Deployment for Consolidated SDDC

02 APR 2019

VMware Validated Design 5.0

VMware Validated Design for Management and Workload Consolidation 5.0

vmware®

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

https://docs.vmware.com/

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

docfeedback@vmware.com

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

Contents

About VMware Validated Design Deployment for Consolidated SDDC

1

VMware Validated Design Deployment for Management and Workload Consolidation (also referred to as VMware Validated Design for Consolidated SDDC) provides step-by-step instructions for installing, configuring, and operating a Software-Defined Data Center (SDDC) based on VMware Validated Design, and usingVMware Cloud Builder to automate the implementation of this Validated Design.

VMware Validated Design Deployment for Management and Workload Consolidation does not contain step-by-step instructions for performing all the required post-configuration tasks because their nature often depends on the requirements of your organization.

Intended Audience

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

Required VMware Software

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

Before You Apply This Guidance

The sequence of the documentation of VMware Validated Design follows the stages for implementing and maintaining an SDDC. See Documentation Map for VMware Validated Design.

To use *VMware Validated Design Deployment for Management and Workload Consolidation*, you must be acquainted with the following guidance:

- *Introducing VMware Validated Designs*
- Optionally *VMware Validated Design Architecture and Design for Consolidated SDDC*
- *VMware Validated Design Planning and Preparation for Consolidated SDDC*

Prepare the Environment for Automated Deployment for Consolidated SDDC

2

Before you start the automated deployment of VMware Validated Design for Software-Defined Data Center using VMware Cloud Builder, your environment must meet target prerequisites and be in a specific starting state. Prepare each layer of the SDDC by deploying and configuring the necessary infrastructure, operational, and management components.

- Prerequisites for Virtual Infrastructure Layer Implementation for Consolidated SDDC

  To prepare the virtual infrastructure layer of the SDDC, you first install ESXi on all hosts for the consolidated cluster, configure the management network, DNS, NTP, and SSH services.

- Prerequisites for Operations Management Layer Implementation for Consolidated SDDC

  To prepare the operations management layer for automated deployment of the SDDC components using Cloud Builder, you deploy and configure a Linux virtual machine for vSphere Update Manager Download Service.

- Prerequisites for Cloud Management Layer Implementation for Consolidated SDDC

  To prepare the cloud management layer for automated deployment of the SDDC components using Cloud Builder, you deploy and configure the Master Windows system for vRealize Automation Infrastructure as a Service (IaaS) nodes and deploy and configure the external SQL server for vRealize Automation.

- Generate Certificates for the SDDC Components for Consolidated SDDC

  To ensure secure and operational connectivity between the SDDC components, you generate new signed certificates for the SDDC components.

Prerequisites for Virtual Infrastructure Layer Implementation for Consolidated SDDC

To prepare the virtual infrastructure layer of the SDDC, you first install ESXi on all hosts for the consolidated cluster, configure the management network, DNS, NTP, and SSH services.

Procedure

1. Prerequisites for Installation of ESXi Hosts for Consolidated SDDC

   Install and configure the ESXi hosts for your workload and management consolidation deployment.

2. Install ESXi Interactively on All Hosts for Consolidated SDDC

   Install ESXi on all hosts in the consolidated cluster interactively.

3 Configure the Network on all Hosts for Consolidated SDDC

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

4 Configure the Virtual Machine Network Port Group on All Hosts for Consolidated SDDC

You perform network configuration for each ESXi host using the VMware Host Client.

5 Configure SSH and NTP on All Hosts for Consolidated SDDC

Complete the initial configuration of all ESXi hosts by enabling the TSM-SSH service. You then configure the NTP service to avoid time synchronization issues in the SDDC.

6 Mount NFS Storage on All ESXi Hosts for Consolidated SDDC

This VMware Validated Design uses NFS storage as secondary storage for the SDDC components. You mount the NFS storage to provide storage capacity for archiving log data, backup, and application templates.

Prerequisites for Installation of ESXi Hosts for Consolidated SDDC

Install and configure the ESXi hosts for your workload and management consolidation deployment.

Before you start:

- Make sure that you have a Windows host that has access to your data center. You use this host to connect to the data center and perform configuration steps.

You must also prepare the installation files.

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

IP Addresses, Hostnames, and Network Configuration

The following values are required to configure your hosts.

Table 2-1. Hosts for the Consolidated SDDC

FQDN	IP	VLAN ID	Default Gateway	NTP Server
sfo01w01esx01.sfo01.rainpole.local	172.16.31.101	1631	172.16.31.253	ntp.sfo01.rainpole.local
sfo01w01esx02.sfo01.rainpole.local	172.16.31.102	1631	172.16.31.253	ntp.sfo01.rainpole.local
sfo01w01esx03.sfo01.rainpole.local	172.16.31.103	1631	172.16.31.253	ntp.sfo01.rainpole.local
sfo01w01esx04.sfo01.rainpole.local	172.16.31.104	1631	172.16.31.253	ntp.sfo01.rainpole.local

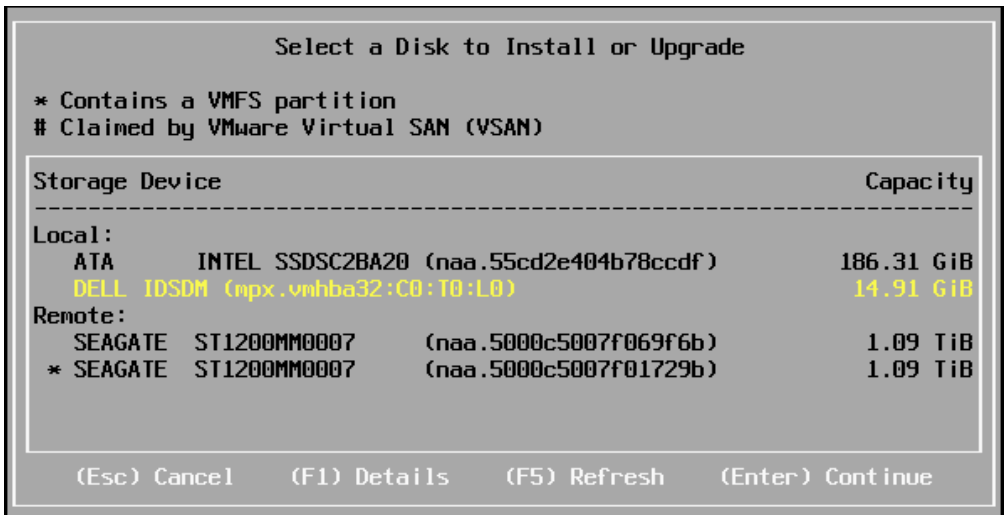
Install ESXi Interactively on All Hosts for Consolidated SDDC

Install ESXi on all hosts in the consolidated cluster interactively.

Repeat this procedure for all hosts in the consolidated cluster. Enter the respective values from the prerequisites section for each host that you configure. See Prerequisites for Installation of ESXi Hosts for Consolidated SDDC.

Procedure

1. Power on the **sfo01w01esx01** host.
2. Mount the USB drive containing the ESXi ISO file and boot from that USB drive.
3. On the **Welcome to the VMware 6.7 U1 Installation** screen, press Enter to start the installation.
4. On the **End User License Agreement (EULA)** screen, press F11 to accept the EULA.
5. On the **Select a Disk to Install or Upgrade** screen, select the USB drive under local storage to install ESXi and press Enter to continue.



6. Select the keyboard layout and press Enter.
7. Enter the ***esxi_root_user_password***, enter the password a second time to confirm the spelling and press Enter.
8. On the **Confirm Install** screen, press F11 to start the installation.
9. After the installation completes successfully, unmount the USB drive and press Enter to reboot the host.

Configure the Network on all Hosts for Consolidated SDDC

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

Perform the following tasks to configure the host network settings:

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

Repeat this procedure for all hosts in the consolidated cluster. Enter the respective values from the prerequisites section for each host that you configure. See Prerequisites for Installation of ESXi Hosts for Consolidated SDDC.

Procedure

1 Open the DCUI on the **sfo01w01esx01.sfo01.rainpole.local** ESXi host.

   a Open a console window to the host.

   b Press F2 to enter the DCUI.

   c Log in using the following credentials.

Setting	Value
User name	root
Password	*esxi_root_user_password*

2 Configure the network.

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

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

   c Enter **1631** as the VLAN ID for the Management Network and press Enter.

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

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

Setting	Value
Set static IPv4 address and network configuration	Selected
IPv4 Address	172.16.31.101
Subnet Mask	255.255.255.0
Default Gateway	172.16.31.253

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

   g Configure DNS using the following settings and press Enter.

Setting	Value
Use the following DNS Server address and hostname	Selected
Primary DNS Server	172.16.11.5
Alternate DNS Server	172.16.11.4
Hostname	sfo01w01esx01.sfo01.rainpole.local

   h Select **Custom DNS Suffixes** and press Enter.

   i Ensure that there are no suffixes listed and press Enter.

3 Press Escape to exit and press Y to confirm the changes.

Configure the Virtual Machine Network Port Group on All Hosts for Consolidated SDDC

You perform network configuration for each ESXi host using the VMware Host Client.

You configure the VLAN ID of the VM Network portgroup on the vSphere Standard Switch. This configuration provides connectivity and common network configuration for virtual machines that reside on each host.

You repeat this procedure for all hosts in the consolidated cluster with the following VLAN IDs.

Table 2-2. Default VM Network Port Group for the Consolidated Cluster

Host	VLAND ID
sfo01w01esx01.sfo01.rainpole.local	1611
sfo01w01esx02.sfo01.rainpole.local	1611
sfo01w01esx03.sfo01.rainpole.local	1611
sfo01w01esx04.sfo01.rainpole.local	1611

Procedure

1 Log in to the vSphere host by using the VMware Host Client.

   a Open a Web browser and go to **`https://sfo01w01esx01.sfo01.rainpole.local`**.

   b Log in by using the following credentials.

Setting	Value
User name	root
Password	*esxi_root_user_password*

2 To join the Customer Experience Improvement Program, click **OK**.

3 Configure a VLAN for the VM Network port group.

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

   b Click the **Port Groups** tab, select the **VM Network** port group, and click **Edit Settings**.

   c On the **Edit port group - VM Network** window, enter **1611** for **VLAN ID**, and click **Save**.

Configure SSH and NTP on All Hosts for Consolidated SDDC

Complete the initial configuration of all ESXi hosts by enabling the TSM-SSH service. You then configure the NTP service to avoid time synchronization issues in the SDDC.

Repeat this procedure for all hosts in the consolidated cluster. See Prerequisites for Installation of ESXi Hosts for Consolidated SDDC.

Procedure

1 Log in to the vSphere host by using the VMware Host Client.

   a Open a Web browser and go to **`https://sfo01w01esx01.sfo01.rainpole.local`**.

   b Log in by using the following credentials.

Setting	Value
User name	root
Password	*esxi_root_user_password*

2 Configure and start the TSM-SSH service.

   a In the **Navigator**, click **Manage** and click the **Services** tab.

   b Select the **TSM-SSH** service, and click the **Actions** menu.

   c Select **Policy** and click **Start and stop with host**.

   d Click **Start** to start the service.

3 Configure and start the NTP service.

   a In the **Navigator**, click **Manage**, and click the **System** tab.

   b Click **Time & date** and click **Edit Settings**.

   c In the **Edit time configuration** dialog box, select the **Use Network Time Protocol (enable NTP client)** radio button, change the NTP service startup policy to **Start and stop with host**.

   d In the **NTP servers** text box, enter **`ntp.sfo01.rainpole.local, ntp.rainpole.local`**, and click **Save**.

   e Start the service by clicking **Actions**, select **NTP service**, and click **Start**.

Mount NFS Storage on All ESXi Hosts for Consolidated SDDC

This VMware Validated Design uses NFS storage as secondary storage for the SDDC components. You mount the NFS storage to provide storage capacity for archiving log data, backup, and application templates.

Repeat this procedure for all hosts in the consolidated cluster. See Prerequisites for Installation of ESXi Hosts for Consolidated SDDC.

Prerequisites

Verify that you have allocated static IP addresses for each ESXi VMkernel storage port.

Procedure

1 Log in to the vSphere host by using the VMware Host Client.

a Open a Web browser and go to **`https://sfo01w01esx01.sfo01.rainpole.local`**.

b Log in by using the following credentials.

Setting	Value
User name	root
Password	*esxi_root_user_password*

2 Configure the Maximum Transmission Units (MTU) on the standard virtual switch.

a In the **Navigator**, select **Networking > Virtual switches > vSwitch0 > Edit**.

b In the **Edit standard virtual switch** dialog box, enter the following values, and click **Save**.

Setting	Value
MTU	9000
Uplink1	vmnic0

3 Configure a VMkernel storage port on all ESXi hosts.

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

b Select the **VMkernel NICs** tab and click **Add VMkernel NIC**.

c In the **Add VMkernel NIC** dialog box, enter the following values, and click **Create**.

