Certificate Replacement

Modified on 21 DEC 2017
VMware Validated Design 4.1
VMware Validated Design for Software-Defined Data Center 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 4

1 Region A Certificate Replacement 5

Create and Add a Microsoft Certificate Authority Template in Region A 5

Generate MSCA-Signed Certificates for the SDDC Management Components in Region A 7

Generate Certificate Signing Requests and Certificates from a Third-Party CA in Region A 10

Replace Certificates of the Management Products in Region A 14

Replace Certificates of the Virtual Infrastructure Components in Region A 14

Replace Certificates of the Cloud Management Platform Components in Region A 40

Replace Certificates of the Operations Management Components in Region A 45

2 Region B Certificate Replacement 50

Create and Add a Microsoft Certificate Authority Template in Region B 50

Generate MSCA-Signed Certificates for the SDDC Management Components in Region B 52

Use the Certificate Generation Tool to Generate Certificate Signing Requests in Region B 54

Replace Certificates of the Management Products in Region B 57

Replace Certificates of the Virtual Infrastructure Components in Region B 58

Replace Certificates of the Operations Management Components in Region B 83

About VMware Validated Design Certificate Replacement

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 Software-Defined Data Center.

In an 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 an 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.

Region A Certificate Replacement

1

You first replace the certificate in Region A. As the protected region, it contains the main management components of the SDDC.

- Create and Add a Microsoft Certificate Authority Template in Region A

  You create a Microsoft Certificate Authority Template to contain the certificate authority (CA) attributes for signing certificates of VMware SDDC solution.

- Generate MSCA-Signed Certificates for the SDDC Management Components in Region A

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

- Generate Certificate Signing Requests and Certificates from a Third-Party CA in Region A

  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 in Region A.

- Replace Certificates of the Management Products in Region A

  After you generate a certificate for a management product in Region A that is signed by the two-layered certificate authority on the child AD server in the region, replace the default certificate or an expired certificate with a newly-signed one.

Create and Add a Microsoft Certificate Authority Template in Region A

You create a Microsoft Certificate Authority Template to contain the certificate authority (CA) attributes for signing certificates of VMware SDDC solution.

This VMware Validated Design sets the CA up on both Active Directory (AD) servers: the main domain dc01rpl.rainpole.local (root CA) and the Region A 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 in Region A

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

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 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 1-1. Certificate Generation Files for Region A

Host Name or Service in Region A		Configuration Files
Virtual Infrastructure Layer		
Platform Services Controller	■ sfo01psc01.sfo01.rainpole.local ■ sfo01m01psc01.sfo01.rainpole.local ■ sfo01w01psc01.sfo01.rainpole.local	sfo01psc01.txt
vCenter Server	sfo01m01vc01.sfo01.rainpole.local	sfo01m01vc01.txt
	sfo01w01vc01.sfo01.rainpole.local	sfo01w01vc01.txt
ESXi Hosts	sfo01m01esx01.sfo01.rainpole.local	sfo01m01esx01.txt
	sfo01m01esx02.sfo01.rainpole.local	sfo01m01esx02.txt
	sfo01m01esx03.sfo01.rainpole.local	sfo01m01esx03.txt
	sfo01m01esx04.sfo01.rainpole.local	sfo01m01esx04.txt
	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	sfo01m01nsx01.sfo01.rainpole.local	sfo01m01nsx01.txt
	sfo01w01nsx01.sfo01.rainpole.local	sfo01w01nsx01.txt
vSphere Data Protection	sfo01m01vdp01.sfo01.rainpole.local	sfo01m01vdp01.txt
Site Recovery Manager and vSphere Replication	sfo01m01srm01.sfo01.rainpole.local	sfo01m01srm01.txt
	sfo01m01vrms01.sfo01.rainpole.local	sfo01m01vrms01.txt
Cloud Management Platform Layer		

Table 1-1. Certificate Generation Files for Region A (Continued)

Host Name or Service in Region A		Configuration Files
vRealize Automation	■ vra01svr01.rainpole.local ■ vra01svr01a.rainpole.local ■ vra01svr01b.rainpole.local ■ vra01iws01.rainpole.local ■ vra01iws01a.rainpole.local ■ vra01iws01b.rainpole.local ■ vra01ims01.rainpole.local ■ vra01ims01a.rainpole.local ■ vra01ims01b.rainpole.local ■ vra01dem01a.rainpole.local ■ vra01dem01b.rainpole.local	vra.txt
vRealize Business Server	vrb01svr01.rainpole.local	vrb.txt
Operations Management Layer		
vRealize Operations Manager	■ vrops01svr01.rainpole.local ■ vrops01svr01a.rainpole.local ■ vrops01svr01b.rainpole.local ■ vrops01svr01c.rainpole.local	vrops.txt
vRealize Log Insight	■ sfo01vrli01.sfo01.rainpole.local ■ sfo01vrli01a.sfo01.rainpole.local ■ sfo01vrli01b.sfo01.rainpole.local ■ sfo01vrli01c.sfo01.rainpole.local	vrli.sfo01.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:

sfo01psc01.txt

```
[CERT]
NAME=default
ORG=default
OU=default
LOC=SFO
ST=default
CC=default
CN=sfo01psc01.sfo01.rainpole.local
keysize=default
[SAN]
sfo01psc01
sfo01m01psc01
sfo01w01psc01
sfo01psc01.sfo01.rainpole.local
sfo01m01psc01.sfo01.rainpole.local
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 Replace Certificates of the Management Products in Region A.

Generate Certificate Signing Requests and Certificates from a Third-Party CA in Region A

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 in Region A.

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 1-2. Certificate Generation Files for Region A

Host Name or Service in Region A		Configuration Files
Virtual Infrastructure Layer		
Platform Services Controller	■ sfo01psc01.sfo01.rainpole.local ■ sfo01m01psc01.sfo01.rainpole.local ■ sfo01w01psc01.sfo01.rainpole.local	sfo01psc01.txt
vCenter Server	sfo01m01vc01.sfo01.rainpole.local	sfo01m01vc01.txt
	sfo01w01vc01.sfo01.rainpole.local	sfo01w01vc01.txt
ESXi Hosts	sfo01m01esx01.sfo01.rainpole.local	sfo01m01esx01.txt
	sfo01m01esx02.sfo01.rainpole.local	sfo01m01esx02.txt
	sfo01m01esx03.sfo01.rainpole.local	sfo01m01esx03.txt
	sfo01m01esx04.sfo01.rainpole.local	sfo01m01esx04.txt
	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	sfo01m01nsx01.sfo01.rainpole.local	sfo01m01nsx01.txt
	sfo01w01nsx01.sfo01.rainpole.local	sfo01w01nsx01.txt

Table 1-2. Certificate Generation Files for Region A (Continued)

Host Name or Service in Region A		Configuration Files
vSphere Data Protection	sfo01m01vdp01.sfo01.rainpole.local	sfo01m01vdp01.txt
Site Recovery Manager and vSphere Replication	sfo01m01srm01.sfo01.rainpole.local	sfo01m01srm01.txt
	sfo01m01vrms01.sfo01.rainpole.local	sfo01m01vrms01.txt
Cloud Management Platform Layer		
vRealize Automation	■ vra01svr01.rainpole.local ■ vra01svr01a.rainpole.local ■ vra01svr01b.rainpole.local ■ vra01iws01.rainpole.local ■ vra01iws01a.rainpole.local ■ vra01iws01b.rainpole.local ■ vra01ims01.rainpole.local ■ vra01ims01a.rainpole.local ■ vra01ims01b.rainpole.local ■ vra01dem01a.rainpole.local ■ vra01dem01b.rainpole.local	vra.txt
vRealize Business Server	vrb01svr01.rainpole.local	vrb.txt
Operations Management Layer		
vRealize Operations Manager	■ vrops01svr01.rainpole.local ■ vrops01svr01a.rainpole.local ■ vrops01svr01b.rainpole.local ■ vrops01svr01c.rainpole.local	vrops.txt
vRealize Log Insight	■ sfo01vrli01.sfo01.rainpole.local ■ sfo01vrli01a.sfo01.rainpole.local ■ sfo01vrli01b.sfo01.rainpole.local ■ sfo01vrli01c.sfo01.rainpole.local	vrli.sfo01.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:

sfo01psc01.txt

```
[CERT]
NAME=default
ORG=default
OU=default
LOC=SFO
ST=default
CC=default
CN=sfo01psc01.sfo01.rainpole.local
keysize=default
[SAN]
sfo01psc01
sfo01m01psc01
sfo01w01psc01
sfo01psc01.sfo01.rainpole.local
sfo01m01psc01.sfo01.rainpole.local
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 Replace Certificates of the Management Products in Region A .

Replace Certificates of the Management Products in Region A

After you generate a certificate for a management product in Region A that is signed by the two-layered certificate authority on the child AD server in the region, replace the default certificate or an expired certificate with a newly-signed one.

Prerequisites

Use the VMware Validated Design Certificate Utility. See Generate MSCA-Signed Certificates for the SDDC Management Components in Region A and Generate Certificate Signing Requests and Certificates from a Third-Party CA in Region A.

Procedure

1 Replace Certificates of the Virtual Infrastructure Components in Region A

In this design, you replace user-facing certificates in Region A with certificates that are 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.

2 Replace Certificates of the Cloud Management Platform Components in Region A

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.

3 Replace Certificates of the Operations Management Components in Region A

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 Virtual Infrastructure Components in Region A

In this design, you replace user-facing certificates in Region A with certificates that are 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 in Region A

   Replace the certificates of the pair of Platform Services Controller instances in Region A. Reconnect the Platform Services Controller pair 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 Certificates in Region A

   Replace the certificates on the Management vCenter Server and Compute vCenter Server and reconnect them to the other management components to update the new certificates on these components.

3 Replace the ESXi Host Certificates in Region A

   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 in Region A

   After you replace the certificates of all Platform Services Controller instances and all vCenter Server instances, replace the certificates for the NSX Manager instances. To update the new certificates on the secondary NSX Manager instances in Region B and on vRealize Operations Manager, reconnect NSX Manager to these components. You also re-establish the connection to vCenter Server and Platform Services Controller.

5 Install a CertGenVVD-Generated Certificate on vSphere Data Protection in Region A

   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 in Region A.

6 Replace the Site Recovery Manager Certificate in Region A

   In a dual-region SDDC, you replace an expired certificate on Site Recovery Manager to keep this component trusted. You generate a custom certificate by using the `CertGenVVD` utility. Pair again the Site Recovery Manager instances in the two regions to re-establish the connection using the new certificate.

