Certificate Replacement

25 SEP 2018
VMware Validated Design 4.3
VMware Validated Design for Remote Office Branch Office 4.3

vmware®

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

https://docs.vmware.com/

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

docfeedback@vmware.com

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

Contents

About VMware Validated Design Certificate Replacement for Remote Office and Branch Office

VMware Validated Design Certificate Replacement for VMware Validated Design™ Remote Office and Branch Office provides step-by-step instructions about replacing certificates on the management components of a running remote office and branch office (ROBO) whose design extends 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.

2 Replace the certificates in the live ROBO 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.

Create and Add a Microsoft Certificate Authority Template in ROBO

1

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

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

1 Set up a Microsoft Certificate Authority template.

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

Prerequisites

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

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

Procedure

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

Setting	Value
FQDN	dc01sfo.sfo01.rainpole.local
User name	Active Directory administrator
Password	*ad_admin_password*

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

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

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

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

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

7 Click the **Extensions** tab and specify extensions information.

   a Select **Application Policies** and click **Edit**.

   b Select **Server Authentication**, click **Remove**, and click **OK**.

   c Select **Key Usage** and click **Edit**.

   d Select the **Signature is proof of origin (nonrepudiation)** check box.

   e Leave the default for all other options.

   f Click **OK**.

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

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

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

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

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

Generate MSCA-Signed Certificates for the SDDC Management Components in ROBO

2

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

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

Prerequisites

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

Procedure

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

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

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

Table 2-1. Certificate Generation Files for ROBO

SDDC Layer	Host Name or Service in Consolidated SDDC		Configuration Files
Virtual Infrastructure	vCenter Server	nyc01r01vc01.rainpole.local	nyc01r01vc01.txt
	NSX Manager	nyc01r01nsx01.rainpole.local	nyc01r01nsx01.txt
Operations Management	vRealize Log Insight	■ nyc01vrli01.rainpole.local ■ nyc01vrli01a.rainpole.local ■ nyc01vrli01b.rainpole.local ■ nyc01vrli01c.rainpole.local	vrli-nyc01.txt

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

For example, the configuration file for the ROBO vCenter Server instance must contain the following properties:

nyc01r01vc01.txt

```
[CERT]
NAME=default
ORG=default
OU=default
LOC=NYC
ST=default
CC=default
CN=nyc01r01vc01.rainpole.local
keysize=default
[SAN]
nyc01r01vc01.rainpole.local
```

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

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

8 Grant permissions to run third-party PowerShell scripts.

```
Set-ExecutionPolicy Unrestricted
```

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

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

10 Generate MSCA-signed certificates.

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

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

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

What to do next

Replace the product certificates with the certificates that the `CertGenVVD` utility has generated. See Chapter 4 Replace Certificates of the Virtual Infrastructure Components in ROBO and Chapter 5 Replace Certificates of the Operations Management Components in ROBO.

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

3

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

Prerequisites

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

Procedure

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

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

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

Table 3-1. Certificate Generation Files for ROBO

SDDC Layer	Host Name or Service in Consolidated SDDC		Configuration Files
Virtual Infrastructure	vCenter Server	nyc01r01vc01.rainpole.local	nyc01r01vc01.txt
	NSX Manager	nyc01r01nsx01.rainpole.local	nyc01r01nsx01.txt
Operations Management	vRealize Log Insight	■ nyc01vrli01.rainpole.local ■ nyc01vrli01a.rainpole.local ■ nyc01vrli01b.rainpole.local ■ nyc01vrli01c.rainpole.local	vrli-nyc01.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:

For example, the configuration file for the ROBO vCenter Server instance must contain the following properties:

nyc01r01vc01.txt

```
[CERT]
NAME=default
ORG=default
OU=default
LOC=NYC
ST=default
CC=default
CN=nyc01r01vc01.rainpole.local
keysize=default
[SAN]
nyc01r01vc01.rainpole.local
```

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

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

8 Grant permissions to run third-party PowerShell scripts.

```
Set-ExecutionPolicy Unrestricted
```

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

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

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

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

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

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

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

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

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

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

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

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

What to do next

Replace the product certificates with the certificates that the `CertGenVVD` utility has generated. See Chapter 4 Replace Certificates of the Virtual Infrastructure Components in ROBO and Chapter 5 Replace Certificates of the Operations Management Components in ROBO.

Replace Certificates of the Virtual Infrastructure Components in ROBO

4

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

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

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

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

Procedure

1 Replace the vCenter Server Certificates in ROBO

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

2 Replace the NSX Manager Certificates in ROBO

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

Replace the vCenter Server Certificates in ROBO

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

Procedure

1 Replace the Certificate of vCenter Server in ROBO

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

2 Connect NSX Manager to vCenter Server in ROBO

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

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

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

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

Replace the Certificate of vCenter Server in ROBO

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

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

vCenter Server FQDN	Files for Certificate Replacement
nyc01r01vc01.rainpole.local	■ nyc01r01vc01.key ■ nyc01r01vc01.1.cer ■ Root64.cer

Procedure

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

a Open an SSH connection to the nyc01r01vc01.rainpole.local virtual machine.

b Log in using the following credentials.