Setting	Value
Port Group	New port group
New Port Group	Storage
Virtual Switch	vSwitch0
VLAN ID	1625
MTU	9000
IP version	IPv4 only
IPv4 settings	Static
Address	172.16.25.101
Subnet mask	255.255.255.0
TCP/IP stack	Default TCP/IP stack
Services	Deselected

4 Mount the NFS datastore on the ESXi host.

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

b Click the **Datastores** tab and click the **New datastore** button.

The **New Datastore** dialog box appears.

c On the **Select creation type** dialog box, select **Mount NFS datastore** and click **Next**.

d On the **Provide NFS mount details** dialog box, enter the following values, and click **Next**.

Setting	Value
Name	sfo01-w01-bkp01
NFS Server	172.16.25.251
NFS Share	/VVD_backup01_nfs01_Consolidated_6TB
NFS Version	NFS 3

e On the **Ready to complete** dialogue box, click **Finish**.

Prerequisites for Operations Management Layer Implementation for Consolidated SDDC

To prepare the operations management layer for automated deployment of the SDDC components using Cloud Builder, you deploy and configure a Linux virtual machine for vSphere Update Manager Download Service.

Deploy and Configure a Linux Virtual Machine for vSphere Update Manager Download Service for Consolidated SDDC

Before you deploy vSphere Update Manager Download Service with Cloud Builder, you deploy and configure a virtual machine with an Ubuntu Server operating system.

You create a virtual machine on the sfo01w01esx01.sfo01.rainpole.local host for vSphere Update Manager Download Service with the following virtual machine and network configuration requirements. Ensure that the virtual machine has access to the Internet.

Table 2-3. Virtual Machine Requirements for the vSphere Update Manager Download Service Linux VM

Setting	Value
ESXi Host	sfo01w01esx01
VM Name	sfo01umds01
Guest OS	Ubuntu Server 18.04 LTS
CPU	2
Memory	2 GB
Hard Disk	120 GB

Table 2-3. Virtual Machine Requirements for the vSphere Update Manager Download Service Linux VM (Continued)

Setting	Value
SCSI Controller	LSI Logic SAS
Network Interface	VM Network
Network Adapter Type	VMXNET3
Datastore	sfo01-w01-bkp01

Table 2-4. Network Requirements for the vSphere Update Manager Download Service Linux VM

Setting	Value
Host Name	sfo01umds01
Static IPv4 Address	172.16.11.67
Default Gateway	172.16.11.253
Subnet Mask	255.255.255.0
DNS Server	172.16.11.5, 172.16.11.4
DNS Domain	sfo01.rainpole.local
DNS Search	sfo01.rainpole.local

Procedure

1 Deploy the vSphere Update Manager Download Service Linux VM with the specified configuration.

2 Log in to the vSphere host by using the VMware Host Client.

   a Open a Web browser and go to **`https://sfo01w01esx01.sfo01.rainpole.local`**.

   b Log in by using the following credentials.

Setting	Value
User name	root
Password	*esxi_root_user_password*

3 In the **Navigator**, click **Virtual Machines**.

4 Select the **sfo01umds01** virtual machine, click the **Console** button, and select **Open browser console**.

5 Create the **svc-umds** service account for vSphere Update Manager Download Service by running the following command.

```
adduser svc-umds
```

When prompted, enter and confirm the password, and provide the **svc-umds** full user name.

6 Assign administrative privileges to the **svc-umds** service account by running the following command.

```
usermod –aG sudo svc–umds
```

7 Install Secure Shell (SSH) server by running the following command.

```
sudo apt–get update
sudo apt–get –y install ssh
```

8 Verify the status of SSH service by running the following command.

```
service ssh status
```

9 Install `Expect` and `Nginx` packages for Ubuntu by running the following commands.

```
sudo apt–get install –y expect
sudo apt–get install –y nginx
```

Prerequisites for Cloud Management Layer Implementation for Consolidated SDDC

To prepare the cloud management layer for automated deployment of the SDDC components using Cloud Builder, you deploy and configure the Master Windows system for vRealize Automation Infrastructure as a Service (IaaS) nodes and deploy and configure the external SQL server for vRealize Automation.

Procedure

1 Deploy and Configure the Master Windows System for vRealize Automation IaaS Nodes for Consolidated SDDC

You deploy and configure a single Master Windows system virtual machine which is cloned and reconfigured during SDDC deployment to provision the vRealize Automation IaaS components - IaaS Web Server and IaaS Manager Service Server.

2 Deploy and Configure the External SQL Server for vRealize Automation for Consolidated SDDC

You deploy and configure a Windows-based virtual machine to host the SQL Server database required for the vRealize Automation IaaS components. After you install the SQL instance, you perform additional configuration to allow Cloud Builder to perform initial validation and deploy the necessary vRealize Automation components.

Deploy and Configure the Master Windows System for vRealize Automation IaaS Nodes for Consolidated SDDC

You deploy and configure a single Master Windows system virtual machine which is cloned and reconfigured during SDDC deployment to provision the vRealize Automation IaaS components - IaaS Web Server and IaaS Manager Service Server.

You create a virtual machine on the sfo01w01esx01.sfo01.rainpole.local host for the Master Windows system with the following virtual machine, software, and network configuration.

Table 2-5. Virtual Machine Requirements for the Master Windows System

Setting	Value
ESXi Host	sfo01w01esx01
VM Name	master-iaas-vm
Guest OS	Microsoft Windows Server 2016 (64-bit)
vCPU	2
Memory	8 GB
Virtual Disk	60 GB
SCSI Controller	LSI Logic SAS
Datastore	sfo01-w01-bkp01
Network Interface	VM Network
Network Adapter Type	1 x VMXNET3

Network Requirements:

- Verify that you have allocated a static or DHCP IP address for the Master Windows system.
- Verify the Master Windows system has access to the Internet.

Table 2-6. Software Requirements for the Master Windows System

Component	Requirement
Operating System	Windows Server 2016 (64-bit)
VMware Tools	Latest version
Active Directory	Join the virtual machine to the sfo01.rainpole.local domain.
Internet Explorer Enhanced Security Configuration	Turn off ESC.
Remote Desktop Protocol	Enable RDP access.
Java	■ Java Runtime Environment (JRE) executable jre-8u191-windows-x64 or later. ■ Set the *JAVA_HOME* environment variable to the Java installation directory. ■ Update the *PATH* system variable to include the `bin` folder of Java installation directory.
Secondary Logon Service	Start Secondary Logon service and set start-up type to Automatic.

Procedure

1 Deploy the Master Windows System for vRealize Automation with the specified configuration.

2 Log in to the vRealize Automation Master Windows virtual machine by using a Remote Desktop Protocol (RDP) client.

   a Open an RDP connection to the virtual machine.

   b Log in by using the following credentials.

Settings	Value
User name	Windows administrator user
Password	*windows_administrator_password*

3 Click **Start**, right-click **Windows PowerShell**, and select **More > Run as Administrator**.

4 Set the execution policy by running the following command.

```
Set-ExecutionPolicy Unrestricted
```

   When prompted, confirm the execution policy change.

5 Disable User Account Control (UAC) by running the following command.

```
set-ItemProperty -Path "HKLM:\Software\Microsoft\Windows\CurrentVersion\Policies\System" -Name
"EnableLUA" -Value "0"
```

6 Disable IPv6 protocol.

```
set-ItemProperty -Path "HKLM:\System\CurrentControlSet\Services\TCPIP6\Parameters" -Name
"DisabledComponents" -Value 0xff
```

7 Verify that the source path for Microsoft Windows Server is available.

   a Mount the Microsoft Windows Server ISO file on the Master Windows system virtual machine.

   b Create the `\sources\sxs` directory by running the following command in Windows PowerShell.

```
mkdir C:\sources\sxs
```

   c Copy the Microsoft Windows Server source files from `sources\sxs` on the ISO file to the `C:\sources\sxs` directory on the virtual machine.

   d Update the registry with the full system path of the Microsoft Windows Server source files by running the following command in Windows PowerShell.

```
New-Item -Path "HKLM:\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\Servicing"
```

```
set-ItemProperty -Path "HKLM:\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\Servicing\" -
Name "LocalSourcePath" -value "c:\sources\sxs"
```

   e Unmount the Microsoft Windows Server ISO file.

8 Add the **svc-vra** service account to the Local Administrators group.

   a Click **Start**, right-click **Windows PowerShell**, and select **More > Run as Administrator**.

   b Run the following command.

```
net localgroup administrators rainpole\svc-vra /add
```

9 Create the **svc-vra** user profile by logging in to the vRealize Automation Master Windows virtual machine.

   a Open an RDP connection to the virtual machine.

   b Log in using the following credentials.

Settings	Value
User name	rainpole\svc-vra
Password	*svc-vra_password*

10 Shut down the Master Windows system virtual machine.

Deploy and Configure the External SQL Server for vRealize Automation for Consolidated SDDC

You deploy and configure a Windows-based virtual machine to host the SQL Server database required for the vRealize Automation IaaS components. After you install the SQL instance, you perform additional configuration to allow Cloud Builder to perform initial validation and deploy the necessary vRealize Automation components.

You create a virtual machine on the sfo01w01esx01.sfo01.rainpole.local host for the Microsoft SQL Server with the following virtual machine, software, and network configuration requirements.

Table 2-7. Virtual Machine Requirements for the External vRealize Automation SQL Server

Setting	Value
ESXi Host	sfo01w01esx01
VM Name	vra01mssql01
Guest OS	Microsoft Windows Server 2016 (64-bit)
vCPU	8
Memory (GB)	16
Hard Disk (GB)	200
SCSI Controller	LSI Logic SAS
Datastore	sfo01-w01-bkp01
Network Interface	VM Network
Network Adapter Type	1 x VMXNET3

Table 2-8. Network Requirements for the External vRealize Automation SQL Server

Setting	Value
Host Name	vra01mssql01
Static IPv4 Address	172.16.11.72
Subnet Mask	255.255.255.0
Default Gateway	172.16.11.253
DNS Server	172.16.11.5
FQDN	vra01mssql01.rainpole.local

Table 2-9. Software Requirements for the External vRealize Automation SQL Server

Component	Requirement
Operating System	Windows Server 2016 (64-bit)
VMware Tools	Latest version
SQL Server	SQL Server 2017 Standard or later (64-bit) Microsoft SQL Server Management Studio **Important** During the SQL Server installation, the Database Engine configuration wizard prompts you to provide the user name and password for the SQL Server administrator. If this user is not added during the SQL Server installation, select **SQL Authentication** from the **Authentication** drop-down menu, enter **sa** in the **User name** text box, and *sa_password* in the **Password** text box.
Active Directory	Join the virtual machine to the rainpole.local domain.
Remote Desktop Protocol	Enable RDP access.

Procedure

1. Deploy the External vRealize Automation SQL Server VM with the specified configuration.
2. Log in to the SQL Server virtual machine by using a Remote Desktop Protocol (RDP) client.
   a. Open an RDP connection to the **`vra01mssql01.rainpole.local`** virtual machine.
   b. Log in by using the following credentials.

Settings	Value
User name	Windows administrator user
Password	*windows_administrator_password*

3 Enable Microsoft Distributed Transaction Coordinator (MSDTC).

   a Click the Windows **Start** button, type **`comexp.msc`**, and press Enter.

     The **Component Services** window opens.

   b In the **Console Root** on the left pane, navigate to **Component Services > Computers > My Computer > Distributed Transaction Coordinator**.

   c Right-click **Local DTC** and select **Properties**.

   d In the **Local DTC Properties** dialog box, click the **Security** tab, configure the following values, and click **OK**.

Setting	Value
Network DTC Access	Selected
Allow Remote Clients	Selected
Allow Inbound	Selected
Allow Outbound	Selected

   e In the **MSDTC Service** dialog box, select **Yes** to restart the MSDTC service.

4 Create the vRealize Automation account in the SQL Server instance.

   a Click the Windows **Start** button and open Microsoft SQL Server Management Studio.

   b In the **Connect to Server** dialog box, leave the default value for the **Server Name** text box, from the drop-down menu select **Windows Authentication**, and click **Connect**.

   c In the **Object Explorer** tree, expand the **VRA01MSSQL01** server instance, right-click the **Security** folder, and select **New > Login**.

   d In the **Login** dialog box, under **General**, enter **`rainpole\svc-vra`** in the **Login name** text box.

   e On the **Server Roles** page, select **sysadmin** and click **OK**.

5 Create the new vRealize Automation database.

   a Click the Windows **Start** button and open Microsoft SQL Server Management Studio.

   b Right-click the **Databases** folder and select **New Database**.

     The **New Database** wizard appears.

c In the **General** page, enter **VRADB01** for **Database name** and **rainpole\svc-vra** for **Owner**.

d On the **Options**page, configure the following recovery model settings, and click **OK**.

Setting	Value
Recovery model	Simple
Compatibility level	SQL Server 2014 (120)
Other options > Miscellaneous > Allow Snapshot Isolation	True
Other options > Miscellaneous > Is Read Committed Snapshot On	True

6 Allow access to Microsoft SQL Server on TCP port 1433.

a Click the Windows **Start** button, type **WF.msc**, and press Enter.

The **Windows Firewall with Advanced Security** window appears.

b In the navigation pane, right-click **Inbound Rules** and select **New Rule**.

