vSphere Authentication

Update 3

VMware vSphere 7.0
VMware ESXi 7.0
vCenter Server 7.0

vmware®

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

https://docs.vmware.com/

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

Copyright © 2019-2021 VMware, Inc. All rights reserved. Copyright and trademark information.

Contents

About *vSphere Authentication*

The *vSphere Authentication* documentation provides information to help you perform common tasks such as certificate management and vCenter Single Sign-On configuration.

At VMware, we value inclusion. To foster this principle within our customer, partner, and internal community, we create content using inclusive language.

vSphere Authentication explains how you can manage certificates for vCenter Server and related services, and set up authentication with vCenter Single Sign-On.

Table 1-1. *vSphere Authentication* Highlights

Topics	Content Highlights
Getting Started with Authentication	■ Managing authentication services. ■ Managing vCenter Server using the vCenter Server Management Interface.
vSphere Security Certificates	■ Certificate model, and options for replacing certificates. ■ Replace certificates from the UI (simple cases). ■ Replace certificates using the Certificate Manager utility. ■ Replace certificates using the CLI (complex situations). ■ Certificate management CLI reference.
vSphere Authentication with vCenter Single Sign-On	■ Architecture of the authentication process. ■ How to add identity sources so users in your domain can authenticate. ■ Two-factor authentication. ■ Managing users, groups, and policies. ■ vCenter Server Identity Provider Federation

What Happened to the Platform Services Controller

Beginning in vSphere 7.0, deploying a new vCenter Server or upgrading to vCenter Server 7.0 requires the use of the vCenter Server appliance, a preconfigured virtual machine optimized for running vCenter Server. The new vCenter Server contains all Platform Services Controller services, preserving the functionality and workflows, including authentication, certificate management, tags, and licensing. It is no longer necessary nor possible to deploy and use an external Platform Services Controller. All Platform Services Controller services are consolidated into vCenter Server, and deployment and administration are simplified.

As these services are now part of vCenter Server, they are no longer described as a part of Platform Services Controller. In vSphere 7.0, the *vSphere Authentication* publication replaces the *Platform Services Controller Administration* publication. The new publication contains complete information about authentication and certificate management. For information about upgrading or migrating from vSphere 6.5 and 6.7 deployments using an existing external Platform Services Controller to vSphere 7.0 using vCenter Server appliance, see the *vSphere Upgrade* documentation.

Related Documentation

A companion document, *vSphere Security*, describes available security features and the measures that you can take to safeguard your environment from attack. That document also explains how you can set up permissions, and includes a reference to privileges.

In addition to these documents, VMware publishes the *vSphere Security Configuration Guide* (formerly known as the *Hardening Guide*) for each release of vSphere, accessible at https://core.vmware.com/security. The *vSphere Security Configuration Guide* contains guidelines on security settings that can or should be set by the customer, and security settings delivered by VMware that should be audited by the customer to ensure that they are still set to default.

Intended Audience

This information is intended for administrators who want to configure vCenter Server authentication and manage certificates. The information is written for experienced Linux system administrators who are familiar with virtual machine technology and data center operations.

Getting Started with Certificate Management and Authentication

1

vCenter Server provides common infrastructure services to the vSphere environment, including certificate management and authentication with vCenter Single Sign-On.

This chapter includes the following topics:

vSphere Certificate Management and Authentication Overview

vSphere provides services that enable you to perform certificate management tasks for vCenter Server and ESXi components, and configure authentication through vCenter Single Sign-On.

vSphere Certificate Management Overview

By default, vSphere enables you to provision vCenter Server components and ESXi hosts with VMware Certificate Authority (VMCA) certificates. You can also use custom certificates, which are stored in the VMware Endpoint Certificate Store (VECS).

vCenter Single Sign-On Overview

vCenter Single Sign-On allows vSphere components to communicate with each other through a secure token mechanism. vCenter Single Sign-On uses specific terms and definitions that are important to understand.

Table 1-1. vCenter Single Sign-On Glossary

Term	Definition
Principal	An entity that can be authenticated, such as a user.
Identity Provider	A service that manages identity sources and authenticates principals. Examples: Microsoft Active Directory Federation Services (AD FS) and vCenter Single Sign-On.

Table 1-1. vCenter Single Sign-On Glossary (continued)

Term	Definition
Identity Source (Directory Service)	Stores and manages principals. Principals consist of a collection of attributes about a user or service account such as name, address, email, and group membership. Examples: Microsoft Active Directory and VMware Directory Service (vmdir).
Authentication	The means of determining whether someone or something is, in fact, who or what it declares itself to be. For example, users are authenticated when they provide their credentials, such as smart cards, user name and correct password, and so on.
Authorization	The process of verifying what objects principals have access to.
Token	A signed collection of data comprising the identity information for a given principal. A token might include not only basic information about the principal such as email address and full name, but also, depending on the token type, the principal's groups and roles.
vmdir	VMware Directory Service. The internal (local) LDAP repository in vCenter Server that contains user identities, groups, and configuration data.
OpenID Connect (OIDC)	Authentication protocol based on OAuth2. vCenter Server uses OIDC capabilities when interacting with Active Directory Federation Services (AD FS).

vCenter Single Sign-On Authentication Types

vCenter Single Sign-On uses different types of authentication, depending on whether the built-in vCenter Server identity provider or an external identity provider is involved.

Table 1-2. vCenter Single Sign-On Authentication Types

Authentication Type	What Acts as the Identity Provider?	Does vCenter Server Handle the Password?	Description
Token-Based Authentication	External identity provider. For example, AD FS.	No	vCenter Server contacts the external identity provider through a particular protocol and obtains a token, which represents a particular user identity.
Simple Authentication	vCenter Server	Yes	The user name and password are passed directly to vCenter Server, which validates the credentials through its identity sources.

Managing Certificates

You manage certificates from the vSphere Client, or by using an API, scripts, or CLIs.

You can manage certificates using different interfaces.

Table 1-3. Interfaces for Managing Certificates

Interface	Description
vSphere Client	Web interface (HTML5-based client). See Managing Certificates with the vSphere Client.
vSphere Automation API	See *VMware vSphere Automation SDKs Programming Guide*.
Certificate Management utility	Command-line tool that supports Certificate Signing Request (CSR) generation and certificate replacement. See Managing Certificates with the vSphere Certificate Manager Utility.
CLIs for managing certificate and directory services	Set of commands for managing certificates, the VMware Endpoint Certificate Store (VECS), and VMware Directory Service (vmdir). See Chapter 3 Managing Services and Certificates with CLI Commands.

Manage Certificates from the vSphere Client

You can manage certificates from the vSphere Client.

Procedure

1. Log in to a vCenter Server as a user with administrator privileges in the local vCenter Single Sign-On domain.

   The default domain is vsphere.local.
2. Select **Administration**.
3. Under **Certificates**, click **Certificate Management**.

   Certificate panels for the different types of certificates appear.
4. Perform certificate tasks, such as viewing certificate details, renewing the Machine SSL certificate, and adding a Trusted Root certificate.

Use Scripts to Manage Certificates

vCenter Server includes scripts for generating Certificate Signing Requests (CSRs), managing certificates, and managing services.

For example, you can use the `certool` utility to generate CSRs and to replace certificates. See Managing Certificates with the vSphere Certificate Manager Utility.

Use the CLIs for management tasks that the vSphere Client does not support, or to create custom scripts for your environment.

Table 1-4. CLIs for Managing Certificates and Associated Services

CLI	Description	Links
`certool`	Generate and manage certificates and keys. Part of VMware Certificate Authority (VMCA).	certool Initialization Commands Reference
`vecs-cli`	Manage the contents of VMware Certificate Store instances. Part of VMware Authentication Framework Daemon (VMAFD).	vecs-cli Command Reference
`dir-cli`	Create and update certificates in VMware Directory Service. Part of VMAFD.	dir-cli Command Reference
`sso-config`	Update Security Token Service (STS) certificates.	Replace a vCenter Server STS Certificate Using the Command Line
`service-control`	Command for starting, stopping, and listing services.	Run this command to stop services before running other CLI commands.

Prerequisites

Enable SSH login to vCenter Server. See Manage vCenter Server with the Management Interface.

Procedure

1. Log in to the vCenter Server shell.

   Usually, you have to be the root or Administrator user. See Required Privileges for Running CLIs for details.

2. Access a CLI at one of the following default locations.

   The required privileges depend on the task that you want to perform. Sometimes, you are prompted for the password twice to safeguard sensitive information.

   ```
   /usr/lib/vmware-vmafd/bin/vecs-cli
   /usr/lib/vmware-vmafd/bin/dir-cli
   /usr/lib/vmware-vmca/bin/certool
   /opt/vmware/bin
   /opt/vmware/bin/sso-config.sh
   ```

   The `service-control` command does not require that you enter the path.

Managing Authentication Services

You manage authentication services from the vSphere Client, or by using the CLI. You can also manage the vCenter Server Identity Provider Federation configuration process by using an API.

You can manage authentication using different interfaces.

Table 1-5. Interfaces for Managing Authentication Services

Interface	Description
vSphere Client	Web interface (HTML5-based client).
API	Manage the vCenter Server Identity Provider Federation configuration process.
`sso-config`	Command-line utility for configuring the vCenter Server built-in identity provider.

Manage Authentication Services from the vSphere Client

You can manage vCenter Server authentication services from the vSphere Client.

Procedure

1. Log in to a vCenter Server as a user with administrator privileges in the local vCenter Single Sign-On domain.

   The default domain is vsphere.local.
2. Select **Administration**.
3. Under **Single Sign On**, click **Configuration** to manage identity providers and configure password and lockout policies.

Use Scripts to Manage Authentication Services

vCenter Server includes a utility, `sso-config`, for managing authentication services.

Use the `sso-config` utility for management tasks that the vSphere Client does not support, or to create custom scripts for your environment.

Table 1-6. CLIs for Managing Authentication and Associated Services

CLI	Description	Links
`sso-config`	Command-line utility for configuring the vCenter Server built-in identity provider.	Refer to the `sso-config` help by running `sso-config.sh -help`, or see the VMware knowledge base article at https://kb.vmware.com/s/article/67304 for usage examples.
`service-control`	Command for starting, stopping, and listing services.	Run this command to stop services before running other CLI commands.

Prerequisites

Enable SSH login to vCenter Server. See Manage vCenter Server with the Management Interface.

Procedure

1 Log in to the vCenter Server shell.

Usually, you have to be the root or Administrator user. See Required Privileges for Running CLIs for details.

2 Access the `sso-config` utility at following default location.

The required privileges depend on the task that you want to perform. Sometimes, you are prompted for the password twice to safeguard sensitive information.

```
/opt/vmware/bin/sso-config.sh
```

The `service-control` command does not require that you specify the path.

Managing the vCenter Server

You can manage the vCenter Server from the vCenter Server Management Interface or from the vCenter Server shell.

For more information about managing vCenter Server, see *vCenter Server Configuration*.

Table 1-7. Interfaces for Managing the vCenter Server

Interface	Description
vCenter Server Management Interface	Use this interface to reconfigure the system settings. See Manage vCenter Server with the Management Interface.
vCenter Server shell	Use this command-line interface to perform service management operations on VMCA, VECS, and VMDIR. See Managing Certificates with the vSphere Certificate Manager Utility and Chapter 3 Managing Services and Certificates with CLI Commands.

Manage vCenter Server with the Management Interface

You can use the vCenter Server Management Interface to configure the system settings. Settings include time synchronization, network settings, and SSH login settings. You can also change the root password, join the appliance to an Active Directory domain, and leave an Active Directory domain.

Procedure

1 In a browser, go to the Web interface at `https://vcenter_server_ip:5480`.

2 If a warning message about an untrusted SSL certificate appears, resolve the issue based on your company security policy and the browser that you are using.

3 Log in as root.

The default root password is the root password that you set when deploying the vCenter Server.

Results

You see the Summary page of the vCenter Server Management Interface.

Manage vCenter Server from the vCenter Server Shell

You can use service management utilities and CLIs from the vCenter Server shell. You can use TTY1 to log in to the console, or can use SSH to connect to the shell.

Procedure

1. Enable SSH login if necessary.
   a. Log in to the vCenter Server Management Interface at https://*vcenter_server_ip*:5480.
   b. In the Navigator, select **Access** and click **Edit**.
   c. Toggle on **Enable SSH Login** and click **OK**.

   You can follow the same steps to enable the Bash shell for the vCenter Server.
2. Access the shell.
   - If you have direct access to the vCenter Server console, select **Log in**, and press Enter.
   - To connect remotely, use SSH or another remote console connection to start a session to the vCenter Server.
3. Log in as root with the password that you set when you initially deployed the vCenter Server.

   If you changed the root password, use the new password.

Add a vCenter Server to an Active Directory Domain

If you want to add an Active Directory identity source to vCenter Server, you must join the vCenter Server to an Active Directory domain.

If you are unable to use vCenter Server Identity Provider Federation, or Active Directory over LDAPS, vCenter Server supports Integrated Windows Authentication (IWA). To use IWA, you must join the vCenter Server to your Active Directory domain.

Procedure

1. Using the vSphere Client, log in to vCenter Server as a user with administrator privileges in the local vCenter Single Sign-On domain (vsphere.local by default).
2. Select **Administration**.
3. Expand **Single Sign On** and click **Configuration**.
4. Under the **Identity Provider** tab, click **Active Directory Domain**.
5. Click **Join AD**, enter the domain, optional organizational unit, and user name and password, and click **Join**.
6. Restart vCenter Server.

What to do next

To attach users and groups from the joined Active Directory domain, add the joined domain as a vCenter Single Sign-On identity source. See Add or Edit a vCenter Single Sign-On Identity Source.

vSphere Security Certificates

2

vSphere provides security by using certificates to encrypt communications, authenticate services, and sign tokens.

vSphere uses certificates to:

- Encrypt communications between two nodes, such as a vCenter Server and an ESXi host.
- Authenticate vSphere services.
- Perform internal actions such as signing tokens.

vSphere's internal certificate authority, VMware Certificate Authority (VMCA), provides all the certificates necessary for vCenter Server and ESXi. VMCA is installed on every vCenter Server host, immediately securing the solution without any other modification. Keeping this default configuration provides the lowest operational overhead for certificate management. vSphere provides a mechanism to renew these certificates in the event they expire.

vSphere also provides a mechanism to replace certain certificates with your own certificates. However, replace only the SSL certificate that provides encryption between nodes, to keep your certificate management overhead low.

The following options are recommended for managing certificates.

Table 2-1. Recommended Options for Managing Certificates

Mode	Description	Advantages
VMCA Default Certificates	VMCA provides all the certificates for vCenter Server and ESXi hosts.	Simplest and lowest overhead. VMCA can manage the certificate life cycle for vCenter Server and ESXi hosts.
VMCA Default Certificates with External SSL Certificates (Hybrid Mode)	You replace the vCenter Server SSL certificates, and allow VMCA to manage certificates for solution users and ESXi hosts. Optionally, for high-security conscious deployments, you can replace the ESXi host SSL certificates as well.	Simple and secure. VMCA manages internal certificates but you get the benefit of using your corporate-approved SSL certificates, and having those certificates trusted by your browsers.

VMware does not recommend replacing either solution user certificates or STS certificates, nor using a subordinate CA in place of the VMCA. If you choose either of these options, you might encounter significant complexity and the potential for a negative impact to your security, and an unnecessary increase in your operational risk. For more information about managing certificates within a vSphere environment, see the blog post titled *New Product Walkthrough - Hybrid vSphere SSL Certificate Replacement* at http://vmware.com/go/hybridvmca.

You can use the following options to replace the existing certificates.

Table 2-2. Different Approaches to Certificate Replacement

Option	See
Use the vSphere Client.	Managing Certificates with the vSphere Client
Use the vSphere Automation API to manage the life cycle of certificates.	*VMware vSphere Automation SDKs Programming Guide*
Use the vSphere Certificate Manager utility from the command line.	Managing Certificates with the vSphere Certificate Manager Utility
Use CLI commands for manual certificate replacement.	Chapter 3 Managing Services and Certificates with CLI Commands

This chapter includes the following topics:

Certificate Requirements for Different Solution Paths

Certificate requirements depend on whether you use VMCA as an intermediate CA or you use custom certificates. Requirements are also different for machine certificates.

Before you begin, ensure that all nodes in your environment are time synchronized.

Note vSphere deploys only RSA certificates for server authentication and does not support generating ECDSA certificates. vSphere verifies ECDSA certificates presented by other servers. For example, if vSphere connects to a syslog server and the syslog server has an ECDSA certificate, vSphere supports verifying that certificate.

Requirements for all Imported Certificates

- Key size: 2048 bits (minimum) to 16384 bits (maximum) (PEM encoded)
- PEM format. VMware supports PKCS8 and PKCS1 (RSA keys). When you add keys to VECS, they are converted to PKCS8.

- x509 version 3
- SubjectAltName must contain DNS Name=*machine_FQDN*
- CRT format
- Contains the following Key Usages: Digital Signature, Key Encipherment.
- Exempting the vpxd-extension solution user certificate, Extended Key Usage can be either empty or contain Server Authentication.

VMCA does not support the following certificates.

- Certificates with wildcards.
- The algorithms md2WithRSAEncryption 1.2.840.113549.1.1.2, md5WithRSAEncryption 1.2.840.113549.1.1.4, and sha1WithRSAEncryption 1.2.840.113549.1.1.5 are not recommended.
- The algorithm RSASSA-PSS with OID 1.2.840.113549.1.1.10 is not supported.

Certificate Compliance to RFC 2253

The certificate must be in compliance with RFC 2253.

If you do not generate CSRs using Certificate Manager, ensure that the CSR includes the following fields.

String	X.500 AttributeType
CN	`commonName`
L	`localityName`
ST	`stateOrProvinceName`
O	`organizationName`
OU	`organizationalUnitName`
C	`countryName`
STREET	`streetAddress`
DC	`domainComponent`
UID	`userid`

If you generate CSRs using Certificate Manager, you are prompted for the following information, and Certificate Manager adds the corresponding fields to the CSR file.

- The password of the administrator@vsphere.local user, or for the administrator of the vCenter Single Sign-On domain that you are connecting to.
- Information that Certificate Manager stores in the `certool.cfg` file. For most fields, you can accept the default or provide site-specific values. The FQDN of the machine is required.
  - Password for administrator@vsphere.local
  - Two-letter country code
  - Company name

- Organization name
- Organization unit
- State
- Locality
- IP address (optional)
- Email
- Host name, that is, the fully qualified domain name of the machine for which you want to replace the certificate. If the host name does not match the FQDN, certificate replacement does not complete correctly and your environment might end up in an unstable state.
- IP address of the vCenter Server node on which you run Certificate Manager.

Requirements When Using VMCA as an Intermediate CA

When you use VMCA as an intermediate CA, the certificates must meet the following requirements.

