Certificate Replacement

26 SEP 2017
VMware Validated Design 4.1
VMware Validated Design for Management and Workload Consolidation 4.1

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

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 cloud architects, infrastructure administrators, cloud administrators and cloud operators who are familiar with and want to use VMware software to deploy in a short time and manage a Consolidated SDDC that meets the requirements for capacity, scalability, backup and restore, and disaster recovery.

Required Software

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.

Create and Add a Microsoft Certificate Authority Template for Consolidated SDDC

1

You create a Microsoft Certificate Authority Template to contain the certificate authority (CA) attributes for signing certificates for the management products in the Consolidated SDDC.

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

- Verify that you installed Microsoft Server 2012 R2 VMs with Active Directory Domain Services enabled.
- Verify that the Certificate Authority Service role and the Certificate Authority Web Enrolment role is installed and configured on both 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-2 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. ■ If you use only the root CA, connect dc01rpl.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 **Enable Certificate Templates** dialog box, select the VMware certificate that you just created in the **Name** column and click **OK.**

Generate MSCA-Signed Certificates for the SDDC Management Components

2

Use the VMware Validated Design Certificate Generation Utility (`CertGenVVD`) to generate with a single operation certificates that are signed by the Microsoft certificate authority (MSCA) for all management components. In this way, you can skip sending Certificate Signing Requests to a third-party CA. The generated certificates are compliant with the requirements of the individual management components.

For information about the VMware Validated Design Certificate Generation Utility, see VMware Knowledge Base article 2146215 and the *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 CA server on the sfo01.rainpole.local

Procedure

1. Log in to the 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 2-1. 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
Business Continuity	vSphere Data Protection	sfo01w01vdp01.sfo01.rainpole.local	sfo01m01vdp01.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 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 FQDNs and host names in the dedicated sections.

For example, the configuration 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
sfo01w01psc01.sfo01.rainpole.local
```

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

```
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 MSCA-signed certificates.

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

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

What to do next

Replace the product certificates with the certificates that the `CertGenVVD` utility has generated. See Chapter 4 Replace the Certificates of the Management Products for Consolidated SDDC.

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

3

Use the VMware Validated Design Certificate Generation Utility (`CertGenVVD`) to generate certificate signing request (CSR) files for the management components in the Consolidated SDDC that you can send to a third-party certificate authority. After you receive the CA-signed certificates, run the `CertGenVVD` utility to convert the certificate for each component in the format that the component supports.

You can then replace the certificates on these components, for example, if they are about to expire or are compromised.

Prerequisites

- Provide a Windows Server 2012 host that is 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 3-1. Certificate Generation Files for Consolidated SDDC

SDDC Layer	Host Name or Service in Consolidated SDDC		Configuration Files
Virtual Infrastructure Layer	Platform Services Controller	sfo01w01psc01.sfo01.rainpole.local	sfo01w01psc01.txt
	vCenter Server	sfo01w01vc01.sfo01.rainpole.local	sfo01w01vc01.txt

Table 3-1. Certificate Generation Files for Consolidated SDDC (Continued)