The **New Inbound Rule Wizard** appears.

c On the **Rule Type** page, select the **Port** radio button, and click **Next**.

d On the **Protocol and Ports** page, select **TCP**, enter the port number **1433** in the **Specific local ports** text box, and click **Next**.

e On the **Action** page, select **Allow the connection**, and click **Next**.

f On the **Profile** page, select the **Domain**, **Private**, and **Public** profiles, and click **Next**.

g On the **Name** page, enter **Microsoft SQL Server Port (1433)** and click **Finish**.

7 Allow access for Microsoft Distributed Transaction Coordinator.

a Click the Windows **Start** button, type **WF.msc** and press Enter.

The **Windows Firewall with Advanced Security** window appears.

b In the navigation pane, select **Inbound Rules > New RuleInbound Rules**.

The **New Inbound Rule Wizard** appears.

c On the **Rule Type** page, click the **Predefined** radio button, select **Distributed Transaction Coordinator**, and click **Next**.

d On the **Predefined Rules** page, select all rules for **Distributed Transaction Coordinator (RPC-EPMAP)**, **Distributed Transaction Coordinator (RPC)**, and **Distributed Transaction Coordinator (TCP-In)**, and click **Next**.

e On the **Action** page, select **Allow the connection**, and click **Finish**.

8 Unmount any ISO files mounted to the virtual machine.

Generate Certificates for the SDDC Components for Consolidated SDDC

To ensure secure and operational connectivity between the SDDC components, you generate new signed certificates for the SDDC components.

You use the Certificate Generation Utility for VMware Validated Design (`CertGenVVD`) to generate the certificate configuration files based on the deployment specification configured in the Deployment Parameters XLS file. You then generate new certificates signed by the Microsoft certificate authority (MSCA) for all management products.

You later upload the newly generated and signed certificates to VMware Cloud Builder as part of the deployment and configuration procedure of the virtual appliance.

For information about the VMware Validated Design Certificate Generation Utility, see VMware Knowledge Base article 2146215 and *VMware Validated Design Planning and Preparation for Consolidated SDDC*.

Procedure

1 Prerequisites for Generating Signed Certificates for the SDDC Components for Consolidated SDDC

Before you generate MSCA signed certificates for the SDDC components, verify that your environment fulfills the requirements for this process.

2 Create and Add a Microsoft Certificate Authority Template for Consolidated SDDC

You first set up a Microsoft Certificate Authority template on the Active Directory (AD) servers. The template contains the certificate authority (CA) attributes for signing certificates for the SDDC components. After you create the template, you add it to the certificate templates of the Microsoft CA.

3 Generate Signed Certificates for the SDDC Components for Consolidated SDDC

Use the Certificate Generation Utility for VMware Validated Design (`CertGenVVD`) to generate new signed certificates for the SDDC components.

Prerequisites for Generating Signed Certificates for the SDDC Components for Consolidated SDDC

Before you generate MSCA signed certificates for the SDDC components, verify that your environment fulfills the requirements for this process.

This VMware Validated Design sets the Certificate Authority service on the Active Directory (AD) dc01rpl.rainpole.local (root CA) server. Verify that your environment satisfies the following prerequisites generating signed certificates for the components of the SDDC.

Certificate Generation Prerequisites

Prerequisite	Value
Active Directory	■ Verify that the Certificate Authority Service role and the Certificate Authority Web Enrollment role are installed and configured on the Active Directory Server. ■ Verify that a new Microsoft Certificate Authority template is created and enabled. ■ Use a hashing algorithm of SHA-256 or higher on the certificate authority. ■ Verify that relevant firewall ports relating to the Microsoft Certificate Authority and related services are open.
Windows Host	■ Ensure the Windows host system where you connect to the data center and generate the certificates is joined to the domain of the Microsoft Certificate Authority. ■ Install Java Runtime Environment version 1.8 or later. ■ Configure the *JAVA_HOME* environment variable to the Java installation directory. ■ Update the *PATH* system variable to include the `bin` folder of Java installation directory. ■ Install OpenSSL toolkit version 1.0.2 for Windows. ■ Update the *PATH* system variable to include the `bin` folder of the OpenSSL installation directory.
Software Features	■ Fill in the Deployment Parameters XLS file for Consolidated SDDC. See Deployment Specification in the *VMware Validated Design Planning and Preparation for Consolidated SDDC* documentation.
Installation Packages	■ Download the `CertGenVVD-`*`version`*`.zip` file of the Certificate Generation Utility from VMware Knowledge Base article 2146215 and extract the ZIP file to the `C:` drive.

Create and Add a Microsoft Certificate Authority Template for Consolidated SDDC

You first set up a Microsoft Certificate Authority template on the Active Directory (AD) servers. The template contains the certificate authority (CA) attributes for signing certificates for the SDDC components. After you create the template, you add it to the certificate templates of the Microsoft CA.

Procedure

1 Log in to the Active Directory server using a Remote Desktop Protocol (RDP) client.

   a Log in using the following credentials.

Setting	Value
User	Active Directory administrator
Password	*ad_admin_password*

2 Click **Start > Run**, enter **`certtmpl.msc`**, and click **OK**.

3 In the **Certificate Template Console**, under **Template Display Name**, right-click **Web Server** and select **Duplicate Template**.

4 In the **Duplicate Template** dialog box, leave **Windows Server 2003 Enterprise** selected for backward compatibility and click **OK**.

5 In the **Properties of New Template** dialog box, click the **General** tab.

6 In the **Template display name** text box, enter **VMware**.

7 Click the **Extensions** tab and configure the following.

   a Select **Application Policies** and click **Edit**.

   b Select **Server Authentication**, click **Remove**, and click **OK**.

   c If the **Client Authentication** policy is present, select it, click **Remove**, and click **OK**.

   d Select **Key Usage** and click **Edit**.

   e Select the **Signature is proof of origin (nonrepudiation)** check box.

   f Leave the default for all other options.

   g Click **OK**.

8 Click the **Subject Name** tab, ensure that the **Supply in the request** option is selected, and click **OK** to save the template.

9 Add the new template to the certificate templates of the Microsoft CA.

   a Click **Start > Run**, enter **certsrv.msc**, and click **OK**

   b In the **Certification Authority** window, expand the left pane, right-click **Certificate Templates**, and select **New > Certificate Template to Issue**.

   c In the **Enable Certificate Templates** dialog box, select **VMware**, and click **OK**.

Generate Signed Certificates for the SDDC Components for Consolidated SDDC

Use the Certificate Generation Utility for VMware Validated Design (CertGenVVD) to generate new signed certificates for the SDDC components.

Procedure

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

2 Set the execution policy to Unrestricted.

   a Click **Start**, right click **Windows PowerShell**, and select **More > Run as Administrator**.

   b Set the execution policy by running the following command.

```
Set-ExecutionPolicy Unrestricted
```

   c Enter **Y** to confirm the execution policy change.

3 Use the CertConfig utility to generate the certificate configuration files.

   a Open the populated Deployment Parameters XLS file and select the **CertConfig** worksheet.

   b From the **File** menu, select **Save As…**, set the file format to **Comma delimited (*.csv)**, rename the file to **SDDC-CertConfig.csv**, and click **Save**.

c Rename the `C:\CertGenVVD-version\ConfigFiles` folder to `ConfigFiles.Old`.

d Create a new `C:\CertGenVVD-version\ConfigFiles` folder.

e In the Windows PowerShell terminal, navigate to the `C:\CertGenVVD-version` folder and run the following command.

```
.\Certconfig-version.ps1 SDDC-Certconfig.csv
```

f Follow the on-screen instructions and set the following values.

Setting	Value
Default Organization	Rainpole Inc
Default OU	Rainpole
Default Location	SFO
Default State	CA
Default Country	US
Default Key Size	2048

g Verify that the `C:\CertGenVVD-version\ConfigFiles` folder is populated with the necessary certificate configuration files.

- sfo01w01vc01.txt
- sfo01w01psc01.txt
- sfo01w01nsx01.txt
- vrops01svr01.txt
- sfo01vrli01.txt
- vra01svr01.txt
- vrb01svr01.txt
- vrs01lcm01a.txt

4 In the Windows PowerShell terminal, navigate to the `C:\CertGenVVD-version` folder and validate the configuration by running the following command.

```
.\CertGenVVD-version.ps1 -validate
```

The local machine configuration is validated successfully.

5 Use the `CertGenVVD` utility to generate the signed certificate files.

   a In the Windows PowerShell terminal, navigate to the `C:\CertGenVVD-version` folder and generate the signed certificates by running the following command.

   ```
   .\CertGenVVD-version.ps1 -MSCASigned -attrib 'CertificateTemplate:VMware'
   ```

   b Follow the on-screen instruction and enter a passphrase for PEM/P12 file encryption.

   All MSCA signed certificates are generated in the `C:\CertGenVVD-version\SignedByMSCACerts` folder.

6 Rename the `C:\CertGenVVD-version\SignedByMSCACerts` folder to `SignedByMSCACerts-sfo-jd`.

VMware Cloud Builder Implementation for Consolidated SDDC

3

You deploy and configure the VMware Cloud Builder virtual appliance to start the automated implementation of the SDDC components.

You deploy a single VMware Cloud Builder virtual appliance to automate the implementation of the SDDC components for Consolidated SDDC.

Procedure

1 Prerequisites for VMware Cloud Builder Implementation for Consolidated SDDC

Before you deploy the virtual appliance of VMware Cloud Builder, verify that your environment fulfills the requirements for this deployment.

2 Deploy the Virtual Appliance of VMware Cloud Builder for Consolidated SDDC

You deploy the virtual appliance of VMware Cloud Builder and configure the appliance to start the automated implementation of the SDDC components for Consolidated SDDC.

Prerequisites for VMware Cloud Builder Implementation for Consolidated SDDC

Before you deploy the virtual appliance of VMware Cloud Builder, verify that your environment fulfills the requirements for this deployment.

IP Addresses and Host Names

Verify that the static IP address and FQDN for the VMware Cloud Builder virtual appliance are available.

Setting	Value
IP address	172.16.11.60
Host name	sfo01cb01
Default gateway	172.16.11.253
DNS servers	■ 172.16.11.5 ■ 172.16.11.4
DNS domain	sfo01.rainpole.local
DNS search	sfo01.rainpole.local,rainpole.local

Setting	Value
Subnet mask	255.255.255.0
NTP Servers	■ ntp.sfo01.rainpole.local

Deployment Prerequisites

Verify that your environment satisfies the following prerequisites for the deployment of the virtual appliance of VMware Cloud Builder.

Prerequisite	Value
Environment	■ Verify that your environment is configured for deployment of VMware Cloud Builder and of the SDDC. See Chapter 2 Prepare the Environment for Automated Deployment for Consolidated SDDC.
Storage	■ Virtual disk provisioning: ■ Thin ■ Required storage: 28 GB
Installation Packages	■ Download the `.ova` file for VMware Cloud Builder.

Deploy the Virtual Appliance of VMware Cloud Builder for Consolidated SDDC

You deploy the virtual appliance of VMware Cloud Builder and configure the appliance to start the automated implementation of the SDDC components for Consolidated SDDC.

Procedure

1 Log in to the vSphere host by using the VMware Host Client.

   a Open a Web browser and go to **`https://sfo01w01esx01.sfo01.rainpole.local`**.

   b Log in by using the following credentials.

Setting	Value
User name	root
Password	*esxi_root_user_password*

2 In the **Navigator**, select **Host** and click the **Create / Register VM** button.

   The **New virtual machine** wizard appears.

3 On the **Select creation type** dialog box, select **Deploy a virtual machine from an OVF or OVA file** and click **Next**.

4 On the **Select OVF and VMDK files** dialog box, enter **`sfo01cb01`** for the virtual machine name, select the VMware Cloud Builder`.ova` file, and click **Next**.

5 In the **Select storage** dialog box, select **sfo01-w01-bkp01**, and click **Next**.

6 On the **License agreements** page, click **I agree** to accept the license agreement, and click **Next**.

7 On the **Deployment options** page, enter the following values and click **Next**.

Setting	Value
Network mappings	VM network
Disk provisioning	Thin
Power on automatically	Selected

8 In the **Additional settings** dialog box, expand **Application**, enter the following values, and click **Next**.

Option	Value
Root password	*sfo01cb01_root_password* Note : The passwords must be at least 8 characters, must contain uppercase, lowercase, digits, and special characters.
Confirm root password	*sfo01cb01_root_password*
Admin user name	admin
Admin password	*sfo01cb01_admin_password*
Confirm admin password	*sfo01cb01_admin_password*
Network 1 IP address	172.16.11.60
Network 1 Subnet mask	255.255.255.0
Default Gateway	172.16.11.253
Enter VM hostname	sfo01cb01
Domain name	sfo01.rainpole.local
Domain search path	sfo01.rainpole.local,rainpole.local
DNS	172.16.11.5,172.16.11.4
NTP	ntp.sfo01.rainpole.local

9 On the **Ready to complete** dialog box, review the virtual machine configuration and click **Finish**.

Deploy the Software-Defined Data Center Components for Consolidated SDDC

4

After you deploy and configure the VMware Cloud Builder appliance, you generate the JSON deployment file based on the values populated in the Deployment Parameters XLS file. You then validate the necessary run parameters and start the automated deployment of the SDDC componentsfor Consolidated SDDC.

