Obtaining SSL Certificates for VMware Horizon View Servers

View 5.2

View Composer 5.2

This document supports the version of each product listed and supports all subsequent versions until the document is replaced by a new edition. To check for more recent editions of this document, see http://www.vmware.com/support/pubs.

EN-001092-00

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

Obtaining SSL Certificates for VMware Horizon View Servers

Obtaining SSL Certificates for VMware Horizon View Servers provides an example that shows you how to obtain signed SSL certificates from Certificate Authorities and ensure that the certificates are in a format that can be used by View servers.

Intended Audience

This information is intended for anyone who wants to install VMware Horizon View and needs to obtain SSL certificates that are used by View servers, including View Connection Server, security server, and View Composer. The information is written for experienced Windows or Linux system administrators who are familiar with virtual machine technology and datacenter operations.

Obtaining SSL Certificates from a Certificate Authority 1

VMware strongly recommends that you configure SSL certificates that are signed by a valid Certificate Authority (CA) for use by View Connection Server instances, security servers, and View Composer instances.

Default SSL certificates are generated when you install View Connection Server, security server, or View Composer instances. Although you can use the default, self-signed certificates for testing purposes, replace them as soon as possible. The default certificates are not signed by a CA. Use of certificates that are not signed by a CA can allow untrusted parties to intercept traffic by masquerading as your server.

In a View environment, you should also replace the default certificate that is installed with vCenter Server with a certificate that is signed by a CA. You can use `openssl` to perform this task for vCenter Server. For details, see "Replacing vCenter Server Certificates" on the VMware Technical Papers site at http://www.vmware.com/resources/techresources/.

This chapter includes the following topics:

Determining If This Document Applies to You

In View 5.1 and later, you configure certificates for View by importing the certificates into the Windows local computer certificate store on the View server host.

Before you can import a certificate, you must generate a Certificate Signing Request (CSR) and obtain a valid, signed certificate from a CA. If the CSR is not generated according to the example procedure described in this document, the resulting certificate and its private key must be available in a PKCS#12 (formerly called PFX) format file.

There are many ways to obtain SSL certificates from a CA. This document shows how to use the Microsoft `certreq` utility to generate a CSR and make a certificate available to a View server. You can use another method if you are familiar with the required tools, and they are installed on your server.

Use this document to solve the following problems:

- You do not have SSL certificates that are signed by a CA, and you do not know how to obtain them
- You have valid, signed SSL certificates, but they are not in PKCS#12 (PFX) format

If your organization provides you with SSL certificates that are signed by a CA, you can use these certificates. Your organization can use a valid internal CA or a third-party, commercial CA. If your certificates are not in PKCS#12 format, you must convert them. See "Convert a Certificate File to PKCS#12 Format," on page 13.

When you have a signed certificate in the proper format, you can import it into the Windows certificate store and configure a View server to use it. To learn more about these tasks, see "Configuring SSL Certificates for View Servers" in the *VMware Horizon View Installation* document.

Selecting the Correct Certificate Type

You can use various types of SSL certificates with View. Selecting the correct certificate type for your deployment is critical. Different certificate types vary in cost, depending on the number of servers on which they can be used.

Single Server Name Certificate

You can generate a certificate with a subject name for a specific server. For example: `dept.company.com`.

This type of certificate is useful if, for example, only one View Connection Server instance needs a certificate.

When you submit a certificate signing request to a CA, you provide the server name that will be associated with the certificate. Be sure that the View server can resolve the server name you provide so that it matches the name associated with the certificate.

Subject Alternative Names

A Subject Alternative Name (SAN) is an attribute that can be added to a certificate when it is being issued. You use this attribute to add subject names (URLs) to a certificate so that it can validate more than one server.

For example, a certificate might be issued for a server with the host name `dept.company.com`. You intend the certificate to be used by external users connecting to View through a security server. Before the certificate is issued, you can add the SAN `dept-int.company.com` to the certificate to allow the certificate to be used on View Connection Server instances or security servers behind a load balancer when tunnelling is enabled.

Wildcard Certificate

A wildcard certificate is generated so that it can be used for multiple services. For example: `*.company.com`.

A wildcard is useful if many servers need a certificate. If other applications in your environment in addition to View need SSL certificates, you can use a wildcard certificate for those servers, too.

NOTE You can use a wildcard certificate only on a single level of domain. For example, a wildcard certificate with the subject name `*.company.com` can be used for the subdomain `dept.company.com` but not `dept.it.company.com`.