SDDC Layer	Host Name or Service in Consolidated SDDC		Configuration Files
	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
Business Continuity	vSphere Data Protection	sfo01w01vdp01.sfo01.rainpole.local	sfo01w01vdp01.txt
Cloud Management Platform Layer	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 Layer	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
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 get 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
```

17 After `CertGenVVD` generates the certificates, go to `C:\CertGenVVD–version\CSRCerts\Root64` folder and rename `Root64.cer` to `chainRoot64.cer`.

What to do next

Replace the product certificates with the certificates that the `CertGenVVD` utility has generated. See Chapter 4 Replace the Certificates of the Management Products for Consolidated SDDC.

Replace the Certificates of the Management Products for Consolidated SDDC

4

After you generate certificates for management products that are signed by the two-layered certificate authority on the child AD server in the region, replace the default certificate or a certificate that is about to expire with a newly-signed one.

Prerequisites

Use the VMware Validated Design Certificate Utility. See Chapter 2 Generate MSCA-Signed Certificates for the SDDC Management Components and Chapter 3 Generate Certificate Signing Requests and Certificates from a Third-Party CA for Consolidated SDDC.

Procedure

1 Replace Certificates of the Virtual Infrastructure Components for Consolidated SDDC

   If the user-facing certificates of the management components in the Consolidated SDDC are about to expire or are compromised, you replace them with certificates that are signed by a Microsoft or another certificate authority. You start from Platform Services Controller, vCenter Server and ESXi because these components are connected to the components in the operations management and cloud management layers.

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

   After you generate signed certificates for the components of the Cloud Management Platform by using the `CertGenVVD` utility, replace them on these components. Update the new certificates on the management components in the Consolidated SDDC to maintain the trusted connection.

3 Replace Certificates of the Operations Management Components for Consolidated SDDC

   If the certificate of vRealize Operations Manager or vRealize Log Insight is about to expire or is compromised, replace it and update it on the management components in the Consolidated SDDC to maintain trusted connection. Generate the certificate using the `CertGenVVD` utility so that it is compliant with this design and with the requirements of vRealize Operations Manager.

Replace Certificates of the Virtual Infrastructure Components for Consolidated SDDC

If the user-facing certificates of the management components in the Consolidated SDDC are about to expire or are compromised, you replace them with certificates that are signed by a Microsoft or another certificate authority. You start from Platform Services Controller, vCenter Server and ESXi because these components are connected to the components in the operations management and cloud management layers.

Infrastructure administrators connect to different SDDC components, such as vCenter Server or 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 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 Certificate for Consolidated SDDC

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

2 Replace the vCenter Server Certificate for Consolidated SDDC

Replace the certificate on the Consolidated vCenter Server if it is about to expire and reconnect vCenter Server to the other management components to update the new certificate on these components for trusted communication.

3 Replace the ESXi Host Certificates in Consolidated SDDC

Replace the default or certificates that are about to expire on the ESXi hosts with certificates that are generated by using the `CertGenVVD` utility. By default, each new ESXi host is provisioned with a signed certificate that has VMware Certificate Authority as the root certificate authority.

4 Replace the NSX Manager Certificates for Consolidated SDDC

After you replace the certificates of the Platform Services Controller instance and the vCenter Server instance, replace the certificates for the NSX Manager instance. Re-establish the trusted connection to vCenter Server and Platform Services Controller, and to vRealize Operations Manager.

5 Replace Certificate on vSphere Data Protection for Consolidated SDDC

After you use the VMware Validated Design Certificate Generation Utility (`CertGenVVD`) to generate certificates for the SDDC management components, replace the certificate on vSphere Data Protection if it is about to expire or is compromised.

Replace the Platform Services Controller Certificate for Consolidated SDDC

Replace the certificate of the Platform Services Controller instance in Consolidated SDDC. Reconnect the Platform Services Controller 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 Certificate Files for Consolidated SDDC

After you generate the SDDC management certificates by using the `CertGenVVD` utility on a Windows host that has access to the data center, replace the SSL certificate on the Platform Services Controller instance in the Consolidated SDDC with a custom certificate that is signed by the certificate authority (CA).

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

After you replace the certificate of the Platform Services Controller instance, update the certificate on vCenter Server and NSX Manager to re-establish trusted communication.

What to do next

If you replace the certificate of vCenter Server after the Platform Services Controller, see Replace the vCenter Server Certificate Files for Consolidated SDDC.

Replace the Platform Services Controller Certificate Files for Consolidated SDDC

After you generate the SDDC management certificates by using the `CertGenVVD` utility on a Windows host that has access to the data center, replace the SSL certificate on the Platform Services Controller instance in the Consolidated SDDC with a custom certificate that is signed by the certificate authority (CA).

The certificate must have a common name that is equal to the Fully Qualified Domain Name (FQDN) of the Platform Services Controller. The short name of the Platform Services Controller must be in the Subject Alternate Name (SAN) of the generated certificate.

Table 4-1. Certificate-Related Files on Platform Services Controller

Platform Services Controller	Certificate File Name
sfo01w01psc01.sfo01.rainpole.local	■ sfo01w01psc01.key ■ sfo01w01psc01.1.cer ■ chainRoot64.cer

Procedure

1 Log in to the Platform Services Controller by using a Secure Shell (SSH) client.

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

   b Log in using the following credentials.

Setting	Value
User name	root
Password	*sfo01m01psc01_root_password*

2 Run the following command to enable Bash shell access for the root user.

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

3 Copy the generated certificates from the Windows host to the Platform Services Controller.

   a Run the following command to create a new temporary folder

```
mkdir –p /root/certs
```

   b Copy the certificate files `sfo01w01psc01.1.cer`, `sfo01w01psc01.key` and `chainRoot64.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/chainRoot64.cer`**.

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

   i The Platform Services Controller services restarts automatically.

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, run the following commands in the SSH terminal to restart the vami-lighttp service and to remove certificate files.

