMs are associated with a non-routable or OOB port group, the configuration drift upgrade fails.
- Take a back up of the workloads deployed on each of the VI domains.
- Take a backup or snapshot of the management components (SDDC Manager Controller VM, SDDC Manager Utility VM, vCenter Server, PSC, NSX Manager, and NSX Controllers) on the management domain and all VI workload domains.
- Unassigned hosts (hosts that do not belong to a VI workload domain) will not be migrated. After the upgrade, these hosts must be re-imaged and added to the Cloud Foundation inventory.
- Collect logs for your Cloud Foundation system using SoS. For more information, see Collect Logs for Your Cloud Foundation System in the *Administering VMware Cloud Foundation* document.
- Run the following commands and save the output. You may need this information to control and configure the network going forward.
  - `/home/vrack/bin/lookup-password`

    Fetches all passwords.
  - `/opt/vmware/sddc-support/sos --health-check`

    Fetches IP addresses of management entities and generates health report.
  - `opt/vmware/sddc-support/sos --get-host-ips`

    Fetches host IP addresses.
- VMware Cloud Foundation 3.5.1 does not manage data center connections to external networks. If you have external networks in your Cloud Foundation 2.3.2.5 system, gather information about them from the SDDC Manager Dashboard (**Settings > Network Settings > Data Center**) before you begin network migration. These networks will not be migrated to 3.5.1.

Verify the ESXi Version of the Cloud Foundation Hosts

In order to upgrade to Cloud Foundation 3.5.1, all assigned hosts must have ESXi 6.5.0-10719125 installed. Before you begin the upgrade verify that the correct version is installed.

In some cases, Cloud Foundation 2.3.2.5 may incorrectly update the ESXi version recorded in the inventory, even though an upgrade did not succeed. Check the actual version of ESXi in the vSphere Client and compare it to the version reported in Cloud Foundation.

Procedure

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

2 Select **Hosts and Clusters** from the menu.

3 Select the first host and click the **Summary** tab.

The **Hypervisor** row should display `VMware ESXi, 6.5.0, 10719125`.

4 Repeat for each host, noting which hosts show a version other than `VMware ESXi, 6.5.0, 10719125`.

If all hosts show `VMware ESXi, 6.5.0, 10719125`, you are ready to upgrade to Cloud Foundation 3.5.1.

If any hosts show an earlier version of ESXi, check the host version reported in Cloud Foundation.

5 Log in to the SDDC Manager Controller VM as root.

6 Run this command to determine the IDs of the Workload Domains in Cloud Foundation:

```
curl -H 'Accept:application/json' -H 'Content-Type:application/json' -X GET https://<ip-address-of-SDDC-Manager-VM>/vrm-ui/api/1.0/vrm/logical-inventory/domains/ -u '<username:password>'
```

You should see output similar to:

```
{"type":"MANAGEMENT","domainId":"c6925a57-3210-306e-a416-98b82effdf24","domainName":"Management-gss-vrack1"},
{"type":"IaaS","domainId":"ff3f197f-3864-4eda-8083-bffc2acb3ba4","domainName":"Iaas-1"}]
```

7 Run this command to get the inventory of each domain using the `domainId` from step 6.:

```
curl -H 'Accept:application/json' -H 'Content-Type:application/json' -X GET https://<ip-address-of-SDDC-Manager-VM>/vrm-ui/api/1.0/vrm/logical-inventory/domains/<domainId>/inventory -u
'<username:password>'
```

The output shows the ESXi hosts in each domain and the version of ESXi. For example:

```
{
"id": "e455705b-8d8e-4889-b4d5-2facb26bf321",
"type": "ESXI",
"value": "6.5.0-10719125"
}
```

8 For each host that displayed a version other than `VMware ESXi, 6.5.0, 10719125` in vCenter Server, make sure the Cloud Foundation reports the same version.

If all hosts show the same ESXi version in Cloud Foundation and vCenter Server, use LCM to upgrade them to `VMware ESXi, 6.5.0, 10719125`. See Patching and Upgrading Cloud Foundation.

If Cloud Foundation reports a later ESXi version than vCenter Server, modify the version in Cloud Foundation to match the version reported by vCenter Server.

9 Run this command to match the ESXi version of a host in the Cloud Foundation inventory to the version reported by vCenter Server:

```
curl -H 'Accept:application/json' -H 'Content-Type:application/json' -X POST https://<ip-address-of-SDDC-Manager-VM>/vrm-ui/api/1.0/vrm/logical-inventory/action/entity/version -u '<username:password>' -d '{"id":"<host-id>", "type": "ESXI", "value": "<esxi-version-from-vcenter>"}'
```

The *<esxi-version-from-vcenter>* should look like this: `6.5.0-10175896`, where `10175896` is the build number. Repeat for each mismatched host.

The Cloud Foundation ESXi versions matches the vCenter ESXi versions.

10 Use LCM to upgrade each modified host to `VMware ESXi, 6.5.0, 10719125`. See Patching and Upgrading Cloud Foundation.

Clean Up Downloaded Cloud Foundation 3.x LCM Bundles

Before you can upgrade to Cloud Foundation 3.5.1, you must turn off Lifecycle Management (LCM) manifest polling and clean up downloaded 3.x bundles that could interfere with the upgrade.

If LCM in Cloud Foundation 2.3.2.5 is set up to poll for update bundles, and Cloud Foundation 3.x bundles are downloaded to the SDDC Manager Controller VM, then these bundles could cause issues in Cloud Foundation 3.5.1.

Procedure

1 SSH in to the SDDC Manager Controller VM as root.

2 Make a backup copy of the `application-evo.properties` file:

```
cp /home/vrack/lcm/lcm-app/conf/application-evo.properties /var/tmp/
```

3 Open the `application-evo.properties` file in a text editor:

```
vi /home/vrack/lcm/lcm-app/conf/application-evo.properties
```

4 Set the value of `lcm.core.enableManifestPolling` to `false`.

```
lcm.core.enableManifestPolling=false
```

5 Save and close the file by typing `:wq`.

6 Restart the lcm service:

```
systemctl restart lcm
```

Cloud Foundation 2.3.2.5 will not download any more update bundles until polling is enabled.

7 Clean up any Cloud Foundation 3.x bundles that were downloaded prior to disabling polling.

Important Contact VMware Support to remove any downloaded 3.x bundles that could interfere with the upgrade.

Configure External Services

You must configure a set of external services before starting the migration.

The following table lists the required external services.

Table 4-1. External Services

Service	Purpose
Dynamic Host Configuration Protocol (DHCP)	Provides automated IP address allocation for VXLAN Tunnel Endpoints (VTEPs).
Domain Name Services (DNS)	Provides name resolution for the various components in the solution.
Network Time Protocol (NTP)	Synchronizes time between the various components.

DHCP

During the migration process, Cloud Foundation uses Dynamic Host Configuration Protocol (DHCP) to automatically configure each VMkernel port of an ESXi host used as a VTEP with an IPv4 address. Previously, the VTEPs were configured using static IP addresses. A new DHCP scope is required to support the VTEP transition from static to DHCP address assignment. You can add the scope to an existing or a new DHCP server.

Requirements for the DHCP server are:

- The DHCP server must be accessible on all NSX VXLAN networks in your environment. For a single Cloud Foundation deployment, this could be a single VXLAN.
- You must define a scope for every unique NSX VXLAN network deployed across the management domain and workload domains. Multiple workloads in a Cloud Foundation deployment can share a single VXLAN network.
- The new scope's subnet (IP address prefix and prefix length) values must be the same as what Cloud Foundation is currently using for VTEP static addresses. You cannot change the VXLAN networks during the upgrade process.
- Minimum host address capacity for a scope is three times the count of ESXi hosts in that scope's network + two extra IP addresses for validation.

You can include currently-assigned static VTEP addresses in the new DHCP scope, if required. For L2 uplinks, VXLAN VLANs must be tagged (enabled) on both north and south bound links of the datacenter uplink.

To check the pre-migration static VTEP address allocations:

1 Use the vSphere Web Client to connect to the vCenter Server for Cloud Foundation.

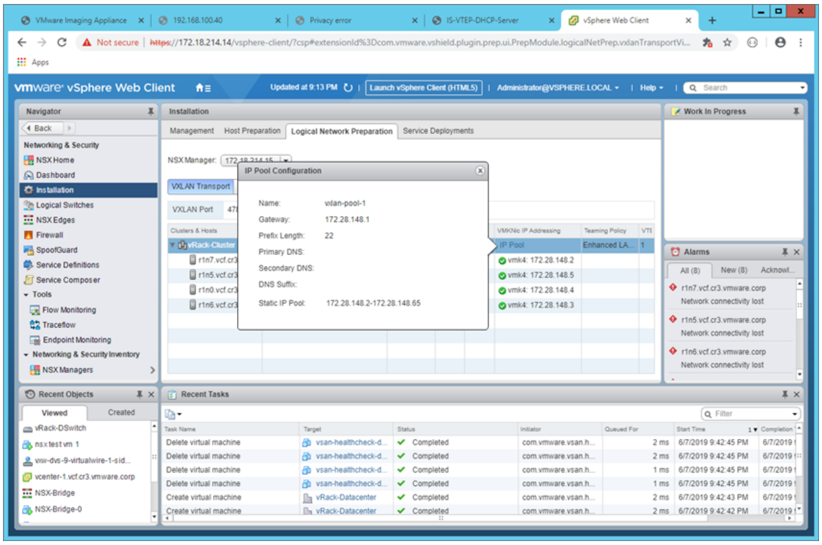
2 Select **Networking & Security**.

3 Select **Installation > Logical Network Preparation > VXLAN Transport**.

4 For each workload, select an NSX Manager from the drop-down menu.

5 Click the cluster name to view the hosts. This lists currently-assigned addresses. The VLAN column shows the VLAN ID presently being used for the workload's VXLAN VTEP network.

6 Click **IP Pool** to view the VTEP subnet parameters. The subnet settings for your new DHCP scope(s) must match these values, although the offered host addresses may be different.