7 Replace the CA-Signed Certificate on vSphere Replication in Region A

In a dual-region SDDC, replace the default certificate on vSphere Replication in Region A with a custom one for improved security. Reconnect the sites in Region A and Region B to update the new certificate on Region B.

Replace the Platform Services Controller Certificates in Region A

Replace the certificates of the pair of Platform Services Controller instances in Region A. Reconnect the Platform Services Controller pair 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 in Region A

You replace the machine SSL certificate on each Platform Services Controller instance with a custom certificate that is signed by the certificate authority (CA). You use the same certificate on the two instances.

2 Update the Platform Services Controller Certificates on the Management Components in Region A

After you replace the certificates on the Platform Services Controller instances in Region A, update the certificates on the vCenter Server and NSX Manager instances, and restore load balancing.

What to do next

If you replace the certificates of vCenter Server after those of the Platform Services Controllers, see Replace the vCenter Server Certificate Files in Region A.

Replace the Platform Services Controller Certificate Files in Region A

You replace the machine SSL certificate on each Platform Services Controller instance with a custom certificate that is signed by the certificate authority (CA). You use the same certificate on the two instances.

The machine certificate on both Platform Services Controller instances in the region must be the same because they instances are load-balanced. The certificate must have a common name that is equal to the load-balanced Fully Qualified Domain Name (FQDN). Each Platform Services Controller FQDN and short name, and the load-balanced FQDN and short name must be in the Subject Alternate Name (SAN) of the generated certificate.

You must repeat this procedure twice: first on the Platform Services Controller sfo01m01psc01.sfo01.rainpole.local, and then on the Platform Services Controller sfo01w01psc01.sfo01.rainpole.local.

Table 1-3. Certificate-Related Files on Platform Services Controllers

Platform Services Controller	Certificate File Name	Replacement Order
sfo01m01psc01.sfo01.rainpole.local	■ sfo01psc01.key ■ sfo01psc01.1.cer ■ chainRoot64.cer	First
sfo01w01psc01.sfo01.rainpole.local	■ sfo01psc01.key ■ sfo01psc01.1.cer ■ chainRoot64.cer	Second

Procedure

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

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

   b Log in using the following credentials.

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

2 Disable the Platform Services Controller for the shared edge and compute cluster fo01w01psc01 in the load balancer to route all traffic to the Platform Services Controller for the management cluster sfo01m01psc01.

   a From the vSphere Web Client **Home** menu, select **Network & Security**.

   b In the **Navigator**, select **NSX Edges**.

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

   d Double-click the **sfo01psc01** edge device to open its network settings.

   e On the **Manage** tab, click the **Load Balancer** tab and click **Pools**.

   f Select **pool-1** and click **Edit**.

   g Select the **sfo01w01psc01** member, click **Edit**, select **Disable** from the **State** drop-down menu, and click **OK**.

   h Repeat the above to disable **sfo01w01psc01** in **pool-2**.

3 Log in to the sfo01m01psc01 Platform Services Controller by using a Secure Shell (SSH) client.

   a Open an SSH connection to sfo01m01psc01.sfo01.rainpole.local.

   b Log in using the following credentials.

Setting	Value
User name	root
Password	*sfo01m01psc01_root_password*

4 Change the Platform Services Controller command shell to the Bash shell.

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

5 Copy the generated certificates 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 `sfo01psc01.1.cer`, `sfo01psc01.key` and `Root64.cer` to the `/root/certs` folder.

You can use an `scp` software like WinSCP.

6 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/sfo01psc01.1.cer`**.

f When prompted for the custom key, enter **`/root/certs/sfo01psc01.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.

7 Verify that the new certificate has been installed successfully.

a Open a Web Browser and go to **`https://sfo01m01psc01.sfo01.rainpole.local`**.

b Verify that the Web browser shows the new certificate.

8 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 sfo01psc01.1.cer sfo01psc01.key chainRoot64.cer
```

9 Switch the shell back to the appliance shell.

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

10 Repeat Step 3 to Step 9 to replace the certificate on sfo01w01psc01.sfo01.rainpole.local.

Update the Platform Services Controller Certificates on the Management Components in Region A

After you replace the certificates on the Platform Services Controller instances in Region A, update the certificates on the vCenter Server and NSX Manager instances, and restore load balancing.

Procedure

1 Restart the services of the Management vCenter Server.

a Open an SSH connection to sfo01m01vc01.sfo01.rainpole.local.

b Log in using the following credentials.

Setting	Values
User name	root
Password	*sfo01m01vc01_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
```

e Repeat the steps to restart the services on the sfo01w01vc01.sfo01.rainpole.local vCenter Server

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

See Connect NSX Manager to the Management vCenter Server After Certificate Replacement in Region A.

3 Restore the load balancer configuration.

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

b Log in using the following credentials.

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

c From the vSphere Web Client **Home** menu, select **Network & Security**.

d In the **Navigator**, select **NSX Edges**.

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

f Double-click the **sfo01psc01** edge device to open its network settings.

g On the **Manage** tab, click the **Load Balancer** tab and click **Pools**.

h Select **pool-1** and click **Edit**.

i Select the **sfo01w01psc01** member, click **Edit**, select **Enabled** from the **State** drop-down menu, and click **OK**.

j Repeat the steps to enable sfo01w01psc01 in **pool-2**.

Replace the vCenter Server Certificates in Region A

Replace the certificates on the Management vCenter Server and Compute vCenter Server and reconnect them to the other management components to update the new certificates on these components.

Procedure

1 Replace the vCenter Server Certificate Files in Region A

You generate a vCenter Server certificate on a Windows host that has access to the data center by using the `CertGenVVD` tool, and replace the certificate over SSH.

2 Connect NSX Manager to the Management vCenter Server After Certificate Replacement in Region A

After you replace the certificates of the Platform Services Controller and vCenter Server instances in Region A, 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.

3 Connect vSphere Data Protection to vCenter Server After Certificate Replacement in Region A

After you replace the certificates on the vCenter Server nodes, connect vSphere Data Protection to the Management vCenter Server to update the vCenter Server certificate on vSphere Data Protection.

4 Update the Certificate of the Compute vCenter Server on the Cloud Management Platform in Region A

After you replace the certificates on the vCenter Server instances in Region A, reconnect vRealize Orchestrator, vRealize Business and vRealize Automation to the Compute vCenter Server to update the vCenter Server certificate on the Cloud Management Platform.

5 Update the vCenter Server Certificates on vRealize Operations Manager in Region A

After you change the certificates of the vCenter Server instances in Region A, update the certificates on the connected vRealize Operations Manager node by reconnecting the vCenter Adapter and vSAN Adapter instances.

Replace the vCenter Server Certificate Files in Region A

You generate a vCenter Server certificate on a Windows host that has access to the data center by using the `CertGenVVD` tool, and replace the certificate over SSH.

You replace certificates twice, once for each vCenter Server instance. You can start replacing certificates on the Management vCenter Server sfo01m01vc01.sfo01.rainpole.local first.

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

vCenter Server FQDN	Files for Certificate Replacement	Replacement Order
sfo01m01vc01.sfo01.rainpole.local	■ sfo01m01vc01.key ■ sfo01m01vc01.1.cer ■ chainRoot64.cer	First
sfo01w01vc01.sfo01.rainpole.local	■ sfo01w01vc01.key ■ sfo01w01vc01.1.cer ■ chainRoot64.cer	Second

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 sfo01m01vc01.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`, `sfo01m01vc01.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 load balancer.

Platform Services Controller Load Balancer VIP Address	IP Address of Platform Services Controller Load Balancer VIP
sfo01psc01.sfo01.rainpole.local	172.16.11.71

   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
sfo01m01vc01.sfo01.rainpole.local	Please provide valid custom certificate for Machine SSL. File : **/root/certs/sfo01m01vc01.1.cer** Please provide valid custom key for Machine SSL. File : **/root/certs/sfo1m01vc01.key** Please provide the signing certificate of the Machine SSL certificate. File : **/root/certs/chainRoot64.cer**
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://sfo01m01vc01.sfo01.rainpole.local/vsphere-client`**.

   b Verify that you see the new certificate.

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

```
service vami-lighttp restart
cd /root/certs
rm sfo01m01vc01.1.cer sfo01m01vc01.key chainRoot64.cer
```

7 After you replace the certificate on the sfo01m01vc01.sfo01.rainpole.local vCenter Server, repeat the procedure to replace the certificate on the compute vCenter Server sfo01w01vc01.sfo01.rainpole.local.

Connect NSX Manager to the Management vCenter Server After Certificate Replacement in Region A

After you replace the certificates of the Platform Services Controller and vCenter Server instances in Region A, 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 Management NSX Manager appliance user interface.

   a Open a Web browser and go to **`https://sfo01m01nsx01.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	sfo01psc01.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 Management Cluster	Value for NSX Manager for the Shared Edge and Compute Cluster
vCenter Server	sfo01m01vc01.sfo01.rainpole.local	sfo01w01vc01.sfo01.rainpole.local
vCenter User Name	svc-nsxmanager@rainpole.local	svc-nsxmanager@rainpole.local
Password	*svc-nsxmanager_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.

10 Repeat the procedure to connect NSX Manager for the shared edge and compute cluster sfo01w01nsx01.sfo01.rainpole.local to the Platform Services Controller load balancer and Compute vCenter Server.

Connect vSphere Data Protection to vCenter Server After Certificate Replacement in Region A

After you replace the certificates on the vCenter Server nodes, connect vSphere Data Protection to the Management vCenter Server to update the vCenter Server certificate on vSphere Data Protection.

You reconnect vCenter Server to vSphere Data Protection to install the new certificate of vCenter Server.

Procedure

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

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

   b Log in using the following credentials.

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

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

3 On the **Welcome to vSphere Data Protection** page, select **sfo01m01vdp01** from the **VDP Appliance** drop-down menu and click **Connect**.

Update the Certificate of the Compute vCenter Server on the Cloud Management Platform in Region A

After you replace the certificates on the vCenter Server instances in Region A, reconnect vRealize Orchestrator, vRealize Business and vRealize Automation to the Compute 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: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 Compute 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 vCenter Server Certificates on vRealize Operations Manager in Region A

After you change the certificates of the vCenter Server instances in Region A, 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=sfo01m01vc01.sfo01.rainpole.local` and click the **Delete** icon.

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

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

7 In the **Manage Solutions** dialog box, select **vCenter Adapter - sfo01m01vc01**, click **Test Connection**, accept the new certificate of the Management vCenter Server, and click **Save Settings**.