Procedure

1 Prerequisites for Automated SDDC Deployment for Consolidated SDDC

Before you start the automated SDDC deployment, verify that your environment fulfills the requirements for this deployment.

2 Upload the VMware Validated Design Software Bundle and Signed Certificates to VMware Cloud Builder for Consolidated SDDC

After you deploy the Cloud Builder virtual appliance, you prepare for an automated deployment of the SDDC components by uploading the software bundle and the generated signed certificates. You then mount the software bundle and configure application properties.

3 Generate the JSON Deployment File for Consolidated SDDC

After you have populated all required configuration values in the Deployment Parameters XLS file, you upload it to the VMware Cloud Builder appliance and generate the JSON file that automates the deployment of the SDDC components in the consolidated cluster.

4 Validate the Deployment Parameters and Target Environment Prerequisites for Consolidated SDDC

You perform validation of the JSON deployment file and specific target environment prerequisites to ensure that you can successfully deploy the components of the consolidated cluster using VMware Cloud Builder.

5 Start the Automated Deployment for Consolidated SDDC

After you have successfully validated the `vvd-consolidated.json` file, you start the automated deployment of the components of the consolidated cluster.

Prerequisites for Automated SDDC Deployment for Consolidated SDDC

Before you start the automated SDDC deployment, verify that your environment fulfills the requirements for this deployment.

Deployment Prerequisites

Verify that your environment satisfies the following prerequisites for the automated SDDC deployment.

Prerequisite	Value
Environment	■ Verify that your environment is configured for deployment of the SDDC. See Chapter 2 Prepare the Environment for Automated Deployment for Consolidated SDDC.
Physical Network	■ Verify that your environment meets all physical network requirements, all host names and IP addresses are allocated for external services and SDDC components.
Active Directory	■ Verify that Active Directory is configured with all child domains, all service accounts and groups are created and configured.
DNS	■ Verify that DNS entries are configured for the root and child domains.
NTP Services	■ Verify that two external to the SDDC NTP servers are configured and time synchronization is configured on all ESXi hosts and AD domain controllers.
Storage	■ Primary vSAN storage: ■ Verify that the necessary primary storage capacity is allocated. See Deployment Parameters XLS file for Consolidated SDDC for automatic capacity calculation. ■ Secondary NFS storage: ■ Verify that NFS storage is mounted. ■ Verify that you have allocated the necessary storage capacity. See Datastore Requirements in the *VMware Validated Design Planning and Preparation for Consolidated SDDC* documentation.
Software Features	■ Fill in the Deployment Parameters XLS file for Consolidated SDDC. See Deployment Specification in the *VMware Validated Design Planning and Preparation for Consolidated SDDC* documentation. ■ Verify that you have generated CA-signed certificates for the management components of the SDDC. See Generate Signed Certificates for the SDDC Components for Consolidated SDDC.
Installation Packages	■ Download the `.iso` file for the software bundle for VMware Validated Design to your local file system.

For additional information, see the VMware Validated Design Planning and Preparation for Consolidated SDDC documentation.

Upload the VMware Validated Design Software Bundle and Signed Certificates to VMware Cloud Builder for Consolidated SDDC

After you deploy the Cloud Builder virtual appliance, you prepare for an automated deployment of the SDDC components by uploading the software bundle and the generated signed certificates. You then mount the software bundle and configure application properties.

Procedure

1 Log in to the VMware Cloud Builder virtual appliance.

   a Open a connection to **sfo01cb01.sfo01.rainpole.local** using a Secure Copy Protocol software like WinSCP.

   b Log in by using the following credentials.

Setting	Value
User name	admin
Password	*cloudbuilder_admin_password*

2 Upload the VMware Validated Design software bundle file `vvd-bundle-johndory-x.x.x-xxxxxxx.iso` to the `/mnt/hgfs` directory on the Cloud Builder appliance.

3 Upload all folders and their content from the `CertGenVVD` folder `C:\CertGenVVD-version\SignedByMSCACerts-sfo-jd` to the `/opt/vmware/vvd/certificates` directory on the Cloud Builder appliance.

4 Configure the Cloud Builder appliance and mount the VMware Validated Design software bundle `.iso` file.

   a Open an SSH connection to sfo01cb01.sfo01.rainpole.local.

   b Log in by using the following credentials.

Setting	Value
User name	admin
Password	*cloudbuilder_admin_password*

   c Switch to the **root** user by running the `su` command.

   d Mount the VMware Validated Design software bundle `.iso` file and configure application properties by running the following command.

```
/opt/vmware/vvd/cloud-builder/install/reconfigure.sh
```

   The script sets the full system path to each application's installation file, configures specific application properties, and restarts the bring-up service.

Generate the JSON Deployment File for Consolidated SDDC

After you have populated all required configuration values in the Deployment Parameters XLS file, you upload it to the VMware Cloud Builder appliance and generate the JSON file that automates the deployment of the SDDC components in the consolidated cluster.

Procedure

1 Log in to VMware Cloud Builder.

   a Open a Web browser and go to **`https://sfo01cb01.sfo01.rainpole.local`**.

   b Log in by using the following credentials.

Setting	Value
User name	admin
Password	*cloudbuilder_admin_password*

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

3 Generate the JSON file used for automated deployment of the SDDC components.

   a In the Cloud Builder**Navigator**, select the **Deployment Wizard** icon.

   b In the **Upload Config File** tab, from the **Select Architecture Type** drop-down menu, select the **VVD for Management and Workload Consolidation** architecture and click the **Upload Config File** button.

   c Navigate to the Deployment Parameters XLS file and click **Open**.

   d Click the **Generate JSON** button.

   Cloud Builder generates the JSON deployment file for the consolidated cluster.

Table 4-1. Consolidated SDDC JSON Deployment File

Architecture Type	JSON Filename	Workload Domain	Deployment Order
VVD for Management and Workload Consolidation	`vvd-consolidated.json`	Consolidated	1

4 Monitor the process and check the following log files for errors.

Table 4-2. VMware Cloud Builder JSON Generator Log File Location

Cloud Builder Component	Location
JSON Generator	`/opt/vmware/sddc-support/cloud_admin_tools/logs/JsonGenerator.log`

What to do next

After the JSON deployment file for Consolidated SDDC is generated, you validate its content for configuration, application, and bring-up readiness, and perform validation of the target platform.

Validate the Deployment Parameters and Target Environment Prerequisites for Consolidated SDDC

You perform validation of the JSON deployment file and specific target environment prerequisites to ensure that you can successfully deploy the components of the consolidated cluster using VMware Cloud Builder.

You validate the JSON deployment file `vvd-consolidated.json` for the consolidated cluster. In case any of the tests fail, you must remediate any errors and perform the validation process again. Additional information can be found in the audit log file.

Table 4-3. VMware Cloud Builder Platform Audit Log File Location

Cloud Builder Component	Location
Platform Audit	`/opt/vmware/sddc-support/cloud_admin_tools/logs/PlatformAudit.log`

Procedure

1 Log in to VMware Cloud Builder.

   a Open a Web browser and go to **`https://sfo01cb01.sfo01.rainpole.local`**.

   b Log in by using the following credentials.

Setting	Value
User name	admin
Password	*cloudbuilder_admin_password*

2 In the Cloud Builder**Navigator**, click the **Deployment Wizard** icon.

3 Select the Validate Environment tab.

4 From the **Select File to Validate** drop-down menu, select the `vvd-consolidated.json` file and click **Validate**.

5 If validation fails because of issues with the signed certificate files, resolve the issues and reupload the modified certificate files.

   a Upload the modified certificate files to the Cloud Builder appliance using an SCP software like WinSCP.

   b Open an SSH connection to sfo01cb01.sfo01.rainpole.local.

   c Run the following command.

```
su /opt/vmware/vvd/cloud-builder/install/reconfigure.sh
```

   When prompted, enter the *cloudbuilder_root_password*.

6 If validation fails with an `user input errors` message, remediate the Deployment Parameters XLS file.

7 In the **Upload Config File** tab, from the **Select Architecture Type** drop-down menu, select the **VVD for Management and Workload Consolidation** architecture and click the **Upload Config File** button.

8 Navigate to the updated Deployment Parameters XLS file and click **Open**.

9 On the **Overwrite Existing JSON File(s)dialog box**, select **Yes**.

10 Select the Validate Environment tab, from the Select File to Validate drop-down menu, select the vvd-consolidated.json file and click Validate.

   The `vvd-consolidated.json` file is successfully validated against the predefined run parameters.

What to do next

After successful validation of `vvd-consolidated.json` file, click **Next** to start the deployment of the management and workload consolidated cluster.

Start the Automated Deployment for Consolidated SDDC

After you have successfully validated the `vvd-consolidated.json` file, you start the automated deployment of the components of the consolidated cluster.

Procedure

1 Log in to VMware Cloud Builder.

   a Open a Web browser and go to **`https://sfo01cb01.sfo01.rainpole.local`**.

   b Log in by using the following credentials.

Setting	Value
User name	admin
Password	*cloudbuilder_admin_password*

2 In the Cloud Builder**Navigator**, select the **Deployment Wizard** icon.

3 Click the **Deploy an SDDC** tab.

4 From the **Select Deployment File** drop-down menu, select the `vvd-consolidated.json` file and click **Deploy**.

   The automated deployment of the components of the consolidated cluster starts.

5 Monitor the deployment and check the following log files for errors.

Table 4-4. VMware Cloud Builder Bring Up Service Log File Location

Cloud Builder Component	Location
Bring Up Service	`/opt/vmware/bringup/logs/vcf-bringup.log`
	`/opt/vmware/bringup/logs/vcf-bringup-debug.log`

Post-Deployment Virtual Infrastructure Configuration for Consolidated SDDC

5

After a successful deployment by using VMware Cloud Builder, complete the SDDC configuration with post-deployment tasks for Consolidated SDDC. For the virtual infrastructure layer, update the host profiles, configure the distributed firewall for traffic from the management applications.

Procedure

1 Distributed Firewall Configuration for Management Applications for Consolidated SDDC

   Configure a distributed firewall to improve the security in your environment by allowing only the network traffic that the SDDC needs. You define explicit firewall rules to allow access to the management applications.

2 Update the Host Profile for Consolidated SDDC

   Update the user name and password in the customizations for the hosts in the management and workload consolidated cluster to be compliant as the host profile does not contain credentials information.

Distributed Firewall Configuration for Management Applications for Consolidated SDDC

Configure a distributed firewall to improve the security in your environment by allowing only the network traffic that the SDDC needs. You define explicit firewall rules to allow access to the management applications.

Procedure

1 Add the vCenter Server Appliance to the NSX Distributed Firewall Exclusion List for Consolidated SDDC

   To keep the network access between the vCenter Server Appliance and NSX, you exclude the vCenter Server Appliance from all distributed firewall rules.

2 Create IP Sets for the Components of the Consolidated Cluster for Consolidated SDDC

   Create IP sets for all management applications in the consolidated cluster. At a later stage, use the IP sets to create security groups to use with the distributed firewall rules.

3 Create Security Groups for Consolidated SDDC

Create security groups that are used in configuring firewall rules for the groups of applications in the SDDC.

4 Create Distributed Firewall Rules for Consolidated SDDC

Create firewall rules that allow administrators to connect to the various VMware solutions, to allow for the user access to the vRealize Automation portal, and to provide for the external connectivity to the SDDC.

Add the vCenter Server Appliance to the NSX Distributed Firewall Exclusion List for Consolidated SDDC

To keep the network access between the vCenter Server Appliance and NSX, you exclude the vCenter Server Appliance from all distributed firewall rules.

Configure the NSX distributed firewall rules by using a vCenter Server Appliance. If a rule prevents network access between NSX Manager and vCenter Server, you cannot manage the firewall. Keep the access between the two products by adding vCenter Server to the firewall exclusion list.

Procedure

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

a Open a Web browser and go to **`https://sfo01w01vc01.sfo01.rainpole.local/ui`**.

b Log in by using the following credentials.

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

2 Exclude the vCenter Server Appliance instances from the distributed firewall rules.

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

b In the **Navigator**, click **Firewall Settings** and click the **Exclusion List** tab.

c From the **NSX Manager** drop-down menu, select **172.16.11.66**.

d Click the **Add** button.

The **Select VM(s) to exclude** dialog box appears.

e Select **sfo01w01vc01**, add it to the **Selected Objects** list, and click **OK**.

Create IP Sets for the Components of the Consolidated Cluster for Consolidated SDDC

Create IP sets for all management applications in the consolidated cluster. At a later stage, use the IP sets to create security groups to use with the distributed firewall rules.

Perform this procedure as many times as required to configure all necessary IP sets. For applications that are load balanced, include their VIP in the IP set.