Generating a Certificate Signing Request and Obtaining a Certificate with Microsoft Certreq

To make a certificate available to a View server, you must create a configuration file, generate a certificate signing request (CSR) from the configuration file, and send the signing request to a CA. When the CA returns the certificate, you must import the signed certificate into the Windows local computer certificate store on the View server host, where it joins the previously generated private key.

A CSR can be generated in several ways, depending on how the certificate itself will be generated.

The Microsoft `certreq` utility is available on Windows Server 2008 R2 and can be used to generate a CSR and import a signed certificate. If you intend to send a request to a third-party CA, using `certreq` is the quickest and simplest way to obtain a certificate for VMware Horizon View.

1 Create a CSR Configuration File on page 9

The Microsoft `certreq` utility uses a configuration file to generate a CSR. You must create a configuration file before you can generate the request. Create the file and generate the CSR on the Windows Server computer that hosts the View server that will use the certificate.

2 Generate a CSR and Request a Signed Certificate from a CA on page 10

Using the completed configuration file, you can generate a CSR by running the `certreq` utility. You send the request to a third-party CA, which returns a signed certificate.

3 Verify That the CSR and Its Private Key Are Stored in the Windows Certificate Store on page 11

If you use the `certreq` utility to generate a CSR, the utility also generates an associated private key. The utility stores the CSR and private key in the Windows local computer certificate store on the computer on which you generated the CSR. You can confirm that the CSR and private key are properly stored by using the Microsoft Management Console (MMC) Certificate snap-in.

4 Import a Signed Certificate by Using Certreq on page 12

When you have a signed certificate from a CA, you can import the certificate into the Windows local computer certificate store on the View server host.

5 Set Up an Imported Certificate for a View Server on page 13

After you import a server certificate into the Windows local computer certificate store, you must take additional steps to allow a View server to use the certificate.

Create a CSR Configuration File

The Microsoft `certreq` utility uses a configuration file to generate a CSR. You must create a configuration file before you can generate the request. Create the file and generate the CSR on the Windows Server computer that hosts the View server that will use the certificate.

Procedure

1 Open a text editor and paste the following text, including the beginning and ending tags, into the file.

```
;----------------- request.inf -----------------

[Version]

Signature="$Windows NT$

[NewRequest]

Subject = "CN=View_Server_FQDN, OU=Organizational_Unit, O=Organization, L=City, S=State,
C=Country"
; Replace View_Server_FQDN with the FQDN of the View server.
; Replace the remaining Subject attributes.
KeySpec = 1
KeyLength = 2048
; KeyLength is usually chosen from 2048, 3072, or 4096. A KeyLength
; of 1024 is also supported, but it is not recommended.
Exportable = TRUE
MachineKeySet = TRUE
SMIME = False
PrivateKeyArchive = FALSE
UserProtected = FALSE
UseExistingKeySet = FALSE
ProviderName = "Microsoft RSA SChannel Cryptographic Provider"
ProviderType = 12
```

```
RequestType = PKCS10
KeyUsage = 0xa0

[EnhancedKeyUsageExtension]

OID=1.3.6.1.5.5.7.3.1 ; this is for Server Authentication

;-----------------------------------------------
```

If an extra CR/LF character is added to the `Subject =` line when you copy and paste the text, delete the CR/LF character.

2 Update the `Subject` attributes with appropriate values for your View server and deployment.

For example: `CN=dept.company.com`

NOTE Some CAs do not allow you to use abbreviations for the state attribute.

3 (Optional) Update the `Keylength` attribute.

The default value, 2048, is adequate unless you specifically need a different `KeyLength` size. Many CAs require a minimum value of 2048. Larger key sizes are more secure but have a greater impact on performance.

A `KeyLength` of 1024 is also supported, although the National Institute of Standards and Technology (NIST) recommends against keys of this size, as computers continue to become more powerful and can potentially crack stronger encryption.

IMPORTANT Do not generate a `KeyLength` value under 1024. View Client for Windows and View Client for Windows with Local Mode will not validate a certificate on a View server that was generated with a `KeyLength` under 1024, and the View Clients will fail to connect to View. Certificate validations that are performed by View Connection Server will also fail, resulting in the affected View servers showing as red in the View Administrator dashboard.

4 Save the file as `request.inf`.

What to do next

Generate a CSR from the configuration file.

Generate a CSR and Request a Signed Certificate from a CA

Using the completed configuration file, you can generate a CSR by running the `certreq` utility. You send the request to a third-party CA, which returns a signed certificate.