```
service vami-lighttp restart
cd /root/certs
rm sfo01w01psc01.1.cer sfo01w01psc01.key chainRoot64.cer
```

7 Switch the shell back to the appliance shell.

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

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

After you replace the certificate of the Platform Services Controller instance, update the certificate on vCenter Server and NSX Manager to re-establish trusted communication.

Procedure

1 Restart the services of the Consolidated vCenter Server.

   a Open an SSH connection to sfo01w01vc01.sfo01.rainpole.local.

   b Log in using the following credentials.

Setting	Values
User name	root
Password	*sfo01w01vc01_root_password*

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

```
shell
```

   d Restart vCenter Server services by using the following command.

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

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

   See Connect NSX Manager to the Consolidated vCenter Server After Certificate Replacement.

Replace the vCenter Server Certificate for Consolidated SDDC

Replace the certificate on the Consolidated vCenter Server if it is about to expire and reconnect vCenter Server to the other management components to update the new certificate on these components for trusted communication.

Procedure

1 Replace the vCenter Server Certificate Files for Consolidated SDDC

After you generate the SDDC management certificates by using the `CertGenVVD` utility on a Windows host that has access to the data center, replace the certificate of the Consolidated vCenter Server over SSH using the vSphere Certificate Manager.

2 Connect NSX Manager to the Consolidated vCenter Server After Certificate Replacement

After you replace the certificates of the Platform Services Controller and vCenter Server instances, you reconnect NSX Manager to these components to update their certificates on NSX Manager. You must re-establishing the trusted connection to the Lookup Service vCenter Single Sign-On on Platform Services Controller and to the vSphere Web Service API on vCenter Server.

3 Connect vSphere Data Protection to the Consolidated vCenter Server After Certificate Replacement

After you replace the certificate on the Consolidated vCenter Server, to update the certificate on vSphere Data Protection, connect vSphere Data Protection to vCenter Server to re-establish trusted connection for backup and restore of virtual machines.

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

After you replace the certificates on the Consolidated vCenter Server, reconnect vRealize Orchestrator, vRealize Business and vRealize Automation to the vCenter Server to update the vCenter Server certificate on the Cloud Management Platform. You must re-establish the trusted connection.

5 Update the Certificate of vCenter Server on vRealize Operations Manager for Consolidated SDDC

After you change the certificate of the Consolidated vCenter Server, update the certificate on the connected vRealize Operations Manager node by reconnecting the vCenter Adapter and vSAN Adapter. You must re-establish the trusted connection.

Replace the vCenter Server Certificate Files for Consolidated SDDC

After you generate the SDDC management certificates by using the `CertGenVVD` utility on a Windows host that has access to the data center, replace the certificate of the Consolidated vCenter Server over SSH using the vSphere Certificate Manager.

You replace certificates the vCenter Server sfo01w01vc01.sfo01.rainpole.local here.

Table 4-2. Certificate-Related Files on the vCenter Server Instances

vCenter Server FQDN	Files for Certificate Replacement
sfo01w01vc01.sfo01.rainpole.local	■ sfo01w01vc01.key ■ sfo01w01vc01.1.cer ■ chainRoot64.cer

Prerequisites

- CA-signed certificate files generated by using VMware Validated Design Certificate Generation Utility (`CertGenVVD`). See the *VMware Validated Design Planning and Preparation* documentation.
- A Windows host with an SSH terminal access software such as PuTTY and an `scp` software such as WinSCP installed.

Procedure

1. Change the vCenter Server Appliance command shell to the Bash shell to allow secure copy (`scp`) connections.
   a. Open an SSH connection to sfo01w01vc01.sfo01.rainpole.local.
   b. Log in using the following credentials.

Setting	Value
User name	root
Password	*vcenter_server_root_password*

   c. Run the following command to enable Bash shell access for the root user.

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

2. Copy the generated certificates from the Windows host 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 `sfo01m01vc01.1.cer`, `sfo01w01vc01.key`, and `chainRoot64.cer`from the Windows host where you run the `CertGenVVD` utility to the `/root/certs` folder.

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

3 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.

Platform Services Controller Address	IP Address of Platform Services Controller
sfo01w01psc01.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 generated 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/chainRoot64.cer`**

4 After Status shows `100% Completed`, wait several minutes until all vCenter Server services are restarted.

5 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.

6 Run the following commands to restart the vami-lighttp service and to remove certificate files.