Table 5-1. IP Sets for the Management Components in the Consolidation Cluster

Name	IP Addresses
Platform Services Controller instances	*Platform-Service-Controller_IPs*
vCenter Server instances	*vCenter-Server_IPs*
vRealize Automation appliances	*vRealize-Automation-Appliances_IPs*
vRealize Automation Windows	*vRealize-Automation-Windows _IPs*
vRealize Automation Proxy Agents	*vRealize-Automation-Proxy-Agents-IPs*
vRealize Business Server	*vRealize-Business_IPs*
vRealize Business Data Collector	*vRealize-Business-Data-Collector_IPs*
VMware VADP Solution	*vStorage-API for Data-Protection-Solution_IPs*
vRealize Operations Manager	*vRealize-Operations-Manager_IP's*
vRealize Operations Manager Remote Collectors	*vRealize-Operations-Manager-Remote-Collectors_IPs*
vRealize Log Insight	*vRealize-Log-Insight_IPs*
vRealize Suite Lifecycle Manager	*vRealize-Suite-Lifecycle-Manager_IPs*
Site Recovery Manager	*Site-Recovery-Manger_IPs*
vSphere Replication	*vSphere-Replication_IPs*
Update Manager Download Service	*UMDS_IPs*
SDDC	*Management-VLAN_Subnets, Management-VXLAN_Subnets*
Administrators	*Administrators_Subnet*

Procedure

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

   a Open a Web browser and go to **`https://sfo01w01vc01.sfo01.rainpole.local/ui`**.

   b Log in by using the following credentials.

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

2 Create an IP set.

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

   b In the **Navigator**, click **Groups and Tags** and click the **IP Sets** tab.

   c From the **NSX Manager** drop-down menu, select **172.16.11.66**.

d Click **Add**.

e In the **New IP Set** dialog box, enter the values for the IP set that you want to add, and click **Add**.

Setting	Value
Name	vCenter Server Instances
IP Addresses	172.16.11.64
Universal Synchronization	On

3 Repeat the previous step to create IP sets for all remaining components.

Create Security Groups for Consolidated SDDC

Create security groups that are used in configuring firewall rules for the groups of applications in the SDDC.

A security group is a collection of assets (or objects) from your vSphere inventory that you group. You perform this procedure multiple times to configure all the necessary security groups. In addition, you create the VMware Appliances and Windows Servers groups from the security groups you add in the previous repetitions of this procedure.

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

Name	Object Type	Selected Object
Platform Services Controller Instances	IP Sets	Platform Services Controller Instances
vCenter Server Instances	IP Sets	vCenter Server Instances
vRealize Automation Appliances	IP Sets	vRealize Automation Appliances
vRealize Automation Windows	IP Sets	vRealize Automation Windows
vRealize Business Server	IP Sets	vRealize Business Server
vRealize Automation Proxy Agents	IP Sets	vRealize Automation Proxy Agents
vRealize Business Data Collector	IP Sets	vRealize Business Data Collector
vSphere Storage APIs - Data Protection based backup solution	IP Sets	VMware VADP
vRealize Operations Manager	IP Sets	vRealize Operations Manager
vRealize Operations Manager Remote Collectors	IP Sets	vRealize Operations Manager Remote Collectors
vRealize Suite Lifecycle Manager	IP Sets	vRealize Suite Lifecycle Manager
Site Recovery Manager	IP Sets	Site Recovery Manager
vSphere Replication	IP Sets	vSphere Replication
vRealize Log Insight	IP Sets	vRealize Log Insight
Update Manager Download Service	IP Sets	Update Manager Download Service
SDDC	IP Sets	SDDC
Administrators	IP Sets	Administrators

Table 5-2. Security Groups for the Management Clusters Components in the SDDC (Continued)

Name	Object Type	Selected Object
Windows Servers	Security Groups	■ Site Recovery Manger ■ vRealize Automation Windows ■ vRealize Automation Proxy Agents
VMware Appliances	Security Groups	■ Platform Services Controller Instances ■ vCenter Server Instances ■ vSphere Replication ■ vRealize Automation Appliances ■ vRealize Business Server ■ vRealize Business Data Collector ■ vSphere Storage APIs - Data Protection based backup solution ■ vRealize Operations Manager ■ vRealize Operations Manager Remote Collectors ■ vRealize Suite Lifecycle Manager ■ vRealize Log Insight

Procedure

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

a Open a Web browser and go to **`https://sfo01w01vc01.sfo01.rainpole.local/ui`**.

b Log in by using the following credentials.

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

2 Create the security group.

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

b In the **Navigator**, click **Groups and Tags**.

c On the **Security Groups** tab, from the **NSX Manager** drop-down menu, select **172.16.11.66**.

d Click **Add**.

The **Create Security Group** wizard appears.

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

Setting	Value
Name	Platform Services Controller Instances
Universal Synchronization	On

f On the **Select Objects to Include** page, enter the following settings and click **Next**.

Setting	Value
Object Type	IP Sets
Selected Objects	Platform Services Controller Instances

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

3 Repeat the previous step to create all security groups.

Create Distributed Firewall Rules for Consolidated SDDC

Create firewall rules that allow administrators to connect to the various VMware solutions, to allow for the user access to the vRealize Automation portal, and to provide for the external connectivity to the SDDC.

Procedure

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

a Open a Web browser and go to **`https://sfo01w01vc01.sfo01.rainpole.local/ui`**.

b Log in by using the following credentials.

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

2 Add a section of rules for the management applications.

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

b From the **NSX Manager** drop-down menu, select **172.16.11.66**.

c Click **Add Section**.

The **New Section** dialog box appears.

d In the **Section Name** text box, enter **`VMware Management Services`**, turn on **Universal Synchronization**, and click **Add**.

3 Create a distributed firewall rule to allow an SSH access to administrators for the different VMware appliances.

a Click **Add rule**.

b In the **Name** column, enter **`Allow SSH to admins`**.

c In the **Source** column, click the **Edit** icon.

d From the **Object Type** drop-down menu, select **Security Group**, add **Administrators** to the **Selected Objects** list, and click **Save**.

e In the **Destination** column, click the **Edit** icon.

f From the **Object Type** drop-down menu, select **Security Group**, add **VMware Appliances** and **Update Manager Download Service** to the **Selected Objects** list, and click **Save**.

g In the **Service** column, click the **Edit** icon, add **SSH** to the **Selected Objects** list, and click **Save**.

h Click the **Publish** button.

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

Name	Source	Destination	Service / Port
Allow vRA Portal to end users	* any	■ vRealize Automation Appliances ■ vRealize Automation Windows ■ vRealize Business Server	HTTP, HTTPS
Allow vRA Console Proxy to end users	* any	vRealize Automation Appliances	TCP: 8444
AllowSDDC to any	SDDC	* any	* any
Allow PSC to admins	Administrators	Platform Services Controller Instances	HTTPS
Allow SSH to admins	Administrators	■ VMware Appliances ■ Update Manager Download Service	SSH
Allow RDP to admins	Administrators	Windows Servers	RDP
Allow Orchestrator to admins	Administrators	vRealize Automation Appliances	TCP: 8281, 8283
Allow vRB Data Collector to admins	Administrators	vRealize Business Data Collector	HTTP, HTTPS
Allow vROPs to admins	Administrators	■ vRealize Operations Manager ■ vRealize Operations Manager Remote Collectors	HTTP, HTTPS
Allow vRLI to admins	Administrators	vRealize Log Insight	HTTP, HTTPS
Allow vRSLCM to admins	Administrators	vRealize Suite Lifecycle Manager	HTTPS
Allow VAMI to admins	Administrators	VMware Appliances	TCP: 5480
Allow VMware VADP Solution to admins	Administrators	VMware Appliances	TCP: 8543

5 Change the allow default rule action to block.

a From the **NSX Manager** drop-down menu, select **172.16.11.66**.

b On the **General** tab, expand **Default Section Layer3**.

c Under **Default Rule**, in the **Action** column, change the action to **Block**.

d Click **Save** and click **Publish**.

You improve the network security by allowing only the network traffic required by the SDDC.

Update the Host Profile for Consolidated SDDC

Update the user name and password in the customizations for the hosts in the management and workload consolidated cluster to be compliant as the host profile does not contain credentials information.

Procedure

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

   a Open a Web browser and go to **`https://sfo01w01vc01.sfo01.rainpole.local/ui`**.

   b Log in by using the following credentials.

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

2 Update the sfo01-w01hp-consolidated01 host profile.

   a From the **Home** menu, select **Policies and Profiles** and click **Host Profiles**.

   b Right-click **sfo01-w01hp-consolidated01**, and select **Copy Settings from Host**.

   c Select **sfo01w01esx01.sfo01.rainpole.local**, and click **OK**.

3 Edit the sfo01-w01hp-consolidated01 host profile.

   a On the **Host Profiles** page, right-click **sfo01-w01hp-consolidated01**, and select **Edit Host Customizations**.

   The **Edit Host Customizations** wizard appears.

   b On the **Select hosts** page, select all hosts and click **Next**.

   c On the **Customize hosts** page, in the **Path** column, click the filtering icon and enter **`active directory`**.

   d For the **User Name** and **Password** properties, enter the following values.

ESXi Host	User Name	Password
sfo01w01esx01.sfo01.rainpole.local	svc-domain-join@rainpole.local	*svc-domain-join_password*
sfo01w01esx02.sfo01.rainpole.local	svc-domain-join@rainpole.local	*svc-domain-join_password*
sfo01w01esx03.sfo01.rainpole.local	svc-domain-join@rainpole.local	*svc-domain-join_password*
sfo01w01esx04.sfo01.rainpole.local	svc-domain-join@rainpole.local	*svc-domain-join_password*

   e Click **Finish**.

4 Verify compliance and remediate the hosts.

   a On the **Host Profiles** page, click **sfo01-w01hp-consolidated01**, and click the **Monitor** tab.

   b Click **Compliance**, click **Actions**, and select **Check Host Profile Compliance**.

   On the **Host profile** page, in the **Host Profile Compliance** column, the first host shows as `Compliant`, and the other hosts show as `Not Compliant`.

   c Select all hosts that are not compliant and click **Remediate**.

d In the **Remediate** dialog box, select **Automatically reboot hosts that require remediation**.

e Click **OK**.

All hosts show as **Compliant**.

Post-Deployment Operations Management Configuration for Consolidated SDDC

6

After you deploy the operations management applications for Consolidated SDDC, perform the post-deployment tasks for the operations management layer. Reconfigure the UMDS application virtual network, enable the automatic synchronization of authentication sources in vRealize Operations Manager, and define monitoring goals for the default policy.

Procedure

1 Post-Deployment Configuration of Update Manager Download Service for Consolidated SDDC

After you deploy Update Manager Download Service (UMDS), perform the post-deployment tasks. Allocate a static IP address and connect UMDS to the application virtual network for Consolidated SDDC.

2 Post-Deployment Configuration of vRealize Operations Manager for Consolidated SDDC

After you deploy vRealize Operations Manager, enable the automatic synchronization of the user membership for configured groups and remove the existing service accounts. Add the service accounts to integrate vRealize Operations Manager with both vRealize Log Insight and vRealize Automation, and define monitoring goals for the default policy.

Post-Deployment Configuration of Update Manager Download Service for Consolidated SDDC

After you deploy Update Manager Download Service (UMDS), perform the post-deployment tasks. Allocate a static IP address and connect UMDS to the application virtual network for Consolidated SDDC.

Reconfigure Update Manager Download Service for Consolidated SDDC

After you deploy Update Manager Download Service (UMDS), the UMDS virtual machine is outside of the application virtual network. Add the UMDS virtual machine to the application virtual network for Consolidated SDDC and update the UMDS virtual machine IP address.

Procedure

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

   a Open a Web browser and go to **`https://sfo01w01vc01.sfo01.rainpole.local/ui`**.

   b Log in by 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**, expand the **sfo01w01vc01.sfo01.rainpole.local** tree.

4 Connect the Update Manager Download Service virtual machine to the **Mgmt-RegionA01-VXLAN** port group.

   a Right-click **sfo01umds01** and select **Edit Settings**.

   b On the **Edit Settings** page, browse to the following network and click **OK**.

Setting	Value
Network adapter 1	A distributed port group that ends with *Mgmt-RegionA01-VXLAN*.

5 Change the IP address of the Update Manager Download Service virtual machine.

   a Right-click **sfo01umds01** and select **Open Console**.

   b Log in by using the following credentials.

Setting	Value
User name	**svc-umds**
Password	*svc_umds_password*

   c To open the `01–netcfg.yaml` file, run the following command.

```
sudo vi /etc/netplan/01–netcfg.yaml
```

   When prompted, provide the password for the **svc-umds** account.

   d In the `01–netcfg.yaml` file, enter the following settings and save the file.

Setting	Value
addresses	[192.168.31.67/24]
gateway4	192.168.31.1

   e To apply the changes, run the following command.

```
sudo netplan apply
```

6 Log in to the **dc01rpl.rainpole.local** DNS server by using a Remote Desktop Protocol (RDP) client.

   a Open an RDP connection to **`dc01rpl.rainpole.local`**.

   b Log in by using the following credentials.

Setting	Value
User name	Active Directory administrator
Password	*ad_admin_password*

7 Open the Windows **Start** menu, in the **Search** text box enter **`dnsmgmt.msc`**, and press Enter.

   The **DNS Manager** dialog box appears.

