Operational Verification

27 MAR 2018
VMware Validated Design 4.2
VMware Validated Design for Software-Defined Data Center 4.2

vmware®

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

https://docs.vmware.com/

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

docfeedback@vmware.com

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

Contents

About VMware Validated Design Operational Verification 5

1 Operational Verification of the Virtual Infrastructure Layer 6
- Authenticate to vCenter Server Using Local System Account 7
- Authenticate to vCenter Server Using Active Directory Service Account 8
- Place an ESXi Host into Maintenance Mode 9
- Ping NSX VTEP Interfaces with Jumbo Frames 10
- Verify NSX Controllers Are Connected to ESXi Hosts 11
- Verify VMs in VXLAN Communicate with Each Other While Residing on Different Hosts 12
- Verify VMs in VXLAN Communicate with VMs in VLAN 13
- Test Host to Host Communication Using VXLAN Logical Switch 15

2 Operational Verification of the Operations Management Layer 17
- Verification of vRealize Operations Manager 17
  - Authenticate to vRealize Operations Manager Using Local System Account and Verify Cluster Status 17
  - Verify Collection Status of vCenter Adapter 18
  - Verify Collection Status of vSAN Adapter 19
  - Verify Collection Status of vRealize Log Insight Adapter 20
  - Verify Collection Status of vRealize Business for Cloud Adapter 21
  - Verify Collection Status of vRealize Automation Adapter 22
  - Verify Collection Status of SRM Adapter 23
  - Verify Collection Status of Storage Devices Adapter 24
  - Verify Collection Status of NSX for vSphere Adapter 25
- Verification of vRealize Log Insight 26
  - Authenticate to vRealize Log Insight Using Local System Account and Verify Cluster Status 27
  - Verify Agent Status for vRealize Operations Manager Virtual Appliances 28
  - Verify Agent Status for vRealize Automation Virtual Appliances 29
  - Verify Agent Status for Embedded vRealize Orchestrator 29
  - Verify Agent Status for vRealize Automation Windows Systems 30
  - Verify Agent Status for Microsoft SQL Server 31
  - Verify Agent Status for Site Recovery Manager Server 32
- Verification of vSphere Update Manager Download Service 33
  - Run the vSphere Update Manager Download Service Cron Job 33

3 Operational Verification of the Cloud Management Layer 35
- Authenticate to vRealize Automation Using Local System Account 36
- Authenticate to vRealize Automation Using Active Directory Admin Account 36

Verify vRealize Automation Components Are Highly Available 37
Verify Integration of vRealize Automation with vSphere Infrastructure 39
Verify Integration of vRealize Automation with vRealize Orchestrator and NSX for vSphere 40
Verify Integration of vRealize Automation with vRealize Business for Cloud 41
Verify Integration of vRealize Automation with vRealize Operations Manager 42

4 Operational Verification of the Business Continuity Layer 44
Verify Pairing of Site Recovery Manager Across Regions 44
Verify Pairing of vSphere Replication Across Regions 45
Perform Test Recovery of Operations Management Recovery Plan 46
Perform Test Recovery of Cloud Management Recovery Plan 48
Verify Status and Configuration of vSphere Storage APIs for Data Protection Based Backup Solution 49

5 Post Upgrade Verification 51
Version Verification of the Virtual Infrastructure Layer 51
Verify the Version of Platform Service Controller 52
Verify the Version of vCenter Server 53
Verify the Version of ESXi Host 53
Verify the Version of NSX for vSphere 54
Version Verification of the Operations Management Layer 55
Verify the Version of vRealize Operations Manager 55
Verify the Version of vRealize Log Insight 55
Verify the Version of vSphere Update Manager Download Service 56
Version Verification of the Cloud Management Layer 57
Verify the Version of vRealize Automation Appliance Nodes 57
Verify the Version of vRealize Automation Windows Nodes 58
Verify the Version of vRealize Business Nodes 59
Version Verification of the Business Continuity Layer 60
Verify the Version of Site Recovery Manager 60
Verify the Version of vSphere Replication 61

6 SDDC Startup and Shutdown 62
Shutdown Order of the Management Virtual Machines 62
Startup Order of the Management Virtual Machines 64

About VMware Validated Design Operational Verification

The VMware Validated Design Operational Verification document provides step-by-step instructions for verifying that the management components in the Software-Defined Data Center (SDDC) that are deployed according to the VMware Validated Design™ for Software-Defined Data Center are operating as expected.

Operational verification is defined as verifying that a component or system is operational and operating within expected parameters, scenarios where operational verification should be performed include:

- Initial deployment of a component or system
- Upgrading or patching of a component or system
- Recovering a component or system from a failure scenario
- Generic maintenance of a component or system

Intended Audience

The *VMware Validated Design Operational Verification* document is intended for cloud architects, infrastructure administrators, cloud administrators, and cloud operators who are familiar with and want to use VMware software to manage an SDDC that meets the requirements for capacity, scalability, backup and restore, and extensibility for disaster recovery support.

Required Software

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

Operational Verification of the Virtual Infrastructure Layer

1

Perform operational verification steps to verify the operational state of the virtual infrastructure layer following initial installation or any type of outage affecting an individual component or system.

Operational verification of the virtual infrastructure layer involves the following management components:

- ESXi hosts
- vCenter Servers
- Platform Services Controllers
- NSX Managers
- Edge Services Gateways
- Authenticate to vCenter Server Using Local System Account

  Verify that you can authenticate to vCenter Server using the administrator@vsphere.local system account.
- Authenticate to vCenter Server Using Active Directory Service Account

  Verify that you can authenticate to vCenter Server using a service account configured in Active Directory.
- Place an ESXi Host into Maintenance Mode

  Verify that when placing an ESXi host into maintenance mode all virtual machines running on the host are evacuated and the host enters maintenance mode without further user interaction.
- Ping NSX VTEP Interfaces with Jumbo Frames

  Verify that ESXi hosts can ping each other VTEP interfaces using the `vmkping` command.
- Verify NSX Controllers Are Connected to ESXi Hosts

  Verify that the NSX controllers are communicating with ESXi hosts by running the `esxcli network ip connection list` command.
- Verify VMs in VXLAN Communicate with Each Other While Residing on Different Hosts

  Verify that virtual machine communication is operational and that virtual machines residing on different ESXi hosts can communicate with each, using the `ping` command.
- Verify VMs in VXLAN Communicate with VMs in VLAN

  Verify virtual machine to virtual machine communication using the `ping` command.

- Test Host to Host Communication Using VXLAN Logical Switch

  Test host-to-host communication with a ping monitor. A ping test checks if two hosts in a network can reach each other using VXLAN standard.

Authenticate to vCenter Server Using Local System Account

Verify that you can authenticate to vCenter Server using the administrator@vsphere.local system account.

Authenticating with a local system account verifies that the vCenter Server and external Platform Services Controllers are configured correctly and that there are no communication issues between systems.

Expected Outcome
You can successfully authenticate using the administrator@vsphere.local system account and have visibility of all vCenter Servers and their inventories with administrative access.

Procedure

1. Log in to vCenter Server by using the vSphere Web Client.
   a. Open a Web browser and go to **`https://sfo01m01vc01.sfo01.rainpole.local/vsphere-client`**.
   b. Log in using the following credentials.

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

2. From the **Home** menu, select **Hosts and Clusters**.
3. In the **Navigator** pane, verify that all four vCenter Server instances are present in the list.

   This operation validates that the Enhanced Linked Mode is intact and active for all vCenter Server instances.

What to do next

If you encounter issues while performing this procedure, use the following troubleshooting tips:

Troubleshooting Tips
■ Ensure that NTP is configured correctly on all vCenter Server and Platform Services Controller virtual appliances. ■ Ensure that all vCenter Server and Platform Services Controller virtual appliances are configured with the correct DNS settings. ■ Ensure that DNS is configured with forward and reverse lookup records for all vCenter Server and Platform Services Controller virtual appliances and the VIP of the Platform Services Controller load balancer. ■ Ensure that there is network connectivity between all vCenter Server and Platform Services Controller virtual appliances. ■ Ensure that all the services on the vCenter Server and Platform Services Controller virtual appliances are running.

Authenticate to vCenter Server Using Active Directory Service Account

Verify that you can authenticate to vCenter Server using a service account configured in Active Directory.

Authenticating with a service account configured in Active Directory verifies that the Platform Services Controllers are configured with the Active Directory Domain as an identity source and that permissions within vCenter Server are correctly assigned.

Expected Outcome
You can successfully authenticate using a service account and have visibility of all vCenter Servers and their inventories with the appropriate user access.

Procedure

1 Log into vCenter Server by using the vSphere Web Client.

   a Open a Web browser and go to **`https://sfo01m01vc01.sfo01.rainpole.local/vsphere-client`**.

   b Log in using the following credentials.

Setting	Value
User name	svc-nsxmanager@rainpole.local
Password	*svc-nsxmanager_password*

2 From the **Home** menu, select **Hosts and Clusters**.

3 In the **Navigator** pane, verify that all four vCenter Server instances are present in the list.

   This operation validates that the Enhanced Linked Mode is intact and active for all vCenter Server instances.

What to do next

If you encounter issues while performing this procedure, use the following troubleshooting tips:

Troubleshooting Tips
■ Ensure that NTP is configured correctly on all vCenter Server and Platform Services Controller virtual appliances. ■ Ensure that all vCenter Server and Platform Services Controller virtual appliances are configured with the correct DNS settings. ■ Ensure that DNS is configured with forward and reverse lookup records for all vCenter Server and Platform Services Controller virtual appliances and the VIP of the Platform Services Controller load balancer. ■ Ensure that there is network connectivity between all vCenter Server and Platform Services Controller virtual appliances. ■ Ensure that all the services on the vCenter Server and Platform Services Controller virtual appliances are running. ■ Ensure that all Platform Services Controllers have successfully joined the active directory domain.

Place an ESXi Host into Maintenance Mode

Verify that when placing an ESXi host into maintenance mode all virtual machines running on the host are evacuated and the host enters maintenance mode without further user interaction.

Placing each ESXi host into maintenance mode ensures that network connectivity between ESXi hosts is operational and that vMotion is configured correctly.

Expected Outcome
All virtual machines running on the ESXi host are migrated with vMotion to another ESXi host in the cluster. When vMotion completes, the ESXi host enters maintenance mode.

Procedure

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

   a Open a Web browser and go to `https://sfo01m01vc01.sfo01.rainpole.local/vsphere-client`.

   b Log in using the following credentials.

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

2 Navigate to the ESXi host.

   a From the **Home** menu, select **Hosts and Clusters**.

   b In the **Navigator** pane, expand the **sfo01m01vc01.sfo01.rainpole.local** > **sfo01-m01dc** > **sfo01-m01-mgmt01** inventory tree.

   c Click the **sfo01m01esx01.sfo01.rainpole.local** host.

3 Put the ESXi host into maintenance mode.

   a Right-click the ESXi host and click **Maintenance Mode** > **Enter Maintenance Mode**.

   b In the **Confirm Maintenance Mode**, leave the default option **Ensure data accessibility from other hosts** for **vSAN data migration**, and click **OK**.

   Virtual machines are migrated to different hosts when the host enters maintenance mode.

   The host remains in maintenance mode until you select **Exit Maintenance Mode**.

4 Right-click the ESXi host and click **Maintenance Mode** > **Exit Maintenance Mode** to exit from maintenance mode

5 Repeat the procedure for other ESXi hosts from different vCenter Servers.

What to do next

If you encounter issues while performing this procedure, use the following troubleshooting tips:

Troubleshooting Tips

- Ensure that the ESXi host has a vmkernel port configured for vMotion and a static IP address is assigned.
- Ensure that there is network connectivity between ESXi hosts by running the `vmkping` command.

