Certificate Replacement

21 AUG 2018
VMware Validated Design 4.3
VMware Validated Design for Software-Defined Data Center 4.3

vmware®

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

https://docs.vmware.com/

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

docfeedback@vmware.com

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

Contents

About VMware Validated Design Certificate Replacement

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)
   a. Use the VMware Validated Design Certificate Generation utility to automatically generate the certificates for all components.
   b. 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

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

- Create and Add a Microsoft Certificate Authority Template

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

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

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

- Generate Certificate Signing Requests and Certificates from a Third-Party CA 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.

- Replace Certificates of the Virtual Infrastructure Components in Region A

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

- Replace Certificates of the Operations Management Components 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 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.

- Replace Certificates of the Business Continuity Components in Region A

  In a dual-region environment, after you generate the signed certificates for Site Recovery Manager and vSphere Replication, replace and update the certificates on the connected management components in the region to maintain secure connection.

Create and Add a Microsoft Certificate Authority Template

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

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

1 Set up a Microsoft Certificate Authority template.

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

Prerequisites

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

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

Procedure

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

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

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

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

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

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

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

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

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

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

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

Prerequisites

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

Procedure

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

4 Verify that the following properties are configured.

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

5 Verify that the `C:\CertGenVVD-`*`version`*`\ConfigFiles` folder contains only the 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
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 LifeCycle Manager	vrslcm01svr01a.rainpole.local	vrslcm01svr01a.txt
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.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` subfolder.

12 In `C:\CertGenVVD-version\SignedByMSCACerts\Root64` subfolder, rename `chainRoot64.cer` to `Root64.cer`.

What to do next

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

Prerequisites

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

Procedure

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

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

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

4 Verify that following properties are configured.

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

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

Table 1-2. Certificate Generation Files for 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
Site Recovery Manager and vSphere Replication	sfo01m01srm01.sfo01.rainpole.local	sfo01m01srm01.txt
	sfo01m01vrms01.sfo01.rainpole.local	sfo01m01vrms01.txt
Cloud Management Platform Layer		

Table 1-2. 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 LifeCycle Manager	vrslcm01svr01a.rainpole.local	vrslcm01svr01a.txt
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
Business Continuity		
Site Recovery Manager and vSphere Replication	sfo01m01srm01.sfo01.rainpole.local	sfo01m01srm01.txt
	sfo01m01vrms01.sfo01.rainpole.local	sfo01m01vrms01.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.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 request the signed certificates.

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

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

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

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

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

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

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

What to do next

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

Replace Certificates of the Virtual Infrastructure Components in Region A

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

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

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

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

Procedure

1 Replace the Platform Services Controller Certificates in Region A

2 Replace the vCenter Server Certificates in Region A

Replace the certificate on each vCenter Server instance in Region A and reconnect it to the other management components to update the new certificate 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

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

Replace the Platform Services Controller Certificates 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 Direct Traffic to Compute Platform Services Controller in Region A

Before you replace the certificate of the Platform Services Controller pair in Region A, disable the Platform Services Controller for the management cluster sfo01m01psc01 in the load balancer to route all traffic to the Platform Services Controller for the compute cluster sfo01w01psc01.

2 Replace the Platform Services Controller Certificates in Region A

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

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

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

4 Re-Enable Compute Platform Services Controller on the Load Balancer in Region A

After you replace the certificate on the Platform Services Controller instances, reenable load balancing the network traffic between them.

What to do next

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

Direct Traffic to Compute Platform Services Controller in Region A

Before you replace the certificate of the Platform Services Controller pair in Region A, disable the Platform Services Controller for the management cluster sfo01m01psc01 in the load balancer to route all traffic to the Platform Services Controller for the compute cluster sfo01w01psc01.

Procedure

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

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

   b Log in using the following credentials.

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

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

3 In the **Navigator**, click **NSX Edges**.

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

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

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

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

8 Select the **sfo01m01psc01** member, click **Edit**, select **Disable** from the **State** drop-down menu, and click **OK**.

9 Repeat the procedure to disable sfo01m01psc01 in **pool-2**.

Replace the Platform Services Controller Certificates in Region A

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

The machine certificate on both Platform Services Controller instances in the region must be the same because they are load-balanced according to this validated design. The certificate must have the same common name as the load-balanced Fully Qualified Domain Name (FQDN). Each Platform Services Controller FQDN and short name, as well as the load-balanced FQDN and short name must be in the Subject Alternative Name (SAN) of the generated certificate.

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

Platform Services Controller	Certificate Filename
sfo01m01psc01.sfo01.rainpole.local	■ sfo01psc01.1.cer ■ sfo01psc01.key ■ Root64.cer
sfo01w01psc01.sfo01.rainpole.local	■ sfo01psc01.1.cer ■ sfo01psc01.key ■ Root64.cer

Procedure

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

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

   b Log in using the following credentials.

Setting	Value
User name	root
Password	*psc_root_password*

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

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

3 Copy the generated certificates to the Platform Services Controller.

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

```
mkdir –p /root/certs
```

   b Copy the certificate files `sfo01psc01.1.cer`, `sfo01psc01.key`, and `Root64.cer` to the `/root/certs` folder.

   You can use an `scp` software like WinSCP.

4 Replace the certificate on the Platform Services Controller.

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

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

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

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

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

e When prompted for the custom certificate, enter **`/root/certs/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/Root64.cer`**.

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

The Platform Services Controller services automatically restart.

5 Verify that the new certificate has been installed successfully.

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

b Verify that the Web browser shows the new certificate.

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

```
service vami-lighttp restart
cd /root/certs
rm sfo01psc01.1.cer sfo01psc01.key Root64.cer
```

7 Switch the shell back to the appliance shell.

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

8 Redirect all traffic from the Compute and Edge Platform Services Controller to the Management Platform Services Controller. See Direct Traffic to Compute Platform Services Controller in Region A

Setting	Value
NSX Manager	172.16.11.65
NSX Edge device	sfo01psc01
Platform Services Controller to re-enable	sfo01m01psc01
Platform Services Controller to disable	sfo01w01psc01
Pools	■ pool-1 ■ pool-2

9 Repeat the procedure 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 certificate on a Platform Services Controller instance, update the certificate on the vCenter Server and NSX Manager instances in the region.