8 Under **Forward Lookup Zones**, select the **sfo01.rainpole.local** domain.

9 In the right pane, double-click the **sfo01umds01** record, modify the IP address, and click **OK**.

Setting	Value
Fully qualified domain name (FQDN)	sfo01umds01.sfo01.rainpole.local
IP Address	192.168.31.67
Update associated pointer (PTR) record	Selected

Post-Deployment Configuration of vRealize Operations Manager for Consolidated SDDC

After you deploy vRealize Operations Manager, enable the automatic synchronization of the user membership for configured groups and remove the existing service accounts. Add the service accounts to integrate vRealize Operations Manager with both vRealize Log Insight and vRealize Automation, and define monitoring goals for the default policy.

Procedure

1 Enable the Automatic Synchronization of Authentication Sources in vRealize Operations Manager for Consolidated SDDC

   After you enable the automatic synchronization of user membership for the rainpole.local and sfo01.rainpole.local Active Directory instances, vRealize Operations Manager maps the imported LDAP users to user groups.

2 Remove Existing Service Accounts in vRealize Operations Manager for Consolidated SDDC

   After you enable automatic synchronization of authentication sources, remove the **svc-vrli-vrops** and **svc-vra-vrops** service accounts and later add them. vRealize Operations Manager does not provide an API to perform an automatic synchronization.

3 Configure the User Privileges for vRealize Operations Manager to Integrate with vRealize Log Insight for Consolidated SDDC

   To use the Launch in Context functionality between vRealize Operations Manager and vRealize Log Insight, assign an administrator role to the **svc-vrli-vrops** service account.

4 Enable the Integration of vRealize Log Insight with vRealize Operations Manager for Consolidated SDDC

   Connect vRealize Log Insight for Consolidated SDDC with vRealize Operations Manager to run vRealize Log Insight from within vRealize Operations Manager. Use the Launch in Context functionality between the two management applications to troubleshoot the management nodes and vRealize Operations Manager by using the dashboards and alerts from the vRealize Log Insight user interface.

5 Configure the User Privileges for vRealize Operations Manager to Integrate with vRealize Automation for Consolidated SDDC

   Configure read-only privileges for the **svc-vra-vrops** service account in vRealize Operations Manager. vRealize Automation uses this account to collect metrics from vRealize Operations Manager for reclamation of tenant workloads that have a low use of CPU, memory, or disk space.

6 Verify the Integration of vRealize Operations Manager as a Metrics Provider in vRealize Automation for Consolidated SDDC

   In vRealize Automation, verify that vRealize Operations Manager is integrated as a metrics provider so that vRealize Automation can pull metrics for the reclamation of tenant workloads.

7 Define the Monitoring Goals for the Default Policy in vRealize Operations Manager for Consolidated SDDC

   Define the default policy settings for monitoring the vCenter Server instances in vRealize Operations Manager. vRealize Operations Manager uses these settings to analyze and monitor the objects associated with a vCenter Server instance.

Enable the Automatic Synchronization of Authentication Sources in vRealize Operations Manager for Consolidated SDDC

After you enable the automatic synchronization of user membership for the rainpole.local and sfo01.rainpole.local Active Directory instances, vRealize Operations Manager maps the imported LDAP users to user groups.

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	*deployment_admin_password*

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

3 In the left pane, expand **Access** and click **Authentication Sources**.

4 To enable an automatic synchronization for the Active Directory instances, configure the authentication sources.

   a On the **Authentication Sources** page, select **rainpole.local** and click **Edit**.

   b In the **Edit Source for User and Group Import** dialog box, expand **Details** and select **Automatically synchronize user membership for configured groups**.

   c Click **OK**.

   d Repeat this step for the **sfo01.rainpole.local** Active Directory instance.

Remove Existing Service Accounts in vRealize Operations Manager for Consolidated SDDC

After you enable automatic synchronization of authentication sources, remove the **svc-vrli-vrops** and **svc-vra-vrops** service accounts and later add them. vRealize Operations Manager does not provide an API to perform an automatic synchronization.

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	*deployment_admin_password*

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

3 In the left pane, expand **Access** and click **Access Control**.

4 Remove the existing **svc-vrli-vrops** and **svc-vra-vrops** service accounts.

   a On the **Access Control** page, select **svc-vrli-vrops** and click **Delete**.

   b In the **Delete User** dialog box, click **Yes**.

   c Repeat this step and remove the **svc-vra-vrops** service account.

Configure the User Privileges for vRealize Operations Manager to Integrate with vRealize Log Insight for Consolidated SDDC

To use the Launch in Context functionality between vRealize Operations Manager and vRealize Log Insight, assign an administrator role to the **svc-vrli-vrops** service account.

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	*deployment_admin_password*

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

3 In the left pane, expand **Access** and click **Access Control**.

4 On the **Access Control** page, click the **User Accounts** tab and click the **Import Users** icon.

5 On the **Import Users** page, import the **svc-vrli-vrops** service account.

   a From the **Import From** drop-down menu, select **rainpole.local**.

   b Select the **Basic** option for the search query.

   c In the **Search String** text box, enter **`svc-vrli-vrops`** and click **Search**.

   d Select **svc-vrli-vrops@rainpole.local** and click **Next**.

6 On the **Assign Groups and Permissions** page, click the **Objects** tab, configure the following settings, and click **Finish**.

Setting	Value
Select Role	Administrator
Assign this role to the user	Selected
Allow access to all objects in the system	Selected

7 To allow access to all objects on the system, in the warning prompt click **Yes**.

Enable the Integration of vRealize Log Insight with vRealize Operations Manager for Consolidated SDDC

Connect vRealize Log Insight for Consolidated SDDC with vRealize Operations Manager to run vRealize Log Insight from within vRealize Operations Manager. Use the Launch in Context functionality between the two management applications to troubleshoot the management nodes and vRealize Operations Manager by using the dashboards and alerts from the vRealize Log Insight user interface.

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 by using the following credentials.

Setting	Value
User name	admin
Password	*deployment_admin_password*

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

3 In the left pane, under **Integration**, click **vRealize Operations**.

4 On the **vRealize Operations Integration** page, select **Enable launch in context**.

5 To validate the connection, click **Test Connection** and click **Save**.

6 In the progress dialog box, click **OK**.

Configure the User Privileges for vRealize Operations Manager to Integrate with vRealize Automation for Consolidated SDDC

Configure read-only privileges for the **svc-vra-vrops** service account in vRealize Operations Manager. vRealize Automation uses this account to collect metrics from vRealize Operations Manager for reclamation of tenant workloads that have a low use of CPU, memory, or disk space.

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	*deployment_admin_password*

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

3 In the left pane, expand **Access** and click **Access Control**.

4 On the **Access Control** page, click the **User Accounts** tab and click the **Import Users** icon.

5 On the **Import Users** page, import the **svc-vra-vrops** service account.

   a From the **Import From** drop-down menu, select **rainpole.local**.

   b Select the **Basic** option for the search query.

c In the **Search String** text box, enter `svc-vra-vrops` and click **Search**.

d Select **svc-vra-vrops@rainpole.local** and click **Next**.

6 On the **Assign Groups and Permissions** page, click the **Objects** tab, configure the following settings, and click **Finish**.

Setting	Value
Select Role	ReadOnly
Assign this role to the user	Selected
Select Object	**vCenter Adapter > vCenter Adapter - sfo01w01vc01**

Verify the Integration of vRealize Operations Manager as a Metrics Provider in vRealize Automation for Consolidated SDDC

In vRealize Automation, verify that vRealize Operations Manager is integrated as a metrics provider so that vRealize Automation can pull metrics for the reclamation of tenant workloads.

Procedure

1 Log in to the vRealize Automation Rainpole portal.

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

b Log in by using the following credentials.

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

2 Click the **Administration** tab.

3 In the left pane, expand **Reclamation** and click **Metrics Provider**.

4 Click **Test Connection** and verify that the test connection is successful.

Define the Monitoring Goals for the Default Policy in vRealize Operations Manager for Consolidated SDDC

Define the default policy settings for monitoring the vCenter Server instances in vRealize Operations Manager. vRealize Operations Manager uses these settings to analyze and monitor the objects associated with a vCenter Server instance.

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	*deployment_admin_password*

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

3 In the left pane, click **Solutions**.

4 On the **Solutions** page, select the **VMware vSphere** solution, and click the **Configure** icon.

   The **Manage Solution - VMware vSphere** dialog box appears.

5 Under **Instance Name**, select the **sfo01w01vc01** vCenter adapter.

6 Click **Define Monitoring Goals**.

   The **Define Monitoring Goals** dialog box appears.

7 Under **Enable vSphere Hardening Guide Alerts**, click **Yes**, leave the default configuration for the other options, and click **Save**.

8 In the **Info** dialog box, click **OK**.

9 Click **Save Settings**.

10 In the **Info** dialog box, click **OK**.

11 In the **Manage Solution - VMware vSphere** dialog box, click **Close**.

Post-Deployment Cloud Management Platform Configuration for Consolidated SDDC

7

After you deploy the Cloud Management Platform (CMP) for Consolidated SDDC, perform the post-deployment tasks for the cloud management layer. Complete the SDDC configuration in your environment and confirm the successful provisioning of virtual machines by using newly created blueprints.

Procedure

1 Create Machine Prefixes for Consolidated SDDC

As a fabric administrator, you create machine prefixes that can be later used for creating names of machines provisioned by using vRealize Automation. Tenant administrators and business group managers select the machine prefixes and assign them to provisioned machines through blueprints and business group defaults.

2 Create Business Groups for Consolidated SDDC

Tenant administrators create business groups to associate a set of services and resources to a set of users that often correspond to a line of business, department, or other organizational unit. To request machines, users must belong to a business group.

3 Create Reservation Policies for Consolidated SDDC

You use reservation policies to group similar reservations together. To allow a tenant administrator or a business group manager to use the reservation policy in a blueprint, first create the reservation policy tag and then add the policy to reservations.

4 Create External Network Profiles for Consolidated SDDC

Before members of a business group can request virtual machines, fabric administrators must create network profiles to define the subnet and routing configuration for the virtual machines. Each network profile is configured for a specific network port group or virtual network to specify the IP address and the routing configuration for virtual machines provisioned to that network.

5 Create Reservations for the Cluster for Consolidated SDDC

Before members of a business group can request machines, as a fabric administrator, you must allocate resources to them by creating a reservation. Each reservation is configured for a specific business group to grant them access to request machines on a specified compute resource.

6 Create Reservations for the User Edge Resources for Consolidated SDDC

Before the members of a business group can request virtual machines, as a fabric administrator, you must allocate NSX Edge resources to that business group by creating a reservation. Each reservation is configured for a specific business group to grant access for the group members to request virtual machines on a specified compute resource.

7 Configure Single Machine Blueprints for Consolidated SDDC

Virtual machine blueprints regulate the attributes, policies, management settings, and provisioning manner of a virtual machine.

8 Reconfigure the Microsoft SQL Server for vRealize Automation for Consolidated SDDC

When you deploy vRealize Automation, the Microsoft SQL Server is outside of the vRealize Automation application virtual network and you must reconfigure the Microsoft SQL Server.

Create Machine Prefixes for Consolidated SDDC

As a fabric administrator, you create machine prefixes that can be later used for creating names of machines provisioned by using vRealize Automation. Tenant administrators and business group managers select the machine prefixes and assign them to provisioned machines through blueprints and business group defaults.

Machine prefixes are shared across all tenants. Every business group has a default machine prefix. Every blueprint must have a machine prefix or use the group default prefix. Fabric administrators are responsible for managing machine prefixes. A prefix consists of a base name to be followed by a counter of a specified number of digits. When all the digits are used, vRealize Automation rolls back to the first number.

Procedure

1 Log in to the vRealize Automation Rainpole portal.

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

b Log in by using the following credentials.

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

2 Click the **Infrastructure** tab.

3 In the left pane, expand **Administration** and click **Machine Prefixes**.

4 Create a default machine prefix for the Production business group.

a On the **Machine Prefixes** page, click **New** and enter the following settings.

Setting	Value
Name	Prod-
Number of Digits	5
Next Number	1

b Click the **Save** icon.

5 Create a default machine prefix for the Development business group.

a On the **Machine Prefixes** page, click **New** and enter the following settings.

Setting	Value
Name	Dev-
Number of Digits	5
Next Number	1

b Click the **Save** icon.

Create Business Groups for Consolidated SDDC

Tenant administrators create business groups to associate a set of services and resources to a set of users that often correspond to a line of business, department, or other organizational unit. To request machines, users must belong to a business group.

For this implementation, you create two business groups, a Production business group and a Development business group.

Procedure

1 Log in to the vRealize Automation Rainpole portal.

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

b Log in by using the following credentials.

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

2 Click the **Administration** tab.

3 In the left pane, expand **Users & Groups** and click **Business Groups**.

4 Create the Production business group.

a On the **Business Groups** page, click **New**.

b On the **General** tab, enter the following settings and click **Next**.

