Certificate Replacement

VMware Validated Design for Remote Office and Branch Office 4.0

EN-002516-00

vmware®

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

http://www.vmware.com/support/

The VMware Web site also provides the latest product updates.

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 in the ROBO 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:

CA Role	AD Server
Root CA	dc01rpl.rainpole.local
Intermediate CA	dc03rpl.rainpole.local

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 dc03rpl.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 dc03rpl.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 exists, go to Step 11.
5. In the Certificate Template Console, under **Template Display Name**, right-click **Web Server** and click **Duplicate Template**.
6. In the Duplicate Template window, leave **Windows Server 2003 Enterprise** selected for backward compatibility and click **OK**.
7. In the Properties of New Template dialog box, click the **General** tab.
8. In the **Template display name** text box, enter **`VMware`** as the name of the new template.

9 Click the **Extensions** tab and specify the 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 CA-Signed Certificates for the SDDC Management Components in ROBO

2

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 dc03rpl.rainpole.local, make sure the Windows host that you use to connect to the data center is a part of the 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=NYC
   ST=NY
   CC=US
   CN=VMware_VVD
   keysize=2048
   ```

5. Verify that only the `c:\CertGenVVD-`*`version`*`\ConfigFiles` folder contains only following files.
   - nyc01esx01.txt
   - nyc01esx02.txt
   - nyc01esx03.txt
   - nyc01esx04.txt
   - nyc01vc01.txt
   - nyc01nsxm01.txt
   - nyc01vdp01.txt
   - nyc01vrli01.txt

6 If any of the files does not exist, create it so that you can generate the required certificates for the ROBO.

a Create a new file in a text editor, add the following properties are configured and save it as `nyc01esx01.txt`.

nyc01esx01.txt

```
[CERT]
NAME=default
ORG=default
OU=default
LOC=default
ST=default
CC=default
CN=nyc01esx01.rainpole.local
keysize=default
[SAN]
nyc01esx01
nyc01esx01.rainpole.local
```

b Repeat the steps for each of the missing configuration files.

nyc01esx02.txt

```
[CERT]
NAME=default
ORG=default
OU=default
LOC=default
ST=default
CC=default
CN=nyc01esx02.rainpole.local
keysize=default
[SAN]
nyc01esx02
nyc01esx02.rainpole.local
```

nyc01esx03.txt

```
[CERT]
NAME=default
ORG=default
OU=default
LOC=default
ST=default
CC=default
CN=nyc01esx03.rainpole.local
keysize=default
[SAN]
nyc01esx03
nyc01esx03.rainpole.local
```

nyc01esx04.txt

```
[CERT]
NAME=default
ORG=default
OU=default
LOC=default
ST=default
CC=default
CN=nyc01esx04.rainpole.local
keysize=default
[SAN]
nyc01esx04
nyc01esx04.rainpole.local
```

nyc01vc01.txt

```
[CERT]
NAME=default
ORG=default
OU=default
LOC=default
ST=default
CC=default
CN=nyc01vc01.rainpole.local
keysize=default
[SAN]
nyc01vc01
nyc01vc01.rainpole.local
```

nyc01nsxm01.txt

```
[CERT]
NAME=default
ORG=default
OU=default
LOC=default
ST=default
CC=default
CN=nyc01nsxm01.rainpole.local
keysize=default
[SAN]
nyc01nsxm01
nyc01nsxm01.rainpole.local
```

nyc01vdp01.txt

```
[CERT]
NAME=default
ORG=default
OU=default
LOC=default
ST=default
CC=default
CN=nyc01vpd01.rainpole.local
keysize=default
[SAN]
nyc01vpd01
nyc01vpd01.rainpole.local
```

nyc01vrli01.txt

```
[CERT]
NAME=default
ORG=default
OU=default
LOC=default
ST=default
CC=default
CN=nyc01vrli01-cluster01.rainpole.local
keysize=default
[SAN]
```

nyc01vrli01.txt