NSX Manager: 172.18.214.15

IP Pool Configuration

Name: vxlan-pool-1
Gateway: 172.28.148.1
Prefix Length: 22
Primary DNS:
Secondary DNS:
DNS Suffix:
Static IP Pool: 172.28.148.2-172.28.148.65

Clusters & Hosts	VMKNic IP Addressing	Teaming Policy	VTE
vRack-Cluster	IP Pool	Enhanced LA...	1
r1n7.vcf.cr3	vmk4: 172.28.148.2		
r1n5.vcf.cr3	vmk4: 172.28.148.5		
r1n0.vcf.cr3	vmk4: 172.28.148.4		
r1n6.vcf.cr3	vmk4: 172.28.148.3		

r1n7.vcf.cr3.vmware.corp
Network connectivity lost
r1n5.vcf.cr3.vmware.corp
Network connectivity lost
r1n6.vcf.cr3.vmware.corp
Network connectivity lost

Recent Tasks

Task Name	Target	Status	Initiator	Queued For	Start Time	Completion
Delete virtual machine	vsan-healthcheck-d...	Completed	com.vmware.vsan.h...	2 ms	6/7/2019 9:42:45 PM	6/7/2019
Delete virtual machine	vsan-healthcheck-d...	Completed	com.vmware.vsan.h...	2 ms	6/7/2019 9:42:45 PM	6/7/2019
Delete virtual machine	vsan-healthcheck-d...	Completed	com.vmware.vsan.h...	1 ms	6/7/2019 9:42:45 PM	6/7/2019
Delete virtual machine	vsan-healthcheck-d...	Completed	com.vmware.vsan.h...	1 ms	6/7/2019 9:42:45 PM	6/7/2019
Create virtual machine	vRack-Datacenter	Completed	com.vmware.vsan.h...	2 ms	6/7/2019 9:42:43 PM	6/7/2019
Create virtual machine	vRack-Datacenter	Completed	com.vmware.vsan.h...	2 ms	6/7/2019 9:42:42 PM	6/7/2019

Important When you run the pre-validation script, it validates the DHCP server configuration. Do not perform manual testing of the DHCP server, since doing so may convert existing VTEPs to have DHCP addressing. Although this will not affect migration, it will affect rollback if migration fails.

DNS

You must configure a DNS server that is reachable from the Cloud Foundation rack over the management VLAN. DNS domain information is used to configure Cloud Foundation components. The root DNS domain and subdomain information are required.

DNS resolution must be available for all of the components contained within the Cloud Foundation solution. This includes servers, virtual machines, and any virtual IPs used.

You must populate the external DNS with FQDNs and with full forward and reverse lookup entries. See Add FQDNs to DNS Server.

Caution Disable any DNS forwarding to the SDDC Manager.

NTP

All components must be synchronized against a common time by using the Network Time Protocol (NTP) on all nodes. Important components of Cloud Foundation, such as vCenter Single Sign-On (SSO), are sensitive to a time drift between distributed components. Synchronized time between the various components also assists troubleshooting efforts.

Requirements for the NTP sources include the following:

- The NTP sources must be reachable by all the components in the Cloud Foundation solution on the:
  - Management network
  - vRealize network
- Time skew is less than 5 minutes between NTP sources

Add FQDNs to DNS Server

You must extract the FQDNs from the current Cloud Foundation installation and add these to the external DNS server you configured.

Procedure

1. Using the root credentials, SSH in to the SDDC Manager Controller VM.
2. Navigate to the `/etc/unbound/` directory.
3. Download the `unbound.conf` file to your local computer.
4. Retrieve the FQDNs from the `unbound.conf` file and add them to the external DNS server.
5. Ensure that both forward and reverse DNS resolution is functional for each component.

Complete the Migration Input Sheet

In the 2.3.2.5 version, Cloud Foundation configured DNS and NTP during the bring-up process, and generated passwords for the SDDC components. In the 3.5.1 version, DNS, NTP, and DHCP are configured externally and SDDC management component passwords are managed by the user. After you configure the external services described in this document, you add the infrastructure and verification details and user passwords in the migration sheet and upload it to the SDDC Manager Controller VM. This information is used by the upgrade process.

Gather Data for Migration Sheet

Gather data for the migration sheet so that it is available when you compete the migration sheet.

- IP addresses of the upstream DNS and NTP servers.

  If you have two DNS or NTP servers configured, retrieve both IP addresses to add to the migration sheet. All IP addresses that you specify in the migration sheet must be reachable from the Cloud Foundation racks.

- Cloud Foundation 2.3.2.5 used to manage the passwords for the system components. These passwords are now managed by the user. Decide on the passwords described in the table below, so that you input them in the migration sheet.

Password	Description
SDDC Manager Super User ("vcf")	Used to SSH into the SDDC Manager appliance.
Password for Backup User	Backup user used to configure LCM and NSX backups.
SDDC Manager REST API User ("admin")	User credentials used as part of BasicAuth, if executing the VCF REST API.
SDDC Manager Appliance Root Password	SDDC Manager Appliance root password. Cannot be used to SSH to the appliance.

  Password requirements:

  - 8-20 characters in length
  - At least 1 upper case letter
  - At least 1 lowercase letter
  - At least 1 digit
  - At least 1 special character from the set `@!#$%?^`. The first character in the password cannot be `@`.
  - Cannot include dictionary words

- DHCP subnet, start IP address, and end IP address for each scope.

Input Data to Migration Sheet

This section describes how to download the migration sheet, input the data required for migration, and then upload it to the SDDC Manager VM.

The fields in yellow contain sample values that you can overwrite as appropriate. If a cell turns red, the required information is missing, or validation has failed. For DHCP, you must enter information in at least one row. If at least one row is completed, you can ignore the red cells in the other DHCP rows.

Caution You must type information into each field in the migration sheet. Do not copy and paste from one cell to another.

Prerequisites

You must have Microsoft Office 365 on your local computer to complete the migration sheet.

Procedure

1 Download the migration sheet (`vcf-migration-input.xlsx`) from KB 67459 to your local computer.

2 In the Infrastructure section, enter the following information.

Field	Description
DNS Server #1	IP address of upstream DNS server. The DNS server must be reachable on management VLAN on Cloud Foundation racks.
DNS Server #2	IP address of second DNS server, if configured. Enter n/a in this field if you have a single DNS server in your environment.
NTP Server #1	IP address of upstream NTP server. The NTP server must be reachable.
NTP Server #2	IP address of second NTP server, if configured. Enter n/a in this field if you have a single NTP server in your environment.

3 Enter the following passwords.

Password	Description
SDDC Manager Super User ("vcf")	Used to SSH into the SDDC Manager appliance.
Password for Backup User	Backup user used to configure LCM and NSX backups.
SDDC Manager REST API User ("admin")	User credentials used as part of BasicAuth, if executing the VCF REST API.
SDDC Manager Appliance Root Password	SDDC Manager Appliance root password. Cannot be used to SSH to the appliance.

Password requirements:

- 8-20 characters in length
- At least 1 upper case letter
- At least 1 lowercase letter
- At least 1 digit
- Cannot include dictionary words

Important Do not use special characters in the passwords for super user, backup user, or root user. The REST API user password can contain special characters from the set `@!#$%?^`, as long as the first character in the password is not `@`. If you want to update the passwords to include special characters at a later point in time, see Update Passwords to Include Special Characters.

4 After you complete steps 2, 3, and 4, check the corresponding check boxes in the Existing Infrastructure Details section.

5 In the Customer Pre-configuration Prerequisites section, confirm that each specified pre-requisite has been met.

6 In the SDDC Manager Access section, confirm the following by checking the corresponding check box.

- You can access the `/etc/unbound/unbound.conf` file, which contains DNS records for forward resolution for all Cloud Foundation components.

- You can access the `/home/vrack` directory, where you will create a directory for uploading the migration sheet.
- Credentials and IP addresses for all SDDC components are available in the `/home/vrack/bin/vrm-cli.sh lookup-passwords` file.

7 In the DHCP Scope Verification Details section, enter the following information for each scope.

Note You must enter at least one scope. Leave the unused rows blank. You can ignore the fact that the blank DHCP rows are red.

Field	Description
Subnet	Enter the subnet in CIDR format. For example, 10.130.217.128/26.
Start IP	Starting IP address of the scope.
End IP	Last IP address for the scope.

8 Save the migration sheet.

9 Copy the migration sheet to the SDDC Manager Controller VM.

```
scp vcf-migration-input.xlsx root@<IP_address_of SDDC_Manager_VM>:/root
```

10 SSH in to the SDDC Manager Controller VM and follow these steps.

```
ssh root@<IP_address_of SDDC_Manager_VM>
mv vcf-migration-input.xlsx /home/vrack
chown vrack: /home/vrack/vcf-migration-input.xlsx
su - vrack
mkdir -p BYON_migration/user_input
mv vcf-migration-input.xlsx BYON_migration/user_input
exit # user vrack
exit # logout from SDDC Manager Controller
```

Note If you make any modifications to the migration sheet, repeat steps 10 and 11.

Run Pre-validation Script

Run the pre-validation script to validate that your network is ready for upgrading to 3.5.1. The script checks the physical and logical configuration of the system and determines if the upgrade can handle the deviations between the 2.3.2.5 and 3.5.1 deployments.

Prerequisites

Ensure that the completed migration sheet (`vcf-migration-input.xlsx`) is uploaded to the `~vrack/BYON_migration/user_input/` directory.

Note If you cancel pre-validation before it completes, you will need to delete `vcf-migration-input.xlsx` and upload a new copy in order to run pre-validation again.

If you already ran the pre-validation script, and you rotated passwords after running the script, then you must delete the password cache (`/home/vrack/.VcfAuthCache/`) on the SDDC Manager Controller VM, before you run the pre-validation script again.

Procedure

1. Obtain the pre-validation script (`byon-network-migration-preval-only.tar` file) from the VMware team supporting your upgrade and download it to your local computer.
2. Using the root credentials, SSH in to the SDDC Manager Controller VM.
3. Copy the `byon-network-migration-preval-only.tar` file to the `/home/vrack` directory.
4. Change ownership of the file to vrack user, switch to the vrack user, and untar the file.