Setting	Value
User name	root
Password	*vcenter_server_root_password*

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

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

3 Copy the generated certificates to the vCenter Server Appliance.

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

   ```
   mkdir –p /root/certs
   ```

   b Copy the certificate files `nyc01r01vc01.1.cer`, `nyc01r01vc01.key`, and `Root64.cer` to the `/root/certs` folder.

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

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

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

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

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

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

vCenter Server instance	IP Address of managing Platform Services Controller
nyc01r01vc01.rainpole.local	172.18.11.61

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

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

vCenter Server	Input to the vSphere Certificate Manager Utility
nyc01r01vc01.rainpole.local	Please provide valid custom certificate for Machine SSL. File : **/root/certs/nyc01r01vc01.1.cer** Please provide valid custom key for Machine SSL. File : **/root/certs/nyc01r01vc01.key** Please provide the signing certificate of the Machine SSL certificate. File : **/root/certs/Root64.cer**

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

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

   a Open a Web browser and go to **`https://nyc01r01vc01.rainpole.local/vsphere-client`**.

   b Verify that you see the new certificate.

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

```
service vami-lighttp restart
cd /root/certs/
rm nyc01r01vc01.1.cer nyc01r01vc01.key Root64.cer
```

Connect NSX Manager to vCenter Server in ROBO

After you replace the certificates of the vCenter Server instances in ROBO, you reconnect the NSX Manager instances to the vCenter Server nodes in the region to update the certificates on NSX Manager.

Procedure

1 Log in to the NSX Manager appliance user interface.

a Open a Web browser and go to **`https://nyc01r01nsx01.rainpole.local`**.

b Log in using the following credentials.

Setting	Value
User name	admin
Password	*nsx_manager_admin_password*

2 Click **Manage vCenter Registration**.

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

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

Setting	Value
Lookup Service Host	nyc01r01vc01.rainpole.local
Lookup Service Port	443
SSO Administrator User Name	administrator@vsphere.local
Password	*vsphere_admin_password*

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

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

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

Setting	Value
vCenter Server	nyc01r01vc01.rainpole.local
vCenter User Name	svc-nsxmanager@rainpole.local
Password	*svc-nsxmanager_password*

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

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

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

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

Procedure

1 Reconnect vRealize Orchestrator to vCenter Server.

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

b Click **Start Orchestrator Client**.

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

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

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

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

f From the **vCenter Server instance** drop-down menu, select **https://nyc01r01vc01.rainpole.local:443/sdk** and click **Next**.

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

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

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

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

2 Reconnect vRealize Business to vCenter Server.

a Open a Web browser and go to **`https://nyc01vrbc01.rainpole.local:9443/dc-ui`**.

b Log in using the following credentials.

Setting	Value
User name	root
Password	*vrb_root_password*

c Click **Manage Private Cloud Connections**, select **vCenter Server**, select the **nyc01r01vc01.rainpole.local** entry, and click the **Edit** icon.

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

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

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

3 Recreate the vSphere endpoint in vRealize Automation.

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

b Log in using the following credentials.

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

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

d Point to **nyc01r01vc01.rainpole.local** and click **Edit**.

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

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

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

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

Procedure

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

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

b Log in using the following credentials.

Setting	Value
User name	admin
Password	*vrops_admin_password*

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

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

4 Select the row that contains `CN=nyc01r01vc01.rainpole.local` and click the **Delete** icon.

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

6 Reconnect each vCenter Adapter.

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

   b In the **Manage Solutions** dialog box, select **vCenter Adapter - nyc01r01vc01**, click **Test Connection**, accept the new certificate of vCenter Server, and click **Save Settings**.

7 Reconnect the VMware vSAN adapter for the management cluster.

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

   b In the **Manage Solutions** dialog box, select **vSAN Adapter - nyc01r01vc01**, click **Test Connection**, accept the new certificate of the Management vCenter Server, and click **Save Settings**.

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

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

   b In the **Manage Solutions** dialog box, select **Storage Devices Adapter - nyc01r01vc01**, click **Test Connection**, accept the new certificate of vCenter Server, and click **Save Settings**.

Replace the NSX Manager Certificates in ROBO

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

Procedure

1 Replace the Certificate of NSX Manager in ROBO

2 Connect NSX Manager to vCenter Server in ROBO

3 Reconnect NSX Manager in ROBO to vRealize Operations Manager

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

Replace the Certificate of NSX Manager in ROBO

After you replace the certificate of vCenter Server instance, replace the expiring certificates for the NSX Manager instances.