```
service vami-lighttp restart
cd /root/certs
rm sfo01w01vc01.1.cer sfo01w01vc01.key chainRoot64.cer
```

Connect NSX Manager to the Consolidated vCenter Server After Certificate Replacement

After you replace the certificates of the Platform Services Controller and vCenter Server instances, you reconnect NSX Manager to these components to update their certificates on NSX Manager. You must re-establishing the trusted connection to the Lookup Service vCenter Single Sign-On on Platform Services Controller and to the vSphere Web Service API on vCenter Server.

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**, click **Edit**.

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

Setting	Value for NSX Manager Instances
Lookup Service IP	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 for NSX Manager for the Consolidated SDDC
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 and vCenter Server to change to the `Connected` status.

Connect vSphere Data Protection to the Consolidated vCenter Server After Certificate Replacement

After you replace the certificate on the Consolidated vCenter Server, to update the certificate on vSphere Data Protection, connect vSphere Data Protection to vCenter Server to re-establish trusted connection for backup and restore of virtual machines.

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 On the vSphere Web Client **Home** page, click the **VDP** icon.

3 On the **Welcome to vSphere Data Protection** page, select **sfo01w01vdp01** from the **VDP Appliance** drop-down menu and click **Connect**.

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

After you replace the certificates on the Consolidated vCenter Server, reconnect vRealize Orchestrator, vRealize Business and vRealize Automation to the vCenter Server to update the vCenter Server certificate on the Cloud Management Platform. You must re-establish the trusted connection.

Procedure

1 Reconnect vRealize Orchestrator to vCenter Server.

   a Open a Web Browser and go to **`https://vra01svr01.rainpole.local:8281`**.

   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:8281
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 Enter the password for the svc-vro@rainpole.local user account and click **Submit**.

h Click **Yes** to ignore the certificate warnings and click **Next**.

2 Reconnect vRealize Business to the Consolidated vCenter Server.

a Open a Web browser and go to `https://vrb01svr01.rainpole.local:9443/dc-ui`.

b Log in using the following credentials.

Setting	Value
User name	root
Password	*vrb_collector_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	itac-tenantadmin
Password	*itac-tenantadmin_password*
Domain	rainpole.local

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

d Have your mouse over **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 Certificate of vCenter Server on vRealize Operations Manager for Consolidated SDDC

After you change the certificate of the Consolidated vCenter Server, update the certificate on the connected vRealize Operations Manager node by reconnecting the vCenter Adapter and vSAN Adapter. You must re-establish the trusted connection.

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 Reconnect the VMware vSAN adapter for the consolidated cluster.

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

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

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

6 Reconnect the VMware vSAN adapter for the consolidated cluster.

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

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

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

Replace the ESXi Host Certificates in Consolidated SDDC

Replace the default or certificates that are about to expire on the ESXi hosts with certificates that are generated by using the `CertGenVVD` utility. By default, each new ESXi host is provisioned with a signed certificate that has VMware Certificate Authority as the root certificate authority.

In each cluster, before you replace the present certificates on a host, configure the certificate mode for hosts to support custom certificate authorities (CAs).

Procedure

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

By default the ESXi hosts are automatically provisioned with VMware Certificate Authority (VMCA) certificates when they are connected to vCenter Server. Set the host certificate mode on the vCenter Server to support a custom certificate authority. In this way, vCenter Server stops pushing VMCA certificates on to the ESXi hosts after you upload a certificate that is signed by a third-party CA .

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

After you generate signed certificates for the ESXi hosts by using the `CertGenVVD` utility and configure vCenter Server to accept custom certificate authorities, replace the present certificates with the custom ones on the hosts. You replace host certificates if they are about to expire, are VMCA-signed or are compromised.

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

By default the ESXi hosts are automatically provisioned with VMware Certificate Authority (VMCA) certificates when they are connected to vCenter Server. Set the host certificate mode on the vCenter Server to support a custom certificate authority. In this way, vCenter Server stops pushing VMCA certificates on to the ESXi hosts after you upload a certificate that is signed by a third-party CA .

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