Certificate Type	Certificate Requirements

Root certificate	■ You can use vSphere Certificate Manager to create the CSR. See Generate CSR with vSphere Certificate Manager and Prepare Root Certificate (Intermediate CA).
	■ If you prefer to create the CSR manually, the certificate that you send to be signed must meet the following requirements.
	■ Key size: 2048 bits (minimum) to 16384 bits (maximum) (PEM encoded)
	■ PEM format. VMware supports PKCS8 and PKCS1 (RSA keys). When keys are added to VECS, they are converted to PKCS8.
	■ x509 version 3
	■ The CA extension must be set to true for root certificates, and cert sign must be in the list of requirements. For example:
	`basicConstraints = critical,CA:true`
	`keyUsage = critical,digitalSignature,keyCertSign`
	■ CRL signing must be enabled.
	■ Extended Key Usage can be either empty or contain Server Authentication.
	■ No explicit limit to the length of the certificate chain. VMCA uses the OpenSSL default, which is 10 certificates.
	■ Certificates with wildcards or with more than one DNS name are not supported.
	■ You cannot create subsidiary CAs of VMCA.
	See the VMware knowledge base article at http://kb.vmware.com/kb/2112009, Creating a Microsoft Certificate Authority Template for SSL certificate creation in vSphere 6.x, for an example using Microsoft Certificate Authority.

Machine SSL certificate	You can use the vSphere Certificate Manager to create the CSR or create the CSR manually. If you create the CSR manually, it must meet the requirements listed previously under *Requirements for All Imported Certificates*. You also have to specify the FQDN for the host.
Solution user certificate	You can use vSphere Certificate Manager to create the CSR or create the CSR manually. **Note** You must use a different value for Name for each solution user. If you generate the certificate manually, this might show up as **CN** under **Subject**, depending on the tool you use.

Certificate Type	Certificate Requirements
	If you use vSphere Certificate Manager, the tool prompts you for certificate information for each solution user. vSphere Certificate Manager stores the information in `certool.cfg`. See *Information that Certificate Manager Prompts For*. For the vpxd-extension solution user, you can either leave Extended Key Usage empty or use "TLS WWW client authentication".

Requirements for Custom Certificates

When you want to use custom certificates, the certificates must meet the following requirements.

Certificate Type	Certificate Requirements
Machine SSL certificate	The machine SSL certificate on each node must have a separate certificate from your third-party or enterprise CA. ■ You can generate the CSR using the vSphere Client or vSphere Certificate Manager, or create the CSR manually. The CSR must meet the requirements listed previously under *Requirements for All Imported Certificates*. ■ For most fields, you can accept the default or provide site-specific values. The FQDN of the machine is required.
Solution user certificate	Each solution user on each node must have a separate certificate from your third-party or enterprise CA. ■ You can generate the CSRs using vSphere Certificate Manager or prepare the CSR yourself. The CSR must meet the requirements listed previously under *Requirements for All Imported Certificates*. ■ If you use vSphere Certificate Manager, the tool prompts you for certificate information for each solution user. vSphere Certificate Manager stores the information in `certool.cfg`. See *Information that Certificate Manager Prompts For*. **Note** You must use a different value for Name for each solution user. A manually generated certificate might show up as **CN** under **Subject**, depending on the tool you use. When later you replace solution user certificates with custom certificates, provide the complete signing certificate chain of the third-party CA. For the vpxd-extension solution user, you can either leave Extended Key Usage empty or use "TLS WWW client authentication".

Certificate Management Overview

The work required for setting up or updating your certificate infrastructure depends on the requirements in your environment. You must consider whether you are performing a fresh install or an upgrade, and whether you are considering ESXi or vCenter Server.

Administrators Who Do Not Replace VMware Certificates

VMCA can handle all certificate management. VMCA provisions vCenter Server components and ESXi hosts with certificates that use VMCA as the root certificate authority. If you are upgrading to vSphere 6 from an earlier version of vSphere, all self-signed certificates are replaced with certificates that are signed by VMCA.

If you do not currently replace VMware certificates, your environment starts using VMCA-signed certificates instead of self-signed certificates.

Administrators Who Replace VMware Certificates with Custom Certificates

If your company policy requires certificates that are signed by a third-party or enterprise CA, or that require custom certificate information, you have several choices for a fresh installation.

- Have the VMCA root certificate signed by a third-party CA or enterprise CA. Replace the VMCA root certificate with that signed certificate. In this scenario, the VMCA certificate is an intermediate certificate. VMCA provisions vCenter Server components and ESXi hosts with certificates that include the full certificate chain.
- If your company policy does not allow intermediate certificates in the chain, you can replace certificates explicitly. You can use the vSphere Client, vSphere Certificate Manager utility, or perform manual certificate replacement using the certificate management CLIs.

When upgrading an environment that uses custom certificates, you can retain some of the certificates.

- ESXi hosts keep their custom certificates during upgrade. Make sure that the vCenter Server upgrade process adds all the relevant root certificates to the TRUSTED_ROOTS store in VECS on the vCenter Server.

  After the upgrade to vSphere 6.0 or later, you can set the certificate mode to **Custom**. If the certificate mode is VMCA, the default, and the user performs a certificate refresh from the vSphere Client, the VMCA-signed certificates replace the custom certificates.
- For an upgrade of a simple vCenter Server installation to an embedded deployment, vCenter Server retains custom certificates. After the upgrade, your environment works as before. The existing vCenter Server and vCenter Single Sign-On certificates are retained. The certificates are used as machine SSL certificates. In addition, VMCA assigns a VMCA-signed certificate to each solution user (collection of vCenter services). The solution user uses this certificate only to authenticate to vCenter Single Sign-On. Replacing solution user certificates is often not required by a company policy.

You can use the command-line utility, vSphere Certificate Manager, for most certificate management tasks.

vSphere Certificate Interfaces

For vCenter Server, you can view and replace certificates with the following tools and interfaces.

Table 2-3. Interfaces for Managing vCenter Server Certificates

Interface	Use
vSphere Client	Perform common certificate tasks with a graphical user interface.
vSphere Automation API	See *VMware vSphere Automation SDKs Programming Guide*.
Certificate Manager utility	Perform common certificate replacement tasks from the command line of the vCenter Server installation.
Certificate management CLIs	Perform all certificate management tasks with `dir-cli`, `certool`, and `vecs-cli`.
`sso-config` utility	Perform STS certificate management from the command line of the vCenter Server installation.

For ESXi, you perform certificate management from the vSphere Client. VMCA provisions certificates and stores them locally on the ESXi host. VMCA does not store ESXi host certificates in VMDIR or in VECS. See the *vSphere Security* documentation.

Supported vCenter Certificates

For vCenter Server and related machines and services, the following certificates are supported:

- Certificates that are generated and signed by VMware Certificate Authority (VMCA).
- Custom certificates.
  - Enterprise certificates that are generated from your own internal PKI.
  - Third-party CA-signed certificates that are generated by an external PKI such as Verisign, GoDaddy, and so on.

Self-signed certificates that were created using OpenSSL in which no Root CA exists are not supported.

Certificate Replacement Overview

You can perform different types of certificate replacement depending on your company policy and requirements for the system that you are configuring. You can perform certificate replacement from the vCenter Server, by using the vSphere Certificate Manager utility, or manually by using the CLIs included with your installation.

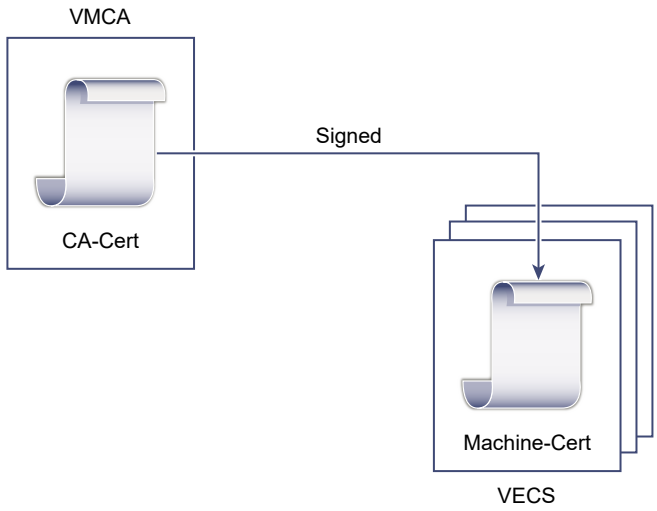
VMCA is included in each vCenter Server deployment. VMCA provisions each node, each vCenter Server solution user, and each ESXi host with a certificate that is signed by VMCA as the certificate authority.

You can replace the default certificates. For vCenter Server components, you can use a set of command-line tools included in your installation. You have several options.

Replace with Certificates Signed by VMCA

If your VMCA certificate expires or you want to replace it for other reasons, you can use the certificate management CLIs to perform that process. By default, the VMCA root certificate expires after 10 years, and all certificates that VMCA signs expire when the root certificate expires, that is, after a maximum of 10 years.

Figure 2-1. Certificates Signed by VMCA Are Stored in VECS



You can use the following vSphere Certificate Manager options:

- Replace Machine SSL Certificate with VMCA Certificate
- Replace Solution User Certificate with VMCA Certificate

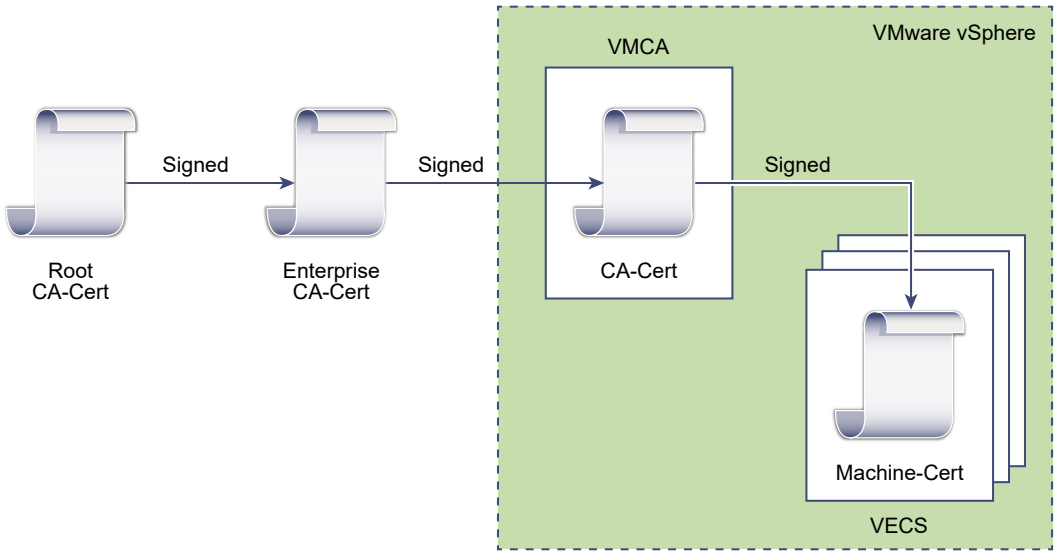
For manual certificate replacement, see Replace Existing VMCA-Signed Certificates with New VMCA-Signed Certificates.

Make VMCA an Intermediate CA

You can replace the VMCA root certificate with a certificate that is signed by an enterprise CA or third-party CA. VMCA signs the custom root certificate each time it provisions certificates, making VMCA an intermediate CA.

Note If you perform a fresh install with a vCenter Server, replace the VMCA root certificate before you add ESXi hosts. If you do, VMCA signs the whole chain, and you do not have to generate new certificates.

Figure 2-2. Certificates Signed by a Third-Party or Enterprise CA Use VMCA as an Intermediate CA



You can use the following vSphere Certificate Manager options:

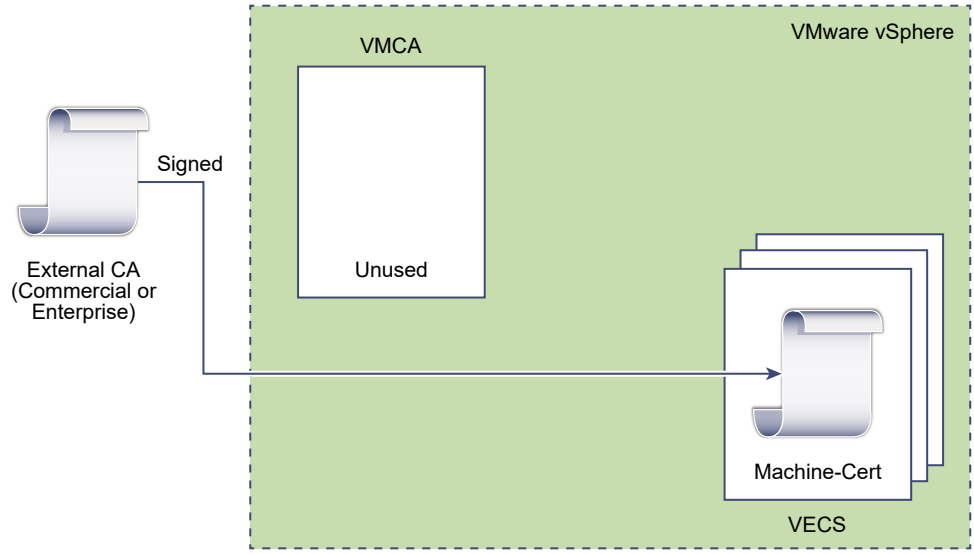
- Replace VMCA Root Certificate with Custom Signing Certificate and Replace All Certificates
- Replace Machine SSL Certificate with VMCA Certificate (multi-node enhanced linked mode deployment)
- Replace Solution User Certificate with VMCA Certificate (multi-node enhanced linked mode deployment)

For manual certificate replacement, see Use VMCA as an Intermediate Certificate Authority.

Do Not Use VMCA, Provision with Custom Certificates

You can replace the existing VMCA-signed certificates with custom certificates. If you use that approach, you are responsible for all certificate provisioning and monitoring.

Figure 2-3. External Certificates Are Stored Directly in VECS



You can use the following vSphere Certificate Manager options:

- Replace Machine SSL Certificate with Custom Certificate
- Replace Solution User Certificates with Custom Certificates

For manual certificate replacement, see Use Custom Certificates with vSphere.

You can also use the vSphere Client to generate a CSR for a machine SSL certificate (custom), and replace the certificate after the CA returns it. See Generate Certificate Signing Request for Machine SSL Certificate Using the vSphere Client (Custom Certificates).

Hybrid Deployment

You can have VMCA supply some of the certificates, but use custom certificates for other parts of your infrastructure. For example, because solution user certificates are used only to authenticate to vCenter Single Sign-On, consider having VMCA provision those certificates. Replace the machine SSL certificates with custom certificates to secure all SSL traffic.

Company policy often does not allow intermediate CAs. For those cases, hybrid deployment is a good solution. It minimizes the number of certificates to replace, and secures all traffic. The hybrid deployment leaves only internal traffic, that is, solution user traffic, to use the default VMCA-signed certificates.

ESXi Certificate Replacement

For ESXi hosts, you can change certificate provisioning behavior from the vSphere Client. See the *vSphere Security* documentation for details.

Table 2-4. ESXi Certificate Replacement Options

Option	Description
VMware Certificate Authority mode (default)	When you renew certificates from the vSphere Client, VMCA issues the certificates for the hosts. If you changed the VMCA root certificate to include a certificate chain, the host certificates include the full chain.
Custom Certificate Authority mode	Allows you to update and use certificates manually that are not signed or issued by VMCA.
Thumbprint mode	Can be used to retain 5.5 certificates during refresh. Use this mode only temporarily in debugging situations.

Where vSphere Uses Certificates

The VMware Certificate Authority (VMCA) provisions your environment with certificates. Certificates include machine SSL certificates for secure connections, solution user certificates for authentication of services to vCenter Single Sign-On, and certificates for ESXi hosts.

The following certificates are in use.

Table 2-5. Certificates in vSphere

Certificate	Provisioned	Comments
ESXi certificates	VMCA (default)	Stored locally on ESXi host.
Machine SSL certificates	VMCA (default)	Stored in VECS.
Solution user certificates	VMCA (default)	Stored in VECS.
vCenter Single Sign-On SSL signing certificate	Provisioned during installation.	Manage this certificate from the command line. **Note** Do not change this certificate in the filesystem or unpredictable behavior results.
VMware Directory Service (VMDIR) SSL certificate	Provisioned during installation.	Starting with vSphere 6.5, the machine SSL certificate is used as the vmdir certificate.

ESXi

ESXi certificates are stored locally on each host in the `/etc/vmware/ssl` directory. ESXi certificates are provisioned by VMCA by default, but you can use custom certificates instead. ESXi certificates are provisioned when the host is first added to vCenter Server and when the host reconnects.

Machine SSL Certificates

The machine SSL certificate for each node is used to create an SSL socket on the server side. SSL clients connect to the SSL socket. The certificate is used for server verification and for secure communication such as HTTPS or LDAPS.

Each vCenter Server node has its own machine SSL certificate. All services that are running on a vCenter Server node use the machine SSL certificate to expose their SSL endpoints.

The following services use the machine SSL certificate.

- The reverse proxy service. SSL connections to individual vCenter services always go to the reverse proxy. Traffic does not go to the services themselves.
- The vCenter Server service (vpxd).
- The VMware Directory Service (vmdir).

VMware products use standard X.509 version 3 (X.509v3) certificates to encrypt session information. Session information is sent over SSL between components.

Solution User Certificates

A solution user encapsulates one or more vCenter Server services. Each solution user must be authenticated to vCenter Single Sign-On. Solution users use certificates to authenticate to vCenter Single Sign-On through SAML token exchange.

A solution user presents the certificate to vCenter Single Sign-On when it first has to authenticate, after a reboot, and after a timeout has elapsed. The timeout (Holder-of-Key Timeout) can be set from the vSphere Client and defaults to 2592000 seconds (30 days).

For example, the vpxd solution user presents its certificate to vCenter Single Sign-On when it connects to vCenter Single Sign-On. The vpxd solution user receives a SAML token from vCenter Single Sign-On and can then use that token to authenticate to other solution users and services.

The following solution user certificate stores are included in VECS:

- `machine`: Used by the license server and the logging service.

  Note The machine solution user certificate has nothing to do with the machine SSL certificate. The machine solution user certificate is used for the SAML token exchange. The machine SSL certificate is used for secure SSL connections for a machine.

- `vpxd`: vCenter service daemon (vpxd) store. vpxd uses the solution user certificate that is stored in this store to authenticate to vCenter Single Sign-On.
- `vpxd-extension`: vCenter extensions store. Includes the Auto Deploy service, inventory service, and other services that are not part of other solution users.
- `vsphere-webclient`: vSphere Client store. Also includes some additional services such as the performance chart service.
- `wcp`: VMware vSphere® with VMware Tanzu™ store.