   ```
   chown vrack: ~vrack/byon-network-migration-preval-only.tar
   su - vrack
   mkdir preval
   cd preval
   tar xf ../byon-network-migration-preval-only.tar
   ```

5. Run the script.

   ```
   cd ~vrack/preval/bin
   ./run-prevalidation.sh
   ```

   Review the status updates on the console.

6 Review the status, report, and log files at `~vrack/preval/logs/`. Fix errors, if any, and re-run the pre-validation script.

a Check the status for each domain.

```
cd ~vrack/preval/logs/
cat prevalidation_<domain>_exit.json | json_pp
```

For example, `cat prevalidation_MGMT_exit.json | json_pp`. If the status is `"success" : true`, check the other domains. If the status is `"success" : false`, proceed to the next step.

b Check the report to get details on the failure.

```
cat prevalidation_<domain>_report_<time stamp>.json | json_pp
```

For example, `cat prevalidation_MGMT_report_2019-05-23T17_32_10.json | json_pp`. The time stamp appears in the output of the previous step. If the report contains enough information to resolve the issues, do so and re-run the pre-validation script.

c To get more details on a failure, check the log for the domain.

```
cat prevalidation_<domain>.log
```

For example, `cat prevalidation_MGMT.log`. Resolve the issues and re-run the pre-validation script.

Note If you are unable to resolve issues after checking the report and log files, contact VMware Support. Proceed with the upgrade only after the pre-validation run is successful.

Download Upgrade Bundles 5

Download the upgrade bundles before starting the upgrade process.

Note After you apply the configuration drift bundle, you will need to download additional bundles to upgrade the Cloud Foundation components to the versions in the 3.5.1 Bill of Materials (BOM). See Chapter 9 Software BOM Upgrade.

Prerequisites

Contact VMware Support to get access to the download location for the upgrade bundles.

Procedure

- Download the following bundles to a computer with access to the SDDC Manager VM:
  - Network migration bundle
  - Data and services migration bundle
  - Configuration drift bundle

  You will need to upload the relevant bundle to the SDDC Manager VM before each stage of the upgrade.

Network Migration

6

After you meet the migration pre-requisites, including downloading the network upgrade bundle, you must schedule the upgrade. The network migration proceeds in stages.

Each stage of the network migration is executed one workload domain at a time, starting with the management domain.

- Network Pre-validation
- Static IP Pool to DHCP-based IP Pool for VXLAN
- External DNS and NTP Servers
- LAG to LBT

During network migration there is some disruption to network traffic. To avoid disruption, you should quiesce workloads, including any storage-related activity using vSAN.

Important Network migration can take a long time depending on your environment. To ensure successful migration, increase the timeout before you begin. See Increase the Timeout for Network Migration.

Network Pre-validation

Before the first stage begins, Cloud Foundation validates the migration sheet and reports any errors. If network migration fails during pre-validation, address the errors and try again. Pre-validation in the network migration bundle performs the same operations as the standalone pre-validation script (Run Pre-validation Script).

It checks migration readiness of the VCF deployment . It discovers the physical and logical configuration and deviations from 2.3.X deployment and checks if migration can tolerate the drift.

Static IP Pool to DHCP-based IP Pool for VXLAN

VXLAN tunnel endpoints (VTEPs) are converted from a static IP pool to DHCP-based IP pools.

External DNS and NTP Servers

Updates the DNS and NTP configuration of all ESXi hosts, vSphere entities (vCenter Server, Platform Services Controller, NSX) and all ToR and Inter-Rack switches to point to the external DNS and NTP sources that you set up as a prerequisite.

LAG to LBT

The system disables vSphere HA, sets the vSphere DRS automation level to manual, and converts uplink ports on vSphere Distributed Switches from a link aggregation group (LAG) port group to standard uplink port groups. For VLAN, port groups are configured to use Route based on physical NIC load (load-based teaming) and for VXLAN, port groups are configured to use Route based on SRC-ID.

This chapter includes the following topics:

Increase the Timeout for Network Migration

Network migration can exceed the available timeout and fail as a result. Increase the timeout before you begin migration.

Procedure

1 Using SSH, log in as root to the SDDC Manager VM.

2 Go to the `/home/vrack/lcm/lcm-app/conf` directory.

3 Open the `application-evo.properties` file in a text editor.

4 Add the following line:

```
lcm.upgrade.timeout=82800000
```

5 Save and close the `/home/vrack/lcm/lcm-app/conf/application-evo.properties` file.

6 While still logged into the SDDC Manager Controller VM, restart the LCM service.

```
systemctl restart lcm
```

Upload the Network Migration Bundle to the SDDC Manager Controller VM

Before you can schedule the network migration bundle, you must upload the bundle files to the SDDC Manager Controller VM, so that the update appears in the SDDC Manager Dashboard.

The bundle includes the following files:

- `bundle-`*number*`.manifest`
- `bundle-`*number*`.manifest.sig`
- `bundle-`*number*`.tar`

Prerequisites

You must have downloaded the network migration bundle to a computer with access to the SDDC Manager Controller VM. See Chapter 5 Download Upgrade Bundles.

Procedure

1 Create a directory on the SDDC Manager Controller VM for the bundle files.

a Using SSH, log in to the SDDC Manager VM as `root`.

b Create a folder named `/home/vrack/bundles`.

```
mkdir /home/vrack/bundles
```

c Issue the following commands to set the proper ownership and permissions on the `/home/vrack/bundles` folder:

```
chown vrack:vfabric /home/vrack/bundles
```

```
chmod 777 /home/vrack/bundles
```

d Using a file transfer utility, copy the bundle files from the local computer to the `/home/vrack/bundles` folder on the SDDC Manager Controller VM.

e Set the correct ownership and permissions on the files copied to the `/home/vrack/bundles` folder.

```
chown vrack:vfabric /home/vrack/bundles/*
```

```
chmod 777 /home/vrack/bundles/*
```

2 Upload the bundle files to LCM.

While logged in to SDDC Manager Controller VM as `root`, run the following command:

```
curl -k http://localhost:9443/lcm/bundle/upload -X POST -d '{"bundle":"/home/vrack/bundles/bundle-<number>.tar","manifest":"/home/vrack/bundles/bundle-<number>.manifest","signature":"/home/vrack/bundles/bundle-<number>.manifest.sig"}' -H 'Content-Type:application/json'
```

3 Log in to the SDDC Manager Dashboard and navigate to **Lifecycle Management > Updates**.

The bundle is displayed and the status is validating.

4 Verify that the bundle file was uploaded correctly.

What to do next

Schedule a time to apply the bundle.

Schedule Network Migration

You can schedule a time to apply the network migration bundle from the SDDC Manager Dashboard.

Use the SDDC Manager Dashboard to apply the network migration bundle to the management domain. Once the management domain is updated, Cloud Foundation applies the bundle to all VI workload domains.

Prerequisites

- Increase the network migration timeout. See Increase the Timeout for Network Migration.
- Upload the network migration bundle. See Upload the Network Migration Bundle to the SDDC Manager Controller VM.

Procedure

1. On the Lifecycle Management page, click the **UPDATE** tab.
2. Click the drop-down next to Available Updates.
3. Click **UPDATE** next to the network migration bundle.
4. On the TARGET page, select the management domain.
5. Click **NEXT**.
6. On the SCHEDULE page, select the date and time for the update to be applied and click **NEXT**.

   Note Do not reboot the physical racks, any devices on the rack, or the SDDC Manager VM while the upgrade is in progress.
7. Click **NEXT**.
8. On the Review Update page, review the update bundle, targets, and schedule.
9. Click **SCHEDULE UPDATE**.

   The scheduled update appears in the SCHEDULED UPDATES section on the UPDATES tab and displays the time it is scheduled to be installed.
10. Monitor the log file.

    a. Click the Update History tab.

    b. For the latest log file, click **Actions > Download Update Log**.

    c. Open the log file and copy the upgrade-ID.

    d. With root credentials, SSH to the SDDC Manager VM and navigate to `/home/vrack/lcm/upgrades/`*`upgrade-ID`*`/thirdparty/network-migration/logs` where *upgrade-ID* is the ID you copied in step c.

After Network Migration

When network migration completes successfully and before you begin data and services migration, you must perform the following steps.

- Configure NTP for the management switch.

Network migration externalizes NTP services for most components. However, for the management switch, you must manually externalize NTP. Refer to the Cumulus Networks documentation (https://docs.cumulusnetworks.com/) for your version of Cumulus Linux to configure NTP for the management switch.

You can refer to the system network settings that you generated using the SoS utility to enable you to control and configure the network going forward. See Upgrade Prerequisites for more information.

- Disable shell mode access on all vCenter Servers and Platform Services Controllers.

7 Data and Services Migration

During the data and services migration, the new SDDC Manager VM is deployed and the data and services from the old SDDC Manager VMs are migrated to the new SDDC Manager VM.

The system performs the following tasks during data and serices migration:

1 The following data is exported from to a JSON file on the old SDDC Manager Controller VM:

   - Inventory
   - User credentials
   - Identity and security (certificates and SSH keys)
   - NFS mounts

   During this phase, network pools are created. During the data export in step 1, IP addresses assigned to hosts and IP addresses assigned to vSAN and vMotion networks were collected in the JSON file. Network pools are created based on this information.

   In the 3.x version of the software, Cloud Foundation has a new construct called network pools. Network pools automatically assign static IP addresses to vMotion and vSAN 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. IP addresses from the 2.3.2.5 version are mapped to the newly created network pools. The naming convention for network pools is as follows:

   `MigratedPool-,VSAN-`*vlanid*`,VMOTION-`*vlanid*

   For example,

   `MigratedPool-,VSAN-200,VMOTION-100`

2 The new SDDC Manager for 3.5.1 is deployed.

3 Data from the JSON file on the old SDDC Manager Controller VM is imported to the new SDDC Manager VM.

4 LCM data, configuration, and logs are migrated to the new SDDC Manager VM.

5 The new SDDC Manager VM is given control of the Cloud Foundation system.

   a The old SDDC Manager Controller VM and SDDC Manager Utility VM are powered down and removed from the inventory. These VMs are left in the datastore since the logs on these VMs can be used for debugging.

   b Transfers control to LCM on the new SDDC Manager VM. New SDDC Manager is available on the old IP address and hostname.

