Certificate Replacement

21 AUG 2018
VMware Validated Design 4.3
VMware Validated Design for Management and Workload Consolidation 4.3

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 Certificate Replacement for Consolidated SDDC 4

1 Certificate Replacement for Consolidated SDDC 6

Create and Add a Microsoft Certificate Authority Template for Consolidated SDDC 7

Generate MSCA-Signed Certificates for the SDDC Management Components for Consolidated SDDC 8

Generate Certificate Signing Requests and Certificates from a Third-Party CA for Consolidated SDDC 11

Replace Certificates of the Virtual Infrastructure Components for Consolidated SDDC 13

Replace the Platform Services Controller Certificates for Consolidated SDDC 14

Replace the vCenter Server Certificates for Consolidated SDDC 17

Replace the ESXi Host Certificates for Consolidated SDDC 23

Replace the NSX Manager Certificates for Consolidated SDDC 27

Replace Certificates of the Operations Management Components for Consolidated SDDC 30

Replace Certificate on the vRealize Suite Lifecycle Manager Appliance for Consolidated SDDC 31

Replace vRealize Operations Manager Certificate for Consolidated SDDC 32

Replace vRealize Log Insight Certificate for Consolidated SDDC 32

Replace Certificates of the Cloud Management Platform Components for Consolidated SDDC 33

Replace the vRealize Automation Certificate for Consolidated SDDC 34

Update the vRealize Automation Certificate on vRealize Orchestrator and vRealize Business for Consolidated SDDC 34

Update the vRealize Automation Certificate on vRealize Operations Manager for Consolidated SDDC 38

Replace the Certificate on vRealize Business for Cloud Server for Consolidated SDDC 38

About VMware Validated Design Certificate Replacement for Consolidated SDDC

VMware Validated Design Certificate Replacement provides step-by-step instructions about replacing certificates on all management components of a running Software-Defined Data Center (SDDC) whose design follows this VMware Validated Design™ for Management and Workload Consolidation.

In a Consolidated SDDC, the security of the environment depends on the validity and trust of the management certificates. As a best practice, you replace management certificates in the following cases:

- Before certificates expire
- When a certificate is compromised.
- When the attributes related to a certificate change, for example, the host name or organization name.

The certificate replacement process consists of the following phases:

1. Obtain certificates for the management components that are signed by a custom certificate authority (CA).
   - Use the VMware Validated Design Certificate Generation utility to automatically generate the certificates for all components.
   - Manually generate Certificate Signing Requests (CSRs) and request CA-signed certificates providing the CSRs to the CA.
2. Replace the certificates in the live SDDC environment.

Intended Audience

The *VMware Validated Design Certificate Replacement* documentation is intended for infrastructure administrators who have deployed a Consolidated SDDC environment using VMware Validated Design for Management and Workload Consolidation.

Required Software

VMware Validated Design Certificate Replacement uses the VMware Validated Design Certificate Generation Utility (CertGenVVD) to generate certificates that are signed by the Microsoft certificate authority (MSCA) for all management products.

VMware Validated Design Certificate Replacement is compliant and validated with certain product versions. See *VMware Validated Design Release Notes* for more information about supported product versions.

Certificate Replacement for Consolidated SDDC

1

In a dual-region environment, you first replace the certificates of the SDDC components in Region A.

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

  The first step in certificate generation and replacement is setting up a Microsoft Certificate Authority template on the Active Directory (AD) servers for the region. The template contains the certificate authority (CA) attributes for signing certificates of VMware SDDC solutions. After you create the new template, you add it to the certificate templates of the Microsoft CA.

- Generate MSCA-Signed Certificates for the SDDC Management Components for Consolidated SDDC

  Use the VMware Validated Design Certificate Generation Utility (`CertGenVVD`) to generate certificates signed by the Microsoft certificate authority (MSCA) for all management products with a single operation.

- Generate Certificate Signing Requests and Certificates from a Third-Party CA for Consolidated SDDC

  Use the VMware Validated Design Certificate Generation Utility (`CertGenVVD`) to generate certificate signing request (CSR) files that you can send to a third-party certificate authority and receive CA-signed certificates for the management components.

- Replace Certificates of the Virtual Infrastructure Components for Consolidated SDDC

  In this design, you replace user-facing certificates with certificates signed by a Microsoft Certificate Authority (CA). If the CA-signed certificates of the management components expire after you deploy the SDDC, you must replace them individually on each affected component.

- Replace Certificates of the Operations Management Components for Consolidated SDDC

  If the certificate of vRealize Operations Manager or vRealize Log Insight expires, replace it and update it on the management components in the region to maintain secure connection.

- Replace Certificates of the Cloud Management Platform Components for Consolidated SDDC

  After you generate signed certificates for the Cloud Management Platform, replace them and update them on the management components in the region to maintain secure connection.

Create and Add a Microsoft Certificate Authority Template for Consolidated SDDC

The first step in certificate generation and replacement is setting up a Microsoft Certificate Authority template on the Active Directory (AD) servers for the region. The template contains the certificate authority (CA) attributes for signing certificates of VMware SDDC solutions. After you create the new template, you add it to the certificate templates of the Microsoft CA.

Creating a certificate authority template for this VMware Validated Design includes the following operations:

1 Set up a Microsoft Certificate Authority template.

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

Prerequisites

This VMware Validated Design sets the Certificate Authority service hierarchies on both Active Directory (AD) servers: the main domain dc01rpl.rainpole.local (root CA) and the subdomain dc01sfo.sfo01.rainpole.local (the intermediate CA).

- Verify that you installed Microsoft Server 2012 R2 VM with Active Directory Domain Services enabled.
- 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 dc01sfo.sfo01.rainpole.local has been set up to be the intermediate CA of the root CA dc01rpl.rainpole.local.
- Use a hashing algorithm of SHA-256 or higher on the certificate authority.

Procedure

1 Log in to the following AD server by using a Remote Desktop Protocol (RDP) client.

Setting	Value
FQDN	■ If you use the intermediate CA, connect to dc01sfo.sfo01.rainpole.local.
User name	Active Directory administrator
Password	*ad_admin_password*

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

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

4 In the **Duplicate Template** window, 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`** as the name of the new template.

7 Click the **Extensions** tab and specify extensions information.
   a Select **Application Policies** and click **Edit**.
   b Select **Server Authentication**, click **Remove**, and click **OK**.
   c Select **Key Usage** and click **Edit**.
   d Select the **Signature is proof of origin (nonrepudiation)** check box.
   e Leave the default for all other options.
   f 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 To add the new template to your CA, click Windows **Start > Run**, enter `certsrv.msc`, and click **OK**.
10 In the **Certification Authority** window, expand the left pane if it is collapsed.
11 Right-click **Certificate Templates** and select **New > Certificate Template to Issue**.
12 In the **Name** column of the **Enable Certificate Templates** dialog box, select the VMware certificate that you created and click **OK**.

Generate MSCA-Signed Certificates for the SDDC Management Components for Consolidated SDDC

Use the VMware Validated Design Certificate Generation Utility (`CertGenVVD`) to generate certificates signed by the Microsoft certificate authority (MSCA) for all management products with a single operation.

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

Prerequisites

- Provide a Window Server 2012 host that is part of the sfo01.rainpole.local domain.
- Install an intermediate Certificate Authority server on the sfo01.rainpole.local domain.