Setting	Value
Name	Production
Send capacity alert emails to	vra-admin-rainpole@rainpole.local

c On the **Members** tab, in the **Group manager role** text box, enter `ug-vra-admins-rainpole@rainpole.local` and press Enter.

d Select the **ug-vra-admins-rainpole@rainpole.local** group, and click **Next**.

e On the **Infrastructure** tab, from the **Default machine prefix** drop-down menu, select **Prod-** and click **Finish**.

5 Create the Development business group.

a On the **Business Groups** page, click **New**.

b On the **General** tab, enter the following settings and click **Next**.

Setting	Value
Name	Development
Send capacity alert emails to	vra-admin-rainpole@rainpole.local

c On the **Members** tab, in the **Group manager role** text box, enter `ug-vra-admins-rainpole@rainpole.local` and press Enter.

d Select the **ug-vra-admins-rainpole@rainpole.local** group, and click **Next**.

e On the **Infrastructure** tab, from the **Default machine prefix** drop-down menu, select **Dev-** and click **Finish**.

Create Reservation Policies for Consolidated SDDC

You use reservation policies to group similar reservations together. To allow a tenant administrator or a business group manager to use the reservation policy in a blueprint, first create the reservation policy tag and then add the policy to reservations.

When you request a machine, it can be provisioned on any reservation of the appropriate type that has sufficient capacity for the machine. To restrict the machines provisioned from a blueprint to a subset of available reservations, you apply a reservation policy to the blueprint. A reservation policy is often used to collect resources into groups for different service levels, or to make a specific type of resource easily available for a particular purpose. A reservation policy can include reservations of different types, but only reservations that match the blueprint type are considered when selecting a reservation for a particular request.

Procedure

1 Log in to the vRealize Automation Rainpole portal.

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

   b Log in by using the following credentials.

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

2 Click the **Infrastructure** tab.

3 In the left pane, expand **Reservations** and click **Reservation Polices**.

4 Create a reservation policy for the Production business group.

   a On the **Reservation Policies** page, click **New** and enter the following settings.

Setting	Value
Name	SFO-Production-Policy
Type	Reservation Policy
Description	Reservation policy for the Production business group

   b Click **OK**.

5 Create a reservation policy for the Development business group.

   a On the **Reservation Policies** page, click **New** and enter the following settings.

Setting	Value
Name	SFO-Development-Policy
Type	Reservation Policy
Description	Reservation policy for the Development business group

   b Click **OK**.

6 Create a reservation policy for the Tenant Edge resources.

   a On the **Reservation Policies** page, click **New** and enter the following settings.

Setting	Value
Name	SFO-Edge-Policy
Type	Reservation Policy
Description	Reservation policy for the Tenant Edge resources

   b Click **OK**.

Create External Network Profiles for Consolidated SDDC

Before members of a business group can request virtual machines, fabric administrators must create network profiles to define the subnet and routing configuration for the virtual machines. Each network profile is configured for a specific network port group or virtual network to specify the IP address and the routing configuration for virtual machines provisioned to that network.

Repeat this procedure six times to create the following six external network profiles.

- Ext-Net-Profile-Production-App
- Ext-Net-Profile-Production-DB
- Ext-Net-Profile-Production-Web
- Ext-Net-Profile-Development-App
- Ext-Net-Profile-Development-DB
- Ext-Net-Profile-Development-Web

Procedure

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

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

2. Click the **Infrastructure** tab.
3. In the left pane, expand **Reservations** and click **Network Profiles**.
4. On the **Network Profiles** page, click **New > External**.

   The **New Network Profile - External** page appears.

5 On the **General** tab, add the network profiles.

a For the Production group external network profile, enter the following settings.

Setting	Production Web Value	Production DB Value	Production App Value
Name	Ext-Net-Profile-Production-Web	Ext-Net-Profile-Production-DB	Ext-Net-Profile-Production-App
Description	External Network profile for Web Tier of Production Business Group	External Network profile for DB Tier of Production Business Group	External Network profile for App Tier of Production Business Group
Subnet mask	255.255.255.0	255.255.255.0	255.255.255.0
Gateway	172.11.10.1	172.11.11.1	172.11.12.1

b For the Development group external network profile, enter the following settings.

Setting	Development Web Value	Development DB Value	Development App Value
Name	Ext-Net-Profile-Development-Web	Ext-Net-Profile-Development-DB	Ext-Net-Profile-Development-App
Description	External Network profile for Web Tier of Development Business Group	External Network profile for DB Tier of Development Business Group	External Network profile for App Tier of Development Business Group
Subnet mask	255.255.255.0	255.255.255.0	255.255.255.0
Gateway	172.12.10.1	172.12.11.1	172.12.12.1

6 Click the **DNS** tab and for the profile you are creating enter the following settings.

Setting	Value
Primary DNS	172.16.11.4
Secondary DNS	172.16.11.5
DNS suffix	sfo01.rainpole.local
DNS search suffixes	sfo01.rainpole.local

7 Click the **Network Ranges** tab and click the **New** button.

a For the Production business network range, enter the following settings.

Setting	Production Web Value	Production DB Value	Production App Value
Name	Production-Web	Production-DB	Production-App
Description	Static IP range for Web Tier of the Production Group	Static IP range for DB Tier of the Production Group	Static IP range for App Tier of the Production Group
Start IP	172.11.10.20	172.11.11.20	172.11.12.20
End IP	172.11.10.250	172.11.11.250	172.11.12.250

b For the Development network range, enter the following settings.

Setting	Development Web Value	Development DB Value	Development App Value
Name	Development-Web	Development-DB	Development-App
Description	Static IP range for Web Tier of the Development Group	Static IP range for DB Tier of the Development Group	Static IP range for App Tier of the Development Group
Start IP	172.12.10.20	172.12.11.20	172.12.12.20
End IP	172.12.10.250	172.12.11.250	172.12.12.250

c Click **OK** to save the network range.

8 Click **OK** to save the network profile.

9 Repeat this procedure to create all external network profiles.

Create Reservations for the Cluster for Consolidated SDDC

Before members of a business group can request machines, as a fabric administrator, you must allocate resources to them by creating a reservation. Each reservation is configured for a specific business group to grant them access to request machines on a specified compute resource.

Repeat this procedure two times to create reservations for both the Production and the Development business groups.

Group	Name
Production	SFO01-Comp01-Prod-Res01
Development	SFO01-Comp01-Dev-Res01

Procedure

1 Log in to the vRealize Automation Rainpole portal.

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

   b Log in by using the following credentials.

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

2 Click the **Infrastructure** tab.

3 In the left pane, expand **Compute Resources** and click **Compute Resources**.

4 In the **Name** column, point to **sfo01-w01-consolidated01**, and from the drop-down menu select **Data Collection**.

5 Click the four **Request now** buttons in each field on the page.

   Wait for the data collection process to finish.

6 Click **Refresh** and verify that **Status** shows `Succeeded` for both **Inventory** and **Network and Security Inventory**.

7 In the left pane, expand **Reservations** and click **Reservations**.

8 On the **Reservations** page, click **New > vSphere (vCenter)**.

   The **New Reservation - vSphere (vCenter)** page appears.

9 On the **General** tab, enter the following settings.

Setting	Production Group Value	Development Group Value
Name	SFO01-Comp01-Prod-Res01	SFO01-Comp01-Dev-Res01
Tenant	Rainpole	Rainpole
Business Group	Production	Development
Reservation Policy	SFO-Production-Policy	SFO-Development-Policy
Priority	100	100
Enable This Reservation	Selected	Selected

10 Click the **Resources** tab and enter the following settings.

Setting	Value
Compute resource	sfo01-w01-consolidated01(sfo01w01vc01.sfo01.rainpole.local)
Memory (GB)	This Reservation **`200`**

Setting	Value
Storage (GB)	■ Select the **sfo01-w01-vsan01** check box. ■ This Reservation Reserved **2000** ■ Priority **1**
Resource Pool	sfo01-w01rp-user-vm

11 Click the **Network** tab.

a For the Production business group, enter the following settings.

Network Adapter	Network Profile
vxw-dvs-xxxxx-Production-Web-VXLAN	Ext-Net-Profile-Production-Web
vxw-dvs-xxxxx-Production-DB-VXLAN	Ext-Net-Profile-Production-DB
vxw-dvs-xxxxx-Production-App-VXLAN	Ext-Net-Profile-Production-App

b For the Development business group, enter the following settings.

Network Adapter	Network Profile
vxw-dvs-xxxxx-Development-Web-VXLAN	Ext-Net-Profile-Development-Web
vxw-dvs-xxxxx-Development-DB-VXLAN	Ext-Net-Profile-Development-DB
vxw-dvs-xxxxx-Development-App-VXLAN	Ext-Net-Profile-Development-App

12 To save this reservation, click **OK**.

13 Repeat this procedure and create a reservation for the Development business group.

Create Reservations for the User Edge Resources for Consolidated SDDC

Before the members of a business group can request virtual machines, as a fabric administrator, you must allocate NSX Edge resources to that business group by creating a reservation. Each reservation is configured for a specific business group to grant access for the group members to request virtual machines on a specified compute resource.

Repeat this procedure two times to create reservations for both the Production and the Development business groups.

Group	Name
Production	SFO01-Edge01-Prod-Res01
Development	SFO01-Edge01-Dev-Res01

Procedure

1 Log in to the vRealize Automation Rainpole portal.

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

   b Log in by using the following credentials.

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

2 Click the **Infrastructure** tab.

3 In the left pane, expand **Reservations** and click **Reservations**.

4 On the **Reservations** page, click **New > vSphere (vCenter)**.

   The **New Reservation - vSphere (vCenter)** page appears.

5 On the **General** tab, nter the following settings.

Setting	Production Group Value	Development Group Value
Name	SFO01-Edge01-Prod-Res01	SFO01-Edge01-Dev-Res01
Tenant	Rainpole	Rainpole
Business Group	Production	Development
Reservation Policy	SFO-Edge-Policy	SFO-Edge-Policy
Priority	100	100
Enable This Reservation	Selected	Selected

6 Click the **Resources** tab and enter the following settings.

Setting	Value
Compute resource	sfo01-w01-consolidated01(sfo01w01vc01.sfo01.rainpole.local)
Memory (GB)	This Reservation **`200`**
Storage (GB)	■ Select the **sfo01-w01-vsan01** check box. ■ This Reservation Reserved **`2000`** ■ Priority **`1`**
Resource Pool	sfo01-w01rp-user-edge

7 Click the **Network** tab.

a For the Production business group, enter the following settings.

Network Adapter	Network Profile
vxw-dvs-xxxxx-Production-Web-VXLAN	Ext-Net-Profile-Production-Web
vxw-dvs-xxxxx-Production-DB-VXLAN	Ext-Net-Profile-Production-DB
vxw-dvs-xxxxx-Production-App-VXLAN	Ext-Net-Profile-Production-App

b For the Development business group, enter the following settings.

Network Adapter	Network Profile
vxw-dvs-xxxxx-Development-Web-VXLAN	Ext-Net-Profile-Development-Web
vxw-dvs-xxxxx-Development-DB-VXLAN	Ext-Net-Profile-Development-DB
vxw-dvs-xxxxx-Development-App-VXLAN	Ext-Net-Profile-Development-App

8 To save this reservation, click **OK**.

9 Repeat this procedure and create a reservation for the Development business group.

Configure Single Machine Blueprints for Consolidated SDDC

Virtual machine blueprints regulate the attributes, policies, management settings, and provisioning manner of a virtual machine.

Procedure

1 Create a Service Catalog for Consolidated SDDC

A service catalog provides a common interface for consumers of IT services to request services, track their requests, and manage their provisioned service items.

2 Create a Single Machine Blueprint for Consolidated SDDC

Create blueprints for cloning the virtual machine templates that use the specified resources on vCenter Server. Tenants can later use these blueprints for automatic provisioning. A blueprint is the complete specification for a virtual, cloud, or physical machine.

3 Create Entitlements for Business Groups for Consolidated SDDC

You add a service, catalog item, or an action to an entitlement, to allow the users and groups identified in the entitlement to request provisionable items from the service catalog. The entitlement allows members of a particular business group (for example, the Production business group) to use the blueprint. Without the entitlement, the users cannot use the blueprint.

4 Configure Entitlements for Blueprints for Consolidated SDDC

You entitle users to the actions and items that belong to the service catalog by associating each blueprint with an entitlement.

5 Test the Deployment of a Single Machine Blueprint for Consolidated SDDC

Test your environment to confirm the successful provisioning of virtual machines by using the newly created blueprints.

Create a Service Catalog for Consolidated SDDC

A service catalog provides a common interface for consumers of IT services to request services, track their requests, and manage their provisioned service items.

Procedure

1 Log in to the vRealize Automation Rainpole portal.

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

b Log in by using the following credentials.

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

2 Click the **Administration** tab.

3 In the left pane, expand **Catalog Management** and click **Services**.

4 On the **Services** page, click **New**.

The **New Service** page appears.

5 Enter the following settings, and click **OK**.

Setting	Value
Name	SFO Service Catalog
Description	Default setting (blank)
Icon	Default setting (blank)
Status	Active

Create a Single Machine Blueprint for Consolidated SDDC

Create blueprints for cloning the virtual machine templates that use the specified resources on vCenter Server. Tenants can later use these blueprints for automatic provisioning. A blueprint is the complete specification for a virtual, cloud, or physical machine.