```
nyc01vrli01-cluster01
nyc01vrli01
nyc01vrli02
nyc01vrli03
nyc01vrli01-cluster01.rainpole.local
nyc01vrli01.rainpole.local
nyc01vrli02.rainpole.local
nyc01vrli03.rainpole.local
```

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

Replace Certificates of the Management Products in ROBO 3

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

This chapter includes the following topics:

Replace the vCenter Server Certificate in ROBO

Replace the certificates on the ROBO vCenter Server and reconnect it to the other management components in the remote office to update the new certificate on these components.

Replace the vCenter Server Certificate in ROBO

You replace the machine SSL certificate on the vCenter Server instance in the ROBO with a custom certificate that is signed by the certificate authority (CA).

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

vSphere vCenter Server	Certificate File Name
nyc01vc01.rainpole.local	■ nyc01vc01.key ■ nyc01vc01.3.pem (CertGenVVD) ■ chainRoot64.cer

Procedure

1 Disconnect the NSX Manager from the embedded Platform Services Controller on the vCenter Server instance in the ROBO temporarily.

   a Open a Web Browser and go to **`https://nyc01nsxm01.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**.

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

a Open an SSH connection to nyc01vc01.rainpole.local.

b Log in using the following credentials.

Setting	Value
Username	root
Password	*vc_root_password*

3 Change the vCenter Server command shell to the Bash shell so that you can use secure copy `scp` connections.

```
shell
chsh –s /bin/bash root
```

4 Copy the generated certificate files `nyc01vc01.key`, `nyc01vc01.3.pem` and `chainRoot64.cer` from the Windows host to the `/tmp/ssl` directory on the vCenter Server Appliance.

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

5 Rename `nyc01vc01.3.pem` to `nyc01vc01.1.chain.cer`.

6 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
```