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

b Log in using the following credentials.

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

c In the **Navigator**, under **Hosts and Cluster**, select **sfo01m01esx01.sfo01.rainpole.local**, and click the **Configure** tab.

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

e Repeat the steps for the other ESXi hosts in the consolidated cluster.

2 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**.

3 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	*mgmt_vc_server_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 generate signed certificates for the ESXi hosts by using the `CertGenVVD` utility and configure vCenter Server to accept custom certificate authorities, replace the present certificates with the custom ones on the hosts. You replace host certificates if they are about to expire, are VMCA-signed or are compromised.

You replace the certificate separately on each hosts in the consolidated cluster.

Table 4-3. Certificate Files Names for the ESXi hosts

ESXi Hosts	Certificate File Names
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 In the **Navigator**, expand the **sfo01w01vc01 > sfo01-w01dc > sfo01-w01-consolidated01** tree, 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 on **Start** button if the status is not showing up as **Running**

   h Click on **OK** to close the **Edit Security Profile** Pop up Window.

3 Place the host in maintenance mode.

   a 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`**.

b Log in using the following credentials.

Setting	Value
User name	administrator@vsphere.local
Password	*vshpere_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.local certificate appears.

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

a Expand the **sfo01w01vc01 > sfo01-w01dc > sfo01-w01-consolidated01** tree, right-click the **sfo01w01esx01.sfo01.rainpole.local** host object and select **Connection > Disconnect**.

b Click **Yes** in the **Confirm Disconnect** popup window.

c Wait until the host is disconnected.

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

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

f 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 In the **Navigator**, 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 consolidated cluster.

Replace the NSX Manager Certificates for Consolidated SDDC

After you replace the certificates of the Platform Services Controller instance and the vCenter Server instance, replace the certificates for the NSX Manager instance. Re-establish the trusted connection to vCenter Server and Platform Services Controller, and to vRealize Operations Manager.

You replace the certificate on the NSX Manager by using the Web interface.

Table 4-4. Certificate-Related Files on NSX Manager

NSX Manager FQDN	Certificate File Name
sfo01w01nsx01.sfo01.rainpole.local	sfo01w01nsx01.4.p12

Procedure

1 On the Windows host that has access to the data center, log in to the NSX Manager Web interface.

   a Open a Web browser and go to following URL.

NSX Manager	URL
NSX Manager for the consolidated cluster	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 NSX Manager to update 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**.

6 Re-register the NSX Manager to the Consolidated vCenter Server and Platform Services Controller pair.

a Open a Web browser and go to the NSX Manager Web interface.

Setting	Value
NSX Manager for Consolidated SDDC	https://sfo01w01nsx01.sfo01.rainpole.local

b Log in using the following credentials.

Setting	Value
User name	admin
Password	*nsx_mngr_admin_password*

c Click **Manage vCenter Registration**.

d Under **Lookup Service ULR**, click the **Edit** button.

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

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

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

g Under **vCenter Server**, click the **Edit** button.

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

Setting	Value for the NSX Manager for Consolidated SDDC
vCenter Server	sfo01w01vc01.sfo01.rainpole.local
vCenter User Name	svc-nsxmanager@rainpole.local
Password	*svc-nsxmanager_password*

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

j Wait until the Status indicators for the Lookup Service and vCenter Server change to `Connected`.

7 Reconnect the NSX Manager instances to vRealize Operations Manager.

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*

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

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

e Delete the certificates with the following CNs.

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

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

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

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

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

Replace Certificate on vSphere Data Protection for Consolidated SDDC

After you use the VMware Validated Design Certificate Generation Utility (`CertGenVVD`) to generate certificates for the SDDC management components, replace the certificate on vSphere Data Protection if it is about to expire or is compromised.

Procedure

1 Log in to the vSphere Data Protection appliance.

a Open an SSH connection to the virtual machine sfo01w01vdp01.sfo01.rainpole.local.

b Log in using the following credentials.

Setting	Value
User name	root
Password	*vdp_root_password*

2 Stop the vSphere Data Protection Web services by running the following command.