Ping NSX VTEP Interfaces with Jumbo Frames

Verify that ESXi hosts can ping each other VTEP interfaces using the `vmkping` command.

Ensures hosts VTEPs can communicate with each other using jumbo frames and that vxlan is functioning.

Expected Outcome
The `vmkping` command between the two VTEP interfaces is successful.

Procedure

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

   a Open a Web browser and go to **`https://sfo01m01vc01.sfo01.rainpole.local/vsphere-client`**.

   b Log in using the following credentials.

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

2 From the **Home** menu, select **Networking & Security**.

3 Click **Installation and Upgrade**, and click the **Logical Network Preparation** tab.

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

5 Click the **VXLAN Transport** tab and expand the **sfo01-m01-mgmt01** cluster.

6 Under **VMKNic IP Addressing**, note the **vmk4** IP address of **sfo01m01esx01.sfo01.rainpole.local** and **sfo01m01esx04.sfo01.rainpole.local**.

7 Verify that the hosts can ping each other VTEPs.

   a Open an SSH connection to the **`sfo01m01esx01.sfo01.rainpole.local`** host.

   b Log in using the following credentials.

Setting	Value
User name	root
Password	*esxi_root_user_password*

c Run the following command.

Region of the ESXi Host	Command
Region A	`vmkping –I vmk4 –S vxlan –s 8800 –d 172.16.14.210`

Note In the syntax `vmkping –I VTEP–VMK –S vxlan –s 8800 –d Remote–VTEP–IP`, the **`172.16.14.210`** address is the remote VTEP IP address of sfo01m01esx04.sfo01.rainpole.local.

d Repeat the procedure on the sfo01m01esx04.sfo01.rainpole.local host with destination IP as the VTEP address of sfo01m01esx01.sfo01.rainpole.local.

e Repeat the procedure for other ESXi hosts from different vCenter servers.

What to do next

If you encounter issues while performing this procedure, use the following troubleshooting tips:

Troubleshooting Tips
■ Ensure that VTEPs have a valid IP address. ■ Ensure that jumbo frame setting is enabled on switch ports and SVIs.

Verify NSX Controllers Are Connected to ESXi Hosts

Verify that the NSX controllers are communicating with ESXi hosts by running the `esxcli network ip connection list` command.

Ensures that NSX controllers can reach and communicate with ESXi hosts.

Expected Outcome
The NSX Controllers are connected to the ESXi hosts when the command outputs `Established` for the NSX Controller IP addresses connected to the netcpa-worker process.

Procedure

1 Log in to the ESXi host by using Secure Shell (SSH) client.

a Open an SSH connection to the **`sfo01m01esx01.sfo01.rainpole.local`** host.

b Log in using the following credentials.

Setting	Value
User name	root
Password	*esxi_root_user_password*

2 Run the following command.

Region of the ESXi Host	Command
Region A	`esxcli network ip connection list | grep 1234`

3 Verify that NSX controllers IP addresses are connected to the `netcpa-worker` process with a state of `Established`.

4 Repeat the procedure for the remaining ESXi hosts.

What to do next

If you encounter issues while performing this procedure, use the following troubleshooting tips:

Troubleshooting Tips
■ Ensure that the NSX controllers are deployed. ■ Ensure that the `Status` of NSX controllers is showing as `Connected`. ■ Ensure that the NSX controllers can ping the ESXi hosts management network IP. ■ Restart the netcpa agent on the ESXi host.

Verify VMs in VXLAN Communicate with Each Other While Residing on Different Hosts

Verify that virtual machine communication is operational and that virtual machines residing on different ESXi hosts can communicate with each, using the `ping` command.

Ensures that the virtual network interfaces are up on the hosts and can carry traffic, and that the physical network has correctly configured IGMP for hybrid replication mode.

Expected Outcome
Virtual machines in VXLAN can communicate with each other while residing on separate hosts.

Procedure

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

a Open a Web browser and go to **`https://sfo01m01vc01.sfo01.rainpole.local/vsphere-client`**.

b Log in using the following credentials.

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

2 On the vRealize Log Insight appliances, run the `ping` command to verify the communication to other VMs in the VXLAN network.

a From the **Home** menu, select **Hosts and Clusters**.

b Expand the entire **sfo01m01vc01.sfo01.rainpole.local** tree.

c Right-click the **sfo01vrli01a** virtual appliance and select **Open Console**.

d Press ALT+F1 to switch to the command prompt.

e Log in using the following credentials.

Setting	Value
User name	root
Password	*vrli_root_password*

f Run the following command.

Command	Remarks
`ping sfo01vrli01b.sfo01.rainpole.local`	ping from **sfo01vrli01a** to **sfo01vrli01b**
`ping vrops01svr01b.rainpole.local`	ping from **sfo01vrli01a** to **vrops01svr01b**

Note The test assumes that appliances are running on separate hosts.

What to do next

If you encounter issues while performing this procedure, use the following troubleshooting tips:

Troubleshooting Tips
■ Move the VMs to the same host, and if ping is successful, move back to separate hosts. ■ Change transport zone and virtual wires to unicast, and if ping is successful, IGMP is not correctly configured on the physical network.

Verify VMs in VXLAN Communicate with VMs in VLAN

Verify virtual machine to virtual machine communication using the `ping` command.

Ensures that routing is configured correctly both in NSX and the physical network.

Expected Outcome
Virtual machines in VXLAN can communicate with virtual machines in VLAN and the reverse.

Procedure

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

a Open a Web browser and go to **`https://sfo01m01vc01.sfo01.rainpole.local/vsphere-client`**.

b Log in using the following credentials.

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

2 On the vRealize Log Insight appliances, run the `ping` command to verify the communication to other VMs in the VLAN network.

a From the **Home** menu, select **Hosts and Clusters**.

b Expand the entire **sfo01m01vc01.sfo01.rainpole.local** tree.

c Right-click the **sfo01vrli01a** virtual appliance and select **Open Console**.

d Press ALT+F1 to switch to the command prompt.

e Log in using the following credentials.

Setting	Value
User name	root
Password	*vrli_root_password*

f Run the following commands.

Command	Remarks
`ping rainpole.local`	ping from **sfo01vrli01a** to **rainpole.local** (Active Directory)
`ping sfo01m01psc01.sfo01.rainpole.local`	ping from **sfo01vrli01a** to **sfo01m01psc01**
`ping sfo01m01vc01.sfo01.rainpole.local`	ping from **sfo01vrli01a** to **sfo01m01vc01**

3 On the platform controller appliances, run the `ping` command to verify the communication to other VMs in the VXLAN network.

a From the **Home** menu, select **Hosts and Clusters**.

b Expand the entire **sfo01m01vc01.sfo01.rainpole.local** tree.

c Right-click the **sfo01m01psc01** virtual appliance and select **Open Console**.

d Log in using the following credentials.

Setting	Value
User name	root
Password	*psc_root_password*

e Run the following commands.

Command	Remarks
`ping sfo01vrli01a.sfo01.rainpole.local`	ping from **sfo01m01psc01** to **sfo01vrli01a**
`ping vrops01svr01a.rainpole.local`	ping from **sfo01m01psc01** to **vrops01svr01a**
`ping vra01svr01a.rainpole.local`	ping from **sfo01m01psc01** to **vra01svr01a**

What to do next

If you encounter issues while performing this procedure, use the following troubleshooting tips:

Troubleshooting Tips

- Open an SSH connection to the Distributed Logical Router, run the `show ip route` command, and verify that routes are being exchanged.
- Open an SSH connection to the ECMP edges, run the `show ip bgp neighbors` and `show ip route` commands, and verify that BGP is `Established` between UDLR and ToRs, and that routes are being exchanged.
- Open an SSH connection to the ToR, verify that BGP is `Established` to ECMP edges, and that routes are being exchanged.

Test Host to Host Communication Using VXLAN Logical Switch

Test host-to-host communication with a ping monitor. A ping test checks if two hosts in a network can reach each other using VXLAN standard.

Ensures that hosts VTEPs can communicate with each other using jumbo frames and that VXLAN is functioning.

Expected Outcome
The `ping` command between the two hosts is successful using VXLAN standard.

Procedure

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

   a Open a Web browser and go to **`https://sfo01m01vc01.sfo01.rainpole.local/vsphere-client`**.

   b Log in using the following credentials.

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

2 Create a logical switch to test the logical network in Region A.

   a From the **Home** menu, select **Networking & Security**.

   b Click **Logical Switches** and select **172.16.11.65** from the **NSX Manager** drop-down menu.

   c Click the **New Logical Switch** icon.

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

Setting	Value
Name	mgmt01-logical-switch
Transport Zone	Mgmt Universal Transport Zone
Replication mode	Hybrid
Enable IP Discovery	Selected
Enable MAC Learning	Deselected

3 Use a ping monitor to test the connectivity.

a On the **Logical Switches** page, double-click **mgmt01-logical-switch**.

b On the **mgmt01-logical-switch** page, under the **Monitor** tab click **Ping**.

c Under **Test Parameters**, enter the parameters for the ping and click **Start Test**.

Ping Test Parameter	Value
Source host	sfo01m01esx04.sfo01.rainpole.local
Destination host	sfo01m01esx01.sfo01.rainpole.local
Size of test packet	VXLAN standard

VXLAN standard packet size is 1550 bytes without fragmentation. With this test, NSX checks connectivity and verifies that the infrastructure is prepared for VXLAN traffic.

When the ping test completes, verify that the **Results** pane displays no error messages.

4 Test the connectivity in Region B.

a From the **Home** menu, select **Networking & Security**.

b Click **Logical Switches** and select **172.17.11.65** from the **NSX Manager** drop-down menu.

c Double-click **mgmt01-logical-switch**, under the **Monitor** tab click **Ping**.

d Under **Test Parameters**, enter the parameters for the ping and click **Start Test**.

Ping Test Parameter	Value
Source host	lax01m01esx04.lax01.rainpole.local
Destination host	lax01m01esx01.lax01.rainpole.local
Size of test packet	VXLAN standard

When the ping test completes, verify that the **Results** pane displays no error messages.

5 After the VXLAN connectivity tests complete, remove the mgmt01-logical-switch logical switch.

a From the **Home** menu, select **Networking & Security**.

b Click **Logical Switches** and select **172.16.11.65** from the **NSX Manager** drop-down menu.

c Select **mgmt01-logical-switch** and click the **Remove** icon.

What to do next

If you encounter issues while performing this procedure, use the following troubleshooting tips:

Troubleshooting Tips
■ Ensure that VTEPs have a valid IP address. ■ Ensure that jumbo frame setting is enabled on switch ports and SVIs.

Operational Verification of the Operations Management Layer 2

Perform operational verification steps to verify the operational state of the operations management layer following initial installation or any type of outage affecting an individual component or system.

Operational verification of the operations management layer involves the following management components:

- vRealize Operations Manager
- vRealize Log Insight
- vSphere Update Manager
- Verification of vRealize Operations Manager

  Verify the authentication and cluster status and verify that vRealize Operations Manager is collecting data metrics trough the adapters of the management packs for vRealize Operations Manager.
- Verification of vRealize Log Insight

  Verify the authentication and cluster status and verify that all vRealize Log Insight agents are listed and have Active status.
- Verification of vSphere Update Manager Download Service

  Verify that vSphere Update Manager Download Service can connect to the VMware Internet service and successfully checks for updates.

Verification of vRealize Operations Manager

Verify the authentication and cluster status and verify that vRealize Operations Manager is collecting data metrics trough the adapters of the management packs for vRealize Operations Manager.

Authenticate to vRealize Operations Manager Using Local System Account and Verify Cluster Status

Verify that you can authenticate to vRealize Operations Manager using the built-in admin account and verify the cluster status.