8 Repeat the procedure to delete the certificate that is installed for the Compute vCenter Server sfo01w01vc01.sfo01.rainpole.local and reconnect vRealize Operations Manager to the Compute vCenter Server to install the new certificate.

9 Reconnect the VMware vSAN adapter for the management 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 - sfo01m01vc01**, click **Test Connection**, accept the new certificate of the Management vCenter Server, and click **Save Settings**.

Replace the ESXi Host Certificates in Region A

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 the Management vCenter Server to Support a Custom Certificate Authority in Region A

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 vCenter Server in Region A to support a custom certificate authority so that vCenter Server stops pushing VMCA certificates on to the ESXi hosts.

2 Replace the Default Certificates with Custom Certificates on the Management ESXi Hosts in Region A

After you obtain signed certificates for the ESXi hosts in Region A 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.

3 Configure Certificate Mode for and Replace Certificates on the Hosts in the Shared Edge and Compute Cluster in Region A

After you replace the certificates of the ESXi hosts in the management cluster, complete certificate replacement in Region A on the hosts in the shared edge and compute cluster.

Set Host Certificate Mode on the Management vCenter Server to Support a Custom Certificate Authority in Region A

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 vCenter Server in Region A to support a custom certificate authority so that vCenter Server stops pushing VMCA certificates on to the ESXi hosts.

vCenter Server	ESXi Host
sfo01m01vc01.sfo01.rainpole.local	sfo01m01esx01.sfo01.rainpole.local
	sfo01m01esx02.sfo01.rainpole.local

vCenter Server	ESXi Host
	sfo01m01esx03.sfo01.rainpole.local
	sfo01m01esx04.sfo01.rainpole.local
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://sfo01m01vc01.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 management ESXi hosts that are controlled by the Management vCenter Server sfo01m01vc01.sfo01.rainpole.local.

2 Change the certificate mode for the ESXi hosts in the management cluster to **`custom`** .

   a In the **Navigator**, under **Hosts and Cluster**, select **sfo01m01vc01.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://sfo01m01vc01.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 Management ESXi Hosts in Region A

After you obtain signed certificates for the ESXi hosts in Region A 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 hosts in the management cluster.

Table 1-5. Certificate Files Names for the Management Hosts in Region A

ESXi Hosts	Certificate File Names
sfo01m01esx01.sfo01.rainpole.local	■ sfo01m01esx01.key ■ sfo01m01esx01.1.cer
sfo01m01esx02.sfo01.rainpole.local	■ sfo01m01esx02.key ■ sfo01m01esx02.1.cer
sfo01m01esx03.sfo01.rainpole.local	■ sfo01m01esx03.key ■ sfo01m01esx03.1.cer
sfo01m01esx04.sfo01.rainpole.local	■ sfo01m01esx04.key ■ sfo01m01esx04.1.cer

Procedure

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

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

   b Log in using the following credentials.

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

2 Disable lockdown mode on the sfo01m01esx01.sfo01.rainpole.local host.

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

   b Under the **sfo01-m01dc** data center, select the **sfo01m01esx01.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 Under the **sfo01-m01dc** data center, right-click the **sfo01m01esx01esx01.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 sfo01m01esx01.sfo01.rainpole.local host using the following credentials.

Option	Description
User name	root
Password	*esxi_root_user_password*

   b Copy the `sfo01m01esx01.key` and `sfo01m01esx01.1.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 sfo01m01esx01.key rui.key
mv sfo01m01esx01.1.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://sfo01m01esx01.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://sfo01m01vc01.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-m01dc** data center, right-click the **sfo01m01esx01.sfo01.rainpole.local** host object and select **Maintenance Mode > Exit Maintenance Mode**.

e Make sure that no warning message about an untrusted sfo01m01esx01.sfo01.rainpole.local certificate appears.

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

a Under the **sfo01-m01dc** data center, right-click the **sfo01m01esx01.sfo01.rainpole.local** vCenter Server object and select **Connection > Disconnect**.

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

c Wait until the host is disconnected.

d Under the **sfo01-m01dc** data center, right-click the **sfo01m01esx01.sfo01.rainpole.local** host object and select **Connection > Connect**.

e In the **Navigator**, under **Hosts and Cluster**, select **sfo01m01esx01.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 Select the **sfo01m01vc01.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://sfo01m01esx01.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 management ESXi hosts in Region A.

Configure Certificate Mode for and Replace Certificates on the Hosts in the Shared Edge and Compute Cluster in Region A

After you replace the certificates of the ESXi hosts in the management cluster, complete certificate replacement in Region A on the hosts in the shared edge and compute cluster.

Table 1-6. Certificate Files Names for the Shared Edge and Compute Hosts in Region A

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

- Repeat Set Host Certificate Mode on the Management vCenter Server to Support a Custom Certificate Authority in Region A and Replace the Default Certificates with Custom Certificates on the Management ESXi Hosts in Region A to replace the certificates on the hosts under the sfo01w01vc01.sfo01.rainpole.local vCenter Server.

Replace the NSX Manager Certificates in Region A

After you replace the certificates of all Platform Services Controller instances and all vCenter Server instances, replace the certificates for the NSX Manager instances. To update the new certificates on the secondary NSX Manager instances in Region B and on vRealize Operations Manager, reconnect NSX Manager to these components. You also re-establish the connection to vCenter Server and Platform Services Controller.

You replace certificates twice, once for each NSX Manager. You first start replacing certificates on the NSX Manager for the sfo01m01nsx01.sfo01.rainpole.local management cluster.

Table 1-7. Certificate-Related Files on the NSX Manager Instances in Region A

NSX Manager FQDN	Certificate File Name	Replacement Order
sfo01m01nsx01.sfo01.rainpole.local	sfo01m01nsx01.4.p12	After you replace the certificate on the Management vCenter Server
sfo01w01nsx01.sfo01.rainpole.local	sfo01w01nsx01.4.p12	After you replace the certificate on the Compute vCenter Server

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 management cluster	https://sfo01m01nsx01.sfo01.rainpole.local
NSX Manager for the shared compute and edge 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 `sfo01m01nsx01.4.p12`, provide the keystore password or passphrase and click **Import.**

5 Restart the 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 Management 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 the management cluster	https://sfo01m01nsx01.sfo01.rainpole.local
NSX Manager for the shared compute and edge cluster	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	sfo01psc01.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 the Management Cluster	Value for the NSX Manager for the Shared Edge and Compute Cluster
vCenter Server	sfo01m01vc01.sfo01.rainpole.local	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 to the secondary NSX Manager instances in Region B.

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

b Log in using the following credentials.

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

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

d Click **Installation** in the **Navigator**.

e On the **Management** tab , select the **172.17.11.65** instance from the **NSX Manager** menu.

f Select **Actions > Disconnect from Primary NSX Manager**.

Roles	Management NSX Managers in both Regions	Shared Edge and Compute NSX Managers in both Regions
Primary	172.16.11.65	172.16.11.66
Secondary	172.17.11.65	172.17.11.66

g On the **Management** tab , select the **172.16.11.65** instance from the **NSX Manager** drop-down menu.

h Select **Actions > Add Secondary NSX Manager**.

i In the **Add Secondary NSX Manager** dialog box, enter the following settings and click **OK**.

Setting	Management NSX Manager in region B	Shared Edge and Compute NSX Manager in region B
NSX Manager	172.17.11.65	172.17.11.66
User name	admin	admin
Password	*nsx_manager_admin_password*	*nsx_manager_admin_password*
Confirm Password	*nsx_manager_admin_password*	*nsx_manager_admin_password*

j In the **Trust Certificate** confirmation dialog box, click **Yes**.

8 Repeat the steps for the NSX Manager instance for the shared edge and compute cluster.

9 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=sfo01m01nsx01.sfo01.rainpole.local`
- `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 **sfo01m01nsx01-sfo01** adapter instance, click **Test Connection**, accept the new certificate, and click **Save settings**.

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

Install a CertGenVVD-Generated Certificate on vSphere Data Protection in Region A

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 in Region A.

Prerequisites

Generate the Microsoft CA-signed certificate by using the `CertGenVVD` tool. See Generate MSCA-Signed Certificates for the SDDC Management Components in Region A and Generate Certificate Signing Requests and Certificates from a Third-Party CA in Region A.

Procedure

1

2 Log in to the vSphere Data Protection appliance.

   a Open an SSH connection to the virtual machine sfo01m01vdp01.sfo01.rainpole.local.

   b Log in using the following credentials.

Setting	Value
User name	root
Password	*vdp_root_password*

3 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.

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

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

5 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.

6 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
```

7 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
```

8 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
```

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