```
emwebapp.sh --stop
```

Note If you see errors related to database server, ignore them.

3 Delete the `tomcat` alias from the Java keystore by running the following command.

```
/usr/java/latest/bin/keytool -delete -alias tomcat -storepass changeit
```

4 Copy the **`.keystore`** file generated by `CertGenVVD` tool to the `/tmp` folder on the vSphere Data Protection virtual appliance.

You can use FileZilla or WinSCP.

5 Run the following command to insert the new certification chain in to the keystore.

```
/usr/java/latest/bin/keytool -importkeystore -srckeystore /tmp/.keystore --
destkeystore /root/.keystore -srcstorepass changeit -deststorepass changeit
```

6 Run the following command and in the command output verify that the certificate entry with the `tomcat` alias exists in the keystore.

```
/usr/java/latest/bin/keytool -list -v -keystore /root/.keystore -storepass changeit -keypass
changeit
```

7 If the certificate entry exists in the keystore, run the `addFingerprint.sh` script to update the vSphere Data Protection server thumbprint.

```
/usr/local/avamar/bin/addFingerprint.sh
```

8 Start the vSphere Data Protection Web services by running the following command.

```
emwebapp.sh --start
```

9 Run the following command to remove the `/tmp/.keystore` file.

```
rm /tmp/.keystore
```

Replace Certificates of the Cloud Management Platform Components for Consolidated SDDC

After you generate signed certificates for the components of the Cloud Management Platform by using the `CertGenVVD` utility, replace them on these components. Update the new certificates on the management components in the Consolidated SDDC to maintain the trusted connection.

Procedure

1 Replace the vRealize Automation Certificate in Consolidated SDDC

Replace the existing certficate 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 trusted communication between the vRealize Automation nodes.

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

After you update the certificate on the vRealize Automation Appliance and IaaS components, reconnect vRealize Business to vRealize Automation to install the new certificate and re-establish the trusted connection.

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 SSL Certificate of vRealize Business Server for Consolidated SDDC

Replace the existing SSL certificate of vRealize Business with a new one using the vRealize Business appliance management console. This certificate is used when you access the Web interface of the vRealize Business server.

Replace the vRealize Automation Certificate in Consolidated SDDC

Replace the existing certficate 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 trusted communication between the vRealize Automation nodes.

Procedure

1 Log in to the vRealize Automation appliance management console.

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

b Log in using the following credentials.

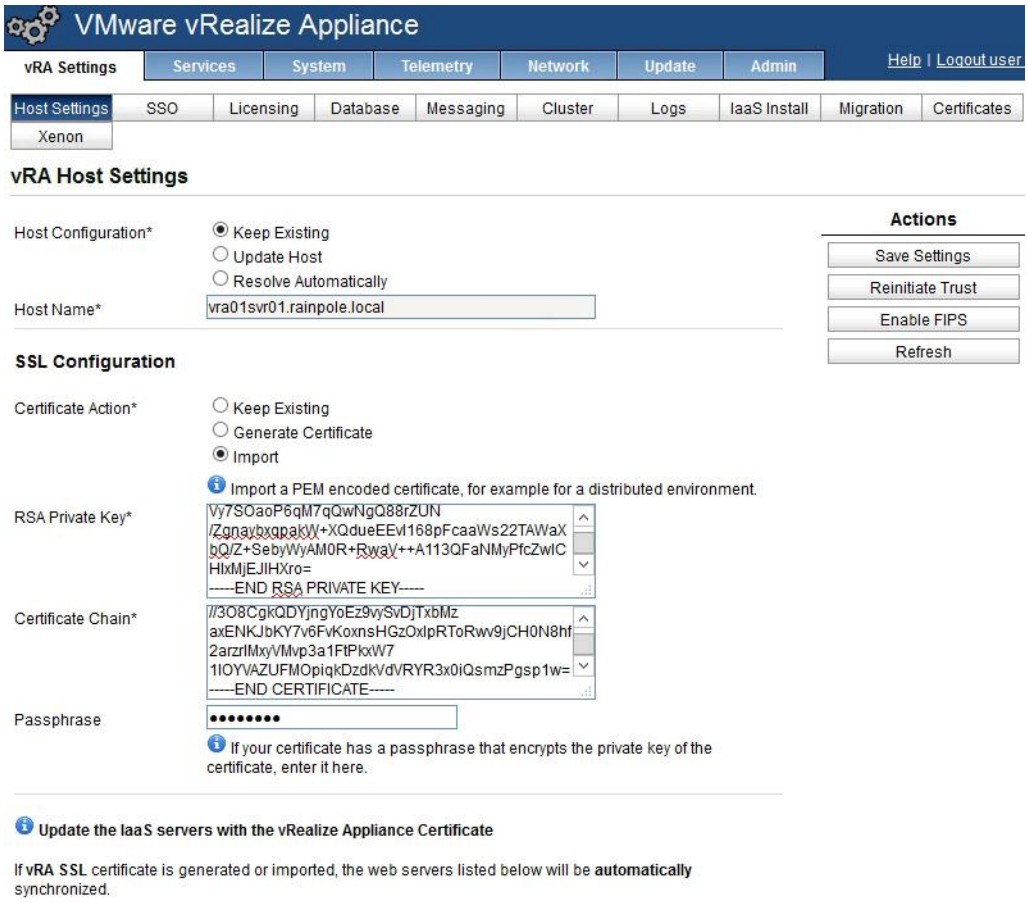
Setting	Value
User name	root
Password	*vra_appA_root_password*

2 On **vRA Settings** tab, click the **Host Settings** tab.

3 Under **SSL Configuration**, select **Import** next to **Certificate Action**.

4 From a text editor on the Windows host where you run the `CertGenVVD` utility, copy the content of the following certificate files and paste it in the corresponding text boxes in the user interface, 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 that you optionally entered at generation	Passphrase