Internal Certificates

vCenter Single Sign-On certificates are not stored in VECS and are not managed with certificate management tools. As a rule, changes are not necessary, but in special situations, you can replace these certificates.

vCenter Single Sign-On Signing Certificate

The vCenter Single Sign-On service includes an identity provider service which issues SAML tokens that are used for authentication throughout vSphere. A SAML token represents the user's identity, and also contains group membership information. When vCenter Single Sign-On issues SAML tokens, it signs each token with its signing certificate so that clients of vCenter Single Sign-On can verify that the SAML token comes from a trusted source.

You can replace this certificate from the CLI. See Replace a vCenter Server STS Certificate Using the Command Line.

VMware Directory Service SSL Certificate

Starting with vSphere 6.5, the machine SSL certificate is used as the VMware directory certificate. For earlier versions of vSphere, see the corresponding documentation.

vSphere Virtual Machine Encryption Certificates

The vSphere Virtual Machine Encryption solution connects with an external Key Management Server (KMS). Depending on how the solution authenticates to the KMS, it might generate certificates and store them in VECS. See the *vSphere Security* documentation.

VMCA and VMware Core Identity Services

Core identity services are part of every vCenter Server system. VMCA is part of every VMware core identity services group. Use the management CLIs and the vSphere Client to interact with these services.

VMware core identity services include several components.

Table 2-6. Core Identity Services

Service	Description
VMware Directory Service (vmdir)	Identity source that handles SAML certificate management for authentication with vCenter Single Sign-On.
VMware Certificate Authority (VMCA)	Issues certificates for VMware solution users, machine certificates for machines on which services are running, and ESXi host certificates. VMCA can be used as is, or as an intermediary certificate authority. VMCA issues certificates only to clients that can authenticate to vCenter Single Sign-On in the same domain.
VMware Authentication Framework Daemon (VMAFD)	Includes the VMware Endpoint Certificate Store (VECS) and several other authentication services. VMware administrators interact with VECS. The other services are used internally.

VMware Endpoint Certificate Store Overview

VMware Endpoint Certificate Store (VECS) serves as a local (client-side) repository for certificates, private keys, and other certificate information that can be stored in a keystore. You can decide not to use VMCA as your certificate authority and certificate signer, but you must use VECS to store all vCenter certificates, keys, and so on. ESXi certificates are stored locally on each host and not in VECS.

VECS runs as part of the VMware Authentication Framework Daemon (VMAFD). VECS runs on every vCenter Server node, and holds the keystores that contain the certificates and keys.

VECS polls VMware Directory Service (vmdir) periodically for updates to the trusted root store. You can also explicitly manage certificates and keys in VECS using `vecs-cli` commands. See vecs-cli Command Reference.

VECS includes the following stores.

Table 2-7. Stores in VECS

Store	Description
Machine SSL store (MACHINE_SSL_CERT)	■ Used by the reverse proxy service on every vSphere node. ■ Used by the VMware Directory Service (vmdir) on each vCenter Server node. All services in vSphere 6.0 and later communicate through a reverse proxy, which uses the machine SSL certificate. For backward compatibility, the 5.x services still use specific ports. As a result, some services such as vpxd still have their own port open.
Solution user stores ■ `machine` ■ `vpxd` ■ `vpxd-extension` ■ `vsphere-webclient` ■ `wcp`	VECS includes one store for each solution user. The subject of each solution user certificate must be unique, for example, the machine certificate cannot have the same subject as the vpxd certificate. Solution user certificates are used for authentication with vCenter Single Sign-On. vCenter Single Sign-On checks that the certificate is valid, but does not check other certificate attributes. The following solution user certificate stores are included in VECS: ■ `machine`: Used by the license server and the logging service. **Note** The machine solution user certificate has nothing to do with the machine SSL certificate. The machine solution user certificate is used for the SAML token exchange. The machine SSL certificate is used for secure SSL connections for a machine. ■ `vpxd`: vCenter service daemon (vpxd) store. vpxd uses the solution user certificate that is stored in this store to authenticate to vCenter Single Sign-On. ■ `vpxd-extension`: vCenter extensions store. Includes the Auto Deploy service, inventory service, and other services that are not part of other solution users. ■ `vsphere-webclient`: vSphere Client store. Also includes some additional services such as the performance chart service. ■ `wcp`: VMware vSphere® with VMware Tanzu™ store. Each vCenter Server node includes a `machine` certificate.
Trusted root store (TRUSTED_ROOTS)	Contains all trusted root certificates.

Table 2-7. Stores in VECS (continued)

Store	Description
vSphere Certificate Manager Utility backup store (BACKUP_STORE)	Used by VMCA (VMware Certificate Manager) to support certificate revert. Only the most recent state is stored as a backup, you cannot go back more than one step.
Other stores	Other stores might be added by solutions. For example, the Virtual Volumes solution adds an SMS store. Do not modify the certificates in those stores unless VMware documentation or a VMware Knowledge Base article instructs you to do so. **Note** Deleting the TRUSTED_ROOTS_CRLS store can damage your certificate infrastructure. Do not delete or modify the TRUSTED_ROOTS_CRLS store.

The vCenter Single Sign-On service stores the token signing certificate and its SSL certificate on disk. You can change the token signing certificate from the CLI.

Some certificates are stored on the file system, either temporarily during startup or permanently. Do not change the certificates on the file system.

Note Do not change any certificate files on disk unless instructed by VMware documentation or Knowledge Base Articles. Unpredictable behavior might result otherwise.

Managing Certificate Revocation

If you suspect that one of your certificates has been compromised, replace all existing certificates, including the VMCA root certificate.

vSphere supports replacing certificates but does not enforce certificate revocation for ESXi hosts or for vCenter Server systems.

Remove revoked certificates from all nodes. If you do not remove revoked certificates, a man-in-the-middle attack might enable compromise through impersonation with the account's credentials.

Certificate Replacement in Large Deployments

When replacing certificates in deployments with large numbers of vCenter Server hosts, you can use the vSphere Certificate Management utility or replace certificates manually. Some best practices guide the process you choose.

Replacement of Machine SSL Certificates in Environments with Multiple vCenter Server Nodes

If your environment includes multiple vCenter Server nodes, you can replace certificates with the vSphere Client or the vSphere Certificate Manager utility, or manually with ESXCLI commands.

vSphere Certificate Manager

You run vSphere Certificate Manager on each machine. Depending on the task you perform, you are also prompted for certificate information.

Manual Certificate Replacement

For manual certificate replacement, you run the certificate replacement commands on each machine. See the following topics for details:

- Replace Machine SSL Certificates with VMCA-Signed Certificates
- Replace Machine SSL Certificates (Intermediate CA)
- Replace Machine SSL Certificates with Custom Certificates

Replacement of Solution User Certificates in Environments with Multiple vCenter Server Systems in Enhanced Linked Mode

If your environment includes multiple vCenter Server systems in enhanced linked mode, follow these steps for certificate replacement.

Note When you list solution user certificates in large deployments, the output of `dir-cli list` includes all solution users from all nodes. Run `vmafd-cli get-machine-id --server-name localhost` to find the local machine ID for each host. Each solution user name includes the machine ID.

vSphere Certificate Manager

You run vSphere Certificate Manager on each machine. Depending on the task you perform, you are also prompted for certificate information.

Manual Certificate Replacement

1. Generate or request a certificate. You need the following certificates:
   - A certificate for the machine solution user on each vCenter Server.
   - A certificate for each of the following solution users on each node:
     - `vpxd` solution user
     - `vpxd-extension` solution user
     - `vsphere-webclient` solution user
     - `wcp` solution user
2. Replace the certificates on each node. The precise process depends on the type of certificate replacement that you are performing. See Managing Certificates with the vSphere Certificate Manager Utility.

See the following topics for details:

- Replace Solution User Certificates with New VMCA-Signed Certificates
- Replace Solution User Certificates (Intermediate CA)

- Replace Solution User Certificates with Custom Certificates

Certificate Replacement in Environments That Include External Solutions

Some solutions, such as VMware vCenter Site Recovery Manager or VMware vSphere Replication, are always installed on a different machine than the vCenter Server system. If you replace the default machine SSL certificate on the vCenter Server system, a connection error results if the solution attempts to connect to the vCenter Server system.

You can run the `ls_update_certs` script to resolve the issue. See the VMware knowledge base article at http://kb.vmware.com/kb/2109074 for details.

Managing Certificates with the vSphere Client

You can view and manage certificates by using the vSphere Client. You also can perform many certificate management tasks with the vSphere Certificate Manager utility.

The vSphere Client enables you to perform these management tasks.

- View the machine SSL, Trusted Root, and Security Token Service (STS) certificates.
- Add new Trusted Root certificates, and renew or replace existing machine SSL and STS certificates.
- Generate a custom Certificate Signing Request (CSR) for a machine SSL certificate and replace the certificate when the Certificate Authority returns it.

Most parts of the certificate replacement workflows are supported fully from the vSphere Client. For generating CSRs for machine SSL certificates, you can use either the vSphere Client or the Certificate Manage utility.

Supported Workflows

After you install a vCenter Server, the VMware Certificate Authority on that node provisions all other nodes in the environment with certificates by default. See Chapter 2 vSphere Security Certificates for the current recommendations for managing certificates.

You can use one of the following workflows to renew or replace certificates.

Renew Certificates

You can have the VMCA renew machine SSL, solution user, and STS certificates in your environment from the vSphere Client.

Make VMCA an Intermediate CA

You can generate a CSR using the vSphere Certificate Manager utility. You can then edit the certificate you receive from the CSR to add the VMCA to the chain, and then add the certificate chain and private key to your environment. When you then renew all certificates, the VMCA provisions all machines and solution users with certificates that the full chain has signed.

Replace Certificates with Custom Certificates

If you do not want to use the VMCA, you can generate CSRs for the certificates that you want to replace. The CA returns a root certificate and a signed certificate for each CSR. You can upload the root certificate and the custom certificates from the vCenter Server.

Note If you use the VMCA as an intermediate CA, or use custom certificates, you might encounter significant complexity and the potential for a negative impact to your security, and an unnecessary increase in your operational risk. For more information about managing certificates within a vSphere environment, see the blog post titled *New Product Walkthrough - Hybrid vSphere SSL Certificate Replacement* at http://vmware.com/go/hybridvmca.

Explore Certificate Stores from the vSphere Client

A VMware Endpoint Certificate Store (VECS) instance is included on each vCenter Server node. You can explore the different stores inside the VMware Endpoint Certificate Store from the vSphere Client, including machine SSL and trusted root certificates.

See VMware Endpoint Certificate Store Overview for details on the different stores inside VECS.

Prerequisites

For most management tasks, you must have the password for the administrator for the local domain account, administrator@vsphere.local or a different domain if you changed the domain during installation.

Procedure

1. Log in with the vSphere Client to the vCenter Server.
2. Specify the user name and password for administrator@vsphere.local or another member of the vCenter Single Sign-On Administrators group.

   If you specified a different domain during installation, log in as administrator@*mydomain*.
3. Navigate to the Certificate Management UI.
   a. From the **Home** menu, select **Administration**.
   b. Under **Certificates**, click **Certificate Management**.
4. If the system prompts you, enter the credentials of your vCenter Server.
5. Explore the certificates stored inside the VMware Endpoint Certificate Store (VECS).

   VMware Endpoint Certificate Store Overview explains what is in the individual stores.

6 To view details for a certificate, select the certificate and click **View Details**.

7 Use the **Actions** menu to renew or replace certificates.

For example, if you replace the existing certificate, you can later remove the old root certificate. Remove certificates only if you are sure that they are no longer in use.

Set the Threshold for vCenter Certificate Expiration Warnings

vCenter Server monitors all certificates in the VMware Endpoint Certificate Store (VECS) and issues an alarm when a certificate is 30 days or less from its expiration. You can change how soon you are warned with the `vpxd.cert.threshold` advanced option.

Procedure

1 Log in to the vSphere Client.

2 Select the vCenter Server object and click **Configure**.

3 Click **Advanced Settings**.

4 Click **Edit Settings** and filter for **`threshold`**.

5 Change the setting of `vpxd.cert.threshold` to the desired value and click **Save**.

Renew VMCA Certificates with New VMCA-Signed Certificates from the vSphere Client

You can replace all VMCA-signed certificates with new VMCA-signed certificates. This process is called renewing certificates. You can renew selected certificates or all certificates in your environment from the vSphere Client.

Prerequisites

For certificate management, you have to supply the password of the administrator of the local domain (administrator@vsphere.local by default). If you are renewing certificates for a vCenter Server system, you also have to supply the vCenter Single Sign-On credentials for a user with administrator privileges on the vCenter Server system.

Procedure

1 Log in with the vSphere Client to the vCenter Server.

2 Specify the user name and password for administrator@vsphere.local or another member of the vCenter Single Sign-On Administrators group.

If you specified a different domain during installation, log in as administrator@*mydomain*.

3 Navigate to the Certificate Management UI.

a From the **Home** menu, select **Administration**.

b Under **Certificates**, click **Certificate Management**.

4 If the system prompts you, enter the credentials of your vCenter Server.

5 Renew the VMCA-signed machine SSL certificate for the local system.

   a Select **Machine SSL Certificate**.

   b Click **Actions > Renew**.

   c Click **Renew**.

   vCenter Server services restart automatically. You must log back in because restarting the services ends the UI session.

Set Up Your System to Use Custom Certificates

You can set up your environment to use custom certificates.

You can generate Certificate Signing Requests (CSRs) for each machine and for each solution user using the Certificate Manager utility. You can also generate CSRs for each machine, and replace certificates when you receive them from the third-party CA, using the vSphere Client. When you submit the CSRs to your internal or third-party CA, the CA returns signed certificates and the root certificate. You can upload both the root certificate and the signed certificates from the vCenter Server UI.

Generate Certificate Signing Request for Machine SSL Certificate Using the vSphere Client (Custom Certificates)

The machine SSL certificate is used by the reverse proxy service on every vCenter Server node. Each machine must have a machine SSL certificate for secure communication with other services. You can use the vSphere Client to generate a Certificate Signing Request (CSR) for the machine SSL certificate and to replace the certificate once it is ready.

Prerequisites

The certificate must meet the following requirements:

- Key size: 2048 bits (minimum) to 16384 bits (maximum) (PEM encoded)
- CRT format
- x509 version 3
- SubjectAltName must contain DNS Name=<machine_FQDN>.
- Contains the following Key Usages: Digital Signature, Key Encipherment

Procedure

1 Log in with the vSphere Client to the vCenter Server.

2 Specify the user name and password for administrator@vsphere.local or another member of the vCenter Single Sign-On Administrators group.

   If you specified a different domain during installation, log in as administrator@*mydomain*.

3 Navigate to the Certificate Management UI.
   a From the **Home** menu, select **Administration**.
   b Under **Certificates**, click **Certificate Management**.
4 Enter the credentials of your vCenter Server.
5 Generate the CSR.
   a For the certificate that you want to replace, under **Machine SSL Certificate**, click **Actions > Generate Certificate Signing Request (CSR)**.
   b Enter your certificate information and click **Next**.

      Note When you use vCenter Server to generate a CSR with a key size of 16384 bits, the generation takes a few minutes to complete because of the CPU-intensive nature of the operation.

   c Copy or download the CSR.
   d Click **Finish**.
   e Provide the CSR to your Certificate Authority.

What to do next

When the Certificate Authority returns the certificate, replace the existing certificate in the certificate store. See Add Custom Certificates.

Generate Certificate Signing Requests with vSphere Certificate Manager (Custom Certificates)

You can use vSphere Certificate Manager to generate Certificate Signing Requests (CSRs) that you can then use with your enterprise CA or send to an external certificate authority. You can use the certificates with the different supported certificate replacement processes.

You can run the Certificate Manager tool from the command line as follows:

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

Prerequisites

vSphere Certificate Manager prompts you for information. The prompts depend on your environment and on the type of certificate you want to replace.

- For any CSR generation, you are prompted for the password of the administrator@vsphere.local user, or for the administrator of the vCenter Single Sign-On domain that you are connecting to.
- You are prompted for the host name or IP address of the vCenter Server.
- To generate a CSR for a machine SSL certificate, you are prompted for certificate properties, which are stored in the `certool.cfg` file. For most fields, you can accept the default or provide site-specific values. The FQDN of the machine is required.

Procedure

1. On each machine in your environment, start vSphere Certificate Manager and select option 1.
2. Supply the password and the vCenter Server IP address or host name if prompted.
3. Select option 1 to generate the CSR, answer the prompts and exit Certificate Manager.

   As part of the process, you have to provide a directory. Certificate Manager places the certificate and key files in the directory.
4. If you also want to replace all solution user certificates, restart Certificate Manager.
5. Select option 5.
6. Supply the password and the vCenter Server IP address or host name if prompted.
7. Select option 1 to generate the CSRs, answer the prompts and exit Certificate Manager.

   As part of the process, you have to provide a directory. Certificate Manager places the certificate and key files in the directory.

What to do next

Perform certificate replacement.

Add a Trusted Root Certificate to the Certificate Store

If you want to use third-party certificates in your environment, you must add a trusted root certificate to the certificate store.

Prerequisites

Obtain the custom root certificate from your third-party or in-house CA.

Procedure

1. Log in with the vSphere Client to the vCenter Server.
2. Specify the user name and password for administrator@vsphere.local or another member of the vCenter Single Sign-On Administrators group.

   If you specified a different domain during installation, log in as administrator@*mydomain*.
3. Navigate to the Certificate Management UI.
   a. From the **Home** menu, select **Administration**.
   b. Under **Certificates**, click **Certificate Management**.
4. If the system prompts you, enter the credentials of your vCenter Server.
5. Under **Trusted Root Certificates**, click **Add**.
6. Click **Browse** and select the location of the certificate chain.

   You can use a file of type CER, PEM, or CRT.

7 Click **Add**.

The certificate is added to the store.

Add Custom Certificates

You can add custom Machine SSL certificates to the certificate store.

Usually, replacing the machine SSL certificate for each component is sufficient.

Prerequisites

Generate certificate signing requests (CSRs) for each certificate that you want to replace. You can generate the CSRs with the Certificate Manager utility. You can also generate a CSR for a machine SSL certificate using the vSphere Client. Place the certificate and private key in a location that the vCenter Server can access.

Procedure

1 Log in with the vSphere Client to the vCenter Server.

2 Specify the user name and password for administrator@vsphere.local or another member of the vCenter Single Sign-On Administrators group.

If you specified a different domain during installation, log in as administrator@*mydomain*.

3 Navigate to the Certificate Management UI.

a From the **Home** menu, select **Administration**.

b Under **Certificates**, click **Certificate Management**.

4 If the system prompts you, enter the credentials of your vCenter Server.

5 Under **Machine SSL Certificate**, for the certificate that you want to replace, click **Actions > Import and Replace Certificate**.