```
emwebapp.sh ––start
```

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

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

Replace the Site Recovery Manager Certificate in Region A

In a dual-region SDDC, you replace an expired certificate on Site Recovery Manager to keep this component trusted. You generate a custom certificate by using the `CertGenVVD` utility. Pair again the Site Recovery Manager instances in the two regions to re-establish the connection using the new certificate.

If you replace the certificates of all management components in Region A, you must replace the certificates of all Platform Services Controller, vCenter Server and NSX Manager instances before Site Recovery Manager.

Site Recovery Manager	Certificate Files
sfo01m01srm01.sfo01.rainpole.local	■ sfo01m01srm01.5.p12 ■ chainRoot64.cer

Procedure

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

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

b Log in using the following credentials.

Settings	Values
User name	rainpole\svc-srm
Password	*svc-srm_password*

2 Install the CA certificates in the Windows trusted root certificate store of the Site Recovery Manager virtual machine.

   a Copy the CA certificate and PKSCS#12 files to the `C:\certs` folder

   b Double-click the `chainRoot64.cer` file in the `C:\certs` folder to open **Certificate** import dialog box.

   c In the **Certificate** dialog box, select the **Install Certificate** option.

   The **Certificate Import Wizard** appears.

   d Select the **Local Machine** option for **Store Location** and click **Next**.

   e Select **Place all certificates in the following store** option, browse to select **Trusted Root Certificate Authorities** store, and click **OK**.

   f On the **Completing the Certificate Import Wizard** page, click **Finish**.

3 Replace the certificate on Site Recovery Manager with the one that you generated.

   a Open **Programs and Features** from the Windows Control Panel.

   b From the list of programs, select **VMware vCenter Site Recovery Manager** and click **Change**.

   c Select the **Modify** option on the **Maintenance Options** screen and follow the wizard until you reach the **Certificate Type** screen.

   d Select the **Use a PKCS#12 certificate file** option and click **Next**.

   e Browse to the `C:\certs` folder, select the `sfo01m01srm01.5.p12` or `lax01m01srm01.5.p12` file, and enter the certificate password that you specified when generating the PKCS#12 file.

   f Click **Yes** in the certificate warning dialog box and complete the modify installation wizard.

4 Reconnect the two Site Recovery Manager sites after replacing the certificate.

   a Open a Web Browser and go to the following URL.

Region	URL
Region A	https://sfo01m01vc01.sfo01.rainpole.local

   b Log in using the following credentials.

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

   c In the vSphere Web Client, click **Site Recovery > Sites**.

   d Right-click the site **sfo01m01vc01.sfo01.rainpole.local** and select **Reconfigure Pairing**.

e Enter the address of the Platform Services Controller **lax01psc01.lax01.rainpole.local** on the remote site and click **Next**.

f Select the vCenter Server instance **lax01m01vc01.lax01.rainpole.local** with which Site Recovery Manager is registered on the remote site, enter the user name **svc-srm@rainpole.local** and ***svc-srm_password*** password, and click **Finish**.

Replace the CA-Signed Certificate on vSphere Replication in Region A

In a dual-region SDDC, replace the default certificate on vSphere Replication in Region A with a custom one for improved security. Reconnect the sites in Region A and Region B to update the new certificate on Region B.

You start replacing certificates on vSphere Replication in Region A `sfo01m01vrms01.sfo01.rainpole.local` first.

Table 1-8. PKCS#12 Files for vSphere Replication in Region A

vSphere Replication	PKCS#12 File Name from the CertGenVVD Tool
sfo01m01vrms01.sfo01.rainpole.local	sfo01m01vrms01.5.p12

Procedure

1 Upload the PKCS#12 file to vSphere Replication by using the vSphere Replication appliance management interface (VAMI).

a Open a Web browser and go to the following URL.

vSphere Replication	URL
vSphere Replication in Region A	https://sfo01m01vrms01.sfo01.rainpole.local:5480

b Log in using the following credentials.

Setting	Value
User name	root
Password	*vr_root_password*

c On the **VR** tab, click the **Configuration** tab.

d Enter the password of the service account svc-vr@rainpole.local.

e Click **Choose File** next to **Upload PKCS#12 (*.pfx) file** and locate the `sfo01m01vrms01.5.p12` file on your local file system.

f Click the **Upload and Install** button and enter the certificate password when prompted.

After you change the SSL certificate, the vSphere Replication status changes to disconnected because the new certificate is not validated by the vSphere Replication instance in the other site.

2 Reconnect the sites to resolve the connection issue.

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

b Log in using the following credentials.

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

c On the vSphere Web Client **Home** page, click **vSphere Replication**.

d On the **Home** tab, select **sfo01m01vc01.sfo01.rainpole.local**, click **Manage**, and select **Target Sites**.

e Right-click **lax01m01vc01.lax01.rainpole.local** and click **Reconnect site**.

f In the **Reconnect Sites** dialog box, click **Yes** to proceed.

Replace Certificates of the Cloud Management Platform Components in Region A

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 in Region A

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 Orchestrator and vRealize Business in Region A

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

3 Update the vRealize Automation Certificate on vRealize Operations Manager

After you change the certificate of vRealize Automation, update the certificate on vRealize Operations Manager by reconnecting the vRealize Automation Adapter.

4 Replace the SSL Certificate of vRealize Business Server in Region A

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 Region A

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 **Database** tab.

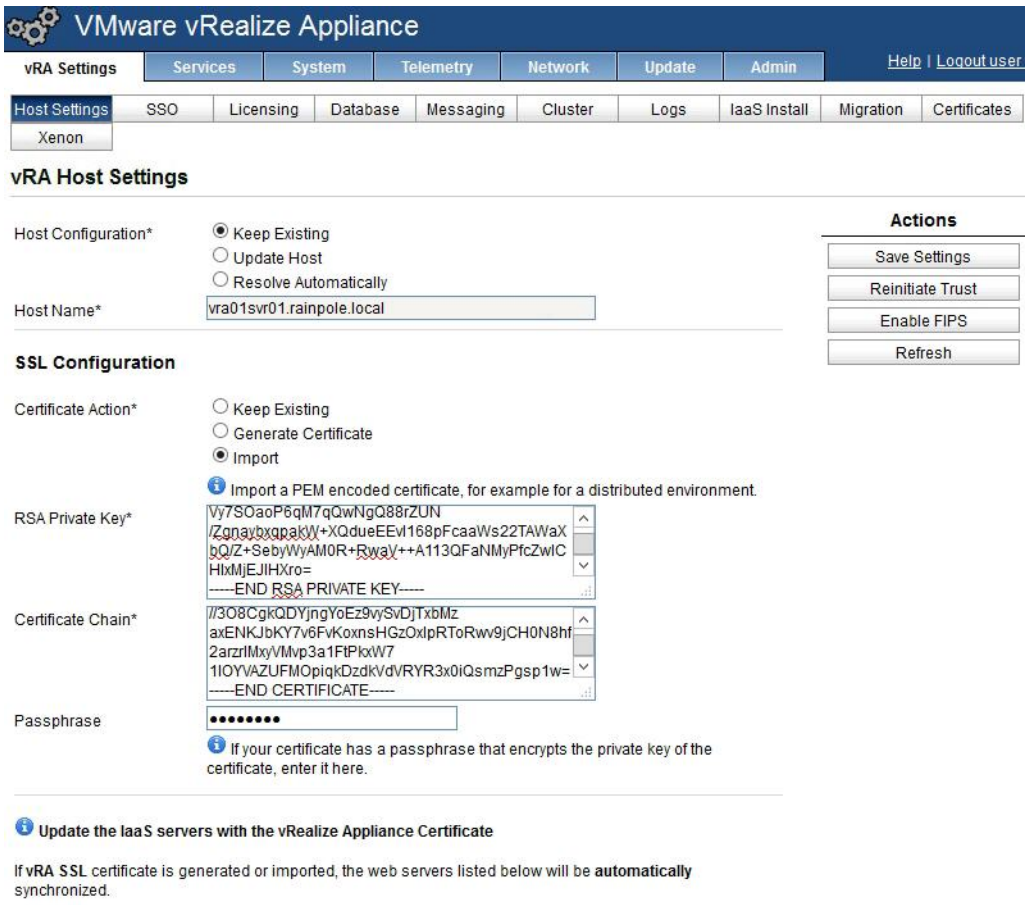
3 If vra01svr01b.rainpole.local is the **MASTER** node, log in to **`https://vra01svr01b.rainpole.local:5480`** using the **`root`** user name and the ***`vra_appB_root_password`*** password instead.

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

5 Under **SSL Configuration**, select **Import** next **Certificate Action**.

6 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.key	RSA Private Key
vra.3.pem	Certificate Chain
Passphrase that you optionally entered at generation	Passphrase



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

8 Click the **Certificates** tab and repeat the procedure to configure the IaaS Web server and IaaS Manager Service with the new certificate details.

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

Update the vRealize Automation Certificate on vRealize Orchestrator and vRealize Business in Region A

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

Procedure

1 Update the vRealize Automation certificate in the component registry authentication with vRealize Automation for 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	*hostA_root_password*

c On the **Home** page, under **Manage**, click **Configure Authentication Provider**.

d On the **Authentication Provider** tab, click **Unregister** next to **Host address** for the **vRealize Automation** mode and click **Unregister** from the **Identity service** section.

e Click **Connect** to register again vRealize Automation as an authentication provider, and in the **Identity service** click **Register** .

f In the **Admin group** text box, enter **`vRO`** and click **Search**.

g From the drop-down menu, select **rainpole.local\ug-vROAdmins** and click **Save Changes**.

h In the restart message that appears on the **Authentication Provider** tab, click the **Startup Options** link and on the **Startup Options** page click **Restart**.

2 Update the vRealize Automation certificate on vRealize Business.

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*

c 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

d 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.`

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

f 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

After you change the certificate of vRealize Automation, update the certificate on vRealize Operations Manager 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**, click **Test Connection**, accept the new certificate, and click **Save Settings**.

Replace the SSL Certificate of vRealize Business Server in Region A

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 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 in Region A

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 vRealize Operations Manager Certificate in Region A

Use the PEM file that is generated using the `CertGenVVD` utility to replace the current certificate on the vRealize Operations Manager administrator 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 in Region A

After you 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.

3 Update the SSL Certificate for Event Forwarding to Region B

After you replace the certificate of vRealize Log Insight in Region A, you update log forwarding from vRealize Log Insight in Region A to vRealize Log Insight in Region B. Log forwarding in this validated design uses SSL connection to exchange log data.

Replace vRealize Operations Manager Certificate in Region A

Use the PEM file that is generated using the `CertGenVVD` utility to replace the current certificate on the vRealize Operations Manager administrator 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 administrator user 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.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 in Region A

After you 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.sfo01.2.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.sfo01.2.chain.pem`.

Update the SSL Certificate for Event Forwarding to Region B

After you replace the certificate of vRealize Log Insight in Region A, you update log forwarding from vRealize Log Insight in Region A to vRealize Log Insight in Region B. Log forwarding in this validated design uses SSL connection to exchange log data.

Procedure

1 Import the root certificate in the Java truststore on each vRealize Log Insight node in Region B.

a Open an SSH session and go to the vRealize Log Insight node.

Name	Role
lax01vrli01a.lax01.rainpole.local	Master node
lax01vrli01b.lax01.rainpole.local	Worker node 1
lax01vrli01c.lax01.rainpole.local	Worker node 2

b Log in using the following credentials.

Name	Role
User name	root
Password	*vrli_regionB_root_password*

c Create a working directory on the vRealize Log Insight node.

```
mkdir /tmp/ssl
cd /tmp/ssl
```

d Extract the root certificate from the destination vRealize Log Insight in Region A.

```
echo "" | openssl s_client –showcerts –servername sfo01vrli01a.sfo01.rainpole.local –connect
sfo01vrli01a.sfo01.rainpole.local:443 –prexit 2>/dev/null | sed –n –e '/BEGIN\
CERTIFICATE/,/END\ CERTIFICATE/ p' > cert.pem
csplit –f individual– cert.pem '/-----BEGIN CERTIFICATE-----/' '{*}'
root_cert=$(ls individual–* | sort –n –t– | tail –1)
cp –f –– "$root_cert" root.crt
```

e Import the `root.crt` in the Java truststore of the vRealize Log Insight node in Region B.