Procedure

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

   a Open an SSH connection to the sfo01m01vc01.sfo01.rainpole.local virtual machine.

   b Log in using the following credentials.

Setting	Value
User name	root
Password	*vcenter_server_root_password*

2 Restart the services of vCenter Server.

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

```
shell
```

   b Restart vCenter Server services by using the following command.

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

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

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

   See Connect NSX Manager to vCenter Server in Region A.

5 Reconnect Site Recovery Manager and vSphere Replication to Platform Services Controller and vCenter Server after you install the custom certificates on the nodes.

   See Update Management vCenter Server Certificate on Site Recovery Manager in Region A and Register vSphere Replication with vCenter Single Sign-On in Region A

Re-Enable Compute Platform Services Controller on the Load Balancer in Region A

After you replace the certificate on the Platform Services Controller instances, reenable load balancing the network traffic between them.

Procedure

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

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

   b Log in using the following credentials.

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

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

3 In the **Navigator**, click **NSX Edges**.

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

5 Restore the load balancer configuration.

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

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

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

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

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

Replace the vCenter Server Certificates in Region A

Replace the certificate on each vCenter Server instance in Region A and reconnect it to the other management components to update the new certificate on these components.

Procedure

1 Replace the Certificate of the Management vCenter Server in Region A

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

2 Connect NSX Manager to vCenter Server in Region A

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

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

4 Update the vCenter Server Certificates on vRealize Operations Managerin Region A

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

5 Update Management vCenter Server Certificate on Site Recovery Manager in Region A

After you replace the certificate of the Platform Services Controller pair or of the Management vCenter Server, update the certificate on the connected Site Recovery Manager instance in Region A to reestablish trust.

6 Register vSphere Replication with vCenter Single Sign-On in Region A

Replace the Certificate of the Management vCenter Server in Region A

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

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

vCenter Server FQDN	Files for Certificate Replacement
sfo01m01vc01.sfo01.rainpole.local	■ sfo01m01vc01.key ■ sfo01m01vc01.1.cer ■ Root64.cer
sfo01w01vc01.sfo01.rainpole.local	■ sfo01w01vc01.key ■ sfo01w01vc01.1.cer ■ Root64.cer

Procedure

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

a Open an SSH connection to the sfo01m01vc01.sfo01.rainpole.local virtual machine.

b Log in using the following credentials.

Setting	Value
User name	root
Password	*vcenter_server_root_password*

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

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

3 Copy the generated certificates to the vCenter Server Appliance.

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

```
mkdir –p /root/certs
```

b Copy the certificate files `sfo01m01vc01.1.cer`, `sfo01m01vc01.key`, and `Root64.cer` to the `/root/certs` folder.

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

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

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

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

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

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

vCenter Server instance	IP Address of managing Platform Services Controller
sfo01m01vc01.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 copied over 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/Root64.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/Root64.cer**

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

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

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

   b Verify that you see the new certificate.

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

```
service vami-lighttp restart
cd /root/certs/
rm sfo01m01vc01.1.cer sfo01m01vc01.key Root64.cer
```

8 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 vCenter Server 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 URL**, click **Edit**.

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

Setting	Value
Lookup Service Host	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 URL 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.

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

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

Procedure

1 Reconnect vRealize Orchestrator to vCenter Server.

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

   b Click **Start Orchestrator Client**.

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

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

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

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

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

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

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

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

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

2 Reconnect vRealize Business to vCenter Server.

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

b Log in using the following credentials.

Setting	Value
User name	root
Password	*vrb_root_password*

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

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

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

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

3 Recreate the vSphere endpoint in vRealize Automation.

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

b Log in using the following credentials.

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

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

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

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

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

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

After you change the certificate of a vCenter Server instance 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 rows that contain `CN=sfo01m01vc01.sfo01.rainpole.local` and `CN=sfo01w01vc01.sfo01.rainpole.local`, and click the **Delete** icon.

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

6 Reconnect each vCenter Adapter.

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

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

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

7 Reconnect the VMware vSAN adapter for the management cluster.

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

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

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

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

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

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

Update Management vCenter Server Certificate on Site Recovery Manager in Region A

After you replace the certificate of the Platform Services Controller pair or of the Management vCenter Server, update the certificate on the connected Site Recovery Manager instance in Region A to reestablish trust.

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	Value
User name	Windows administrator user
Password	*windows_administrator_password*

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

3 Select **VMware vCenter Site Recovery Manager** and click **Change**.

   The VMware Site Recovery Manager installation wizard appears.

4 On the **Welcome** page, click **Next**.

5 On the **Program Maintenance** page, select **Modify** and click **Next**.

6 On the **vSphere Platform Services Controller** page, enter the password for authentication to Platform Services Controller, verify that the settings are correct and click **Next**.

Setting	Value
Address	sfo01psc01.sfo01.rainpole.local
HTTPS Port	443
User name	**`svc-srm@rainpole.local`**
Password	***`svc-srm_password`***

7 When prompted to accept the certificate in the **Platform Services Controller Certificate** dialog box, click **Accept**.

8 On the **VMware vCenter Server** page, click **Next**.

9 When prompted to accept the certificate in the **vCenter Server Certificate** dialog box, click **Accept**.

10 On the **Site Recovery Manager Extension** page, leave the existing settings, and click **Next**.

Setting	Value
Administrator email	*srm_admin_sfo_email_address*
Local Host	172.16.11.124
Listener Port	9086

11 On the **Certificate Type** page, select **Use existing certificate** and click **Next**.

12 On the **Database Server Selection** page, select **Use the embedded database server** and click **Next**.

13 On the **Embedded Database Configuration** page, enter the database password, leave the existing settings and click **Next**.

Setting	Value
Data Source Name	SRM_SITE_SFO
Database User Name	srm_db_admin
Database Password	***srm_db_admin_sfo_password***
Database Port	5678
Connection Count	5
Max. Connections	20

14 On the **Site Recovery Manager Service Account** page, enter password for the administrator user, leave the existing credentials, and click **Next**.

	Value
Use Local System account	Deselected
User name	MGMT01SRM01\Administrator
Password	*mgmt01srm01_admin_password*

15 On the **Ready to Install the Program** page, click **Install**.

16 Click **Finish** to complete the installation.

17 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*

18 Reconnect the Site Recovery Manager instance in Region A.

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

b On the **Site Recovery** page, click **Sites**.

c On the **Sites** page, right-click **mgmt01vc01.sfo01.rainpole.local** and select **Reconfigure Pairing**.

