Replacing vCenter Server 4.0 Certificates

VMware vSphere 4.0

Certificates are automatically generated when you install vCenter Server and ESX/ESXi. These default certificates are not signed by a commercial certificate authority (CA) and may not provide strong security. You can replace default vCenter Server and ESX/ESXi certificates with certificates signed by a commercial CA.

This Technical Note includes the following topics:

NOTE If you have replaced the default vCenter Server or ESX/ESXi host certificates with certificates signed by a commercial CA, you do not need to perform the tasks in this document. You can configure server-certificate verification settings using the vSphere Client. See the *Basic System Administration Guide* for more information.

About vCenter Server Certificates

VMware products use standard X.509 version 3 (X.509v3) certificates to encrypt session information sent over Secure Socket Layer (SSL) protocol connections between components.

For example, communications between a vCenter Server system and each ESX/ESXi host that it manages are encrypted, and some features, such as VMware Fault Tolerance, require the certificate verification provided by SSL. The authenticity of the certificate presented during the SSL handshake phase (prior to encryption), is verified by the client, which protects against "man-in-the-middle" attacks.

In new installations of vCenter Server 4.0, host certificate verification is enabled by default. Do not disable certificate verification. If a host's certificate cannot be verified for some reason, verification can be temporarily disabled to help determine the cause of the problem.

For environments that require strong security, perform the following tasks:

- Install certificates signed by a commercial Certificate Authority (CA) on all vCenter Server systems and ESX/ESXi hosts.
- Upgrade existing VirtualCenter Server and Virtual Infrastructure Client deployments to vCenter Server 4.0 and vSphere Client 4.0.
- Enable certificate verification on all vSphere Clients and the vCenter Server system.

When you replace default vCenter Server certificates, the certificates you obtain for your servers must meet the specifications described in "Certificate Specifications" on page 2.

Pre-Trusting Server Certificates

Certificates signed by a commercial certificate authority, such as Entrust or VeriSign, are pre-trusted on the Windows operating system. However, if you replace a certificate with one signed by your own local root CA, or if you plan to continue using a default certificate, you must pre-trust the certificate by importing it into the local certificate store for each vSphere Client instance.

You must pre-trust all certificates that are signed by your own local root CA, unless you pre-trust the parent certificate, the root CA's own certificate. You will also have to pre-trust any valid default certificates that you will continue to use on ESX/ESXi and vCenter Server.

Certificate Specifications

VMware products use standard X.509 version 3 (X.509v3) certificates. If you replace the default certificate, you must replace it with a signed certificate that conforms to the Privacy Enhanced Mail (PEM), a key format that stores data in a Base-64 encoded Distinguished Encoding Rules (DER) format.

The key used to sign the certificates must be a standard RSA key with an encryption length ranging from 512 to 2048 bits. The recommended length is 1024 bits.

The key and certificate names for ESX/ESXi and vCenter Server are shown in Table 1. The syntax examples create certificates and keys in the required format. Personal Information Exchange Format (PFX) enables transfer of certificates and their private keys from one computer to another or to removable media. The Microsoft Windows CryptoAPI uses the PFX format (also known as PKCS #12).

Table 1. Names of Key and Certificate Files

Server	Private Key	Certificate	PFX
ESX/ESXi 4.0	`rui.key`	`rui.crt`	
vCenter Server 4.0	`rui.key`	`rui.crt`	`rui.pfx`

Certificate Locations

The directory locations of the keys and certificates are shown in Table 2.

Table 2. Default Locations for ESX/ESXi and vCenter Server Certificates

Server	Directory Location for Certificate
ESX/ESXi 4.0	`/etc/vmware/ssl/`
vCenter Server 4.0	`C:\Users\All Users\VMware\VMware VirtualCenter\SSL\` For Windows Server 2008, `C:\ProgramData\VMware\VMware VirtualCenter\SSL\`

The process for generating keys and certificates described in this document is the same for Windows or Linux, although the precise syntax is platform specific.

Replacing Default Server Certificates with Certificates Signed by a Commercial CA

When you replace default server certificates in a production environment, deploy new certificates in stages, rather than all at the same time. Be sure you understand the full scope of the process as it applies to your specific environment before taking any actions.

NOTE Allow time to obtain certificates from a commercial CA before starting this process.