```
cd /usr/java/default/lib/security/
../../bin/keytool –import –alias loginsight –file /tmp/ssl/root.crt –keystore cacerts
```

f When prompted for a keystore password, type **`changeit`**.

g When prompted to accept the certificate, type **`yes`**.

h Reboot the vRealize Log Insight node.

```
reboot
```

i Repeat this operation on all vRealize Log Insight nodes in Region B.

2 Log in to the vRealize Log Insight user interface.

a Open a Web browser and go to **`https://lax01vrli01.lax01.rainpole.local`**.

b Log in using the following credentials.

Setting	Value
User name	admin
Password	*vrli_admin_password*

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

4 Under **Management**, click **Event Forwarding**.

5 On the **Event Forwarding** page, select **LAX01 to SFO01** and click the **Edit** icon.

6 In the **Edit Destination** dialog box, click **Test** to verify that the connection settings are correct.

7 Click **Save** to save the forwarding new destination.

Region B Certificate Replacement 2

After you first replace the certificates in Region A, you continue with the certificate replacement on the components in Region B.

- Create and Add a Microsoft Certificate Authority Template in Region B

  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. After you have created the new template, you add it to the certificate templates of the Microsoft CA.

- Generate MSCA-Signed Certificates for the SDDC Management Components in Region B

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

- Use the Certificate Generation Tool to Generate Certificate Signing Requests in Region B

  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 in Region B.

- Replace Certificates of the Management Products in Region B

  After you generate a certificate for a management product in Region B that is signed by the certificate authority on the parent or child AD server in the region, replace the default certificate or an expired certificate with newly-signed one on the product instance in the region..

Create and Add a Microsoft Certificate Authority Template in Region B

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. After you have created the new template, you add it to the certificate templates of the Microsoft CA.

Prerequisites

- Verify that you installed Microsoft Server 2012 R2 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 the Active Directory Server.

- Verify that dc51lax.lax01.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 dc01lax.lax01.rainpole.local. ■ If you use only the root CA, connect dc01rpl.rainpole.local.
User name	Active Directory administrator
Password	*ad_admin_password*

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

3 In the **Certificate Template Console**, under **Template Display Name,** search the list to see if you can find a template with the name `VMware` exists.

4 If a template with the name VMware already exists, go to Step 11.

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

6 In the **Duplicate Template** window, leave **Windows Server 2003 Enterprise** selected for backward compatibility and click **OK**.

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

8 In the **Template display name** text box, enter **`VMware`** as the name of the new template.

9 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 Click the **Signature is proof of origin (nonrepudiation)** check box.

   e Leave the default for all other options.

   f Click **OK**.

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

11 To add the new template to your CA, click **Start > Run**, enter **`certsrv.msc`**, and click **OK**.

12 In the **Certification Authority** window, expand the left pane if it is collapsed.

13 Right-click **Certificate Templates** and select **New > Certificate Template to Issue**.

14 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 in Region B

Use the VMware Validated Design Certificate Generation Utility (`CertGenVVD`) to generate certificates that are 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 the *VMware Validated Design Planning and Preparation*.

Prerequisites

- If you use an intermediate CA such as lax01.rainpole.local, make the Windows host that you use to connect to the data center a part of the lax01.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 Verify that following properties are configured.

```
ORG=Rainpole Inc.
OU=Rainpole.local
LOC=LAX
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 Region B

Host Name or Service in Region B		Configuration Files
Virtual Infrastructure Layer		
Platform Services Controller	■ lax01psc01.lax01.rainpole.local ■ lax01m01psc01.lax01.rainpole.local ■ lax01w01psc01.lax01.rainpole.local	lax01psc01.txt
vCenter Server	lax01m01vc01.lax01.rainpole.local	lax01m01vc01.txt

Table 2-1. Certificate Generation Files for Region B (Continued)

Host Name or Service in Region B		Configuration Files
	lax01w01vc01.lax01.rainpole.local	lax01w01vc01.txt
ESXi Hosts	lax01m01esx01.lax01.rainpole.local	lax01m01esx01.txt
	lax01m01esx02.lax01.rainpole.local	lax01m01esx02.txt
	lax01m01esx03.lax01.rainpole.local	lax01m01esx03.txt
	lax01m01esx04.lax01.rainpole.local	lax01m01esx04.txt
	lax01w01esx01.lax01.rainpole.local	lax01w01esx01.txt
	lax01w01esx02.lax01.rainpole.local	lax01w01esx02.txt
	lax01w01esx03.lax01.rainpole.local	lax01w01esx03.txt
	lax01w01esx04.lax01.rainpole.local	lax01w01esx04.txt
NSX Manager	lax01m01nsx01.lax01.rainpole.local	lax01m01nsx01.txt
	lax01w01nsx01.lax01.rainpole.local	lax01w01nsx01.txt
vSphere Data Protection	lax01m01vdp01.lax01.rainpole.local	lax01m01vdp01.txt
Site Recovery Manager and vSphere Replication	lax01m01srm01.lax01.rainpole.local	lax01m01srm01.txt
	lax01m01vrms01.lax01.rainpole.local	lax01m01vrms01.txt
Operations Management Layer		
vRealize Log Insight	■ lax01vrli01.lax01.rainpole.local ■ lax01vrli01.lax01a.rainpole.local ■ lax01vrli01.lax01b.rainpole.local ■ lax01vrli01.lax01c.rainpole.local	vrli.lax01.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:

lax01psc01.txt

```
[CERT]
NAME=default
ORG=default
OU=default
LOC=LAX
ST=default
CC=default
CN=lax01psc01.lax01.rainpole.local
keysize=default
[SAN]
lax01psc01
lax01m01psc01
lax01w01psc01
lax01psc01.lax01.rainpole.local
lax01m01psc01.lax01.rainpole.local
lax01w01psc01.lax01.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'
```

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

What to do next

Replace the default certificates with the certificates that the `CertGenVVD` utility has generated. See Replace Certificates of the Management Products in Region B.

Use the Certificate Generation Tool to Generate Certificate Signing Requests in Region B

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 in Region B.

Prerequisites

A Window 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=LAX
ST=CA
CC=US
CN=VMware_VVD
keysize=2048
```

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

Table 2-2. Certificate Generation Files for Region B

Host Name or Service in Region B		Configuration Files
Virtual Infrastructure Layer		
Platform Services Controller	■ lax01psc01.lax01.rainpole.local ■ lax01m01psc01.lax01.rainpole.local ■ lax01w01psc01.lax01.rainpole.local	lax01psc01.txt
vCenter Server	lax01m01vc01.lax01.rainpole.local	lax01m01vc01.txt
	lax01w01vc01.lax01.rainpole.local	lax01w01vc01.txt
ESXi Hosts	lax01m01esx01.lax01.rainpole.local	lax01m01esx01.txt
	lax01m01esx02.lax01.rainpole.local	lax01m01esx02.txt
	lax01m01esx03.lax01.rainpole.local	lax01m01esx03.txt
	lax01m01esx04.lax01.rainpole.local	lax01m01esx04.txt
	lax01w01esx01.lax01.rainpole.local	lax01w01esx01.txt
	lax01w01esx02.lax01.rainpole.local	lax01w01esx02.txt
	lax01w01esx03.lax01.rainpole.local	lax01w01esx03.txt
	lax01w01esx04.lax01.rainpole.local	lax01w01esx04.txt

Table 2-2. Certificate Generation Files for Region B (Continued)

Host Name or Service in Region B		Configuration Files
NSX Manager	lax01m01nsx01.lax01.rainpole.local	lax01m01nsx01.txt
	lax01w01nsx01.lax01.rainpole.local	lax01w01nsx01.txt
vSphere Data Protection	lax01m01vdp01.lax01.rainpole.local	lax01m01vdp01.txt
Site Recovery Manager and vSphere Replication	lax01m01srm01.lax01.rainpole.local	lax01m01srm01.txt
	lax01m01vrms01.lax01.rainpole.local	lax01m01vrms01.txt
Operations Management Layer		
vRealize Log Insight	■ lax01vrli01.lax01.rainpole.local ■ lax01vrli01.lax01a.rainpole.local ■ lax01vrli01.lax01b.rainpole.local ■ lax01vrli01.lax01c.rainpole.local	vrli.lax01.txt

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

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

lax01psc01.txt

```
[CERT] NAME=default
ORG=default
OU=default
LOC=LAX
ST=default
ORG=default
OU=default
LOC=LAX
ST=default
CC=default
CN=lax01psc01.lax01.rainpole.local
keysize=default
[SAN]
lax01psc01
lax01m01psc01
lax01w01psc01
lax01psc01.lax01.rainpole.local
lax01m01psc01.lax01.rainpole.local
lax01w01psc01.lax01.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 Replace Certificates of the Management Products in Region B.

Replace Certificates of the Management Products in Region B

After you generate a certificate for a management product in Region B that is signed by the certificate authority on the parent or child AD server in the region, replace the default certificate or an expired certificate with newly-signed one on the product instance in the region..

Prerequisites

Use the VMware Validated Design Certificate Utility. See Generate MSCA-Signed Certificates for the SDDC Management Components in Region B and Use the Certificate Generation Tool to Generate Certificate Signing Requests in Region B.

Procedure

1 Replace Certificates of the Virtual Infrastructure Components in Region B

   In this design, you replace user-facing certificates in Region B with certificates that are 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.

2 Replace Certificates of the Operations Management Components in Region B

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

Replace Certificates of the Virtual Infrastructure Components in Region B

In this design, you replace user-facing certificates in Region B with certificates that are 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.

Procedure

1 Replace the Platform Services Controller Certificates in Region B

   Replace the certificates of the pair of Platform Services Controller instances in Region B, for example, if the certificates have expired. Reconnect the Platform Services Controller pair to the vCenter Server and NSX Manager instances to update the certificates for vCenter Single Sign-on on these components.

2 Replace vCenter Server Certificates in Region B

   Replace the certificates on the Management vCenter Server and Compute vCenter Server in Region B and reconnect them to the other management components to update the new certificates on these components.

3 Replace the ESXi Host Certificates in Region B

   Replace the default or expired certificate on the ESXi host. Use the `CertGenVVD` utility to generate the certificates.

4 Replace the NSX Manager Certificates in Region B

   After you replace the certificates of all Platform Services Controller instances and all vCenter Server instances, replace the certificates for the NSX Manager instances in Region B. After you replace the certificates, to update them on the primary NSX Manager instances in Region A and on vRealize Operations Manager, reconnect NSX Manager to these components. You also re-establish the connection to vCenter Server and Platform Services Controller.