The **Reconfigure Site Recovery Manager Server Pairing** wizard appears.

d On the **Select Site** page, validate the following settings and click **Next**.

Settings	Value
PSC address	lax01psc01.lax01.rainpole.local
Port	443

e On the **Select vCenter Server** page, enter the administrator@vsphere.local password, validate the following settings, and click **Finish**.

Settings	Value
vCenter Servers with matching SRM Extension	lax01m01vc01.lax01.rainpole.local
User name	svc-srm@rainpole.local
Password	*svc-srm_password*

Register vSphere Replication with vCenter Single Sign-On in Region A

After you replace the default or expiring certificate on the vSphere Replication appliance, reconnect it to vCenter Single Sign-On on the Platform Services Controller pair in the region.

Procedure

1 Log in to the Virtual Appliance Management Interface of the vSphere Replication appliance.

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

b Log in using the following credentials.

Settings	Value
User name	root
Password	*vr_sfo_root_password*

2 On the **VR** tab, click **Configuration**, enter the following settings, and click **Save and Restart Service**.

Setting	Value
Configuration Mode	Configure using the embedded database
LookupService Address	sfo01psc01.sfo01.rainpole.local
SSO Administrative Account	svc-vr@rainpole.local
Password	*svc-vr_password*

Setting	Value
vSphere Replication Manager Host	172.16.11.123
vSphere Replication Site Name	sfo01m01vc01.sfo01.rainpole.local
vCenter Server Address	sfo01m01vc01.sfo01.rainpole.local
vCenter Server Port	80
vCenter Server Admin Mail	*vcenter_server_admin_email*

3 In the **Confirm SSL Certificate** dialog box, click **Accept**.

4 Wait for the vSphere Replication Management server to save the configuration.

5 Under **Service Status**, verify that the status of the vSphere Replication service is `running`.

Note If a `Bad exit code: 1` error appears, restart the sfo01m01vrms01 virtual machine. Refer to KB article 2112332.

6 Log out from the vSphere Replication appliance management interface.

7 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 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. You set the host certificate mode on vCenter Server to support a custom certificate authority to prevent the vCenter Server from replacing certificates on to the ESXi hosts.

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

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

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. You set the host certificate mode on vCenter Server to support a custom certificate authority to prevent the vCenter Server from replacing certificates on to the ESXi hosts.

vCenter Server	ESXi Host
sfo01m01vc01.sfo01.rainpole.local	sfo01m01esx01.sfo01.rainpole.local
	sfo01m01esx02.sfo01.rainpole.local
	sfo01m01esx03.sfo01.rainpole.local
	sfo01m01esx04.sfo01.rainpole.local

Procedure

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

a Open a Web browser and go to **`https://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 Verify that all CA certificates from vCenter Server are updated on all hosts.

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

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

   c Repeat the steps for the ESXi hosts that are controlled by the Management vCenter Server sfo01m01vc01.sfo01.rainpole.local.

3 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**.

4 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	*vcenter_server_root_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 the region and configure vCenter Server to accept custom certificate authorities, replace the default VMware Certificate Authority (VMCA) signed certificates with the custom ones on the hosts.

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

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

ESXi Hosts	Certificate Filenames
sfo01m01esx01.sfo01.rainpole.local	■ sfo01m01esx01.key ■ sfo01m01esx01.1.cer
sfo01m01esx02.sfo01.rainpole.local	■ sfo01m01esx02.key ■ sfo01m01esx02.1.cer

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

ESXi Hosts	Certificate Filenames
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 the **Start** button if the status is not showing up as **Running**

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

3 Place the host in maintenance mode.

   a Under the sfo01-m01dc data center, right-click the **sfo01m01esx01.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/vsphere-client`**.

b Log in using the following credentials.

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

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

d Under the sfo01-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.locall 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** host object and select **Connection > Disconnect**.

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

c Wait until the host is disconnected.

d Right-click the **sfo01m01esx01.sfo01.rainpole.local** host object and select **Connection > Connect**.

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

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

a Select the **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 the region.

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

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

Procedure

1. Replace the Certificate of NSX Manager for the Management Cluster in Region A
2. Connect NSX Manager to the Management vCenter Server in Region A
3. Re-Join Secondary NSX Manager to Primary NSX Manager in Region A

   After you replace the certificate on the NSX Manager in Region A, update its certificate on the paired NSX Manager in Region B.
4. Replace the NSX Manager Certificate for the Shared Edge and Compute Cluster in Region A

   After you deploy the NSX Manager appliance, replace the default certificate to establish a trusted connection with the management components in the SDDC. The certificate generated by the `CertGenVVD` utility is signed by a certificate authority (CA) on the parent Active Directory server.
5. Reconnect NSX Manager in Region A to vRealize Operations Manager

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

Replace the Certificate of NSX Manager for the Management Cluster in Region A

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

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

Table 1-7. Certificate-Related Files on the NSX Manager Instance for the Management Cluster in Region A

NSX Manager FQDN	Certificate Filename
sfo01m01nsx01.sfo01.rainpole.local	sfo01m01nsx01.4.p12

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 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 propagate the CA-signed certificate.

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

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

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

Connect NSX Manager to the Management vCenter Server in Region A

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

Procedure

1 Log in to the 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 URL**, click **Edit**.

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

Setting	Value
Lookup Service Host	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
vCenter Server	sfo01m01vc01.sfo01.rainpole.local
vCenter User Name	svc-nsxmanager@rainpole.local
Password	*svc-nsxmanager_password*

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

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

Re-Join Secondary NSX Manager to Primary NSX Manager in Region A

After you replace the certificate on the NSX Manager in Region A, update its certificate on the paired NSX Manager in Region B.

Procedure

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

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

   b Log in using the following credentials.