6 Click the appropriate certificate replacement option and click **Next**.

Option	Description
Replace with VMCA	Creates a VMCA-generated CSR to replace the current certificate.
Replace with certificate generated from vCenter Server	Use a certificate signed using a vCenter Server generated CSR to replace the current certificate.
Replace with external CA certificate (requires private key)	Use a certificate signed by an external CA to replace the current certificate.

7 Enter the CSR information, or upload the appropriate certificates.

8 Click **Replace**.

vCenter Server services restart automatically.

Managing Certificates with the vSphere Certificate Manager Utility

The vSphere Certificate Manager utility allows you to perform most certificate management tasks interactively from the command line. vSphere Certificate Manager prompts you for the task to perform, for certificate locations and other information as needed, and then stops and starts services and replaces certificates for you.

If you use vSphere Certificate Manager, you are not responsible for placing the certificates in VECS (VMware Endpoint Certificate Store) and you are not responsible for starting and stopping services.

Before you run vSphere Certificate Manager, be sure that you understand the replacement process and procure the certificates that you want to use.

Caution vSphere Certificate Manager supports one level of revert. If you run vSphere Certificate Manager twice and notice that you unintentionally corrupted your environment, the tool cannot revert the first of the two runs.

Certificate Manager Utility Location

You can run the tool on the command line as follows:

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

Certificate Manager Options and the Workflows in This Document

You run Certificate Manager options in sequence to complete a workflow. Several options, for example, generating CSRs, are used in different workflows.

Replace VMCA Root Certificate with Custom Signing Certificate and Replace All Certificates.

This single-option workflow (Option 2) can be used by itself, or in the intermediate certificate workflow. See Regenerate a New VMCA Root Certificate and Replace All Certificates.

Make VMCA an Intermediate Certificate Authority

To make VMCA an intermediate CA, you have to run Certificate Manager several times. The workflow gives the complete set of steps for replacing both machine SSL certificates and solution user certificates.

1 To generate a CSR, select Option 2, Replace VMCA Root certificate with Custom Signing Certificate and replace all Certificates. You might have to provide some information about the certificate next. When prompted for an option again, select Option 1.

   Submit the CSR to your external or enterprise CA. You receive a signed certificate and a root certificate from the CA.

2 Combine the VMCA root certificate with the CA root certificate and save the file.

3 Select Option 2, Replace VMCA Root certificate with Custom Signing Certificate and replace all Certificates. This process replaces all certificates on the local machine.

4 When multiple vCenter Server instances are connected in Enhanced Linked Mode configuration, you must replace certificates on each node.

   a First you replace the machine SSL certificate with the (new) VMCA certificate (Option 3)

   b Then you replace the solution user certificates with the (new) VMCA certificate (Option 6).

See Make VMCA an Intermediate Certificate Authority (Certificate Manager).

Replacing All Certificate with Custom Certificates

To replace all certificates with custom certificates, you have to run Certificate Manager several times. The workflow gives the complete set of steps for replacing both machine SSL certificates and solution user certificates.

1 You generate certificate signing requests for the machine SSL certificate and the solution user certificates separately on each machine.

   a To generate CSRs for the machine SSL certificate, you select Option 1.

   b If company policy requires that you replace all certificates, you also select Option 5.

2 After you received the signed certificates and the root certificate from your CA, you replace the machine SSL certificate on each machine by using Option 1.

3 If you also want to replace the solution user certificates, you select Option 5.

4 Finally, when multiple vCenter Server instances are connected in Enhanced Linked Mode configuration, you must repeat the process on each node.

See Replace All Certificates with Custom Certificate (Certificate Manager).

Note The following prompt appears when you run the Certificate Manager utility:

```
Enter proper value for VMCA 'Name':
```

Respond to the prompt by entering the fully qualified domain name of the machine on which the certificate configuration is running.

Regenerate a New VMCA Root Certificate and Replace All Certificates

You can regenerate the VMCA root certificate, and replace the local machine SSL certificate and the local solution user certificates with VMCA-signed certificates. When multiple vCenter Server instances are connected in Enhanced Linked Mode configuration, you must replace certificates on each vCenter Server.

When you replace the existing machine SSL certificate with a new VMCA-signed certificate, vSphere Certificate Manager prompts you for information and enters all values, except for the password and the IP address of the vCenter Server, into the `certool.cfg` file.

- Password for administrator@vsphere.local
- Two-letter country code
- Company name
- Organization name
- Organization unit
- State
- Locality
- IP address (optional)
- Email
- Host name, that is, the fully qualified domain name of the machine for which you want to replace the certificate. If the host name does not match the FQDN, certificate replacement does not complete correctly and your environment might end up in an unstable state.
- IP address of vCenter Server.
- VMCA name, that is, the fully qualified domain name of the machine on which the certificate configuration is running.

Prerequisites

You must know the following information when you run vSphere Certificate Manager with this option.

- Password for administrator@vsphere.local.
- The FQDN of the machine for which you want to generate a new VMCA-signed certificate. All other properties default to the predefined values but can be changed.

Procedure

1. Start vSphere Certificate Manager on the vCenter Server.
2. Select option 4.
3. Respond to the prompts.

   Certificate Manager generates a new VMCA root certificate based on your input and replaces all certificates on the system where you are running Certificate Manager. The replacement process is complete after Certificate Manager has restarted the services.
4. To replace the machine SSL certificate, run vSphere Certificate Manager with option 3, `Replace Machine SSL certificate with VMCA Certificate`.

5 To replace the solution user certificates, run Certificate Manager with option 6, `Replace Solution user certificates with VMCA certificates.`

Make VMCA an Intermediate Certificate Authority (Certificate Manager)

You can make VMCA an Intermediate CA by following the prompts from Certificate Manager utility. After you complete the process, VMCA signs all new certificates with the full chain. If you want, you can use Certificate Manager to replace all existing certificates with new VMCA-signed certificates.

VMware does not recommend replacing STS certificates, nor using a subordinate CA in place of the VMCA. If you choose either of these options, you might encounter significant complexity and the potential for a negative impact to your security, and an unnecessary increase in your operational risk. For more information about managing certificates within a vSphere environment, see the blog post titled *New Product Walkthrough - Hybrid vSphere SSL Certificate Replacement* at http://vmware.com/go/hybridvmca.

To make VMCA an intermediate CA, you have to run Certificate Manager several times. The workflow gives the complete set of steps for replacing machine SSL certificates.

1 To generate a CSR, select Option 1, Replace Machine SSL certificate with Custom Certificate then Option 1.

   You receive a signed certificate and a root certificate from the CA.

2 Combine the VMCA root certificate with the CA root certificate and save the file.

3 Select Option 2, Replace VMCA Root certificate with Custom Signing Certificate and replace all Certificates. This process replaces all certificates on the local machine.

Generate CSR with vSphere Certificate Manager and Prepare Root Certificate (Intermediate CA)

You can use vSphere Certificate Manager to generate Certificate Signing Requests (CSRs). Submit those CSRs to your enterprise CA or to an external certificate authority for signing. You can use the signed certificates with the different supported certificate replacement processes.

- You can use vSphere Certificate Manager to create the CSR.
- If you prefer to create the CSR manually, the certificate that you send to be signed must meet the following requirements.
  - Key size: 2048 bits (minimum) to 16384 bits (maximum) (PEM encoded)
  - PEM format. VMware supports PKCS8 and PKCS1 (RSA keys). When keys are added to VECS, they are converted to PKCS8.
  - x509 version 3

- The CA extension must be set to true for root certificates, and cert sign must be in the list of requirements. For example:

```
basicConstraints        = critical,CA:true
keyUsage                = critical,digitalSignature,keyCertSign
```

- CRL signing must be enabled.
- Extended Key Usage can be either empty or contain Server Authentication.
- No explicit limit to the length of the certificate chain. VMCA uses the OpenSSL default, which is 10 certificates.
- Certificates with wildcards or with more than one DNS name are not supported.
- You cannot create subsidiary CAs of VMCA.

  See the VMware knowledge base article at http://kb.vmware.com/kb/2112009, Creating a Microsoft Certificate Authority Template for SSL certificate creation in vSphere 6.x, for an example using Microsoft Certificate Authority.

Prerequisites

vSphere Certificate Manager prompts you for information. The prompts depend on your environment and on the type of certificate that you want to replace.

For any CSR generation, you are prompted for the password of the administrator@vsphere.local user, or for the administrator of the vCenter Single Sign-On domain that you are connecting to.

Procedure

1. Run the vSphere Certificate Manager.

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

2. Select Option 2.

   Initially, you use this option to generate the CSR, not to replace certificates.

3. Supply the password and the vCenter Server IP address or host name if prompted.
4. Select Option 1 to generate the CSR and answer the prompts.

   As part of the process, you have to provide a directory. Certificate Manager places the certificate to be signed (`*.csr` file) and the corresponding key file (`*.key` file) in the directory.

5. Name the certificate signing request (CSR) `root_signing_cert.csr`.
6. Send the CSR to your enterprise or external CA for signing and name the resulting signed certificate `root_signing_cert.cer`.
7. In a text editor, combine the certificates as follows.

```
-----BEGIN CERTIFICATE-----
Signed VMCA root certificate
```

```
-----END CERTIFICATE-----
-----BEGIN CERTIFICATE-----
CA intermediate certificates
-----END CERTIFICATE-----
-----BEGIN CERTIFICATE-----
Root certificate of enterprise or external CA
-----END CERTIFICATE-----
```

8 Save the file as `root_signing_chain.cer`.

What to do next

Replace the existing root certificate with the chained root certificate. See Replace VMCA Root Certificate with Custom Signing Certificate and Replace All Certificates.

Replace VMCA Root Certificate with Custom Signing Certificate and Replace All Certificates

You can use vSphere Certificate Manager to generate a CSR and send the CSR to an enterprise or third-party CA for signing. You can then replace the VMCA root certificate with a custom signing certificate and replace all existing certificates with certificates that are signed by the custom CA.

You run vSphere Certificate Manager on vCenter Server to replace the VMCA root certificate with a custom signing certificate.

Prerequisites

- Generate the certificate chain.
  - You can use vSphere Certificate Manager to create the CSR or create the CSR manually.
  - After you receive the signed certificate from your third-party or enterprise CA, combine it with the initial VMCA root certificate to create the full chain.

    See Generate CSR with vSphere Certificate Manager and Prepare Root Certificate (Intermediate CA) for certificate requirements and the process of combining the certificates.
- Gather the information that you need.
  - Password for administrator@vsphere.local
  - Valid custom certificate for Root (`.crt` file)
  - Valid custom key for Root (`.key` file)

Procedure

1 Start vSphere Certificate Manager on the vCenter Server host and select option 2.

2 Select option 2 again to start certificate replacement and respond to the prompts.

   a Specify the full path to the root certificate when prompted.

   b If you are replacing certificates for the first time, you are prompted for information to be used for the machine SSL certificate.

      This information includes the required FQDN of the machine and is stored in the `certool.cfg` file.

Replace Machine SSL Certificate with VMCA Certificate (Intermediate CA)

When you use VMCA as an intermediate CA, you can replace the machine SSL certificate explicitly. First you replace the VMCA root certificate on the vCenter Server, then you can replace the machine SSL certificate, which will be signed by the VMCA's new root. You can also use this option to replace machine SSL certificates that are corrupt or about to expire.

When you replace the existing machine SSL certificate with a new VMCA-signed certificate, vSphere Certificate Manager prompts you for information and enters all values, except for the password and the IP address of the vCenter Server, into the `certool.cfg` file.

- Password for administrator@vsphere.local
- Two-letter country code
- Company name
- Organization name
- Organization unit
- State
- Locality
- IP address (optional)
- Email
- Host name, that is, the fully qualified domain name of the machine for which you want to replace the certificate. If the host name does not match the FQDN, certificate replacement does not complete correctly and your environment might end up in an unstable state.
- IP address of vCenter Server.
- VMCA name, that is, the fully qualified domain name of the machine on which the certificate configuration is running.

Prerequisites

- You must know the following information to run Certificate Manager with this option.
  - Password for administrator@vsphere.local.
  - The FQDN of the machine for which you want to generate a new VMCA-signed certificate. All other properties default to the predefined values but can be changed.

- Host name or IP address of the vCenter Server system.

Procedure

1. Start vSphere Certificate Manager and select option 3.
2. Respond to the prompts.

   Certificate Manager stores the information in the `certool.cfg` file.

Results

vSphere Certificate Manager replaces the machine SSL certificate.

Replace Solution User Certificates with VMCA Certificates (Intermediate CA)

When you use VMCA as an intermediate CA, you can replace the solution user certificate explicitly. First you replace the VMCA root certificate on the vCenter Server, then you can replace the solution user certificate, which will be signed by the VMCA's new root. You can also use this option to replace solution certificates that are corrupt or about to expire.

Prerequisites

- Restart all vCenter Server nodes explicitly if you replaced the VMCA root certificate in a deployment consisting of multiple instances of vCenter Server in Enhanced Linked Mode configuration.
- You must know the following information to run Certificate Manager with this option.
  - Password for administrator@vsphere.local
  - Host name or IP address of the vCenter Server system

Procedure

1. Start vSphere Certificate Manager and select option 6.
2. Respond to the prompts.

   See the VMware knowledge base article at http://kb.vmware.com/kb/2112281 for more information.

Results

vSphere Certificate Manager replaces all solution user certificates.

Replace All Certificates with Custom Certificate (Certificate Manager)

You can use the vSphere Certificate Manager utility to replace all certificates with custom certificates. Before you start the process, you must send CSRs to your CA. You can use Certificate Manager to generate the CSRs.

One option is to replace only the machine SSL certificate, and to use the solution user certificates that are provisioned by VMCA. Solution user certificates are used only for communication between vSphere components.

When you use custom certificates, you replace the VMCA-signed certificates with custom certificates. You can use the vSphere Client, the vSphere Certificate Manager utility, or CLIs for manual certificate replacement. Certificates are stored in VECS.

To replace all certificates with custom certificates, you have to run Certificate Manager several times. The workflow gives the complete set of steps for replacing both machine SSL certificates and solution user certificates.

1 You generate certificate signing requests for the machine SSL certificate and the solution user certificates separately on each machine.
   a To generate CSRs for the machine SSL certificate, you select Option 1.
   b If company policy does not allow a hybrid deployment, you select Option 5.
2 After you received the signed certificates and the root certificate from your CA, you replace the machine SSL certificate on each machine by using Option 1.
3 If you also want to replace the solution user certificates, you select Option 5.
4 Finally, when multiple vCenter Server instances are connected in Enhanced Linked Mode configuration, you have to repeat the process on each node.

Generate Certificate Signing Requests with vSphere Certificate Manager (Custom Certificates)

You can use vSphere Certificate Manager to generate Certificate Signing Requests (CSRs) that you can then use with your enterprise CA or send to an external certificate authority. You can use the certificates with the different supported certificate replacement processes.

You can run the Certificate Manager tool from the command line as follows:

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

Prerequisites

vSphere Certificate Manager prompts you for information. The prompts depend on your environment and on the type of certificate you want to replace.

- For any CSR generation, you are prompted for the password of the administrator@vsphere.local user, or for the administrator of the vCenter Single Sign-On domain that you are connecting to.
- You are prompted for the host name or IP address of the vCenter Server.
- To generate a CSR for a machine SSL certificate, you are prompted for certificate properties, which are stored in the `certool.cfg` file. For most fields, you can accept the default or provide site-specific values. The FQDN of the machine is required.

Procedure

1. On each machine in your environment, start vSphere Certificate Manager and select option 1.
2. Supply the password and the vCenter Server IP address or host name if prompted.

3 Select option 1 to generate the CSR, answer the prompts and exit Certificate Manager.

   As part of the process, you have to provide a directory. Certificate Manager places the certificate and key files in the directory.

4 If you also want to replace all solution user certificates, restart Certificate Manager.

5 Select option 5.

6 Supply the password and the vCenter Server IP address or host name if prompted.

7 Select option 1 to generate the CSRs, answer the prompts and exit Certificate Manager.

   As part of the process, you have to provide a directory. Certificate Manager places the certificate and key files in the directory.

What to do next

Perform certificate replacement.

Replace Machine SSL Certificate with Custom Certificate

The machine SSL certificate is used by the reverse proxy service on every vCenter Server node. Each machine must have a machine SSL certificate for secure communication with other services. You can replace the certificate on each node with a custom certificate.

Prerequisites

Before you start, you need a CSR for each machine in your environment. You can generate the CSR using vSphere Certificate Manager or explicitly.

1 To generate the CSR using vSphere Certificate Manager, see Generate Certificate Signing Requests with vSphere Certificate Manager (Custom Certificates).

2 To generate the CSR explicitly, request a certificate for each machine from your third-party or enterprise CA. The certificate must meet the following requirements:

   - Key size: 2048 bits (minimum) to 16384 bits (maximum) (PEM encoded)
   - CRT format
   - x509 version 3
   - SubjectAltName must contain DNS Name=<machine_FQDN>.
   - Contains the following Key Usages: Digital Signature, Key Encipherment

See also the VMware knowledge base article at http://kb.vmware.com/kb/2112014, Obtaining vSphere certificates from a Microsoft Certificate Authority.

Procedure

1 Start vSphere Certificate Manager and select option 1.

2 Select option 2 to start certificate replacement and respond to the prompts.

vSphere Certificate Manager prompts you for the following information:

- Password for administrator@vsphere.local
- Valid Machine SSL custom certificate (`.crt` file)
- Valid Machine SSL custom key (`.key` file)
- Valid signing certificate for the custom machine SSL certificate (`.crt` file)
- IP address of the vCenter Server

Replace Solution User Certificates with Custom Certificates

Many companies only require that you replace certificates of services that are accessible externally. However, Certificate Manager also supports replacing solution user certificates. Solution users are collections of services, for example, all services that are associated with the vSphere Client.

When you are prompted for a solution user certificate, provide the complete signing certificate chain of the third-party CA.

The format looks similar to the following.

```
-----BEGIN CERTIFICATE-----
Signing certificate
-----END CERTIFICATE-----
-----BEGIN CERTIFICATE-----
CA intermediate certificates
-----END CERTIFICATE-----
-----BEGIN CERTIFICATE-----
Root certificate of enterprise or external CA
-----END CERTIFICATE-----
```

Prerequisites

Before you start, you need a CSR for each machine in your environment. You can generate the CSR using vSphere Certificate Manager or explicitly.

1 To generate the CSR using vSphere Certificate Manager, see Generate Certificate Signing Requests with vSphere Certificate Manager (Custom Certificates).

2 Request a certificate for each solution user on each node from your third-party or enterprise CA. You can generate the CSR using vSphere Certificate Manager or prepare it yourself. The CSR must meet the following requirements:

- Key size: 2048 bits (minimum) to 16384 bits (maximum) (PEM encoded)
- CRT format
- x509 version 3
- SubjectAltName must contain DNS Name=<machine_FQDN>.

