# Certificate Replacement

VMware Validated Design 4.0
VMware Validated Design for Software-Defined Data Center 4.0

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.

The certificate replacement process consists of the following phases:

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

## Intended Audience

The *VMware Validated Design Certificate Replacement* documentation is intended for cloud architects, infrastructure administrators, cloud administrators and cloud operators who are familiar with and want to use VMware software to deploy in a short time and manage an SDDC that meets the requirements for capacity, scalability, backup and restore, and disaster recovery.

## Required Software

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

# Region A Certificate Replacement

1

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

- Create and Add a Microsoft Certificate Authority Template

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

- Use the Certificate Generation Utility to Generate Certificates Automatically in Region A

  You can use the VMware Validated Design Certificate Generation Utility (CertGenVVD) to generate signed certificates for all management components of this design in Region B. You can then import the certificates to these components to maintain secure connection to the external network and between the components themselves.

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

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

- Replace Certificates of the Management Products in Region A

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

## Create and Add a Microsoft Certificate Authority Template

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

- The first step is setting up a Microsoft Certificate Authority template through a Remote Desktop Protocol session.
- After you have created the new template, you add it to the certificate templates of the Microsoft CA.

### Prerequisites

This VMware Validated Design sets the CA up on both Active Directory (AD) servers: the main domain dc01rpl.rainpole.loca l(root CA) and the Region A subdomain dc01sfo.sfo01.rainpole.local (the intermediate CA). Both AD servers are running the Microsoft Windows Server 2012 R2 operating system.

- Verify that you installed Microsoft Server 2012 R2 VMs with Active Directory Domain Services enabled.
- Verify that The Certificate Authority Service role and the Certificate Authority Web Enrolment role is installed and configured on both Active Directory Server.
- Verify that dc01sfo.sfo01.rainpole.local has been set up to be the intermediate CA of the root CA dc01rpl.rainpole.local.

### Procedure

1. Log in to the AD server by using a Remote Desktop Protocol (RDP) client as the AD administrator with the *ad_admin_password* password.
   - If you use the intermediate CA, connect to dc01sfo.sfo01.rainpole.local.
   - If you use only the root CA, connect dc01rpl.sfo01.rainpole.local.
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. Click the **Signature is proof of origin (nonrepudiation)** check box.
   e. Leave the default for all other options.
   f. Click **OK**.
8. Click the **Subject Name** tab, ensure that the **Supply in the request** option is selected, and click **OK** to save the template.
9. To add the new template to your CA, click Windows **Start > Run**, enter `certsrv.msc`, and click **OK**.
10. In the **Certification Authority** window, expand the left pane if it is collapsed.
11. Right-click **Certificate Templates** and select **New** > **Certificate Template to Issue**.

12 In the **Enable Certificate Templates** dialog box, select the VMware certificate that you just created in the **Name** column and click **OK.**

## Use the Certificate Generation Utility to Generate Certificates Automatically in Region A

You can use the VMware Validated Design Certificate Generation Utility (CertGenVVD) to generate signed certificates for all management components of this design in Region B. You can then import the certificates to these components to maintain secure connection to the external network and between the components themselves.

### Procedure

1 Use the Certificate Generation Utility to Generate CA-Signed Certificates for the SDDC Management Components in Region A

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

2 Additional Configuration for Intermediate Certificate Authority in Region A

   If you use an intermediate certificate authority on sfo01.rainpole.local as certificate signer, CertGenVVD utility only retrieves the intermediate Base 64 certificate from the Microsoft CA. You must create a certificate chain file that also includes the root CA certificate.

## Use the Certificate Generation Utility to Generate CA-Signed Certificates for the SDDC Management Components in Region A

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

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

### Prerequisites

- If you use an intermediate CA such as sfo01.rainpole.local, make the Windows host that you use to connect to the data center a part of 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 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.

- comp01esx01.sfo01.txt
- comp01esx02.sfo01.txt
- comp01esx03.sfo01.txt
- comp01esx04.sfo01.txt
- comp01nsxm01.sfo01.txt
- comp01vc01.sfo01.txt
- mgmt01nsxm01.sfo01.txt
- sfo01psc01.sfo01.txt
- mgmt01esx01.sfo01.txt
- mgmt01esx02.sfo01.txt
- mgmt01esx03.sfo01.txt
- mgmt01esx04.sfo01.txt
- mgmt01srm01.sfo01.txt
- mgmt01vc01.sfo01.txt
- mgmt01vdp01.sfo01.txt
- mgmt01vrms01.sfo01.txt
- vra.txt
- vrb.txt
- vrli.sfo01.txt
- vro.txt
- vrops-forVVD4.0.txt

6 If `sfo01psc01.sfo01.txt` does not exist, create it so that you can generate certificates for the Platform Services Controllers that are behind a load balancer in Region A.

   a Make a copy of `mgmt01vc01.sfo01.txt` and save it as `sfo01psc01.sfo01.txt`.

   b Open the copied file in a text editor, and verify that the following properties are configured.

**sfo01psc01.sfo01.txt**

```
[CERT]
NAME=default
ORG=default
OU=default
LOC=SFO
ST=default
CC=default
CN=sfo01psc01.sfo01.rainpole.local
keysize=default
[SAN]
comp01psc01
mgmt01psc01
comp01psc01.sfo01.rainpole.local
mgmt01psc01.sfo01.rainpole.local
sfo01psc01
sfo01psc01.sfo01.rainpole.local
```

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

For example, of you use CertGenVVD 2.1, navigate to the following folder:

```
cd C:\CertGenVVD-2.1
```

8 Run the following command to grant PowerShell permissions to run third-party shell scripts.

```
Set-ExecutionPolicy Unrestricted
```

9 Run the following command to validate prerequisites for running the utility.

Verify that VMware is included in the available CA Template Policy.

```
.\CertgenVVD-2.1.ps1 -validate
```

10 Run the following command to generate MSCA-signed certificates.

```
.\CertGenVVD-2.1.ps1 -MSCASigned -attrib 'CertificateTemplate:VMware'
```

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

### What to do next

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

## Additional Configuration for Intermediate Certificate Authority in Region A

If you use an intermediate certificate authority on sfo01.rainpole.local as certificate signer, CertGenVVD utility only retrieves the intermediate Base 64 certificate from the Microsoft CA. You must create a certificate chain file that also includes the root CA certificate.

### Procedure

1 Log in to the site for certificate request on the sfo01.rainpole.local AD server.

   a Open a Web browser and go to **`https://dc01sfo.sfo01.rainpole.local/certsrv`**.

   b Log in using the following credentials.

   | Setting | Values |
   |---|---|
   | User name | *ad_administrator* |
   | password | *ad_administrator_password* |

2 Download and export the certificates of the intermediate and root CAs.

   a Click **Download a CA certificate, certificate chain, or CRL**.

   b Select **Current[sfo01-DC01SFO-CA** in the CA certificate list, select **Base 64** and click **Download CA certificate chain**.

   c Save the file as `chainroot.p7b`.

   d Open `chainroot.p7b`.

   The **certmgr** utility appears.

   e Navigate to Certificates folder

   f Right-click **sfo01-DC01SfO-CA** and select **All Tasks > Export**.

   The Certificate Export Wizard appears.

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

   h Select **Base-64 encoded X.509 (.CER)** and click **Next**

   i On the **File to Export** page, browse to the `C:\CertGenVVD-`*`version`*`\SignedByMSCACerts\sfo01-intermediate-ca.cer`, click **Next** and click **Finish**.

   j Click **Okay** when you see a message about successful export.

   k In the **certmgr** utility, right click **rainpole-DC01RPL-CA** and select **All Tasks > Export** and repeat the steps to save the rainpole.local root CA certificate as `C:\CertGenVVD-`*`version`*`\SignedByMSCACerts\rainpole-root-ca.cer`.

3 Create the `chainRoot64.cer` file that includes both root and intermediate CA certificates.

   a Open `rainpole-root-ca.cer` in a text editor.

   b Copy the entire content and close the file.

   c Open `sfo01-intermediate-ca.cer` in a text editor, press Enter to insert a new line at the end of the file, paste the `rainpole-root-ca.cer` content.

   d Save the file as `chainRoot64.cer` to the `C:\CertGenVVD-`*`version`*`\SignedByMSCACerts\`.

   e Close all files.

   f Verify that the new file `C:\CertGenVVD-`*`version`*`\SignedByMSCACerts\chainRoot64.cer` exists and contains the content of both `sfo01-intermediate-ca.cer` and `rainpole-root-ca.cer`.

4 Refresh all MSCA-signed certificates with new intermediate and root CAs.

   a Open the `C:\CertGenVVD-`*`version`* folder.

   b Make a copy of the `SignedByMSCACerts` folder and name is as `SignedByMSCACerts-backup`.

   c Rename the `SignedByMSCACerts` folder to `CSRCerts`.

   d Open the `C:\CSRCerts\RootCA\` folder.

   e Delete the `Root64.cer` file

   f Create a copy of `chainRoot64.cer` as `Root64.cer`.

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

   h Run the following command to regenerate all certificate files and packages using the new `Root64.cer`.

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

   i Rename the `CSRCerts` folder back to `SignedByMSCACerts`.

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

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

### Prerequisites

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

### Procedure

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

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

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

4 Verify that following properties are configured.

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

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

### Table 1-1. 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<br>■ sfo01m01psc01.sfo01.rainpole.local<br>■ sfo01w01psc01.sfo01.rainpole.local | sfo01psc01.txt |
| vCenter Server | sfo01m01vc01.sfo01.rainpole.local | sfo01m01vc01.txt |
| | sfo01w01vc01.sfo01.rainpole.local | sfo01w01vc01.txt |
| ESXi Hosts | sfo01m01esx01.sfo01.rainpole.local | sfo01m01esx01.txt |
| | sfo01m01esx02.sfo01.rainpole.local | sfo01m01esx02.txt |
| | sfo01m01esx03.sfo01.rainpole.local | sfo01m01esx03.txt |
| | sfo01m01esx04.sfo01.rainpole.local | sfo01m01esx04.txt |
| | sfo01w01esx01.sfo01.rainpole.local | sfo01w01esx01.txt |
| | sfo01w01esx02.sfo01.rainpole.local | sfo01w01esx02.txt |
| | sfo01w01esx03.sfo01.rainpole.local | sfo01w01esx03.txt |
| | sfo01w01esx04.sfo01.rainpole.local | sfo01w01esx04.txt |
| NSX Manager | sfo01m01nsx01.sfo01.rainpole.local | sfo01m01nsx01.txt |
| | sfo01w01nsx01.sfo01.rainpole.local | sfo01w01nsx01.txt |
| vSphere Data Protection | sfo01m01vdp01.sfo01.rainpole.local | sfo01m01vdp01.txt |
| Site Recovery Manager and vSphere Replication | sfo01m01srm01.sfo01.rainpole.local | sfo01m01srm01.txt |
| | sfo01m01vrms01.sfo01.rainpole.local | sfo01m01vrms01.txt |
| Cloud Management Platform Layer | | |

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

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

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

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

**sfo01psc01.txt**

```
[CERT]
NAME=default
ORG=default
OU=default
LOC=SFO
ST=default
CC=default
CN=sfo01psc01.sfo01.rainpole.local
keysize=default
[SAN]
sfo01psc01
sfo01m01psc01
sfo01w01psc01
sfo01psc01.sfo01.rainpole.local
sfo01m01psc01.sfo01.rainpole.local
sfo01w01psc01.sfo01.rainpole.local
```

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

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

8 Grant permissions to run third-party PowerShell scripts.

```
Set-ExecutionPolicy Unrestricted
```

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

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

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

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

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

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

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

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

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

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

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

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

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

#### What to do next

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

# Replace Certificates of the Management Products in Region A

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

### Prerequisites

Generate a certificate for the products in this validated design in one of the following ways:

- Use the VMware Validated Design Certificate Utility. See Use the Certificate Generation Utility to Generate Certificates Automatically in Region A.
- Generate Certificate Signing Requests manually and use them to have the product certificates signed by the certificate authority on the child AD server in Region A. See GUID-77202566-4B96-4C13-8693-3B1C956FDD19#GUID-77202566-4B96-4C13-8693-3B1C956FDD19 and GUID-BB614D41-1EF4-4701-A480-6327C93510D1#GUID-BB614D41-1EF4-4701-A480-6327C93510D1.

### Procedure

1 Replace Certificates of the Virtual Infrastructure Components in Region A

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

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

After you generate a signed certificate for a component of the Cloud Management Platform, replace it and update it on the management components in the region to maintain secure connection.

3 Replace Certificates of the Operations Management Components in Region A

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

# Replace Certificates of the Virtual Infrastructure Components in Region A

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

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

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

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

### Procedure

1. Replace the Platform Services Controller Certificates in Region A

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

2. Replace the vCenter Server Certificates in Region A

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

3. Replace the Default Certificate with a Custom Certificate on the ESXi Hosts in Region A

   Optionally, after you obtain signed certificate for the ESXi hosts in Region A, use it to replace the default VMware Certificate Authority (VMCA) signed certificates on the hosts.

4. Replace the NSX Manager Certificates in Region A

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

5. Replace the Certificate of vSphere Data Protection in Region A

   vSphere Data Protection comes with a default self-signed certificate. Install a CA-signed certificate that authenticates vSphere Data Protection over HTTPS.

## Replace the Platform Services Controller Certificates in Region A

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

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

You must repeat this procedure twice: first on the Platform Services Controller for the Management vCenter Server, and then on the Platform Services Controller for the Compute vCenter Server.

## Table 1-2. Certificate-Related Files on Platform Services Controllers

| Platform Services Controller | Certificate File Name | Replacement Order |
|---|---|---|
| mgmt01psc01.sfo01.rainpole.local | ▪ sfo01psc01.sfo01.key<br>▪ sfo01psc01.sfo01.3.pem (CertGenVVD)<br>▪ sfo01psc01.sfo01.chain.cer (Manual)<br>▪ chainRoot64.cer | First |
| comp01psc01.sfo01.rainpole.local | ▪ sfo01psc01.sfo01.key<br>▪ sfo01psc01.sfo01.3.pem (CertGenVVD)<br>▪ sfo01psc01.sfo01.1.chain.cer (Manual)<br>▪ chainRoot64.cer | Second |

### Procedure

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

   a Open a Web browser and go to `https://mgmt01vc01.sfo01.rainpole.local/vsphere-client`.

   b Log in using the following credentials.

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

2 Disable the Platform Services Controller for the shared edge and compute cluster comp01psc01 in the load balancer to route all traffic to the Platform Services Controller for the management cluster mgmt01psc01.

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

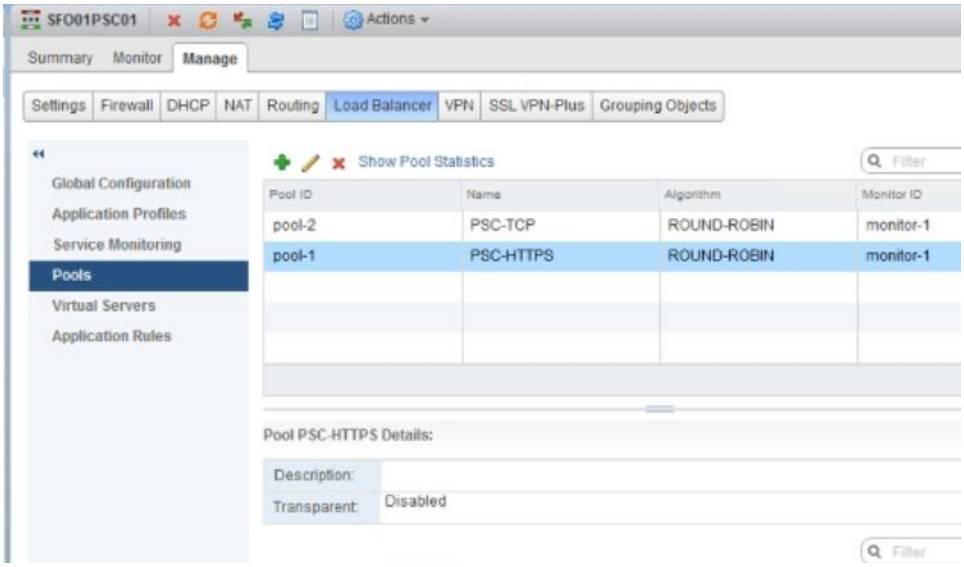
   b In the **Navigator**, select **NSX Edges**.

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

   d Double-click the **SFO01PSC01** edge device to open its network settings.

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

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



| Pool ID | Name | Algorithm | Monitor ID |
|---|---|---|---|
| pool-2 | PSC-TCP | ROUND-ROBIN | monitor-1 |
| pool-1 | PSC-HTTPS | ROUND-ROBIN | monitor-1 |

Pool PSC-HTTPS Details:

| | |
|---|---|
| Description: | |
| Transparent: | Disabled |

g Select the **comp01psc01** member, click **Edit**, select **Disable** from the **State** drop-down menu and click **OK**.

h Repeat Step 2f and Step 2g to disable comp01psc01 in **pool-2**.

**3** Disconnect the NSX Manager instances from the Platform Services Controller temporarily.

a Open a Web Browser and go to **`https://mgmt01nsxm01.sfo01.rainpole.local`**.

b Log in using the following credentials

| Setting | Value |
|---|---|
| User name | admin |
| Password | *nsx_manager_admin_password* |

c Click **Manage vCenter Registration**

d Click the **Unconfigure** button next to **Lookup Service URL**.

e Repeat the steps on **`https://comp01nsxm01.sfo01.rainpole.local`**.

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

a Open an SSH connection to mgmt01psc01.sfo01.rainpole.local.

b Log in using the following credentials.

| Setting | Value |
|---|---|
| **User name** | root |
| **Password** | *mgmtpsc_root_password* |

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

   ```
   shell
   chsh -s /bin/bash root
   ```

6. Copy the generated certificate files `sfo01psc01.sfo01.key`, `sfo01psc01.sfo01.3.pem` and `chainRoot64.cer` from the Windows host to the `/tmp/ssl` directory on the Platform Services Controller.