This chapter includes the following topics:

- Upload the Data and Services Migration Bundle to the SDDC Manager Controller VM
- Schedule Data and Services Migration
- Update Passwords to Include Special Characters

Upload the Data and Services Migration Bundle to the SDDC Manager Controller VM

Before you can schedule the data and services migration bundle, you must upload the bundle files to the SDDC Manager Controller VM, so that the update appears in the SDDC Manager Dashboard.

The bundle includes the following files:

- `bundle-`*number*`.manifest`
- `bundle-`*number*`.manifest.sig`
- `bundle-`*number*`.tar`

Prerequisites

You must have downloaded the data and services migration bundle to a computer with access to the SDDC Manager Controller VM. See Chapter 5 Download Upgrade Bundles.

Procedure

1 Create a directory on the SDDC Manager Controller VM for the bundle files.

   a Using SSH, log in to the SDDC Manager VM as `root`.

   b Create a folder named `/home/vrack/bundles`.

   ```
   mkdir /home/vrack/bundles
   ```

   c Set the correct ownership and permissions on the `/home/vrack/bundles` folder.

   ```
   chown vcf_lcm:vcf /home/vrack/bundles
   ```

   ```
   chmod -R 777 /home/vrack/bundles
   ```

   d Using a file transfer utility, copy the bundle files from the local computer to the `/home/vrack/bundles` folder on the SDDC Manager Controller VM.

   e Set the correct ownership and permissions on the files copied to the `/home/vrack/bundles` folder.

   ```
   chown vcf_lcm:vcf /home/vrack/bundles/*
   ```

   ```
   chmod -R 777 /home/vrack/bundles/*
   ```

2 Upload the bundle files to LCM.

While logged in to SDDC Manager Controller VM as `root`, run the following command:

```
curl -k https://192.168.100.40:9443/lcm/bundle/upload -X POST -d '{"bundle":"/home/vrack/bundles/
bundle-<number>.tar","manifest":"/home/vrack/bundles/bundle-<number>.manifest","signature":"/home/
vrack/bundles/bundle-<number>.manifest.sig"}' -H 'Content-Type:application/json'
```

3 Log in to the SDDC Manager Dashboard and navigate to **Lifecycle Management > Updates**.

The bundle is displayed and the status is validating.

4 Verify that the bundle file was uploaded correctly.

What to do next

Schedule a time to apply the bundle.

Schedule Data and Services Migration

You can schedule a time to apply the data and services migration bundle from the SDDC Manager Dashboard.

Use the SDDC Manager Dashboard to apply the data and services migration bundle to the management domain. Once the management domain is updated, Cloud Foundation applies the bundle to all VI workload domains.

Prerequisites

- You must have uploaded the data and services migration bundle. See Upload the Data and Services Migration Bundle to the SDDC Manager Controller VM.
- Ensure that there are no files with root-only privileges in the `/home/vrack/lcm/logs/` or `/home/vrack/lcm` directory, otherwise data migration may fail.

Procedure

1 On the Lifecycle Management page, click the **UPDATE** tab.

2 Click the drop-down next to Available Updates.

3 Click **UPDATE** next to the data and services migration bundle.

4 On the TARGET page, select the management domain.

5 Click **NEXT**.

6 On the SCHEDULE page, select the date and time for the update to be applied and click **NEXT**.

Note Do not reboot the physical racks, any devices on the rack, or the SDDC Manager VM while the upgrade is in progress.

7 Click **NEXT**.

8 On the Review Update page, review the update bundle, targets, and schedule.

9 Click **SCHEDULE UPDATE**.

   The scheduled update appears in the SCHEDULED UPDATES section on the UPDATES tab and displays the time it is scheduled to be installed.

10 Monitor the progress by navigating to the log file.

   a Click the Update History tab.

   b For the latest log file, click **Actions > Download Update Log**.

   c Open the log file and copy the upgrade-ID.

   d With root credentials, SSH to the SDDC Manager VM and navigate to `/home/vrack/lcm/upgrades/`*`upgrade-ID`*`/thirdparty/platform-exports/logs` where *upgrade-ID* is the ID you copied in step c.

   e When this log file shows the status as being completed, navigate to the second log file at `/home/vrack/lcm/upgrades/`*`upgrade-ID`*`/sddcmanager-migration-app/logs`.

The system transfers control to the new SDDC Manager VM. After the control has been passed to the new SDDC Manager, the UI may display an error or show no progress. Refresh the browser to be redirected to the new UI. Use the same credentials to log in to the SDDC Manager Dashboard as your 2.3.2.5 instance.

Update Passwords to Include Special Characters

Some of the passwords that you provided in the migration sheet could not include special characters. If you want to update those passwords to include special characters, you can do so before you apply the configuration drift bundle.

The following passwords that you provided in the migration sheet could not include special characters (`@!#$%?^`).

Password	Description
SDDC Manager Super User ("vcf")	Used to SSH into the SDDC Manager appliance.
Password for Backup User	Backup user used to configure LCM and NSX backups.
SDDC Manager Appliance Root Password	SDDC Manager Appliance root password. Cannot be used to SSH to the appliance.

After you complete the data and services migration, you can update those passwords to include special characters. Password requirements:

- 8-20 characters in length
- At least 1 upper case letter
- At least 1 lowercase letter
- At least 1 digit
- At least 1 special character from the set `@!#$%?^`. The first character in the password cannot be `@`.

- Cannot include dictionary words

Procedure

1. SSH in to the SDDC Manager VM as `vcf` and then switch to the root user by issuing the `su -` command.
2. Type one of the following commands to update a password.

Option	Description
`passwd`	To update the root password.
`passwd vcf`	To update the super user ("vcf") password.
`passwd backup`	To update the backup user password.

3. Enter the new password.
4. Re-enter the new password.

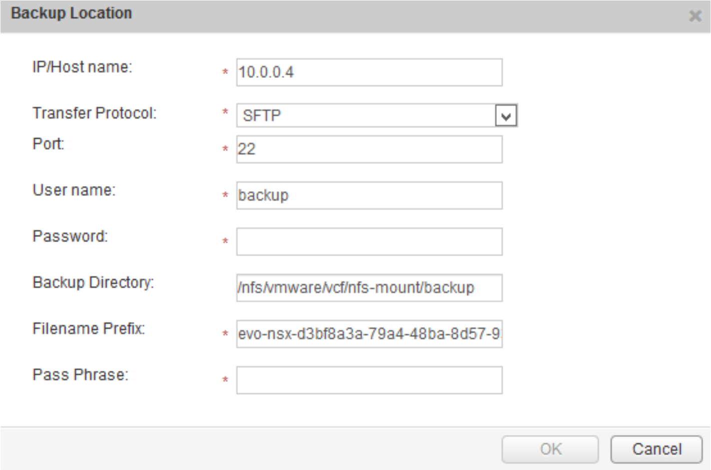
   The password is updated.

5. If you updated the backup user password, you must enter the new password in NSX Manager.

   a. Using a web browser, log in to the NSX Manager Virtual Appliance, `https://<hostname>`, where *<hostname>* is the FQDN or IP address of the NSX Manager.

   b. Click **Backup & Restore**.

   c. Click the **Change** button next to FTP Server Settings.



Backup Location

IP/Host name: * 10.0.0.4

Transfer Protocol: * SFTP

Port: * 22

User name: * backup

Password: *

Backup Directory: /nfs/vmware/vcf/nfs-mount/backup

Filename Prefix: * evo-nsx-d3bf8a3a-79a4-48ba-8d57-9

Pass Phrase: *

   d. Make sure the user name is `backup`, then enter the new password for both **Password** and **Pass Phrase**.

   e. Click **OK**.

8 Configuration Drift

During the configuration drift stage of the upgrade process, new configurations are applied to the Cloud Foundation components to make them compatible with 3.5.1 features.

During the configuration drift update, the system performs the following tasks.

- Creates, assigns, and authorizes the necessary Admin groups
- Re-configures SSO On NSX
- Creates VM clusters and sets up monitoring rules
- Configures NSX backup depot
- Create PSC/VC VmGroups
- Creates cluster VM to VM rule
- Configures cluster VM monitoring settings
- Creates NFS datastore on hosts in the management domain
- Disables Bash Shell on Platform Services Controller and vCenter Server
- Deletes anti-affinity rule setup by 2.3.x SDDC Manager
- Configures vSAN storage policy
- Cleans up Out of Band vmknic from hosts and VMs and deletes the portgroup
- Moves migrated management VMs to the SDDC-Management-ResourcePool
- Applies configuration drift on vRealize components
- Updates vRealize DNS and NTP for all vRealize Components
- Performs the following steps for vRealize Log Insight
- - Enables log collection for vSphere
  - Configures vRealize Log Insight Agent
- Performs the following steps for vRealize Operations
  - Cleans up existing NSX Edge configuration
  - Generates certificates for NSX Edge
  - Generates application profiles
  - Configure anti-affinity rules

- Performs the following steps for vRealize Automation
  - Cleans up NSX Load Balancer configuration.
  - Cleans up existing NSX Edge configuration
  - Configures NSX Load Balancer
  - Configures anti-affinity rules

This chapter includes the following topics:

- Upload the Configuration Drift Bundle to the SDDC Manager VM
- Schedule the Configuration Drift Update

Upload the Configuration Drift Bundle to the SDDC Manager VM

Before you can schedule the configuration drift bundle update, you must upload the bundle files to the SDDC Manager VM, so that the update appears in the SDDC Manager Dashboard.

The bundle includes the following files:

- `bundle-`*number*`.manifest`
- `bundle-`*number*`.manifest.sig`
- `bundle-`*number*`.tar`

Prerequisites

You must have downloaded the configuration drift bundle to a computer with access to the SDDC Manager VM. See Chapter 5 Download Upgrade Bundles.

Procedure

1. Create a directory on the SDDC Manager VM for the bundle files.

   a. SSH to the SDDC Manager VM as the **vcf** user and use the `su -` command to switch to the root user.

   b. Create a folder named `/home/vcf/bundles`.

   ```
   mkdir /home/vcf/bundles
   ```

   c. Set the correct ownership and permissions on the `/home/vcf/bundles` folder.