Procedure

1 Log in to a Windows host that has access to your data center.
2 Download the `CertGenVVD-`*`version`*`.zip` file of the Certificate Generation Utility from VMware Knowledge Base article 2146215 on the Windows host where you connect to the data center and extract the ZIP file to the `C:` drive.
3 In the `C:\CertGenVVD-`*`version`* folder, open the `default.txt` file in a text editor.
4 A step under a sfo01w01vc01.

5 Verify that the following properties are configured.

```
ORG=Rainpole Inc.
OU=Rainpole.local
LOC=SFO
ST=CA
CC=US
CN=VMware_VVD
keysize=2048
```

6 Verify that the `C:\CertGenVVD-`*`version`*`\ConfigFiles` folder contains only the following files.

Table 1-1. Certificate Generation Files for Consolidated SDDC

SDDC Layer	Host Name or Service in Consolidated SDDC		Configuration Files
Virtual Infrastructure	Platform Services Controller	sfo01w01psc01.sfo01.rainpole.local	sfo01w01psc01.txt
	vCenter Server	sfo01w01vc01.sfo01.rainpole.local	sfo01w01vc01.txt
	ESXi Hosts	sfo01w01esx01.sfo01.rainpole.local	sfo01w01esx01.txt
		sfo01w01esx02.sfo01.rainpole.local	sfo01w01esx02.txt
		sfo01w01esx03.sfo01.rainpole.local	sfo01w01esx03.txt
		sfo01w01esx04.sfo01.rainpole.local	sfo01w01esx04.txt
	NSX Manager	sfo01w01nsx01.sfo01.rainpole.local	sfo01w01nsx01.txt
Cloud Management Platform	vRealize Automation	■ vra01svr01.rainpole.local ■ vra01svr01a.rainpole.local ■ vra01iws01.rainpole.local ■ vra01iws01a.rainpole.local ■ vra01ims01.rainpole.local ■ vra01ims01a.rainpole.local	vra-for-1-pod.txt
	vRealize Business Server	vrb01svr01.rainpole.local	vrb.txt
Operations Management	vRealize LifeCycle Manager	vrslcm01svr01a.rainpole.local	vrslcm01svr01a.txt

Table 1-1. Certificate Generation Files for Consolidated SDDC (Continued)

SDDC Layer	Host Name or Service in Consolidated SDDC	Configuration Files
	vRealize Operations Manager ■ vrops01svr01.rainpole.local ■ vrops01svr01a.rainpole.local	vrops-for-1-pod.txt
	vRealize Log Insight ■ sfo01vrli01.sfo01.rainpole.local ■ sfo01vrli01a.sfo01.rainpole.local	vrli-for-1-pod.txt

7 Verify that each configuration file includes FQDNs and host names in the dedicated sections.

For example, the configuration file for the Platform Service Controller instance must contain the following properties:

sfo01w01psc01.txt

```
[CERT]
NAME=default
ORG=default
OU=default
LOC=SFO
ST=default
CC=default
CN=sfo01w01psc01.sfo01.rainpole.local
keysize=default
[SAN]
sfo01w01psc01.sfo01.rainpole.local
```

8 Open a Windows PowerShell prompt and navigate to the `CertGenVVD` folder.

```
cd C:\CertGenVVD-version
```

9 Grant permissions to run third-party PowerShell scripts.

```
Set-ExecutionPolicy Unrestricted
```

10 Validate if you can run the utility using the configuration on the host and verify if VMware is included in the printed CA template policy.

```
.\CertgenVVD-version.ps1 -validate
```

11 Generate MSCA-signed certificates.

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

12 In the `C:\CertGenVVD-version` folder, verify that the utility created the `SignedByMSCACerts` subfolder.

13 In C:\CertGenVVD–*version**SignedByMSCACerts**Root64* subfolder, rename chainRoot64.cer to Root64.cer.

What to do next

Replace the product certificates with the certificates that the CertGenVVD utility has generated. See Replace Certificates of the Virtual Infrastructure Components for Consolidated SDDC, Replace Certificates of the Operations Management Components for Consolidated SDDC, and Replace Certificates of the Cloud Management Platform Components for Consolidated SDDC.

Generate Certificate Signing Requests and Certificates from a Third-Party CA for Consolidated SDDC

Use the VMware Validated Design Certificate Generation Utility (CertGenVVD) to generate certificate signing request (CSR) files that you can send to a third-party certificate authority and receive CA-signed certificates for the management components.

Prerequisites

- Provide a Windows Server 2012 host that has access to your data center.

Procedure

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

2 Download the CertGenVVD–*version*.zip file of the Certificate Generation Utility from VMware Knowledge Base article 2146215 on the Windows host where you connect to the data center and extract the ZIP file to the C: drive.

3 In the C:\CertGenVVD–*version* folder, open the default.txt file in a text editor.

4 Verify that following properties are configured.

```
ORG=Rainpole Inc.
OU=Rainpole.local
LOC=SFO
ST=CA
CC=US
CN=VMware_VVD
keysize=2048
```

5 Verify that only the C:\CertGenVVD–*version*\ConfigFiles folder contains only following files.

Table 1-2. Certificate Generation Files for Consolidated SDDC

Host Name or Service in Consolidated SDDC		Configuration Files
Platform Services Controller	sfo01w01psc01.sfo01.rainpole.local	sfo01w01psc01.txt
vCenter Server	sfo01w01vc01.sfo01.rainpole.local	sfo01w01vc01.txt
ESXi Hosts	sfo01w01esx01.sfo01.rainpole.local	sfo01w01esx01.txt
	sfo01w01esx02.sfo01.rainpole.local	sfo01w01esx02.txt

Table 1-2. Certificate Generation Files for Consolidated SDDC (Continued)

Host Name or Service in Consolidated SDDC		Configuration Files
	sfo01w01esx03.sfo01.rainpole.local	sfo01w01esx03.txt
	sfo01w01esx04.sfo01.rainpole.local	sfo01w01esx04.txt
NSX Manager	sfo01w01nsx01.sfo01.rainpole.local	sfo01w01nsx01.txt
vSphere Data Protection	sfo01w01vdp01.sfo01.rainpole.local	sfo01w01vdp01.txt
vRealize Automation	■ vra01svr01.rainpole.local ■ vra01svr01a.rainpole.local ■ vra01iws01.rainpole.local ■ vra01iws01a.rainpole.local ■ vra01ims01.rainpole.local ■ vra01ims01a.rainpole.local	vra-for-1-pod.txt
vRealize Business Server	vrb01svr01.rainpole.local	vrb.txt
vRealize Operations Manager	■ vrops01svr01.rainpole.local ■ vrops01svr01a.rainpole.local	vrops-for-1-pod.txt
vRealize Log Insight	■ sfo01vrli01.sfo01.rainpole.local ■ sfo01vrli01a.sfo01.rainpole.local	vrli-for-1-pod.txt

6 Verify that each configuration file includes FQDN and host names in the dedicated sections.

For example, the configurations files for the Platform Service Controller instances must contain the following properties:

sfo01w01psc01.txt

```
[CERT]
NAME=default
ORG=default
OU=default
LOC=SFO
ST=default
CC=default
CN=sfo01w01psc01.sfo01.rainpole.local
keysize=default
[SAN]
sfo01w01psc01.sfo01.rainpole.local
```

7 Open a Windows PowerShell prompt and navigate to the folder of the CertGenVVD utility.

```
cd C:\CertGenVVD-version
```

8 Grant permissions to run third-party PowerShell scripts.

```
Set-ExecutionPolicy Unrestricted
```

9 Validate if you can run the utility using the configuration on the host and verify if VMware is included in the printed CA template policy.

```
.\CertgenVVD-version.ps1 -validate
```

10 Generate certificate request files for the management components in the SDDC.

```
.\CertGenVVD-version.ps1 -CSR
```

11 Locate the CSR files in the `C:\CertGenVVD-version\CSRCerts` folder and send it to the third-party CA to request the signed certificates.