To replace a server certificate

1 "Edit the OpenSSL Configuration File" on page 3

2 "Create Certificate-Signing Requests for vCenter Server and ESX/ESXi" on page 4

3 "Copy the Replacement Certificate to vCenter Server or ESX/ESXi" on page 5

4 "Load Replacement Certificates into Memory" on page 5

5 "Enable Certificate Verification and Reconnect Each System" on page 5

Some details might not apply to every deployment.

Edit the OpenSSL Configuration File

VMware products implement the OpenSSL libraries and toolkits to generate the default certificates that are created during installation process. You can use OpenSSL to create certificate-signing requests (CSR). You can download OpenSSL from http://www.openssl.org.

NOTE VMware strongly recommends that you create CSRs and other security-related artifacts on trusted, air-gapped physical hardware over which you have complete control. VMware also recommends using a hardware RNG (random-number generator) to efficiently and quickly generate random numbers that have the appropriate characteristics (sufficient degree of entropy, for example) for cryptographic purposes.

The examples shown in this document are run from a Windows host machine and assume that the OpenSSL home directory is `c:\openssl\bin`.

The default OpenSSL installation includes a configuration file, `openssl.cfg`, located in the `\bin` directory. You can preconfigure many settings in this configuration file, and you can overwrite many default values by passing values to the command line. The syntax examples in the remainder of this document assume the following settings in the OpenSSL configuration file.

- The `$dir` variable is set to the local (.) directory path.
- The [req] section of the `openssl.cfg` has a `default_keyfile` variable set to `$dir/rui.key`.
- The [CA] section references a `CA_default` section.
- The [CA_default] section references a `private_key` named `myroot.key`.

To create or modify OpenSSL configuration file for your environment

1 Navigate to the OpenSSL directory.

2 Create backup of the original OpenSSL configuration file (`openssl.cfg`) to a safe location, in case you have problems and must restore your system to its previous state.

3 Edit the openssl.cfg, specifying the details appropriate for your environment. For example:

NOTE Modify all entries so that they are specific to your environment. Providing the commonName is mandatory.

```
[ req ]
default_bits            = 1024
default_keyfile         = rui.key
distinguished_name      = req_distinguished_name
#Don't encrypt the key
encrypt_key             = no
prompt                  = no
string_mask = nombstr

[ req_distinguished_name ]
countryName             = US
stateOrProvinceName     = California
localityName            = Palo Alto
0.organizationName      = VMware, Inc.
emailAddress            = ssl-certificates@vmware.com
commonName              = <NAME_OF_SERVER_THAT_WILL_HAVE_CERTIFICATE>
```

Create Certificate-Signing Requests for vCenter Server and ESX/ESXi

You must generate a certificate-signing requests (CSR) for each system that requires a replacement certificate.

You have the option of pre-trusting the default certificates for ESX/ESXi hosts on the Windows client, because these certificates are valid.

Before you begin this task, edit your OpenSSL configuration file (openssl.cfg) to suit your environment as described in "Edit the OpenSSL Configuration File" on page 3.

Refer to the OpenSSL documentation at http://www.openssl.org for more information about OpenSSL commands and options.

To create certificate-signing requests

1 Generate the RSA key for the vCenter Server system or ESX/ESXi host and the CSR. For example:

```
openssl req -new -nodes -out mycsr.csr -config openssl.cfg
```

2 When prompted, specify the fully qualified host name as the system's commonName.

The system generates the mycsr.csr file and the rui.key file.

3 Back up the original rui.key file to a safe location.

4 Send the certificate request to the commercial certificate authority of your choice (for example, Entrust or VeriSign) and await the return of the signed certificate.

Create the PFX File

In addition, you must create a PFX-formatted certificate file specific for Windows.

The rui.pfx file is a concatenation of the system's certificate and private key, exported in the PFX format. You should copy this file to the subdirectory on the vCenter Server system specified in Table 2, "Default Locations for ESX/ESXi and vCenter Server Certificates," on page 2.

To create the PFX file

Export the certificate and the key file together to PFX format using OpenSSL. For example:

```
openssl pkcs12 -export -in rui.crt -inkey rui.key -name rui -passout pass:testpassword -out
rui.pfx
```

Copy the Replacement Certificate to vCenter Server or ESX/ESXi

1 Before you replace a certificate or key on any system, back up the original, default certificate, key, and PFX file to a safe location, in case you have problems and must restore your system to its previous state.

2 Copy the new signed certificate, key, and PFX file (`rui.crt`, `rui.key, rui.pfx`) to the location specified in Table 2, "Default Locations for ESX/ESXi and vCenter Server Certificates," on page 2.