   Use `scp`, FileZilla or WinSCP to copy the files.

7. Rename `sfo01psc01.sfo01.3.pem` to `sfo01psc01.sfo01.1.chain.cer`.

8. Add the root certificate to the VMware Endpoint Certificate Store as a trusted root certificate using the following command.

   Enter the vCenter Single Sign-On password when prompted.

   ```
   /usr/lib/vmware-vmafd/bin/dir-cli trustedcert publish --chain --cert /tmp/ssl/chainRoot64.cer
   ```

9. 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`*** 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 **`/tmp/ssl/sfo01psc01.sfo01.1.chain.cer`**.

   f. When prompted for the custom key, enter **`/tmp/ssl/sfo01psc01.sfo01.key`**.

   g. When prompted for the signing certificate, enter **`/tmp/ssl/ChainRoot64.cer`**.

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

      Wait until the Platform Services Controller services restart successfully.

10. Validate that the new certificate has been installed successfully.

    a. Open a Web Browser and go to **`https://mgmt01psc01.sfo01.rainpole.local`**.

    b. Verify that the Web browser shows the new certificate.

11 Restart VAMI service to update certificates for the appliance management interface.

   a Go back to the mgmt01psco1.sfo01.rainpole.local SSH terminal.

   b Enter the following command to update certificates for the appliance management interface.

```
/etc/init.d/vami-lighttp restart
```

12 Switch the shell back to the appliance shell.

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

13 Repeat Step 4 to Step 11 to replace the certificate on comp01psc01.sfo01.rainpole.local.

14 Restart the services on the Management vCenter Server.

   a Open an SSH connection to mgmt01vc01.sfo01.rainpole.local.

   b Log in using the following credentials.

| Setting | Values |
|---|---|
| User name | root |
| Password | *mgmtvc_root_password* |

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

```
shell
```

   d Restart vCenter Server services by using the following command.

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

15 Restore the load balancer configuration.

   a Open a Web browser and go to **`https://mgm01vc01.sfo01.rainpole.local/vsphere-client`**.

   b Log in using the following credentials.

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

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

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

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

   f Double-click the **SFO01PSC01** edge device to open its network settings.

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

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

i Select the **comp01psc01** member, click **Edit**, select **Enabled** from the **State** drop-down menu and click **OK**.

j Repeat Step 15h and Step 15i to enable comp01psc01 in **pool-2**.

**16** Repeat Step 14 to restart the services on the Compute vCenter Server comp01vc01.sfo01.rainpole.local in Region A and on the vCenter Server instances mgmt01vc51.lax01.rainpole.local and comp01vc51.lax01.rainpole.local in Region B.

### What to do next

If you replace only the certificate of the Platform Services Controller instances, reconnect the NSX Managers to the Platform Services Controller load balancer and to vCenter Server after you install the custom certificates on the nodes. See Connect NSX Manager to the Management vCenter Server in Region A.

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

## Replace the vCenter Server Certificates in Region A

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

### Procedure

1 Replace the vCenter Server Certificate Files in Region A

After you replace the Platform Services Controller certificate, you replace the vCenter Server machine SSL certificate. You generate a vCenter Server certificate manually or by using the CertGenVVD tool.

2 Connect NSX Manager to the Management 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 Managers to the vCenter Server nodes in the region.

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

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

4 Update the vCenter Server Certificates on the Cloud Management Platform in Region A

After you replace the certificates on the vCenter Server instances in Region A, reconnect vRealize Orchestrator to vCenter Server.

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

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

## Replace the vCenter Server Certificate Files in Region A

After you replace the Platform Services Controller certificate, you replace the vCenter Server machine SSL certificate.  You generate a vCenter Server certificate manually or by using the CertGenVVD tool.

You replace certificates twice, once for each vCenter Server instance.  You can start replacing certificates on Management vCenter Server mgmt01vc01.sfo01.rainpole.local first.

Table 1-3.  Certificate-Related Files on the vCenter Server Instances

| vCenter Server FQDN | Files for Certificate Replacement | Replacement Order |
|---|---|---|
| mgmt01vc01.sfo01.rainpole.local | ■ mgmt01vc01.sfo01.key<br>■ mgmt01vc01.sfo01.3.pem (CertGenVVD2.1)<br>■ mgmt01vc01.sfo01.1.chain.cer (Manually)<br>■ chainRoot64.cer | After you replace the certificate on the management Platform Services Controller. |
| comp01vc01.sfo01.rainpole.local | ■ comp01vc01.sfo01.key<br>■ comp01vc01.sfo01.3.pem (CertGenVVD2.1)<br>■ comp01vc01.sfo01.1.chain.cer (Manually)<br>■ chainRoot64.cer | After you replace the certificate on the compute Platform Services Controller. |

### Procedure

1. Use the `scp` command, FileZilla, or WinSCP to copy the machine and CA certificate files to the `/tmp/ssl` directory on the Management vCenter Server.

2. Log in to the vCenter Server instance by using Secure Shell (SSH) client.

   a. Open an SSH connection to the vCenter Server Appliance mgmt01vc01.sfo01.rainpole.local.

   b. Log in using the following credentials.

   | Setting | Value |
   |---|---|
   | User name | root |
   | Password | *vcenter_server_root_password* |

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

   a. Add the root certificate to the VMware Endpoint Certificate Store as a Trusted Root Certificate using the following command and enter the vCenter Single Sign-On password when prompted.

   ```
   /usr/lib/vmware-vmafd/bin/dir-cli trustedcert publish --chain --cert /tmp/ssl/chainRoot64.cer
   ```

   b. Rename `mgmt01vc01.sfo01.3.pem` to `mgmt01vc01.sfo01.1.chain.cer`.

   ```
   mv /tmp/ssl/mgmt01vc01.sfo01.3.pem /tmp/ssl/mgmt01vc01.sfo01.1.chain.cer
   ```

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

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

d 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.

e When prompted for the **Infrastructure Server IP**, enter the IP address of the Platform Services Controller that is connected to this vCenter Server instance.

| Option | IP Address of Connected Platform Services Controller |
|---|---|
| **mgmt01vc01.sfo01.rainpole.local** | 172.16.11.61 |
| **comp01vc01.sfo01.rainpole.local** | 172.16.11.63 |

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

g 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 |
|---|---|
| **mgmt01vc01.sfo01.rainpole.local** | Please provide valid custom certificate for Machine SSL.<br>File : **`/tmp/ssl/mgmt01vc01.sfo01.1.chain.cer`**<br>Please provide valid custom key for Machine SSL.<br>File : **`/tmp/ssl/mgmt01vc01.sfo01.key`**<br>Please provide the signing certificate of the Machine SSL certificate.<br>File : **`/tmp/ssl/chainRoot64.cer`** |
| **comp01vc01.sfo01.rainpole.local** | Please provide valid custom certificate for Machine SSL.<br>File : **`/tmp/ssl/comp01vc01.sfo01.1.chain.cer`**<br>Please provide valid custom key for Machine SSL.<br>File : **`/tmp/ssl/comp01vc01.sfo01.key`**<br>Please provide the signing certificate of the Machine SSL certificate.<br>File : **`/tmp/ssl/chainRoot64.cer`** |

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

**5** Log into the vSphere Web client to verify that certificate replacement is successful.

a Open a Web browser and go to **`https://mgmt01vc01.sfo01.rainpole.local/vsphere-client`**.

b Log in using the following credential

| Settings | Values |
|---|---|
| User name | administrator@vsphere.local |
| Password | *vsphere_admin_password* |

6 After you replace the certificate on the mgmt01vc01.sfo01.rainpole.local vCenter Server, repeat the procedure to replace the certificate on the compute vCenter Server comp01vc01.sfo01.rainpole.local.

### Connect NSX Manager to the Management 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 Managers to the vCenter Server nodes in the region.

#### Procedure

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

   a Open a Web browser and go to `https://mgmt01nsxm01.sfo01.rainpole.local`.

   b Log in using the following credentials.

| Setting | Value |
|---|---|
| User name | admin |
| Password | *nsx_manager_admin_password* |

2 Click **Manage vCenter Registration**.

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

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

| Setting | Value for Both NSX Managers |
|---|---|
| Lookup Service IP | sfo01psc01.sfo01.rainpole.local |
| Lookup Service Port | 443 |
| SSO Administrator User Name | administrator@vsphere.local |
| Password | *vsphere_admin_password* |

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

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

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

| Setting | Value for NSX Manager for the Management Cluster | Value for NSX Manager for the Shared Edge and Compute Cluster |
|---|---|---|
| vCenter Server | mgmt01vc01.sfo01.rainpole.local | comp01vc01.sfo01.rainpole.local |
| vCenter User Name | svc-nsxmanager@rainpole.local | svc-nsxmanager@rainpole.local |
| Password | *svc-nsxmanager_password* | *svc-nsxmanager_password* |

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

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

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

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

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

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

#### Procedure

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

   a Open a Web browser and go to **`https://mgmt01vc01.sfo01.rainpole.local/vsphere-client`**.

   b Log in using the following credentials.

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

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

3 On the **Welcome to vSphere Data Protection** page, select **mgmt01vdp01** from the **VDP Appliance** drop-down menu and click **Connect**.

### Update the vCenter Server Certificates on the Cloud Management Platform in Region A

After you replace the certificates on the vCenter Server instances in Region A, reconnect vRealize Orchestrator to vCenter Server.

#### Procedure

1 Reconnect vRealize Orchestrator to vCenter Server.

   a Open a Web Browser and go to **`https://vra01vro01a.rainpole.local:8281`**.

   b Click **Start Orchestrator Client**.

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

| Setting | Value |
|---|---|
| Host name | vra01vro01a.rainpole.local:8281 |
| User name | svc-vra |
| Password | *svc-vra-password* |

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

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

   f From the **vCenter Server instance** drop-down menu, select **https://comp01vc01.sfo01.rainpole.local:443/sdk** and click **Next**.

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

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

**2** Reconnect vRealize Business with the Compute vCenter Server.

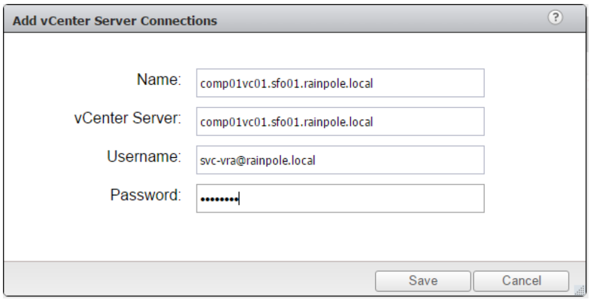
a Open a Web browser and go to **`https://vra01buc01.sfo01.rainpole.local:9443/dc-ui`**.

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 comp01vc01.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**.



Add vCenter Server Connections

Name: comp01vc01.sfo01.rainpole.local

vCenter Server: comp01vc01.sfo01.rainpole.local

Username: svc-vra@rainpole.local

Password: ••••••••

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

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

**3** Recreate the vSphere endpoint in vRealize Automation.

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

b Log in using the following credentials.

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

c Navigate to **Infrastructure > Endpoints > Credentials**, select **comp01vc01sfo01 admin** and click **Edit**.

d On the **Credentials** page, enter the password for the vRealize Automation credential for the administrator of comp01vc01.sfo01.rainpole.local, and click **Save**.

| Setting | Value |
|---|---|
| Name | comp01vc01sfo01 admin |
| Description | Administrator of comp01vc01.sfo01.rainpole.local |
| User Name | svc-vra@rainpole.local |
| Password | ***svc_vra_password*** |

e Navigate to **Infrastructure > Endpoints > Endpoints**.

f Have your mouse over **comp01vc01.sfo01.rainpole.local** and click **Edit** from the menu.

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

h A certificate warning should popup, 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 the vCenter Server instances in Region A, update the certificate on the connected vRealize Operations Manager node by reconnecting the vCenter Adapter instances.

### Procedure

1 Log in to vRealize Operations Manager by using the administration console.

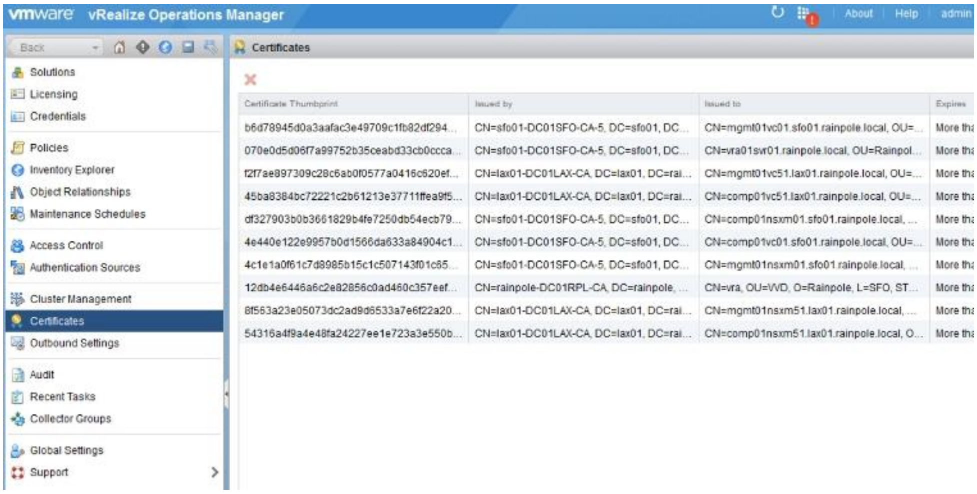
a Open a Web browser and go to **`https://vrops-cluster-01.rainpole.local`**.

b Log in using the following credentials.

| Setting | Value |
|---|---|
| **User name** | admin |
| **Password** | *vrops_admin_password* |

2 In the left pane of vRealize Operations Manager, click **Administration** and click **Certificates**.

3 Select the row that contains `CN=mgmt01vc01.sfo01.rainpole.local` and click the **Delete** icon.



| Certificate Thumbprint | Issued by | Issued to | Expires |
|---|---|---|---|
| b6d78945d0a3aafac3e49709c1fb82df294... | CN=sfo01-DC01SFO-CA-5, DC=sfo01, DC... | CN=mgmt01vc01.sfo01.rainpole.local, OU=... | More tha |
| 070e0d5d06f7a99752b35ceabd33cb0ccca... | CN=sfo01-DC01SFO-CA-5, DC=sfo01, DC... | CN=vra01svr01.rainpole.local, OU=Rainpol... | More tha |
| f2f7ae897309c28c6ab0f0577a0416c620ef... | CN=lax01-DC01LAX-CA, DC=lax01, DC=rai... | CN=mgmt01vc51.lax01.rainpole.local, OU=... | More tha |
| 45ba8384bc72221c2b61213e37711ffea9f5... | CN=lax01-DC01LAX-CA, DC=lax01, DC=rai... | CN=comp01vc51.lax01.rainpole.local, OU=... | More tha |
| df327903b0b3661829b4fe7250db54ecb79... | CN=sfo01-DC01SFO-CA-5, DC=sfo01, DC... | CN=comp01nsxm01.sfo01.rainpole.local, ... | More tha |
| 4e440e122e9957b0d1566da633a84904c1... | CN=sfo01-DC01SFO-CA-5, DC=sfo01, DC... | CN=comp01vc01.sfo01.rainpole.local, OU=... | More tha |
| 4c1e1a0f61c7d8985b15c1c507143f01c65... | CN=sfo01-DC01SFO-CA-5, DC=sfo01, DC... | CN=mgmt01nsxm01.sfo01.rainpole.local, ... | More tha |
| 12db4e6446a6c2e82856c0ad460c357eef... | CN=rainpole-DC01RPL-CA, DC=rainpole, ... | CN=vra, OU=WD, O=Rainpole, L=SFO, ST... | More tha |
| 8f563a23e05073dc2ad9d6533a7e6f22a20... | CN=lax01-DC01LAX-CA, DC=lax01, DC=rai... | CN=mgmt01nsxm51.lax01.rainpole.local, ... | More tha |
| 54316a4f9a4e48fa24227ee1e723a3e550b... | CN=lax01-DC01LAX-CA, DC=lax01, DC=rai... | CN=comp01nsxm51.lax01.rainpole.local, O... | More tha |

4 In the left pane of vRealize Operations Manager, click **Administration** and click **Solutions**.

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

6 In the **Manage Solutions** dialog box, select **mgmt01vc01-sfo01**, click **Test Connection**, accept the new certificate of the Management vCenter Server and click **Save Settings**.

7 Repeat the procedure to delete the certificate that is installed for the Compute vCenter Server comp01vc01.sfo01.rainpole.local and reconnect vRealize Operations Manager to the Compute vCenter Server to install the new certificate.

## Replace the Default Certificate with a Custom Certificate on the ESXi Hosts in Region A

Optionally, after you obtain signed certificate for the ESXi hosts in Region A, use it to replace the default VMware Certificate Authority (VMCA) signed certificates on the hosts.

### Procedure

1 Change the certificate mode for the ESXi hosts in the management cluster.

By default the ESXi hosts are automatically provisioned with VMCA certificates when they are connected to VC. We will change the certificate mode so VC will not push VMCA certificates on to ESXi hosts when they are added to VC.

a Open a Web browser and go to `https://mgmt01vc01.sfo01.rainpole.local`.

b Log in using the following credentials.