12 After you obtain all the signed certificate files and the root CA certificate, move the signed certificate files back to each directory where the CSR files reside.

13 In a command prompt, navigate to the folder that contains the CA root certificate and rename it to `Root64.cer`.

14 If the certificates are signed by multiple intermediate CAs, concatenate the certificates in one certificate chain file by running the following command.

```
copy IntermediateCAroot01.cer+IntermediateCAroot02.cer+RootCA.cer > Root64.cer
```

15 Move the `Root64.cer` to the `C:\CertGenVVD-version\CSRCerts\Root64` folder.

16 Run `CertGenVVD` tool with the `-CSR` and `-extra` command options to generate all certificates that are required for the SDDC management components.

```
.\CertGenVVD-version.ps1 -CSR -extra
```

What to do next

Replace the product certificates with the certificates that the `CertGenVVD` utility has generated. See Replace Certificates of the Virtual Infrastructure Components for Consolidated SDDC, Replace Certificates of the Operations Management Components for Consolidated SDDC, and Replace Certificates of the Cloud Management Platform Components for Consolidated SDDC.

Replace Certificates of the Virtual Infrastructure Components for Consolidated SDDC

In this design, you replace user-facing certificates with certificates signed by a Microsoft Certificate Authority (CA). If the CA-signed certificates of the management components expire after you deploy the SDDC, you must replace them individually on each affected component.

By default, virtual infrastructure management components use TLS/SSL certificates that are signed by the VMware Certificate Authority (VMCA).

Infrastructure administrators connect to different SDDC components, such as vCenter Server systems or a Platform Services Controller, from a Web browser to perform configuration, management, and troubleshooting. The authenticity of the network node to which the administrator connects must be confirmed with a valid TLS/SSL certificate.

You can use other certificate authorities according to the requirements of your organization. You do not replace certificates for machine-to-machine communication. If necessary, you can manually mark these certificates as trusted.

Procedure

1 Replace the Platform Services Controller Certificates for Consolidated SDDC

2 Replace the vCenter Server Certificates for Consolidated SDDC

Replace the certificate on each vCenter Server instance for Consolidated SDDC and reconnect it to the other management components to update the new certificate on these components.

3 Replace the ESXi Host Certificates for Consolidated SDDC

Replace the default or expired certificates on the ESXi hosts with certificates that are generated by using the `CertGenVVD` utility.

4 Replace the NSX Manager Certificates for Consolidated SDDC

Replace the certificate on an NSX Manager instance, for example, if it is about to expire, and update it on the management components connected to this instance.

Replace the Platform Services Controller Certificates for Consolidated SDDC

Replace the certificate of the Platform Services Controller instance. Reconnect the Platform Services Controller instance to the vCenter Server and NSX Manager instances to update the certificates for vCenter Single Sign-on on these components.

Procedure

1 Replace the Platform Services Controller Certificates for Consolidated SDDC

To establish trusted connection with the other SDDC management components, you replace the default or expiring machine SSL certificate on each Platform Services Controller instance in the region with a custom certificate. The certificate, generated by the `CertGenVVD` utility, is signed by the certificate authority (CA) available on the parent Active Directory (AD) server or on the intermediate Active Directory (AD) server.

2 Update the Platform Services Controller Certificates on the Management Components for Consolidated SDDC

After you replace the certificate on a Platform Services Controller instance, update the certificate on the vCenter Server and NSX Manager instances in the region.

What to do next

If you replace the certificates of vCenter Server after those of the Platform Services Controllers, see Replace the Certificate of vCenter Server for Consolidated SDDC.

Replace the Platform Services Controller Certificates for Consolidated SDDC

To establish trusted connection with the other SDDC management components, you replace the default or expiring machine SSL certificate on each Platform Services Controller instance in the region with a custom certificate. The certificate, generated by the `CertGenVVD` utility, is signed by the certificate authority (CA) available on the parent Active Directory (AD) server or on the intermediate Active Directory (AD) server.

Table 1-3. Certificate-Related Files on Platform Services Controller Instance

Platform Services Controller	Certificate Filename
sfo01w01psc01.sfo01.rainpole.local	■ sfo01w01psc01.1.cer ■ sfo01w01psc01.key ■ Root64.cer

Procedure

1 Open a Secure SHell connection to the Platform Services Controller virtual machine.

   a Open an SSH connection to sfo01w01psc01.sfo01.rainpole.local.

   b Log in using the following credentials.

Setting	Value
User name	root
Password	*psc_root_password*

2 To allow secure copy (`scp`) connections for the root user, change the Platform Services Controller command shell to the Bash shell.

```
shell
chsh –s "/bin/bash" root
```

3 Copy the generated certificates to the Platform Services Controller.

   a To create a new temporary folder, run the following command.

```
mkdir –p /root/certs
```

   b Copy the certificate files `sfo01w01psc01.1.cer`, `sfo01w01psc01.key`, and `Root64.cer` to the `/root/certs` folder.

   You can use an `scp` software like WinSCP.

4 Replace the certificate on the Platform Services Controller.

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

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

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

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

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

   e When prompted for the custom certificate, enter **/root/certs/sfo01w01psc01.1.cer**.

   f When prompted for the custom key, enter **/root/certs/sfo01w01psc01.key**.

   g When prompted for the signing certificate, enter **/root/certs/Root64.cer**.

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

   The Platform Services Controller services automatically restart.

5 Verify that the new certificate has been installed successfully.

   a Open a Web Browser and go to **https://sfo01w01psc01.sfo01.rainpole.local**.

   b Verify that the Web browser shows the new certificate.

6 After Certificate Manager replaces the certificates, restart the vami-lighttp service to update the certificate in the virtual application management interface (VAMI) and to remove certificate files from Platform Services Controller.

   ```
   service vami-lighttp restart
   cd /root/certs

   rm sfo01w01psc01.1.cer sfo01w01psc01.key Root64.cer
   ```

7 Switch the shell back to the appliance shell.

   ```
   chsh -s /bin/appliancesh root
   ```

Update the Platform Services Controller Certificates on the Management Components for Consolidated SDDC

After you replace the certificate on a Platform Services Controller instance, update the certificate on the vCenter Server and NSX Manager instances in the region.

Procedure

1 Log in to vCenter Server by using Secure Shell (SSH) client.

a Open an SSH connection to the sfo01w01vc01.sfo01.rainpole.local virtual machine.

b Log in using the following credentials.