Repeat this procedure three times to create the following three blueprints.

Blueprint Name	VM Template	Customization Specification	Reservation Policy
Windows Server 2012 R2 - SFO Prod	windows-2012r2-64 (sfo01w01vc01.sfo01.rainpole.local)	os-windows-joindomain-custom-spec	SFO-Production-Policy
Windows Server 2012 R2 With SQL2012 - SFO Prod	windows-2012r2-64-sql2012(sfo01w01vc01.sfo01.rainpole.local)	os-windows-joindomain-custom-spec	SFO-Production-Policy
Redhat Enterprise Linux 6 - SFO Prod	redhat6-enterprise-64(sfo01w01vc01.sfo01.rainpole.local)	os-linux-custom-spec	SFO-Production-Policy

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 by using the following credentials.

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

2 Click the **Design** tab.

3 In the left pane, click **Blueprints**.

4 On the **Blueprints** page, click **New**.

   The **New Blueprint** dialog box appears.

5 On the **General** tab, enter the following settings, and click **OK**.

Setting	Value
Name	Windows Server 2012 R2 - SFO Prod
Deployment limit	Default setting (blank)
Lease (days): Minimum	30
Lease (days): Maximum	270
Archive (days)	15

6 Select the **vSphere (vCenter) Machine** icon and drag it in the **Design Canvas**.

7 Click the **General** tab, enter the following settings, and click **Save**.

Setting	
ID	Default setting (vSphere_vCenter_Machine_1)
Description	Default setting (blank)
Display location on request	Deselected

Setting	
Reservation policy	SFO -Production-Policy
Machine prefix	Use group default
Instances: Minimum	Default setting
Instances: Maximum	1

8 Click the **Build Information** tab, enter the following settings, and click **Save**.

Setting	Value
Blueprint type	Server
Action	Clone
Provisioning workflow	CloneWorkflow
Clone from	windows-2012r2-64
Customization spec	os-windows-joindomain-custom-spec

Note If the value of the **Clone from** setting does not list the **windows-2012r2-64** template, you must perform a data collection on the sfo01-w01-consolidated01 Compute resource.

Verify that the required customization specification is available in the vSphere Client under **Menu > Policies and Profiles > VM Customization Specifications**.

9 Click the **Machine Resources** tab, enter the following settings, and click **Save**.

Setting	Minimum	Maximum
CPUs	2	4
Memory (MB)	4096	16384
Storage (GB)	Default setting	Same value as Minimum

10 Click the **Network** tab.

a In the **Categories** section, select **Network & Security** to display the list of available network and security components.

b Select the **Existing Network** component and drag it in the **Design Canvas**.

c Click the **Existing network** object and on the **General** tab, select the **Ext-Net-Profile-Production-Web** network profile , and click **OK**.

Blueprint Name	Existing network
Windows Server 2012 R2 - SFO Prod	Ext-Net-Profile-Production-Web
Windows Server 2012 R2 With SQL2012 - SFO Prod	Ext-Net-Profile-Production-DB
Redhat Enterprise Linux 6 - SFO Prod	Ext-Net-Profile-Production-App

d Click **Save**.

e In the **Design Canvas**, select the **vSphere_vCenter_Machine** object.

f Select the **Network** tab, click **New**, enter the following settings, and click **OK**.

Network	Assignment Type	Address
Ext-Net-Profile-Production-Web	Static IP	Default setting (blank)
Ext-Net-Profile-Production-DB	Static IP	Default setting (blank)
Ext-Net-Profile-Production-App	Static IP	Default setting (blank)

g Click **Finish** to save the blueprint.

11 Select the blueprint **Windows Server 2012 R2 - SFO Prod** and click **Publish**.

12 Repeat this procedure to create the remaining blueprints.

To test blueprints in a development environment, or according to your business needs, create development blueprints using the same process as for production blueprints.

Create Entitlements for Business Groups for Consolidated SDDC

You add a service, catalog item, or an action to an entitlement, to allow the users and groups identified in the entitlement to request provisionable items from the service catalog. The entitlement allows members of a particular business group (for example, the Production business group) to use the blueprint. Without the entitlement, the users cannot use the blueprint.

Perform this procedure to create an entitlement for the Production business group.

Entitlement Name	Status	Business Group	User & Groups
Prod-SingleVM-Entitlement	Active	Production	**ug-vra-admins-rainpole**

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 by using the following credentials.

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

2 Click the **Administration** tab.

3 In the left pane, expand **Catalog Management** and click **Entitlements**.

4 On the **Entitlements** page, click **New**.

The **New Entitlement** page appears.

5 Click the **General** tab, enter the following settings, and click **Next**.

Setting	Value
Name	Prod-SingleVM-Entitlement
Description	Default setting (blank)
Expiration Date	Default setting (blank)
Status	Active
Business Group	Production
All Users and Groups	Deselected
Users & Groups	**ug-vra-admins-rainpole**

6 On the **Items & Approvals** tab, add the actions that the users from the Production business group are entitled to.

a In the **Entitled Actions** section, click the **Add Actions** icon, select the following actions, and click **OK**.

- Connect using RDP (Machine)
- Power Cycle (Machine)
- Power off (Machine)
- Power on (Machine)
- Reboot (Machine)
- Shutdown (Machine)

b Click **Finish**.

Configure Entitlements for Blueprints for Consolidated SDDC

You entitle users to the actions and items that belong to the service catalog by associating each blueprint with an entitlement.

Repeat this procedure to associate the following blueprints with their entitlement.

Blueprint Name	Service Catalog	Add to Entitlement
Windows Server 2012 R2 - SFO Prod	SFO Service Catalog	Prod-SingleVM-Entitlement
Windows Server 2012 R2 With SQL2012 - SFO Prod	SFO Service Catalog	Prod-SingleVM-Entitlement
Red hat Enterprise Linux 6 - SFO Prod	SFO Service Catalog	Prod-SingleVM-Entitlement

Procedure

1 Log in to the vRealize Automation Rainpole portal.

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

   b Log in by using the following credentials.

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

2 Configure the service catalog for the blueprint.

   a Click the **Administration** tab.

   b In the left pane, expand **Catalog Management** and click **Catalog Items**.

   c On the **Catalog Items** page, click the **Windows Server 2012 R2 - SFO Prod** blueprint.

   The **Configure Catalog Item** page appears.

   d On the **General** tab, from the **Service** drop-down menu select **SFO Service Catalog**, and click **OK**.

3 Associate the blueprint with an entitlement.

   a In the left pane, under **Catalog Management** click **Entitlements**.

   b On the **Entitlements** page, click the **Prod-SingleVM-Entitlement** entitlement.

   The **Edit Entitlement** page appears.

   c Click the **Items & Approvals** tab.

   d Under **Entitled Items**, click the **Add Items** icon and select the **Windows Server 2012 R2 - SFO Prod** blueprint.

   e Click **OK**.

   f Click **Finish**.

4 Click the **Catalog** tab and verify that the blueprints are listed.

5 Repeat this procedure to associate all blueprints with their entitlements.

Test the Deployment of a Single Machine Blueprint for Consolidated SDDC

Test your environment to confirm the successful provisioning of virtual machines by using the newly created blueprints.

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 by using the following credentials.

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

2 Click the **Catalog** tab.

3 On the **Catalog** page, click the **Click here to apply filters** icon.

4 In the left pane, select the **SFO Service Catalog** check box.

5 Under one of the blueprints, click **Request** and click **Submit**.

6 Verify that the request finishes successfully.

   a On the **Deployments** tab, click the deployment that you submitted.

   b Click the **History** tab, and wait several minutes for the request to finish.

   c Under **Status**, verify that the virtual machine is successfully provisioned.

7 Verify that the virtual machine provisions in the consolidated cluster.

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

   b In the **Navigator**, expand **sfo01-w01rp-user-vm**, and verify that the provisioned virtual machine is present.

Reconfigure the Microsoft SQL Server for vRealize Automation for Consolidated SDDC

When you deploy vRealize Automation, the Microsoft SQL Server is outside of the vRealize Automation application virtual network and you must reconfigure the Microsoft SQL Server.

Procedure

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

   a Open a Web browser and go to **`https://sfo01w01vc01.sfo01.rainpole.local/ui`**.

   b Log in by using the following credentials.

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

2 Shut down the vRealize Automation components.

a From the **Home** menu, select **Hosts and Clusters** and expand the **sfo01w01vc01.sfo01.rainpole.local** tree.

b Right-click each of the following virtual machines, according to their shutdown order, and select **Power > Shut Down Guest OS**.

3 Migrate the Microsoft SQL Server virtual machine to the sfo01-w01fd-vra folder and connect it to the Mgmt-xRegion01-VXLAN port group.

a From the **Home** menu, select **Hosts and Clusters** and expand the **sfo01w01vc01.sfo01.rainpole.local** tree.

b Right-click **vra01mssql01**, select **Move to folder > sfo01-w01fd-vra**, and click **OK**.

c Right-click **vra01mssql01** and select **Edit Settings**.

d On the **Edit Settings** page, browse to the following network and click **OK**.

Setting	Value
Network adapter 1	A distributed port group that ends with *Mgmt-xRegion01-VXLAN*.

e Right-click **vra01mssql01** and select **Power > Power on**.

4 Change the IP address of the vra01mssql01 virtual machine.

a Right click **vra01mssql01** and select **Open Console**.

b Log in by using the following credentials.

Setting	Value
User name	Windows administrator user
Password	*windows_administrator_password*

c From the Windows **Start Menu**, select **Control Panel > Network and Internet > Network and Sharing Center > Change adapter settings**.

d Right-click the Ethernet adapter and select **Properties**.

e Select **Internet Protocol Version 4 (TCP/IPv4)** and click **Properties**.

f Enter the following settings and click **OK**.

Setting	Value
IP address	192.168.11.62
Subnet mask	255.255.255.0
Default gateway	192.168.11.1

5 Change the IP address in the DNS that resides in the sfo01.rainpole.local domain for the vra01mssql01 virtual machine.

a Use a Remote Desktop Protocol (RDP) client to login to the DNS server by opening an RDP connection to **`dc01rpl.rainpole.local`**.

b Log in by using the following credentials.

Setting	Value
User name	Active Directory administrator
Password	*ad_admin_password*

c Open the Windows **Start** menu, in the **Search** text box enter **`dnsmgmt.msc`**, and press Enter.

The **DNS Manager** dialog box appears.

d Under **Forward Lookup Zones**, select the **rainpole.local** domain and in the right pane locate vra01mssql01.

e Double-click the **vra01mssql01** record, modify the **IP Address**, and click **OK**.

Setting	Value
Fully qualified domain name (FQDN)	vra01mssql01.rainpole.local
IP Address	192.168.11.62
Update associated pointer (PTR) record	Selected

6 Log in to the SQL Server virtual machine by using a Remote Desktop Protocol (RDP) client.

a Open an RDP connection to the **`vra01mssql01.rainpole.local`** virtual machine.

b Log in by using the following credentials.

Settings	Value
User name	Windows administrator user
Password	*windows_administrator_password*

7 Install vRealize Log Insight Windows Agents in the vra01mssql01 virtual machine.

From the vra01mssql01 Windows environment, 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 by using the following credentials.

Setting	Value
User name	admin
Password	*deployment_admin_password*

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

d Under **Management**, click **Agents** and click the **Download Log Insight Agent Version** link.

e In the **Download Log Insight Agent Version** dialog box, click **Windows MSI (32-bit/64-bit)** and save the `.msi` file to the vra01mssql01 virtual machine.

f Open a command prompt as **Administrator**, and navigate to the directory where you saved the `.msi` file.

g Run the following command and install the vRealize Log Insight agent with custom values.

```
VMware-Log-Insight-Agent-4.7.0-build_number_192.168.31.10.msi SERVERPORT=9000 AUTOUPDATE=yes
LIAGENT_SSL=no
```

h In the **VMware vRealize Log Insight Agent Setup** wizard, accept the license agreement and click **Next**.

i In the **Host** text box, enter sfo01vrli01.sfo01.rainpole.local, and click **Install**.

j Click **Finish**.

8 Log in to vCenter Server by using the vSphere Client.

a Open a Web browser and go to **`https://sfo01w01vc01.sfo01.rainpole.local/ui`**.

b Log in by using the following credentials.

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

9 Power on the remaining vRealize Automation components.

a From the **Home** menu, select **Hosts and Clusters** and expand the **sfo01w01vc01.sfo01.rainpole.local** tree.

b Right-click each of the following virtual machines, according to their startup order, and select **Power > Power on**.

Table 7-2. Startup Order

Product	Virtual Machine Name	Startup Order
vRealize Automation	Total Number of VMs (4)	1
	vra01mssql01	1
	vra01svr01a	2
	vra01iws01a	3
	vra01ims01a	4
vRealize Business for Cloud	Total Number of VMs (2)	2
	vrb01svr01	1
	sfo01vrbc01	2

What to do next

Test your environment to confirm the successful provisioning of virtual machines. See Test the Deployment of a Single Machine Blueprint for Consolidated SDDC.