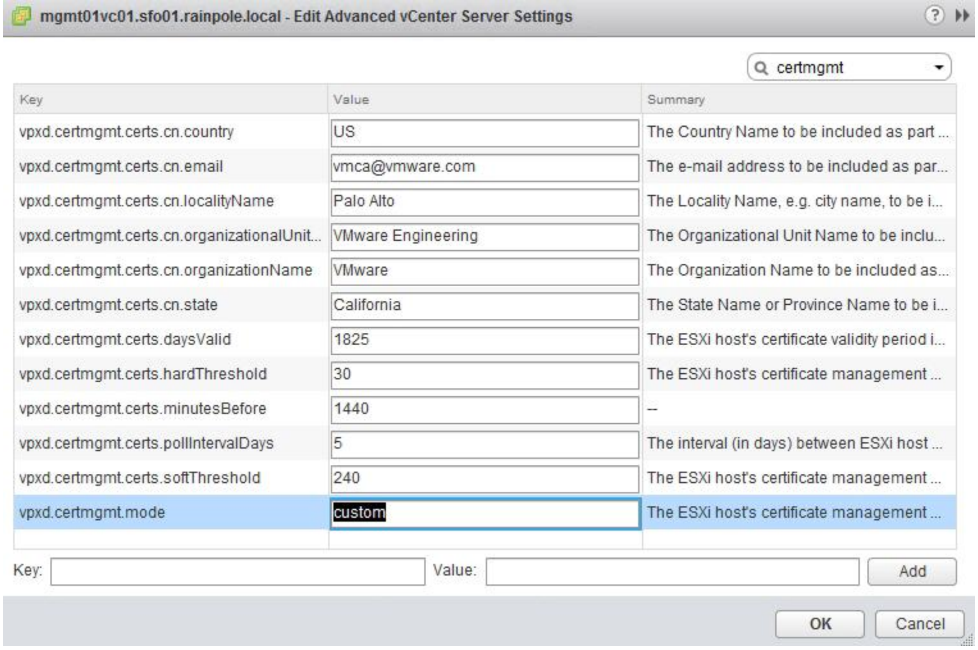
| Setting | Value |
|---|---|
| User name | administrator@vsphere.local |
| Password | *vshpere_admin_password* |

c In the **Navigator**, under **Hosts and Cluster**, select **mgmt01vc01.sfo01.rainpole.local**, and click the **Configure** tab.

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

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

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



mgmt01vc01.sfo01.rainpole.local - Edit Advanced vCenter Server Settings

certmgmt

| Key | Value | Summary |
|---|---|---|
| vpxd.certmgmt.certs.cn.country | US | The Country Name to be included as part ... |
| vpxd.certmgmt.certs.cn.email | vmca@vmware.com | The e-mail address to be included as par... |
| vpxd.certmgmt.certs.cn.localityName | Palo Alto | The Locality Name, e.g. city name, to be i... |
| vpxd.certmgmt.certs.cn.organizationalUnit... | VMware Engineering | The Organizational Unit Name to be inclu... |
| vpxd.certmgmt.certs.cn.organizationName | VMware | The Organization Name to be included as... |
| vpxd.certmgmt.certs.cn.state | California | The State Name or Province Name to be i... |
| vpxd.certmgmt.certs.daysValid | 1825 | The ESXi host's certificate validity period i... |
| vpxd.certmgmt.certs.hardThreshold | 30 | The ESXi host's certificate management ... |
| vpxd.certmgmt.certs.minutesBefore | 1440 | -- |
| vpxd.certmgmt.certs.pollIntervalDays | 5 | The interval (in days) between ESXi host ... |
| vpxd.certmgmt.certs.softThreshold | 240 | The ESXi host's certificate management ... |
| vpxd.certmgmt.mode | custom | The ESXi host's certificate management ... |

g From the vSphere Web Client **Home** menu, select **Administration**, and under **Deployment** on the **Administration** page, select **System Configuration**.

h Under **System Configuration**, select **Services**, select **VMware vCenter Server (mgmt01vc01.sfo01.rainpole.local )** and select **Actions > Restart**.

**2** If you have not replaced the certificate of the mgmt01vc01.sfo01.rainpole.local vCenter Server, add the CA root certificate to the vCenter Server `TRUSTED_ROOTS` store.

If you already replaced the certificate for mgmt01vc01.sfo01.rainpole.local, you added the root certificate to the `TRUSTED_ROOTS` stores.

a Open an SSH connection to mgmt01vc01.sfo01.rainpole.local.

b Log in using the following credentials.

| Setting | Value |
|---|---|
| User name | root |
| Password | *mgmtvc_root_password* |

c Copy the `Root64.cer` chain file from the Windows host that you use to access the data center to the temporary directory `/tmp/ssl` on the vCenter Server Appliance.

You can use `scp`, FileZilla or WinSCP.

d Run the following command.

```
/usr/lib/vmware-vmafd/bin/vecs-cli entry create --store TRUSTED_ROOTS --alias RainpoleCA.crt --
cert /tmp/ssl/chainRoot64.cer
```

**3** Replace the certificates on ESXi hosts.

a Open a Web browser and go to **`https://mgmt01vc01.sfo01.rainpole.local`**.

b Log in using the following credentials.

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

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

d Under the SFO01-Mgmt01 data center, right-click the **mgmt01esx01.sfo01.rainpole.local** vCenter Server object and select **Maintenance Mode > Enter Maintenance Mode**.

e Select **Move powered-off and suspended virtual machines to other hosts in the cluster** and click **OK**.

f After the maintenance task is complete, open an SSH connection to the mgmt01esx01.sfo01.rainpole.local host.

g Transfer `mgmt01esx01.key` and `mgmt01esx01.1.cer` from the Windows host that you use to access the data center to the `/etc/vmware/ssl` directory on the host.

h Run the following commands.

```
mv rui.crt orig.rui.crt
mv rui.key orig.rui.key
mv mgmt01esx01.key rui.key
mv mgmt01esx01.1.cer rui.crt
```

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

j Press the F2 key to access the **System Customization** menu.

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

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

m Press F11 key to confirm the restart.

4 Verify that the custom certificate is installed.

   a Open a Web browser and go to **`https://mgmt01esx01.sfo01.rainpole.local`**.

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

5 Exit the maintenance mode of the host.

   a Open a Web browser and go to **`https://mgmt01vc01.sfo01.rainpole.local`**.

   b Log in using the following credentials.

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

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

   d Under the SFO01-Mgmt01 data center, right-click the **mgmt01esx01.sfo01.rainpole.local** vCenter Server object and select . **Maintenance Mode > Exit Maintenance Mode**

   e Make sure that no warning message about an untrusted mgmt01esx01.sfo01.rainpole.local certificate appears.

6 Repeat Step 3 to Step 5 for the rest of the ESXi hosts.

| ESX hosts | Managed by | Certificate file names |
|---|---|---|
| mgmt01esx02.sfo01.rainpole.local | mgmt01vc01.sfo01.rainpole.local | ■ mgmt01esx02.key<br>■ mgmt01esx02.1.cer |
| mgmt01esx03.sfo01.rainpole.local | mgmt01vc01.sfo01.rainpole.local | ■ mgmt01esx03.key<br>■ mgmt01esx03.1.cer |
| mgmt01esx04.sfo01.rainpole.local | mgmt01vc01.sfo01.rainpole.local | ■ mgmt01esx04.key<br>■ mgmt01esx04.1.cer |
| comp01esx01.sfo01.rainpole.local | comp01vc01.sfo01.rainpole.local | ■ comp01esx01.key<br>■ comp01esx01.1.cer |
| comp01esx02.sfo01.rainpole.local | comp01vc01.sfo01.rainpole.local | ■ comp01esx02.key<br>■ comp01esx02.1.cer |
| comp01esx03.sfo01.rainpole.local | comp01vc01.sfo01.rainpole.local | ■ comp01esx03.key<br>■ comp01esx03.1.cer |
| comp01esx04.sfo01.rainpole.local | comp01vc01.sfo01.rainpole.local | ■ comp01esx04.key<br>■ comp01esx04.1.cer |

## Replace the NSX Manager Certificates in Region A

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

You replace certificates twice, once for each NSX Manager. You first start replacing certificates on the NSX Manager for the mgmt01nsxm01.sfo01.rainpole.local management cluster.

### Table 1-4. Certificate-Related Files on the NSX Manager Instances in Region A

| NSX Manager FQDN | Certificate File Name | Replacement Time |
|---|---|---|
| mgmt01nsxm01.sfo01.rainpole.local | ■ mgmt01nsxm01.sfo01.chain.cer from manual generation<br>■ mgmt01nsxm01.sfo01.4.p12 from the automation generation | After you replace the certificate on the Management vCenter Server |
| comp01nsxm01.sfo01.rainpole.local | ■ comp01nsxm01.sfo01.chain.cer from manual generation<br>■ comp01nsxm01.sfo01.4.p12 from the automation generation | After you replace the certificate on the Compute vCenter Server |

### Procedure

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

   a Open a Web browser and go to following URL.

   | NSX Manager | URL |
   |---|---|
   | NSX Manager for the management cluster | https://mgmt01nsxm01.sfo01.rainpole.local |
   | NSX Manager for the shared compute and edge cluster | https://comp01nsxm01.sfo01.rainpole.local |

   b Log in using the following credentials.

   | Setting | Value |
   |---|---|
   | **User name** | admin |
   | **Password** | *nsx_manager_admin_password* |

2 On the **Manage** tab, click **SSL Certificates**, click **Import** and provide the certificate chain file.

3 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**.

4 Re-register the NSX Manager to the Management vCenter Server.

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

| Setting | Value |
|---|---|
| **NSX Manager for the management cluster** | https://mgmt01nsxm01.sfo01.rainpole.local |
| **NSX Manager for the shared compute and edge cluster** | https://comp01nsxm01.sfo01.rainpole.local |

b Log in using the following credentials.

| Setting | Value |
|---|---|
| **User name** | admin |
| **Password** | *nsx_mngr_admin_password* |

c Click **Manage vCenter Registration**.

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

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

| Setting | Value |
|---|---|
| **Lookup Service IP** | sfo01psc01.sfo01.rainpole.local |
| **Lookup Service Port** | 443 |
| **SSO Administrator User Name** | administrator@vsphere.local |
| **Password** | *vsphere_admin_password* |

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

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

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

| Setting | Value for the NSX Manager for the Management Cluster | Value for the NSX Manager for the Shared Edge and Compute Cluster |
|---|---|---|
| vCenter Server | mgmt01vc01.sfo01.rainpole.local | comp01vc01.sfo01.rainpole.local |
| vCenter User Name | svc-nsxmanager@rainpole.local | |
| Password | *svc-nsxmanager_password* | |

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

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

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

6 Reconnect to the secondary NSX Manager instances in Region B.

   a Open a Web browser and go to **`https://mgmt01vc01.sfo01.rainpole.local`**.

   b Log in using the following credentials.

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

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

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

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

   f If primary and secondary nodes are not syncing correctly

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

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

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

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

| Setting | Value |
|---|---|
| NSX Manager | 172.17.11.65 |
| User name | admin |
| Password | *mgmtnsx_admin_password* |
| Confirm Password | *mgmtnsx_admin_password* |

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

   l Repeat Step 6e to Step 6k for the NSX Manager instances for the shared edge and compute cluster.

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

7 Reconnect the NSX Manager instances to vRealize Operations Manager.

   a Open a Web browser and go to **`https://vrops-cluster-01.rainpole.local`**.

   b Log in using the following credentials.

| Setting | Value |
|---|---|
| User name | admin |
| Password | *vrops_admin_password* |

   c In the left pane of vRealize Operations Manager, click **Administration** and click **Certificates**.

d Select the row that contains `CN=mgmt01nsxm01.sfo01.rainpole.local` and click the **Delete** icon.

e Select the row that contains `CN=comp01nsxm01.sfo01.rainpole.local` and click the **Delete** icon.

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

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

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

i Click the **mgmt01nsxm01-sfo01** adapter instance, click **Test Connection**, accept the new certificate and click **Save settings**.

j Click the **comp01nsxm01-sfo01** adapter instance, click **Test Connection**, accept the new certificate and click **Save settings**.

## Replace the Certificate of vSphere Data Protection in Region A

vSphere Data Protection comes with a default self-signed certificate. Install a CA-signed certificate that authenticates vSphere Data Protection over HTTPS.

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

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

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

  Replace the certificate on vSphere Data Protection in Region A with the certificate that is signed by the Microsoft CA on the dc01sfo.sfo01.rainpole.local AD server.

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

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

#### Prerequisites

Generate the Microsoft CA-signed certificate by using the `CertGenVVD` tool. See Use the Certificate Generation Utility to Generate Certificates Automatically in Region A.

#### Procedure

1 Copy the `.keystore` file that `CertGenVVD` tool generated to the `/root` folder on the vSphere Data Protection virtual appliance.

You can use `scp`, FileZilla or WinSCP.

2 Log in to the vSphere Data Protection appliance.

a Open an SSH connection to the virtual machine mgmt01vdp01.sfo01.rainpole.local.

b Log in using the following credentials.

| Setting | Value |
|---|---|
| User name | root |
| Password | *vdp_root_password* |

3 Restart all  vSphere Data Protection services by running the following commands.

```
dpnctl stop all
dpnctl start all
```

4 Run the `addFingerprint.sh` script to update the vSphere Data Protection server thumbprint displayed in the VM console welcome screen.

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

### Install a Manually Generated Certificate on vSphere Data Protection in Region A

Replace the certificate on vSphere Data Protection in Region A with the certificate that is signed by the Microsoft CA on the dc01sfo.sfo01.rainpole.local AD server.

#### Procedure

1 On the Windows host that has access to the data center, copy the `vdp.p7b` certificate file to the `/root` folder on the vSphere Data Protection virtual appliance.

You can use `scp`, FileZilla or WinSCP.

2 Log in to the vSphere Data Protection appliance.

a Open an SSH connection to the virtual machine mgmt01vdp01.sfo01.rainpole.local.

b Log in using the following credentials.

| Setting | Value |
|---|---|
| User name | root |
| Password | *vdp_root_password* |

3 Verify that the vSphere Data Protection services are stopped.

```
emwebapp.sh --test
```

If the services are running, stop them by running the following command.

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

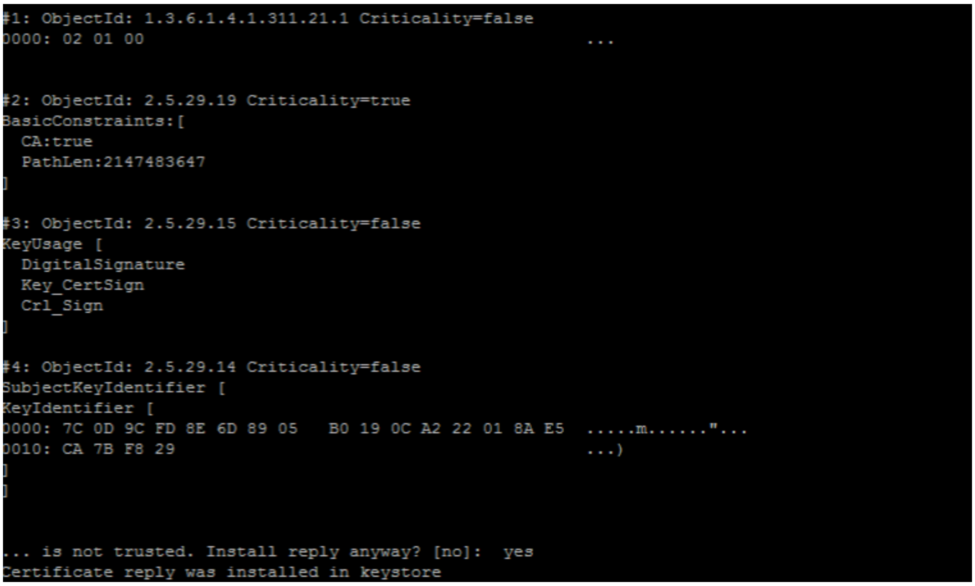
4 Import the certificate in the vSphere Data Protection keystore.

   a Run the following console command.

   ```
   /usr/java/latest/bin/keytool –import –alias tomcat –keystore /root/.keystore –
   file /root/vdp.p7b
   ```

   b When prompted for the keystore password, enter **`changeit`**.

   c When prompted to trust the certificate, type **`yes`** and press Enter.



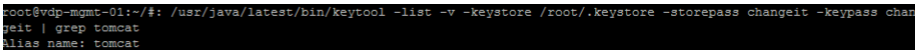
```
#1: ObjectId: 1.3.6.1.4.1.311.21.1 Criticality=false
0000: 02 01 00                                            ...


#2: ObjectId: 2.5.29.19 Criticality=true
BasicConstraints:[
  CA:true
  PathLen:2147483647
]

#3: ObjectId: 2.5.29.15 Criticality=false
KeyUsage [
  DigitalSignature
  Key_CertSign
  Crl_Sign
]

#4: ObjectId: 2.5.29.14 Criticality=false
SubjectKeyIdentifier [
KeyIdentifier [
0000: 7C 0D 9C FD 8E 6D 89 05   B0 19 0C A2 22 01 8A E5  .....m......"...
0010: CA 7B F8 29                                         ...)
]
]


... is not trusted. Install reply anyway? [no]:  yes
Certificate reply was installed in keystore
```

5 Verify that the certificate is installed successfully.

   a Run the following command.

   ```
   /usr/java/latest/bin/keytool –list –v –keystore /root/.keystore –storepass changeit –keypass
   changeit | grep tomcat
   ```

   b Verify that the output contains `Alias name: tomcat`.



```
root@vdp-mgmt-01:~/#: /usr/java/latest/bin/keytool -list -v -keystore /root/.keystore -storepass changeit -keypass chan
geit | grep tomcat
Alias name: tomcat
```

6 Run the `addFingerprint.sh` script to update the vSphere Data Protection server thumbprint that is displayed in the VM console welcome screen.

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

This script does not return any output.

7 Start the vSphere Data Protection services.

```
emwebapp.sh ––start
```

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

After you generate a signed certificate for a component of the Cloud Management Platform, replace it and update it on the management components in the region to maintain secure connection.

### Procedure

1 Replace vRealize Automation Certificate in Region A

   Replacing the existing certficates for all vRealize Automation Services from the vRealize Automation Management Console

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

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

3 Update the vRealize Automation Certificate on vRealize Operations Manager

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

4 Replace the Certificate of vRealize Orchestrator in Region A

   Import the generated custom certificates to vRealize Orchestrator from the vRealize Orchestrator Control Center. You must import the certificates on both of the vRealize Orchestrator virtual machines.