Setting	Value
User name	root
Password	*vcenter_server_root_password*

2 Restart the services of vCenter Server.

a Switch from the vCenter Server Appliance command shell to the Bash shell.

```
shell
```

b Restart vCenter Server services by using the following command.

```
service-control --stop --all
service-control --start --all
```

3 Reconnect NSX Manager to Platform Services Controller and vCenter Server after you install the custom certificates on the nodes.

See Connect NSX Manager to vCenter Server for Consolidated SDDC.

Replace the vCenter Server Certificates for Consolidated SDDC

Replace the certificate on each vCenter Server instance for Consolidated SDDC and reconnect it to the other management components to update the new certificate on these components.

Procedure

1 Replace the Certificate of vCenter Server for Consolidated SDDC

To establish trusted connection with the other SDDC components, you replace the machine SSL certificate on each vCenter Server instance in the region with a custom certificate. The certificate, generated by the CertGenVVD utility, is signed by the certificate authority (CA) available on the parent Active Directory (AD) server or on the intermediate Active Directory (AD) server.

2 Connect NSX Manager to vCenter Server for Consolidated SDDC

3 Update the Certificate of vCenter Server on the Cloud Management Platform for Consolidated SDDC

After you replace the certificate on the vCenter Server instance for Consolidated SDDC, reconnect vRealize Orchestrator, vRealize Business, and vRealize Automation to vCenter Server to update the vCenter Server certificate on the Cloud Management Platform.

4 Update the vCenter Server Certificates on vRealize Operations Managerfor Consolidated SDDC

After you change the certificate of a vCenter Server instance for Consolidated SDDC, update the certificates on the connected vRealize Operations Manager node by reconnecting the vCenter Adapter and vSAN Adapter instances.

Replace the Certificate of vCenter Server for Consolidated SDDC

To establish trusted connection with the other SDDC components, you replace the machine SSL certificate on each vCenter Server instance in the region with a custom certificate. The certificate, generated by the CertGenVVD utility, is signed by the certificate authority (CA) available on the parent Active Directory (AD) server or on the intermediate Active Directory (AD) server.

Table 1-4. Certificate-Related Files on the vCenter Server Instance

vCenter Server FQDN	Files for Certificate Replacement
sfo01w01vc01.sfo01.rainpole.local	■ sfo01w01vc01.key ■ sfo01w01vc01.1.cer ■ Root64.cer

Procedure

1 Log in to vCenter Server by using Secure Shell (SSH) client.

a Open an SSH connection to the sfo01w01vc01.sfo01.rainpole.local virtual machine.

b Log in using the following credentials.

Setting	Value
User name	root
Password	*vcenter_server_root_password*

2 To allow secure copy (`scp`) connections for the root user, change the vCenter Server Appliance command shell to the Bash shell .

```
shell
chsh –s "/bin/bash" root
```

3 Copy the generated certificates to the vCenter Server Appliance.

a Run the following command to create a new temporary folder.

```
mkdir –p /root/certs
```

b Copy the certificate files `sfo01w01vc01.1.cer`, `sfo01w01vc01.key`, and `Root64.cer` to the `/root/certs` folder.

You can use an `scp` software such as WinSCP.

4 Replace the CA-signed certificate on the vCenter Server instance.

a Start the vSphere Certificate Manager utility on the vCenter Server instance.

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

b Select **Option 1 (Replace Machine SSL certificate with Custom Certificate)**, enter the default vCenter Single Sign-On user name **`administrator@vsphere.local`** and the ***`vsphere_admin_password`*** password.

c When prompted for the Infrastructure Server IP, enter the IP address of the Platform Services Controller that manages this vCenter Server instance.

vCenter Server instance	IP Address of managing Platform Services Controller
sfo01w01vc01.sfo01.rainpole.local	172.16.11.63

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

e When prompted, provide the full path to the custom certificate, the root certificate file, and the key file that you copied over earlier, and confirm the import with **Yes (Y)**.

vCenter Server	Input to the vSphere Certificate Manager Utility
sfo01w01vc01.sfo01.rainpole.local	Please provide valid custom certificate for Machine SSL. File : **`/root/certs/sfo01w01vc01.1.cer`** Please provide valid custom key for Machine SSL. File : **`/root/certs/sfo01w01vc01.key`** Please provide the signing certificate of the Machine SSL certificate. File : **`/root/certs/Root64.cer`**

5 When status shows `100% Completed`, wait several minutes until all vCenter Server services are restarted.

6 Open the vSphere Web Client to verify that certificate replacement is successful.

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

b Verify that you see the new certificate.

7 Restart the vami-lighttp service to update the certificate on the virtual appliance management interface (VAMI) and to remove certificate files.

```
service vami-lighttp restart
cd /root/certs/
rm sfo01w01vc01.1.cer sfo01w01vc01.key Root64.cer
```

Connect NSX Manager to vCenter Server for Consolidated SDDC

After you replace the certificates of the Platform Services Controller and vCenter Server instances for Consolidated SDDC, you reconnect the NSX Manager instances to the Platform Services Controller and vCenter Server nodes in the region to update the certificates on NSX Manager.

Procedure

1 Log in to the NSX Manager appliance user interface.

   a Open a Web browser and go to **`https://sfo01w01nsx01.sfo01.rainpole.local`**.

   b Log in using the following credentials.

Setting	Value
User name	admin
Password	*nsx_manager_admin_password*

2 Click **Manage vCenter Registration**.

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

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

Setting	Value
Lookup Service Host	sfo01w01psc01.sfo01.rainpole.local
Lookup Service Port	443
SSO Administrator User Name	administrator@vsphere.local
Password	*vsphere_admin_password*

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

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

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

Setting	Value
vCenter Server	sfo01w01vc01.sfo01.rainpole.local
vCenter User Name	svc-nsxmanager@rainpole.local
Password	*svc-nsxmanager_password*

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

9 Wait for the **Status** indicators for the Lookup Service URL and vCenter Server to change to the `Connected` status.

Update the Certificate of vCenter Server on the Cloud Management Platform for Consolidated SDDC

After you replace the certificate on the vCenter Server instance for Consolidated SDDC, reconnect vRealize Orchestrator, vRealize Business, and vRealize Automation to vCenter Server to update the vCenter Server certificate on the Cloud Management Platform.

Procedure

1 Reconnect vRealize Orchestrator to vCenter Server.

   a Open a Web Browser and go to **`https://vra01svr01.rainpole.local/vco`**.

   b Click **Start Orchestrator Client**.

   c On the **VMware vRealize Orchestrator** login page, log in to the embedded vRealize Orchestrator by using the following host name and credentials.

Setting	Value
Host name	https://vra01svr01.rainpole.local:443
User name	svc-vra
Password	*svc-vra-password*

   d In the left pane, click **Workflows**, and navigate to **Library > vCenter > Configuration**.

   e Right-click the **Update a vCenter Server instance** workflow and click **Start Workflow**.

   f From the **vCenter Server instance** drop-down menu, select **https://sfo01w01vc01.sfo01.rainpole.local:443/sdk** and click **Next**.

   g On **Start Workflow: Update a vCenter Server instance** tab, click **Next**.

   h Enter the password for the svc-vro@rainpole.local user account and click **Submit**.

   i On the certificate warning windows click, **Next**.

   j Select **Yes** to import the certificate and click **Submit**.