   ```
   chown vcf_lcm:vcf /home/vcf/bundles
   ```

   ```
   chmod -R 777 /home/vcf/bundles
   ```

   d. Using a file transfer utility, copy the bundle files from the local computer to the `/home/vcf/bundles` folder on the SDDC Manager VM.

   e. Set the correct ownership and permissions on the files copied to the `/home/vcf/bundles` folder.

```
chown vcf_lcm:vcf /home/vcf/bundles/*
```

```
chmod -R 777 /home/vcf/bundles/*
```

2 Upload the bundle files to LCM.

While logged in to SDDC Manager VM as `root`, run the following command:

```
curl -k http://localhost/lcm/bundle/upload -X POST -d '{"bundle":"/home/vcf/bundles/bundle-
<number>.tar","manifest":"/home/vcf/bundles/bundle-<number>.manifest", "signature":"/home/vcf/
bundles/bundle-<number>.manifest.sig"}' -H 'Content-Type:application/json'
```

3 Log in to the SDDC Manager Dashboard and navigate to **Repository > Bundles**.

The bundle is displayed and the status is validating.

4 Verify that the bundle file was uploaded correctly.

What to do next

Schedule a time to apply the bundle.

Schedule the Configuration Drift Update

You can schedule a time to apply the configuration drift bundle from the SDDC Manager Dashboard.

Prerequisites

You must have uploaded the configuration drift bundle. See Upload the Configuration Drift Bundle to the SDDC Manager VM.

Procedure

1 On the SDDC Manager Dashboard, click **Inventory > Workload Domains**.

2 Click the management domain and then click the Updates/Patches tab.

The Configuration drift upgrade bundle that you downloaded before starting the upgrade process is available here.

3 Schedule the Configuration drift bundle by clicking **Schedule** next to the bundle and selecting the date and time you want the bundle to be applied.

The configuration drift is applied on the management domain first and then on each VI workload domain in your environment. The Updates/Patches tab displays the status of this task.

4 Monitor the log file.

a Click the Update History tab.

b For the latest log file, click **Actions > Download Update Log**.

c Open the log file and copy the upgrade-ID.

d With root credentials, SSH to the SDDC Manager VM and navigate to `/var/log/vmware/vcf/lcm/upgrades/`*`upgrade-ID`*`/sddcmanager-migration-app/logs/` where *upgrade-ID* is the ID you copied in step c.

Software BOM Upgrade

9

You must apply a series of bundles to all workload domains in your environment to upgrade the Cloud Foundation components to the versions in the 3.5.1 Bill of Materials (BOM).

This chapter includes the following topics:

Turn On LCM Manifest Polling

In order for the software BOM bundles to appear in the SDDC Manager Dashboard, you must turn on LCM manifest polling.

Procedure

1 SSH in to the SDDC Manager VM as `vcf` and then switch to the root user by issuing the `su -` command.

2 Make a backup copy of the `application-prod.properties` file:

```
cp /opt/vmware/vcf/lcm/lcm-app/conf/application-prod.properties /var/tmp/
```

3 Open the `application-prod.properties` file in a text editor:

```
vi /opt/vmware/vcf/lcm/lcm-app/conf/application-prod.properties
```

4 Set the value of `lcm.core.enableManifestPolling` to `true`.

```
lcm.core.enableManifestPolling=true
```

5 Save and close the file by typing `:wq`.

6 Restart the lcm service:

```
systemctl restart lcm
```

Log In to Your My VMware Account

You must be logged in to your My VMware Account to download the software BOM upgrade bundles.

Procedure

1 In the SDDC Manager Dashboard, click **Administration > Repository Settings** .

2 Click **Login**.

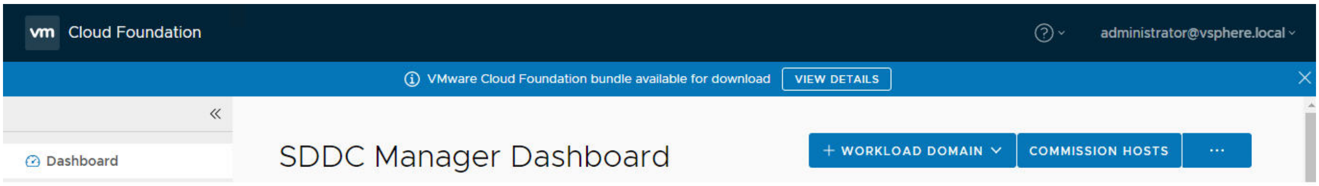
The sign in page appears.

3 Type your My VMware account user name and password.

4 Click **Log In**.

Download Bundles from SDDC Manager

When upgrade bundles are available for your environment, a message is displayed on the SDDC Manager Dashboard.



VMware Cloud Foundation bundle available for download

To download an install bundle, navigate to **Repository > Bundles** on the SDDC Manager Dashboard to view the available bundles. Then follow the instructions in step 4 below.

Prerequisites

If you have previously edited the application-prod.properties file on SDDC Manager VM to download upgrade bundles in an offline mode, you must edit it again before downloading bundles from SDDC Manager. Follow the steps below:

1 Using SSH, log in to the SDDC Manager VM with the following credentials:

Username: vcf

Password: use the password specified in the deployment parameter sheet

2 Enter su to switch to the root user.

3 Open the `/opt/vmware/vcf/lcm/lcm-app/conf/application-prod.properties` file.

4 Set `lcm.core.enableManifestPolling=true`.

5 Restart LCM service witht the command below:

```
systemctl restart lcm
```

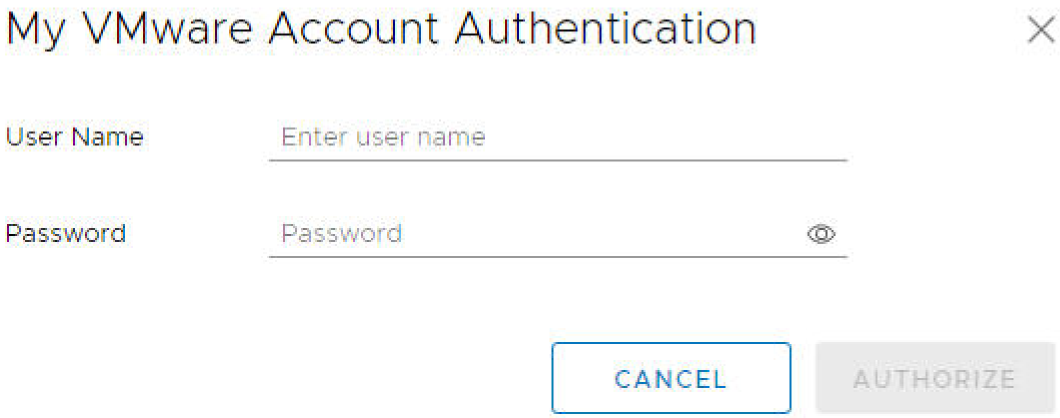
Procedure

1 Log in to your My VMware Account.

   a On the SDDC Manager Dashboard, click **Administration > Repository Settings**.

   b Click **Authenticate**.

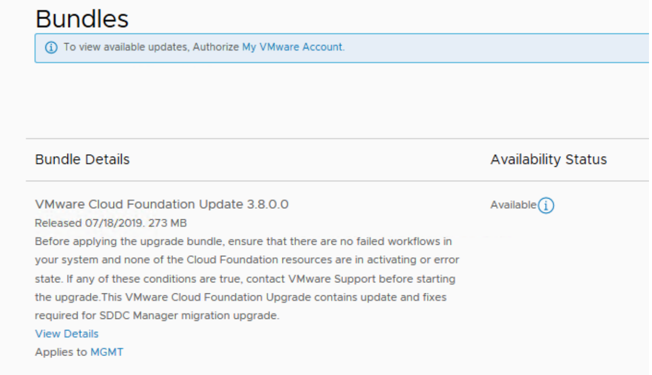
   The My VMware Account Authentication page appears.



   c Type your user name and password.

   d Click **Authorize**.

2 To download a bundle, navigate to **Repository > Bundles** on the SDDC Manager Dashboard to view the available bundles.



Bundles

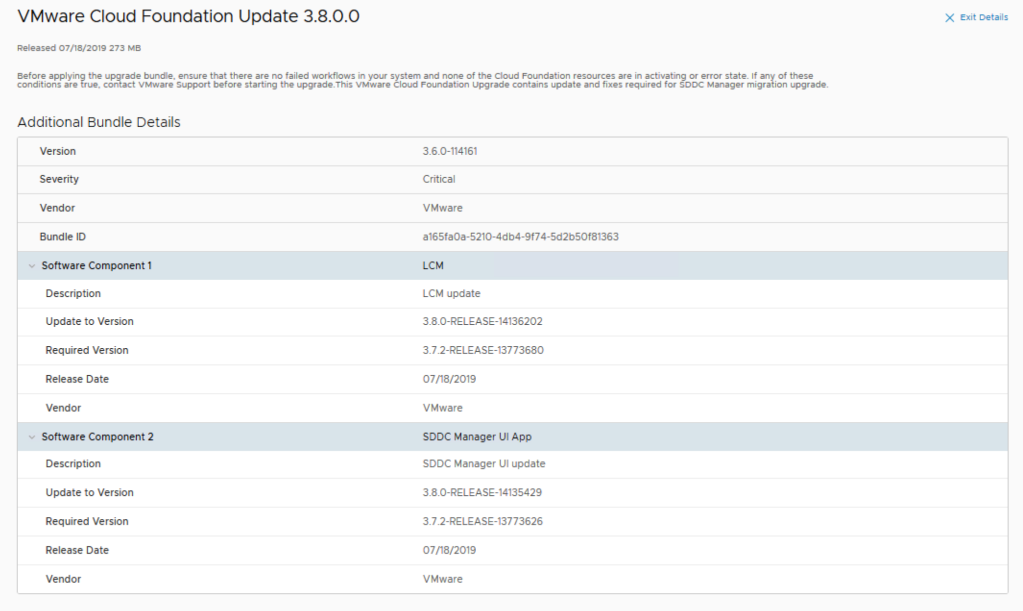
ⓘ To view available updates, Authorize My VMware Account.