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

Table 4-2. Certificate-Related Files on the NSX Manager Instance in ROBO SDDC

NSX Manager FQDN	Certificate Filename
nyc01r01nsx01.rainpole.local	nyc01r01nsx01.4.p12

Procedure

1 Log in to the NSX Manager appliance user interface.

   a Open a Web browser and go to **`https://nyc01r01nsx01.rainpole.local`**.

   b Log in using the following credentials.

Setting	Value
User name	admin
Password	*nsx_manager_admin_password*

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

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

4 Browse to the certificate chain file `nyc01r01nsx01.4.p12`, provide the keystore password or passphrase, and click **Import**.

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

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

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

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

Connect NSX Manager to vCenter Server in ROBO

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

Procedure

1 Log in to the NSX Manager appliance user interface.

   a Open a Web browser and go to **`https://nyc01r01nsx01.rainpole.local`**.

   b Log in using the following credentials.

Setting	Value
User name	admin
Password	*nsx_manager_admin_password*

2 Click **Manage vCenter Registration**.

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

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

Setting	Value
Lookup Service Host	nyc01r01vc01.rainpole.local
Lookup Service Port	443

Setting	Value
SSO Administrator User Name	administrator@vsphere.local
Password	*vsphere_admin_password*

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

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

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

Setting	Value
vCenter Server	nyc01r01vc01.rainpole.local
vCenter User Name	svc-nsxmanager@rainpole.local
Password	*svc-nsxmanager_password*

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

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

Reconnect NSX Manager in ROBO to vRealize Operations Manager

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

Procedure

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

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

   b Log in using the following credentials.

Setting	Value
User name	admin
Password	*vrops_admin_password*

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

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

4 Delete the certificates with the following CNs.

   - `CN=nyc01r01nsx01.rainpole.local`

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

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

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

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

Replace Certificates of the Operations Management Components in ROBO

5

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 Log Insight Certificate in ROBO

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

2 Update the SSL Certificate for Event Forwarding to Region A and Region B

After you replace the certificate of vRealize Log Insight in ROBO, you update log forwarding from vRealize Log Insight in ROBO to vRealize Log Insight in Region A and Region B. Log forwarding in this validated design uses SSL connection to push ROBO log data back to Region A and Region B. You skip this procedure if the root certificate (Certificate Authority) in vRealize Log Insight in ROBO is not replaced.

Replace vRealize Log Insight Certificate in ROBO

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

Procedure

1 Log in to the vRealize Log Insight user interface.

a Open a Web browser and go to **`https://nyc01vrli01.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.nyc01.2.chain.pem`

The certificate is uploaded to vRealize Log Insight.

5 Open a Web browser and go to **`https://nyc01vrli01.rainpole.local`**

A warning message that the connection is not trusted appears.

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

Update the SSL Certificate for Event Forwarding to Region A and Region B

After you replace the certificate of vRealize Log Insight in ROBO, you update log forwarding from vRealize Log Insight in ROBO to vRealize Log Insight in Region A and Region B. Log forwarding in this validated design uses SSL connection to push ROBO log data back to Region A and Region B. You skip this procedure if the root certificate (Certificate Authority) in vRealize Log Insight in ROBO is not replaced.

Procedure

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

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

Name	Role
lax01vrli01a.lax01.rainpole.local	Master node
lax01vrli01b.lax01.rainpole.local	Worker node 1
lax01vrli01c.lax01.rainpole.local	Worker node 2
sfo01vrli01a.sfo01.rainpole.local	Master node
sfo01vrli01b.sfo01.rainpole.local	Worker node 1
sfo01vrli01c.sfo01.rainpole.local	Worker node 2

b Log in using the following credentials.

Setting	Value
User Name	root
Password	*vrli_regionB_root_password*

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

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

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

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

```
echo "" | openssl s_client -showcerts -servername nyc01vrli01a.rainpole.local -connect
nyc01vrli01a.rainpole.local:443 -prexit 2>/dev/null | sed -n -e '/BEGIN\ CERTIFICATE/,/END\
CERTIFICATE/ p' > cert.pem
csplit -f individual- cert.pem '/-----BEGIN CERTIFICATE-----/' '{*}'
root_cert=$(ls individual-* | sort -n -t- | tail -1)
cp -f -- "$root_cert" root.crt
```

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

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

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

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

f Reboot the vRealize Log Insight node.

```
reboot
```

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

3 Log in to vRealize Log Insight user interface.

a Open a Web browser and go to **`https://nyc01vrli01.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 **NYC01 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.

9 Repeat the above with **NYC01 to LAX01**