Performing authentication using the built-in admin account verifies that vRealize Operations Manager is online and accessible.

Expected Outcome
You can successfully authenticate to the vRealize Operations Manager using the built-in admin account and verify the status of the cluster.

Procedure

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

   a Open a Web browser and go to **`https://vrops01svr01.rainpole.local`**.

   b Log in using the following credentials.

Setting	Value
User name	admin
Password	*vrops_admin_password*

2 Verify that the vRealize Operations Manager cluster is online, and all data nodes are running.

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

   b In the left pane of vRealize Operations Manager, select **Management > Cluster Management**.

   c Verify the cluster status and high availability mode.

Setting	Value
Cluster Status	Online
High Availability	Enabled

What to do next

If you encounter issues while performing this procedure, use the following troubleshooting tips:

Troubleshooting Tips
■ Ensure that each of the vRealize Operations Manager appliance is powered on. ■ Ensure that there is network connectivity to the vRealize Operations Manager appliances and that the host names are resolvable in DNS. ■ Ensure that there is network connectivity between the vRealize Operations Manager nodes. ■ Ensure that you have supplied the correct login credentials.

Verify Collection Status of vCenter Adapter

Verify that vRealize Operations Manager is collecting data metrics through the vCenter Adapter of the VMware vSphere Management Pack for vRealize Operations Manager.

Validating the status of data collection between vRealize Operations Manager and vCenter Server ensures that the vCenter adapter is correctly configured, the provided service account has correct privileges and that dashboards are populated.

Expected Outcome
The vCenter Adapter has a **Collection State** of `Collecting` and a **Collection Status** of `Data receiving`.

Procedure

1. Log in to vRealize Operations Manager by using the operations interface.
   a. Open a Web browser and go to **`https://vrops01svr01.rainpole.local`**.
   b. Log in using the following credentials.

Setting	Value
User name	admin
Password	*vrops_admin_password*

2. On the main navigation bar, click **Administration**.
3. In the left pane of vRealize Operations Manager, click **Solutions**.
4. On the **Solutions** page, in the solutions table select the **VMware vSphere** solution.
5. Under **Configured Adapter Instances**, verify that the **Collection State** is `Collecting` and the **Collection Status** is `Data receiving` for all vCenter Adapter instances.

What to do next

If you encounter issues while performing this procedure, use the following troubleshooting tips:

Troubleshooting Tips
■ Ensure that the vCenter Adapter is configured with the correct target vCenter Server. ■ Ensure that there is network connectivity between the vRealize Operations Manager and the vCenter Server. ■ Ensure that the service account credentials are correct.

Verify Collection Status of vSAN Adapter

Verify that vRealize Operations Manager is collecting data metrics trough the vSAN Adapter of the VMware vSAN Management Pack for vRealize Operations Manager.

Validating the status of data collection between vRealize Operations Manager and vCenter Server ensures that the vSAN Adapter is correctly configured, the provided service account has correct privileges and that dashboards are populated.

Expected Outcome
The vSAN Adapter has a **Collection State** of `Collecting` and a **Collection Status** of `Data receiving`.

Procedure

1. Log in to vRealize Operations Manager by using the operations interface.
   a. Open a Web browser and go to **`https://vrops01svr01.rainpole.local`**.
   b. Log in using the following credentials.

Setting	Value
User name	admin
Password	*vrops_admin_password*

2. On the main navigation bar, click **Administration.**
3. In the left pane of vRealize Operations Manager, click **Solutions**.
4. On the **Solutions** page, in the solutions table select the **VMware vSAN** solution.
5. Under **Configured Adapter Instances**, verify that the **Collection State** is `Collecting` and the **Collection Status** is `Data receiving` for all vSAN Adapter instances.

What to do next

If you encounter issues while performing this procedure, use the following troubleshooting tips:

Troubleshooting Tips
■ Ensure that the vSAN Adapter is configured with the correct target vCenter Server. ■ Ensure that there is network connectivity between the vRealize Operations Manager and the vCenter Server. ■ Ensure that the service account credentials are correct.

Verify Collection Status of vRealize Log Insight Adapter

Verify that vRealize Operations Manager is integrated with vRealize Log Insight trough the vRealize Log Insight Adapter of the VMware vRealize Log Insight Management Pack for vRealize Operations Manager.

Validating the status of data collection between vRealize Operations Manager and vRealize Log Insight ensures that the vRealize Log Insight Adapter is configured correctly.

Expected Outcome
The vRealize Log Insight Adapter has a **Collection State** of `Collecting` and a **Collection Status** of `Data receiving`.

Procedure

1. Log in to vRealize Operations Manager by using the operations interface.
   a. Open a Web browser and go to **`https://vrops01svr01.rainpole.local`**.
   b. Log in using the following credentials.

Setting	Value
User name	admin
Password	*vrops_admin_password*

2. On the main navigation bar, click **Administration.**
3. In the left pane of vRealize Operations Manager, click **Solutions**.
4. On the **Solutions** page, in the solutions table select the **VMware vRealize Log Insight** solution.
5. Under **Configured Adapter Instances**, verify that the **Collection State** is `Collecting` and the **Collection Status** is `Data receiving` for the vRealize Log Insight Adapter instance.

What to do next

If you encounter issues while performing this procedure, use the following troubleshooting tips:

Troubleshooting Tips
■ Ensure that the vRealize Log Insight Adapter is configured with the correct target vRealize Log Insight cluster. ■ Ensure that there is network connectivity between the vRealize Operations Manager and the vRealize Log Insight.

Verify Collection Status of vRealize Business for Cloud Adapter

Verify that vRealize Operations Manager is collecting data metrics trough the vRealize Business for Cloud Adapter of the VMware vRealize Business for Cloud Management Pack for vRealize Operations Manager.

Validating the status of data collection between vRealize Operations Manager and vRealize Business for Cloud ensures that the vRealize Business for Cloud Adapter is configured correctly.

Expected Outcome
The vRealize Business for Cloud Adapter has a**Collection State** of `Collecting` and a **Collection Status** of `Data receiving`.

Procedure

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

   a Open a Web browser and go to **`https://vrops01svr01.rainpole.local`**.

   b Log in using the following credentials.

Setting	Value
User name	admin
Password	*vrops_admin_password*

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

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

4 On the **Solutions** page, in the solutions table select the **VMware vRealize Business for Cloud** solution.

5 Under **Configured Adapter Instances**, verify that the **Collection State** is `Collecting` and the **Collection Status** is `Data receiving` for the vRealize Business for Cloud Adapter instance.

What to do next

If you encounter issues while performing this procedure, use the following troubleshooting tips:

Troubleshooting Tips
■ Ensure that the vRealize Business for Cloud Adapter is configured with the correct target vRealize Business for Cloud Server. ■ Ensure that there is network connectivity between the vRealize Operations Manager and the vRealize Business for Cloud Server.

Verify Collection Status of vRealize Automation Adapter

Verify that vRealize Operations Manager is collecting data metrics trough the vRealize Automation Adapter of the VMware vRealize Automation Management Pack for vRealize Operations Manager.

Validating the status of data collection between vRealize Operations Manager and vRealize Automation ensures that the vRealize Automation Adapter is configured correctly, the provided service account has correct privileges and that dashboards are populated.

Expected Outcome
The vRealize Automation Adapter has a **Collection State** of `Collecting` and a **Collection Status** of `Data receiving`.

Procedure

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

   a Open a Web browser and go to **`https://vrops01svr01.rainpole.local`**.

   b Log in using the following credentials.

Setting	Value
User name	admin
Password	*vrops_admin_password*

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

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

4 On the **Solutions** page, in the solutions table select the **VMware vRealize Automation** solution.

5 Under **Configured Adapter Instances**, verify that the **Collection State** is `Collecting` and the **Collection Status** is `Data receiving` for the vRealize Automation Adapter instance.

What to do next

If you encounter issues while performing this procedure, use the following troubleshooting tips:

Troubleshooting Tips
■ Ensure that the vRealize Automation Adapter is configured with the correct target vRealize Automation cluster. ■ Ensure that there is network connectivity between the vRealize Operations Manager and the vRealize Automation. ■ Ensure that the service account credentials are correct.

Verify Collection Status of SRM Adapter

Verify that vRealize Operations Manager is collecting data metrics trough the SRM Adapter of the VMware SRM Management Pack for vRealize Operations Manager.

Validating the status of data collection between vRealize Operations Manager and Site Recovery Manager server ensures that the SRM Adapter is configured correctly, the provided service account has correct privileges and that dashboards are populated.

Expected Outcome
The SRM Adapter has a **Collection State** of `Collecting` and a **Collection Status** of `Data receiving`.

Procedure

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

   a Open a Web browser and go to **`https://vrops01svr01.rainpole.local`**.

   b Log in using the following credentials.

Setting	Value
User name	admin
Password	*vrops_admin_password*

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

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

4 On the **Solutions** page, in the solutions table select the **Srm Adapter** solution.

5 Under **Configured Adapter Instances**, verify that the **Collection State** is `Collecting` and the **Collection Status** is `Data receiving` for the SRM Adapter instance.

What to do next

If you encounter issues while performing this procedure, use the following troubleshooting tips:

Troubleshooting Tips
■ Ensure that the SRM Adapter is configured with the correct target Site Recovery Manager instance. ■ Ensure that there is network connectivity between the vRealize Operations Manager and the Site Recovery Manager Server. ■ Ensure that the service account credentials are correct.

Verify Collection Status of Storage Devices Adapter

Verify that vRealize Operations Manager is collecting data metrics trough the Storage Devices Adapter of the VMware Storage Devices Management Pack for vRealize Operations Manager.

Validating the status of data collection between vRealize Operations Manager and vCenter Server ensures that the Storage Devices Adapter is configured correctly, the provided service account has correct privileges and that dashboards are populated.

Expected Outcome
The Storage Devices Adapter has a **Collection State** of `Collecting` and a **Collection Status** of `Data receiving`.

Procedure

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

   a Open a Web browser and go to **`https://vrops01svr01.rainpole.local`**.

   b Log in using the following credentials.

Setting	Value
User name	admin
Password	*vrops_admin_password*

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

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

4 On the **Solutions** page, in the solutions table select the **Management Pack for Storage Devices** solution.

5 Under **Configured Adapter Instances**, verify that the **Collection State** is `Collecting` and the **Collection Status** is `Data receiving` for all Storage Devices Adapter instances.

What to do next

If you encounter issues while performing this procedure, use the following troubleshooting tips:

Troubleshooting Tips
■ Ensure that the Storage Devices Adapter is configured with the correct target vCenter Server. ■ Ensure that there is network connectivity between the vRealize Operations Manager and the vCenter Server. ■ Ensure that the service account credentials are correct.

Verify Collection Status of NSX for vSphere Adapter

Verify that vRealize Operations Manager is collecting data metrics trough the NSX-vSphere Adapter of the VMware NSX-vSphere Management Pack for vRealize Operations Manager.

Validating the status of data collection between vRealize Operations Manager and vCenter Server ensures that the NSX-vSphere Adapter and the Network Devices Adapter are configured correctly, the provided service account has correct privileges and that dashboards are populated.

Expected Outcome
The NSX-vSphere Adapter instances and the Network Devices Adapter have **Collection State** of `Collecting` and **Collection Status** of `Data receiving`.

Procedure

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

   a Open a Web browser and go to **`https://vrops01svr01.rainpole.local`**.

   b Log in using the following credentials.

Setting	Value
User name	admin
Password	*vrops_admin_password*

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

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

4 On the **Solutions** page, in the solutions table select the **Management Pack for NSX-vSphere** solution.

5 Under **Configured Adapter Instances**, verify that the **Collection State** is `Collecting` and the **Collection Status** is `Data receiving` for all NSX-vSphere Adapter instances and the Network Devices Adapter instance.