Bundle Details	Availability Status
VMware Cloud Foundation Update 3.8.0.0 Released 07/18/2019. 273 MB Before applying the upgrade bundle, ensure that there are no failed workflows in your system and none of the Cloud Foundation resources are in activating or error state. If any of these conditions are true, contact VMware Support before starting the upgrade.This VMware Cloud Foundation Upgrade contains update and fixes required for SDDC Manager migration upgrade. View Details Applies to MGMT	Available ⓘ

The Bundles page displays the bundles available for download. The Bundle Details section displays the bundle version and release date.

If the bundle can be applied right away, the Bundle Details column displays the workload domains to which the bundle needs to be applied to, and the Availability column says Available. If another bundle needs to be applied before a particular bundle, the Availability field displays Future.

3 Click View Details for more information about the bundle.



VMware Cloud Foundation Update 3.8.0.0

Released 07/18/2019 273 MB

Before applying the upgrade bundle, ensure that there are no failed workflows in your system and none of the Cloud Foundation resources are in activating or error state. If any of these conditions are true, contact VMware Support before starting the upgrade.This VMware Cloud Foundation Upgrade contains update and fixes required for SDDC Manager migration upgrade.

Additional Bundle Details

Version	3.6.0-114161
Severity	Critical
Vendor	VMware
Bundle ID	a165fa0a-5210-4db4-9f74-5d2b50f81363
Software Component 1	LCM
Description	LCM update
Update to Version	3.8.0-RELEASE-14136202
Required Version	3.7.2-RELEASE-13773680
Release Date	07/18/2019
Vendor	VMware
Software Component 2	SDDC Manager UI App
Description	SDDC Manager UI update
Update to Version	3.8.0-RELEASE-14135429
Required Version	3.7.2-RELEASE-13773626
Release Date	07/18/2019
Vendor	VMware

The bundle page displays the version, bundle ID, and software components to be updated by this bundle.

4 Click **Exit Details**.

5 Do one of the following:

- Click **Download Now**.

  The bundle download begins right away.

- Click **Schedule Download**.

  Select the date and time for the bundle download and click **Schedule**.

The Download Status section on the Bundles page displays the date and time at which the bundle download has been scheduled. When the download begins, the status bar displays the download progress.

Upgrade NSX for vSphere

On the management domain, the NSX for vSphere upgrade bundle is available to be applied after SDDC Manager is upgraded. On VI workload domains, NSX for vSphere is the first component to be upgraded.

Procedure

1 Click **Precheck** to validate that NSX for vSphere is ready to be updated.

Click **View Status** to see the update status for each component and the tests performed. Expand a test by clicking the arrow next to it to see further details.

If any of the tests fail, fix the issue and click **Retry Precheck**.

The precheck results are displayed below the Precheck button. Ensure that the precheck results are green before proceeding. A failed precheck may cause the update to fail.

2 Click **Upgrade Now** to start the update or click **Schedule** to schedule the update for a specific date and time depending on your maintenance window.

3 Monitor the update. See Monitor Update.

Upgrade vCenter Server and Platform Services Controllers

After NSX for vSphere is upgraded, the vCenter Server and Platform Services Controllers upgrade bundle is available to be applied.

During the upgrade process, you provide a temporary IP address. LCM uses this IP address to deploy a new appliance and then copies over the data from the source appliance to the newly deployed appliance. After the upgrade, the new appliance inherits the IP address and networking configuration of the source appliance.

The source appliances are powered off and left in inventory. These VMs can be deleted. They should not be powered on with their network cards connected as this will cause a conflict with the appliances.

Procedure

1 Click **Precheck** to validate that vCenter Server is ready to be upgraded.

Click **View Status** to see the update status for each component and the tests performed. Expand a test by clicking the arrow next to it to see further details.

If any of the tests fail, fix the issue and click **Retry Precheck**.

The precheck results are displayed below the Precheck button. Ensure that the precheck results are green before proceeding. A failed precheck may cause the update to fail.

2 Click **Schedule** to schedule the update for a specific date and time depending on your maintenance window.

3 On the Introduction page, read the text and click **Next**.

4 On the Configure Target Appliance page, enter an available IP address from the management domain IP range.

This IP address is used only during the upgrade process.

5 Enter the subnet mask and gateway IP address of the management domain.

6 Click **Next**.

7 Select a date and time and click **Next**.

8 Review the information displayed and click **Finish**.

The upgrade is scheduled at the specified date and time.

9 Monitor the update. See Monitor Update.

Upgrade ESXi

After vCenter Server and Platform Services Controllers are upgraded, the ESXi upgrade bundle is available to be applied.

If you installed Cloud Foundation with custom ESXi ISOs from a partner, see Knowledge Base article 65047.

If you want to skip any hosts while applying an ESXi update to the management domain or a VI workload domain, you must add these hosts to the `application-evo.properties` file before you begin the update. See Skip Hosts During ESXi Update.

Prerequisites

Make sure that the servers you are upgrading are vSAN ReadyNodes that are certified for use with ESXi 6.7 EP5.

- See KB 52084 for guidance on what components can be modified in a vSAN ReadyNode.
- For information on certified vSAN ReadyNodes, see the VMware Compatibility Guide.

Procedure

1 Click **Precheck** to validate that ESXi is ready to be updated.

  Click **View Status** to see the update status for each component and the tests performed. Expand a test by clicking the arrow next to it to see further details.

  If any of the tests fail, fix the issue and click **Retry Precheck**. If you see a warning about the vSAN HCL being out of date, see KB 2145116 to fix the issue.

  The precheck results are displayed below the Precheck button. Ensure that the precheck results are green before proceeding. A failed precheck may cause the update to fail.

2 Click **Upgrade Now** to start the update or click **Schedule** to schedule the update for a specific date and time depending on your maintenance window.

3 Monitor the update. See Monitor Update.

Upgrade vRealize Suite Lifecycle Manager

If you deployed vRealize Operations or vRealize Automation in your Cloud Foundation 2.3.2.5 environment, you must upgrade vRealize Suite Lifecycle Manager after upgrading the management domain.

Note The SDDC Manager Dashboard will display the current version of vRealize Suite Lifecycle Manager as 1.0, even though the correct version is 1.2. This will not impact your ability to upgrade to vRealize Suite Lifecycle Manager 2.0.

Procedure

1 Click **Precheck** to validate that vRealize Suite Lifecycle Manager is ready to be updated.

   Click **View Status** to see the update status for each component and the tests performed. Expand a test by clicking the arrow next to it to see further details.

   If any of the tests fail, fix the issue and click **Retry Precheck**.

   The precheck results are displayed below the Precheck button. Ensure that the precheck results are green before proceeding. A failed precheck may cause the update to fail.

2 Click **Upgrade Now** to start the update or click **Schedule** to schedule the update for a specific date and time depending on your maintenance window.

3 Monitor the update. See Monitor Update.

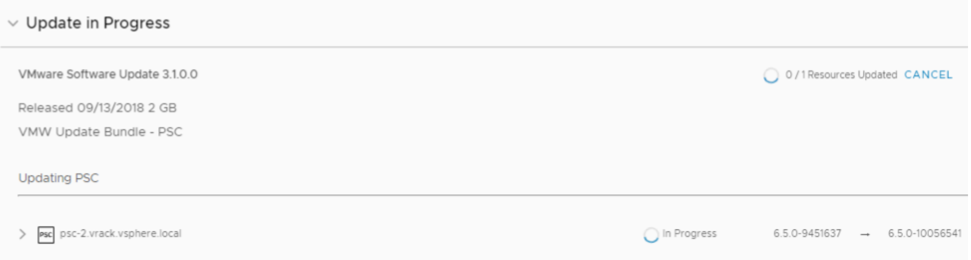
Monitor Update

Monitor the update progress on your workload domain

Procedure

1 The Update in Progress section in the workload domain detail page displays the high level update progress and the number of components to be updated.

2 Details of the component being updated is shown below that.



Update in Progress

VMware Software Update 3.1.0.0

0 / 1 Resources Updated

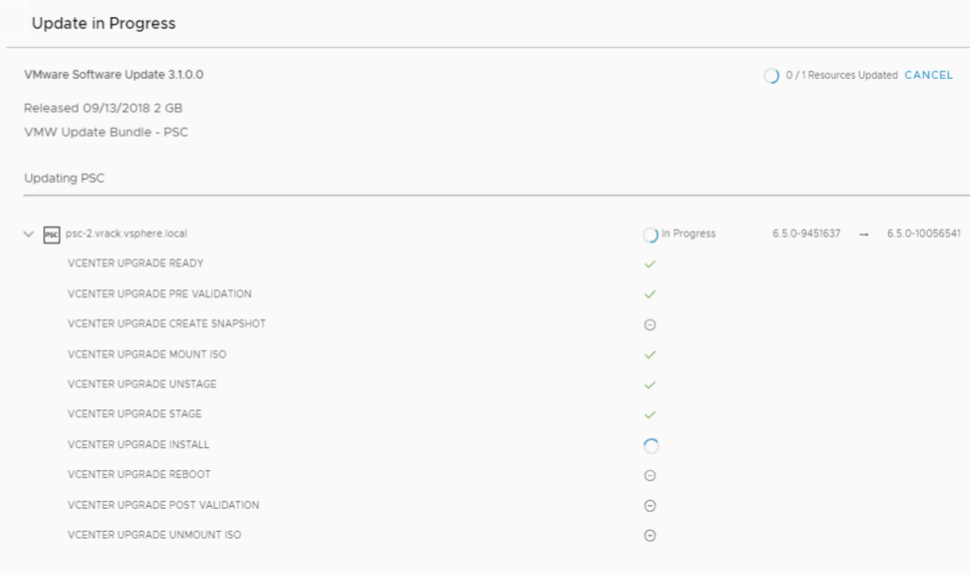
Released 09/13/2018 2 GB

VMW Update Bundle - PSC

Updating PSC

psc-2.vrack.vsphere.local In Progress 6.5.0-9451637 → 6.5.0-10056541

3 Click the arrow to see a list of tasks being performed to update the component. As the task is completed, it shows a green check mark.