2 Reconnect vRealize Business to vCenter Server.

   a Open a Web browser and go to **`https://sfo01vrbc01.sfo01.rainpole.local:9443/dc-ui:9443/dc-ui`**.

   b Log in using the following credentials.

Setting	Value
User name	root
Password	*vrb_root_password*

   c Click **Manage Private Cloud Connections**, select **vCenter Server**, select the **sfo01w01vc01.sfo01.rainpole.local** entry, and click the **Edit** icon.

d In the **Edit vCenter Server Connection** dialog box, enter the password for the svc-vra@rainpole.local user and click **Save**.

e In the **SSL Certificate warning** dialog box, click **Install**.

f In the **Success** dialog box, click **OK**.

3 Recreate the vSphere endpoint in vRealize Automation.

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

b Log in using the following credentials.

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

c Navigate to **Infrastructure > Endpoints > Endpoints**.

d Point to **sfo01w01vc01.sfo01.rainpole.local** and click **Edit** from the menu.

e On the **Edit Endopint - vSphere (vCenter)** page, click **OK**.

f In the certificate warning dialog box, click **OK** to accept the new certificate .

Update the vCenter Server Certificates on vRealize Operations Manager for Consolidated SDDC

After you change the certificate of a vCenter Server instance for Consolidated SDDC, update the certificates on the connected vRealize Operations Manager node by reconnecting the vCenter Adapter and vSAN Adapter instances.

Procedure

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

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

b Log in using the following credentials.

Setting	Value
User name	admin
Password	*vrops_admin_password*

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

3 In the left pane of vRealize Operations Manager, under **Management**, click **Certificates**.

4 Select the row that contains `CN=sfo01w01vc01.sfo01.rainpole.local` and click the **Delete** icon.

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

6 Reconnect each vCenter Adapter.

   a Select the **VMware vSphere** solution and click **Configure**.

   b In the **Manage Solutions** dialog box, select **vCenter Adapter - sfo01w01vc01**, click **Test Connection**, accept the new certificate of vCenter Server, and click **Save Settings**.

7 Reconnect the VMware vSAN adapter for the management cluster.

   a Select the **VMware vSAN** solution and click **Configure**.

   b In the **Manage Solutions** dialog box, select **vSAN Adapter - sfo01w01vc01**, click **Test Connection**, accept the new certificate of the Management vCenter Server, and click **Save Settings**.

8 Reconnect the Management Pack for Storage adapter for the management cluster.

   a Select the **Management Pack for Storage Devices** solution and click **Configure**.

   b In the **Manage Solutions** dialog box, select **Storage Devices Adapter - sfo01w01vc01**, click **Test Connection**, accept the new certificate of vCenter Server, and click **Save Settings**.

Replace the ESXi Host Certificates for Consolidated SDDC

Replace the default or expired certificates on the ESXi hosts with certificates that are generated by using the `CertGenVVD` utility.

In each cluster, you configure the certificate mode for hosts to support custom certificate authorities (CAs) and replace the old certificates with certificates that are signed by a custom CA.

Procedure

1 Set Host Certificate Mode on vCenter Server to Support a Custom Certificate Authority for Consolidated SDDC

   By default the ESXi hosts are automatically provisioned with VMware Certificate Authority (VMCA) certificates when they are connected to vCenter Server. You set the host certificate mode on vCenter Server to support a custom certificate authority to prevent the vCenter Server from replacing certificates on to the ESXi hosts.

2 Replace the Default Certificates with Custom Certificates on the ESXi Hosts for Consolidated SDDC

   After you obtain signed certificates for the ESXi hosts in the region and configure vCenter Server to accept custom certificate authorities, replace the default VMware Certificate Authority (VMCA) signed certificates with the custom ones on the hosts.

Set Host Certificate Mode on vCenter Server to Support a Custom Certificate Authority for Consolidated SDDC

By default the ESXi hosts are automatically provisioned with VMware Certificate Authority (VMCA) certificates when they are connected to vCenter Server. You set the host certificate mode on vCenter Server to support a custom certificate authority to prevent the vCenter Server from replacing certificates on to the ESXi hosts.

vCenter Server	ESXi Host
sfo01w01vc01.sfo01.rainpole.local	sfo01w01esx01.sfo01.rainpole.local
	sfo01w01esx02.sfo01.rainpole.local
	sfo01w01esx03.sfo01.rainpole.local
	sfo01w01esx04.sfo01.rainpole.local

Procedure

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

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

   b Log in using the following credentials.

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

2 Verify that all CA certificates from vCenter Server are updated on all hosts.

   a In the **Navigator**, under **Hosts and Cluster**, select **sfo01w01esx01.sfo01.rainpole.local**, and click the **Configure** tab.

   b Under **System**, select **Certificate** and click **Refresh CA Certificates**.

   c Repeat the steps for the ESXi hosts that are controlled by the vCenter Server sfo01w01vc01.sfo01.rainpole.local.

3 Change the certificate mode for the ESXi hosts in the consolidated cluster to **`custom`** .

   a In the **Navigator**, under **Hosts and Cluster**, select **sfo01w01vc01.sfo01.rainpole.local**, and click the **Configure** tab.

   b Under **Settings**, click **Advanced Settings** and click **Edit**.

   c In the filter box, enter **`certmgmt`** and press Enter to view only certificate management properties.

   d Change the value of the `vpxd.certmgmt.mode` property to **`custom`** and click **OK**.

4 Restart the vCenter Server Appliance to apply the changes.

   a Open a Web browser and go to **`https://sfo01w01vc01.sfo01.rainpole.local:5480`**

   b Log in using the following credentials.

Settings	Values
User name	root
Password	*vcenter_server_root_password*

   c Click **Reboot** to restart the vCenter Server Appliance.

Replace the Default Certificates with Custom Certificates on the ESXi Hosts for Consolidated SDDC

After you obtain signed certificates for the ESXi hosts in the region and configure vCenter Server to accept custom certificate authorities, replace the default VMware Certificate Authority (VMCA) signed certificates with the custom ones on the hosts.

You replace the certificate separately on each host in the management cluster.

Table 1-5. Certificate Files Names for the Hosts in the Consolidated SDDC

ESXi Hosts	Certificate Filenames
sfo01w01esx01.sfo01.rainpole.local	■ sfo01w01esx01.key ■ sfo01w01esx01.1.cer
sfo01w01esx02.sfo01.rainpole.local	■ sfo01w01esx02.key ■ sfo01w01esx02.1.cer
sfo01w01esx03.sfo01.rainpole.local	■ sfo01w01esx03.key ■ sfo01w01esx03.1.cer
sfo01w01esx04.sfo01.rainpole.local	■ sfo01w01esx04.key ■ sfo01w01esx04.1.cer

Procedure

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

   a Open a Web browser and go to `https://sfo01w01vc01.sfo01.rainpole.local/vsphere-client`.

   b Log in using the following credentials.