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

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

3 In the **Navigator**, click **Installation and Upgrade**.

4 From the **NSX Managers** tab, verify if there are any **SYNC ISSUES** for NSX Manager **172.16.11.65**.

5 If there are **SYNC ISSUES**, select the **172.16.11.65** NSX Manager.

6 Select **Actions > Update Secondary Manager**.

7 On **Update Secondary Manager** window, enter the following values and click **UPDATE**

Settings	Values
Primary NSX Manager	172.16.11.65
NSX Manager	172.17.11.65
New IP address/Hostname	172.17.11.65

8 Verify that all **SYNC ISSUES** are resolved.

Replace the NSX Manager Certificate for the Shared Edge and Compute Cluster in Region A

After you deploy the NSX Manager appliance, replace the default certificate to establish a trusted connection with the management components in the SDDC. The certificate generated by the `CertGenVVD` utility is signed by a certificate authority (CA) on the parent Active Directory server.

Use the following files to replace the certificate on NSX Manager for the shared edge and compute cluster.

Table 1-8. Certificate-Related Files on the NSX Manager Instance for the Shared Edge and Compute Cluster in Region A

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

Procedure

1 Log in to the Compute NSX Manager appliance user interface.

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

   b Log in using the following credentials.

Setting	Value
User name	admin
Password	*nsx_manager_admin_password*

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

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

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

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

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

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

6 Repeat Connect NSX Manager to the Management vCenter Server in Region A procedure for the compute NSX Manager.

7 Repeat Re-Join Secondary NSX Manager to Primary NSX Manager in Region A procedure for the compute NSX Manager with the following values.

Settings	Values
Primary NSX Manager	172.16.11.66
NSX Manager	172.17.11.66
New IP address/Hostname	172.17.11.66

Reconnect NSX Manager in Region A to vRealize Operations Manager

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

Procedure

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

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

   b Log in using the following credentials.

Setting	Value
User name	admin
Password	*vrops_admin_password*

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

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

4 Delete the certificates with the following CNs.

- `CN=sfo01m01nsx01.sfo01.rainpole.local`
- `CN=sfo01w01nsx01.sfo01.rainpole.local`

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

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

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

8 Click the **sfo01m01nsx01-sfo01** adapter instance, click **Test Connection**, accept the new certificate, and click **Save settings**.

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

Replace Certificates of the Operations Management Components 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 Certificate on the vRealize Suite Lifecycle Manager Appliance in Region A

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

2 Replace vRealize Operations Manager Certificate in Region A

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

3 Replace vRealize Log Insight Certificate in Region A

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

4 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. You skip this procedure if the root certificate (Certificate Authority) in vRealize Log Insight in Region A is not replaced.

Replace Certificate on the vRealize Suite Lifecycle Manager Appliance in Region A

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

Procedure

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

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

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

You can use SCP software like WinSCP.

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

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

b Log in using following credentials.

Setting	Value
User name	root
Password	*vrslcm_root_password*

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

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

```
systemctl restart vlcm-xserver
```

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

```
systemctl status vlcm-xserver
```

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

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

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

Replace vRealize Operations Manager Certificate in Region A

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

Procedure

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

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

   b Log in using the following credentials.

Setting	Value
User name	admin
Password	*vrops_admin_password*

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

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

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

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

Replace vRealize Log Insight Certificate in Region A

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

Procedure

1 Log in to the vRealize Log Insight user interface.

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

   b Log in using the following credentials.

Setting	Value
User name	admin
Password	*vrli_admin_password*

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

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

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

Certificate Generation Option	Certificate File
Using the CertGenVVD tool	`vrli.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 icon in the address bar of the browser, and verify that **Subject Alternative Name** contains the names of the vRealize Log Insight cluster nodes.

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. You skip this procedure if the root certificate (Certificate Authority) in vRealize Log Insight in Region A is not replaced.

Procedure

1 Open a Secure Shell connection to the vRealize Log Insight node.

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.

Setting	Value
User Name	root
Password	*vrli_regionB_root_password*

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

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

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

b 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
```

c 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
```

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

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

f Reboot the vRealize Log Insight node.

```
reboot
```

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

3 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*

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

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

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

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

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

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

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

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

3 Update the vRealize Automation Certificate on vRealize Operations Manager in Region A

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

4 Replace the Certificate on vRealize Business for Cloud Server in Region A

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

Replace the vRealize Automation Certificate in Region A

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

Procedure

1 Log in to the first vRealize Automation appliance.

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

b Log in using the following credentials.

Settings	Value
User name	root
Password	*vra_appA_root_password*

2 On the **vRA Settings** tab, click the **Database** subtab and check which node has the `MASTER` label.

If the vra01svr01a.rainpole.local appliance is not listed as the `MASTER` node, log in to the management console of the `MASTER` appliance using the previous instruction.

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

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

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

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

6 Verify that all cluster nodes have been successfully updated.

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

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

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

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

Procedure

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

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

b Log in using the following credentials.

Setting	Value
User Name	root
Password	*vro_appA_root_password*

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

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

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

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

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

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

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

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

   When prompted, press Y to accept the new certificate.

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

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

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

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

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

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

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

6 Re-Authenticate vRealize Automation with the embedded vRealize Orchestrator

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

   b Log in using the following credentials.

Setting	Value
User Name	root
Password	*vra_root_password*

   c Click **Configure Authentication Provider**.

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

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

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

7 Restart vRealize Orchestrator servers

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

b Log in using the following credentials.

Setting	Value
User Name	root
Password	*vra_root_password*

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

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

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

8 Validate the embedded vRealize Orchestrator configuration.

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

b Log in using the following credentials.

Setting	Value
User Name	root
Password	*vra_root_password*

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

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

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

b Log in using the following credentials.

Setting	Value
User name	root
Password	*vrb_server_root_password*

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

Setting	Value
Hostname	vra01svr01.rainpole.local
SSO Default Tenant	rainpole
SSO Admin User	svc-vra

Setting	Value
SSO Admin Password	*svc-vra_password*
Accept vRealize Automation Certificate	Deselected

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

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

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

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

SSO Status changes to `Connected to vRealize Automation`.

Update the vRealize Automation Certificate on vRealize Operations Manager in Region A

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

Procedure

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

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

b Log in using the following credentials.

Setting	Value
User name	admin
Password	*vrops_admin_password*

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

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

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

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

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

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

Replace the Certificate on vRealize Business for Cloud Server in Region A

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

Procedure

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

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

   b Log in using the following credentials.

Setting	Value
User name	root
Password	*vrb_server_root_password*

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

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

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

Setting	Value
Choose mode	Import PEM encoded Certificate

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

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

Private Key Passphrase	*vrb_cert_passphrase*

   The `Successfully imported the certificate` message appears.