5 Certificate Replacement for vRealize Business Server in Region A

   Replace the existing certificate of vRealize Business with a new one using the vRealize Business appliance management console.

## Replace vRealize Automation Certificate in Region A

Replacing the existing certficates for all vRealize Automation Services from the vRealize Automation Management Console

### Procedure

1 Log in to the vRealize Automation appliance management console.

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

   b Log in using the following credentials.

| Setting | Value |
|---|---|
| User name | root |
| Password | *vra_appA_root_password* |

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

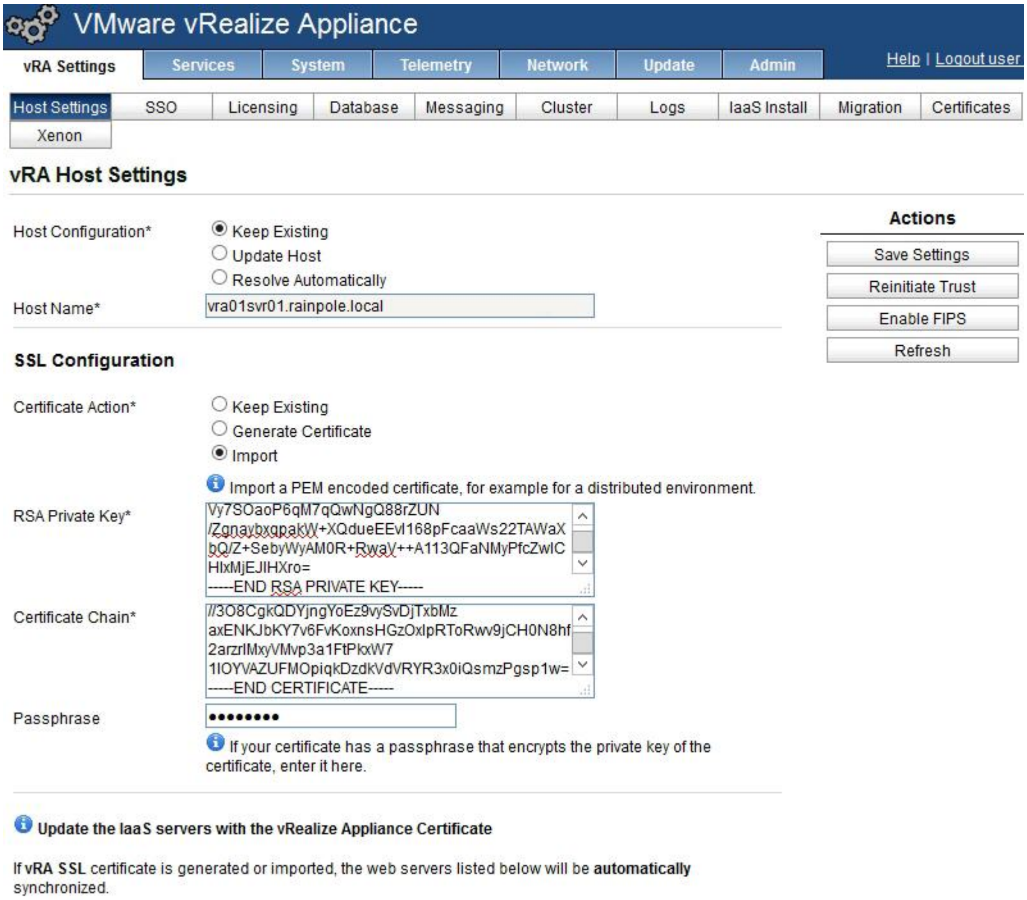
3 If vra01svr01b.rainpole.local is the **MASTER** node, log in to **`https://vra01svr01b.rainpole.local:5480`** using the **`root`** user name and the ***`vra_appB_root_password`*** password instead.

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

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

6 From a text editor on the Windows host that you use to access the data center, copy the content of the following certificate files and paste it in the corresponding text boxes in the user interface, and click **Save Settings**.

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



**vRA Host Settings**

Host Configuration*
● Keep Existing
○ Update Host
○ Resolve Automatically

Host Name* vra01svr01.rainpole.local

**SSL Configuration**

Certificate Action*
○ Keep Existing
○ Generate Certificate
● Import

Import a PEM encoded certificate, for example for a distributed environment.

RSA Private Key*

```
Vy7SOaoP6qM7qQwNgQ88rZUN
/ZgnaybxqpakW+XQdueEEvl168pFcaaWs22TAWaX
bQ/Z+SebyWyAM0R+RwaV++A113QFaNMyPfcZwIC
HlxMjEJlHXro=
-----END RSA PRIVATE KEY-----
```

Certificate Chain*

```
//3O8CgkQDYjngYoEz9vySvDjTxbMz
axENKJbKY7v6FvKoxnsHGzOxlpRToRwv9jCH0N8hf
2arzrlMxyVMvp3a1FtPkxW7
1IOYVAZUFMOpiqkDzdkVdVRYR3x0iQsmzPgsp1w=
-----END CERTIFICATE-----
```

Passphrase ••••••••

If your certificate has a passphrase that encrypts the private key of the certificate, enter it here.

**Update the IaaS servers with the vRealize Appliance Certificate**

If **vRA SSL** certificate is generated or imported, the web servers listed below will be **automatically** synchronized.

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

| IaaS Component | Component Type |
|---|---|
| IaaS Web server | IaaS Web |
| IaaS Manager Service | Manager Service |

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

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

### Procedure

1 Update the vRealize Automation certificate in the component registry authentication with vRealize Automation for vRealize Orchestrator.

   a Open a Web browser and go to **`https://vra01vro01a.rainpole.local:8283/vco-controlcenter`**.

   b Log in using the following credentials.

   | Setting | Value |
   |---|---|
   | User name | root |
   | Password | *hostA_root_password* |

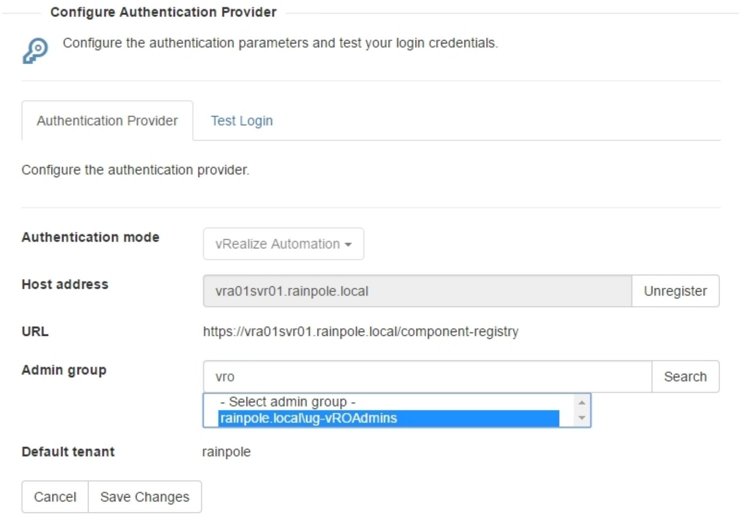
   c On the **Home** page, under **Manage** click **Configure Authentication Provider**.

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

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

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

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



Configure Authentication Provider

Configure the authentication parameters and test your login credentials.

Configure the authentication provider.

Authentication mode: vRealize Automation

Host address: vra01svr01.rainpole.local

URL: https://vra01svr01.rainpole.local/component-registry

Admin group: vro

- Select admin group -

rainpole.local\ug-vROAdmins

Default tenant: rainpole

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

2 Update the vRealize Automation certificate on vRealize Business.

a Open a Web browser and go to **`https://vra01bus01.rainpole.local:5480`**.

b Log in using the following credentials.

| Setting | Value |
|---|---|
| User name | root |
| Password | *vrb_server_root_password* |

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

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

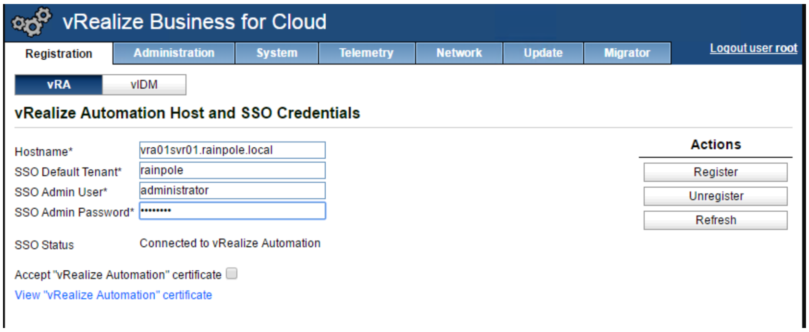
d Click **Register** to connect to vRealize Automation and get its certificate.

A failure message appears at the top of the page. Wait until the SSO Status changes to The `certificate of "vRealize Automation" is not trusted. Please view and accept to register.`

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

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

**SSO Status** changes to `Connected to vRealize Automation`.



vRealize Automation Host and SSO Credentials

Hostname* vra01svr01.rainpole.local
SSO Default Tenant* rainpole
SSO Admin User* administrator
SSO Admin Password* ••••••••

SSO Status Connected to vRealize Automation

Accept "vRealize Automation" certificate □
View "vRealize Automation" certificate

## Update the vRealize Automation Certificate on vRealize Operations Manager

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

### Procedure

1 Log in to vRealize Operations Manager by using the administration console.

   a Open a Web browser and go to **`https://vrops-cluster-01.rainpole.local`**.

   b Log in using the following credentials.

| Setting | Value |
|---|---|
| **User name** | admin |
| **Password** | *vrops_admin_password* |

2 In the left pane of vRealize Operations Manager, click **Administration** and click **Certificates**.

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

4 In the left pane of vRealize Operations Manager, click **Administration** and click **Solutions**.

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

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

## Replace the Certificate of vRealize Orchestrator in Region A

Import the generated custom certificates to vRealize Orchestrator from the vRealize Orchestrator Control Center. You must import the certificates on both of the vRealize Orchestrator virtual machines.

### Procedure

1 Log in to the vRealize Orchestrator Control Center.

   a Open a Web browser and go to `https://vra01vro01a.rainpole.local:8283/vco-controlcenter`.

   b Log in using the following credentials.

| Setting | Value |
|---|---|
| User name | root |
| Password | *hostA_root_password* |

2 From the **Home** page, under **Manage**, click **Certificates**.

3 Click the **Orchestrator Server SSL Certificate** tab, and click **Import > Import from a PEM-encoded file**.

4 Browse to the `vro.2.chain.pem` file in the `vro` folder on your local machine.

5 In the **Key Password** text box, enter the ***`vro_vrealize_full_pem_pass`*** password that you entered during certificate generation and click **Import**.

6 Restart the vRealize Orchestrator appliance for the changes to take effect.

   a From the **Home** page, under **Manage**, click **Startup Options**.

   b On the **Startup Options** page, click **Restart**.

7 Update the certificate on vRealize Automation.

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

   b Log in using the following credentials.

| Setting | Value |
|---|---|
| User name | administrator |
| Password | *vra_administrator_password* |

   c On the **Server Configuration** page, select the **Use an external Orchestrator server** radio button, and click **Test Connection**.

## Certificate Replacement for vRealize Business Server in Region A

Replace the existing certificate of vRealize Business with a new one using the vRealize Business appliance management console.

### Procedure

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

   a Open a Web browser and go to **`https://vra01bus01.rainpole.local:5480`**.

   b Log in using the following credentials.

   | Setting | Value |
   |---|---|
   | User name | root |
   | Password | *vrb_server_root_password* |

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

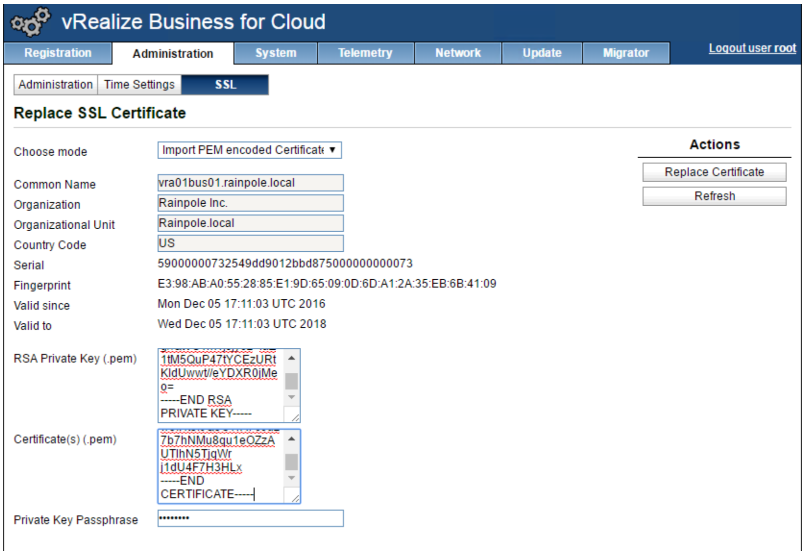
3 On the **Replace SSL Certificate** page, select **Import PEM encoded Certificate** from the **Choose mode** drop-down menu.

4 Enter the values from the generated certificate for vRealize Business and click **Replace Certificate**.

   Use the `vrb.key` file as the **RSA Private Key (.key)** and the `vrb.3.pem` file for the **Certificate(s) (.pem)** entry. chainRoot64laxThese files are in the `vrb` folder that you created during certificate generation.

   | Setting | Value |
   |---|---|
   | Choose mode | Import PEM encoded Certificate |
   | RSA Private Key (.key) | ------BEGIN RSA PRIVATE KEY-----<br>*private_key_value*<br>-----END RSA PRIVATE KEY----- |
   | Certificate(s) (.pem) | -----BEGIN CERTIFICATE-----<br>*Server_certificate_value*<br>-----END CERTIFICATE-----<br>-----BEGIN CERTIFICATE-----<br>*Intermediate_CA*<br>-----END CERTIFICATE-----<br>-----BEGIN CERTIFICATE-----<br>*Root_CA_certificate_value*<br>-----END CERTIFICATE----- |
   | Private Key Passphrase | *vrb_cert_passphrase* |

   chainRoot64lax



Replace SSL Certificate

| | |
|---|---|
| Choose mode | Import PEM encoded Certificate |
| Common Name | vra01bus01.rainpole.local |
| Organization | Rainpole Inc. |
| Organizational Unit | Rainpole.local |
| Country Code | US |
| Serial | 59000000732549dd9012bbd875000000000073 |
| Fingerprint | E3:98:AB:A0:55:28:85:E1:9D:65:09:0D:6D:A1:2A:35:EB:6B:41:09 |
| Valid since | Mon Dec 05 17:11:03 UTC 2016 |
| Valid to | Wed Dec 05 17:11:03 UTC 2018 |
| RSA Private Key (.pem) | 1tM5QuP47tYCEzURt<br>KldUwwt//eYDXR0jMe<br>o=<br>-----END RSA<br>PRIVATE KEY----- |
| Certificate(s) (.pem) | 7b7hNMu8qu1eOZzA<br>UTlhN5TjqWr<br>j1dU4F7H3HLx<br>-----END<br>CERTIFICATE----- |
| Private Key Passphrase | •••••••• |

5 Verify that the certificate changed successfully.

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

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

## Replace Certificates of the Operations Management Components in Region A

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

### Procedure

1 Replace vRealize Operations Manager Certificate in Region A

Use the generated PEM file to replace the current certificate on the vRealize Operations Manager administrator user interface.

2 Replace the Certificate of vRealize Log Insight in Region A

After you generate the PEM certificate chain file that contains the own certificate, the signer certificate and the private key file, upload the certificate chain to vRealize Log Insight.

3 Update Event Forwarding in Region B

After you replace the certificate of vRealize Log Insight in Region A, you update log forwarding from vRealize Log Insight in Region B to vRealize Log Insight in Region A.

## Replace vRealize Operations Manager Certificate in Region A

Use the generated PEM file to replace the current certificate on the vRealize Operations Manager administrator user interface.

### Procedure

1 Log in to the vRealize Operations Manager administrator user interface.

   a Open a Web browser and go to `https://vrops-cluster-01.rainpole.local/admin`.

   b Log in using the following credentials.

   | Setting | Value |
   |---|---|
   | User name | admin |
   | Password | *vrops_admin_password* |

2 At the upper right corner of the UI, click on the yellow **SSL Certificate** icon.

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

4 Click **Browse**, locate the PEM file, and click **Open** .

   | Certificate Generation Option | Certificate File |
   |---|---|
   | Using the CertGenVVD tool | vrops-forVVD4.0.2.chain.pem |
   | Manual generation | vrops01-chain.pem |

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

6 Update the vRealize Operations Manager certificate for workload reclamation communication with vRealize Automation.

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

   b Log in using the following credentials

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

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

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

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

## Replace the Certificate of vRealize Log Insight in Region A

After you generate the PEM certificate chain file that contains the own certificate, the signer certificate and the private key file, upload the certificate chain to vRealize Log Insight.

### Procedure

1 Log in to the vRealize Log Insight user interface.

 a Open a Web browser and go to **`https://vrli-cluster-01.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 |
| Manual generation | vrli-sfo01.chain.pem |

The certificate is uploaded to vRealize Log Insight.