- Each solution user certificate must have a different `Subject`. Consider, for example, including the solution user name (such as vpxd) or other unique identifier.
- Contains the following Key Usages: Digital Signature, Key Encipherment

See also the VMware knowledge base article at http://kb.vmware.com/kb/2112014, Obtaining vSphere certificates from a Microsoft Certificate Authority.

Procedure

1. Start vSphere Certificate Manager and select option 5.
2. Select option 2 to start certificate replacement and respond to the prompts.

   vSphere Certificate Manager prompts you for the following information:

   - Password for administrator@vsphere.local
   - Certificate and key for machine solution user
   - The certificate and key (`vpxd.crt` and `vpxd.key`) for the machine solution user
   - The full set of certificates and keys (`vpxd.crt` and `vpxd.key`) for all solution users

Revert Last Performed Operation by Republishing Old Certificates

When you perform a certificate management operation by using vSphere Certificate Manager, the current certificate state is stored in the BACKUP_STORE store in VECS before certificates are replaced. You can revert the last performed operation and return to the previous state.

Note The revert operation restores what is currently in the BACKUP_STORE. If you run vSphere Certificate Manager with two different options and you then attempt to revert, only the last operation is reverted.

Reset All Certificates

Use the `Reset All Certificates` option to replace all existing vCenter certificates with certificates that are signed by VMCA.

When you use this option, you overwrite all custom certificates that are currently in VECS.

vSphere Certificate Manager can replace all certificates. Which certificates are replaced depends on which options you select.

Manual Certificate Replacement

For some special certificate replacement cases, you cannot use the vSphere Certificate Manager utility. Instead, you can use the CLIs included with your installation for certificate replacement.

Understanding Stopping and Starting of Services

For certain parts of manual certificate replacement, you must stop all services and then start only the services that manage the certificate infrastructure. If you stop services only when needed, you can minimize downtime.

You have to stop and start services as part of the certificate replacement process. You can use the `service-control` command for starting and stopping services. You can start and stop all services or individual services. See the command-line help for more information.

Follow these guidelines.

- Do not stop services to generate new public/private key pairs or new certificates.
- If you are the only administrator, you do not have to stop services when you add a new root certificate. The old root certificate remains available, and all services can still authenticate with that certificate. Stop and immediately restart all services after you add the root certificate to avoid problems with your hosts.
- If your environment includes multiple administrators, stop services before you add a new root certificate and restart services after you add a new certificate.
- Stop services right before you delete a machine SSL certificate in VECS.

Replace Existing VMCA-Signed Certificates with New VMCA-Signed Certificates

If the VMCA root certificate expires in the near future, or if you want to replace it for other reasons, you can generate a new root certificate and add it to the VMware Directory Service. You can then generate new machine SSL certificates and solution user certificates using the new root certificate.

Use the vSphere Certificate Manager utility to replace certificates for most cases.

If you need fine-grained control, this scenario gives detailed step-by-step instructions for replacing the complete set of certificates using CLI commands. You can instead replace only individual certificates using the procedure in the corresponding task.

Prerequisites

Only administrator@vsphere.local or other users in the CAAdmins group can perform certificate management tasks. See Add Members to a vCenter Single Sign-On Group.

Generate a New VMCA-Signed Root Certificate

You generate new VMCA-signed certificates with the `certool` CLI or the vSphere Certificate Manager utility and publish the certificates to vmdir.

Procedure

1 On the vCenter Server, generate a new self-signed certificate and private key.

```
certool --genselfcacert --outprivkey <key_file_path> --outcert <cert_file_path> --config
<config_file>
```

2 Replace the existing root certificate with the new certificate.

```
certool --rootca --cert <cert_file_path> --privkey <key_file_path>
```

The command generates the certificate, adds it to vmdir, and adds it to VECS.

3 Stop all services and start the services that handle certificate creation, propagation, and storage.

```
service-control --stop --all
service-control --start vmafdd
service-control --start vmdird
service-control --start vmcad
```

4 (Optional) Publish the new root certificate to vmdir.

```
dir-cli trustedcert publish --cert newRoot.crt
```

The command updates all instances of vmdir immediately. If you do not run the command, propagation of the new certificate to all nodes might take a while.

5 Restart all services.

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

Example: Generate a New VMCA-Signed Root Certificate

The following example shows all the steps for verifying the current root CA information, and for regenerating the root certificate.

1 (Optional) On the vCenter Server, list the VMCA root certificate to make sure it is in the certificate store.

```
/usr/lib/vmware-vmca/bin/certool --getrootca
```

The output looks similar to this:

```
output:
Certificate:
    Data:
        Version: 3 (0x2)
        Serial Number:
            cf:2d:ff:49:88:50:e5:af
    ...
```

2 (Optional) List the VECS TRUSTED_ROOTS store and compare the certificate serial number there with the output from Step 1.

```
/usr/lib/vmware-vmafd/bin/vecs-cli entry list --store TRUSTED_ROOTS --text
```

In the simplest case with only one root certificate, the output looks like this:

```
Number of entries in store :    1
Alias : 960d43f31eb95211ba3a2487ac840645a02894bd
Entry type :    Trusted Cert
Certificate:
    Data:
        Version: 3 (0x2)
        Serial Number:
            cf:2d:ff:49:88:50:e5:af
```

3 Generate a new VMCA root certificate. The command adds the certificate to the TRUSTED_ROOTS store in VECS and in vmdir (VMware Directory Service).

```
/usr/lib/vmware-vmca/bin/certool --selfca --config=/usr/lib/vmware-vmca/share/config/
certool.cfg
```

Replace Machine SSL Certificates with VMCA-Signed Certificates

After you generate a new VMCA-signed root certificate, you can replace all machine SSL certificates in your environment.

Each machine must have a machine SSL certificate for secure communication with other services. When multiple vCenter Server instances are connected in Enhanced Linked Mode configuration, you must run the Machine SSL certificate generation commands on each node.

Prerequisites

Be prepared to stop all services and to start the services that handle certificate propagation and storage.

Procedure

1 Make one copy of `certool.cfg` for each machine that needs a new certificate.

You can find the `certool.cfg` file in the `/usr/lib/vmware-vmca/share/config/` directory.

2 Edit the custom configuration file for each machine to include that machine's FQDN.

Run `NSLookup` against the machine's IP address to see the DNS listing of the name, and use that name for the Hostname field in the file.

3 Generate a public/private key file pair and a certificate for each file, passing in the configuration file that you just customized.

For example:

```
certool --genkey --privkey=machine1.priv --pubkey=machine1.pub
certool --gencert --privkey=machine1.priv --cert machine1.crt --Name=Machine1_Cert --
config machine1.cfg
```

4 Stop all services and start the services that handle certificate creation, propagation, and storage.

```
service-control --stop --all
service-control --start vmafdd
service-control --start vmdird
service-control --start vmcad
```

5 Add the new certificate to VECS.

All machines need the new certificate in the local certificate store to communicate over SSL. You first delete the existing entry, then add the new entry.

```
vecs-cli entry delete --store MACHINE_SSL_CERT --alias __MACHINE_CERT
vecs-cli entry create --store MACHINE_SSL_CERT --alias __MACHINE_CERT --cert machine1.crt
--key machine1.priv
```

6 Restart all services.

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

Example: Replacing Machine Certificates with VMCA-Signed Certificates

1 Create a configuration file for the SSL certificate and save it as `ssl-config.cfg` in the current directory.

```
Country = US
Name = vmca-<FQDN-example>
Organization = <my_company>
OrgUnit = <my_company Engineering>
State = <my_state>
Locality = <mytown>
Hostname = <FQDN>
```

2 Generate a key pair for the machine SSL certificate. In a deployment of multiple vCenter Server instances connected in Enhanced Linked Mode configuration, run this command on each vCenter Server node.

```
/usr/lib/vmware-vmca/bin/certool --genkey --privkey=ssl-key.priv --pubkey=ssl-key.pub
```

The `ssl-key.priv` and `ssl-key.pub` files are created in the current directory.

3 Generate the new machine SSL certificate. This certificate is signed by VMCA. If you replaced the VMCA root certificate with custom certificate, VMCA signs all certificates with the full chain.

```
/usr/lib/vmware-vmca/bin/certool --gencert --cert=new-vmca-ssl.crt --privkey=ssl-key.priv
--config=ssl-config.cfg
```

The `new-vmca-ssl.crt` file is created in the current directory.

4 (Optional) List the content of VECS.

```
/usr/lib/vmware-vmafd/bin/vecs-cli store list
```

- Sample output on vCenter Server:

```
output (on vCenter):
MACHINE_SSL_CERT
TRUSTED_ROOTS
TRUSTED_ROOT_CRLS
machine
vsphere-webclient
vpxd
vpxd-extension
hvc
data-encipherment
APPLMGMT_PASSWORD
SMS
wcp
KMS_ENCRYPTION
```

5 Replace the Machine SSL certificate in VECS with the new Machine SSL certificate. The `--store` and `--alias` values have to exactly match with the default names.

- On each vCenter Server, run the following commands to update the Machine SSL certificate in the MACHINE_SSL_CERT store. You must update the certificate for each machine separately because each has a different FQDN.

```
/usr/lib/vmware-vmafd/bin/vecs-cli entry delete --store MACHINE_SSL_CERT --alias
__MACHINE_CERT
/usr/lib/vmware-vmafd/bin/vecs-cli entry create --store MACHINE_SSL_CERT --alias
__MACHINE_CERT --cert new-vmca-ssl.crt --key ssl-key.priv
```

What to do next

You can also replace the certificates for your ESXi hosts. See the *vSphere Security* publication.

Replace Solution User Certificates with New VMCA-Signed Certificates

After you replace the machine SSL certificates, you can replace all solution user certificates. Solution user certificates must be valid, that is, not expired, but none of the other information in the certificate is used by the certificate infrastructure.

Many VMware customers do not replace solution user certificates. They replace only the machine SSL certificates with custom certificates. This hybrid approach satisfies the requirements of their security teams.

- Certificates either sit behind a proxy, or they are custom certificates.
- No intermediate CAs are used.

You replace the machine solution user certificate and the solution user certificate on each vCenter Server system.

Note When you list solution user certificates in large deployments, the output of `dir-cli list` includes all solution users from all nodes. Run `vmafd-cli get-machine-id --server-name localhost` to find the local machine ID for each host. Each solution user name includes the machine ID.

Prerequisites

Be prepared to stop all services and to start the services that handle certificate propagation and storage.

Procedure

1. Make one copy of `certool.cfg`, remove the Name, IP address, DNS name, and email fields, and rename the file, for example, to `sol_usr.cfg`.

   You can name the certificates from the command line as part of generation. The other information is not needed for solution users. If you leave the default information, the certificates that are generated are potentially confusing.

2. Generate a public/private key file pair and a certificate for each solution user, passing in the configuration file that you just customized.

   For example:

   ```
   certool --genkey --privkey=vpxd.priv --pubkey=vpxd.pub
   certool --gencert --privkey=vpxd.priv --cert vpxd.crt --Name=VPXD_1 --config sol_usr.cfg
   ```

3. Find the name for each solution user.

   ```
   dir-cli service list
   ```

   You can use the unique ID that is returned when you replace the certificates. The input and output might look as follows.

   ```
   dir-cli service list
   Enter password for administrator@vsphere.local:
   1. machine-623bef28-0311-436e-b21f-6e0d39aa5179
   2. vsphere-webclient-623bef28-0311-436e-b21f-6e0d39aa5179
   ```

```
3. vpxd-623bef28-0311-436e-b21f-6e0d39aa5179
4. vpxd-extension-623bef28-0311-436e-b21f-6e0d39aa5179
5. hvc-623bef28-0311-436e-b21f-6e0d39aa5179
6. wcp-1cbe0a40-e4ce-4378-b5e7-9460e2b8200e
```

In a deployment of multiple vCenter Server instances connected in Enhanced Linked Mode configuration, the output of `dir-cli service list` includes all solution users from all nodes. Run `vmafd-cli get-machine-id --server-name localhost` to find the local machine ID for each host. Each solution user name includes the machine ID.

4 Stop all services and start the services that handle certificate creation, propagation, and storage.

```
service-control --stop --all
service-control --start vmafdd
service-control --start vmdird
service-control --start vmcad
```

5 For each solution user, replace the existing certificate in vmdir and then in VECS.

The following example shows how to replace the certificates for the vpxd service.

```
dir-cli service update --name <vpxd-xxxx-xxx-7c7b769cd9f4> --cert ./vpxd.crt
vecs-cli entry delete --store vpxd --alias vpxd
vecs-cli entry create --store vpxd --alias vpxd --cert vpxd.crt --key vpxd.priv
```

Note Solution users cannot authenticate to vCenter Single Sign-On if you do not replace the certificate in vmdir.

6 Restart all services.

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

Example: Using VMCA-Signed Solution User Certificates

1 Generate a public/private key pair for each solution user on each vCenter Server node in an Enhanced Linked Mode configuration. That includes a pair for the machine solution and a pair for each additional solution user (vpxd, vpxd-extension, vsphere-webclient, wcp).

a Generate a key pair for the machine solution user.

```
/usr/lib/vmware-vmca/bin/certool --genkey --privkey=machine-key.priv --pubkey=machine-key.pub
```

b Generate a key pair for the vpxd solution user on each node.

```
/usr/lib/vmware-vmca/bin/certool --genkey --privkey=vpxd-key.priv --pubkey=vpxd-key.pub
```

c Generate a key pair for the vpxd-extension solution user on each node.

```
/usr/lib/vmware-vmca/bin/certool --genkey --privkey=vpxd-extension-key.priv --
pubkey=vpxd-extension-key.pub
```

d Generate a key pair for the vsphere-webclient solution user on each node.

```
/usr/lib/vmware-vmca/bin/certool --genkey --privkey=vsphere-webclient-key.priv --
pubkey=vsphere-webclient-key.pub
```

e Generate a key pair for the wcp solution user on each node.

```
/usr/lib/vmware-vmca/bin/certool --genkey --privkey=wcp-key.priv --pubkey=wcp-key.pub
```

2 Generate solution user certificates that are signed by the new VMCA root certificate for the machine solution user and for each additional solution user (vpxd, vpxd-extension, vsphere-webclient, wcp) on each vCenter Server node.

Note The `--Name` parameter has to be unique. Including the name of the solution user store name makes it easy to see which certificate maps to which solution user. The example includes the name, for example `vpxd` or `vpxd-extension` in each case.

a Run the following command to generate a solution user certificate for the machine solution user on that node.

```
/usr/lib/vmware-vmca/bin/certool --gencert --cert=new-machine.crt --privkey=machine-
key.priv --Name=machine
```

b Generate a certificate for the machine solution user on each node.

```
/usr/lib/vmware-vmca/bin/certool --gencert --cert=new-machine.crt --privkey=machine-
key.priv --Name=machine
```

c Generate a certificate for the vpxd solution user on each node.

```
/usr/lib/vmware-vmca/bin/certool --gencert --cert=new-vpxd.crt --privkey=vpxd-key.priv
--Name=vpxd
```

d Generate a certificate for the vpxd-extensions solution user on each node.

```
/usr/lib/vmware-vmca/bin/certool --gencert --cert=new-vpxd-extension.crt --
privkey=vpxd-extension-key.priv --Name=vpxd-extension
```

e Generate a certificate for the vsphere-webclient solution user on each node by running the following command.

```
/usr/lib/vmware-vmca/bin/certool --gencert --cert=new-vsphere-webclient.crt --
privkey=vsphere-webclient-key.priv --Name=vsphere-webclient
```

f Generate a certificate for the wcp solution user on each node by running the following commands.

```
/usr/lib/vmware-vmca/bin/certool --gencert --cert=new-wcp.crt --privkey=wcp-key.priv --
Name=wcp
```

3 Replace the solution user certificates in VECS with the new solution user certificates.

Note The `--store` and `--alias` parameters have to exactly match the default names for services.

a Replace the machine solution user certificate on each node:

```
/usr/lib/vmware-vmafd/bin/vecs-cli entry delete --store machine --alias machine
/usr/lib/vmware-vmafd/bin/vecs-cli entry create --store machine --alias machine --cert
new-machine-vc.crt --key machine-vc-key.priv
```

b Replace the vpxd solution user certificate on each node.

```
/usr/lib/vmware-vmafd/bin/vecs-cli entry delete --store vpxd --alias vpxd
/usr/lib/vmware-vmafd/bin/vecs-cli entry create --store vpxd --alias vpxd --cert new-
vpxd.crt --key vpxd-key.priv
```

c Replace the vpxd-extension solution user certificate on each node.

```
/usr/lib/vmware-vmafd/bin/vecs-cli entry delete --store vpxd-extension --alias vpxd-
extension
/usr/lib/vmware-vmafd/bin/vecs-cli entry create --store vpxd-extension --alias vpxd-
extension --cert new-vpxd-extension.crt --key vpxd-extension-key.priv
```

d Replace the vsphere-webclient solution user certificate on each node.

```
/usr/lib/vmware-vmafd/bin/vecs-cli entry delete --store vsphere-webclient --alias
vsphere-webclient
/usr/lib/vmware-vmafd/bin/vecs-cli entry create --store vsphere-webclient --alias
vsphere-webclient --cert new-vsphere-webclient.crt --key vsphere-webclient-key.priv
```

e Replace the wcp solution user certificate on each node.

```
/usr/lib/vmware-vmafd/bin/vecs-cli entry delete --store wcp --alias wcp
/usr/lib/vmware-vmafd/bin/vecs-cli entry create --store wcp --alias wcp --cert new-
wcp.crt --key wcp-key.priv
```

4 Update VMware Directory Service (vmdir) with the new solution user certificates. You are prompted for a vCenter Single Sign-On administrator password.

a Run `dir-cli service list` to get the unique service ID suffix for each solution user. You run this command on a vCenter Server system.

```
/usr/lib/vmware-vmafd/bin/dir-cli service list
output:
1. machine-623bef28-0311-436e-b21f-6e0d39aa5179
```

```
2. vsphere-webclient-623bef28-0311-436e-b21f-6e0d39aa5179
3. vpxd-623bef28-0311-436e-b21f-6e0d39aa5179
4. vpxd-extension-623bef28-0311-436e-b21f-6e0d39aa5179
5. hvc-623bef28-0311-436e-b21f-6e0d39aa5179
6. wcp-1cbe0a40-e4ce-4378-b5e7-9460e2b8200e
```

Note When you list solution user certificates in large deployments, the output of `dir-cli list` includes all solution users from all nodes. Run `vmafd-cli get-machine-id --server-name localhost` to find the local machine ID for each host. Each solution user name includes the machine ID.

b Replace the machine certificate in vmdir on each vCenter Server node. For example, if machine-6fd7f140-60a9-11e4-9e28-005056895a69 is the machine solution user on the vCenter Server, run this command:

```
/usr/lib/vmware-vmafd/bin/dir-cli service update --name
machine-6fd7f140-60a9-11e4-9e28-005056895a69 --cert new-machine-2.crt
```

c Replace the vpxd solution user certificate in vmdir on each node. For example, if vpxd-6fd7f140-60a9-11e4-9e28-005056895a69 is the vpxd solution user ID, run this command:

```
/usr/lib/vmware-vmafd/bin/dir-cli service update --name
vpxd-6fd7f140-60a9-11e4-9e28-005056895a69 --cert new-vpxd.crt
```

d Replace the vpxd-extension solution user certificate in vmdir on each node. For example, if vpxd-extension-6fd7f140-60a9-11e4-9e28-005056895a69 is the vpxd-extension solution user ID, run this command:

```
/usr/lib/vmware-vmafd/bin/dir-cli update --name vpxd-
extension-6fd7f140-60a9-11e4-9e28-005056895a69 --cert new-vpxd-extension.crt
```

e Replace the vsphere-webclient solution user certificate on each node. For example, if vsphere-webclient-6fd7f140-60a9-11e4-9e28-005056895a69 is the vsphere-webclient solution user ID, run this command:

```
/usr/lib/vmware-vmafd/bin/dir-cli service update --name vsphere-
webclient-6fd7f140-60a9-11e4-9e28-005056895a69 --cert new-vsphere-webclient.crt
```

f Replace the wcp solution user certificate on each node. For example, if wcp-1cbe0a40-e4ce-4378-b5e7-9460e2b8200e is the wcp solution user ID, run this command:

```
/usr/lib/vmware-vmafd/bin/dir-cli service update --name wcp-1cbe0a40-e4ce-4378-
b5e7-9460e2b8200e --cert new-wcp.crt
```

What to do next

Restart all services on each vCenter Server node.