Update in Progress

VMware Software Update 3.1.0.0

0 / 1 Resources Updated CANCEL

Released 09/13/2018 2 GB

VMW Update Bundle - PSC

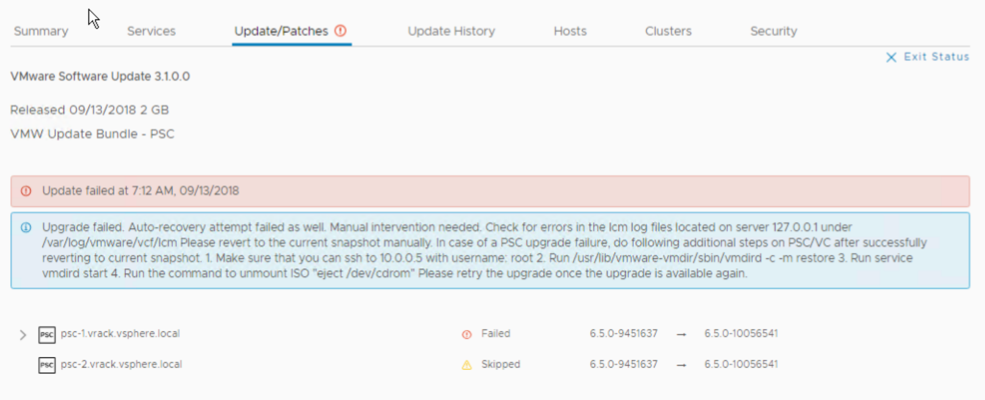
Updating PSC

psc-2.vrack.vsphere.local — In Progress — 6.5.0-9451637 → 6.5.0-10056541

VCENTER UPGRADE READY ✓
VCENTER UPGRADE PRE VALIDATION ✓
VCENTER UPGRADE CREATE SNAPSHOT ⊝
VCENTER UPGRADE MOUNT ISO ✓
VCENTER UPGRADE UNSTAGE ✓
VCENTER UPGRADE STAGE ✓
VCENTER UPGRADE INSTALL
VCENTER UPGRADE REBOOT ⊝
VCENTER UPGRADE POST VALIDATION ⊝
VCENTER UPGRADE UNMOUNT ISO ⊝

4 When all tasks to update a component have been completed, the update status for the component is displayed as Updated.

5 If a component fails to be updated, the status is displayed as Failed. The reason for the failure as well as remediation steps are displayed.



VMware Software Update 3.1.0.0

Released 09/13/2018 2 GB

VMW Update Bundle - PSC

Update failed at 7:12 AM, 09/13/2018

Upgrade failed. Auto-recovery attempt failed as well. Manual intervention needed. Check for errors in the lcm log files located on server 127.0.0.1 under /var/log/vmware/vcf/lcm Please revert to the current snapshot manually. In case of a PSC upgrade failure, do following additional steps on PSC/VC after successfully reverting to current snapshot. 1. Make sure that you can ssh to 10.0.0.5 with username: root 2. Run /usr/lib/vmware-vmdir/sbin/vmdird -c -m restore 3. Run service vmdird start 4. Run the command to unmount ISO "eject /dev/cdrom" Please retry the upgrade once the upgrade is available again.

psc-1.vrack.vsphere.local	Failed	6.5.0-9451637	→	6.5.0-10056541
psc-2.vrack.vsphere.local	Skipped	6.5.0-9451637	→	6.5.0-10056541

6 After you resolve the issues, the bundle becomes available. You can then apply the bundle or schedule it to be applied at a specific date and time.

What to do next

1 Remove the VM snapshots you had taken before starting the update.

2 Take a backup of the newly installed components.

Skip Hosts During ESXi Update

You can skip hosts while applying an ESXi update to the management domain or a VI workload domain. The skipped hosts are not updated.

Procedure

1. Retrieve the host IDs for the hosts you want to skip.

   a. Open a new tab in the browser where you are running SDDC Manager and type the following URL:

      `https://`*SDDC_Manager_IP*`/inventory/esxis`

      Here is a sample output:

      ```
      {
      "vcenterId": "d1a239e1-baef-11e8-a2de-d1b89736a031",
      "networkPoolId": "d3643003-c854-43e7-91ad-fd8d0711a02f",
      "bundleRepoDatastore": "lcm-bundle-repo",
      "domainId": "d0ef8bb0-baef-11e8-a2de-d1b89736a031",
      "clusterId": "d1b106f1-baef-11e8-a2de-d1b89736a031",
      "vsanIpAddress": "10.0.4.3",
      "vmotionIpAddress": "10.0.8.3",
      "hostAttributes": {},
      "dirty": false,
      "id": "d19d57e1-baef-11e8-a2de-d1b89736a031",
      "status": "ACTIVE",
      "version": "6.5.0-9298722",
      "hostName": "esxi-1.vrack.vsphere.local",
      "privateIpAddress": "10.0.0.100",
      "managementIpAddress": "10.0.0.100"
      }
      ```

   b. Copy the appropriate host IDs.

2. Using SSH, log in to the SDDC Manager VM with the user name `vcf` and password you specified in the deployment parameter sheet.

3. Type `su` to switch to the root account.

4. Open the `/opt/vmware/vcf/lcm-app/conf/application-prod.properties` file.

5. At the end of the file , add the following line:

   `esx.upgrade.skip.host.ids=`*host id1*`,`*host id2*

6. Save and close the file.

7. Restart the LCM server by typing the following command in the console window:

   ```
   systemctl restart lcm
   ```

The hosts added to the `application-prod.properties` are not updated when you update the workload domain.

Post-Upgrade Tasks

10

After you upgrade from VMware Cloud Foundation 2.3.2.5 to 3.5.1, there are some additional tasks to complete.

- Make sure the VLANs for all networks (management, vSAN, vMotion, and VXLAN) used in all the VI workload domains, including the management domain, are tagged on all the ToR switches and inter-rack switches.
- Add IP addresses for vSAN and vMotion networks to the network pools created during migration. See Edit a Network Pool.
- If you plan to add or expand workload domains after upgrade, make sure that the VXLAN DHCP scope has enough IP addresses to accommodate this growth.
- Install ESXi software on any free hosts. See Installing ESXi Software on Cloud Foundation Servers.
- Update the vRealize Log Insight version in SDDC Manager. See Update the vRealize Log Insight Version Recorded in SDDC Manager.
- If you upgraded vRealize Operations, see Update the vRealize Operations Manager Version Recorded in SDDC Manager.
- If you upgraded vRealize Automation, see Update the vRealize Automation Version Recorded in SDDC Manager.

This chapter includes the following topics:

Update the vRealize Log Insight Version Recorded in SDDC Manager

After you complete the upgrade from Cloud Foundation 2.3.2.5 to 3.5.1, you must update the version of vRealize Log Insight in the SDDC Manager inventory.

Procedure

1 Download the `60278_vrli_version_updater.zip` file from KB 60278.

2. Use a file transfer utility to copy the zip file to the `/home/vcf` folder on the SDDC Manager VM.
3. Log in to the SDDC Manager VM as the **`vcf`** user.
4. Issue the following command to extract the contents of the `60278_vrli_version_updater.zip` file:

   ```
   unzip 60278_vrli_version_updater.zip
   ```

5. Issue the following command to run the extracted `vrli_version.updater.py` script:

   ```
   python vrli_version_updater.py
   ```

You will see output similar to the following:

```
Verifying VRLI version and updating it in SDDC manager logical inventory, if needed
Checking VRLI version
API response: [{"id":"618a2421-edca-11e8-8b0f-6d7f5b3308a7","domainId":"60b5bd20-
edca-11e8-8b0f-6d7f5b3308a7","loadBalancerHostname":"vrli.vcf.corp.local","nodeSize":"MEDIUM","enhance
dLoggingEnabled":false,"masterNode":{"id":"6189d600-
edca-11e8-8b0f-6d7f5b3308a7","hostName":"vrli-1.vcf.corp.local","managementIpAddress":"192.168.16.17",
"vmName":"vrli-1"},"workerNodes":[{"id":"6189fd10-
edca-11e8-8b0f-6d7f5b3308a7","hostName":"vrli-2.vcf.corp.local","managementIpAddress":"192.168.16.18",
"vmName":"vrli-2"},{"id":"6189fd11-
edca-11e8-8b0f-6d7f5b3308a7","hostName":"vrli-3.vcf.corp.local","managementIpAddress":"192.168.16.19",
"vmName":"vrli-3"}],"version":"DefaultVersion","status":"ACTIVE"}]
API response: [{"id":"a037ffeb-3749-4d40-a23b-79daf2a23e36","entityId":"618a2421-
edca-11e8-8b0f-6d7f5b3308a7","entityType":"VRLI","credentialType":"API","username":"admin","secret":"V
Mware123!"}]
Successful authentication to vRLI node with IP address vrli.vcf.corp.local
API response: {"releaseName":"GA","version":"4.6.1-8597028"}
Found the following version for vRLI: 4.6.1-8597028
Found version 4.6.1-8597028
Updating vRLI version in logical inventory
```

Enable Pre-Upgrade Verification in vRealize Log Insight

You must enable pre-upgrade verification after you update the vRealize Log Insight version recorded in SDDC Manager.

Procedure

1. Log in to the vRealize Log Insight user interface on the Log Insight master node as the admin user.
2. Open a second tab in the same browser and connect to `https://<Log Insight master node>/internal/config`.
3. Remove the following line inside the `<upgrade></upgrade>` stanza:

   `<upgrade-prevalidation-enabled value="false" /> #`

4. Click the **SAVE** button.

Update the vRealize Operations Manager Version Recorded in SDDC Manager

If you upgraded vRealize Operations before you upgraded from Cloud Foundation 2.3.2.5 to 3.5.1, you must update the version of vRealize Operations Manager in the SDDC Manager inventory.

Procedure

1 Download the `65079_vrops_version_updater.zip` file from KB 65079.

2 Use a file transfer utility to copy the zip file to the `/tmp` folder on the SDDC Manager VM.

3 SSH to the SDDC Manager VM as the **`vcf`** user and use the **`su –`** command to switch to the root user.

4 Issue the following command to extract the contents of the `65079_vrops_version_updater.zip` file:

```
unzip -d /tmp/ /tmp/65079_vrops_version_updater.zip
```

5 Issue the following command to execute the `/tmp/vrops_version_updater.py` script:

```
python /tmp/vrops_version_updater.py
```

Update the vRealize Automation Version Recorded in SDDC Manager

If you upgraded vRealize Automation before you upgraded from Cloud Foundation 2.3.2.5 to 3.5.1, you must update the version of vRealize Automation in the SDDC Manager inventory.