5 Import the certificate into the Java Keystore on each vRealize Log Insight node.

 a Open an SSH session and go each of the vRealize Log Insight nodes.

| Name | Role |
|---|---|
| vrli-mstr-01.sfo01.rainpole.local | Master node |
| vrli-wrkr-01.sfo01.rainpole.local | Worker node 1 |
| vrli-wrkr-02.sfo01.rainpole.local | Worker node 2 |

 b Log in using the following credentials.

| Setting0 | Value |
|---|---|
| User name | root |
| Password | *vrli_root_password* |

 c Convert the on-disk **`vrli.sfo01.2.chain.pem`** file into a **`vrli.sfo01.2.chain.crt`** file.

```
openssl x509 -in /root/vrli.sfo01.2.chain.pem -inform PEM -out /root/vrli.sfo01.2.chain.crt
```

d Import the vrli.sfo01.2.chain.crt into the Java Keystore:

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

../../bin/keytool -import -alias loginsight -file /root/vrli.sfo01.2.chain.crt -keystore
cacerts
```

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

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

g Repeat this operation on all vRealize Log Insight nodes until complete.

6 Open a Web browser and go to **`https://vrli-cluster-01.sfo01.rainpole.local`**

A warning message that the connection is not trusted appears.

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

8 Import the certificate in your Web browser.

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

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

## Update Event Forwarding in Region B

After you replace the certificate of vRealize Log Insight in Region A, you update log forwarding from vRealize Log Insight in Region B to vRealize Log Insight in Region A.

### Procedure

1 Copy the certificate PEM file for vRealize Log Insight in Region A to the root directory of vrli-mstr-01.sfo01.rainpole.local.

a Use the `scp` command, FileZilla, or WinSCP to connect to vrli-mstr-01.sfo01.rainpole.local

b Log in using the following credentials.

| Setting | Value |
|---|---|
| user name | root |
| Password | *vrli_regionA_root_password* |

c Navigate to the `\root` directory on vrli-mstr-01.sfo01.rainpole.local.

d Copy the certificate PEM file `vrli.sfo01.2.chain.pem` on your computer to the `\root` directory on the master node. Overwrite any existing file with the same name.

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

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

| Name | Role |
|---|---|
| vrli-mstr-51.lax01.rainpole.local | Master node |
| vrli-wrkr-51.lax01.rainpole.local | Worker node 1 |
| vrli-wrkr-52.lax01.rainpole.local | Worker node 2 |

b Log in using the following credentials.

| Name | Role |
|---|---|
| User name | root |
| Password | *vrli_regionB_root_password* |

c Using `scp`, remotely copy the the SSL certificate from the master node in Region A.

```
scp root@vrli-
mstr-01.sfo01.rainpole.local:/root/vrli.sfo01.2.chain.pem /root/vrli.sfo01.2.chain.pem
```

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

e When prompted for the root password, type the following

| Setting | Value |
|---|---|
| User name | root |
| Password | *vrli_regionA_root_password* |

f Convert the `vrli.sfo01.2.chain.pem` file into a `vrli.sfo01.2.chain.crt` file:

```
openssl x509 -in /root/vrli.sfo01.2.chain.pem -inform PEM -out /root/vrli.sfo01.2.chain.crt
```

g Import the `vrli.sfo01.2.chain.crt` in the Java keystore of the vRealize Log Insight node.

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

../../bin/keytool -import -alias loginsight -file /root/vrli.sfo01.2.chain.crt -keystore
cacerts
```

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

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

j Repeat this operation on all vRealize Log Insight nodes and restart them.

3 Log in to the vRealize Log Insight user interface.

a Open a Web browser and go to **`https://vrli-cluster-51.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.

# Region B Certificate Replacement

2

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

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

  The first step in certificate generation and replacement is setting up a Microsoft Certificate Authority template through a Remote Desktop Protocol session. After you have created the new template, you add it to the certificate templates of the Microsoft CA.

- Use the Certificate Generation Utility to Generate Certificates Automatically in Region B

  You can use the VMware Validated Design Certificate Generation Utility (CertGenVVD) to generate signed certificates that you can import to the SDDC management products in Region B. You can then import the certificates to these components to maintain secure connection to the external network and between the components themselves.

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

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

- Replace Certificates of the Management Products in Region B

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

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

The first step in certificate generation and replacement is setting up a Microsoft Certificate Authority template through a Remote Desktop Protocol session. After you have created the new template, you add it to the certificate templates of the Microsoft CA.

### Prerequisites

This VMware Validated Design sets the CA up on both Active Directory (AD) servers: the main domain dc01rpl.rainpole.local (root CA) and the Region B subdomain dc51lax.lax01.rainpole.local (the intermediate CA). Both AD servers are running the Microsoft Windows Server 2012 R2 operating system.

- Verify that you installed Microsoft Server 2012 R2 with Active Directory Domain Services enabled.
- Verify that The Certificate Authority Service role and the Certificate Authority Web Enrolment role is installed and configured on the Active Directory Server.
- Verify that dc51lax.lax01.rainpole.local has been set up to be the intermediate CA of the root CA dc01rpl.rainpole.local.

### Procedure

1. Use Remote Desktop Protocol to connect to the CA server dc01lax.lax01.rainpole.local as the AD administrator with the *ad_admin_password* password.
2. Click **Start > Run**, enter `certtmpl.msc`, and click **OK**.
3. In the **Certificate Template Console**, under **Template Display Name,** search the list to see if you can find a template with the name vmware exists
4. if a template with the name vmware already existed, you can skip to Step 11
5. In the **Certificate Template Console**, under **Template Display Name**, right-click **Web Server** and click **Duplicate Template**.
6. In the **Duplicate Template** window, leave **Windows Server 2003 Enterprise** selected for backward compatibility and click **OK**.
7. In the **Properties of New Template** dialog box, click the **General** tab.
8. In the **Template display name** text box, enter `VMware` as the name of the new template.
9. Click the **Extensions** tab and specify extensions information:
   a. Select **Application Policies** and click **Edit**.
   b. Select **Server Authentication**, click **Remove**, and click **OK**.
   c. Select **Key Usage** and click **Edit**.
   d. Click the **Signature is proof of origin (nonrepudiation)** check box.
   e. Leave the default for all other options.
   f. Click **OK**.
10. Click the **Subject Name** tab, ensure that the **Supply in the request** option is selected, and click **OK** to save the template.
11. To add the new template to your CA, click **Start > Run**, enter `certsrv.msc`, and click **OK**.
12. In the **Certification Authority** window, expand the left pane if it is collapsed.
13. Right-click **Certificate Templates** and select **New** > **Certificate Template to Issue**.

14 In the **Enable Certificate Templates** dialog box, select the VMware certificate that you just created in the **Name** column and click **OK.**

## Use the Certificate Generation Utility to Generate Certificates Automatically in Region B

You can use the VMware Validated Design Certificate Generation Utility (CertGenVVD) to generate signed certificates that you can import to the SDDC management products in Region B. You can then import the certificates to these components to maintain secure connection to the external network and between the components themselves.

### Procedure

1 Use the Certificate Generation Utility to Generate CA-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 product with a single operation.

2 Additional Configuration for Intermediate Certificate Authority in Region B

   If you use an intermediate certificate authority on lax01.rainpole.local as certificate signer, CertGenVVD utility only retrieves the intermediate Base 64 certificate from the Microsoft CA. You must create a certificate chain file that also includes the root CA certificate.

## Use the Certificate Generation Utility to Generate CA-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 product with a single operation.

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

### Prerequisites

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

### Procedure

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

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

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

4. Verify that following properties are configured.

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

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

   - comp01esx51.lax01.txt
   - comp01esx52.lax01.txt
   - comp01esx53.lax01.txt
   - comp01esx54.lax01.txt
   - comp01nsxm51.lax01.txt
   - comp01vc51.lax01.txt
   - comp01psc51.lax01.txt
   - mgmt01esx51.lax01.txt
   - mgmt01esx52.lax01.txt
   - mgmt01esx53.lax01.txt
   - mgmt01esx54.lax01.txt
   - mgmt01nsxm51.lax01.txt
   - mgmt01srm51.lax01.txt
   - mgmt01vc51.lax01.txt
   - mgmt01vdp51.lax01.txt
   - mgmt01vrms51.lax01.txt
   - lax01psc51.lax01.txt
   - vrli.lax01.txt

6. If `lax01psc51.lax01.txt` does not exist, create it so that you can generate certificates for the Platform Services Controllers that are behind a load balancer in Region B.

   a. Make a copy of `mgmt01psc51.lax01.txt` and save it as `lax01psc51.lax01.txt`.

   b. Open the copied file in a text editor, and verify that the following properties are configured.

      **lax01psc51.lax01.txt**

      ```
      [CERT]
      NAME=default
      ORG=default
      OU=default
      LOC=LAC
      ST=default
      CC=default
      CN=lax01psc51.lax01.rainpole.local
      keysize=default
      [SAN]
      lax01psc51
      lax01psc51.lax01.rainpole.local
      ```

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

   For example, of you use CertGenVVD 2.1, navigate to the following folder:

   ```
   cd C:\CertGenVVD-2.1
   ```

8. Run the following command to grant PowerShell permissions to run third-party shell scripts.

   ```
   Set-ExecutionPolicy Unrestricted
   ```

9. Run the following command to validate prerequisites for running the utility.

   Verify that VMware is included in the available CA Template Policy.

   ```
   .\CertgenVVD-2.1.ps1 -validate
   ```

10. Run the following command to generate MSCA-signed certificates.

    ```
    .\CertGenVVD-2.1.ps1 -MSCASigned -attrib 'CertificateTemplate:VMware'
    ```

11. In the `c:\CertGenVVD-`*`version`* folder, verify that the utility created the `SignedByMSCACerts` subfolder.

### What to do next

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

## Additional Configuration for Intermediate Certificate Authority in Region B

If you use an intermediate certificate authority on lax01.rainpole.local as certificate signer, CertGenVVD utility only retrieves the intermediate Base 64 certificate from the Microsoft CA. You must create a certificate chain file that also includes the root CA certificate.

### Procedure

1 Log in to the site for certificate request on the lax01.rainpole.local AD server.

  a Open a browser and go to `https://dc51lax.lax01.rainpole.local/certsrv`.

  b Log in using the following credentials.

| Setting | Values |
|---|---|
| User name | *ad_administrator* |
| password | *ad_administrator_password* |

2 Download and export the certificates of the intermediate and root CAs.

  a Click **Download a CA certificate, certificate chain, or CRL**.

  b Select **Current[lax01-DC01LAX-CA** in the CA certificate list, select **Base 64** and click **Download CA certificate chain**.

  c Save the file as `chainroot.p7b`.

  d Open `chainroot.p7b`.

  The **certmgr** utility appears.

  e Navigate to Certificates folder

  f Right-click **lax01-DC01LAX-CA** and select **All Tasks > Export**.

  The Certificate Export Wizard appears.

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

  h Select **Base-64 encoded X.509 (.CER)** and click **Next**

  i On the **File to Export** page, browse to the `C:\CertGenVVD-`*`version`*`\SignedByMSCACerts\lax01-intermediate-ca.cer`, click **Next** and click **Finish**.

  j Click **Okay** when you see a message about successful export.

  k In the **certmgr** utility, right click **rainpole-DC01RPL-CA** and select **All Tasks > Export** and repeat the steps to save the rainpole.local root CA certificate as `C:\CertGenVVD-`*`version`*`\SignedByMSCACerts\rainpole-root-ca.cer`.

3 Create the `chainRoot64lax.cer` file that includes both root and intermediate CA certificates.

   a Open `rainpole-root-ca.cer` in a text editor.

   b Copy the entire content and close the file.

   c Open `lax01-intermediate-ca.cer` in a text editor, press Enter to insert a new line at the end of the file, paste the `rainpole-root-ca.cer` content.

   d Save the file as `chainRoot64lax.cer` to the `C:\CertGenVVD-`*`version`*`\SignedByMSCACerts\`.

   e Close all files.

   f Verify that the new file `C:\CertGenVVD-`*`version`*`\SignedByMSCACerts\chainRoot64lax.cer` exists and contains the content of both `lax01-intermediate-ca.cer` and `rainpole-root-ca.cer`.

4 Refresh all MSCA-signed certificates with new intermediate and root CAs.

   a Open the `C:\CertGenVVD-`*`version`* folder.

   b Make a copy of the `SignedByMSCACerts` folder and name is as `SignedByMSCACerts-backup`.

   c Rename the `SignedByMSCACerts` folder to `CSRCerts`.

   d Open the `C:\CSRCerts\RootCA\` folder.

   e Delete the `Root64.cer` file

   f Create a copy of `chainRoot64lax.cer` as `Root64.cer`.

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

   h Run the following command to regenerate all certificate files and packages using the new `Root64.cer`.

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

   i Rename the `CSRCerts` folder back to `SignedByMSCACerts`.

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

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

### Prerequisites

A Window host that is that has access to your data center.

### Procedure

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

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

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

4. Verify that following properties are configured.

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

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

**Table 2-1. 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<br>■ lax01m01psc01.lax01.rainpole.local<br>■ 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 |
| vSphere Data Protection | lax01m01vdp01.lax01.rainpole.local | lax01m01vdp01.txt |
| Site Recovery Manager and vSphere Replication | lax01m01srm01.lax01.rainpole.local | lax01m01srm01.txt |

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

| Host Name or Service in Region B | | Configuration Files |
|---|---|---|
| | lax01m01vrms01.lax01.rainpole.local | lax01m01vrms01.txt |
| Operations Management Layer | | |
| vRealize Log Insight | ■ lax01vrli01.lax01.rainpole.local<br>■ lax01vrli01.lax01a.rainpole.local<br>■ lax01vrli01.lax01b.rainpole.local<br>■ lax01vrli01.lax01c.rainpole.local | vrli.lax01.txt |

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

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

**lax01psc01.txt**

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

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

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

8 Grant permissions to run third-party PowerShell scripts.

```
Set-ExecutionPolicy Unrestricted
```

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

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

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

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

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

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

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

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

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

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

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

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

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

### What to do next

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

## Replace Certificates of the Management Products in Region B

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

### Prerequisites

Generate a certificate for the products in this validated design in one of the following ways:

- Use the VMware Validated Design Certificate Utility. See Use the Certificate Generation Utility to Generate Certificates Automatically in Region B.
- Generate Certificate Signing Requests manually and use them to have the product certificates signed by the certificate authority on the child AD server in Region B. See GUID-99249BA6-6137-4001-A38E-200A9D3DEE03#GUID-99249BA6-6137-4001-A38E-200A9D3DEE03 and GUID-9DC7BCC2-7BC6-4A67-B4FC-2CAD32145CCB#GUID-9DC7BCC2-7BC6-4A67-B4FC-2CAD32145CCB.

### Procedure

1. Replace Certificates of the Virtual Infrastructure Components in Region B

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

2. Replace Certificates of the Operations Management Components in Region B

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

## Replace Certificates of the Virtual Infrastructure Components in Region B

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

### Procedure

1. Replace the Platform Services Controller Certificates in Region B

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

2. Replace vCenter Server Certificates in Region B

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

3. Replace the Default Certificate with a Custom Certificate on the ESXi Hosts in Region B

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

4. Replace the NSX Manager Certificates in Region B

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

5 Replace the Certificate of vSphere Data Protection in Region B

   vSphere Data Protection comes with a default self-signed certificate. Install a CA-signed certificate that authenticates vSphere Data Protection over HTTPS.

6 Replace the VMware Site Recovery Manager Certificates

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

7 Install the CA-Signed Certificate on vSphere Replication

   After you generate a PKCS#12 certificate file, replace the default VMware-signed certificate with this certificate on vSphere Replication in both regions.

## Replace the Platform Services Controller Certificates in Region B

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

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

You must repeat this procedure twice: first on the Platform Services Controller for the Management vCenter Server, and then on the Platform Services Controller for the Compute vCenter Server.

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

| Platform Services Controller | Certificate File Name | Replacement Order |
|---|---|---|
| mgmt01psc51.lax01.rainpole.local | ■ lax01psc51.lax01.key<br>■ lax01psc51.lax01.3.pem (CertGenVVD)<br>■ lax01psc51.lax01.1.chain.cer (Manual)<br>■ chainRoot64.cer | First |
| comp01psc51.lax01.rainpole.local | ■ lax01psc51.lax01.key<br>■ lax01psc51.lax01.3.pem (CertGenVVD)<br>■ lax01psc51.lax01.1.chain.cer (Manual)<br>■ chainRoot64.cer | Second |

### Procedure

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

  a Open a Web browser and go to **`https://mgmt01vc51.lax01.rainpole.local/vsphere-client`**.

  b Log in using the following credentials.

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

2 Disable the Platform Services Controller for the shared edge and compute cluster comp01psc51 in the load balancer to route all traffic to the Platform Services Controller for the management cluster mgmt01psc51.

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

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

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

  d Double-click the **LAX01PSC51** edge device to open its network settings.

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

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

  g Select the **comp01psc51** member, click **Edit**, select **Disable** from the **State** drop-down menu and click **OK**.

  h Repeat Step 2f and Step 2g to disable comp01psc51 in **pool-2**.

3 Disconnect the NSX Manager instances from the Platform Services Controller temporarily.

  a Open a Web Browser and go to **`https://mgmt01nsxm51.lax01.rainpole.local`**.

  b Log in using the following credentials

| Setting | Value |
|---|---|
| User name | admin |
| Password | *nsx_manager_admin_password* |

  c Click **Manage vCenter Registration**

  d Click the **Unconfigure** button next to **Lookup Service URL**.

  e Repeat the steps on **`https://comp01nsxm51.sfo01.rainpole.local`**.

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

   a Open an SSH connection to mgmt01psc51.lax01.rainpole.local.

   b Log in using the following credentials.

| Setting | Value |
|---|---|
| **Username** | root |
| **Password** | *mgmtpsc_root_password* |

5 Change the Platform Services Controller command shell to the Bash shell so that you can use secure copy `scp` connections.

```
shell
chsh -s /bin/bash root
```

6 Copy the generated certificate files `lax01psc51.lax01.key`, `lax01psc51.lax01.3.pem` and `chainRoot64.cer` from the Windows host to the `/tmp/ssl` directory on the Platform Services Controller.

   Use `scp`, FileZilla or WinSCP to copy the files.

7 Rename `lax01psc51.lax01.3.pem` to `lax01psc51.lax01.1.chain.cer`.

8 Add the root certificate to the VMware Endpoint Certificate Store as a trusted root certificate using following command.