Prerequisites

- Verify that you completed a CSR configuration file. See "Create a CSR Configuration File," on page 9.
- Perform the `certreq` operation described in this procedure on the computer where the CSR configuration file is located.

Procedure

1 Open a command prompt by right-clicking on **Command Prompt** in the **Start** menu and selecting **Run as administrator**.

2 Navigate to the directory where you saved the `request.inf` file.

For example: **`cd c:\certificates`**

3 Generate the CSR file.

For example: **`certreq –new request.inf certreq.txt`**

4 In a text editor, open the CSR file (such as `certreq.txt`) and copy the contents of the file, including the beginning and ending tags.

For example:

```
-----BEGIN NEW CERTIFICATE REQUEST-----
MIID2jCCAsICAQAwazEWMBQGA1UEBhMNVW5pdGVkIFN0YXRlczELMAkGA1UECAwC
Q0ExEjAQBgNVBAcMCVBhbG8gQWx0bzEKMAgGA1UECgwBTzELMAkGA1UECwwCT1Ux
FzAVBgNVBAMMDm15LmNvbXBhbnkuY29tMIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8A
. . .
. . .
L9nPYX76jeu5rwQfXLivSCea6nZiIOZYw8Dbn8dgwAqpJdzBbrwuM1TuSnx6bAK8
S52Tv0GxW58jUTtxFV+Roz8TE8wZDFB51jx+FmLs
-----END NEW CERTIFICATE REQUEST-----
```

5 Use the contents of the CSR file to submit a certificate request to the CA in accordance with the CA's enrollment process.

a When you submit the request to a CA, the CA prompts you to select the type of server on which you will install the certificate. Since View uses the Microsoft Certificates MMC to manage certificates, select a certificate for a server type of Microsoft, Microsoft IIS 7, or something similar. The CA should produce a certificate in the format needed to work with View.

b If you request a single server name certificate, use a name that the View server can resolve. The name that computers use to connect to the View server should match the name associated with the certificate.

After conducting some checks on your company, the CA signs your request, encrypts it with a private key, and sends you a validated certificate.

The CA also sends you a root CA certificate and, if applicable, an intermediate CA certificate.

6 Rename the certificate text file to `cert.cer`.

Make sure that the file is located on the View server on which the certificate request was generated.

7 Rename the root CA and intermediate CA certificate files to `root.cer` and `intermediate.cer`.

Make sure that the files are located on the View server on which the certificate request was generated.

What to do next

Verify that the CSR file and its private key were stored in the Windows local computer certificate store.

Verify That the CSR and Its Private Key Are Stored in the Windows Certificate Store

If you use the `certreq` utility to generate a CSR, the utility also generates an associated private key. The utility stores the CSR and private key in the Windows local computer certificate store on the computer on which you generated the CSR. You can confirm that the CSR and private key are properly stored by using the Microsoft Management Console (MMC) Certificate snap-in.

The private key must later be joined with the signed certificate to enable the certificate to be properly imported and used by a View server.

Prerequisites

- Verify that you generated a CSR by using the `certreq` utility and requested a signed certificate from a CA. See "Generate a CSR and Request a Signed Certificate from a CA," on page 10.

- Familiarize yourself with the procedure for adding a Certificate snap-in to the Microsoft Management Console (MMC). See "Add the Certificate Snap-in to MMC" in the chapter, "Configuring SSL Certificates for View Servers," in the *VMware Horizon View Installation* document.

Procedure

1 On the Windows Server computer, add the Certificate snap-in to MMC.

2 In the MMC window on the Windows Server computer, expand the **Certificates (Local Computer)** node and select the **Certificate Enrollment Request** folder.

3 Expand the **Certificate Enrollment Request** folder and select the **Certificates** folder.

4 Verify that the certificate entry is displayed in the **Certificates** folder.

The **Issued To** and **Issued By** fields must show the domain name that you entered in the **`subject:CN`** field of the `request.inf` file that was used to generate the CSR.

5 Verify that the certificate contains a private key by taking one of the following steps:

- Verify that a yellow key appears on the certificate icon.
- Double-click the certificate and verify that the following statement appears in the Certificate Information dialog box: `You have a private key that corresponds to this certificate.`.

What to do next

Import the certificate into the Windows local computer certificate store.

Import a Signed Certificate by Using Certreq

When you have a signed certificate from a CA, you can import the certificate into the Windows local computer certificate store on the View server host.

If you used the `certreq` utility to generate a CSR, the certificate private key is local to the server on which you generated the CSR. To work correctly, the certificate must be combined with the private key. Use the `certreq` command shown in this procedure to ensure that the certificate and private key are properly combined and imported into the Windows certificate store.