What to do next

If you encounter issues while performing this procedure, use the following troubleshooting tips:

Troubleshooting Tips
■ Ensure that the NSX-vSphere Adapter is configured with the correct target vCenter Server and the NSX Manager. ■ Ensure that there is network connectivity between the vRealize Operations Manager and the NSX Manager. ■ Ensure that the Network Devices Adapter is configured with the correct network settings. ■ Ensure that the service account credentials are correct.

Verification of vRealize Log Insight

Verify the authentication and cluster status and verify that all vRealize Log Insight agents are listed and have Active status.

- Authenticate to vRealize Log Insight Using Local System Account and Verify Cluster Status

  Verify that you can authenticate to vRealize Log Insight using the built-in admin account.

- Verify Agent Status for vRealize Operations Manager Virtual Appliances

  Verify that vRealize Operations Manager is sending syslog data to the vRealize Log Insight cluster.

- Verify Agent Status for vRealize Automation Virtual Appliances

  Verify that vRealize Automation virtual appliances are sending syslog data to the vRealize Log Insight cluster.

- Verify Agent Status for Embedded vRealize Orchestrator

  Verify that vRealize Orchestrator is sending syslog data to the vRealize Log Insight cluster.

- Verify Agent Status for vRealize Automation Windows Systems

  Verify that vRealize Automation Windows systems are sending syslog data to the vRealize Log Insight cluster.

- Verify Agent Status for Microsoft SQL Server

  Verify that Microsoft SQL server used for the vRealize Automation database is sending syslog data to the vRealize Log Insight cluster.

- Verify Agent Status for Site Recovery Manager Server

  Verify that Site Recovery Manager server is sending syslog data to the vRealize Log Insight cluster.

Authenticate to vRealize Log Insight Using Local System Account and Verify Cluster Status

Verify that you can authenticate to vRealize Log Insight using the built-in admin account.

Performing authentication using the built-in admin account validates that vRealize Log Insight is online and accessible.

Expected Outcome
You can successfully authenticate using the built-in admin account and verify the status of the cluster.

Procedure

1 Log in to the vRealize Log Insight user interface.

   a Open a Web browser and go to **`https://sfo01vrli01.sfo01.rainpole.local`**.

   b Log in using the following credentials.

Setting	Value
User name	admin
Password	*vrli_admin_password*

2 Verify the status of vRealize Log Insight cluster nodes.

   a Click the configuration drop-down menu  , and click **Administration**.

   b Under **Management** in the navigator area, click **Cluster**.

   c Verify that the status of each cluster node is `Connected` and the status of Integrated Load Balancer is `Available`.

3 Repeat the procedure and validate for the **`lax01vrli01.lax01.rainpole.local`** vRealize Log Insight cluster.

What to do next

If you encounter issues while performing this procedure, use the following troubleshooting tips:

Troubleshooting Tips

- Ensure that the vRealize Log Insight appliances are powered on.
- Ensure that there is network connectivity to the vRealize Log Insight appliances and that the host names are resolvable in DNS.
- Ensure that there is network connectivity between the vRealize Log Insight nodes.
- Ensure that you have supplied the correct login credentials.

Verify Agent Status for vRealize Operations Manager Virtual Appliances

Verify that vRealize Operations Manager is sending syslog data to the vRealize Log Insight cluster.

Validating that agent communication between the vRealize Operations Manager virtual appliances and the vRealize Log Insight cluster ensures that the agent is configured correctly and that there is network connectivity.

Expected Outcome

Each vRealize Operations Manager virtual appliance is listed in the vRealize Log Insight agent list and has `Active` **Status**.

Procedure

1 Log in to the vRealize Log Insight user interface.

   a Open a Web browser and go to **`https://sfo01vrli01.sfo01.rainpole.local`**.

   b Log in using the following credentials.

Setting	Value
User name	admin
Password	*vrli_admin_password*

2 Click the configuration drop-down menu  , and click **Administration**.

3 Under **Management**, click **Agents**.

4 From the **All Agents** drop-down menu, select **vROPs - Appliance Agent Group**.

5 Verify that each vRealize Operations Manager virtual appliance is listed and has `Active` **Status**.

6 Repeat the procedure and validate for the **`lax01vrli01.lax01.rainpole.local`** vRealize Log Insight cluster.

What to do next

If you encounter issues while performing this procedure, use the following troubleshooting tips:

Troubleshooting Tips

- Ensure that the vRealize Log Insight agent service is running on the virtual appliance.
- Ensure that there is network connectivity between the systems.
- Ensure that the configuration file `liagent.ini` is configured correctly on the virtual appliance.

Verify Agent Status for vRealize Automation Virtual Appliances

Verify that vRealize Automation virtual appliances are sending syslog data to the vRealize Log Insight cluster.

Validating that agent communication between the vRealize Automation virtual appliances and the vRealize Log Insight cluster ensures that the agent is configured correctly and that there is network connectivity.

Expected Outcome
Each vRealize Automation virtual appliance is listed in the vRealize Log Insight agent list and has `Active` **Status**.

Procedure

1 Log in to the vRealize Log Insight user interface.

   a Open a Web browser and go to **`https://sfo01vrli01.sfo01.rainpole.local`**.

   b Log in using the following credentials.

Setting	Value
User name	admin
Password	*vrli_admin_password*

2 Click the configuration drop-down menu  , and click **Administration**.

3 Under **Management**, click **Agents**.

4 From the **All Agents** drop-down menu, select **vRA7 - Appliance Agent Group**.

5 Verify that each vRealize Automation virtual appliance is listed and has `Active` **Status**.

What to do next

If you encounter issues while performing this procedure, use the following troubleshooting tips:

Troubleshooting Tips
■ Ensure that the vRealize Log Insight agent service is running on the virtual appliance. ■ Ensure that there is network connectivity between the systems. ■ Ensure that the configuration file `liagent.ini` is configured correctly on the virtual appliance.

Verify Agent Status for Embedded vRealize Orchestrator

Verify that vRealize Orchestrator is sending syslog data to the vRealize Log Insight cluster.

Validating that agent communication between the embedded vRealize Orchestrator and the vRealize Log Insight cluster ensures that the agent is configured correctly and that there is network connectivity.

Expected Outcome
Each embedded vRealize Orchestrator virtual appliance is listed in the vRealize Log Insight agent list and has `Active` **Status**.

Procedure

1 Log in to the vRealize Log Insight user interface.

   a Open a Web browser and go to **`https://sfo01vrli01.sfo01.rainpole.local`**.

   b Log in using the following credentials.

Setting	Value
User name	admin
Password	*vrli_admin_password*

2 Click the configuration drop-down menu  , and click **Administration**.

3 Under **Management**, click **Agents**.

4 From the **All Agents** drop-down menu, select **vRO7 - Appliance Agent Group**.

5 Verify that each embedded vRealize Orchestrator virtual appliance is listed and has `Active` **Status**.

What to do next

If you encounter issues while performing this procedure, use the following troubleshooting tips:

Troubleshooting Tips
■ Ensure that the vRealize Log Insight agent service is running on the virtual appliance. ■ Ensure that there is network connectivity between the systems. ■ Ensure that the configuration file `liagent.ini` is configured correctly on the virtual appliance.

Verify Agent Status for vRealize Automation Windows Systems

Verify that vRealize Automation Windows systems are sending syslog data to the vRealize Log Insight cluster.

Validating that agent communication between the vRealize Automation Windows Systems and the vRealize Log Insight cluster ensures that the agent is configured correctly and that there is network connectivity.

Expected Outcome
Each vRealize Automation Windows System is listed in the vRealize Log Insight agent list and has `Active` **Status**.

Procedure

1 Log in to the vRealize Log Insight user interface.

   a Open a Web browser and go to **`https://sfo01vrli01.sfo01.rainpole.local`**.

   b Log in using the following credentials.

Setting	Value
User name	admin
Password	*vrli_admin_password*

2 Click the configuration drop-down menu and click **Administration**.

3 Under **Management**, click **Agents**.

4 From the **All Agents** drop-down menu, select **vRA - Windows Agent Group**.

5 Verify that each vRealize Automation Windows System is listed and has `Active` **Status**.

6 Repeat the procedure and validate for the **`lax01vrli01.lax01.rainpole.local`** vRealize Log Insight cluster.

What to do next

If you encounter issues while performing this procedure, use the following troubleshooting tips:

Troubleshooting Tips
■ Ensure that the vRealize Log Insight agent service is running on the virtual machine. ■ Ensure that there is network connectivity between the systems.

Verify Agent Status for Microsoft SQL Server

Verify that Microsoft SQL server used for the vRealize Automation database is sending syslog data to the vRealize Log Insight cluster.

Validating that agent communication between the Microsoft SQL Server and the vRealize Log Insight cluster ensures that the agent is configured correctly and that there is network connectivity.

Expected Outcome
The Microsoft SQL Server is listed in the vRealize Log Insight agent list and has `Active` **Status**.

Procedure

1 Log in to the vRealize Log Insight user interface.

   a Open a Web browser and go to **`https://sfo01vrli01.sfo01.rainpole.local`**.

   b Log in using the following credentials.

Setting	Value
User name	admin
Password	*vrli_admin_password*

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

3 Under **Management**, click **Agents**.

4 From the **All Agents** drop-down menu, select **vRA - SQL Agent Group**.

5 Verify that the Microsoft SQL Server is listed and has `Active` **Status**.

What to do next

If you encounter issues while performing this procedure, use the following troubleshooting tips:

Troubleshooting Tips
■ Ensure that the vRealize Log Insight agent service is running on the virtual machine. ■ Ensure that there is network connectivity between the systems.

Verify Agent Status for Site Recovery Manager Server

Verify that Site Recovery Manager server is sending syslog data to the vRealize Log Insight cluster.

Validating agent communication between the Site Recovery Manager server and the vRealize Log Insight cluster ensures that the agent is configured correctly and that there is network connectivity.

Expected Outcome
The Site Recovery Manager server is listed in the vRealize Log Insight agent list and has `Active` **Status**.

Procedure

1 Log in to the vRealize Log Insight user interface.

   a Open a Web browser and go to **`https://sfo01vrli01.sfo01.rainpole.local`**.

   b Log in using the following credentials.

Setting	Value
User name	admin
Password	*vrli_admin_password*

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

3 Under **Management**, click **Agents**.

4 From the **All Agents** drop-down menu, select **SRM - Agent Group**.

5 Verify that the Site Recovery Manager server is listed and has `Active` **Status**.

6 Repeat the procedure and validate for the **`lax01vrli01.lax01.rainpole.local`** vRealize Log Insight cluster.

What to do next

If you encounter issues while performing this procedure, use the following troubleshooting tips:

Troubleshooting Tips
■ Ensure that the vRealize Log Insight agent service is running on the virtual machine. ■ Ensure there is network connectivity between the systems.

Verification of vSphere Update Manager Download Service

Verify that vSphere Update Manager Download Service can connect to the VMware Internet service and successfully checks for updates.

Run the vSphere Update Manager Download Service Cron Job

Verify that the vSphere Update Manager Download Service cron job runs and checks for updates to download.

Validating that you can run the cron job ensures that the configuration is correct and that the vSphere Update Manager Download Service (UMDS) virtual machine has network connectivity to the VMware Internet service.

Expected Outcome
The vSphere Update Manager Download Service connects to the VMware Internet service and checks for new updates to download.

Procedure

1 Log in to the vSphere Update Manager Download Service using a Secure Shell (SSH) client.

   a Open an SSH connection to **`sfo01umds01.sfo01.rainpole.local`**.

   b Log in using the following credentials.