5 Scroll down on the page and verify that all cluster nodes have been successfully updated.

6 Click the **Certificates** tab and use the following procedure to configure IaaS Web server with the new certificate first and repeat the following procedure again with IaaS Manager Service.

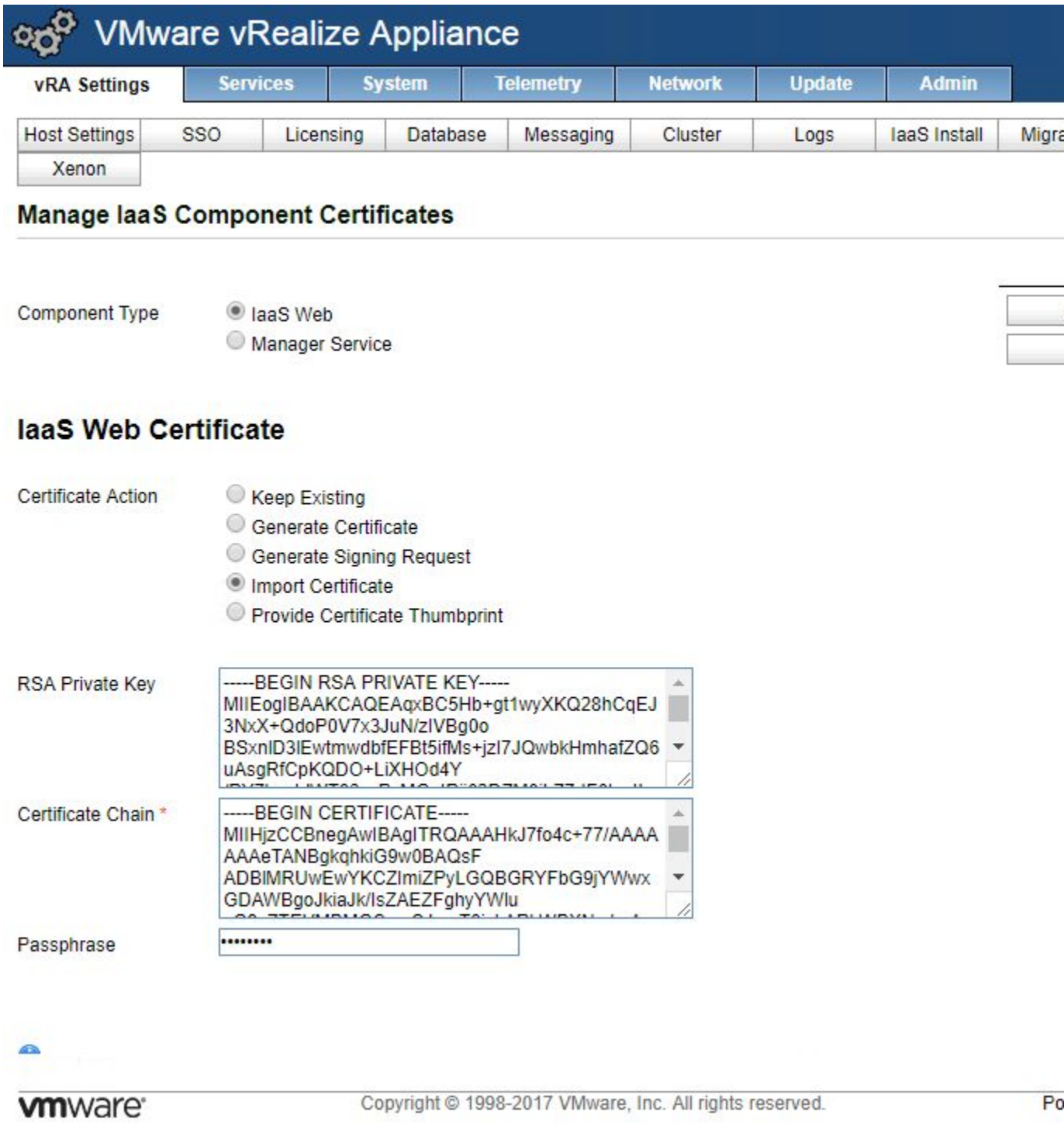
7 Select IaaS Web next to Component Type

IaaS Component	Component Type
IaaS Web server	IaaS Web
IaaS Manager Service	Manager Service

8 Select Import Certificate next to Certificate Action

9 From a text editor on the Windows host where you run the `CertGenVVD` utility, copy the content of the following certificate files and paste it in the corresponding text boxes in the user interface, 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 that you optionally entered at generation	Passphrase



10 Scroll down on the page and verify that all cluster nodes have been successfully updated.

Update the vRealize Automation Certificate on vRealize Business for Consolidated SDDC

After you update the certificate on the vRealize Automation Appliance and IaaS components, reconnect vRealize Business to vRealize Automation to install the new certificate and re-establish the trusted connection.

Procedure

1. Open a Web browser and go to **`https://vrb01svr01.rainpole.local:5480`**.
2. Log in using the following credentials.

Setting	Value
User name	root
Password	*vrb_server_root_password*

3. On the **Registration** tab, click the **vRA** tab, enter the following credentials to register with the vRealize Automation server.

Setting	Value
Hostname	vra01svr01.rainpole.local
SSO Default Tenant	rainpole
SSO Admin User	**`administrator`**
SSO Admin Password	***`vra_administrator_password`***
Accept "vRealize Automation" certificate	Deselected

4. Click **Register** to connect to vRealize Automation and get its certificate.

   A failure message appears at the top of the page. Wait until the SSO Status changes to `The certificate of "vRealize Automation" is not trusted. Please view and accept to register.`
5. Click the **View "vRealize Automation" certificate** link to download the vRealize Automation certificate.
6. 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, click **Certificates** under **Management**.

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 - vra01svr01**, click **Test Connection**, accept the new certificate, and click **Save Settings**.

Replace the SSL Certificate of vRealize Business Server for Consolidated SDDC

Replace the existing SSL certificate of vRealize Business with a new one using the vRealize Business appliance management console. This certificate is used when you access the Web interface of the vRealize Business 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, select **Import PEM encoded Certificate** from the **Choose mode** drop-down menu.

4 Copy the content of the generated certificate files for vRealize Business from a text editor on the Windows host where you run the `CertGenVVD` utility and click **Replace Certificate**.

   Use the `vrb.key` file as the **RSA Private Key (.key)** and the `vrb.3.pem` file for the **Certificate(s) (.pem)** entry.

Setting	Value
Choose mode	Import PEM encoded Certificate
RSA Private Key (.key)	------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*

5 Verify that the certificate changed successfully.

A message appears that informs you that the SSL certificate was successfully configured.