If you use another method to obtain a signed certificate from a CA, you can use the Microsoft Management Console (MMC) Snap-in to import a certificate into the Windows certificate store. This method is described in "Configuring SSL Certificates for View Servers" in the *VMware Horizon View Installation* document.

Prerequisites

- Verify that you received a signed certificate from a CA. See "Generate a CSR and Request a Signed Certificate from a CA," on page 10.
- Perform the `certreq` operation described in this procedure on the computer on which you generated a CSR and stored the signed certificate.

Procedure

1 Open a command prompt by right-clicking on **Command Prompt** in the **Start** menu and selecting **Run as administrator**.

2 Navigate to the directory where you saved the signed certificate file such as `cert.cer`.

For example: **`cd c:\certificates`**

3 Import the signed certificate by running the `certreq –accept` command.

For example: **`certreq –accept cert.cer`**

The certificate is imported into the Windows local computer certificate store.

What to do next

Configure the imported certificate to be used by a View server. See "Set Up an Imported Certificate for a View Server," on page 13.

Set Up an Imported Certificate for a View Server

After you import a server certificate into the Windows local computer certificate store, you must take additional steps to allow a View server to use the certificate.

Procedure

1 Verify that the server certificate was imported successfully.

2 Change the certificate Friendly name to **vdm**.

3 Install the root CA certificate and intermediate CA certificate in the Windows certificate store.

4 Restart the View Connection Server service, security server service, or View Composer service to allow the View service to start using the new certificates.

To perform the tasks in this procedure, see "Configure View Connection Server, Security Server, or View Composer to Use a New SSL Certificate" in the *VMware Horizon View Installation* document. Follow the instructions in these topics:

- "Modify the Certificate Friendly Name"
- "Import a Root Certificate and Intermediate Certificates into a Windows Certificate Store"

NOTE The *VMware Horizon View Installation* topic "Import a Signed Server Certificate into a Windows Certificate Store" is not shown here because you already imported the server certificate by using the `certreq` utility. You should not use the MMC Snap-in to import the server certificate again.

However, you can use the MMC Snap-in to import the root CA certificate and intermediate CA certificate into the Windows certificate store, as described in the *VMware Horizon View Installation* document.

Convert a Certificate File to PKCS#12 Format

If you obtained a certificate and its private key in PEM or another format, you must convert it to PKCS#12 (PFX) format before you can import the certificate into a Windows certificate store on a View server host.

You might obtain a certificate keystore file from a CA, or your organization might provide you with certificate files, in various formats. For example, your certificates might be in PEM format, which is often used in a Linux environment. Your files might have a certificate file, key file, and CSR file with the following extensions:

```
server.crt
server.csr
server.key
```

The CRT file contains the SSL certificate that was returned by the CA. The CSR file is the original certificate signing request file and is not needed. The KEY file contains the private key.

Prerequisites

Verify that OpenSSL is installed on the system. You can download `openssl` from `http://www.openssl.org`. To run `openssl` from any directory on the system, see "Add openssl to the System Path," on page 14.

Procedure

- Generate a PKCS#12 (PFX) keystore file from the certificate file and your private key.

  For example: `openssl pkcs12 –export –out server.p12 –inkey server.key –in server.crt –certfile CACert.crt`

  In this example, `CACert.crt` is the name of the root certificate that was returned by the certificate authority.

  You can also generate a keystore with a PFX extension. For example: `–out server.pfx`

What to do next

Import the certificate into the Windows local computer certificate store on the View server host. See "Configure View Connection Server, Security Server, or View Composer to Use a New SSL Certificate" in the *VMware Horizon View Installation* document.

Add openssl to the System Path

You can use the `openssl` to request certificates from a CA and create and export private keys for use with View servers. You can add the path to `openssl` to the system environment Path variable so that you can run the utility from any directory on your system.

Procedure

1. On the system on which you intend to request a certificate from a CA, right-click **My Computer** and select **Properties**.
   a. On the **Advanced** tab, click **Environment Variables**.
   b. In the System variables group, select **Path** and click **Edit**.
   c. Type the paths to the JRE and Apache directories in the **Variable Value** text box. Use a semicolon (;) to separate each entry from other entries in the text box.

      For example: *`install_directory`*`\VMware\VMware View\Server\httpd\bin;`*`install_directory`*`\VMware\VMware View\Server\jre\bin`
2. Click **OK** until the Windows System Properties dialog box closes.

Index