Setting	Value
User Name	svc-umds
Password	*svc-umds_password*

2 Verify the cron job checks for updates.

   a Run the following command.

   ```
   sudo /etc/cron.daily/umds-download
   ```

   When prompted for the password of the svc-umds user, enter *svc-umds_password*.

   b Verify that vSphere Update Manager Download Service connects to the VMware Internet service and checks for updates. Details for the new updates are displayed in the console.

3 Repeat the procedure and validate for the **`lax01umds01.lax01.rainpole.local`** vSphere Update Manager Download Service instance.

What to do next

If you encounter issues while performing this procedure, use the following troubleshooting tips:

Troubleshooting Tips
■ Ensure that there is network connectivity from vSphere Update Manager Download Service virtual machine to the Internet.

Operational Verification of the Cloud Management Layer

3

Perform operational verification steps to verify the operational state of the cloud management layer following initial installation or any type of outage affecting an individual component or system.

Operational verification of the cloud management layer involves the following management components:

- vRealize Automation
- vRealize Business for Cloud
- Authenticate to vRealize Automation Using Local System Account

  Verify that you can authenticate to vRealize Automation portal using the administrator@vsphere.local system account.
- Authenticate to vRealize Automation Using Active Directory Admin Account

  Verify that you can authenticate to vRealize Automation portal using the vra-admin-rainpole@rainpole.local Active Directory account within the rainpole tenant.
- Verify vRealize Automation Components Are Highly Available

  Verify that you can continue to operate the vRealize Automation stack even as individual stack components become unavailable.
- Verify Integration of vRealize Automation with vSphere Infrastructure

  Verify that you can provision virtual machines using vRealize Automation blueprints into the vCenter for which a vSphere endpoint was created during the initial deployment and configuration.
- Verify Integration of vRealize Automation with vRealize Orchestrator and NSX for vSphere

  Verify that you can provision NSX objects using the vRealize Automation multi-tiered blueprint provisioning.
- Verify Integration of vRealize Automation with vRealize Business for Cloud

  Verify that you can access the vRealize Business for Cloud menu in vRealize Automation portal to view costing reports.
- Verify Integration of vRealize Automation with vRealize Operations Manager

  Verify that you can use the reclamation menu in vRealize Automation to identify virtual machines that have not been powered on for a defined period as reported by the vRealize Operations Manager.

Authenticate to vRealize Automation Using Local System Account

Verify that you can authenticate to vRealize Automation portal using the administrator@vsphere.local system account.

Performing authentication using the local system account verifies that the vRealize Automation authentication function is functional.

Expected Outcome
You can successfully authenticate using the **`administrator@vsphere.local`** system account and have visibility of all the tenants.

Procedure

1 Log in to the vRealize Automation portal.

   a Open a Web browser and go to **`https://vra01svr01.rainpole.local/vcac`**.

   b Log in using the following credentials.

Setting	Value
User name	administrator
Password	*vra_administrator_password*
Domain	vsphere.local

2 On the `Tenants` page, verify that you can see the tenants listed.

What to do next

If you encounter issues while performing this procedure, use the following troubleshooting tips:

Troubleshooting Tips
■ Ensure that the correct login credentials are used. ■ Ensure that all the vRealize Automation services are running. ■ Ensure that all the vRealize Automation virtual machines are configured to use the same NTP server and they are time synchronized.

Authenticate to vRealize Automation Using Active Directory Admin Account

Verify that you can authenticate to vRealize Automation portal using the vra-admin-rainpole@rainpole.local Active Directory account within the rainpole tenant.

Performing authentication using a tenant admin account configured in Active Directory verifies that the tenant is correctly configured and that the embedded vIDM can authenticate against the Active Directory for this tenant.

Expected Outcome
You can successfully authenticate and log in using vra-admin-rainpole@rainpole.local which has a tenant (rainpole) wide access for performing administrator functions.

Procedure

1 Log in to the vRealize Automation Rainpole portal.

   a Open a Web browser and go to **`https://vra01svr01.rainpole.local/vcac/org/rainpole`**.

   b Log in using the following credentials.

Setting	Value
User name	vra-admin-rainpole
Password	*vra-admin-rainpole_password*
Domain	rainpole.local

2 Verify that you see the **Administration**, **Infrastructure**, and **Business Management** menus.

What to do next

If you encounter issues while performing this procedure, use the following troubleshooting tips:

Troubleshooting Tips
■ Ensure that there is network connectivity between the Active Directory infrastructure and the vRealize Automation servers. ■ Ensure that the Active Directory user group that vra-admin-rainpole account is a member of, has been synchronized in vRealize Automation. ■ Ensure that the vra-admin-rainpole account has been granted the IaaS Administrator and Tenant Admin privileges. ■ Ensure that the vra-admin-rainpole account is an active account and has not been locked in Active Directory.

Verify vRealize Automation Components Are Highly Available

Verify that you can continue to operate the vRealize Automation stack even as individual stack components become unavailable.

Performing system login and provisioning blueprints while some of the stack components are unavailable validates that the vRealize Automation stack is built for resiliency and eliminates single points of failure.

Expected Outcome
You can successfully perform all the login and provisioning operations without any disruptions.

Procedure

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

   a Open a Web browser and go to **`https://sfo01m01vc01.sfo01.rainpole.local/vsphere-client`**.

   b Log in using the following credentials.

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

2 Shut down the secondary node of vRealize Automation.

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

   b In the **Navigator** pane, expand the **sfo01m01vc01.sfo01.rainpole.local > sfo01-m01dc > sfo01-m01fd-vra** tree.

   c Right-click the **vra01svr01b** virtual machine, select **Power > Shut Down Guest OS** and click **Yes** in the confirmation box that appears.

3 Log in to the vRealize Automation Rainpole portal.

   a Open a Web browser and go to **`https://vra01svr01.rainpole.local/vcac/org/rainpole`**.

   b Log in using the following credentials.

Setting	Value
User name	vra-admin-rainpole
Password	*vra-admin-rainpole_password*
Domain	rainpole.local

4 Request a single-machine blueprint item from the service catalog of vRealize Automation.

   a In the **Infrastructure Service Portal**, click the **Catalog** tab.

   b Locate the **Windows Server 2012 R2 - SFO Prod** single-machine blueprint and click **Request**.

   c On the **New Request** page, click **Submit** to request a virtual machine provisioning.

5 Click the **Requests** tab and verify that the **Status** column for the **Windows Server 2012 R2 - SFO Prod** single-machine blueprint provisioning is `Successful`.

6 Repeat the procedure and validate for the other nodes of vRealize Automation by shutting down either primary or secondary node.

What to do next

If you encounter issues while performing this procedure, use the following troubleshooting tips:

Troubleshooting Tips

- Ensure that automatic failover of Manager Service is enabled.

  Note This feature is available in vRA 7.3.
- Ensure that the load balancer is operational and the application profiles, pools, service monitoring, and virtual servers pertaining to vRealize Automation are configured correctly.
- Ensure that vRealize Automation appliance clustering is configured correctly.
- Ensure that at least one component in each layer of the stack is up and running.
- Ensure that all the service monitoring URLs are functional.

Verify Integration of vRealize Automation with vSphere Infrastructure

Verify that you can provision virtual machines using vRealize Automation blueprints into the vCenter for which a vSphere endpoint was created during the initial deployment and configuration.

Validating the ability to provision virtual machines into the vSphere infrastructure verifies the integration between vRealize Automation and vSphere infrastructure that consists of one or more vCenter servers.

Expected Outcome

You can perform data collection on vSphere endpoints and you can provision and destroy virtual machines in the vCenter that represent the vSphere endpoints.

Procedure

1 Log in to the vRealize Automation Rainpole portal.

  a Open a Web browser and go to **`https://vra01svr01.rainpole.local/vcac/org/rainpole`**.

  b Log in using the following credentials.

Setting	Value
User name	vra-admin-rainpole
Password	*vra-admin-rainpole_password*
Domain	rainpole.local

2 Verify virtual machine provisioning.

  a On the **Infrastructure Service Portal**, click the **Catalog** tab.

  b Choose a service catalog, for example **Windows Server 2012 R2 - SFO Prod** and click **Request**.

  c On the **New Request** page, click **Submit** to request a virtual machine provisioning.

  d Click the **Requests** tab and verify that the **Status** column for the **Windows Server 2012 R2 - SFO Prod** single-machine blueprint provisioning is `Successful`.

3 Verify virtual machine destroy operation.
   a On the **Infrastructure Service Portal**, click the **Infrastructure** tab.
   b Click **Managed Machines**, point to the chosen virtual machine, click **Destroy** and click **OK**.
   c Verify that the virtual machine is removed from the list.
4 Repeat the verification procedure using the **Windows Server 2012 R2 - LAX Prod** single-machine blueprint for Region B vCenter Server.

What to do next

If you encounter issues while performing this procedure, use the following troubleshooting tips:

Troubleshooting Tips
■ Ensure that there is network connectivity between vRealize Automation servers and the vCenter Servers. ■ Ensure that the correct credentials are used for the endpoints. ■ Ensure that data collection is successful.

Verify Integration of vRealize Automation with vRealize Orchestrator and NSX for vSphere

Verify that you can provision NSX objects using the vRealize Automation multi-tiered blueprint provisioning.

Provisioning NSX objects like load balancers or edge gateways within a vRealize Automation blueprint verifies the integration with NSX infrastructure, and verifies the embedded vRealize Orchestrator which facilitates the communication between vRealize Automation and NSX.

Expected Outcome
You can successfully add NSX endpoints, perform data collection on these endpoints, and provision NSX objects from within vRealize Automation when an appropriately configured multi-tiered blueprint is provisioned.

Procedure

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

Setting	Value
User name	vra-admin-rainpole
Password	*vra-admin-rainpole_password*
Domain	rainpole.local

2 Verify the data collection of vRealize Orchestrator endpoint.
   a On the **Infrastructure Service Portal**, click **Infrastructure > Endpoints > Endpoints**.
   b Select the vRealize Orchestrator endpoint, click **Actions > Data Collection**, and click **Start**.
   c Wait until the data collection is successful.
   d Click the **Refresh** button and verify that the **Status** shows `Data collection succeeded` with date and time details.
3 Verify the provisioning of NSX objects using multi-tiered blueprint.
   a On the **Infrastructure Service Portal**, click the **Catalog** tab.
   b Select the service catalog which has NSX components like load balancers or edge gateways, click **Request**, and click **Submit**.
   c Click the **Requests** tab and verify that the **Status** column for the NSX multi-tiered blueprint provisioning is `Successful`.

What to do next

If you encounter issues while performing this procedure, use the following troubleshooting tips:

Troubleshooting Tips
■ Ensure that there is network connectivity between vRealize Automation servers and the NSX infrastructure. ■ Ensure that the correct credentials are used for the NSX endpoints. ■ Ensure that data collection is successful. ■ Ensure that the blueprints are configured correctly.

Verify Integration of vRealize Automation with vRealize Business for Cloud

Verify that you can access the vRealize Business for Cloud menu in vRealize Automation portal to view costing reports.

Validating the integration between vRealize Automation and vRealize Business for Cloud ensures that integration between the components is configured and that there are no network connectivity issues.

Expected Outcome
You can successfully authenticate using a service account and have visibility of all vCenter Servers and their inventories with the appropriate user access.

Procedure

1 Log in to the vRealize Automation Rainpole portal.

   a Open a Web browser and go to **https://vra01svr01.rainpole.local/vcac/org/rainpole** .

   b Log in using the following credentials.