7 Replace the certificate on vCenter Server.

a Start the vSphere Certificate Manager utility on vCenter Server.

```
/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/nyc01vc01.1.chain.cer`**.

f When prompted for the custom key, enter **`/tmp/ssl/nyc01vc01.key.`**

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

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

i Wait until the vCenter Server services restart successfully.

8 Validate that the new certificate has been installed successfully.

a Open a Web Browser and go to **`https://nyc01vc01.rainpole.local`**.

b Verify that the Web browser shows the new certificate.

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

a Go back to the nyc01vc01.rainpole.local SSH terminal.

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

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

10 Switch the command shell back to the appliance shell.

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

11 If you plan to keep the certificate of the NSX Manager unchanged after you replace the certificate of vCenter Server, reconnect the NSX Manager instance to vCenter Server.

a Open a Web Browser and go to **`https://nyc01nsxm01.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 Under Lookup Service, click **Edit**.

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

Setting	Value
Lookup Service IP	nyc01vc01.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 **Edit**.

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

Setting	Value
vCenter Server	nyc01vc01.rainpole.local
vCenter User name	svc-nsxmanager@rainpole.local
Password	*svc-nsxmanager_password*

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

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

Reconnect vSphere Data Protection to vCenter Server After Certificate Replacement in ROBO

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

Procedure

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

a Open a Web browser and go to **`https://nyc01vc01.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 **nyc01vdp01** from the **VDP Appliance** drop-down menu and click **Connect**.

Update the vCenter Server Certificate on the Cloud Management Platform in ROBO

After you replace the certificates on the vCenter Server instance in the ROBO, 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://nyc01vc01.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 vCenter Server.

a Open a Web browser and go to **`https://nyc01buc01.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 **nyc01vc01.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 Reconnect 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 **nyc01vc01 admin** and click **Edit**.

d On the Credentials page, enter the password for the vRealize Automation credential for the administrator of nyc01vc01.rainpole.local, and click **Save**.

Setting	Value
Name	nyc01vc01 admin
Description	Administrator of nyc01vc01.rainpole.local
User Name	svc-vra@rainpole.local
Password	***`svc_vra_password`***

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

f Have your mouse over **nyc01vc01.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 Certificate for ROBO on vRealize Operations Manager

After you change the certificate of the vCenter Server instance in the ROBO, update the certificate on the connected vRealize Operations Manager in the hub by reconnecting the vCenter Adapter instance for the ROBO vCenter Server.

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=nyc01vc01.rainpole.local` and click the **Delete** icon.

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 **nyc01vc01**, click **Test Connection**, accept the new certificate of the ROBO vCenter Server and click **Save Settings**.

Replace the NSX Manager Certificate in ROBO

After you replace the certificate of the vCenter Server instance in the ROBO, replace the certificate of NSX Manager.

Table 3-2. Certificate-Related Files on the NSX Manager Instance in ROBO

NSX Manager FQDN	Certificate File Name	Replacement Time
nyc01nsxm01.rainpole.local	nyc01nsxm01.4.p12 from the CertGenVVD tool	After you replace the certificate on the vSphere 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 **`https://nyc01nsxm01.rainpole.local`**.

   b Log in using the following credentials

Setting	Value
User name	admin
Password	*nsx_manager_admin_password*

2 Click the **Manage Appliance Settings** button.

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

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

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

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

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

6 Re-register the NSX Manager to the ROBO vCenter Server.

a Open a Web browser and go to the NSX Manager Web interface **`https://nyc01nsxm01.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 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	nyc01vc01.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 ROBO Cluster
vCenter Server	nyc01vc01.rainpole.local
vCenter User Name	svc-nsxmanager@rainpole.local
Password	*svc-nsxmanager_password*

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

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

7 Reconnect the NSX Manager instance 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=nyc01nsxm01.rainpole.local` and click the **Delete** icon.

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

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

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

h Click the nyc01nsxm01 adapter instance, click **Test Connection**, accept the new certificate and click **Save settings**.

8 Restart vROps remote collector nodes to update the nsx certification changes.

a Open a Web browser and go to **https://nyc01vc01.rainpole.local**.

b Log in using the following credentials.

Setting	Value
vCenter User Name	*vc_admin_user_name*
Password	*vc_admin_password*

c From Home select Hosts and Clusters

d Expands **NYC01-MGMT** computer resources

e Right click on **nyc01rmtcol01** and select **Power** -> **Guest OS restart**

f Right click on **nyc01rmtcol02** and select **Power** -> **Guest OS restart**

Install a CertGenVVD-Generated Certificate on vSphere Data Protection in ROBO

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 the ROBO with the certificate that is generated by `CertGenVVD`.

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 a SSH connection to the virtual machine nyc01vdp01.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
```

Replace the Certificate of vRealize Log Insight in ROBO

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 the ROBO.

Procedure

1 Log in to the vRealize Log Insight user interface.

a Open a Web browser and go to **`https://nyc01vrli01-cluster01.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.nyc01.2.chain.pem` file on your computer, and click **Save**.

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
nyc01vrli01.rainpole.local	Master node
nyc01vrli02.rainpole.local	Worker node 1
nyc01vrli03.rainpole.local	Worker node 2

b Log in using the following credentials.

Setting	Value
User name	root
Password	*vrli_root_password*

c Convert the on-disk `vrli.nyc01.2.chain.pem` file in to a `vrli.nyc01.2.chain.crt` file.

```
openssl x509 –in /root/vrli.nyc01.2.chain.pem –inform PEM –
out /root/vrli.nyc01.2.chain.crt
```

d Import the `vrli.nyc01.2.chain.crt` in to the Java keystore.

```
cd /usr/java/default/lib/security/
../../bin/keytool –import –alias loginsight –file /root/vrli.nyc01.2.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://nyc01vrli01-cluster01.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.nyc01.2.chain.pem`.

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