   Enter the vCenter Single Sign-On password when prompted.

```
/usr/lib/vmware-vmafd/bin/dir-cli trustedcert publish --chain --cert /tmp/ssl/chainRoot64.cer
```

9 Replace the certificate on the Platform Services Controller.

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

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

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

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

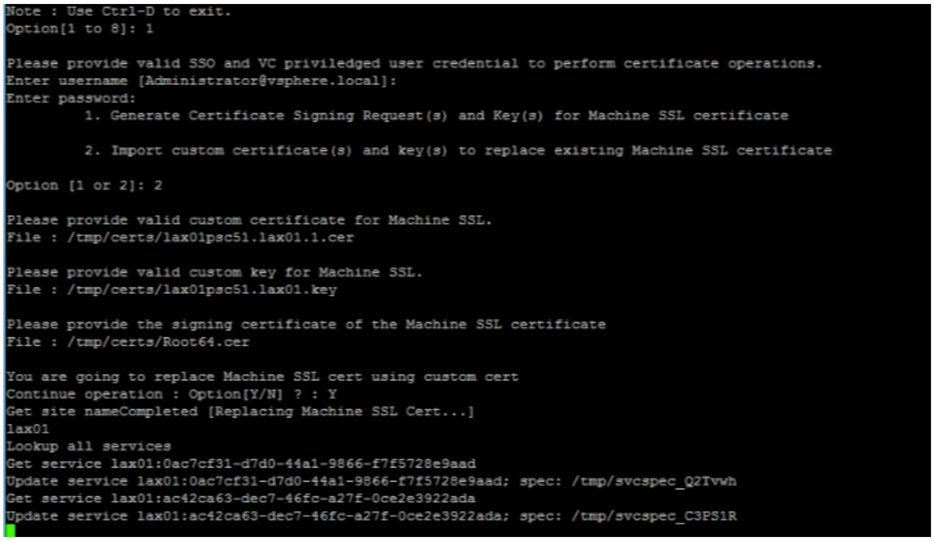
   d Select **Option 2 (Import custom certificate(s) and key(s) to replace existing Machine SSL certificate).**

   e When prompted for the custom certificate, enter **`/tmp/ssl/lax01psc51.lax01.1.chain.cer`**.

   f When prompted for the custom key, enter **`/tmp/ssl/lax01psc51.lax01.key.`**

g When prompted for the signing certificate, enter **`/tmp/ssl/chainRoot64.cer.`**

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



```
Note : Use Ctrl-D to exit.
Option[1 to 8]: 1

Please provide valid SSO and VC priviledged user credential to perform certificate operations.
Enter username [Administrator@vsphere.local]:
Enter password:
         1. Generate Certificate Signing Request(s) and Key(s) for Machine SSL certificate

         2. Import custom certificate(s) and key(s) to replace existing Machine SSL certificate

Option [1 or 2]: 2

Please provide valid custom certificate for Machine SSL.
File : /tmp/certs/lax01psc51.lax01.1.cer

Please provide valid custom key for Machine SSL.
File : /tmp/certs/lax01psc51.lax01.key

Please provide the signing certificate of the Machine SSL certificate
File : /tmp/certs/Root64.cer

You are going to replace Machine SSL cert using custom cert
Continue operation : Option[Y/N] ? : Y
Get site nameCompleted [Replacing Machine SSL Cert...]
lax01
Lookup all services
Get service lax01:0ac7cf31-d7d0-44a1-9866-f7f5728e9aad
Update service lax01:0ac7cf31-d7d0-44a1-9866-f7f5728e9aad; spec: /tmp/svcspec_Q2Tvwh
Get service lax01:ac42ca63-dec7-46fc-a27f-0ce2e3922ada
Update service lax01:ac42ca63-dec7-46fc-a27f-0ce2e3922ada; spec: /tmp/svcspec_C3PS1R
```

Wait until the Platform Services Controller services restart successfully.

10 Validate that the new certificate has been installed successfully.

a Open a Web Browser and go to **`https://mgmt01psc51.lax01.rainpole.local`**.

b Verify that the Web browser shows the new certificate.

11 Restart the VAMI service to update certificate for the appliance management interface.

a Go back to the mgmt01psc51.lax01.rainpole.local SSH terminal.

b Enter the following command to update certificate for the appliance management interface.

```
/etc/init.d/vami-lighttp restart
```

12 Switch the shell back to the appliance shell.

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

13 Repeat Step 4 to Step 11 to replace the certificate on comp01psc51.lax01.rainpole.local.

14 Restart the services on the Management vCenter Server.

a Open an SSH connection to mgmt01vc51.lax01.rainpole.local.

b Log in using the following credentials.

| Setting | Values |
|---|---|
| Username | root |
| Password | *mgmtvc_root_password* |

c Switch from appliance shell to the Bash shell.

```
shell
```

d Restart vCenter Server services by using the following command.

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

**15** Restore load balancer configuration.

a Open a Web Browser and go to **`https://mgmt01vc51.lax01.rainpole.local/vsphere-client`**.

b Log in using the following credentials

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

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

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

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

f Double-click the **LAX01PSC51** edge device to open its network settings.

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

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

i Select the **comp01psc51** member, click **Edit**, select **Enabled** from the **State** drop-down menu, and click **OK**.

j Repeat Step 15h and Step 15i to enable comp01psc51 in **pool-2**.

**16** Repeat Step 15 to restart the services on the Compute vCenter Server comp01vc51.lax01.rainpole.local in Region B and on the vCenter Server instances mgmt01vc01.sfo01.rainpole.local and comp01vc01.sfo01.rainpole.local in Region A.

### What to do next

If you replace only the certificate of the Platform Services Controller instances, reconnect the NSX Managers to the Platform Services Controller load balancer and to vCenter Server after you install the custom certificates on the nodes. See Connect NSX Manager to the Management vCenter Server in Region B.

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

## Replace vCenter Server Certificates in Region B

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

### Procedure

1. Replace the vCenter Server Certificates in Region B

   After you replace the Platform Services Controller certificate, you replace the vCenter Server machine SSL certificate.  You generate a vCenter Server certificate manually or by using the CertGenVVD tool.

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

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

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

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

4. Update the vCenter Server Certificates on the Cloud Management Platform in Region B

   After you replace the certificates on the vCenter Server instances in Region B, reconnect vRealize Orchestrator to vCenter Server.

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

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

### Replace the vCenter Server Certificates in Region B

After you replace the Platform Services Controller certificate, you replace the vCenter Server machine SSL certificate.  You generate a vCenter Server certificate manually or by using the CertGenVVD tool.

You replace certificates twice, once for each vCenter Server instance. You can start replacing certificates on Management vCenter Server mgmt01vc51.lax01.rainpole.local first.

### Table 2-3. Certificate-Related Files on the vCenter Server Instances

| vCenter Server FQDN | Files for Certificate Replacement | Replacement Order |
|---|---|---|
| mgmt01vc51.lax01.rainpole.local | ■ mgmt01vc51.lax01_ssl.key<br>■ mgmt01vc51.lax01.3.pem (CertGenVVD2.1)<br>■ mgmt01vc51.lax01.1.chain.cer (Manual)<br>■ chainRoot64.cer | After you replace the certificate on the management Platform Services Controller. |
| comp01vc51.lax01.rainpole.local | ■ comp01vc51.lax01_ssl.key<br>■ comp01vc51.lax01.3.pem (CertGenVVD2.1)<br>■ comp01vc51.lax01.1.chain.cer (Manual)<br>■ chainRoot64.cer | After you replace the certificate on the compute Platform Services Controller. |

### Procedure

1 Use the `scp` command, FileZilla, or WinSCP to copy the machine and CA certificate files to the `/tmp/ssl` directory on the Management vCenter Server.

2 Log in to the vCenter Server instance by using Secure Shell client.

   a Open an SSH connection to the FQDN of the vCenter Server appliance. **mgmt01vc51.lax01.rainpole.local**.

   b Log in using the following credentials.

| Setting | Value |
|---|---|
| User name | root |
| Password | *vcenter_server_root_password* |

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

   a Add the root certificate to the VMware Endpoint Certificate Store as a trusted root certificate using the following command and enter the vCenter Single Sign-On password when prompted.

```
/usr/lib/vmware-vmafd/bin/dir-cli trustedcert publish --chain --cert /tmp/ssl/chainRoot64.cer
```

   b Rename `mgmt01vc51.lax01.3.pem` to `mgmt01vc51.lax01.1.chain.cer`.

```
mv /tmp/ssl/mgmt01vc51.lax01.3.pem /tmp/ssl/mgmt01vc51.lax01.1.chain.cer
```

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

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

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

e When prompted for the **Infrastructure Server IP**, enter the IP address of the Platform Services Controller that is connected to this vCenter Server instance.

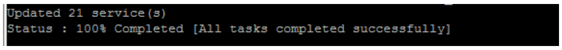
| vCenter Server | IP Address of Connected Platform Services Controller |
|---|---|
| **mgmt01vc51.lax01.rainpole.local** | 172.17.11.61 |
| **comp01vc51.lax01.rainpole.local** | 172.17.11.63 |

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

g When prompted, provide the full path to the custom certificate, the root certificate file, and the key file that have been generated by vSphere Certificate Manager earlier, and confirm the import with **`Yes (Y)`**.

| vCenter Server | Path to Certificate-Related Files |
|---|---|
| **mgmt01vc51.lax01.rainpole.local** | Please provide valid custom certificate for Machine SSL.<br>File: **`/tmp/ssl/mgmt01vc51.lax01.1.chain.cer`**<br>Please provide valid custom key for Machine SSL.<br>File: **`/tmp/ssl/mgmt01vc51.lax01.key`**<br>Please provide the signing certificate of the Machine SSL certificate<br>File: **`/tmp/ssl/chainRoot64.cer`** |
| **comp01vc51.lax01.rainpole.local** | Please provide valid custom certificate for Machine SSL.<br>File: **`/tmp/ssl/comp01vc51.lax01.1.chain.cer`**<br>Please provide valid custom key for Machine SSL.<br>File: **`/tmp/ssl/comp01vc51.lax01.key`**<br>Please provide the signing certificate of the Machine SSL certificate<br>File: **`/tmp/ssl/chainRoot64.cer`** |

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



```
Updated 21 service(s)
Status : 100% Completed [All tasks completed successfully]
```

**5** Log into the vSphere Web client to verify that the certificate replacement is successful.

a Open a Web browser and go to **`https://mgmt01vc51.lax01.rainpole.local/vsphere-client`**.

b Log in using the following credentials.

| Settings | Values |
|---|---|
| User name | administrator@vsphere.local |
| Password | *vsphere_admin_password* |

**6** After you replace the certificate on the mgmt01vc51.lax01.rainpole.local, repeat the procedure to replace the certificate on the compute vCenter Server comp01vc51.lax01.rainpole.local.

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

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

#### Procedure

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

   a Open a Web browser and go to `http://mgmt01nsxm51.lax01.rainpole.local`.

   b Log in using the following credentials.

| Setting | Value |
|---|---|
| User name | admin |
| Password | *nsx_manager_admin_password* |

2 Click **Manage vCenter Registration**.

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

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

| Setting | Value for Both NSX Managers |
|---|---|
| Lookup Service IP | lax01psc51.lax01.rainpole.local |
| Lookup Service Port | 443 |
| SSO Administrator User Name | administrator@vsphere.local |
| Password | *vsphere_admin_password* |

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

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

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

| Setting | Value for NSX Manager for the Management Cluster | Value for NSX Manager for the Shared Edge and Compute Cluster |
|---|---|---|
| vCenter Server | mgmt01vc51.lax01.rainpole.local | comp01vc51.lax01.rainpole.local |
| vCenter User Name | svc-nsxmanager@rainpole.local | svc-nsxmanager@rainpole.local |
| Password | *svc-nsxmanager_password* | *svc-nsxmanager_password* |

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

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

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

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

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

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

#### Procedure

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

   a Open a Web browser and go to `https://mgmt01vc51.lax01.rainpole.local/vsphere-client`.

   b Log in using the following credentials.

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

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

3 On the **Welcome to vSphere Data Protection** page, select **mgmt01vdp51** from the **VDP Appliance** drop-down menu and click **Connect**.

### Update the vCenter Server Certificates on the Cloud Management Platform in Region B

After you replace the certificates on the vCenter Server instances in Region B, reconnect vRealize Orchestrator to vCenter Server.

#### Procedure

1 Reconnect vRealize Orchestrator to vCenter Server.

   a Open a Web Browser and go to `https://vra01vro01a.rainpole.local:8281`.

   b Click **Start Orchestrator Client**.

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

| Setting | Value |
|---|---|
| Host name | vra01vro01a.rainpole.local:8281 |
| User name | svc-vra |
| Password | *svc-vra-password* |

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

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

   f From the **vCenter Server instance** drop-down menu, select **https://comp01vc51.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 with the Compute vCenter Server.

a Open a Web browser and go to **`https://vra01buc51.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 **comp01vc51.laxo01.rainpole.local** entry and click the **Edit** icon.

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

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

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

**3** Recreate the vSphere endpoint in vRealize Automation.

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

b Log in using the following credentials.

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

c Navigate to **Infrastructure > Endpoints > Credentials**, select **comp01vc51lax01 admin** and click **Edit**.

d On the **Credentials** page, enter the password for the vRealize Automation credential for the administrator of comp01vc51.lax01.rainpole.local, and click **Save**.

| Setting | Value |
|---|---|
| Name | comp01vc51lax01 admin |
| Description | Administrator of comp01vc51.lax01.rainpole.local |
| User Name | svc-vra@rainpole.local |
| Password | ***svc_vra_password*** |

e Navigate to **Infrastructure > Endpoints > Endpoints**.

f Have your mouse over **comp01vc01.lax01.rainpole.local** and click **Edit** from the menu.

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

h A certificate warning should popup, 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 instances.

#### Procedure

1 Log in to vRealize Operations Manager by using the administration console.

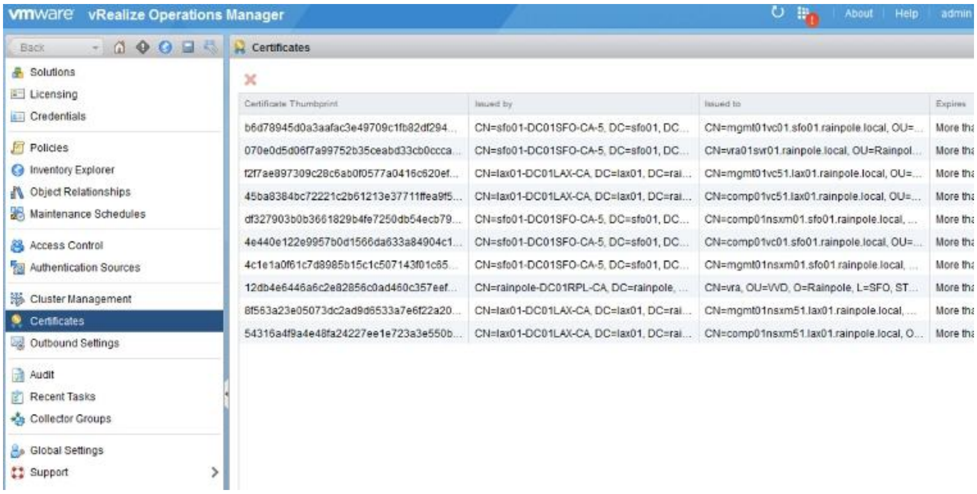
   a Open a Web browser and go to **`https://vrops-cluster-01.rainpole.local`**.

   b Log in using the following credentials.

| Setting | Value |
|---|---|
| **User name** | admin |
| **Password** | *vrops_admin_password* |

2 In the left pane of vRealize Operations Manager, click **Administration** and click **Certificates**.

3 Select the row that contains `CN=mgmt01vc51.lax01.rainpole.local` and click the **Delete** icon.



| Certificate Thumbprint | Issued by | Issued to | Expires |
|---|---|---|---|
| b6d78945d0a3aafac3e49709c1fb82df294... | CN=sfo01-DC01SFO-CA-5, DC=sfo01, DC... | CN=mgmt01vc01.sfo01.rainpole.local, OU=... | More tha |
| 070e0d5d06f7a99752b35ceabd33cb0ccca... | CN=sfo01-DC01SFO-CA-5, DC=sfo01, DC... | CN=vra01svr01.rainpole.local, OU=Rainpol... | More tha |
| f2f7ae897309c28c6ab0f0577a0416c620ef... | CN=lax01-DC01LAX-CA, DC=lax01, DC=rai... | CN=mgmt01vc51.lax01.rainpole.local, OU=... | More tha |
| 45ba8384bc72221c2b61213e37711ffea9f5... | CN=lax01-DC01LAX-CA, DC=lax01, DC=rai... | CN=comp01vc51.lax01.rainpole.local, OU=... | More tha |
| df327903b0b3661829b4fe7250db54ecb79... | CN=sfo01-DC01SFO-CA-5, DC=sfo01, DC... | CN=comp01nsxm01.sfo01.rainpole.local, ... | More tha |
| 4e440e122e9957b0d1566da633a84904c1... | CN=sfo01-DC01SFO-CA-5, DC=sfo01, DC... | CN=comp01vc01.sfo01.rainpole.local, OU=... | More tha |
| 4c1e1a0f61c7d8985b15c1c507143f01c65... | CN=sfo01-DC01SFO-CA-5, DC=sfo01, DC... | CN=mgmt01nsxm01.sfo01.rainpole.local, ... | More tha |
| 12db4e6446a6c2e82856c0ad460c357eef... | CN=rainpole-DC01RPL-CA, DC=rainpole, ... | CN=vra, OU=VVD, O=Rainpole, L=SFO, ST... | More tha |
| 8f563a23e05073dc2ad9d6533a7e6f22a20... | CN=lax01-DC01LAX-CA, DC=lax01, DC=rai... | CN=mgmt01nsxm51.lax01.rainpole.local, ... | More tha |
| 54316a4f9a4e48fa24227ee1e723a3e550b... | CN=lax01-DC01LAX-CA, DC=lax01, DC=rai... | CN=comp01nsxm51.lax01.rainpole.local, O... | More tha |

4 In the left pane of vRealize Operations Manager, click **Administration** and click **Solutions**.

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

6 In the **Manage Solutions** dialog box, select **mgmt01vc51-lax01**, click **Test Connection**, accept the new certificate of the Management vCenter Server and click **Save Settings**.