Setting	Value
User name	vra-admin-rainpole
Password	*vra-admin-rainpole_password*
Domain	rainpole.local

2 On the **Infrastructure Service Portal**, select the **Business Management** tab.

3 Click **Overview** and verify that the vCenter Server inventories are visible with costing reports.

What to do next

If you encounter issues while performing this procedure, use the following troubleshooting tips:

Troubleshooting Tips
■ Ensure that there is network connectivity between vRealize Automation virtual appliances and vRealize Business for Cloud Server. ■ Ensure that the correct credentials are used.

Verify Integration of vRealize Automation with vRealize Operations Manager

Verify that you can use the reclamation menu in vRealize Automation to identify virtual machines that have not been powered on for a defined period as reported by the vRealize Operations Manager.

Identifying the candidate virtual machines that have not been powered on as reclamation candidates can help prevent a virtual machine sprawl and also validates the integration between vRealize Automation and vRealize Operations Manager components.

Expected Outcome
You can access the reclamation menu in vRealize Automation portal where dormant virtual machines are reported.

Procedure

1 Log in to the vRealize Automation Rainpole portal.

   a Open a Web browser and go to **`https://vra01svr01.rainpole.local/vcac/org/rainpole`**.

   b Log in using the following credentials.

Setting	Value
User name	vra-admin-rainpole
Password	*vra-admin-rainpole_password*
Domain	rainpole.local

2 On the **Infrastructure Service Portal**, click the **Administration** tab.

3 Click **Reclamation > Metrics Provider** on the left side.

4 On the **Metrics Provider** page, click **Test Connection** and verify that the connection is successful.

What to do next

If you encounter issues while performing this procedure, use the following troubleshooting tips:

Troubleshooting Tips
■ Ensure that there is network connectivity between vRealize Automation servers and vRealize Operations Manager servers. ■ Ensure that the correct credentials are used.

Operational Verification of the Business Continuity Layer

4

Perform operational verification steps to verify the operational state of the business continuity layer following initial installation or any type of outage affecting an individual component or system.

Operational verification of the business continuity layer involves the following management components:

- Site Recovery Manager
- vSphere Replication
- Verify Pairing of Site Recovery Manager Across Regions

  Verify that the Site Recover Manager instances are paired.
- Verify Pairing of vSphere Replication Across Regions

  Verify that the vSphere Replication instances are paired.
- Perform Test Recovery of Operations Management Recovery Plan

  Verify the recovery plan for the operations management layer.
- Perform Test Recovery of Cloud Management Recovery Plan

  Verify the recovery plan for the cloud management layer.
- Verify Status and Configuration of vSphere Storage APIs for Data Protection Based Backup Solution

  Verify the operational status of the vSphere Storage APIs for Data Protection (VADP) based backup solution after you perform a software maintenance operation.

Verify Pairing of Site Recovery Manager Across Regions

Verify that the Site Recover Manager instances are paired.

Verifying that Site Recovery Manager instances are paired validates that the network communication between regions is operational and that the service account has the correct privileges.

Expected Outcome
You can successfully authenticate to vCenter Server and verify that the regions are paired and connected.

Procedure

1 Log into vCenter Server by using the vSphere Web Client.

   a Open a Web browser and go to **`https://sfo01m01vc01.sfo01.rainpole.local/vsphere-client`**.

   b Log in using the following credentials.

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

2 From the **Home** menu, select **Site Recovery**.

3 In the **Navigator** pane, click **Sites** and click the **sfo01m01vc01.sfo01.rainpole.local** site.

4 On the **Summary** tab, verify the following details.

Settings	Site	Paired Site
Name	sfo01m01vc01.sfo01.rainpole.local	lax01m01vc01.lax01.rainpole.local
Client Connection	Connected	Connected
Server Connection	Connected	Connected
SRM Server	sfo01m01srm01.sfo01.rainpole.local:9086	lax01m01srm01.lax01.rainpole.local:9086
vCenter Server	sfo01m01vc01.sfo01.rainpole.local:443	lax01m01vc01.lax01.rainpole.local:443
SRM Server Build	*srm_build_version*	*srm_build_version*
Organization	VMware, Inc.	VMware, Inc.
Logged in as	VSPHERE.LOCAL\Administrator	VSPHERE.LOCAL\Administrator
VR Compatibility	*vr_version* - Compatible	*vr_version* - Compatible

What to do next

If you encounter issues while performing this procedure, use the following troubleshooting tips:

Troubleshooting Tips
■ Ensure that there is network connectivity between all vCenter Server and Site Recovery Manager Servers.

Verify Pairing of vSphere Replication Across Regions

Verify that the vSphere Replication instances are paired.

Verifying that vSphere Replication instances are paired validates that the network communication between regions is operational and that the service accounts has the correct privileges.

Expected Outcome
You can successfully authenticate to vCenter Server and verify that the regions are connected and paired.

Procedure

1 Log into vCenter Server by using the vSphere Web Client.

   a Open a Web browser and go to **`https://sfo01m01vc01.sfo01.rainpole.local/vsphere-client`**.

   b Log in using the following credentials.

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

2 From the **Home** menu, select **Hosts and Clusters**.

3 In the **Navigator** pane, select the **sfo01m01vc01.sfo01.rainpole.local** instance.

4 Click the **Configure** tab, and click **Target Sites** under **vSphere Replication**.

5 Verify the following details.

Settings	Value
Name	lax01m01vc01.lax01.rainpole.local
VR Appliance	172.17.11.123
Status	Connected

What to do next

If you encounter issues while performing this procedure, use the following troubleshooting tips:

Troubleshooting Tips
■ Ensure there is network connectivity between all vCenter Server and vSphere Replication instances

Perform Test Recovery of Operations Management Recovery Plan

Verify the recovery plan for the operations management layer.

Performing a test recovery of the operations management recovery plan ensures that the virtual machines are being replicated correctly and the power on order is accurate with the correct timeout values and dependencies. Site Recovery Manager runs the analytic cluster nodes on an isolated test network using a temporary snapshot of replicated data while performing test recovery.

Expected Outcome
You can successfully complete the operations management recovery plan under a test recovery scenario.

Procedure

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

   a Open a Web browser and go to **`https://sfo01m01vc01.sfo01.rainpole.local/vsphere-client`**.

   b Log in using the following credentials.

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

2 From the **Home** menu, select **Site Recovery**.

3 Under Inventory Trees, click the **Recovery Plans** and click the **SDDC Operations Management RP** recovery plan.

4 On the **SDDC Operations Management RP** page, click the **Monitor** tab and click **Recovery Steps**.

5 Click the **Test Recovery Plan** icon to run a test recovery.

   The **Test** wizard appears.

6 On the **Confirmation options** page, leave the **Replicate recent changes to recovery site** check box selected and click **Next**.

7 On the **Ready to complete** page, click **Finish** to start the test recovery.

   Test failover starts. You can follow the progress on the **Recovery Steps** page.

8 After the test recovery is complete, click the **Cleanup Recovery Plan** icon to clean up all the created test VMs.

9 On the **Confirmation options** page of the **Cleanup** wizard, click **Next**.

10 On the **Ready to complete** page, click **Finish** to start the clean-up process.

Note Log in to **`lax01m01vc01.lax01.rainpole.local`** vCenter Server and follow the procedure if the protected vRealize Operations Manager virtual machines are located in Region B.

What to do next

If you encounter issues while performing this procedure, use the following troubleshooting tips

Troubleshooting Tips
■ Ensure that there is network connectivity between all vCenter Server and vSphere Replication instances. ■ Ensure that there is network connectivity between all vCenter Server and Site Recovery Manager Servers. ■ Ensure that the replication is occurring for the protected VMs.

Perform Test Recovery of Cloud Management Recovery Plan

Verify the recovery plan for the cloud management layer.

Performing a test recovery of the cloud management recovery plan ensures that the virtual machines are being replicated correctly and the power on order is accurate with the correct timeout values and dependencies. Site Recovery Manager runs the vRealize Automation and vRelize Business for Cloud nodes on an isolated test network using a temporary snapshot of replicated data while performing test recovery.

Expected Outcome
You can successfully complete the cloud management recovery plan under a test recovery scenario.

Procedure

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

   a Open a Web browser and go to **`https://sfo01m01vc01.sfo01.rainpole.local/vsphere-client`**.

   b Log in using the following credentials.

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

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

3 On the Site Recovery home page, click **Sites** and double-click the **sfo01m01vc01.sfo01.rainpole.local** protected site.

4 If the **Log In Site** dialog box appears, re-authenticate by using the **`svc-srm@rainpole.local`** user name and the ***`svc-srm_password`*** password.

   Re-authentication is required if the network connection between Region A and Region B has been interrupted after the last successful authentication.

5 On the **Related Objects** tab, click the **Recovery Plans** tab and click the **SDDC Cloud Management RP** recovery plan.

6 On the **SDDC Cloud Management RP** page, click the **Monitor** tab and click **Recovery Steps**.

7 Click the **Test Recovery Plan** icon to run a test recovery.

   The **Test** wizard appears.

8 On the **Confirmation options** page, leave the **Replicate recent changes to recovery site** check box selected and click **Next**.

9 On the **Ready to complete** page, click **Finish** to start the test recovery.

Test failover starts. You can follow the progress on the **Recovery Steps** page.

Note Because recovered virtual machines are using the test network, VMware Tools in the vra01svr01a.rainpole.local and vra01svr01b.rainpole.local virtual machines might not become online within the default timeout. In the recovery plan, increase the startup delay for VMware Tools for these virtual machines to complete the test.

10 After the test recovery is complete, click the **Cleanup Recovery Plan** icon to clean up all the created test VMs.

11 On the **Confirmation options** page of the **Cleanup** wizard, click **Next**.

12 On the **Ready to complete** page, click **Finish** to start the clean-up process.

Note Log in to the `lax01m01vc01.lax01.rainpole.local` vCenter Server and follow the procedure if the protected vRealize Operations Manager VMs are located in Region B.

What to do next

If you encounter issues while performing this procedure, use the following troubleshooting tips

Troubleshooting Tips
■ Ensure that there is network connectivity between all vCenter Server and vSphere Replication instances. ■ Ensure that there is network connectivity between all vCenter Server and Site Recovery Manager Servers. ■ Ensure that the replication is occurring for the protected VMs.

Verify Status and Configuration of vSphere Storage APIs for Data Protection Based Backup Solution

Verify the operational status of the vSphere Storage APIs for Data Protection (VADP) based backup solution after you perform a software maintenance operation.

Verifying the operational status of vSphere Storage APIs for Data Protection (VADP) based backup solution validates the correct configuration.

Expected Outcome
You can confirm that a backup of the Management cluster has occurred in the past 24 hours.

Procedure

- Verify that the VADP-based backup solution is registered with the Management vCenter Server.
- Verify that all the services are correctly running on the storage solution.
- Verify that any proxies that have been deployed from the VADP-based backup solution are registered and running.

- Verify that sufficient space has been allocated for the Management cluster applications.

  Consult the sizing guide for an estimate on the initial deployment size of the validated design.
- Verify that the VADP-based backup solution has successfully taken backups of the Management cluster in the past 24 hours.

Post Upgrade Verification 5

After an upgrade of the Software Defined Data Center, perform post upgrade verification to ensure that each SDDC component has been upgraded successfully.

Post upgrade verification involves the following layers:

- Virtual Infrastructure Layer
- Operations Management Layer
- Cloud Management Layer
- Business Continuity Layer
- Version Verification of the Virtual Infrastructure Layer

  After an upgrade of the virtual infrastructure layer, perform post upgrade verification to ensure that each component has been upgraded successfully.
- Version Verification of the Operations Management Layer

  After an upgrade of the operations management layer, perform post upgrade verification to ensure that each component has been upgraded successfully.
- Version Verification of the Cloud Management Layer

  After an upgrade of the cloud management layer, perform post upgrade verification to ensure that each component has been upgraded successfully.
- Version Verification of the Business Continuity Layer

  After an upgrade of the business continuity layer, perform post upgrade verification to ensure that each component has been upgraded successfully.