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

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

Replace Certificates of the Business Continuity Components in Region A

In a dual-region environment, after you generate the signed certificates for Site Recovery Manager and vSphere Replication, replace and update the certificates on the connected management components in the region to maintain secure connection.

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 the communication with this component trusted. You generate a custom certificate by using the `CertGenVVD` utility. Pair the Site Recovery Manager instances again in the two regions to re-establish the trusted 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	Value
User name	Windows administrator user
Password	*windows_administrator_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 `Root64.cer` file in the `C:\certs` folder to open the **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/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 **sfo01m01vc01.sfo01.rainpole.local** and select **Reconfigure Pairing**.

e Enter the address of the Platform Services Controller **`lax01m01psc01.lax01.rainpole.local`** on the remote site and click **Next**.

f Select the vCenter Server instance **lax01m01psc01.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

Replace the certificates on vSphere Replication to reestablish secure communication with connected management solutions.

Table 1-9. PKCS#12 Files for vSphere Replication in Region A

vSphere Replication	PKCS#12 Filename 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 **`https://sfo01m01vrms01.sfo01.rainpole.local:5480`**.

   b Log in using the following credentials.

Settings	Value
User name	root
Password	*vr_sfo_root_password*

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

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

   e Click the **Upload and Install** button.

   f Enter the certificate password when prompted and click **OK**.

   g If prompted, click **OK** in the certificate dialog box.

   After you apply the SSL certificate, the VAMI session of vSphere Replication is closed.

2 Log in again by using the root credential.

3 On the **VR** tab, click the **Security** tab.

4 Verify that the **Current SSL Certificate** shows the updated certificate information.

Region B Certificate Replacement

2

In a dual-region environment, after you replace the certificates in Region A, you continue with the certificate replacement on the SDDC 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. The template contains the certificate authority (CA) attributes for signing certificates of VMware SDDC solutions. After you create the new template, you add it to the certificate templates of the Microsoft CA.

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

- 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 Business Continuity Components in Region B

  In a dual-region environment, after you generate signed certificates for Site Recovery Manager and vSphere Replication, replace them and update them on the connected management components in Region B to maintain secure connection.

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. The template contains the certificate authority (CA) attributes for signing certificates of VMware SDDC solutions. After you create the new template, you add it to the certificate templates of the Microsoft CA.

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 are installed and configured on the Active Directory Server.
- Verify that dc51lax.lax01.rainpole.local is the intermediate CA of the root CA dc51rpl.rainpole.local.
- Use a hashing algorithm of SHA-256 or higher on the certificate authority.

Procedure

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

Setting	Value
FQDN	■ If you use the intermediate CA, connect to dc51lax.lax01.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 check if 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 **Name** column of the **Enable Certificate Templates** dialog box, select the VMware certificate that you just created 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 *VMware Validated Design Planning and Preparation*.

Prerequisites

To use certificates that are signed by an intermediate CA, provide the following configuration:

- Provide a Window Server 2012 host that is part of the lax01.rainpole.local domain.
- Install an intermediate CA server on 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 the 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
	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
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 ■ lax01vrli01a.lax01.rainpole.local ■ lax01vrli01b.lax01.rainpole.local ■ lax01vrli01c.lax01.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.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.

12 In the `C:\CertGenVVD-version\SignedByMSCACerts\Root64` folder, rename `chainRoot64.cer` to `Root64.cer`.

What to do next

Replace the default certificates with the certificates that the `CertGenVVD` utility has generated. See Replace Certificates of the Virtual Infrastructure Components in Region B and Replace Certificates of the Operations Management Components 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 the following properties are configured.

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

5. Verify that 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

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

Host Name or Service in Region B		Configuration Files
	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
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 ■ lax01vrli01a.lax01.rainpole.local ■ lax01vrli01b.lax01.rainpole.local ■ lax01vrli01c.lax01.rainpole.local	vrli.lax01.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:

lax01psc01.txt

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

What to do next

Replace the product certificates with the certificates that the `CertGenVVD` utility has generated. See Replace Certificates of the Virtual Infrastructure Components in Region B and Replace Certificates of the Operations Management Components in Region B.

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 certificate on each vCenter Server in Region B and reconnect it to the other management components to update the new certificate 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

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

Replace the Platform Services Controller Certificates 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 Direct Traffic to Compute Platform Services Controller in Region B

Before you replace the certificate of the Platform Services Controller pair in Region B, disable the Platform Services Controller for the management cluster lax01m01psc01.lax01.rainpole.local in the load balancer to route all traffic to the Platform Services Controller for the shared edge and compute cluster lax01w01psc01.lax01.rainpole.local.

2 Replace the Platform Services Controller Certificates in Region B

To establish a trusted connection with the other SDDC management components, you replace the machine SSL certificate on each Platform Services Controller instance in Region B with a custom certificate signed by the certificate authority (CA) available on the parent Active Directory (AD) server or on the intermediate Active Directory (AD) server.

3 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 and NSX Manager instances.

4 Re-Enable Compute Platform Services Controller on the Load Balancer in Region B

After you replace the certificate on the Platform Services Controller instances in Region B, reenable load balancing the network traffic between them.

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.

Direct Traffic to Compute Platform Services Controller in Region B

Before you replace the certificate of the Platform Services Controller pair in Region B, disable the Platform Services Controller for the management cluster lax01m01psc01.lax01.rainpole.local in the load balancer to route all traffic to the Platform Services Controller for the shared edge and compute cluster lax01w01psc01.lax01.rainpole.local.

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

3 In the **Navigator**, click **NSX Edges**.

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

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

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

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

8 Select the **lax01m01psc01** member, click **Edit**, select **Disable** from the **State** drop-down menu, and click **OK**.

9 Repeat the procedure to disable **lax01m01psc01** in **pool-2**.

Replace the Platform Services Controller Certificates in Region B

To establish a trusted connection with the other SDDC management components, you replace the machine SSL certificate on each Platform Services Controller instance in Region B with a custom certificate signed by the certificate authority (CA) available on the parent Active Directory (AD) server or on the intermediate Active Directory (AD) server.

The machine certificate on both Platform Services Controller instances in the region must be the same because they are load-balanced according to this Validated Design. 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, as well as the load-balanced FQDN and short name must be in the Subject Alternative Name (SAN) of the generated certificate.