Procedure

1 Download the `65101_vra_version_updater.zip` file from KB 65101.

2 Use a file transfer utility to copy the zip file to the `/tmp` folder on the SDDC Manager VM.

3 SSH to the SDDC Manager VM as the **`vcf`** user and use the **`su –`** command to switch to the root user.

4 Issue the following command to extract the contents of the `65101_vra_version_updater.zip` file:

```
unzip -d /tmp/ /tmp/65101_vra_version_updater.zip
```

5 Issue the following command to execute the `/tmp/vra_version_updater.py` script:

```
python /tmp/vra_version_updater.py
```

Clean Up vRack-LAG Uplink Port Groups

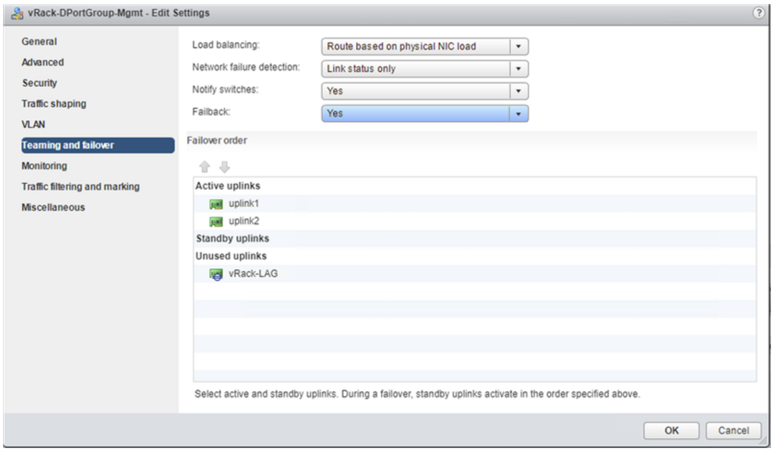
The network migration stage of upgrade converts uplink ports on vSphere Distributed Switches from a link aggregation group (LAG) port group to standard uplink port groups. After upgrade, you can clean up unused LAG portgroups.

Procedure

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

2 From the **Home** menu of the vSphere Web Client, select **Networking**.

3 Find and remove any unused vRack-LAG uplinks from the vSphere Distributed Switches for the management domain and VI workload domains.



Load balancing: Route based on physical NIC load

Network failure detection: Link status only

Notify switches: Yes

Failback: Yes

Failover order

Active uplinks
uplink1
uplink2
Standby uplinks
Unused uplinks
vRack-LAG

Select active and standby uplinks. During a failover, standby uplinks activate in the order specified above.

11 Known Issues

This section describes known issues that you may experience during or after the upgrade

Network Migration Fails Due to NTP Update Error

NTP updates can sometimes exceed the timeout and network migration fails as a result.

Workaround: If rollback succeeded, retry network migration. If rollback failed, contact VMware Support.

Network Migration Logs Show Red Text

When you tail the network migration log on the SDDC Manager Controller VM in an SSH session using Putty, the text may turn red. This does not necessarily indicate an error or warning. If the text does not specify an error or warning, you can ignore the red text.

Workaround: None.

Data Migration Fails with NAS DS Exception

The SDDC Manager App migration fails with the following exception in the `sddcmanager_migration_app_upgrade.log` file:

```
Exception trying to create NAS DS on host 172.18.143.31

com.vmware.vim.binding.vim.fault.PlatformConfigFault: An error occurred during host configuration.
        at sun.reflect.NativeConstructorAccessorImpl.newInstance0(Native Method) ~[na:1.8.0_201]
```

The creation of NAS DS fails if the previous NFS datastore `lcm-bundle-repo` that is pointed to the SDDC Manager Utility VM is not cleaned properly. The name of the datastore is the same as the one being created on the new SDDC Manager VM.

To confirm that the esxi host still has references to the old NFS config, SSH to the esxi host and run the following command:

`cat /etc/vmware/esx.conf | grep lcm-bundle-repo`

The output is similar to the following:

```
/nas/lcm-bundle-repo/host = ”192.168.100.46’
/nas/lcm-bundle-repo/readOnly = “true”
/nas/lcm-bundle-repo/enabled = “true”
```

Workaround: To fix the issue login to the ESXi host using SSH and run the following command.

```
esxcli storage nfs remove --volume-name=lcm-bundle-repo
```

Data Migration Fails with Invalid Login Error

Data migration fails with the following error:

```
Caused by: com.vmware.vim.binding.vim.fault.InvalidLogin: Cannot complete login due to an incorrect
user name or password.
```

The cause may be that the Platform Services Controllers (PSCs) are powered off and cannot be powered on using the vSphere or ESXi Client.

Workaround: Connect to vCenter Server using the vSphere Client and unregister the powered-off PSCs. After they are successfully unregistered, register the PSCs, power them on, and retry data migration.

Configuration Drift Fails with NTP Configuration Error on vRealize Operations

For a successful upgrade, all NTP servers must be reachable by all components in the Cloud Foundation system on both the management network and the vRealize network. If you have an NTP server that is not reachable by all networks, then the configuration drift update will fail with a message similar to the following:

```
com.vmware.evo.sddc.orchestrator.exceptions.OrchTaskException: Failed to configure NTP servers to
vROps cluster
```

Workaround: Temporarily remove the unreachable NTP server, reapply the configuration drift bundle, then add the NTP server back.

SSH to the SDDC Manager VM and run the following commands:

```
cqlsh --cqlversion=3.4.4
use inventory;
expand on;
select * from systeminfo;
```

You should see output similar to:

```
@ Row 1
------------------
+-------------------------------------------------------------------------------------------------
 id | 0dbe12c1-7d9d-4aa8-873f-105cde7d709c
 creationtime | 1550818463052
 dnsinfo |
{"rootDomain":"rootZone","subDomain":"childZone","primaryDns":"172.17.0.249","secondaryDns":""}
 features | null
 modificationtime | 1550818463052
 ntpinfo | {"ntps":["172.17.0.251","172.25.0.251"]}
```

This shows two NTP servers `172.17.0.251` and `172.25.0.251`. For this example, assume that `172.17.0.251` is not reachable by all networks.

Update `systeminfo` to remove the unreachable NTP server:

```
update systeminfo set ntpinfo = '{"ntps":["172.25.0.251"]}' where id =
'0dbe12c1-7d9d-4aa8-873f-105cde7d709c';
```

Use the `id` that matches your environment.

Exit `cqlsh` and run the following command to check the update:

```
curl http://localhost/inventory/system-info | json_pp
```

The system displays output similar to:

```
  % Total % Received % Xferd Average Speed Time Time Time Current
                                 Dload Upload Total Spent Left Speed
100 143 0 143 0 0 15888 0 --:--:-- --:--:-- --:--:-- 15888
{
   "dnsInfo" : {
      "primaryDns" : "172.17.0.249",
      "rootDomain" : "rootZone",
      "secondaryDns" : "",
      "subDomain" : "childZone"
   },
   "ntpInfo" : {
      "ntps" : [
         "172.25.0.251"
      ]
   }
}
```

In this example, you can see that `172.25.0.251` is the only NTP server.

Now you can reapply the configuration drift bundle. When it completes successfully, update `systeminfo` to re-add the NTP server you removed previously.

```
update systeminfo set ntpinfo = '{"ntps":["172.17.0.251","172.25.0.251"]}' where id =
'0dbe12c1-7d9d-4aa8-873f-105cde7d709c';
```

Some Configuration Drift Stages are not Updated

After you apply the configuration drift bundle, some of the stages do not show an `Updated` status. The specific stages are:

- VCF SERVICE UPGRADE INITIATION
- VCF SERVICE UPGRADE
- VCF SERVICE UPGRADE POST VALIDATION

These stages are not required and you can proceed the software BOM upgrade.

Cluster Alerts After Upgrade to 3.5.1

If your Cloud Foundation environment contained multiple workload domains, SDDC Manager displays an alert for the cluster VLAN IDs after Cloud Foundation is upgraded to 3.5.1. You can ignore these alerts.

SDDC Manager VM Contains Stale or Unrelated Entries After Upgrade to 3.5.1

The known hosts file in the SDDC Manager VM may contain stale or unrelated entries in addition to the hosts or other VMs. You can ignore these entries.

Cannot Register VMs After Upgrade to 3.5.1

During migration the ESXi hosts establish locks on critical VMs and file systems. In some cases these locks may not be released, causing issues in the upgraded system.

Workaround:

- Identify the VMs that have a lock from ESXi hosts
- Identify the ESXi host that owns the lock.
- Register the VM from that ESXi host.

To identify the locked VMs and the hosts that owns the lock, SSH into the ESXi host and run a command similar to the following:

```
vmfsfilelockinfo -p /vmfs/volumes/vsan\:cc5d69e3fc024ade-89e3e71d0235e648/sddc-manager/sddc-
manager_2.vmdk -v vcenter-1.vrack.vsphere.local -u administrator@vsphere.local
```

In this example, **`/vmfs/volumes/vsan\:cc5d69e3fc024ade-89e3e71d0235e648/sddc-manager/sddc-manager_2.vmdk`** is the datastore path for the **`sddc-manager_2`** VMDK. Run the command multiple times to check multiple VMDKs for locks.

`vcenter-1.vrack.vsphere.local` is the FQDN for the vCenter Server and **`administrator@vsphere.local`** is the user name for vCenter Single Sign-on.

If there is no lock you will see output similar to:

```
vmfsfilelockinfo Version 2.0
Looking for lock owners on "sddc-manager_2.vmdk"
"sddc-manager_2.vmdk" is not locked by any ESX host and is Free
Total time taken : 0.17358810198493302 seconds.
```

If there is a lock, the output identifies the ESXi host that owns the lock. Log in to the host using the ESXi Client and register the VM.