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

2 Disable lockdown mode on the sfo01w01esx01.sfo01.rainpole.local host.

   a From the **Home** menu of the vSphere Web Client, select **Hosts and Clusters**.

   b Under the **sfo01-w01dc** data center, select the **sfo01w01esx01.sfo01.rainpole.local** host object and click the **Configure** tab on the right.

   c Under **System**, click **Security Profile**, scroll down to **Lockdown Mode**, and click **Edit**.

   d In the **Lockdown Mode** dialog box, select **Disabled** and click **OK**.

   e Scroll up to the **Services** pane and click **Edit**.

   f In **Edit Security Profile** dialog box, select **SSH**.

   g Click the **Start** button if the status is not showing up as **Running**

   h Click **OK** to close the **Edit Security Profile** dialog box.

3 Place the host in maintenance mode.

   a Under the sfo01-w01dc data center, right-click the **sfo01w01esx01.sfo01.rainpole.local** host object and select **Maintenance Mode > Enter Maintenance Mode**.

   b In the **Confirm Maintenance Mode** dialog box, select **Move powered-off and suspended virtual machines to other hosts in the cluster** and click **OK**.

4 Replace the certificate files on the host.

   a After the maintenance task is complete, open an SSH connection to the sfo01w01esx01.sfo01.rainpole.local host using the following credentials.

Option	Description
User name	root
Password	*esxi_root_user_password*

   b Copy the `sfo01w01esx01.key` and `sfo01w01esx01.1.cer` files from the Windows host where you run the `CertGenVVD` tool to the `/etc/vmware/ssl` directory on the host.

   c Run the following commands to back up the present certificate and key files and to replace them with the generated files.

```
cd /etc/vmware/ssl
cat rui.crt >> rui.bak
cat rui.key >> rui.bak
mv sfo01w01esx01.key rui.key
mv sfo01w01esx01.1.cer rui.crt
```

5 Restart the management agents on the host.

   a Run the `dcui` command to open the Direct Console User Interface (DCUI).

   b Press the F12 key to access the **System Customization** menu.

   c Select **Troubleshooting Options** and press Enter.

   d Select **Restart Management Agents** and press Enter.

   e Press F11 key to confirm the restart and press Enter to confirm completion.

   f Press Control+C to close DCUI application.

   g Run the following commands to restart the vsanvpd and vsanmgmtd services

```
/etc/init.d/vsanvpd restart
/etc/init.d/vsanmgmtd restart
```

6 Verify that the custom certificate is installed.

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

   b Verify that the certificate returned by the host is signed by *Rainpole* instead of by VMware.

7 Exit maintenance mode of the host.

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

b Log in using the following credentials.

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

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

d Under the sfo01-w01dc data center, right-click the **sfo01w01esx01.sfo01.rainpole.local** host object and select **Maintenance Mode > Exit Maintenance Mode**.

e Make sure that no warning message about an untrusted sfo01w01esx01.sfo01.rainpole.locall certificate appears.

8 Reconnect the ESXi host to vCenter Server to refresh the host certificate on vCenter Server.

a Under the sfo01-w01dc data center, right-click the **sfo01w01esx01.sfo01.rainpole.local** host object and select **Connection > Disconnect**.

b Click **Yes** in the **Confirm Disconnect** pop-up window.

c Wait until the host is disconnected.

d Right-click the **sfo01w01esx01.sfo01.rainpole.local** host object and select **Connection > Connect**.

e On the **Configure** tab, under **System**, select **Certificates** and verify that the certificate displayed for the host is the new one.

9 Verify that the storage providers are online for the ESXi host.

a Select the **sfo01w01vc01.sfo01.rainpole.local** vCenter Server object and click the **Configure** tab.

b Under **More**, select **Storage Providers**.

c Verify that the status for the `http://sfo01w01esx01.sfo01.rainpole.local:8080/version.xml` URL of the vSAN storage provider is `Online`.

d If the status of the URL is different from `Online`, select the URL, click the **Unregister the selected storage provider** icon, and click **Synchronizes all the storage providers with the current states of the environment** icon.

10 Repeat the procedure for the rest of the ESXi hosts in the region.

Replace the NSX Manager Certificates for Consolidated SDDC

Replace the certificate on an NSX Manager instance, for example, if it is about to expire, and update it on the management components connected to this instance.

Procedure

1 Replace the Certificate of NSX Manager for Consolidated SDDC

2 Connect NSX Manager to vCenter Server for Consolidated SDDC

3 Reconnect NSX Manager for Consolidated SDDC to vRealize Operations Manager

After you replace the certificate on each NSX Manager instance in the region, reconnect the NSX adapter in vRealize Operations Manager to update the certificate on vRealize Operations Manager.

Replace the Certificate of NSX Manager for Consolidated SDDC

After you replace the certificates of all Platform Services Controller instances and all vCenter Server instances, replace the expiring certificates for the NSX Manager instances.

Use the following certificate file to replace the certificate on the NSX Manager instance:

Table 1-6. Certificate-Related Files on the NSX Manager Instance for Consolidated SDDC

NSX Manager FQDN	Certificate Filename
sfo01w01nsx01.sfo01.rainpole.local	sfo01w01nsx01.sfo01.4.p12

Procedure

1 Log in to the NSX Manager appliance user interface.

a Open a Web browser and go to **`https://sfo01w01nsx01.sfo01.rainpole.local`**.

b Log in using the following credentials.

Setting	Value
User name	admin
Password	*nsx_manager_admin_password*

2 On the **Home** page, select **Manage Appliance Settings**.

3 On the **Manage** tab, click **SSL Certificates**, click **Upload PKCS#12 Keystore**.

4 Browse to the certificate chain file `sfo01w01nsx01.4.p12`, provide the keystore password or passphrase, and click **Import**.

5 Restart the NSX Manager to propagate the CA-signed certificate.

a In the right corner of the **NSX Manager** page, click the **Settings** icon.

b From the drop-down menu, select **Reboot Appliance**.

c On the **Reboot Confirmation** dialog box, click **Yes**.

Connect NSX Manager to vCenter Server for Consolidated SDDC

After you replace the certificate of an NSX Manager instance, you reconnect it to Platform Services Controller and vCenter Server to update the certificate on these components.

Procedure

1 Log in to the NSX Manager appliance user interface.

   a Open a Web browser and go to **`https://sfo01w01nsx01.sfo01.rainpole.local`**.

   b Log in using the following credentials.

Setting	Value
User name	admin
Password	*nsx_manager_admin_password*

2 Click **Manage vCenter Registration**.

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

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

Setting	Value
Lookup Service Host	sfo01w01psc01.sfo01.rainpole.local
Lookup Service Port	443
SSO Administrator User Name	administrator@vsphere.local
Password	*vsphere_admin_password*

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

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

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

Setting	Value
vCenter Server	sfo01w01vc01.sfo01.rainpole.local
vCenter User Name	svc-nsxmanager@rainpole.local
Password	*svc-nsxmanager_password*

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

9 Wait for the **Status** indicators for the Lookup Service URL and vCenter Server to change to the `Connected` status.

Reconnect NSX Manager for Consolidated SDDC to vRealize Operations Manager

After you replace the certificate on each NSX Manager instance in the region, reconnect the NSX adapter in vRealize Operations Manager to update the certificate on vRealize Operations Manager.

Procedure

1 Log in to vRealize Operations Manager master node by using the administration interface.

   a Open a Web browser and go to **`https://vrops01svr01a.rainpole.local`**.

   b Log in using the following credentials.