Use VMCA as an Intermediate Certificate Authority

You can replace the VMCA root certificate with a third-party CA-signed certificate that includes VMCA in the certificate chain. Going forward, all certificates that VMCA generates include the full chain. You can replace existing certificates with newly generated certificates.

If you use VMCA as an intermediate CA, or use custom certificates, you might encounter significant complexity and the potential for a negative impact to your security, and an unnecessary increase in your operational risk. For more information about managing certificates within a vSphere environment, see the blog post titled *New Product Walkthrough - Hybrid vSphere SSL Certificate Replacement* at http://vmware.com/go/hybridvmca.

Replace the Root Certificate (Intermediate CA)

The first step in replacing the VMCA certificates with custom certificates is generating a CSR, and sending the CSR to be signed. You then add the signed certificate to VMCA as a root certificate.

You can use the Certificate Manager utility or other tool to generate the CSR. The CSR must meet the following requirements:

- Key size: 2048 bits (minimum) to 16384 bits (maximum) (PEM encoded)
- PEM format. VMware supports PKCS8 and PKCS1 (RSA keys). When keys are added to VECS, they are converted to PKCS8.
- x509 version 3
- The CA extension must be set to true for root certificates, and cert sign must be in the list of requirements. For example:

```
basicConstraints        = critical,CA:true
keyUsage                = critical,digitalSignature,keyCertSign
```

- CRL signing must be enabled.
- Extended Key Usage can be either empty or contain Server Authentication.
- No explicit limit to the length of the certificate chain. VMCA uses the OpenSSL default, which is 10 certificates.
- Certificates with wildcards or with more than one DNS name are not supported.
- You cannot create subsidiary CAs of VMCA.

  See the VMware knowledge base article at http://kb.vmware.com/kb/2112009, Creating a Microsoft Certificate Authority Template for SSL certificate creation in vSphere 6.x, for an example using Microsoft Certificate Authority.

VMCA validates the following certificate attributes when you replace the root certificate:

- Key size: 2048 bits (minimum) to 16384 bits (maximum)
- Key Usage: Cert Sign
- Basic Constraint: Subject Type CA

Procedure

1 Generate a CSR and send it to your CA.

   Follow your CA's instructions.

2 Prepare a certificate file that includes the signed VMCA certificate and the full CA chain of your third-party CA or enterprise CA. Save the file, for example as `rootca1.crt`.

   You can accomplish this step by copying all CA certificates in PEM format into a single file. You start with the VMCA root certificate and end up with the root CA PEM certificate. For example:

```
-----BEGIN CERTIFICATE-----
<Certificate of VMCA>
-----END CERTIFICATE-----
-----BEGIN CERTIFICATE-----
<Certificate of intermediary CA>
-----END CERTIFICATE-----
-----BEGIN CERTIFICATE-----
<Certificate of Root CA>
-----END CERTIFICATE-----
```

3 Stop all services and start the services that handle certificate creation, propagation, and storage.

```
service-control --stop --all
service-control --start vmafdd
service-control --start vmdird
service-control --start vmcad
```

4 Replace the existing VMCA root CA.

```
certool --rootca --cert=rootca1.crt --privkey=root1.key
```

   When you run this command, it:

   - Adds the new custom root certificate to the certificate location in the file system.
   - Appends the custom root certificate to the TRUSTED_ROOTS store in VECS (after a delay).
   - Adds the custom root certificate to vmdir (after a delay).

5 (Optional) To propagate the change to all instances of vmdir (VMware Directory Service), publish the new root certificate to vmdir, supplying the full file path for each file.

   For example, if the certificate has only one certificate in the chain:

```
dir-cli trustedcert publish --cert rootca1.crt
```

   If the certificate has more than one certificate in the chain:

```
dir-cli trustedcert publish --cert rootca1.crt --chain
```

Replication between vmdir nodes happens every 30 seconds. You do not have to add the root certificate to VECS explicitly because VECS polls vmdir for new root certificate files every 5 minutes.

6 (Optional) If necessary, you can force a refresh of VECS.

```
vecs-cli force-refresh
```

7 Restart all services.

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

Example: Replacing the Root Certificate

Replace the VMCA root certificate with the custom CA root certificate using the `certool` command with the `--rootca` option.

```
/usr/lib/vmware-vmca/bin/certool --rootca --cert=<path>/root.pem --privkey=<path>/root.key
```

When you run this command, it:

- Adds the new custom root certificate to the certificate location in the file system.
- Appends the custom root certificate to the TRUSTED_ROOTS store in VECS.
- Adds the custom root certificate to vmdir.

What to do next

You can remove the original VMCA root certificate from the certificate store if your company policy requires it. If you do, you have to replace the vCenter Single Sign-On Signing certificate. See Replace a vCenter Server STS Certificate Using the Command Line.

Replace Machine SSL Certificates (Intermediate CA)

After you have received the signed certificate from the CA and made it the VMCA root certificate, you can replace all machine SSL certificates.

These steps are essentially the same as the steps for replacing with a certificate that uses VMCA as the certificate authority. However, in this case, VMCA signs all certificates with the full chain.

Each machine must have a machine SSL certificate for secure communication with other services. When multiple vCenter Server instances are connected in Enhanced Linked Mode configuration, you must run the Machine SSL certificate generation commands on each node.

Prerequisites

For each machine SSL certificate, the `SubjectAltName` must contain `DNS Name=<Machine FQDN>`.

Procedure

1 Make one copy of `certool.cfg` for each machine that needs a new certificate.

The `certool.cfg` file is located in the `/usr/lib/vmware-vmca/share/config/` directory.

2 Edit the custom configuration file for each machine to include that machine's FQDN.

Run `NSLookup` against the machine's IP address to see the DNS listing of the name, and use that name for the Hostname field in the file.

3 Generate a public/private key file pair and a certificate for each machine, passing in the configuration file that you just customized.

For example:

```
certool --genkey --privkey=machine1.priv --pubkey=machine1.pub
certool --gencert --privkey=machine1.priv --cert machine42.crt --Name=Machine42_Cert --
config machine1.cfg
```

4 Stop all services and start the services that handle certificate creation, propagation, and storage.

```
service-control --stop --all
service-control --start vmafdd
service-control --start vmdird
service-control --start vmcad
```

5 Add the new certificate to VECS.

All machines need the new certificate in the local certificate store to communicate over SSL. You first delete the existing entry, then add the new entry.

```
vecs-cli entry delete --store MACHINE_SSL_CERT --alias __MACHINE_CERT
vecs-cli entry create --store MACHINE_SSL_CERT --alias __MACHINE_CERT --cert machine1.cert
--key machine1.priv
```

6 Restart all services.

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

Example: Replacing Machine SSL Certificates (VMCA Is Intermediate CA)

1 Create a configuration file for the SSL certificate and save it as `ssl-config.cfg` in the current directory.

```
Country = US
Name = vmca-<FQDN-example>
Organization = VMware
OrgUnit = VMware Engineering
State = California
Locality = Palo Alto
Hostname = <FQDN>
```

2 Generate a key pair for the machine SSL certificate. In a deployment of multiple vCenter Server instances connected in Enhanced Linked Mode configuration, run this command on each vCenter Server node.

```
/usr/lib/vmware-vmca/bin/certool --genkey --privkey=ssl-key.priv --pubkey=ssl-key.pub
```

The `ssl-key.priv` and `ssl-key.pub` files are created in the current directory.

3 Generate the new machine SSL certificate. This certificate is signed by VMCA. If you replaced the VMCA root certificate with custom certificate, VMCA signs all certificates with the full chain.

```
/usr/lib/vmware-vmca/bin/certool --gencert --cert=new-vmca-ssl.crt --privkey=ssl-key.priv
--config=ssl-config.cfg
```

The `new-vmca-ssl.crt` file is created in the current directory.

4 (Optional) List the content of VECS.

```
/usr/lib/vmware-vmafd/bin/vecs-cli store list
```

- Sample output on vCenter Server:

```
output (on vCenter):
MACHINE_SSL_CERT
TRUSTED_ROOTS
TRUSTED_ROOT_CRLS
machine
vsphere-webclient
vpxd
vpxd-extension
hvc
data-encipherment
APPLMGMT_PASSWORD
SMS
wcp
KMS_ENCRYPTION
```

5 Replace the Machine SSL certificate in VECS with the new Machine SSL certificate. The `--store` and `--alias` values have to exactly match with the default names.

- On each vCenter Server, run the following commands to update the Machine SSL certificate in the MACHINE_SSL_CERT store. You must update the certificate for each machine separately because each has a different FQDN.

```
/usr/lib/vmware-vmafd/bin/vecs-cli entry delete --store MACHINE_SSL_CERT --alias
__MACHINE_CERT
/usr/lib/vmware-vmafd/bin/vecs-cli entry create --store MACHINE_SSL_CERT --alias
__MACHINE_CERT --cert new-vmca-ssl.crt --key ssl-key.priv
```

Replace Solution User Certificates (Intermediate CA)

After you replace the machine SSL certificates, you can replace the solution user certificates.

Many VMware customers do not replace solution user certificates. They replace only the machine SSL certificates with custom certificates. This hybrid approach satisfies the requirements of their security teams.

- Certificates either sit behind a proxy, or they are custom certificates.
- No intermediate CAs are used.

You replace the machine solution user certificate and the solution user certificate on each vCenter Server system.

Note When you list solution user certificates in large deployments, the output of `dir-cli list` includes all solution users from all nodes. Run `vmafd-cli get-machine-id --server-name localhost` to find the local machine ID for each host. Each solution user name includes the machine ID.

Prerequisites

Each solution user certificate must have a different `Subject`. Consider, for example, including the solution user name (such as vpxd) or other unique identifier.

Procedure

1. Make one copy of `certool.cfg`, remove the Name, IP address, DNS name, and email fields, and rename the file, for example, to `sol_usr.cfg`.

   You can name the certificates from the command line as part of generation. The other information is not needed for solution users. If you leave the default information, the certificates that are generated are potentially confusing.

2. Generate a public/private key file pair and a certificate for each solution user, passing in the configuration file that you just customized.

   For example:

   ```
   certool --genkey --privkey=vpxd.priv --pubkey=vpxd.pub
   certool --gencert --privkey=vpxd.priv --cert vpxd.crt --Name=VPXD_1 --config sol_usr.cfg
   ```

3. Find the name for each solution user.

   ```
   dir-cli service list
   ```

   You can use the unique ID that is returned when you replace the certificates. The input and output might look as follows.

   ```
   dir-cli service list
   Enter password for administrator@vsphere.local:
   1. machine-623bef28-0311-436e-b21f-6e0d39aa5179
   2. vsphere-webclient-623bef28-0311-436e-b21f-6e0d39aa5179
   ```

```
3. vpxd-623bef28-0311-436e-b21f-6e0d39aa5179
4. vpxd-extension-623bef28-0311-436e-b21f-6e0d39aa5179
5. hvc-623bef28-0311-436e-b21f-6e0d39aa5179
6. wcp-1cbe0a40-e4ce-4378-b5e7-9460e2b8200e
```

In a deployment of multiple vCenter Server instances connected in Enhanced Linked Mode configuration, the output of `dir-cli service list` includes all solution users from all nodes. Run `vmafd-cli get-machine-id --server-name localhost` to find the local machine ID for each host. Each solution user name includes the machine ID.

4 Stop all services and start the services that handle certificate creation, propagation, and storage.

```
service-control --stop --all
service-control --start vmafdd
service-control --start vmdird
service-control --start vmcad
```

5 Replace the existing certificate in vmdir and then in VECS.

For solution users, you must add the certificates in that order. For example:

```
dir-cli service update --name <vpxd-xxxx-xxx-7c7b769cd9f4> --cert ./vpxd.crt
vecs-cli entry delete --store vpxd --alias vpxd
vecs-cli entry create --store vpxd --alias vpxd --cert vpxd.crt --key vpxd.priv
```

Note Solution users cannot log in to vCenter Single Sign-On if you do not replace the certificate in vmdir.

6 Restart all services.

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

Example: Replacing Solution User Certificates (Intermediate CA)

1 Generate a public/private key pair for each solution user on each vCenter Server node in an Enhanced Linked Mode configuration. That includes a pair for the machine solution and a pair for each additional solution user (vpxd, vpxd-extension, vsphere-webclient, wcp).

a Generate a key pair for the machine solution user.

```
/usr/lib/vmware-vmca/bin/certool --genkey --privkey=machine-key.priv --pubkey=machine-key.pub
```

b Generate a key pair for the vpxd solution user on each node.

```
/usr/lib/vmware-vmca/bin/certool --genkey --privkey=vpxd-key.priv --pubkey=vpxd-key.pub
```

c Generate a key pair for the vpxd-extension solution user on each node.

```
/usr/lib/vmware-vmca/bin/certool --genkey --privkey=vpxd-extension-key.priv --
pubkey=vpxd-extension-key.pub
```

d Generate a key pair for the vsphere-webclient solution user on each node.

```
/usr/lib/vmware-vmca/bin/certool --genkey --privkey=vsphere-webclient-key.priv --
pubkey=vsphere-webclient-key.pub
```

e Generate a key pair for the wcp solution user on each node.

```
/usr/lib/vmware-vmca/bin/certool --genkey --privkey=wcp-key.priv --pubkey=wcp-key.pub
```

2 Generate solution user certificates that are signed by the new VMCA root certificate for the machine solution user and for each additional solution user (vpxd, vpxd-extension, vsphere-webclient, wcp) on each vCenter Server node.

Note The `--Name` parameter has to be unique. Including the name of the solution user store name makes it easy to see which certificate maps to which solution user. The example includes the name, for example `vpxd` or `vpxd-extension` in each case.

a Run the following command to generate a solution user certificate for the machine solution user on that node.

```
/usr/lib/vmware-vmca/bin/certool --gencert --cert=new-machine.crt --privkey=machine-
key.priv --Name=machine
```

b Generate a certificate for the machine solution user on each node.

```
/usr/lib/vmware-vmca/bin/certool --gencert --cert=new-machine.crt --privkey=machine-
key.priv --Name=machine
```

c Generate a certificate for the vpxd solution user on each node.

```
/usr/lib/vmware-vmca/bin/certool --gencert --cert=new-vpxd.crt --privkey=vpxd-key.priv
--Name=vpxd
```

d Generate a certificate for the vpxd-extensions solution user on each node.

```
/usr/lib/vmware-vmca/bin/certool --gencert --cert=new-vpxd-extension.crt --
privkey=vpxd-extension-key.priv --Name=vpxd-extension
```

e Generate a certificate for the vsphere-webclient solution user on each node by running the following command.

```
/usr/lib/vmware-vmca/bin/certool --gencert --cert=new-vsphere-webclient.crt --
privkey=vsphere-webclient-key.priv --Name=vsphere-webclient
```

f Generate a certificate for the wcp solution user on each node by running the following commands.

```
/usr/lib/vmware-vmca/bin/certool --gencert --cert=new-wcp.crt --privkey=wcp-key.priv --
Name=wcp
```

3 Replace the solution user certificates in VECS with the new solution user certificates.

Note The `--store` and `--alias` parameters have to exactly match the default names for services.

a Replace the machine solution user certificate on each node:

```
/usr/lib/vmware-vmafd/bin/vecs-cli entry delete --store machine --alias machine
/usr/lib/vmware-vmafd/bin/vecs-cli entry create --store machine --alias machine --cert
new-machine-vc.crt --key machine-vc-key.priv
```

b Replace the vpxd solution user certificate on each node.

```
/usr/lib/vmware-vmafd/bin/vecs-cli entry delete --store vpxd --alias vpxd
/usr/lib/vmware-vmafd/bin/vecs-cli entry create --store vpxd --alias vpxd --cert new-
vpxd.crt --key vpxd-key.priv
```

c Replace the vpxd-extension solution user certificate on each node.

```
/usr/lib/vmware-vmafd/bin/vecs-cli entry delete --store vpxd-extension --alias vpxd-
extension
/usr/lib/vmware-vmafd/bin/vecs-cli entry create --store vpxd-extension --alias vpxd-
extension --cert new-vpxd-extension.crt --key vpxd-extension-key.priv
```

d Replace the vsphere-webclient solution user certificate on each node.

```
/usr/lib/vmware-vmafd/bin/vecs-cli entry delete --store vsphere-webclient --alias
vsphere-webclient
/usr/lib/vmware-vmafd/bin/vecs-cli entry create --store vsphere-webclient --alias
vsphere-webclient --cert new-vsphere-webclient.crt --key vsphere-webclient-key.priv
```

e Replace the wcp solution user certificate on each node.

```
/usr/lib/vmware-vmafd/bin/vecs-cli entry delete --store wcp --alias wcp
/usr/lib/vmware-vmafd/bin/vecs-cli entry create --store wcp --alias wcp --cert new-
wcp.crt --key wcp-key.priv
```

4 Update VMware Directory Service (vmdir) with the new solution user certificates. You are prompted for a vCenter Single Sign-On administrator password.

a Run `dir-cli service list` to get the unique service ID suffix for each solution user. You run this command on a vCenter Server system.

```
/usr/lib/vmware-vmafd/bin/dir-cli service list
output:
1. machine-623bef28-0311-436e-b21f-6e0d39aa5179
```

```
2. vsphere-webclient-623bef28-0311-436e-b21f-6e0d39aa5179
3. vpxd-623bef28-0311-436e-b21f-6e0d39aa5179
4. vpxd-extension-623bef28-0311-436e-b21f-6e0d39aa5179
5. hvc-623bef28-0311-436e-b21f-6e0d39aa5179
6. wcp-1cbe0a40-e4ce-4378-b5e7-9460e2b8200e
```

Note When you list solution user certificates in large deployments, the output of `dir-cli list` includes all solution users from all nodes. Run `vmafd-cli get-machine-id --server-name localhost` to find the local machine ID for each host. Each solution user name includes the machine ID.

b Replace the machine certificate in vmdir on each vCenter Server node. For example, if machine-6fd7f140-60a9-11e4-9e28-005056895a69 is the machine solution user on the vCenter Server, run this command:

```
/usr/lib/vmware-vmafd/bin/dir-cli service update --name
machine-6fd7f140-60a9-11e4-9e28-005056895a69 --cert new-machine-2.crt
```

c Replace the vpxd solution user certificate in vmdir on each node. For example, if vpxd-6fd7f140-60a9-11e4-9e28-005056895a69 is the vpxd solution user ID, run this command:

```
/usr/lib/vmware-vmafd/bin/dir-cli service update --name
vpxd-6fd7f140-60a9-11e4-9e28-005056895a69 --cert new-vpxd.crt
```

d Replace the vpxd-extension solution user certificate in vmdir on each node. For example, if vpxd-extension-6fd7f140-60a9-11e4-9e28-005056895a69 is the vpxd-extension solution user ID, run this command:

```
/usr/lib/vmware-vmafd/bin/dir-cli update --name vpxd-
extension-6fd7f140-60a9-11e4-9e28-005056895a69 --cert new-vpxd-extension.crt
```

e Replace the vsphere-webclient solution user certificate on each node. For example, if vsphere-webclient-6fd7f140-60a9-11e4-9e28-005056895a69 is the vsphere-webclient solution user ID, run this command:

```
/usr/lib/vmware-vmafd/bin/dir-cli service update --name vsphere-
webclient-6fd7f140-60a9-11e4-9e28-005056895a69 --cert new-vsphere-webclient.crt
```

f Replace the wcp solution user certificate on each node. For example, if wcp-1cbe0a40-e4ce-4378-b5e7-9460e2b8200e is the wcp solution user ID, run this command:

```
/usr/lib/vmware-vmafd/bin/dir-cli service update --name wcp-1cbe0a40-e4ce-4378-
b5e7-9460e2b8200e --cert new-wcp.crt
```

Use Custom Certificates with vSphere

If your company policy requires it, you can replace some or all certificates used in vSphere with certificates that are signed by a third-party or enterprise CA. If you do that, VMCA is not in your certificate chain. You are responsible for storing all vCenter certificates in VECS.