Version Verification of the Virtual Infrastructure Layer

After an upgrade of the virtual infrastructure layer, perform post upgrade verification to ensure that each component has been upgraded successfully.

Version verification of the virtual infrastructure layer involves the following components:

- ESXi hosts
- vCenter Servers
- Platform Services Controllers

- NSX Managers
- NSX Controllers
- NSX Edge services gateways
- Verify the Version of Platform Service Controller

  Verify the version of the Platform Services Controllers after you perform an upgrade operation in the Software Defined Data Center.
- Verify the Version of vCenter Server

  Verify the version of the vCenter Server instances after you perform an upgrade operation in the Software Defined Data Center.
- Verify the Version of ESXi Host

  Verify the version of the ESXi hosts after you perform an upgrade operation in the Software Defined Data Center.
- Verify the Version of NSX for vSphere

  Verify the version of NSX Manager, NSX Controller, and NSX Edge appliances, and NSX for vSphere Installation Bundles after you perform an upgrade operation in the Software Defined Data Center.

Verify the Version of Platform Service Controller

Verify the version of the Platform Services Controllers after you perform an upgrade operation in the Software Defined Data Center.

Procedure

1. Log in to the management interface of the Platform Services Controller virtual appliance.
   a. Open a Web browser and go to **`https://sfo01m01psc01.sfo01.rainpole.local:5480`**.
   b. Log in using the following credentials.

Setting	Value
User name	root
Password	*mgmtpsc_root_password*

2. Verify the version of the Platform Services Controller.
   a. In the **Navigator**, click **Update**.
   b. On the **Update** page, under **Current version details**, verify that **Update version** shows the expected version and build number.
3. Repeat the procedure for the remaining Platform Services Controller instances.

Verify the Version of vCenter Server

Verify the version of the vCenter Server instances after you perform an upgrade operation in the Software Defined Data Center.

Procedure

1 Log in to the management interface of the vCenter Server Appliance.

a Open a Web browser and go to **`https://sfo01m01vc01.sfo01.rainpole.local:5480`**.

b Log in using the following credentials.

Setting	Value
User name	root
Password	*mgmtvc_root_password*

2 Verify the version of the vCenter Server instance.

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

b On the **Update** page, under **Current version details**, verify that **Update version** shows the expected version and build number.

3 Repeat the procedure for the remaining vCenter Server instances.

Verify the Version of ESXi Host

Verify the version of the ESXi hosts after you perform an upgrade operation in the Software Defined Data Center.

Procedure

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

a Open a Web browser and go to **`https://sfo01m01vc01.sfo01.rainpole.local/vsphere-client`**.

b Log in using the following credentials.

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

2 Navigate to the ESXi host.

a From the **Home** menu, select **Hosts and Clusters**.

b In the **Navigator**, expand the **sfo01m01vc01.sfo01.rainpole.local > sfo01-m01dc > sfo01-m01-mgmt01** inventory tree.

c Click the **sfo01m01esx01.sfo01.rainpole.local** host.

3 On the **Summary** tab, verify that the **Hypervisor** shows the expected version number for the ESXi host.

4 Repeat the procedure for all remaining ESXi hosts across all vCenter Server instances.

Verify the Version of NSX for vSphere

Verify the version of NSX Manager, NSX Controller, and NSX Edge appliances, and NSX for vSphere Installation Bundles after you perform an upgrade operation in the Software Defined Data Center.

Procedure

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

   a Open a Web browser and go to **`https://sfo01m01vc01.sfo01.rainpole.local/vsphere-client`**.

   b Log in using the following credentials.

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

2 From the **Home** menu, click **Networking & Security**.

3 Verify the version of NSX Manager and NSX Controller nodes.

   a In the **Navigator** pane, click **Installation and Upgrade**.

   b On the **Management** tab, under **NSX Managers**, verify that the **Version** column has the expected version number for each NSX Manager.

   c Under **NSX Controller nodes**, verify that the **Software Version** column has the expected version number for each NSX Controller.

4 Verify the version of NSX Edge appliances.

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

   b From the **NSX Manager** drop-down menu, select the **172.16.11.65** NSX Manager.

   c Verify that the **Version** column has the expected version number for each NSX Edge.

5 Verify the version of NSX for vSphere Installation Bundles.

   a In the **Navigator** pane, click **Installation and Upgrade**.

   b Click the **Host Preparation** tab, and under **NSX Component Installation on Hosts** expand the management cluster `sfo01-m01-mgmt01` to see the ESXi hosts.

   c Verify that the **Installation Status** column has the expected version number for each of the hosts.

6 Repeat the procedure for the remaining NSX Manager and NSX Edge appliances and NSX for vSphere Installation Bundles for ESXi hosts.

Version Verification of the Operations Management Layer

After an upgrade of the operations management layer, perform post upgrade verification to ensure that each component has been upgraded successfully.

Version verification of the operations management layer involves the following components:

- vRealize Operations Manager
- vRealize Log Insight
- vSphere Update Manager Download Service
- Verify the Version of vRealize Operations Manager

  Verify the version of the analytics and remote collector nodes of vRealize Operations Manager after you perform an upgrade operation in the Software Defined Data Center.
- Verify the Version of vRealize Log Insight

  Verify the version of vRealize Log Insight nodes after you perform an upgrade operation in the Software Defined Data Center.
- Verify the Version of vSphere Update Manager Download Service

  Verify the version of vSphere Update Manager Download Service (UMDS) after you perform an upgrade operation in the Software Defined Data Center.

Verify the Version of vRealize Operations Manager

Verify the version of the analytics and remote collector nodes of vRealize Operations Manager after you perform an upgrade operation in the Software Defined Data Center.

Procedure

1. Log in to vRealize Operations Manager by using the operations interface.
   a. Open a Web browser and go to **`https://vrops01svr01.rainpole.local`**.
   b. Log in using the following credentials.

Setting	Value
User name	admin
Password	*vrops_admin_password*

2. Click the **Administration** tab, and click **Management > Cluster Management**.
3. In the **Cluster Management** page, under the **Nodes in the vRealize Operations Manager Cluster** table, verify that the **Version** column has the expected version for each of the nodes.

Verify the Version of vRealize Log Insight

Verify the version of vRealize Log Insight nodes after you perform an upgrade operation in the Software Defined Data Center.

Procedure

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

a Open a Web browser and go to **`https://vrops01svr01.rainpole.local`**.

b Log in using the following credentials.

Setting	Value
User name	admin
Password	*vrops_admin_password*

2 Click the configuration drop-down menu  , and click **Administration**.

3 Verify the version of the vRealize Log Insight cluster nodes.

a Under **Management** in the navigator area, click **Cluster**.

b In the **Nodes** table, verify that the **Version** column shows the correct version number for each of the nodes.

4 Repeat the procedure and validate for the **`lax01vrli01.lax01.rainpole.local`** vRealize Log Insight instance.

Verify the Version of vSphere Update Manager Download Service

Verify the version of vSphere Update Manager Download Service (UMDS) after you perform an upgrade operation in the Software Defined Data Center.

Procedure

1 Log in to the UMDS virtual appliance by using a Secure Shell (SSH) client.

a Open an SSH connection to **`sfo01umds01.sfo01.rainpole.local`**.

b Log in using the following credentials.

Setting	Value
User Name	svc-umds
Password	*svc-umds_password*

2 Verify the version of vSphere Update Manager Download Service.

a Run the following command.

```
cat /var/lib/vmware-umds/version.txt
```

b Verify that the vSphere Update Manager Download Service is upgraded with the correct version number.

3 Verify the version of nginx and postgreSQL.

   a Run the following commands.

```
nginx –v
psql –V
```

   b Verify that the version of nginx and postgreSQL are correct.

4 Repeat the procedure and validate for the **`lax01umds01.lax01.rainpole.local`** vSphere Update Manager Download Service instance.

Version Verification of the Cloud Management Layer

After an upgrade of the cloud management layer, perform post upgrade verification to ensure that each component has been upgraded successfully.

Version verification of the cloud management layer involves the following components:

- vRealize Automation nodes
- vRealize Automation Windows nodes
- vRealize Business
- Verify the Version of vRealize Automation Appliance Nodes

  Verify the version of the vRealize Automation appliance nodes after you perform an upgrade operation in the Software Defined Data Center.
- Verify the Version of vRealize Automation Windows Nodes

  Verify the version of the vRealize Automation windows nodes after you perform an upgrade operation in the Software Defined Data Center.
- Verify the Version of vRealize Business Nodes

  Verify the version of the vRealize Business for Cloud instances after you perform an upgrade operation in the Software Defined Data Center.

Verify the Version of vRealize Automation Appliance Nodes

Verify the version of the vRealize Automation appliance nodes after you perform an upgrade operation in the Software Defined Data Center.

Procedure

1 Log in to the management interface of the vRealize Automation Appliance.

   a Open a Web browser and go to **`https://vra01svr01a.rainpole.local:5480`**.

   b Log in using the following credentials.

Setting	Value
User name	root
Password	*vra_appliance_root_password*

2 Verify the version of the vRealize Automation appliance.

   a In the appliance management console, click the **Update** tab and click the **Status** tab.

   b Verify that the **Appliance Version** parameter shows the correct version number.

3 Repeat the procedure for the **`vra01svr01b.rainpole.local`** vRealize Automation appliance.

Verify the Version of vRealize Automation Windows Nodes

Verify the version of the vRealize Automation windows nodes after you perform an upgrade operation in the Software Defined Data Center.

Procedure

1 Log in to the Windows virtual machines of the vRealize Automation component.

a Open a Remote Desktop Protocol (RDP) connection to each of the following vRealize Automation virtual machines.

vRealize Automation Component	FQDN	Program Names for Version Check
IaaS Web Server	■ `vra01iws01a.rainpole.local` ■ `vra01iws01b.rainpole.local`	■ VMware vCloud Automation Center Management Agent ■ VMware vCloud Automation Center Server ■ VMware vCloud Automation Center WAPI
IaaS Manager Service and DEM Orchestrator	■ `vra01ims01a.rainpole.local` ■ `vra01ims01b.rainpole.local`	■ VMware vCloud Automation Center DEM-Orchestrator - <*ims-fqdn*> DEO ■ VMware vCloud Automation Center Management Agent ■ VMware vCloud Automation Center Server
vRealize Automation DEM Worker	■ `vra01dem01a.rainpole.local` ■ `vra01dem01b.rainpole.local`	■ VMware vCloud Automation Center DEM-Worker - DEM-WORKER-*xx* ■ VMware vCloud Automation Center DEM-Worker - DEM-WORKER-*yy* ■ VMware vCloud Automation Center DEM-Worker - DEM-WORKER-*zz* ■ VMware vCloud Automation Center Management Agent
vRealize Automation Proxy Agents	■ `sfo01ias01a.sfo01.rainpole.local` ■ `sfo01ias01b.sfo01.rainpole.local` ■ `lax01ias01a.lax01.rainpole.local` ■ `lax01ias01b.lax01.rainpole.local`	■ VMware vCloud Automation Center Agents - vSphere-Agent-*xx* ■ VMware vCloud Automation Center Management Agent

b Log in using the following credentials.

Setting	Value
User name	Rainpole\svc-vra
Password	*svc-vra-user-password*

2 From the Windows **Start** menu, select **Control Panel > Programs and Features** and verify that the **Version** column shows the correct version number for the program names as per the table above.

Verify the Version of vRealize Business Nodes

Verify the version of the vRealize Business for Cloud instances after you perform an upgrade operation in the Software Defined Data Center.