Setting	Value
User name	admin
Password	*vrops_admin_password*

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

3 In the left pane of vRealize Operations Manager, under **Management**, click **Certificates**.

4 Delete the certificates with the following CNs.

   ◆ `CN=sfo01w01nsx01.sfo01.rainpole.local`

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

6 From the solution table on the **Solutions** page, select the **Management Pack for NSX-vSphere** solution, and click the **Configure** icon.

7 In the **Manage Solutions** dialog box, from the **Adapter Type** table, select **NSX-vSphere Adapter**.

8

9 Click the **sfo01w01nsx01-sfo01** adapter instance, click **Test Connection**, accept the new certificate, click **Save settings**, and click **Close**.

Replace Certificates of the Operations Management Components for Consolidated SDDC

If the certificate of vRealize Operations Manager or vRealize Log Insight expires, replace it and update it on the management components in the region to maintain secure connection.

Procedure

1 Replace Certificate on the vRealize Suite Lifecycle Manager Appliance for Consolidated SDDC

   To establish a trusted connection to vRealize Suite Lifecycle Manager, you replace the SSL certificate on the appliance with a custom certificate signed by a certificate authority available on the parent Active Directory or on the intermediate Active Directory.

2 Replace vRealize Operations Manager Certificate for Consolidated SDDC

   Log in to the administrator interface of the master node of vRealize Operations Manager and use the `PEM` file generated by the CertGenVVD utility to replace the current certificate.

3 Replace vRealize Log Insight Certificate for Consolidated SDDC

   Update the certificate chain of vRealize Log Insight to use a trusted non-default certificate after deployment or to replace a certificate that is soon to expire. In this way, connection to the vRealize Log Insight user interface remains trusted.

Replace Certificate on the vRealize Suite Lifecycle Manager Appliance for Consolidated SDDC

To establish a trusted connection to vRealize Suite Lifecycle Manager, you replace the SSL certificate on the appliance with a custom certificate signed by a certificate authority available on the parent Active Directory or on the intermediate Active Directory.

Procedure

1 Rename the certificates generated using the VMware Validated Design Certificate Generation Utility for vrslcm01svr01a.rainpole.local.

Original Certificate Filename	New Certificate Filename
vrslcm01svr01a.2.chain.pem	server.crt
vrslcm01svr01a-orig.key	server.key

2 Overwrite the existing `server.crt` and `server.key` files in the `/opt/vmware/vlcm/cert` directory with the previously generated CA signed certificate files.

You can use SCP software like WinSCP.

3 Log in to vRealize Suite Lifecycle Manager appliance by using Secure Shell (SSH) client.

a Open an SSH connection to vrslcm01svr01a.rainpole.local.

b Log in using following credentials.

Setting	Value
User name	root
Password	*vrslcm_root_password*

4 Restart the vRealize Suite Lifecycle Manager services to update the appliance certificate.

a Restart the system services by running the following command in the SSH session.

```
systemctl restart vlcm-xserver
```

b Check the status of the system services by running the following command in the SSH session.

```
systemctl status vlcm-xserver
```

5 After restarting the services, verify that the certificate is updated on the appliance.

a Close any opened Web browsers, open a new Web browser window, and go to **`https://vrslcm01svr01a.rainpole.local/vrlcm`**.

b Verify that you see the new certificate in the browser.

Replace vRealize Operations Manager Certificate for Consolidated SDDC

Log in to the administrator interface of the master node of vRealize Operations Manager and use the `PEM` file generated by the CertGenVVD utility to replace the current certificate.

Procedure

1 Log in to vRealize Operations Manager master node by using the administration interface.

   a Open a Web browser and go to **`https://vrops01svr01a.rainpole.local`**/admin.

   b Log in using the following credentials.

Setting	Value
User name	admin
Password	*vrops_admin_password*

2 At the upper right corner of the user interface, click the **SSL Certificate** icon.

3 In the **SSL Certificate** dialog box, click **Install New Certificate**.

4 In the **Install New Certificate** dialog box, click **Browse**, locate the `vrops-for-1-pod.2.chain.pem` PEM file, and click **Open**.

5 In the **Install New Certificate** dialog box, verify the certificate details, and click **Install**.

Replace vRealize Log Insight Certificate for Consolidated SDDC

Update the certificate chain of vRealize Log Insight to use a trusted non-default certificate after deployment or to replace a certificate that is soon to expire. In this way, connection to the vRealize Log Insight user interface remains trusted.

Procedure

1 Log in to the vRealize Log Insight user interface.

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

   b Log in using the following credentials.

Setting	Value
User name	admin
Password	*vrli_admin_password*

2 In the vRealize Log Insight user interface, click the configuration drop-down menu icon and select **Administration**.

3 Under **Configuration**, click **SSL**.

4 On the **SSL Configuration** page, next to **New Certificate File (PEM format)** click **Choose File**, browse to the location of the PEM file on your computer, and click **Save**.

Certificate Generation Option	Certificate File
Using the CertGenVVD tool	`vrli-for-1-pod.2.chain.pem`

The certificate is uploaded to vRealize Log Insight.

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

A warning message that the connection is not trusted appears.

6 To review the certificate, click the padlock icon in the address bar of the browser, and verify that **Subject Alternative Name** contains the names of the vRealize Log Insight cluster nodes.

Replace Certificates of the Cloud Management Platform Components for Consolidated SDDC

After you generate signed certificates for the Cloud Management Platform, replace them and update them on the management components in the region to maintain secure connection.

Procedure

1 Replace the vRealize Automation Certificate for Consolidated SDDC

Replace the existing certificate for all vRealize Automation services from the vRealize Automation Management Console. You replace the certificate on the vRealize Automation Appliance, IaaS Web server, and IaaS Manager server to maintain a trusted communication between the vRealize Automation nodes.

2 Update the vRealize Automation Certificate on vRealize Orchestrator and vRealize Business for Consolidated SDDC

After you update the vRealize Automation certificate, reconnect vRealize Orchestrator and vRealize Business to vRealize Automation to install the new certificate on each component.

3 Update the vRealize Automation Certificate on vRealize Operations Manager for Consolidated SDDC

After you change the certificate of the vRealize Automation Appliance and IaaS components, update the certificate on vRealize Operations Manager to keep the communication trusted by reconnecting the vRealize Automation Adapter.

4 Replace the Certificate on vRealize Business for Cloud Server for Consolidated SDDC

Replace the default or existing SSL certificate of vRealize Business for Cloud with a new certificate using the vRealize Business appliance management console. This certificate is used when you access the Web interface of the vRealize Business for Cloud Server.

Replace the vRealize Automation Certificate for Consolidated SDDC

Replace the existing certificate for all vRealize Automation services from the vRealize Automation Management Console. You replace the certificate on the vRealize Automation Appliance, IaaS Web server, and IaaS Manager server to maintain a trusted communication between the vRealize Automation nodes.

Procedure

1 Log in to the vRealize Automation appliance.

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

   b Log in using the following credentials.

Settings	Value
User name	root
Password	*vra_appA_root_password*

2 On the **vRA Settings** tab, click the **Certificates** subtab.

3 Under **vRA Certificate**, select **Import**.

4 From a text editor on the Windows host where you run the `CertGenVVD` utility, copy the content of the certificate files to the respective text boxes, and click **Save Settings**.