7 Repeat the procedure to delete the certificate that is installed for the Compute vCenter Server comp01vc51.lax01.rainpole.local and reconnect vRealize Operations Manager to the Compute vCenter Server to install the new certificate.

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

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

### Procedure

1 Change the certificate mode for the ESXi hosts in the management cluster.

The hosts are not automatically provisioned with VMCA certificates when you refresh their certificates.

a Open a Web browser and go to **`https://mgmt01vc51.lax01.rainpole.local`**.

b Log in using the following credentials.

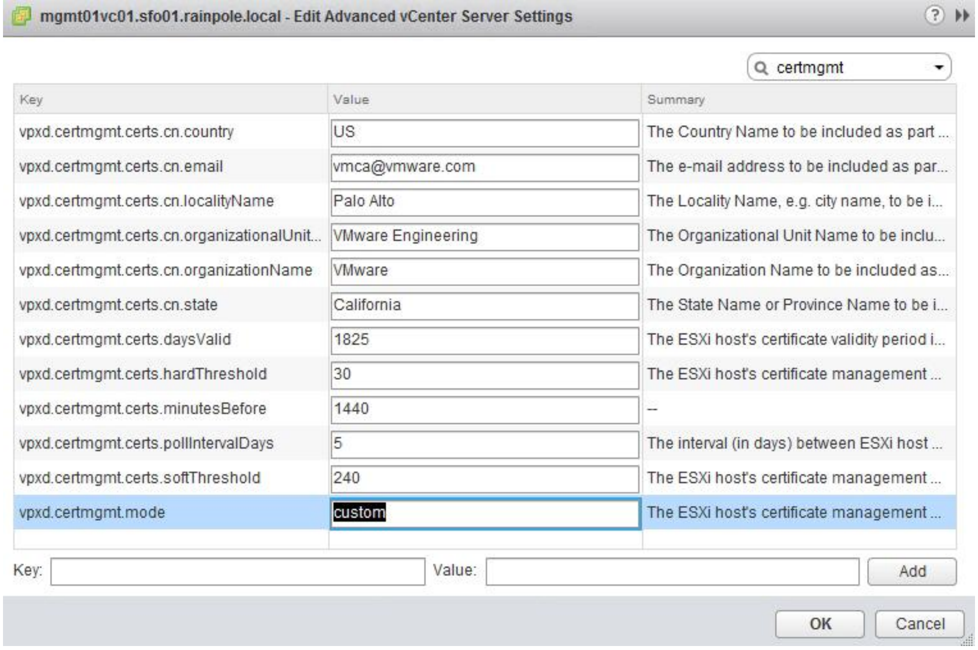
| Setting | Value |
|---|---|
| User name | administrator@vsphere.local |
| Password | *vshpere_admin_password* |

c In the **Navigator**, under **Hosts and Cluster**, select **mgmt01vc51.lax01.rainpole.local**, and click the **Configure** tab.

d Under **Settings**, click **Advanced Setting** and click **Edit**.

e In the Filter box, enter **`certmgmt`** and press Enter to display only certificate management properties.

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



mgmt01vc01.sfo01.rainpole.local - Edit Advanced vCenter Server Settings

| Key | Value | Summary |
|---|---|---|
| vpxd.certmgmt.certs.cn.country | US | The Country Name to be included as part ... |
| vpxd.certmgmt.certs.cn.email | vmca@vmware.com | The e-mail address to be included as par... |
| vpxd.certmgmt.certs.cn.localityName | Palo Alto | The Locality Name, e.g. city name, to be i... |
| vpxd.certmgmt.certs.cn.organizationalUnit... | VMware Engineering | The Organizational Unit Name to be inclu... |
| vpxd.certmgmt.certs.cn.organizationName | VMware | The Organization Name to be included as... |
| vpxd.certmgmt.certs.cn.state | California | The State Name or Province Name to be i... |
| vpxd.certmgmt.certs.daysValid | 1825 | The ESXi host's certificate validity period i... |
| vpxd.certmgmt.certs.hardThreshold | 30 | The ESXi host's certificate management ... |
| vpxd.certmgmt.certs.minutesBefore | 1440 | -- |
| vpxd.certmgmt.certs.pollIntervalDays | 5 | The interval (in days) between ESXi host ... |
| vpxd.certmgmt.certs.softThreshold | 240 | The ESXi host's certificate management ... |
| vpxd.certmgmt.mode | custom | The ESXi host's certificate management ... |

g From the **Home** menu, select **Administration**, and under **Deployment** on the **Administration** page select **System Configuration**.

h Under **System Configuration**, select **Services**, select the **VMware vCenter Server (mgmt01vc51.lax01.rainpole.local )** and select **Actions > Restart**.

2 Add the CA root certificate to the vCenter Server `TRUSTED_ROOTS` store.

If you already replaced the certificate for mgmt01vc51.lax01.rainpole.local, you added the root certificate to the `TRUSTED_ROOTS` stores.

a Open an SSH connection to mgmt01vc51.lax01.rainpole.local.

b Log in using the following credentials.

| Setting | Value |
|---|---|
| User name | root |
| Password | *mgmtvc_root_password* |

c Copy `chainRoot64.cer` from the Windows host that you use to access the data center to the temporary directory `/tmp/ssl` on the vCenter Server Appliance.

You can use `scp`, FileZilla or WinSCP.

d Run the following command.

```
/usr/lib/vmware-vmafd/bin/vecs-cli entry create --store TRUSTED_ROOTS --alias RainpoleCA.crt --
cert /tmp/ssl/chainRoot64.cer
```

3 Replace the certificates on ESXi hosts.

a Open a Web browser and go to **`https://mgmt01vc51.lax01.rainpole.local`**.

b Log in using the following credentials.

| Setting | Value |
|---|---|
| User name | *vcenteradmin* |
| Password | *vshpere_admin_password* |

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

d Under the **LAX01** data center, right-click the **mgmt01esx51.lax01.rainpole.local** vCenter Server object and select **Maintenance Mode > Enter Maintenance Mode**.

e Select **Move powered-off and suspended virtual machines to other hosts in the cluster** and click **OK**.

f After the maintenance task is complete, open an SSH connection to mgmt01esx51.lax01.rainpole.local.

g Transfer `mgmt01esx51.key` and `mgmt01esx51.cer` from the Windows host to the `/etc/vmware/ssl` directory on the host.

h Run the following commands.

```
mv rui.crt orig.rui.crt
mv rui.key orig.rui.key
mv mgmt01esx51.key rui.key
mv mgmt01esx51.cer rui.crt
```

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

j Press the F2 key to access the **System Customization** menu.

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

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

m Press F11 key to confirm the restart.

4 Verify that the custom certificate is installed.

a Open a Web browser and go to **`https://mgmt01esx51.lax01.rainpole.local`**.

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

5 Exit the maintenance mode of the host.

a Open a Web browser and go to **`https://mgmt01vc51.lax01.rainpole.local`**.

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-Mgmt01** data center, right-click the **mgmt01esx51.lax01.rainpole.local** vCenter Server object and select **Maintenance Mode > Exit Maintenance Mode**.

e Make sure that no warning message about an untrusted mgmt01esx51.lax01.rainpole.local certificate appears.

6 Repeat Step 3 to Step 5 for the rest of the management ESXi hosts.

| ESX hosts | Managed by | Certificate file names |
|---|---|---|
| mgmt01esx52.lax01.rainpole.local | mgmt01vc51.lax01.rainpole.local | ■ mgmt01esx52.key<br>■ mgmt01esx52.cert |
| mgmt01esx53.lax01.rainpole.local | mgmt01vc51.lax01.rainpole.local | ■ mgmt01esx53.key<br>■ mgmt01esx53.cert |
| mgmt01esx54.lax01.rainpole.local | mgmt01vc51.lax01.rainpole.local | ■ mgmt01esx54.key<br>■ mgmt01esx54.cert |
| comp01esx51.lax01.rainpole.local | comp01vc51.lax01.rainpole.local | ■ comp01esx51.key<br>■ comp01esx51.cert |

| ESX hosts | Managed by | Certificate file names |
|---|---|---|
| comp01esx52.lax01.rainpole.local | comp01vc51.lax01.rainpole.local | ■ comp01esx52.key<br>■ comp01esx52.cert |
| comp01esx53.lax01.rainpole.local | comp01vc51.lax01.rainpole.local | ■ comp01esx53.key<br>■ comp01esx53.cert |
| comp01esx54.lax01.rainpole.local | comp01vc51.lax01.rainpole.local | ■ comp01esx54.key<br>■ comp01esx54.cert |

## Replace the NSX Manager Certificates in Region B

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

You replace certificates twice, once for each NSX Manager. You start by replacing certificates on NSX Manager for the mgmt01nsxm51.lax01.rainpole.local management cluster.

### Table 2-4. Certificate-Related Files on the NSX Manager Instances in Region B

| NSX Manager FQDN | Certificate File Name | Replacement Time |
|---|---|---|
| mgmt01nsxm51.lax01.rainpole.local | ■ mgmt01nsxm51.lax01.chain.cer from manual generation<br>■ mgmt01nsxm51.lax01.4.p12 from the CertGenVVD tool | After you replace the certificate on the Management vCenter Server |
| comp01nsxm51.lax01.rainpole.local | ■ comp01nsxm51.lax01.cer.chain.cer from manual generation<br>■ comp01nsxm51.lax01.4.p12 from the CertGenVVD tool | After you replace the certificate on the Compute vCenter Server |

### Procedure

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

a Open a Web browser and go to following URL.

| NSX Manager | URL |
|---|---|
| NSX Manager for the management cluster | https://mgmt01nsxm51.lax01.rainpole.local |
| NSX Manager for the shared compute and edge cluster | https://comp01nsxm51.lax01.rainpole.local |

b Log in using the following credentials.

| Setting | Value |
|---|---|
| **User name** | admin |
| **Password** | *nsx_manager_admin_password* |

2 On the **Manage** tab, click **SSL Certificates**, click **Import** and provide the certificate chain file.

3 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**.

4 Re-register the NSX Manager to the Management vCenter Server.

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

| NSX Manager | URL |
|---|---|
| NSX Manager for the management cluster | https://mgmt01nsxm51.lax01.rainpole.local |
| NSX Manager for the shared compute and edge cluster | https://comp01nsxm51.lax01.rainpole.local |

   b Log in using the following credentials.

| Setting | Value |
|---|---|
| **User name** | admin |
| **Password** | *nsx_mngr_admin_password* |

   c Click **Manage vCenter Registration**.

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

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

| Setting | Value |
|---|---|
| **Lookup Service IP** | lax01psc51.lax01.rainpole.local |
| **Lookup Service Port** | 443 |
| **SSO Administrator User Name** | administrator@vsphere.local |
| **Password** | *vsphere_admin_password* |

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

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

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

| Setting | Value for the NSX Manager for the Management Cluster | Value for the NSX Manager for the Shared Edge and Compute Cluster |
|---|---|---|
| vCenter Server | mgmt01vc51.lax01.rainpole.local | comp01vc51.lax01.rainpole.local |
| vCenter User Name | svc-nsxmanager@rainpole.local | |
| Password | *svc-nsxmanager_password* | |

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

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

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

6 Reconnect to the NSX Manager instances in Region A.

a Open a Web browser and go to `https://mgmt01vc51.lax01.rainpole.local`

b Log in using the following credentials.

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

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

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

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

f If primary and secondary nodes are not syncing correctly

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

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

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

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

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

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

l Repeat Step 6e to Step 6k for the NSX Manager instances for the shared edge and compute cluster.

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

7 Reconnect the NSX Manager instances to vRealize Operations Manager.

a Open a Web browser and go to `https://vrops-cluster-01.rainpole.local`.

b Log in using the following credentials.

| Setting | Value |
|---|---|
| User name | admin |
| Password | *vrops_admin_password* |

c In the left pane of vRealize Operations Manager, click **Administration** and click **Certificates**.

d Select the row that contains `CN=mgmt01nsxm51.lax01.rainpole.local` and click the **Delete** icon.

e Select the row that contains `CN=comp01nsxm51.lax01.rainpole.local` and click the **Delete** icon.

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

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

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

i Click the **mgmt01nsxm51-lax01** adapter instance, click **Test Connection**, accept the new certificate and click **Save settings**.

j Click **comp01nsxm51-lax01** adapter instance, click **Test Connection**, accept the new certificate and click **Save settings**.

## Replace the Certificate of vSphere Data Protection in Region B

vSphere Data Protection comes with a default self-signed certificate. Install a CA-signed certificate that authenticates vSphere Data Protection over HTTPS.

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

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

- Install a Manually Generated Certificate on vSphere Data Protection in Region B

  Replace the default VMware-signed certificate on vSphere Data Protection in Region B with the certificate that is signed by the Microsoft CA on the dc01lax.lax01.rainpole.local AD server.

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

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

#### Prerequisites

Generate the Microsoft CA-signed certificate by using the `CertGenVVD` tool. See Use the Certificate Generation Utility to Generate Certificates Automatically in Region A.

#### Procedure

1 Copy the `.keystore` file that `CertGenVVD` tool generated to the `/root` folder on the vSphere Data Protection virtual appliance.

  You can use `scp`, FileZilla or WinSCP.

2 Log in to the vSphere Data Protection appliance.

a Open an SSH connection to the virtual machine mgmt01vdp51.lax01.rainpole.local.

b Log in using the following credentials.

| Setting | Value |
|---|---|
| User name | root |
| Password | *vdp_root_password* |

3 Restart all vSphere Data Protection services by running the following commands.

```
dpnctl stop all
dpnctl start all
```

4 Run the `addFingerprint.sh` script to update the vSphere Data Protection server thumbprint displayed in the VM console welcome screen.

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

### Install a Manually Generated Certificate on vSphere Data Protection in Region B

Replace the default VMware-signed certificate on vSphere Data Protection in Region B with the certificate that is signed by the Microsoft CA on the dc01lax.lax01.rainpole.local AD server.

#### Prerequisites

Generate a certificate for vSphere Data Protection on the dc01lax.lax01.rainpole.local AD server. See GUID-9DC7BCC2-7BC6-4A67-B4FC-2CAD32145CCB#GUID-9DC7BCC2-7BC6-4A67-B4FC-2CAD32145CCB.

#### Procedure

1 On the Windows host that has access to the data center, copy the `vdp.p7b` certificate file to the `/root` folder on the vSphere Data Protection virtual appliance.

You can use `scp`, FileZilla or WinSCP.

2 Log in to the vSphere Data Protection appliance.

a Open an SSH connection to the virtual machine mgmt01vdp51.lax01.rainpole.local.

b Log in using the following credentials.

| Setting | Value |
|---|---|
| User name | root |
| Password | *vdp_root_password* |

3 Verify that the vSphere Data Protection services are stopped.

```
emwebapp.sh --test
```

If the services are running, stop them by running the following command.

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

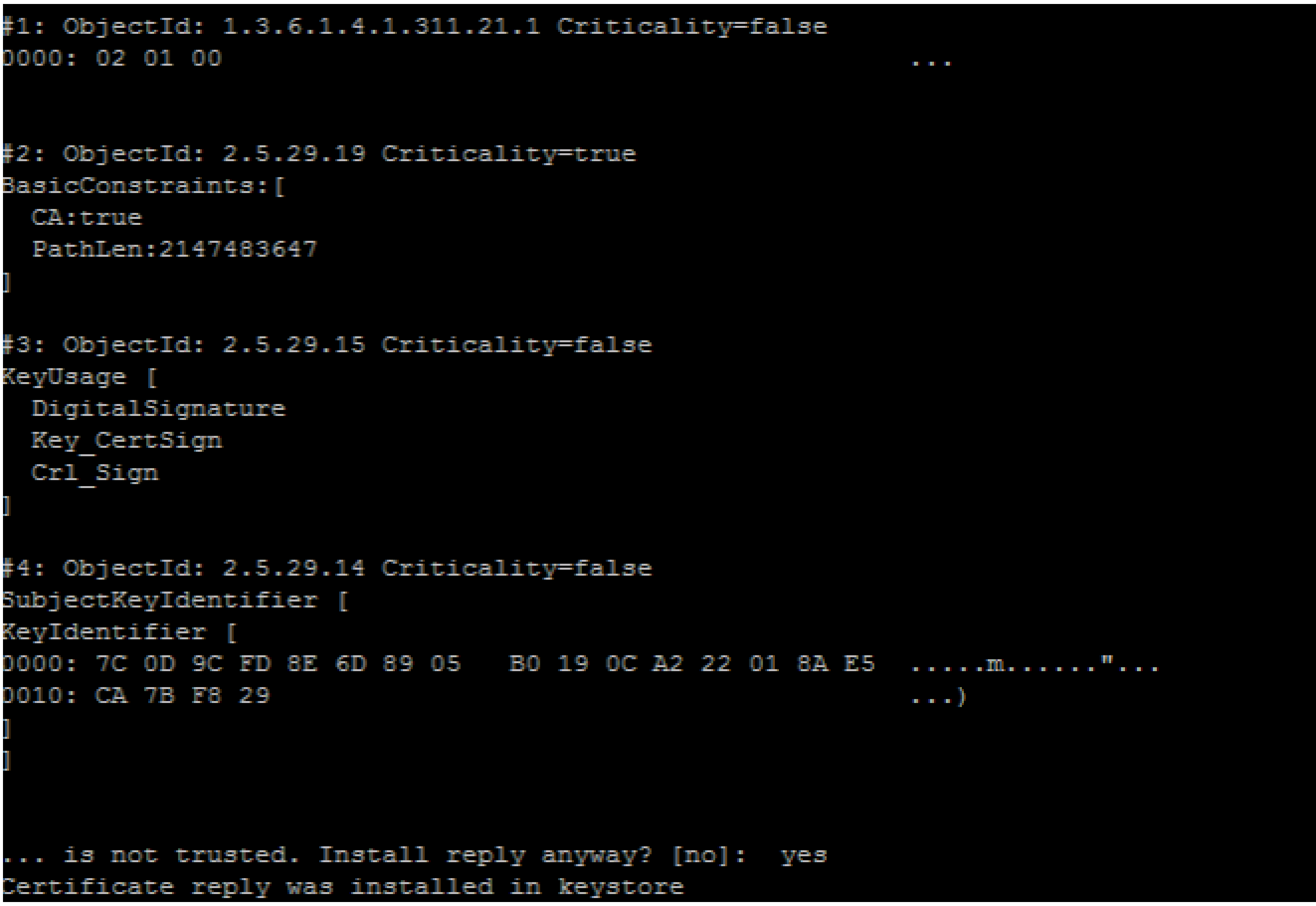
4 Import the certificate.

a Run the following console command.

```
/usr/java/latest/bin/keytool -import -alias tomcat -keystore /root/.keystore -
file /root/vdp.p7b
```

b When prompted for the keystore password, enter **changeit**.

c When prompted to trust the certificate, enter **yes** and press Enter.