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

Platform Services Controller	Certificate Filename
lax01m01psc01.lax01.rainpole.local	■ `lax01psc01.1.cer` ■ `lax01psc01.key` ■ `Root64.cer`
lax01w01psc01.lax01.rainpole.local	■ `lax01psc01.1.cer` ■ `lax01psc01.key` ■ `Root64.cer`

Procedure

1 Open a Secure Shell (SSH) connection to the Platform Services Controller virtual machine.

   a Open an SSH connection to lax01m01psc01.lax01.rainpole.local and log in with the following credentials.

Setting	Value
User name	root
Password	*mgmtpsc_root_password*

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

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

3 Copy the generated certificates to the Platform Services Controllers.

   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 `Root64.cer` to the `/root/certs` folder.

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

4 Replace the certificate on the Platform Services Controller instance.

a Start the vSphere Certificate Manager utility on 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.

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/Root64.cer`**

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

The Platform Services Controller services automatically restart.

5 Verify that the new certificate has been installed successfully.

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

b Verify that the Web browser shows the new certificate.

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

```
service vami-lighttp restart
cd /root/certs
rm lax01psc01.1.cer lax01psc01.key Root64.cer
```

7 Switch the shell back to the appliance shell.

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

8 Redirect all traffic from the Compute and Edge Platform Services Controller to the Management Platform Services Controller. See Direct Traffic to Compute Platform Services Controller in Region A

Setting	Value
NSX Manager	172.17.11.65
NSX Edge device	lax01psc01
Platform Services Controller to re-enable	lax01m01psc01

Setting	Value
Platform Services Controller to disable	lax01w01psc01
Pools	■ pool-1 ■ pool-2

9 Repeat the procedure 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 and NSX Manager instances.

Procedure

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

a Open an SSH connection to the virtual machine lax01m01vc01.lax01.rainpole.local.

b Log in using the following credentials.

Setting	Value
User name	root
Password	*vcenter_server_root_password*

2 Restart the services on the Management vCenter Server.

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

```
shell
```

b Restart vCenter Server services by using the following command.

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

c Repeat the steps to restart the services on the lax01w01vc01.lax01.rainpole.local vCenter Server.

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

See Connect NSX Manager to the Management vCenter Server in Region B and Register vSphere Replication with vCenter Single Sign-On in Region B.

Re-Enable Compute Platform Services Controller on the Load Balancer in Region B

After you replace the certificate on the Platform Services Controller instances in Region B, reenable load balancing the network traffic between them.

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

3 In the **Navigator**, click **NSX Edges**.

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

5 Restore the load balancer configuration.

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

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

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

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

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

Replace vCenter Server Certificates in Region B

Replace the certificate on each vCenter Server in Region B and reconnect it to the other management components to update the new certificate on these components.

Procedure

1 Replace the Certificate of vCenter Server in Region B

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

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

3 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.

4 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.

5 Update Management vCenter Server Certificate on Site Recovery Manager in Region B

After you replace the certificate of the Platform Services Controller pair or the Management vCenter Server, update the certificate on the connected Site Recovery Manager instance in Region B to reestablish the trusted connection.

6 Register vSphere Replication with vCenter Single Sign-On in Region B

Replace the Certificate of vCenter Server in Region B

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

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

vCenter Server FQDN	Files for Certificate Replacement
lax01m01vc01.lax01.rainpole.local	■ `lax01m01vc01.key` ■ `lax01m01vc01.1.cer` ■ `Root64.cer`
lax01w01vc01.lax01.rainpole.local	■ `lax01w01vc01.key` ■ `lax01w01vc01.1.cer` ■ `Root64.cer`

Procedure

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

a Open an SSH connection to the virtual machine lax01m01vc01.lax01.rainpole.local.

b Log in using the following credentials.

Setting	Value
User name	root
Password	*vcenter_server_root_password*

2 Change the vCenter Server appliance command shell to the Bash shell to allow secure copy (SCP) connections for the root user.

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

3 Copy the generated certificates from the Windows host where you run the `CertGenVVD` utility 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`, `Root64.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.

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

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

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

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

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

vCenter Server instance	IP Address of managing Platform Services Controller
lax01m01vc01.lax01.rainpole.local	172.17.11.61

   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
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/Root64.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/Root64.cer`

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

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

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

   b Verify that you see the new certificate.

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

```
service vami-lighttp restart
cd /root/certs
rm lax01m01vc01.1.cer lax01m01vc01.key Root64.cer
```

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

Connect NSX Manager to the Management vCenter Server in Region B

After you deploy the NSX Manager virtual appliance, connect the NSX Manager to the vCenter Server.

Procedure

1 Log in to the appliance interface of NSX Manager for the management cluster.

   a Open a Web browser and go to **`https://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
Lookup Service Host	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
vCenter Server	lax01m01vc01.lax01.rainpole.local
vCenter User Name	svc-nsxmanager@rainpole.local
Password	*svc-nsxmanager_password*

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

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

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/vco`**.

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:443
User name	svc-vra
Password	*svc-vra-password*

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

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

f From the **vCenter Server instance** drop-down menu, select **https://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.lax01.rainpole.local** entry, and click the **Edit** icon.

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

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

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

3 Recreate the vSphere endpoint in vRealize Automation.

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

   b Log in using the following credentials.

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

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

   d Have your point to **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 rows that contain `CN=lax01m01vc01.lax01.rainpole.local` and `CN=lax01w01vc01.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 Reconnect each vCenter Adapter.

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

   b 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**.

   c In the **Manage Solutions** dialog box, select **vCenter Adapter - lax01w01vc01**, click **Test Connection**, accept the new certificate of the Management vCenter Server, and click **Save Settings**.

8 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**.

Update Management vCenter Server Certificate on Site Recovery Manager in Region B

After you replace the certificate of the Platform Services Controller pair or the Management vCenter Server, update the certificate on the connected Site Recovery Manager instance in Region B to reestablish the trusted connection.

Reconnect the two site recovery sites after you re-trust the certificate of Platform Services Controller and vCenter Server.

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 lax01m01srm01.lax01.rainpole.local virtual machine.

   b Log in using the following credentials.