Source Content	Target Text Box
vra-for-1-pod.key	RSA Private Key
vra-for-1-pod.3.pem	Certificate Chain
Passphrase you optionally entered at generation	Passphrase

5 Repeat the procedure to configure the IaaS Web server and IaaS Manager Service with the new certificate details.

IaaS Component	Component Type	Certificate Action
IaaS Web server	IaaS Web	Import Certificate
IaaS Manager Service	Manager Service	Import Certificate

Update the vRealize Automation Certificate on vRealize Orchestrator and vRealize Business for Consolidated SDDC

After you update the vRealize Automation certificate, reconnect vRealize Orchestrator and vRealize Business to vRealize Automation to install the new certificate on each component.

Procedure

1 Log in to the first vRealize Automation appliance by using a Secure Shell (SSH) client.

   a Open an SSH connection to the primary vRealize Automation virtual appliance **`vra01svr01a.rainpole.local`**.

   b Log in using the following credentials.

Setting	Value
User Name	root
Password	*vro_appA_root_password*

2 Stop the Orchestrator server and the Control Center services of the embedded vRealize Orchestrator server.

```
service vco-server stop && service vco-configurator stop
```

3 Update the vRealize Automation certificate in the component registration with vRealize Automation for embedded vRealize Orchestrator.

   a Verify the trusted certificate in the embedded vRealize Orchestrator trust store `vco.cafe.component-registry.ssl.certificate` using the command-line interface.

```
/var/lib/vco/tools/configuration-cli/bin/vro-configure.sh list-trust
```

   The SHA1 thumbprint must match that of vRealize Automation's certificate.

   b Run the following commands to update the trust store with the new vRealize Automation certificate.

```
/var/lib/vco/tools/configuration-cli/bin/vro-configure.sh trust --uri
https://vra01svr01.rainpole.local/
/var/lib/vco/tools/configuration-cli/bin/vro-configure.sh trust --registry-certificate --uri
https://vra01svr01.rainpole.local
```

   When prompted, press Y to accept the new certificate.

   c After you complete both operations, verify that the trusted certificate in the embedded vRealize Orchestrator trust is updated.

```
/var/lib/vco/tools/configuration-cli/bin/vro-configure.sh list-trust
```

   The SHA1 thumbprint must match that of vRealize Automation's certificate.

   An alias store, `Alias: Imported<hash>`, is created for all certificates in the chain presented from vRealize Automation.

4 Start the Orchestrator server and the Control Center services of the built-in vRealize Orchestrator server on the vRealize Automation appliance, and verify their status.

```
service vco-configurator start && service vco-server start
service vco-configurator status && service vco-server status
```

5 Repeat this process on the other vRealize Automation appliance nodes.

6 Re-Authenticate vRealize Automation with the embedded vRealize Orchestrator

a Open a Web browser and go to **`https://vra01svr01.rainpole.local:8283/vco-controlcenter/`**.

b Log in using the following credentials.

Setting	Value
User Name	root
Password	*vra_root_password*

c Click **Configure Authentication Provider**.

d In **Default tenant**, enter **`rainpole`** and click **Change**.

e In **Admin group**, enter **ug-admin** and click **Search**.

f From the drop-down menu, select **rainpole\ug-admin** and click **Save Changes**.

7 Restart vRealize Orchestrator servers

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

b Log in using the following credentials.

Setting	Value
User Name	root
Password	*vra_root_password*

c Click the **vRA Settings** tab and click **Orchestrator**.

d Select **Orchestrator server** and click **Restart**.

e Select **Orchestrator user interface** and click **Restart**.

8 Validate the embedded vRealize Orchestrator configuration.

a Open a Web browser and go to **`https://vra01svr01.rainpole.local:8283/vco-controlcenter/`**.

b Log in using the following credentials.

Setting	Value
User Name	root
Password	*vra_root_password*

c Click **Validate Configuration** and verify that each section is validated successfully.

9 Log in to the vRealize Business Server appliance management console.

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

b Log in using the following credentials.

Setting	Value
User name	root
Password	*vrb_server_root_password*

10 On the **Registration** tab, click the **vRA** tab, enter the following to register with the vRealize Automation server and initiate an update of a vRealize Automation certificate.

Setting	Value
Hostname	vra01svr01.rainpole.local
SSO Default Tenant	rainpole
SSO Admin User	svc-vra
SSO Admin Password	*svc-vra_password*
Accept vRealize Automation Certificate	Deselected

11 Click **Register** to connect to vRealize Automation and update its certificate.

12 Wait until the SSO Status changes to `The certificate of "vRealize Automation" is not trusted. Please view and accept to register.`

13 Click the **View "vRealize Automation" certificate** link to download the vRealize Automation certificate.

14 Select the **Accept "vRealize Automation" certificate** check box and click **Register**.

SSO Status changes to `Connected to vRealize Automation`.

Update the vRealize Automation Certificate on vRealize Operations Manager for Consolidated SDDC

After you change the certificate of the vRealize Automation Appliance and IaaS components, update the certificate on vRealize Operations Manager to keep the communication trusted by reconnecting the vRealize Automation Adapter.

Procedure

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

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

   b Log in using the following credentials.

Setting	Value
User name	admin
Password	*vrops_admin_password*

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

3 In the left pane of vRealize Operations Manager, under **Management,** click **Certificates**.

4 Select the row that contains `CN=vra01svr01.rainpole.local` and click the **Delete** icon.

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

6 Select the **vRealize Automation Management Pack** solution and click **Configure**.

7 In the **Manage Solutions** dialog box, select **vRealize Automation Adapter**, click **Test Connection**, accept the new certificate, and click **Save Settings**.

Replace the Certificate on vRealize Business for Cloud Server for Consolidated SDDC

Replace the default or existing SSL certificate of vRealize Business for Cloud with a new certificate using the vRealize Business appliance management console. This certificate is used when you access the Web interface of the vRealize Business for Cloud Server.

Procedure

1 Log in to the vRealize Business Server appliance management console.

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

   b Log in using the following credentials.

Setting	Value
User name	root
Password	*vrb_server_root_password*

2 Click the **Administration** tab and click **SSL**.

3 On the **Replace SSL Certificate** page, upload the certificate files that you previously generated for vRealize Business and click **Replace Certificate**.

Use the `vrb.key` file as the **RSA Private Key (.pem)** and the `vrb.3.pem` file for the **Certificate(s) (.pem)** entry. These files are in the `vrb` folder that you created during certificate generation.

Setting	Value
Choose mode	Import PEM encoded Certificate

RSA Private Key (.pem)	`------BEGIN RSA PRIVATE KEY-----`
	`private_key_value`
	`-----END RSA PRIVATE KEY-----`

Certificate(s) (.pem)	`-----BEGIN CERTIFICATE-----`
	`Server_certificate_value`
	`-----END CERTIFICATE-----`
	`-----BEGIN CERTIFICATE-----`
	`Intermediate_CA`
	`-----END CERTIFICATE-----`
	`-----BEGIN CERTIFICATE-----`
	`Root_CA_certificate_value`
	`-----END CERTIFICATE-----`

Private Key Passphrase	*vrb_cert_passphrase*

The `Successfully imported the certificate` message appears.

4 Click the **System** tab and click **Reboot**.

5 On the **System Reboot** window, click **Reboot**.