5 Replace vSphere Data Protection Certificates in Region B

After you use the VMware Validated Design Certificate Generation Utility (`CertGenVVD`) to generate certificates for the SDDC management components, replace the default VMware-signed certificate on vSphere Data Protection in Region B with the certificate that is generated by `CertGenVVD`.

6 Replace the VMware Site Recovery Manager Certificates in Region B

In a dual-region SDDC, you replace an expired certificate on Site Recovery Manager to keep this component trusted. You generate a custom certificate by using the `CertGenVVD` utility.

7 Replace the CA-Signed Certificate on vSphere Replication in Region B

In a dual-region SDDC, replace the certificate on vSphere Replication in Region B, for example if the certificate expires, to maintain your environment secure and trusted. Reconnect the sites in Region A and Region B to update the new certificate on Region A.

Replace the Platform Services Controller Certificates in Region B

Replace the certificates of the pair of Platform Services Controller instances in Region B, for example, if the certificates have expired. Reconnect the Platform Services Controller pair 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 in Region B

You replace the machine SSL certificate on each Platform Services Controller instance in Region B with a custom certificate that is signed by the certificate authority (CA). You use the same certificate on the two instances.

2 Update Platform Services Controller Certificates on the Management Components in Region B

After you replace the certificates on the Platform Services Controller instances in Region B, update the certificates on the vCenter Server instances, reconnect NSX Manager to the Platform Services Controller VIP address, and restore load balancing.

What to do next

If you replace the certificates of vCenter Server after those of the Platform Services Controllers, see Replace vCenter Server Certificates in Region B.

Replace the Platform Services Controller Certificates in Region B

You replace the machine SSL certificate on each Platform Services Controller instance in Region B with a custom certificate that is signed by the certificate authority (CA). You use the same certificate on the two instances.

The machine certificate on both Platform Services Controller instances in the region must be the same because they instances are load-balanced. The certificate must have a common name that is equal to the load-balanced Fully Qualified Domain Name (FQDN). Each Platform Services Controller FQDN and short name, and the load-balanced FQDN and short name must be in the Subject Alternate Name (SAN) of the generated certificate.

You must repeat this procedure twice: first on the Platform Services Controller lax01m01psc01.lax01.rainpole.local, and then on the Platform Services Controller lax01w01psc01.lax01.rainpole.local.

Table 2-3. Certificate-Related Files on Platform Services Controllers

Platform Services Controller	Certificate File Name	Replacement Order
lax01m01psc01.lax01.rainpole.local	■ lax01psc01.key ■ lax01psc01.1.cer ■ chainRoot64.cer	First
lax01w01psc01.lax01.rainpole.local	■ lax01psc01.key ■ lax01psc01.1.cer ■ chainRoot64.cer	Second

Procedure

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

   a Open a Web browser and go to **`https://lax01m01vc01.lax01.rainpole.local/vsphere-client`**.

   b Log in using the following credentials.

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

2 Disable the Platform Services Controller for the shared edge and compute cluster lax01w01psc01 in the load balancer to route all traffic to the Platform Services Controller for the management cluster lax01m01psc01.

   a From the vSphere Web Client **Home** menu, select **Network & Security**.

   b In the **Navigator**, select **NSX Edges**.

   c From the **NSX Manager** drop-down menu, select **172.17.11.65**.

   d Double-click the **lax01psc01** edge device to open its network settings.

   e On the **Manage** tab, click the **Load Balancer** tab and click **Pools**.

   f Select **pool-1** and click **Edit**.

   g Select the **lax01w01psc01** member, click **Edit**, select **Disable** from the **State** drop-down menu, and click **OK**.

   h Repeat the above steps to disable la01w01psc01 in **pool-2**.

3 Log in to the lax01m01psc01 Platform Services Controller by using a Secure Shell (SSH) client.

a Open an SSH connection to lax01m01psc01.lax01.rainpole.local.

b Log in using the following credentials.

Setting	Value
Username	root
Password	*mgmtpsc_root_password*

4 Change the Platform Services Controller command shell to the Bash shell.

```
shell
chsh –s /bin/bash root
```

5 Copy the generated certificates 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 `lax01psc01.1.cer`, `lax01psc01.key` and `chainRoot64.cer`) from the Windows host where you run the `CertGenVVD` utility to the `/root/certs` folder on the Platform Services Controller.

You can use an `scp` software like WinSCP.

6 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 default vCenter Single Sign-On user name **`administrator@vsphere.local`** and the ***`vsphere_admin_password`*** 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/lax01psc01.1.cer`**.

f When prompted for the custom key, enter **`/root/certs/lax01psc01.key.`**

g When prompted for the signing certificate, enter **`/root/certs/chainRoot64.cer.`**

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

Wait until the Platform Services Controller services restart successfully.

7 Verify that the new certificate has been installed successfully.

   a Open a Web Browser and go to **`https://lax01m01psc01.lax01.rainpole.local`**.

   b Verify that the Web browser shows the new certificate.

8 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 lax01psc01.1.cer lax01psc01.key chainRoot64.cer
```

9 Switch the shell back to the appliance shell.

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

10 Repeat Step 3 to Step 9 to replace the certificate on lax01w01psc01.lax01.rainpole.local.

Update Platform Services Controller Certificates on the Management Components in Region B

After you replace the certificates on the Platform Services Controller instances in Region B, update the certificates on the vCenter Server instances, reconnect NSX Manager to the Platform Services Controller VIP address, and restore load balancing.

Procedure

1 Restart the services on the Management vCenter Server.

   a Open an SSH connection to lax01m01vc01.lax01.rainpole.local.

   b Log in using the following credentials.

Setting	Values
Username	root
Password	*lax01m01vc01_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
```

   e Repeat the steps to restart the lax01w01vc01.lax01.rainpole.local vCenter Server.

2 Reconnect the NSX Managers to the Platform Services Controller load balancer and to vCenter Server after you install the custom certificates on the nodes. See Connect NSX Manager to the Management vCenter Server After Certificate Replacement in Region B.

3 Restore load balancer configuration.

a Open a Web Browser and go to `https://lax01m01vc01.lax01.rainpole.local/vsphere-client`.

b Log in using the following credentials

Setting	Values
Username	administrator@vsphere.local
Password	*vsphere_admin_password*

c From the vSphere Web Client **Home** menu, select **Network & Security**.

d In the **Navigator**, select **NSX Edges**.

e Select **172.17.11.65** from the **NSX Manager** drop-down menu.

f Double-click the **lax01psc01** edge device to open its network settings.

g On the **Manage** tab, click the **Load Balancer** tab and click **Pools**.

h Select **pool-1** and click **Edit**.

i Select the **lax01w01psc01** member, click **Edit**, select **Enabled** from the **State** drop-down menu, and click **OK**.

j Repeat the steps to enable **lax01w01psc01** in **pool-2**.

Replace vCenter Server Certificates in Region B

Replace the certificates on the Management vCenter Server and Compute vCenter Server in Region B and reconnect them to the other management components to update the new certificates on these components.

Procedure

1 Replace the vCenter Server Certificates in Region B

You generate a vCenter Server certificate by using the `CertGenVVD` tool on a Windows host that has access to the data center and replace the certificate over SSH.

2 Connect NSX Manager to the Management vCenter Server After Certificate Replacement in Region B

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

3 Connect vSphere Data Protection to vCenter Server After Certificate Replacement in Region B

After you replace the certificates on the vCenter Server nodes in Region B, connect vSphere Data Protection to the Management vCenter Server to update the vCenter Server certificate on vSphere Data Protection.

4 Update the Certificate of the Compute vCenter Server on the Cloud Management Platform in Region B

After you replace the certificates on the vCenter Server instances in Region B, reconnect vRealize Orchestrator, vRealize Business and vRealize Automation to vCenter Server to update the vCenter Server certificate on the Cloud Management Platform.

5 Update the vCenter Server Certificates on vRealize Operations Manager in Region B

After you change the certificate of the vCenter Server instances in Region B, update the certificate on the connected vRealize Operations Manager node by reconnecting the vCenter Adapter and vSAN Adapter instances.

Replace the vCenter Server Certificates in Region B

You generate a vCenter Server certificate by using the `CertGenVVD` tool on a Windows host that has access to the data center and replace the certificate over SSH.

You replace certificates twice, once for each vCenter Server instance. You can start replacing certificates on Management vCenter Server lax01m01vc01.lax01.rainpole.local first.

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

vCenter Server FQDN	Files for Certificate Replacement	Replacement Order
lax01m01vc01.lax01.rainpole.local	■ lax01m01vc01.key ■ lax01m01vc01.1.cer ■ chainRoot64.cer	First
lax01w01vc01.lax01.rainpole.local	■ lax01w01vc01.key ■ lax01w01vc01.1.cer ■ chainRoot64.cer	Second

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 the FQDN of the vCenter Server appliance lax01m01vc01.lax01.rainpole.local.

b Log in using the following credentials.

Settings	Values
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 `lax01m01vc01.1.cer`, `lax01m01vc01.key`, `chainRoot64.cer` from the Windows host where you run the `CertGenVVD` utility to the `/root/certs` folder on the vCenter Server Appliance.

   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 load balancer.

Platform Services Controller Load Balancer VIP	IP Address of Platform Services Controller Load Balancer VIP
lax01psc01.lax01.rainpole.local	172.17.11.71

   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	Path to Certificate-Related Files
lax01m01vc01.lax01.rainpole.local	Please provide valid custom certificate for Machine SSL. File: **`/root/certs/lax01m01vc01.1.cer`** Please provide valid custom key for Machine SSL. File: **`/root/certs/lax01m01vc01.key`** Please provide the signing certificate of the Machine SSL certificate File: **`/root/certs/chainRoot64.cer`**
lax01w01vc01.lax01.rainpole.local	Please provide valid custom certificate for Machine SSL. File: **`/root/certs/lax01w01vc01.1.cer`** Please provide valid custom key for Machine SSL. File: **`/root/certs/lax01w01vc01.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://lax01m01vc01.lax01.rainpole.local/vsphere-client`**.

   b Verify that you see the new certificate.

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

```
service vami-lighttp restart
cd /root/certs
rm lax01m01vc01.1.cer lax01m01vc01.key chainRoot64.cer
```

7 After you replace the certificate on the lax01m01vc01.lax01.rainpole.local, repeat the procedure to replace the certificate on the Compute vCenter Server lax01w01vc01.rainpole.local.