Procedure

1 Log in to the management interface of the vRealize Business for Cloud Server virtual appliance.

   a Open a Web browser and go to **`https://vrb01svr01.rainpole.local:5480`**.

   b Log in using the following credentials.

Setting	Value
User name	root
Password	*vrb_server_root_password*

2 Verify the version of the vRealize Business for Cloud appliance.

   a In the appliance management console, click the **Update** tab and click the **Status** tab.

   b Verify that the **Appliance Version** parameter shows the correct version number.

3 Repeat the procedure for the **`sfo01vrbc01.sfo01.rainpole.local`** and **`lax01vrbc01.lax01.rainpole.local`** vRealize Business Collector nodes.

Version Verification of the Business Continuity Layer

After an upgrade of the business continuity layer, perform post upgrade verification to ensure that each component has been upgraded successfully.

Version verification of the cloud management layer involves the following components:

- Site Recovery Manager
- vSphere Replication
- Verify the Version of Site Recovery Manager

  Verify the version of the Site Recovery Manager instances after you perform an upgrade operation in the Software Defined Data Center.
- Verify the Version of vSphere Replication

  Verify the version of the vSphere Replication instances after you perform an upgrade operation in the Software Defined Data Center.

Verify the Version of Site Recovery Manager

Verify the version of the Site Recovery Manager instances after you perform an upgrade operation in the Software Defined Data Center.

Procedure

1 Log in to the Site Recovery Manager by using a Remote Desktop Protocol (RDP) client.

   a Open an RDP connection to the **`sfo01m01srm01.sfo01.rainpole.local`** virtual machine.

   b Log in using the following credentials.

Setting	Value
User name	Windows administrator user
Password	*windows_administrator_password*

2 Verify the version of Site Recovery Manager.

   a From the Windows **Start** menu, select **Control Panel > Programs and Features**.

   b Verify that the **Version** column shows the correct version number for the following programs.

   - VMware vCenter Site Recovery Manager
   - VMware vCenter Site Recovery Manager Embedded Database

3 Repeat the procedure for the **`lax01m01srm01.lax01.rainpole.local`** Site Recovery Manager instance.

Verify the Version of vSphere Replication

Verify the version of the vSphere Replication instances after you perform an upgrade operation in the Software Defined Data Center.

Procedure

1 Log in to the vSphere Replication appliance management interface.

   a Open a Web browser and go to **`https://sfo01m01vrms01.sfo01.rainpole.local:5480`**.

   b Log in using the following credentials.

Setting	Value
User name	root
Password	*vr_sfo_root_password*

2 Verify the version of the vSphere Replication appliance.

   a In the appliance management console, click the **Update** tab and click the **Status** tab.

   b Verify that the **Appliance Version** parameter shows the correct version number.

3 Repeat the procedure for the **`lax01m01vrms01.lax01.rainpole.local`** vSphere Replication instance.

SDDC Startup and Shutdown

6

When you perform patch, upgrade, recovery, or failover of the SDDC management applications, make sure that you start up and shut down the management virtual machines according to a predefined order.

- Shutdown Order of the Management Virtual Machines

  Shut down the virtual machines of the SDDC management stack by following a strict order to avoid data loss and faults in the components.

- Startup Order of the Management Virtual Machines

  Start up the virtual machines of the SDDC management stack by following a strict order to guarantee the faultless operation of and the integration between the components.

Shutdown Order of the Management Virtual Machines

Shut down the virtual machines of the SDDC management stack by following a strict order to avoid data loss and faults in the components.

Before you begin:

- Verify that virtual machines are not running on snapshots.
- Ensure verified backups of all management and tenant virtual machines are available.
- If a data protection solution is running on the management clusters, ensure that the solution is properly shutdown following the vendor guidance.
- If the hosts in a vSAN cluster are to be shut down, appropriately shut down the tenant workloads in the shared edge and compute cluster.

Shutting down the management virtual machines:

- Refer to VMware Knowledge Base article 2142676 for information on verifying the state of the vSAN cluster before a shutdown.
- Shut down the virtual machines of the SDDC management stack by following the shutdown order provided in the following table.

- Ensure that the console of the virtual machine and its services are fully shut down before moving to the next virtual machine.

Note The vCenter Server instances, NSX load balancers for the Platform Services Controllers, the Platform Services Controllers, and the management clusters are the last virtual machines to be shut down.

Virtual Machine Name in Region A	Virtual Machine Name in Region B	Shutdown Order
vRealize Log Insight **Total Number of VMs (3)**	**vRealize Log Insight** **Total Number of VMs (3)**	**1**
sfo01vrli01c	lax01vrli01c	1
sfo01vrli01b	lax01vrli01b	1
sfo01vrli01a	lax01vrli01a	2
vRealize Operations Manager **Total Number of VMs (5)**	**vRealize Operations Manager** **Total Number of VMs (2)**	**1**
sfo01vropsc01b	lax01vropsc01b	1
sfo01vropsc01a	lax01vropsc01a	1
vrops01svr01c	-	2
vrops01svr01b	-	3
vrops01svr01a	-	4
vRealize Business for Cloud **Total Number of VMs (2)**	**Realize Business for Cloud** **Total Number of VMs (2)**	**2**
sfo01vrbc01	lax01vrbc01	1
vrb01svr01	-	2
vRealize Automation **Total Number of VMs (11)**	**vRealize Automation** **Total Number of VMs (2)**	**3**
vra01dem01a	-	1
vra01dem01b	-	1
sfo01ias01b	lax01ias01b	1
sfo01ias01a	lax01ias01a	1
vra01ims01b	-	2
vra01ims01a	-	2
vra01iws01b	-	3
vra01iws01a	-	4
vra01svr01b	-	5
vra01svr01a	-	5
vra01mssql01	-	6
Site Recovery Manager and vSphere Replication **Total Number of VMs (2)**	**Site Recovery Manager and vSphere Replication** **Total Number of VMs (2)**	**4**

Virtual Machine Name in Region A	Virtual Machine Name in Region B	Shutdown Order
sfo01m01vrms01	lax01m01vrms01	1
sfo01m01srm01	lax01m01srm01	2
Update Manager Download Service (UMDS) **Total Number of VMs (1)**	**Update Manager Download Service (UMDS)** **Total Number of VMs (1)**	**4**
sfo01umds01	lax01umds01	1
Core Stack **Total Number of VMs (26)**	**Core Stack** **Total Number of VMs (16)**	**5**
sfo01m01lb01 (0,1)	lax01m01lb01 (0,1)	1
sfo01m01udlr01 (0,1)	-	1
sfo01m01esg01	lax01m01esg01	1
sfo01m01esg02	lax01m01esg02	1
sfo01w01udlr01 (0,1)	-	1
sfo01w01dlr01 (0,1)	lax01w01dlr01 (0,1)	1
sfo01w01esg01	lax01w01esg01	1
sfo01w01esg02	lax01w01esg02	1
sfo01m01nsx01	lax01m01nsx01	2
sfo01w01nsx01	lax01w01nsx01	2
sfo01m01nsxc01	-	3
sfo01m01nsxc02	-	3
sfo01m01nsxc03	-	3
sfo01w01nsxc01	-	3
sfo01w01nsxc02	-	3
sfo01w01nsxc03	-	3
sfo01m01vc01	lax01m01vc01	4
sfo01w01vc01	lax01w01vc01	4
sfo01psc01 (0,1)	lax01psc01 (0,1)	5
sfo01w01psc01	lax01w01psc01	6
sfo01m01psc01	lax01m01psc01	6

Shutting down the ESXi hosts in the vSAN clusters:

- Refer to VMware Knowledge Base article 2142676 for information on preparing and shutting down ESXi hosts in vSAN clusters.

Startup Order of the Management Virtual Machines

Start up the virtual machines of the SDDC management stack by following a strict order to guarantee the faultless operation of and the integration between the components.

Before you begin:

- Verify that external dependencies for the SDDC, such as, Active Directory, DNS, NTP, SMTP, and FTP/SFTP are available.

Starting up the ESXi hosts in the vSAN clusters:

- If the vSAN clusters have been shut down, refer to VMware Knowledge Base article 2142676 for information on starting up hosts and exiting maintenance mode.

Starting up the management virtual machines:

- Start up the virtual machines by following the startup order provides in the following table.
- Ensure that the console of the virtual machine and its services are all up before proceeding with the next virtual machine.
- Refer to VMware Knowledge Base article 2142676 for information on checking the health of the vSAN clusters before starting up tenant workloads.
- If a data protection solution is deployed on the management cluster, ensure that the solution is properly started and operational, following the vendor guidance.

Virtual Machine in Region A	Virtual Machine in Region B	Startup Order
Core Stack Total Number of VMs (26)	**Core Stack Total Number of VMs (16)**	**1**
sfo01m01psc01	lax01m01psc01	1
sfo01w01psc01	lax01w01psc01	1
sfo01psc01 (0,1)	lax01psc01 (0,1)	2
sfo01m01vc01	lax01m01vc01	3
sfo01w01vc01	lax01w01vc01	3
sfo01m01nsx01	lax01m01nsx01	4
sfo01w01nsx01	lax01w01nsx01	4
sfo01m01nsxc01	-	5
sfo01m01nsxc02	-	5
sfo01m01nsxc03	-	5
sfo01w01nsxc01	-	5
sfo01w01nsxc02	-	5
sfo01w01nsxc03	-	5
sfo01m01lb01 (0,1)	lax01m01lb01 (0,1)	6
sfo01m01udlr01 (0,1)	-	6
sfo01m01esg01	lax01m01esg01	6
sfo01m01esg02	lax01m01esg02	6
sfo01w01udlr01 (0,1)	-	6
sfo01w01dlr01 (0,1)	lax01w01dlr01(0,1)	6

Virtual Machine in Region A	Virtual Machine in Region B	Startup Order
sfo01w01esg01	lax01w01esg01	6
sfo01w01esg02	lax01w01esg02	6
Update Manager Download Service (UMDS) **Total Number of VMs (1)**	**Update Manager Download Service (UMDS)** **Total Number of VMs (1)**	**2**
sfo01umds01	lax01umds01	1
Site Recovery Manager and vSphere Replication **Total Number of VMs (2)**	**Site Recovery Manager and vSphere Replication** **Total Number of VMs (2)**	**2**
sfo01m01vrms01	lax01m01vrms01	1
sfo01m01srm01	lax01m01srm01	1
vRealize Automation **Total Number of VMs (11)**	**vRealize Automation** **Total Number of VMs (2)**	**3**
vra01mssql01	-	1
vra01svr01a	-	2
vra01svr01b	-	2
vra01iws01a	-	3
vra01iws01b	-	4
vra01ims01a	-	5
vra01ims01b	-	6
sfo01ias01a	lax01ias01a	7
sfo01ias01b	lax01ias01b	7
vra01dem01a	-	7
vra01dem01b	-	7
vRealize Business for Cloud **Total Number of VMs (2)**	**vRealize Business for Cloud** **Total Number of VMs (1)**	**4**
vrb01svr01	-	1
sfo01vrbc01	lax01vrbc01	2
vRealize Operations **Manager Total Number of VMs (5)**	**vRealize Operations Manager** **Total Number of VMs (2)**	**5**
vrops01svr01a	-	1
vrops01svr01b	-	2
vrops01svr01c	-	3
sfo01vropsc01a	lax01vropsc01a	4
sfo01vropsc01b	lax01vropsc01b	4
vRealize Log Insight **Total Number of VMs (3)**	**vRealize Log Insight** **Total Number of VMs (3)**	**5**
sfo01vrli01a	lax01vrli01a	1

Virtual Machine in Region A	Virtual Machine in Region B	Startup Order
sfo01vrli01b	lax01vrli01b	2
sfo01vrli01c	lax01vrli01c	2