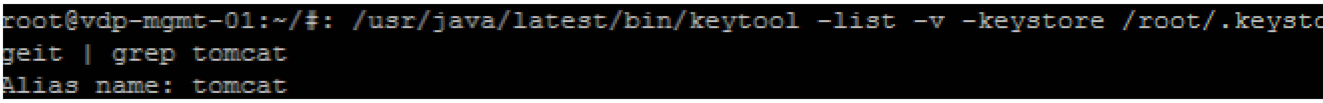
```
#1: ObjectId: 1.3.6.1.4.1.311.21.1 Criticality=false
0000: 02 01 00                                            ...


#2: ObjectId: 2.5.29.19 Criticality=true
BasicConstraints:[
  CA:true
  PathLen:2147483647
]

#3: ObjectId: 2.5.29.15 Criticality=false
KeyUsage [
  DigitalSignature
  Key_CertSign
  Crl_Sign
]

#4: ObjectId: 2.5.29.14 Criticality=false
SubjectKeyIdentifier [
KeyIdentifier [
0000: 7C 0D 9C FD 8E 6D 89 05   B0 19 0C A2 22 01 8A E5  .....m......"...
0010: CA 7B F8 29                                         ...)
]
]



... is not trusted. Install reply anyway? [no]:  yes
Certificate reply was installed in keystore
```

5 Verify that the certificate is installed successfully.

   a Run the following command.

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

   b Verify that the output contains `Alias name: tomcat`.



```
root@vdp-mgmt-01:~/#: /usr/java/latest/bin/keytool -list -v -keystore /root/.keysto
geit | grep tomcat
Alias name: tomcat
```

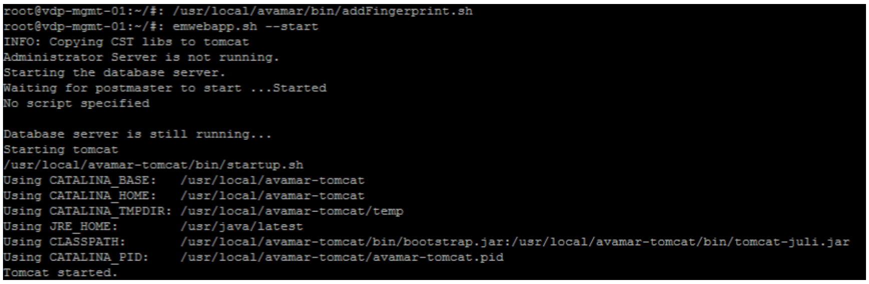
6 Run the `addFingerprint.sh` script to update the vSphere Data Protection server thumbprint displayed in the VM console welcome screen.

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

This script does not return any output.

7 Start the vSphere Data Protection services.

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



```
root@vdp-mgmt-01:~/#: /usr/local/avamar/bin/addFingerprint.sh
root@vdp-mgmt-01:~/#: emwebapp.sh --start
INFO: Copying CST libs to tomcat
Administrator Server is not running.
Starting the database server.
Waiting for postmaster to start ...Started
No script specified

Database server is still running...
Starting tomcat
/usr/local/avamar-tomcat/bin/startup.sh
Using CATALINA_BASE:   /usr/local/avamar-tomcat
Using CATALINA_HOME:   /usr/local/avamar-tomcat
Using CATALINA_TMPDIR: /usr/local/avamar-tomcat/temp
Using JRE_HOME:        /usr/java/latest
Using CLASSPATH:       /usr/local/avamar-tomcat/bin/bootstrap.jar:/usr/local/avamar-tomcat/bin/tomcat-juli.jar
Using CATALINA_PID:    /usr/local/avamar-tomcat/avamar-tomcat.pid
Tomcat started.
```

## Replace the VMware Site Recovery Manager Certificates

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

You replace certificates twice, once for each Site Recovery Manager. You start by replacing certificates on mgmt01srm01.sfo01.rainpole.local, the Site Recovery Manager in Region A.

### Table 2-5. 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 Chain | chainRoot64.cer | chainRoot64.cer |
| PKCS#12 File Name from Manual Generation | mgmt01srm01.sfo01.p12 | mgmt01srm51.lax01.p12 |
| PKCS#12 File Name from the CertGenVVD tool | mgmt01srm01.sfo01.5.p12 | mgmt01srm51.lax01.5.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** | mgmt01srm01.sfo01.rainpole.local |
   | **Region B** | mgmt01srm51.lax01.rainpole.local |

   b Log in using the following credentials.

   | Setting | 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 Locate the `chainRoot64.cer` file in `C:\manual-certs` folder.

   b Double-click the `chainRoot64.cer` file 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 the **Store Location** and click **Next**.

   e Select **Place all certificates in the following store** option, browse to select the **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 manually or by using the CertGenVVD tool.

   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 `C:\manual-certs`, select the `mgmt01srm01.sfo01.p12` or `mgmt01srm51.lax01.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 To restore the connection between the two Site Recovery Manager sites after replacing the certificates with CA-signed certificates.

- a Open a Web Browser and go to **`https://mgmt01vc01.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 **mgmt01vc01.sfo01.rainpole.local** and select **Reconfigure Pairing**.
- e Enter the address of the Platform Services Controller **`lax01psc51.lax01.rainpole.local`** on the remote site and click **Next**.
- f Select the vCenter Server instance **mgmt01vc51.lax01.rainpole.local** with which Site Recovery Manager is registered on the remote site, enter the vCenter Single Sign-On administrator user name **`administrator@vsphere.local`** and ***`vsphere_admin_password`*** password, and click **Finish**.

5 Repeat the procedure to replace the default VMware-signed certificate with this one on mgmt01srm51.lax01.rainpole.local.

## Install the CA-Signed Certificate on vSphere Replication

After you generate a PKCS#12 certificate file, replace the default VMware-signed certificate with this certificate on vSphere Replication in both regions.

You can start replacing certificates on vSphere Replication in Region A `mgmt01vrms01.sfo01.rainpole.local` first.

Table 2-6. PKCS#12 Files for vSphere Replication in Region A and Region B

| vSphere Replication FQDN | PKCS#12 File Name from Manual Generation | PKCS#12 File Name from the CertGenVVD Tool |
|---|---|---|
| mgmt01vrms01.sfo01.rainpole.local | mgmt01vrms01.sfo01.p12 | mgmt01vrms01.sfo01.5.p12 |
| mgmt01vrms51.lax01.rainpole.local | mgmt01vrms01.lax01.p12 | mgmt01vrms51.lax01.5.p12 |

## Procedure

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

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

| vSphere Replication | URL |
|---|---|
| **vSphere Replication in Region A** | https://mgmt01vrms01.sfo01.rainpole.local:5480 |
| **vSphere Replication in Region B** | https://mgmt01vrms51.lax01.rainpole.local:5480 |

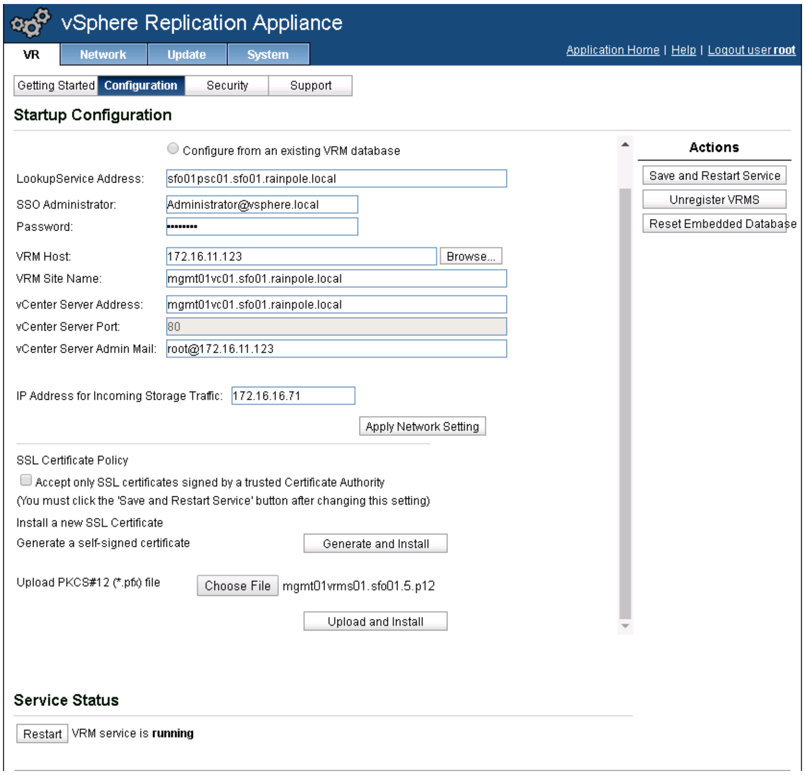
b Log in using the following credentials.

| Setting | Value |
|---|---|
| **User name** | root |
| **Password** | *vr_root_password* |

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

d Enter the vCenter Single Sign-On administrator password ***vsphere_admin_password***.

e Click **Choose File** next to **Upload PKCS#12 (*.pfx)** file and locate the PKCS#12 file that you created.



Startup Configuration

○ Configure from an existing VRM database

LookupService Address: sfo01psc01.sfo01.rainpole.local

SSO Administrator: Administrator@vsphere.local

Password: ••••••••

VRM Host: 172.16.11.123

VRM Site Name: mgmt01vc01.sfo01.rainpole.local

vCenter Server Address: mgmt01vc01.sfo01.rainpole.local

vCenter Server Port: 80

vCenter Server Admin Mail: root@172.16.11.123

IP Address for Incoming Storage Traffic: 172.16.16.71

SSL Certificate Policy

□ Accept only SSL certificates signed by a trusted Certificate Authority

(You must click the 'Save and Restart Service' button after changing this setting)

Install a new SSL Certificate

Generate a self-signed certificate

Upload PKCS#12 (*.pfx) file mgmt01vrms01.sfo01.5.p12

Service Status

VRM service is **running**

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

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

2 Reconnect the sites to resolve the connection issue.

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

a Open a Web browser and go to `https://mgmt01vc01.sfo01.rainpole.local/vsphere-client`.

b Log in using the following credentials.

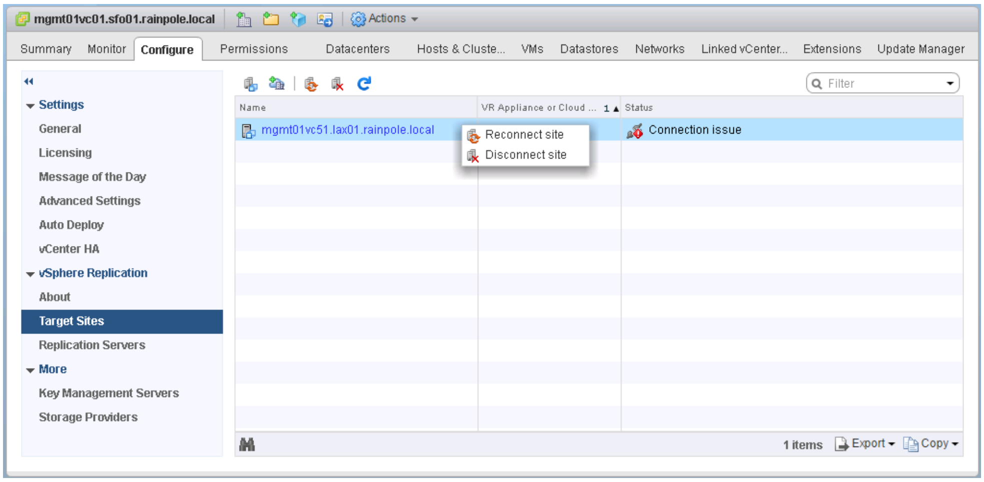
| Setting | Value |
|---|---|
| **User name** | administrator@vsphere.local |
| **Password** | *vsphere_admin_password* |

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

d Select **mgmt01vc01.sfo01.rainpole.local**, click **Manage**, and select **Target Sites**.

e Right-click **mgmt01vc51.lax01.rainpole.local** and click **Reconnect site**.

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



| Name | VR Appliance or Cloud ... | Status |
|---|---|---|
| mgmt01vc51.lax01.rainpole.local | | Connection issue |

3 Repeat the steps to install the CA-signed certificate on the other vSphere Replication instance.

## Replace Certificates of the Operations Management Components in Region B

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

## Replace the Certificate to vRealize Log Insight in Region B

After you generate the PEM certificate chain file that contains the own certificate, the signer certificate and the private key file, upload the certificate chain to vRealize Log Insight in Region B.

### Procedure

1 Log in to the vRealize Log Insight user interface.

  a Open a Web browser and go to **`https://vrli-cluster-51.lax01.rainpole.local`**.

  b Log in using the following credentials.

| Setting | Value |
|---|---|
| User name | admin |
| Password | *vrli_admin_password* |

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

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

4 On the **SSL Configuration** page, next to **New Certificate File (PEM format)** click **Choose File**, browse to the location of the `vrli.lax01.2.chain.pem` file on your computer, and click **Save**.

| Certificate Generation Option | Certificate File |
|---|---|
| Using the CertGenVVD tool | vrli.lax01.2.chain.pem |
| Manual Generation | vrli-lax01.chain.pem |

The certificate is uploaded to vRealize Log Insight.

5 Import the certificate into the Java Keystore on each vRealize Log Insight node.

  a Open an SSH session and go each of the vRealize Log Insight nodes.

| Name | Role |
|---|---|
| vrli-mstr-51.lax01.rainpole.local | Master node |
| vrli-wrkr-51.lax01.rainpole.local | Worker node 1 |
| vrli-wrkr-52.lax01.rainpole.local | Worker node 2 |

  b Log in using the following credentials.

| Setting | Value |
|---|---|
| Username | root |
| Password | *vrli_root_password* |

c. Convert the on-disk **vrli.sfo01.2.chain.pem** file into a **vrli.lax01.2.chain.crt** file.

```
openssl x509 -in /root/vrli.lax01.2.chain.pem -inform PEM -out /root/vrli.lax01.2.chain.crt
```

d. Import the vrli.sfo01.2.chain.crt into the Java Keystore:

```
cd /usr/java/default/lib/security/
../../bin/keytool -import -alias loginsight -file /root/vrli.lax01.2.chain.crt -keystore
cacerts
```

e. When prompted for a keystore password, type **changeit**.

f. When prompted to accept the certificate, type **yes**.

g. Repeat this operation on all vRealize Log Insight nodes until complete.

**6** In a Web browser, go to **`https://vrli-cluster-51.lax01.rainpole.local`**.

A warning message that the connection is not trusted appears.

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

**8** Import the certificate in your Web browser.

For example, in Google Chrome under the **HTTPS/TLS** settings click the **Manage certificates** button, and in the **Certificates** dialog box import `vrli.lax01.2.chain.pem`.

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

## Update Event Forwarding in 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.

### Procedure

**1** Copy the certificate PEM file for vRealize Log Insight in Region B to the root directory of vrli-mstr-51.lax01.rainpole.local

a. Use the `scp` command, FileZilla, or WinSCP to connect to vrli-mstr-51.lax01.rainpole.local

b. Log in using the following credentials.

| Setting | Value |
|---|---|
| user name | root |
| Password | *vrli_regionB_root_password* |

c. Navigate to the `\root` directory on vrli-mstr-51.lax01.rainpole.local

d. Copy the certificate PEM file `vrli.lax01.2.chain.pem` from your computer to the `\root` directory on the master node. Overwrite any existing file with the same name.

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

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

| Name | Role |
|---|---|
| vrli-mstr-01.sfo01.rainpole.local | Master node |
| vrli-wrkr-01.sfo01.rainpole.local | Worker node 1 |
| vrli-wrkr-02.sfo01.rainpole.local | Worker node 2 |

b Log in using the following credentials.

| Setting | Value |
|---|---|
| User name | root |
| Password | *vrli_regionA_root_password* |

c By using `scp` copy the SSL certificate from the master node of vRealize Log Insight in Region B.

```
scp root@vrli-
mstr-51.lax01.rainpole.local:/root/vrli.lax01.2.chain.pem /root/vrli.lax01.2.chain.pem
```

d When prompted to accept the certificate, type **`yes`**

e When prompted for the root password, use the following credentials.

| Setting | Value |
|---|---|
| User name | root |
| Password | *vrli_regionB_root_password* |

f Convert the `vrli.lax01.2.chain.pem` file to a `vrli.lax01.2.chain.crt` file.

```
openssl x509 -in /root/vrli.lax01.2.chain.pem -inform PEM -out /root/vrli.lax01.2.chain.crt
```

g Import the `vrli.lax01.2.chain.crt` in the Java keystore of the vRealize Log Insight node:

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

../../bin/keytool -import -alias loginsight -file /root/vrli.lax01.2.chain.crt -keystore
cacerts
```

h When prompted for a keystore password, type **`changeit`**

i When prompted to accept the certificate, type **`yes`**

j Repeat this operation on all vRealize Log Insight nodes in Region A and restart them.

3 Log in to the vRealize Log Insight user interface.

   a Open a Web browser and go to **`https://vrli-cluster-01.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.