For vCenter Servers only:

1 Stop the vCenter Server service.

```
net stop vpxd
```

2 Reset the password of the vCenter Server database by entering the following command in the command line interface on the system where vCenter Server is installed.

```
cd <root directory of vCenter Server> vpxd -p
```

The password is randomly generated.

3 When prompted for your new password, enter your existing database password.

4 Start the vCenter Server service.

```
net start vpxd
```

Load Replacement Certificates into Memory

After you copy the replacement certificates to the vCenter Server system or ESX/ESXi host, you must load the new certificates into memory.

To load the certificates into memory

1 Disconnect each ESX/ESXi host from the pool that vCenter Server manages.

2 If necessary, upgrade VirtualCenter Server instances to vCenter Server 4.0.

3 If necessary, upgrade all Virtual Infrastructure Client instances to vSphere Client 4.0.

4 Restart all affected systems to load the new certificates into memory.

Enable Certificate Verification and Reconnect Each System

If you are upgrading from a previous version of VirtualCenter Server, you must enable certificate verification after you replace the default certificates. In new installations of vCenter Server 4.0, certificate verification is enabled by default.

To enable certificate verification

1 In the vSphere Client, select **Administration > vCenter Server Settings**.

2 Select **SSL Settings** and review the list of ESX/ESXi host thumbprints.

Thumbprints listed in the SSL Settings dialog box must correspond to the thumbprints on the ESX/ESXi host. To obtain the thumbprint, enter the following command on the host:

```
openssl x509 –in /etc/vmware/ssl/rui.crt –fingerprint –sha1 –noout
```

3 If the resulting thumbprint at the command line matches that listed in the vSphere Client SSL Settings dialog box, click **Verified**.

4 Select the **Check host certificates** check box.

5 Click **OK**.

6 Using the vSphere Client, connect to the vCenter Server system.

7 Reconnect all hosts to vCenter Server.

If you replaced the vCenter Server certificate, you must reenter credentials for each host.

Replacing Default Server Certificates with Self-Signed Certificates

VMware recommends that you replace default certificates with those signed by a commercial certificate authority. If you choose to replace vCenter Server certificates with self-signed certificates, perform the following tasks in the order listed.

To replace default certificates with self-signed certificates

1. Read "Using OpenSSL to Create Security Artifacts" on page 6.
2. "Edit the OpenSSL Configuration File" on page 3.
3. "Create a Local Root CA" on page 6.
4. "Create Certificate-Signing Requests for vCenter Server and ESX/ESXi" on page 4
5. "Create Self-Signed Certificates" on page 7
6. "Copy the Replacement Certificate to vCenter Server or ESX/ESXi" on page 5
7. "Load Replacement Certificates into Memory" on page 5
8. "Enable Certificate Verification and Reconnect Each System" on page 5
9. "Install Certificates on Windows Client Hosts" on page 7

Some details might not apply to every deployment.

Using OpenSSL to Create Security Artifacts

VMware products implement the OpenSSL libraries and toolkits to generate the default certificates created during installation process. VMware strongly recommends that you install certificates signed by a commercial Certificate Authority (CA). However, you have the option to use OpenSSL to create new keys and certificates and a root CA (if appropriate). You can download OpenSSL from http://www.openssl.org.

If you intend o create your own root CA and keys, properly secure the host system used to create local root CA certificate and its private key. The private key associated with the root CA must remain private.

NOTE VMware strongly recommends creating keys, CSRs, and other security-related artifacts on trusted, air-gapped physical hardware over which you have complete control. VMware also recommends using a hardware RNG (random-number generator) to efficiently and quickly generate random numbers that have the appropriate characteristics (sufficient degree of entropy, for example) for cryptographic purposes.

The examples shown are run from a Windows host machine and assume that the OpenSSL home directory is: `c:\openssl\bin`.

Inside the `openssl\bin` directory, you can create subdirectories to contain your keys, certificates, and other files. The syntax examples shown in the following subsections assume a flat directory structure.

NOTE The following instructions assume that a single self-signed root CA is used to sign all certificate signing requests (CSRs).

Create a Local Root CA

To replace the default certificates with certificates signed by your own local CA, you must create a root CA. The root CA's certificate must then be installed in any client systems that will connect to the managed hosts. Assuming you use the same root CA key to sign all the CSRs, you will have only one root CA certificate to install in the Windows clients.