Connect NSX Manager to the Management vCenter Server After Certificate Replacement in Region B

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

Procedure

1 Log in to the appliance interface of the Management NSX Manager.

   a Open a Web browser and go to **`http://lax01m01nsx01.lax01.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 Both NSX Managers
Lookup Service IP	lax01psc01.lax01.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 Management Cluster	Value for NSX Manager for the Shared Edge and Compute Cluster
vCenter Server	lax01m01vc01.lax01.rainpole.local	lax01w01vc01.lax01.rainpole.local
vCenter User Name	svc-nsxmanager@rainpole.local	svc-nsxmanager@rainpole.local
Password	*svc-nsxmanager_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.

10 Repeat the procedure to connect NSX Manager for the shared edge and compute cluster lax01w01nsx01.lax01.rainpole.local to the Platform Services Controller load balancer and Compute vCenter Server.

Connect vSphere Data Protection to vCenter Server After Certificate Replacement in Region B

After you replace the certificates on the vCenter Server nodes in Region B, connect vSphere Data Protection to the Management vCenter Server to update the vCenter Server certificate on vSphere Data Protection.

You reconnect vCenter Server to vSphere Data Protection to install the new certificate of vCenter Server.

Procedure

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

   a Open a Web browser and go to **`https://lax01m01vc01.lax01.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 **lax01m01vdp01** from the **VDP Appliance** drop-down menu and click **Connect**.

Update the Certificate of the Compute vCenter Server on the Cloud Management Platform in Region B

After you replace the certificates on the vCenter Server instances in Region B, 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:8281`**.

   b Click **Start Orchestrator Client**.

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

Setting	Value
Host name	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://lax01w01vc01.lax01.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 Compute vCenter Server.

   a Open a Web browser and go to **`https://lax01vrbc01.lax01.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 **lax01w01vc01.laxo01.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 **lax01w01vc01.lax01.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 in Region B

After you change the certificate of the vCenter Server instances in Region B, update the certificate 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** and click **Certificates**.

4 Select the row that contains `CN=lax01m01vc01.lax01.rainpole.local` and click the **Delete** icon.

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

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

7 In the **Manage Solutions** dialog box, select **vCenter Adapter - lax01m01vc01**, click **Test Connection**, accept the new certificate of the Management vCenter Server, and click **Save Settings**.

8 Repeat the procedure to delete the certificate that is installed for the Compute vCenter Server lax01w01vc01.lax01.rainpole.local and reconnect vRealize Operations Manager to the Compute vCenter Server to install the new certificate.

9 Reconnect VMware vSAN adapter for the management 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 - lax01m01vc01**, click **Test Connection**, accept the new certificate of the Management vCenter Server, and click **Save Settings**.

Replace the ESXi Host Certificates in Region B

Replace the default or expired certificate on the ESXi host. Use the `CertGenVVD` utility to generate the certificates.

Procedure

1 Set Host Certificate Mode on the Management vCenter Server to Support a Custom Certificate Authority in Region B

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 vCenter Server in Region B to support a custom certificate authority so that vCenter Server stops pushing VMCA certificates on to the ESXi hosts.

2 Replace the Default Certificate with a Custom Certificate on the Management ESXi Hosts in Region B

After you obtain signed certificates for the management ESXi hosts in Region B, use them to replace the default VMware Certificate Authority (VMCA) signed certificates on the hosts.

3 Configure Certificate Mode for and Replace Certificates on the Hosts in the Shared Edge and Compute Cluster in Region B

After you replace the certificates of the ESXi hosts in the management cluster, complete certificate replacement in Region B on the hosts in the shared edge and compute cluster.

Set Host Certificate Mode on the Management vCenter Server to Support a Custom Certificate Authority in Region B

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 vCenter Server in Region B to support a custom certificate authority so that vCenter Server stops pushing VMCA certificates on to the ESXi hosts.

vCenter Server	ESXi Host
lax01m01vc01.lax01.rainpole.local	lax01m01esx01.lax01.rainpole.local
	lax01m01esx02.lax01.rainpole.local
	lax01m01esx03.lax01.rainpole.local
	lax01m01esx04.lax01.rainpole.local
lax01w01vc01.lax01.rainpole.local	lax01w01esx01.lax01.rainpole.local

vCenter Server	ESXi Host
	lax01w01esx02.lax01.rainpole.local
	lax01w01esx03.lax01.rainpole.local
	lax01w01esx04.lax01.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://lax01m01vc01.lax01.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 **lax01m01esx01.lax01.rainpole.local**, and click the **Configure** tab.

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

   e Repeat the steps for the management ESXi hosts that are controlled by the Management vCenter Server lax01m01vc01.lax01.rainpole.local.

2 Change the certificate mode for the ESXi hosts in the management cluster to **`custom`**.

   a In the **Navigator**, under **Hosts and Cluster**, select **lax01m01vc01.lax01.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://lax01m01vc01.lax01.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 Certificate with a Custom Certificate on the Management ESXi Hosts in Region B

After you obtain signed certificates for the management ESXi hosts in Region B, use them to replace the default VMware Certificate Authority (VMCA) signed certificates on the hosts.

You replace the certificate separately on each hosts in the management cluster and in the shared edge and compute cluster.

Table 2-5. Certificate Files Names for the Management Hosts in Region B

ESXi Hosts	Certificate File Names
lax01m01esx01.lax01.rainpole.local	■ lax01m01esx01.key ■ lax01m01esx01.1.cer
lax01m01esx02.lax01.rainpole.local	■ lax01m01esx02.key ■ lax01m01esx02.1.cer
lax01m01esx03.lax01.rainpole.local	■ lax01m01esx03.key ■ lax01m01esx03.1.cer
lax01m01esx04.lax01.rainpole.local	■ lax01m01esx04.key ■ lax01m01esx04.1.cer

Procedure

1 Replace the certificates on ESXi hosts.

   a Open a Web browser and go to **`https://lax01m01vc01.lax01.rainpole.local`**.

   b Log in using the following credentials.

Setting	Value
User name	*vcenteradmin*
Password	*vshpere_admin_password*

   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.

2 Place the host in maintenance mode.

   a Under the **lax01-m01dc** data center, right-click the **lax01m01esx01.lax01.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**.

3 Replace the certificate files on the host.

a After the maintenance task is complete, open an SSH connection to the lax01m01esx01.lax01.rainpole.local host using the following credentials.

Option	Description
User name	root
Password	*esxi_root_user_password*

b Copy the `lax01m01esx01.key` and `lax01m01esx01.1.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 lax01m01esx01.key rui.key
mv lax01m01esx01.1.cer rui.crt
```

4 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
```

5 Verify that the custom certificate is installed.

a Open a Web browser and go to **`https://lax01m01esx01.lax01.rainpole.local`**.

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

6 Exit maintenance mode of the host.

a Open a Web browser and go to **`https://lax01m01vc01.lax01.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 **lax01-m01dc** data center, right-click the **lax01m01esx01.lax01.rainpole.local** host object and select **Maintenance Mode > Exit Maintenance Mode**.

e Make sure that no warning message about an untrusted lax01m01esx01.lax01.rainpole.local certificate appears.

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

a Under the **lax01-m01dc** data center, right-click the **lax01m01esx01.lax01.rainpole.local** vCenter Server object and select **Connection > Disconnect**.

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

c Wait until the host is disconnected.

d Under the **lax01-m01dc** data center, right-click the **lax01m01esx01.lax01.rainpole.local** host object and select **Connection > Connect**.

e In the **Navigator**, under **Hosts and Cluster**, select **lax01m01esx01.lax01.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.

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

a Under the **lax01-m01dc** data center, select the **lax01m01vc01.lax01.rainpole.local** vCenter Server object and click the **Configure** tab.

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

c Verify the status for the `http://lax01m01esx01.lax01.rainpole.local:8080/version.xml` URL for 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.

9 Repeat the procedure for the rest of the management ESXi hosts in Region B.

Configure Certificate Mode for and Replace Certificates on the Hosts in the Shared Edge and Compute Cluster in Region B

After you replace the certificates of the ESXi hosts in the management cluster, complete certificate replacement in Region B on the hosts in the shared edge and compute cluster.

Table 2-6. Certificate Files Names for the Shared Edge and Compute Hosts in Region B

ESXi Hosts	Certificate File Names
lax01w01esx01.lax01.rainpole.local	■ lax01w01esx01.key ■ lax01w01esx01.1.cer
lax01w01esx02.lax01.rainpole.local	■ lax01w01esx02.key ■ lax01w01esx02.1.cer
lax01w01esx03.lax01.rainpole.local	■ lax01w01esx03.key ■ lax01w01esx03.1.cer
lax01w01esx04.lax01.rainpole.local	■ lax01w01esx04.key ■ lax01w01esx04.1.cer

Procedure

- Repeat Set Host Certificate Mode on the Management vCenter Server to Support a Custom Certificate Authority in Region B and Replace the Default Certificate with a Custom Certificate on the Management ESXi Hosts in Region B to replace the certificates on the hosts under the lax01w01vc01.lax01.rainpole.local vCenter Server.

Replace the NSX Manager Certificates in Region B

After you replace the certificates of all Platform Services Controller instances and all vCenter Server instances, replace the certificates for the NSX Manager instances in Region B. After you replace the certificates, to update them on the primary NSX Manager instances in Region A and on vRealize Operations Manager, reconnect NSX Manager to these components. You also re-establish the connection to vCenter Server and Platform Services Controller.

You replace certificates twice, once for each NSX Manager. You start by replacing certificates on NSX Manager for the lax01m01nsx01.lax01.rainpole.local management cluster.

Table 2-7. Certificate-Related Files on the NSX Manager Instances in Region B

NSX Manager FQDN	Certificate File Name	Replacement Time
lax01m01nsx01.lax01.rainpole.local	■ lax01m01nsx01.4.p12	First
lax01w01nsx01.lax01.rainpole.local	■ lax01w01nsx01.4.p12	Second

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 management cluster	https://lax01m01nsx01.lax01.rainpole.local
NSX Manager for the shared compute and edge cluster	https://lax01w01nsx01.lax01.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 **lax01m01nsx01.4.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**.

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

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

NSX Manager	URL
NSX Manager for the management cluster	https://lax01m01nsx01.lax01.rainpole.local
NSX Manager for the shared egde and compute cluster	https://lax01w01nsx01.lax01.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**, click the **Edit** button.

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

Setting	Value
Lookup Service IP	lax01psc01.lax01.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 the Management Cluster	Value for the NSX Manager for the Shared Edge and Compute Cluster
vCenter Server	lax01m01vc01.lax01.rainpole.local	lax01w01vc01.lax01.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 to the NSX Manager instance in Region A.

a Open a Web browser and go to **`https://lax01m01vc01.lax01.rainpole.local`**

b Log in using the following credentials.