6 Click the **System** tab and click **Reboot** for the changes to take effect.

Replace Certificates of the Operations Management Components for Consolidated SDDC

If the certificate of vRealize Operations Manager or vRealize Log Insight is about to expire or is compromised, replace it and update it on the management components in the Consolidated SDDC to maintain trusted connection. Generate the certificate using the `CertGenVVD` utility so that it is compliant with this design and with the requirements of vRealize Operations Manager.

Procedure

1 Replace vRealize Operations Manager Certificate for Consolidated SDDC

Use the PEM file that is generated using the `CertGenVVD` utility to replace the current certificate on the vRealize Operations Manager administration user interface. You re-connect vRealize Automation to vRealize Operations Manager to update the certificate in the workload reclamation connection.

2 Replace the Certificate of vRealize Log Insight for Consolidated SDDC

After you use the `CertGenVVD` utility to generate the PEM certificate chain file that contains the own certificate, the signer certificate and the private key file, upload the certificate chain to vRealize Log Insight to support trusted connection to the vRealize Log Insight user interface.

Replace vRealize Operations Manager Certificate for Consolidated SDDC

Use the PEM file that is generated using the `CertGenVVD` utility to replace the current certificate on the vRealize Operations Manager administration user interface. You re-connect vRealize Automation to vRealize Operations Manager to update the certificate in the workload reclamation connection.

Procedure

1 Log in to the vRealize Operations Manager administration interface.

   a Open a Web browser and go to **`https://vrops01svr01.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 UI, click the yellow **SSL Certificate** icon.

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

4 Click **Browse**, locate the `vrops-for-1-pod.2.chain.pem` PEM file, and click **Open** .

5 Verify the certificate details and click **Install**.

6 Update the vRealize Operations Manager certificate for workload reclamation communication with 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	itac-tenantadmin
Password	*itac-tenantadmin_password*
Domain	rainpole.local

   c Navigate to **Administration > Reclamation > Metrics Provider**.

   d On the **Metrics Provider** page, click **Test Connection** for the **vRealize Operations Manager endpoint** provider, verify that the test connection is successful, and click **Save**

   e In the certificate warning message box, click **OK**.

Replace the Certificate of vRealize Log Insight for Consolidated SDDC

After you use the `CertGenVVD` utility to generate the PEM certificate chain file that contains the own certificate, the signer certificate and the private key file, upload the certificate chain to vRealize Log Insight to support trusted connection to 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 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 in the address bar of the browser, and verify that **Subject Alternative Name** contains the names of the vRealize Log Insight cluster nodes.

7 Import the certificate in your Web browser.

   For example, in Google Chrome under the HTTPS/TLS settings click **Manage certificates**, and in the **Certificates** dialog box import `vrli-for-1-pod.2.chain.pem`.