The following example creates a new root CA and an RSA key:

```
C:\OpenSSL\bin>openssl req –new –x509 –extensions v3_ca –keyout myroot.key –out myroot.crt
–days 3650 –config openssl.cfg
```

Create Self-Signed Certificates

If you choose to install self-signed certificates, you can create them using OpenSSL.

Before you begin this task, edit your OpenSSL configuration file (`openssl.cfg`) to suit your environment as described in "Edit the OpenSSL Configuration File" on page 3.

To create a self-signed certificate

1. Create the self-signed certificate (`rui.crt`) by running the following command:

   ```
   openssl ca -out rui.crt -config openssl.cfg -infiles mycsr.csr
   ```

   NOTE This command assumes that the `openssl.cfg` file is in the same folder as where the certificate is generated. If the certificate is in another folder, supply the full patch with the `openssl.cfg` file name.

   The system generates the `rui.crt` file.

2. Copy the generated self-signed certificate (`rui.crt`) to vCenter Server or ESX/ESXi as described in "Copy the Replacement Certificate to vCenter Server or ESX/ESXi" on page 5.

Install Certificates on Windows Client Hosts

The vSphere Client uses the local Windows certificate store during the server-certificate verification process. After you have valid certificates on all servers, you can add the certificates and root CAs necessary to verify the server certificates.

NOTE If you obtained certificates signed by a commercial CA, you do not need to perform this task.

If you created your own root CA certificate and used it to sign server certificates, you must import the root certificate into each vSphere Client where you will enable server-certificate verification. The vCenter Server system is a client of the ESX/ESXi to which it connects, so you must import the new certificate into the vCenter Server system. The root CA (or other server certificates) must be imported into the certificate store associated with the proper Windows account for the type of vCenter Server system (server or client), as follows:

- For the vCenter Server host, you must install the root CA (or certificate) as Administrator, since the certificate must be available to the Windows service.
- For vSphere Client systems, log in to the Windows host system using the regular user credentials that you use to connect to the vCenter Server system or ESX/ESXi systems.

Before you begin this task, use the security-conscious mechanism of your choice (for example, nonwritable media or a known-trusted server) and make the signing certificate (`rui.crt` or equivalent) available for import to the client hosts and the vCenter Server host.

NOTE The `.crt` file comprises the digital signature plus the public key only—not the private key.

To install certificates on Windows client hosts

1. Launch the Certificates Microsoft Management Console (MMC) snap-in.
2. Navigate to the **%SystemRoot%\System32\** directory on the Windows system and find the certmgr.msc file.
3. Right-click the `certmgr.msc` file.

   If you are importing the certificate to the vCenter Server host system:

   a. Select **Run as** from the pop-up menu.

   b. Enter the Administrator credentials specific to the Windows local Administrator group in the dialog.
4. Click **OK** to continue.
5. Install the local root CA certificate used to sign server certificates into the Windows certificate store.

6 On the Certificates pane, click the **Trusted Root Certification Authorities** folder.

7 From the Action menu, select **All Tasks** > **Import** to launch the Certificate Import Wizard.

The Certificate Import Wizard lets you navigate to the location of the certificate file and import it into the Trusted Root Certification Authorities folder.

8 Clcik **Next**.

9 Click **Browse** in the File to import window and select the local root CA certificate.

10 Click **Next**.

11 Select the **Place all certificates in the following store** radio button in the Certificate Store window.

12 Click **Browse** and select the **Show physical stores** check box.

13 Select **Local Computer** under the Trusted Root Certification Authorities.

14 Click **OK** and click **Next**.

15 Click **Finish**.

The Certificate Import Wizard displays the following message:

```
The import was successful.
```

If you created your own local root CA and used it to sign all server certificates, you need only import the local root CA certificate. If your ESX/ESXi hosts continue using the default certificates, you must also import those certificates into the Trusted Root Certification Authorities folder.

Related Publications

For more information about using certificates with ESX/ESXi and vCenter Server systems, see the VMware vSphere 4.0 documentation for ESX/ESXi 4.0 and vCenter Server 4.0, including the *ESX Configuration Guide*, *ESXi Configuration Guide*, and the *vSphere Basic System Administration* guide.

Refer to the Knowledge Base (KB) article *Default vCenter Server certificates prevent some client applications from connecting to vSphere 4.0 systems* (KB 1009407) for information about using legacy client applications with vSphere 4.0 systems.

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

Item: EN-000176-01