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

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

d Click **Installation** in the **Navigator**.

e On the **Management** tab , select the **172.17.11.65** instance from the **NSX Manager** menu.

f Select **Actions > Disconnect from Primary NSX Manager**.

g On the **Management** tab , select the **172.16.11.65** instance from the **NSX Manager** drop-down menu.

h Select **Actions** > **Add Secondary NSX Manager**

i In the **Add Secondary NSX Manager** dialog box, enter the following settings and click **OK**.

Setting	Value
NSX Manager	172.17.11.65
Username	admin
Password	*mgmtnsx_admin_password*
Confirm Password	*mgmtnsx_admin_password*

j In the **Trust Certificate** confirmation dialog box, click **Yes**.

k Repeat the above for the NSX Manager instances for the shared edge and compute cluster.

Reconnect the 172.17.11.66 secondary NSX Manager for the shared edge and compute cluster in Region B to the primary NSX Manager 172.16.11.66 for the shared edge and compute cluster in Region A.

8 Repeat the steps for the NSX Manager instance for the shared edge and compute cluster.

9 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 Delete the certificates with the following CNs.

- `CN=lax0101nsx01.lax01.rainpole.local`
- `CN=lax01w01nsx01.lax01.rainpole.local`

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

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

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

h Click the **lax01m01nsx01-lax01** adapter instance, click **Test Connection**, accept the new certificate, and click **Save settings**.

i Click the **lax01w01nsx01-lax01** adapter instance, click **Test Connection**, accept the new certificate, click **Save settings** and click **Close**.

Replace vSphere Data Protection Certificates in Region B

After you use the VMware Validated Design Certificate Generation Utility (`CertGenVVD`) to generate certificates for the SDDC management components, replace the default VMware-signed certificate on vSphere Data Protection in Region B with the certificate that is generated by `CertGenVVD`.

Prerequisites

Generate the Microsoft CA-signed certificate by using the `CertGenVVD` tool. See Generate MSCA-Signed Certificates for the SDDC Management Components in Region B and Use the Certificate Generation Tool to Generate Certificate Signing Requests in Region B.

Procedure

1 Log in to the vSphere Data Protection appliance.

   a Open an SSH connection to the virtual machine lax01m01vdp01.lax01.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 the 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 the `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 into the keystore

```
keytool -importkeystore -srckeystore /tmp/.keystore --destkeystore /root/.keystore -srcstorepass
changeit -deststorepass changeit
```

6 Run the following command and in the command output verify whether 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 the VMware Site Recovery Manager Certificates in Region B

In a dual-region SDDC, you replace an expired certificate on Site Recovery Manager to keep this component trusted. You generate a custom certificate by using the `CertGenVVD` utility.

If you replace the certificates of all management components in Region B, you must replace the certificates of all Platform Services Controller, vCenter Server and NSX Manager instances before Site Recovery Manager.

Table 2-8. Certificate-Related Files for Site Recovery Manager in Region B

Hostname or Service	Certificate Files
lax01m01srm01.lax01.rainpole.local	lax01m01srm01.5.p12 chainRoot64.cer

Procedure

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

a Open an RDP connection to the following virtual machine.

Region	Site Recovery Manager
Region B	lax01m01srm01.lax01.rainpole.local

b Log in using the following credentials.

Setting	Value
User name	rainpole\svc-srm
Password	*svc-srm_password*

2 Install the CA certificates in the Windows trusted root certificate store of the Site Recovery Manager virtual machine.

   a Copy the CA certificate and PKCS#12 file from the Windows hosts where you run the `CertGenVVD` utility to the `C:\certs` folder.

   b Locate the `chainRoot64.cer` file in `C:\certs` folder.

   c Double-click the `chainRoot64.cer` file to open **Certificate** import dialog box.

   d In the **Certificate** dialog box, select the **Install Certificate** option.

   The **Certificate Import Wizard** appears.

   e Select the **Local Machine** option for the **Store Location** and click **Next**.

   f Select **Place all certificates in the following store** option, browse to select the **Trusted Root Certificate Authorities** store and click **OK**.

   g On the **Completing the Certificate Import Wizard** page, click **Finish**.

3 Replace the certificate on Site Recovery Manager with the one that you generated.

   a Open **Programs and Features** from the Windows Control Panel.

   b From the list of programs, select **VMware vCenter Site Recovery Manager** and click **Change**.

   c Select the **Modify** option on the **Maintenance Options** screen and follow the wizard until you reach the **Certificate Type** screen.

   d Select the **Use a PKCS#12 certificate file** option and click **Next**.

   e Browse to the `C:\certs` folder, select the `lax01m01srm01.lax01.5.p12` file, and enter the certificate password that you specified when generating the PKCS#12 file.

   f Click **Yes** in the certificate warning dialog box and complete the modify installation wizard.

4 Reconnect the two Site Recovery Manager sites.

   a Open a Web browser and go to **`https://lax01m01vc01.lax01.rainpole.local/vsphere-client`**.

   b Log in using the following credentials.

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

   c In the vSphere Web Client, click **Site Recovery > Sites**.

   d Right-click the site **lax01m01vc01.lax01.rainpole.local** and select **Reconfigure Pairing**.

e Enter the address of the Platform Services Controller **sfo01psc01.sfo01.rainpole.local** on the remote site and click **Next**.

f Select the vCenter Server instance **sfo01m01vc01.sfo01.rainpole.local** with which Site Recovery Manager is registered on the remote site, enter the user name **svc-srm@vsphere.local** and ***svc-srm_password*** password, and click **Finish**.

Replace the CA-Signed Certificate on vSphere Replication in Region B

In a dual-region SDDC, replace the certificate on vSphere Replication in Region B, for example if the certificate expires, to maintain your environment secure and trusted. Reconnect the sites in Region A and Region B to update the new certificate on Region A.

Table 2-9. PKCS#12 Files for vSphere Replication in Region B

vSphere Replication FQDN	PKCS#12 File Name from the CertGenVVD Tool
lax01m01vrms01.lax01.rainpole.local	lax01m01vrms01.5.p12

Procedure

1 Upload the PKCS#12 file to vSphere Replication by using the vSphere Replication appliance management interface (VAMI).

a Open a Web browser and go to the following URL.

vSphere Replication	URL
vSphere Replication in Region B	https://lax01m01vrms01.lax01.rainpole.local:5480

b Log in using the following credentials.

Setting	Value
User name	root
Password	*vr_root_password*

c On the **VR** tab, click the **Configuration** tab.

d Enter the password of the service account svc-vr@rainpole.local.

e Click **Choose File** next to **Upload PKCS#12 (*.pfx) file** and locate the `lax01m01vrms01.5.p12` file on your local file system.

f Click the **Upload and Install** button and enter the certificate password when prompted.

After you change the SSL certificate, the vSphere Replication status changes to disconnected because the new certificate is not trusted by the vSphere Replication instance on the other site.

2 Reconnect the sites to resolve the connection issue.

a Open a Web browser and go to **`https://lax01m01vc01.lax01.rainpole.local/vsphere-client`**.

b Log in using the following credentials.

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

c On the vSphere Web Client **Home** page, click **vSphere Replication**.

d Select **lax01m01vc01.lax01.rainpole.local**, click **Manage**, and select **Target Sites**.

e Right-click **sfo01m01vc01.sfo01.rainpole.local** and click **Reconnect site**.

f In the **Reconnect Sites** dialog box, click **Yes** to proceed.

Replace Certificates of the Operations Management Components in Region B

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

Replace the Certificate to vRealize Log Insight in Region B

After you 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 in Region B 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://lax01vrli01.lax01.rainpole.local`**.

b Log in using the following credentials.

Setting	Value
User name	admin
Password	*vrli_admin_password*

2 In the vRealize Log Insight UI, 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 `vrli.lax01.2.chain.pem` file on your computer, and click **Save**.

The certificate is uploaded to vRealize Log Insight.

5 Open a Web browser, go to **`https://lax01vrli01.lax01.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 the **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 the **Manage certificates** button, and in the **Certificates** dialog box import `vrli.lax01.2.chain.pem`.

You can also use Certificate Manager on Windows or Keychain Access on MAC OS X.

Update the SSL Certificate for Event Forwarding to Region A

After you replace the certificate of vRealize Log Insight in Region B, you update log forwarding from vRealize Log Insight in Region A to vRealize Log Insight in Region B. Log forwarding in this validated design uses SSL connection to exchange log data

Procedure

1 Import the root certificate in the Java truststore on each vRealize Log Insight node in Region A.

a Open an SSH session to the vRealize Log Insight node.

Name	Role
sfo01vrli01a.sfo01.rainpole.local	Master node
sfo01vrli01b.sfo01.rainpole.local	Worker node 1
sfo01vrli01c.sfo01.rainpole.local	Worker node 2

b Log in using the following credentials.

Setting	Value
User name	root
Password	*vrli_regionA_root_password*

c Create a working directory on the vRealize Log Insight node.

```
mkdir /tmp/ssl
cd /tmp/ssl
```

d Extract the root certificate from the destination vRealize Log Insight in Region A.

```
echo "" | openssl s_client –showcerts –servername lax01vrli01a.lax01.rainpole.local –connect
lax01vrli01a.lax01.rainpole.local:443 –prexit 2>/dev/null | sed –n –e '/BEGIN\
CERTIFICATE/,/END\ CERTIFICATE/ p' > cert.pem
csplit –f individual– cert.pem '/–––––BEGIN CERTIFICATE–––––/' '{*}'
root_cert=$(ls individual–* | sort –n –t– | tail –1)
cp –f –– "$root_cert" root.crt
```

e Import the root certificate in the Java truststore of the vRealize Log Insight node in Region A.

```
cd /usr/java/default/lib/security/

../../bin/keytool –import –alias loginsight –file /tmp/ssl/root.crt –keystore cacerts
```

f When prompted for a keystore password, type **changeit**

g When prompted to accept the certificate, type **yes**

h Reboot the vRealize Log Insight node.

```
reboot
```

i Repeat this operation on all vRealize Log Insight nodes in Region A.

2 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*

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

4 Under **Management**, click **Event Forwarding**.

5 On the **Event Forwarding** page, select **SFO01 to LAX01** and select the **Edit** icon.

6 In the **Edit Destination** dialog box, click **Test** to verify that the connection settings are correct.

7 Click **Save** to save the forwarding new destination.