Settings	Value
User name	Windows administrator user
Password	*windows_administrator_password*

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

3 Select the entry for the **VMware vCenter Site Recovery Manager** and click **Change**.

   The VMware Site Recovery Manager installation wizard appears.

4 On the Welcome page, click **Next**.

5 On the **Program Maintenance** page, select **Modify** and click **Next**.

6 On the **vSphere Platform Services Controller** page, enter the password for authentication to Platform Services Controller, verify that the settings are correct, and click **Next**..

Setting	Value
Address	lax01psc51.lax01.rainpole.local
HTTPS Port	443
Username	**`svc-srm@rainpole.local`**
Password	***`svc-srm_password`***

7 When prompted to accept the certificate of the Platform Services Controller in the **Platform Services Controller Certificate** dialog box, click **Accept**.

8 On the **VMware vCenter Server** page, click **Next**.

9 When prompted, in the **vCenter Server Certificate** dialog box, click **Accept**.

10 On the **Site Recovery Manager Extension** page, leave the existing settings, and click **Next**.

Setting	Value
Administrator email	*srm_admin_lax_email_address*
Local Host	172.17.11.124
Listener Port	9086

11 On the **Certificate Type** page, select **Use existing certificate** and click **Next**.

12 On the **Database Server Selection** page, select **Use the embedded database server** and click **Next**.

13 On the **Embedded Database Configuration** page, leave the existing settings and click **Next**.

Setting	Value
Data Source Name	SRM_SITE_LAX
Database User Name	srm_db_admin
Database Password	*srm_db_admin_lax_password*
Database Port	5678
Connection Count	5
Max. Connections	20

14 On the **Site Recovery Manager Service Account** page, leave the existing credentials, and click **Next**.

Setting	Value
Use Local System account	Deselected
User Name	MGMT01SRM51\Administrator
Password	*mgmt01srm51_admin_password*

15 On the **Ready to Install the Program** page, click **Install**.

16 Click **Finish** to complete the installation.

17 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*

18 Reconnect the Site Recovery Manager instance in Region B.

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

b On the **Site Recovery** page, click **Sites**.

c On the **Sites** page, right-click **mgmt01vc51.lax01.rainpole.local** and select **Reconfigure Pairing**.

The **Reconfigure Site Recovery Manager Server Pairing** wizard appears.

d On the **Select Site** page, validate the following settings and click **Next**.

Settings	Value
PSC address	sfo01psc01.sfo01.rainpole.local
Port	443

e On the **Select vCenter Server** page, enter the administrator@vsphere.local password, validate the following settings, and click **Finish**.

Settings	Value
vCenter Servers with matching SRM Extension	mgmt01vc01.sfo01.rainpole.local
User Name	svc-srm@rainpole.local
Password	*svc-srm_password*

Register vSphere Replication with vCenter Single Sign-On in Region B

After you replace the default or expiring certificate on Platform Services Controller or vCenter Server, reconnect the vSphere Replication instance in the region to vCenter Single Sign-On.

Procedure

1 Log in to the Virtual Appliance Management Interface of the vSphere Replication appliance.

a Open a Web browser and go to **`https://lax01m01vrms01.lax01.rainpole.local:5480`**.

b Log in using the following credentials.

Settings	Value
User name	root
Password	*vr_sfo_root_password*

2 On the **VR** tab, click **Configuration**, enter the following settings, and click **Save and Restart Service**.

Setting	Value
Configuration Mode	Configure using the embedded database
LookupService Address	lax01psc01.lax01.rainpole.local
SSO Administrative Account	svc-vr@rainpole.local
Password	*svc-vr_password*
VRM Host	172.17.11.123
VRM Site Name	lax01m01vc01.lax01.rainpole.local
vCenter Server Address	lax01m01vc01.lax01.rainpole.local
vCenter Server Port	80
vCenter Server Admin Mail	*vcenter_server_admin_email*

3 In the **Confirm SSL Certificate** dialog box, click **Accept**.

4 Wait for the vSphere Replication Management (VRM) server to save the configuration.

5 Under **Service Status**, verify that the status of the VRM service is `running`.

6 Log out from the vSphere Replication appliance management interface.

7 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 Reconnect site**.

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

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 ESXi hosts in Region B and configure vCenter Server to accept customer certificate authorities, 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
	lax01m01esx03.lax01.rainpole.local

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

   a In the **Navigator**, under **Hosts and Cluster**, select **lax01m01esx01.lax01.rainpole.local**, and click the **Configure** tab.

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

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

3 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**.

4 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 ESXi hosts in Region B and configure vCenter Server to accept customer certificate authorities, 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 management 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 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 Disable lockdown mode on lax01m01esx01.lax01.rainpole.local.

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

   b Under the **lax01-m01dc** data center, select the **lax01m01esx01.lax01.rainpole.local** host object and click the **Configure** tab on the right.

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

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

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

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

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

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

3 Place the host in maintenance mode.

   a Under the**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**.

4 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
```

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 the 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://lax01m01esx01.lax01.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://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 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.

8 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 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.

9 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.

10 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
lax01w01esx03.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

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

Replace the Certificate of NSX Manager for the Management Cluster 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.

Table 2-7. Certificate-Related Files on the NSX Manager Instance for the Management Cluster in Region B

NSX Manager FQDN	Certificate filename
lax01m01nsx01.lax01.rainpole.local	lax01m01nsx01.4.p12

Procedure

1 Log in to the appliance interface of NSX Manager for the management cluster.

   a Open a Web browser and go to **`https://lax01m01nsx01.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** and click **Upload PKSCS#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 top right corner of the NSX Manager page, click the **Settings** icon.

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

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

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

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

Procedure

1 Log in to the appliance interface of NSX Manager for the management cluster.

   a Open a Web browser and go to **`https://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 NSX Manager
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
vCenter Server	lax01m01vc01.lax01.rainpole.local
vCenter User Name	svc-nsxmanager@rainpole.local
Password	*svc-nsxmanager_password*

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

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

Re-Join the Secondary NSX Manager to the Primary NSX Manager in Region A

After you replace the certificate on NSX Manager in Region B, update its certificate on the paired NSX Manager in Region A.

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

3 In the **Navigator**, click **Installation and Upgrade**.

4 From the **NSX Manager** drop-down menu, select **172.16.11.65** and verify there are no **SYNC ISSUES**.

5 If there is a **SYNC ISSUES**, select **172.16.11.65**.

6 Select **Actions > Update Secondary Manager**.

7 On **Update Secondary Manager** window, enter the following values and click **UPDATE**.

Setting	Values
Primary NSX Manager	172.16.11.65
NSX Manager	172.17.11.65
New IP address/Hostname	172.17.11.65

8 Verify that any **SYNC ISSUES** have been resolved.

Replace the NSX Manager Certificate for the Shared Edge and Compute Cluster in Region B

After you replace and re-trust the certificate of the NSX Manager for the management cluster, repeat the operation on NSX Manager for the shared edge and compute cluster lax01w01nsxc01.lax01.rainpole.local.

Procedure

1 Repeat Replace the Certificate of NSX Manager for the Management Cluster in Region B to replace the certificate on NSX Manager for the shared edge and compute cluster.

Table 2-8. Certificate-Related Files on the NSX Manager for the Shared Edge and Compute Cluster in Region A

NSX Manager FQDN	Certificate File Name
lax01w01nsxc01.lax01.rainpole.local	lax01w01nsx01.4.p12

2 Repeat Connect NSX Manager to vCenter Server After Certificate Replacement in Region B to update the NSX Manager certificate on the connected vCenter Server and Platform Services Controller.

Setting	Value for NSX Manager for the Shared Edge and Compute Cluster
vCenter Server	lax01w01vc01.lax01.rainpole.local
vCenter User Name	svc-nsxmanager@rainpole.local
Password	*svc-nsxmanager_password*

3 Repeat Re-Join the Secondary NSX Manager to the Primary NSX Manager in Region A to re-join the secondary NSX Manager in Region B to NSX Manager in Region A.

Roles	Primary	Secondary
Shared Edge and Compute NSX Manager Instances in Both Regions	172.16.11.66	172.17.11.66

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

Reconnect the NSX Manager Instances in Region B to vRealize Operations Manager

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

Procedure

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

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

b Log in using the following credentials.

Setting	Value
User name	admin
Password	*vrops_admin_password*

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

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

4 Delete the certificates with the following CNs.
   - `CN=lax01m01nsx01.lax01.rainpole.local`
   - `CN=lax01w01nsx01.lax01.rainpole.local`
5 In the left pane of vRealize Operations Manager, click **Solutions**.
6 From the solution table on the **Solutions** page, select the **Management Pack for NSX-vSphere** solution, and click the **Configure** icon at the top.
7 In the **Manage Solutions** dialog box, from the **Adapter Type** table at the top, select **NSX-vSphere Adapter**.
8 Click the **lax01m01nsx01-lax01** adapter instance, click **Test Connection**, accept the new certificate, and click **Save settings**.
9 Click the **lax01w01nsx01-lax01** adapter instance, click **Test Connection**, accept the new certificate, click **Save settings**, and click **Close**.

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

Update the certificate chain of vRealize Log Insight to use a trusted non-default certificate after deployment, to replace the self-signed certificate used during the deployment process, and 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 PEM file on your computer, and click **Save**.

Certificate Generation Option	Certificate File
Using the CertGenVVD tool	`vrli.lax01.2.chain.pem`

The certificate is uploaded to vRealize Log Insight.

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 Open a Secure Shell (SSH) connection to the master node of vRealize Log Insight.

a Open an SSH session to the following 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*

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

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

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

b Extract the root certificate from the destination vRealize Log Insight in Region B.

```
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
```

c 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
```

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

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

f Reboot the vRealize Log Insight node.

```
reboot
```

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

3 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*

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

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

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

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

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

Replace Certificates of the Business Continuity Components in Region B

In a dual-region environment, after you generate signed certificates for Site Recovery Manager and vSphere Replication, replace them and update them on the connected management components in Region B to maintain secure connection.

Replace the VMware Site Recovery Manager Certificates

After you replace the certificates of all Platform Services Controller, vCenter Server and NSX Manager instances, replace the certificates on the Site Recovery Manager instances.

You replace certificates twice, once for each Site Recovery Manager. You start by replacing certificates on sfo01m01srm01.sfo01.rainpole.local, the Site Recovery Manager in Region A.

Table 2-9. Certificate-Related Files for Site Recovery Manager in Region A and Region B

File Name	Site Recovery Manager in Region A	Site Recovery Manager in Region B
CA Certificate Name	Root64.cer	Root64.cer
PKCS#12 File Name	sfo01m01srm01.5.p12	lax01m01srm01.5.p12

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 A	sfo01m01srm01.sfo01.rainpole.local
Region B	lax01m01srm01.lax01.rainpole.local

   b Log in using the following credentials.

Setting	Value
User name	rainpole\svc-srm
Password	*svc-srm_user_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 File to the `C:\certs` folder

   b Double-click the `CA Certificate` 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 CA-signed Certificates.

   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 `VMware1!` 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 If you were previously using credential-based authentication, you might need to restore the connection between the two Site Recovery Manager sites after replacing the default certificates with CA-signed certificates.

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 vCenter Single Sign-On administrator user name **`svc-srm@rainpole.local`** and ***`svc-srm_password`*** password, and click **Finish**.

5 Repeat the steps to replace the default VMware-signed certificate on lax01m01srm01.lax01.rainpole.local.

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

Replace the certificates on vSphere Replication in Region B so that vSphere Replication can communicate with connected management solutions over a secure connection.

Table 2-10. PKCS#12 Files for vSphere Replication in Region B

vSphere Replication FQDN	PKCS#12 Filename 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 **`https://lax01m01vrms01.lax01.rainpole.local:5480`**.
   b. Log in using the following credentials.

Settings	Value
User name	root
Password	*vr_sfo_root_password*

   c. On the **VR** tab, click the **Configuration** tab.
   d. Click **Choose File** next to **Upload PKCS#12 (*.pfx)** file and locate the `lax01m01vrms01.5.p12` file on your local file system.
   e. Click the **Upload and Install** button.
   f. Enter the certificate password when prompted and click **OK**.
   g. If prompted, click **OK** in the certificate dialog box.

   After you apply the SSL certificate, the VAMI session of vSphere Replication will be disconnected.
2. Log in again by using the root credential.
3. On the **VR** tab, click the **Security** tab.
4. Verify that the **Current SSL Certificate** shows the updated certificate information.