You can replace all certificates or use a hybrid solution. For example, consider replacing all certificates that are used for network traffic but leaving VMCA-signed solution user certificates. Solution user certificates are used only for authentication to vCenter Single Sign-On. vCenter Server uses solution user certificates for internal communication only. Solution user certificates are not used for external communication.

Note If you do not want to use VMCA, you are responsible for replacing all certificates yourself, for provisioning new components with certificates, and for tracking certificate expiration.

Even if you decide to use custom certificates, you can still use the VMware Certificate Manager utility for certificate replacement. See Replace All Certificates with Custom Certificate (Certificate Manager).

If you encounter problems with vSphere Auto Deploy after replacing certificates, see the VMware knowledge base article at http://kb.vmware.com/kb/2000988.

Request Certificates and Import a Custom Root Certificate

You can use custom certificates from an enterprise or third-party CA. The first step is requesting the certificates from the certificate authority and importing the root certificates into VMware Endpoint Certificate Store (VECS).

Prerequisites

The certificate must meet the following requirements:

- Key size: 2048 bits (minimum) to 16384 bits (maximum) (PEM encoded)
- PEM format. VMware supports PKCS8 and PKCS1 (RSA keys). When keys are added to VECS, they are converted to PKCS8.
- x509 version 3
- For root certificates, the CA extension must be set to true, and the cert sign must be in the list of requirements.
- SubjectAltName must contain DNS Name=<machine_FQDN>.
- CRT format
- Contains the following Key Usages: Digital Signature, Key Encipherment
- Start time of one day before the current time.
- CN (and SubjectAltName) set to the host name (or IP address) that the ESXi host has in the vCenter Server inventory.

Procedure

1. Send the Certificate Signing Requests (CSRs) for the following certificates to your enterprise or third-party certificate provider.
   - A machine SSL certificate for each machine. For the machine SSL certificate, the SubjectAltName field must contain the fully qualified domain name (DNS NAME=*machine_FQDN*).
   - Optionally, five solution user certificates for each node. Solution user certificates do not need to include IP address, host name, or email address. Each certificate must have a different certificate Subject.

   Typically, the result is a PEM file for the trusted chain, plus the signed SSL certificates for each vCenter Server node.
2. List the TRUSTED_ROOTS and the machine SSL stores.

   ```
   vecs-cli store list
   ```

   a. Ensure that the current root certificate and all machine SSL certificates are signed by VMCA.

   b. Note down the Serial number, issuer, and Subject CN fields.

   c. (Optional) With a Web browser, open an HTTPS connection to a node where the certificate is to be replaced, view the certificate information, and ensure that it matches the machine SSL certificate.
3. Stop all services and start the services that handle certificate creation, propagation, and storage.

   ```
   service-control --stop --all
   service-control --start vmafdd
   service-control --start vmdird
   service-control --start vmcad
   ```
4. Publish the custom root certificate.

   ```
   dir-cli trustedcert publish --cert <my_custom_root>
   ```

   If you do not specify a user name and password on the command line, you are prompted.
5. Restart all services.

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

What to do next

You can remove the original VMCA root certificate from the certificate store if your company policy requires it. If you do, you have to refresh the vCenter Single Sign-On certificate. See Replace a vCenter Server STS Certificate Using the Command Line.

Replace Machine SSL Certificates with Custom Certificates

After you receive the custom certificates, you can replace each machine certificate.

You must have the following information before you can start replacing the certificates:

- Password for administrator@vsphere.local
- Valid Machine SSL custom certificate (`.crt` file)
- Valid Machine SSL custom key (`.key` file)
- Valid custom certificate for Root (`.crt` file)

Prerequisites

You must have received a certificate for each machine from your third-party or enterprise CA.

- Key size: 2048 bits (minimum) to 16384 bits (maximum) (PEM encoded)
- CRT format
- x509 version 3
- SubjectAltName must contain DNS Name=<machine_FQDN>.
- Contains the following Key Usages: Digital Signature, Key Encipherment

Procedure

1. Stop all services and start the services that handle certificate creation, propagation, and storage.

   ```
   service-control --stop --all
   service-control --start vmafdd
   service-control --start vmdird
   service-control --start vmcad
   ```

2. Log in to each node and add the new machine certificates that you received from the CA to VECS.

   All machines need the new certificate in the local certificate store to communicate over SSL.

   ```
   vecs-cli entry delete --store MACHINE_SSL_CERT --alias __MACHINE_CERT
   vecs-cli entry create --store MACHINE_SSL_CERT --alias __MACHINE_CERT --cert <cert-file-
   path>
   --key <key-file-path>
   ```

3. Update the lookup service registration endpoint.

   ```
   /usr/lib/vmware-lookupsvc/tools/ls_update_certs.py --url https://<vCenterServer_FQDN>/
   lookupservice/sdk --certfile <cert-file-path> --user 'administrator@vsphere.local' --
   password '<password>' --fingerprint <SHA1_hash_of_the_old_certificate_to_replace>
   ```

4 Restart all services.

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

Managing Services and Certificates with CLI Commands

3

You can manage VMCA (VMware Certificate Authority), VECS (VMware Endpoint Certificate Store), VMware Directory Service (vmdir), and Security Token Service (STS) certificates by using a set of CLIs. The vSphere Certificate Manager utility supports many related tasks as well, but the CLIs are required for manual certificate management and for managing other services.

You normally access the CLI tools for managing certificates and associated services by using SSH to connect to the appliance shell. See the VMware knowledge base article at http://kb.vmware.com/kb/2100508 for more information.

Manual Certificate Replacement gives examples for replacing certificates using CLI commands.

Table 3-1. CLI Tools for Managing Certificates and Associated Services

CLI	Description	See
`certool`	Generate and manage certificates and keys. Part of VMCAD, the VMware Certificate Management service.	certool Initialization Commands Reference
`vecs-cli`	Manage the contents of VMware Certificate Store instances. Part of VMware Authentication Framework Daemon (VMAFD).	vecs-cli Command Reference
`dir-cli`	Create and update certificates in VMware Directory Service. Part of VMAFD.	dir-cli Command Reference
`sso-config`	Manage STS certificates.	Command-line help.
`service-control`	Start or stop services, for example as part of a certificate replacement workflow.	Run this command to stop services before running other CLI commands.

CLI Locations

By default, you find the CLIs in the following locations.

```
/usr/lib/vmware-vmafd/bin/vecs-cli
/usr/lib/vmware-vmafd/bin/dir-cli
```

```
/usr/lib/vmware-vmca/bin/certool
/opt/vmware/bin/sso-config.sh
```

Note The `service-control` command does not require that you specify the path.

This chapter includes the following topics:

Required Privileges for Running CLIs

Required privileges depend on the CLI that you are using and on the command that you want to run. For example, for most certificate management operations, you have to be an Administrator for the local vCenter Single Sign-On domain (vsphere.local by default). Some commands are available for all users.

dir-cli

You must be a member of the Administrators group in the local domain (vsphere.local by default) to run `dir-cli` commands. If you do not specify a user name and password, you are prompted for the password for the administrator of the local vCenter Single Sign-On domain, administrator@vsphere.local by default.

vecs-cli

Initially, only the store owner and users with blanket access privileges have access to a store. Users in the Administrators group have blanket access privileges.

The MACHINE_SSL_CERT and TRUSTED_ROOTS stores are special stores. Only the root user or administrator user, depending on the type of installation, has complete access.

certool

Most of the `certool` commands require that the user is in the Administrators group. All users can run the following commands.

- `genselfcacert`
- `initscr`
- `getdc`
- `waitVMDIR`

- `waitVMCA`
- `genkey`
- `viewcert`

Changing the certool Configuration Options

When you run `certool --gencert` or certain other certificate initialization or management commands, the command reads all the values from a configuration file. You can edit the existing file, override the default configuration file with the `--config=<file name>` option, or override values on the command line.

The configuration file, `certool.cfg`, is located in the `/usr/lib/vmware-vmca/share/config/` directory by default.

The file has several fields with the following default values:

```
Country = US
Name= Acme
Organization = AcmeOrg
OrgUnit = AcmeOrg Engineering
State = California
Locality = Palo Alto
IPAddress = 127.0.0.1
Email = email@acme.com
Hostname = server.acme.com
```

You can change the values by specifying a modified file on the command line, or by overriding individual values on the command line, as follows.

- Create a copy of the configuration file and edit the file. Use the `--config` command-line option to specify the file. Specify the full path to avoid path name issues.
- ```
  /usr/lib/vmware-vmca/bin/certool --gencert --config /tmp/myconfig.cfg
  ```
- Override individual values on the command line. For example, to override Locality, run this command:

  ```
  /usr/lib/vmware-vmca/bin/certool --gencert --privkey=private.key --Locality="Mountain View"
  ```

Specify `--Name` to replace the CN field of the Subject name of the certificate.

- For solution user certificates, the name is <sol_user name>@<domain> by convention, but you can change the name if a different convention is used in your environment.
- For machine SSL certificates, the FQDN of the machine is used.

  VMCA allows only one DNSName (in the `Hostname` field) and no other Alias options. If the IP address is specified by the user, it is stored in SubAltName as well.
  ```

Use the `--Hostname` parameter to specify the DNSName of a certificate's SubAltName.

certool Initialization Commands Reference

The `certool` initialization commands allow you to generate certificate signing requests, view and generate certificates and keys that are signed by VMCA, import root certificates, and perform other certificate management operations.

In many cases, you pass a configuration file in to a `certool` command. See Changing the certool Configuration Options. See Replace Existing VMCA-Signed Certificates with New VMCA-Signed Certificates for some usage examples. The command-line help provides details about the options.

certool --initcsr

Generates a Certificate Signing Request (CSR). The command generates a PKCS10 file and a private key.

Option	Description
`--gencsr`	Required for generating CSRs.
`--privkey <key_file>`	Name of the private key file.
`--pubkey <key_file>`	Name of the public key file.
`--csrfile <csr_file>`	File name for the CSR file to be sent to the CA provider.
`--config <config_file>`	Optional name of the configuration file. Defaults to `certool.cfg`.

Example:

```
certool --gencsr --privkey=<filename> --pubkey=<filename> --csrfile=<filename>
```

certool --selfca

Creates a self-signed certificate and provisions the VMCA server with a self-signed root CA. Using this option is one of the simplest ways to provision the VMCA server. You can instead provision the VMCA server with a third-party root certificate so that VMCA is an intermediate CA. See Use VMCA as an Intermediate Certificate Authority.

This command generates a certificate that is predated by three days to avoid time zone conflicts.

Option	Description
`--selfca`	Required for generating a self-signed certificate.
`--predate <number_of_minutes>`	Allows you to set the Valid Not Before field of the root certificate to the specified number of minutes before the current time. This option can be helpful to account for potential time zone issues. The maximum is three days.

Option	Description
`--config <config_file>`	Optional name of the configuration file. Defaults to `certool.cfg`.
`--server <server>`	Optional name of the VMCA server. By default, the command uses localhost.

Example:

```
machine-70-59:/usr/lib/vmware-vmca/bin # ./certool --predate=2280  --selfca --server=
192.0.2.24 --srp-upn=administrator@vsphere.local
```

certool --rootca

Imports a root certificate. Adds the specified certificate and private key to VMCA. VMCA always uses the most recent root certificate for signing, but other root certificates remain trusted until you manually delete them. That means you can update your infrastructure one step at a time, and finally delete certificates that you no longer use.

Option	Description
`--rootca`	Required for importing a root CA.
`--cert <certfile>`	Name of the certificate file.
`--privkey <key_file>`	Name of the private key file. This file must be in PEM encoded format.
`--server <server>`	Optional name of the VMCA server. By default, the command uses localhost.

Example:

```
certool --rootca --cert=root.cert --privkey=privatekey.pem
```

certool --getdc

Returns the default domain name that is used by vmdir.

Option	Description
`--server <server>`	Optional name of the VMCA server. By default, the command uses localhost.
`--port <port_num>`	Optional port number. Defaults to port 389.

Example:

```
certool --getdc
```

certool --waitVMDIR

Wait until the VMware Directory Service is running or until the timeout specified by `--wait` has elapsed. Use this option along with other options to schedule certain tasks, for example returning the default domain name.

Option	Description
`--wait`	Optional number of minutes to wait. Defaults to 3.
`--server <server>`	Optional name of the VMCA server. By default, the command uses localhost.
`--port <port_num>`	Optional port number. Defaults to port 389.

Example:

```
certool --waitVMDIR --wait 5
```

certool --waitVMCA

Wait until the VMCA service is running or until the specified timeout has elapsed. Use this option in conjunction with other options to schedule certain tasks, for example, generating a certificate.

Option	Description
`--wait`	Optional number of minutes to wait. Defaults to 3.
`--server <server>`	Optional name of the VMCA server. By default, the command uses localhost.
`--port <port_num>`	Optional port number. Defaults to port 389.

Example:

```
certool --waitVMCA --selfca
```

certool --publish-roots

Forces an update of root certificates. This command requires administrative privileges.

Option	Description
`--server <server>`	Optional name of the VMCA server. By default, the command uses localhost.

Example:

```
certool --publish-roots
```

certool Management Commands Reference

The `certool` management commands allow you to view, generate, and revoke certificates and to view information about certificates.

certool --genkey

Generates a private and public key pair. Those files can then be used to generate a certificate that is signed by VMCA.

Option	Description
`--genkey`	Required for generating a private and public key.
`--privkey <keyfile>`	Name of the private key file.
`--pubkey <keyfile>`	Name of the public key file.
`--server <server>`	Optional name of the VMCA server. By default, the command uses localhost.

Example:

```
certool --genkey --privkey=<filename> --pubkey=<filename>
```

certool --gencert

Generates a certificate from the VMCA server. This command uses the information in `certool.cfg` or in the specified configuration file. You can use the certificate to provision machine certificates or solution user certificates.

Option	Description
`--gencert`	Required for generating a certificate.
`--cert <certfile>`	Name of the certificate file. This file must be in PEM encoded format.
`--privkey <keyfile>`	Name of the private key file. This file must be in PEM encoded format.
`--config <config_file>`	Optional name of the configuration file. Defaults to `certool.cfg`.
`--server <server>`	Optional name of the VMCA server. By default, the command uses localhost.

Example:

```
certool --gencert --privkey=<filename> --cert=<filename>
```

certool --getrootca

Prints the current root CA certificate in human-readable form. This output is not usable as a certificate, it is changed to be human readable.

Option	Description
`--getrootca`	Required for printing the root certificate.
`--server <server>`	Optional name of the VMCA server. By default, the command uses localhost.

Example:

```
certool --getrootca --server=remoteserver
```

certool --viewcert

Print all the fields in a certificate in human-readable form.

Option	Description
`--viewcert`	Required for viewing a certificate.
`--cert <certfile>`	Optional name of the configuration file. Defaults to `certool.cfg`.

Example:

```
 certool --viewcert --cert=<filename>
```

certool --enumcert

List all certificates that the VMCA server knows about. The required `filter` option lets you list all certificates or only revoked, active, or expired certificates.

Option	Description
`--enumcert`	Required for listing all certificates.
`--filter [all | active]`	Required filter. Specify all or active. The revoked and expired options are not currently supported.

Example:

```
certool --enumcert --filter=active
```

certool --status

Sends a specified certificate to the VMCA server to check whether the certificate has been revoked. Prints `Certificate: REVOKED` if the certificate is revoked, and `Certificate: ACTIVE` otherwise.

Option	Description
`--status`	Required to check the status of a certificate.
`--cert <certfile>`	Optional name of the configuration file. Defaults to `certool.cfg`.
`--server <server>`	Optional name of the VMCA server. By default, the command uses localhost.

Example:

```
certool --status --cert=<filename>
```

certool --genselfcacert

Generates a self-signed certificate based on the values in the configuration file. This command generates a certificate that is predated by three days to avoid time zone conflicts.

Option	Description
`--genselfcacert`	Required for generating a self-signed certificate.
`--outcert <cert_file>`	Name of the certificate file. This file must be in PEM encoded format.
`--outprivkey <key_file>`	Name of the private key file. This file must be in PEM encoded format.
`--config <config_file>`	Optional name of the configuration file. Defaults to `certool.cfg`.

Example:

```
certool --genselfcert --privkey=<filename> --cert=<filename>
```

vecs-cli Command Reference

The `vecs-cli` command set allows you to manage instances of VMware Certificate Store (VECS). Use these commands together with `dir-cli` and `certool` to manage your certificate infrastructure and authentication services.

vecs-cli store create

Creates a certificate store.

Option	Description
`--name <name>`	Name of the certificate store.
`--server <server-name>`	Used to specify a server name if you connect to a remote VECS instance.
`--upn <user-name>`	User Principle Name that is used to log in to the server instance specified by `--server <server-name>` . When you create a store, it is created in the context of the current user. Therefore, the owner of the store is the current user context and not always the root user.

Example:

```
vecs-cli store create --name <store>
```

vecs-cli store delete

Deletes a certificate store. You cannot delete the MACHINE_SSL_CERT, TRUSTED_ROOTS and TRUSTED_ROOT_CRLS system stores. Users with required privileges can delete solution user stores.

Option	Description
`--name <name>`	Name of the certificate store to delete.
`--server <server-name>`	Used to specify a server name if you connect to a remote VECS instance.
`--upn <user-name>`	User Principle Name that is used to log in to the server instance specified by `--server <server-name>` . When you create a store, it is created in the context of the current user. Therefore, the owner of the store is the current user context and not always the root user.

Example:

```
vecs-cli store delete --name <store>
```

vecs-cli store list

List certificate stores.

Option	Description
`--server <server-name>`	Used to specify a server name if you connect to a remote VECS instance.
`--upn <user-name>`	User Principle Name that is used to log in to the server instance specified by `--server <server-name>` . When you create a store, it is created in the context of the current user. Therefore, the owner of the store is the current user context and not always the root user.

VECS includes the following stores.

Table 3-2. Stores in VECS

Store	Description
Machine SSL store (MACHINE_SSL_CERT)	■ Used by the reverse proxy service on every vSphere node. ■ Used by the VMware Directory Service (vmdir) on each vCenter Server node. All services in vSphere 6.0 and later communicate through a reverse proxy, which uses the machine SSL certificate. For backward compatibility, the 5.x services still use specific ports. As a result, some services such as vpxd still have their own port open.
Solution user stores ■ `machine` ■ `vpxd` ■ `vpxd-extension` ■ `vsphere-webclient` ■ `wcp`	VECS includes one store for each solution user. The subject of each solution user certificate must be unique, for example, the machine certificate cannot have the same subject as the vpxd certificate. Solution user certificates are used for authentication with vCenter Single Sign-On. vCenter Single Sign-On checks that the certificate is valid, but does not check other certificate attributes. The following solution user certificate stores are included in VECS: ■ `machine`: Used by the license server and the logging service. **Note** The machine solution user certificate has nothing to do with the machine SSL certificate. The machine solution user certificate is used for the SAML token exchange. The machine SSL certificate is used for secure SSL connections for a machine. ■ `vpxd`: vCenter service daemon (vpxd) store. vpxd uses the solution user certificate that is stored in this store to authenticate to vCenter Single Sign-On. ■ `vpxd-extension`: vCenter extensions store. Includes the Auto Deploy service, inventory service, and other services that are not part of other solution users. ■ `vsphere-webclient`: vSphere Client store. Also includes some additional services such as the performance chart service. ■ `wcp`: VMware vSphere® with VMware Tanzu™ store. Each vCenter Server node includes a `machine` certificate.
Trusted root store (TRUSTED_ROOTS)	Contains all trusted root certificates.

Table 3-2. Stores in VECS (continued)

Store	Description
vSphere Certificate Manager Utility backup store (BACKUP_STORE)	Used by VMCA (VMware Certificate Manager) to support certificate revert. Only the most recent state is stored as a backup, you cannot go back more than one step.
Other stores	Other stores might be added by solutions. For example, the Virtual Volumes solution adds an SMS store. Do not modify the certificates in those stores unless VMware documentation or a VMware Knowledge Base article instructs you to do so. **Note** Deleting the TRUSTED_ROOTS_CRLS store can damage your certificate infrastructure. Do not delete or modify the TRUSTED_ROOTS_CRLS store.

Example:

```
vecs-cli store list
```

vecs-cli store permissions

Grants or revokes permissions to the store. Use either the `--grant` or the `--revoke` option.

The owner of the store can perform all operations, including granting and revoking permissions. The administrator of the local vCenter Single Sign-On domain, administrator@vsphere.local by default, has all privileges on all stores, including granting and revoking permissions.

You can use `vecs-cli get-permissions --name <store-name>` to retrieve the current settings for the store.

Option	Description
`--name <name>`	Name of the certificate store.
`--user <username>`	Unique name of the user who is granted permissions.
`--grant [read|write]`	Permission to grant, either read or write.
`--revoke [read|write]`	Permission to revoke, either read or write. Not currently supported.

vecs-cli store get-permissions

Retrieves the current permission settings for the store.

Option	Description
`--name <name>`	Name of the certificate store.
`--server <server-name>`	Used to specify a server name if you connect to a remote VECS instance.
`--upn <user-name>`	User Principle Name that is used to log in to the server instance specified by `--server <server-name>` . When you create a store, it is created in the context of the current user. Therefore, the owner of the store is the current user context and not always the root user.

vecs-cli entry create

Creates an entry in VECS. Use this command to add a private key or certificate to a store.

Note Do not use this command to add root certificates to the TRUSTED_ROOTS store. Instead, use the `dir-cli` command to publish root certificates.

Option	Description
`--store <NameOfStore>`	Name of the certificate store.
`--alias <Alias>`	Optional alias for the certificate. This option is ignored for the trusted root store.
`--cert <certificate_file_path>`	Full path of the certificate file.
`--key <key-file-path>`	Full path of the key that corresponds to the certificate. Optional.
`--password <password>`	Optional password for encrypting the private key.
`--server <server-name>`	Used to specify a server name if you connect to a remote VECS instance.
`--upn <user-name>`	User Principle Name that is used to log in to the server instance specified by `--server <server-name>` . When you create a store, it is created in the context of the current user. Therefore, the owner of the store is the current user context and not always the root user.

vecs-cli entry list

Lists all entries in a specified store.

Option	Description
`--store <NameOfStore>`	Name of the certificate store.

vecs-cli entry getcert

Retrieves a certificate from VECS. You can send the certificate to an output file or display it as human-readable text.

Option	Description
`--store <NameOfStore>`	Name of the certificate store.
`--alias <Alias>`	Alias of the certificate.
`--output <output_file_path>`	File to write the certificate to.
`--text`	Displays a human-readable version of the certificate.
`--server <server-name>`	Used to specify a server name if you connect to a remote VECS instance.
`--upn <user-name>`	User Principle Name that is used to log in to the server instance specified by `--server <server-name>` . When you create a store, it is created in the context of the current user. Therefore, the owner of the store is the current user context and not always the root user.

vecs-cli entry getkey

Retrieves a key that is stored in VECS. You can send the key to an output file or display it as human-readable text.

Option	Description
`--store <NameOfStore>`	Name of the certificate store.
`--alias <Alias>`	Alias for the key.
`--output <output_file_path>`	Output file to write the key to.
`--text`	Displays a human-readable version of the key.
`--server <server-name>`	Used to specify a server name if you connect to a remote VECS instance.
`--upn <user-name>`	User Principle Name that is used to log in to the server instance specified by `--server <server-name>` . When you create a store, it is created in the context of the current user. Therefore, the owner of the store is the current user context and not always the root user.

vecs-cli entry delete

Deletes an entry in a certificate store. If you delete an entry in VECS, you permanently remove it from VECS. The only exception is the current root certificate. VECS polls vmdir for a root certificate.

Option	Description
`--store <NameOfStore>`	Name of the certificate store.
`--alias <Alias>`	Alias for the entry you want to delete.
`--server <server-name>`	Used to specify a server name if you connect to a remote VECS instance.
`--upn <user-name>`	User Principle Name that is used to log in to the server instance specified by `--server <server-name>` . When you create a store, it is created in the context of the current user. Therefore, the owner of the store is the current user context and not always the root user.
`-y`	Suppresses the confirmation prompt. For advanced users only.

vecs-cli force-refresh

Forces a refresh of VECS. By default, VECS polls vmdir for new root certificate files every 5 minutes. Use this command for an immediate update of VECS from vmdir.

Option	Description
`--server <server-name>`	Used to specify a server name if you connect to a remote VECS instance.
`--upn <user-name>`	User Principle Name that is used to log in to the server instance specified by `--server <server-name>` . When you create a store, it is created in the context of the current user. Therefore, the owner of the store is the current user context and not always the root user.

dir-cli Command Reference

The `dir-cli` utility supports creation and updates to solution users, account management, and management of certificates and passwords in VMware Directory Service (vmdir). You can use `dir-cli` to manage and query the domain functional level of vCenter Server instances.

dir-cli nodes list

Lists all the enhanced linked mode connected vCenter Server systems.

Option	Description
`--login <admin_user_id>`	The administrator of the local vCenter Single Sign-On domain, administrator@vsphere.local by default.
`--password <admin_password>`	Password of the administrator user. If you do not specify the password, you are prompted.
`--server <psc_ip_or_fqdn>`	Use this option to connect to another vCenter Server to see its replication partners.

dir-cli computer password-reset

Enables you to reset the password of the machine account in the domain.

Option	Description
`--login <admin_user_id>`	The administrator of the local vCenter Single Sign-On domain, administrator@vsphere.local by default.
`--password <admin_password>`	Password of the administrator user. If you do not specify the password, you are prompted.
`--live-dc-hostname <server name>`	Current name of the vCenter Server instance.

dir-cli service create

Creates a solution user. Primarily used by third-party solutions.

Option	Description
`--name <name>`	Name of the solution user to create
`--cert <cert file>`	Path to the certificate file. This can be a certificate signed by VMCA or a third-party certificate.
`--ssogroups <comma-separated-groupnames>`	Makes the solution user a member of the specified groups.
`--wstrustrole <ActAsUser>`	Makes the solution user a member of the built-in administrators or users group. In other words, determines whether the solution user has administrative privileges.
`--ssoadminrole <Administrator/User>`	Makes the solution user a member of the ActAsUser group. The ActAsUser role enables users to act on behalf of other users.
`--login <admin_user_id>`	The administrator of the local vCenter Single Sign-On domain, administrator@vsphere.local by default.
`--password <admin_password>`	Password of the administrator user. If you do not specify the password, you are prompted.

dir-cli service list

List the solution users that `dir-cli` knows about.

Option	Description
`--login <admin_user_id>`	The administrator of the local vCenter Single Sign-On domain, administrator@vsphere.local by default.
`--password <admin_password>`	Password of the administrator user. If you do not specify the password, you are prompted.

dir-cli service delete

Delete a solution user in vmdir. When you delete the solution user, all associated services become unavailable to all management nodes that use this instance of vmdir.

Option	Description
`--name`	Name of the solution user to delete.
`--login <admin_user_id>`	The administrator of the local vCenter Single Sign-On domain, administrator@vsphere.local by default.
`--password <admin_password>`	Password of the administrator user. If you do not specify the password, you are prompted.

dir-cli service update

Updates the certificate for a specified solution user, that is, collection of services. After running this command, VECS picks up the change after 5 minutes, or you can use `vecs-cli force-refresh` to force a refresh.

Option	Description
`--name <name>`	Name of the solution user to update .
`--cert <cert_file>`	Name of the certificate to assign to the service.
`--login <admin_user_id>`	The administrator of the local vCenter Single Sign-On domain, administrator@vsphere.local by default.
`--password <admin_password>`	Password of the administrator user. If you do not specify the password, you are prompted.

dir-cli user create

Creates a regular user inside vmdir. This command can be used for human users who authenticate to vCenter Single Sign-On with a user name and password. Use this command only during prototyping.

Option	Description
`--account <name>`	Name of the vCenter Single Sign-On user to create.
`--user-password <password>`	Initial password for the user.
`--first-name <name>`	First name for the user.
`--last-name <name>`	Last name for the user.
`--login <admin_user_id>`	The administrator of the local vCenter Single Sign-On domain, administrator@vsphere.local by default.
`--password <admin_password>`	Password of the administrator user. If you do not specify the password, you are prompted.

dir-cli user modify

Modifies the specified user inside vmdir.

Option	Description
`--account <name>`	Name of the vCenter Single Sign-On user to modify.
`--password-never-expires`	Set this option to true if you are modifying a user account for automated tasks that have to authenticate to vCenter Server, and you want to ensure that the tasks do not stop running because of password expiration. Use this option with care.
`--password-expires`	Set this option to true if you want to revert the `--password-never-expires` option.
`--login <admin_user_id>`	The administrator of the local vCenter Single Sign-On domain, administrator@vsphere.local by default.
`--password <admin_password>`	Password of the administrator user. If you do not specify the password, you are prompted.

dir-cli user delete

Deletes the specified user inside vmdir.

Option	Description
`--account <name>`	Name of the vCenter Single Sign-On user to delete.
`--login <admin_user_id>`	The administrator of the local vCenter Single Sign-On domain, administrator@vsphere.local by default.
`--password <admin_password>`	Password of the administrator user. If you do not specify the password, you are prompted.

dir-cli user find-by-name

Finds a user inside vmdir by name. The information that this command returns depends on what you specify in the `--level` option.

Option	Description
`--account <name>`	Name of the vCenter Single Sign-On user to delete.
`--level <info level 0|1|2>`	Returns the following information: ■ Level 0 - Account and UPN ■ Level 1 - level 0 info + First and last name ■ Level 2 : level 0 + Account disabled flag, Account locked flag, Password never expires flag, password expired flag and password expiry flag. The default level is 0.

Option	Description
`--login <admin_user_id>`	The administrator of the local vCenter Single Sign-On domain, administrator@vsphere.local by default.
`--password <admin_password>`	Password of the administrator user. If you do not specify the password, you are prompted.

dir-cli group modify

Adds a user or group to an existing group.

Option	Description
`--name <name>`	Name of the group in vmdir.
`--add <user_or_group_name>`	Name of the user or group to add.
`--login <admin_user_id>`	The administrator of the local vCenter Single Sign-On domain, administrator@vsphere.local by default.
`--password <admin_password>`	Password of the administrator user. If you do not specify the password, you are prompted.

dir-cli group list

Lists a specified vmdir group.

Option	Description
`--name <name>`	Optional name of the group in vmdir. This option allows you to check whether a specific group exists.
`--login <admin_user_id>`	The administrator of the local vCenter Single Sign-On domain, administrator@vsphere.local by default.
`--password <admin_password>`	Password of the administrator user. If you do not specify the password, you are prompted.

dir-cli ssogroup create

Create a group inside the local domain (vsphere.local by default).

Use this command if you want to create groups to manage user permissions for the vCenter Single Sign-On domain. For example, if you create a group and then add it to the Administrators group of the vCenter Single Sign-On domain, then all users that you add to that group have administrator permissions for the domain.

It is also possible to give permissions to vCenter inventory objects to groups in the vCenter Single Sign-On domain. See the *vSphere Security* documentation.

Option	Description
`--name <name>`	Name of the group in vmdir. Maximum length is 487 characters.
`--description <description>`	Optional description for the group.
`--login <admin_user_id>`	The administrator of the local vCenter Single Sign-On domain, administrator@vsphere.local by default.
`--password <admin_password>`	Password of the administrator user. If you do not specify the password, you are prompted.

dir-cli trustedcert publish

Publishes a trusted root certificate to vmdir.

Option	Description
`--cert <file>`	Path to certificate file.
`--crl <file>`	This option is not supported by VMCA.
`--login <admin_user_id>`	The administrator of the local vCenter Single Sign-On domain, administrator@vsphere.local by default.
`--password <admin_password>`	Password of the administrator user. If you do not specify the password, you are prompted.
`--chain`	Specify this option if you are publishing a chained certificate. No option value is needed.

dir-cli trustedcert publish

Publishes a trusted root certificate to vmdir.

Option	Description
`--cert <file>`	Path to certificate file.
`--crl <file>`	This option is not supported by VMCA.
`--login <admin_user_id>`	The administrator of the local vCenter Single Sign-On domain, administrator@vsphere.local by default.
`--password <admin_password>`	Password of the administrator user. If you do not specify the password, you are prompted.
`--chain`	Specify this option if you are publishing a chained certificate. No option value is needed.

dir-cli trustedcert unpublish

Unpublishes a trusted root certificate currently in vmdir. Use this command, for example, if you added a different root certificate to vmdir that is now the root certificate for all other certificates in your environment. Unpublishing certificates that are no longer in use is part of hardening your environment.

Option	Description
`--cert-file <file>`	Path to the certificate file to unpublish
`--login <admin_user_id>`	The administrator of the local vCenter Single Sign-On domain, administrator@vsphere.local by default.
`--password <admin_password>`	Password of the administrator user. If you do not specify the password, you are prompted.

dir-cli trustedcert list

Lists all trusted root certificates and their corresponding IDs. You need the certificate IDs to retrieve a certificate with `dir-cli trustedcert get`.

Option	Description
`--login <admin_user_id>`	The administrator of the local vCenter Single Sign-On domain, administrator@vsphere.local by default.
`--password <admin_password>`	Password of the administrator user. If you do not specify the password, you are prompted.

dir-cli trustedcert get

Retrieves a trusted root certificate from vmdir and writes it to a specified file.

Option	Description
`--id <cert_ID>`	ID of the certificate to retrieve. The `dir-cli trustedcert list` command shows the ID.
`--outcert <path>`	Path to write the certificate file to.
`--outcrl <path>`	Path to write the CRL file to. Not currently used.
`--login <admin_user_id>`	The administrator of the local vCenter Single Sign-On domain, administrator@vsphere.local by default.
`--password <admin_password>`	Password of the administrator user. If you do not specify the password, you are prompted.

dir-cli password create

Creates a random password that meets the password requirements. This command can be used by third-party solution users.

Option	Description
`--login <admin_user_id>`	The administrator of the local vCenter Single Sign-On domain, administrator@vsphere.local by default.
`--password <admin_password>`	Password of the administrator user. If you do not specify the password, you are prompted.

dir-cli password reset

Allows an administrator to reset a user's password. If you are a non-administrator user who wants to reset a password, use `dir-cli password change` instead.

Option	Description
`--account`	Name of the account to assign a new password to.
`--new`	New password for the specified user.
`--login <admin_user_id>`	The administrator of the local vCenter Single Sign-On domain, administrator@vsphere.local by default.
`--password <admin_password>`	Password of the administrator user. If you do not specify the password, you are prompted.

dir-cli password change

Allows a user to change their password. You must be the user who owns the account to make this change. Administrators can use `dir-cli password reset` to reset any password.

Option	Description
`--account`	Account name.
`--current`	Current password of the user who owns the account.
`--new`	New password of the user who owns the account.

vSphere Authentication with vCenter Single Sign-On

4

vCenter Single Sign-On is an authentication broker and security token exchange infrastructure. vCenter Single Sign-On issues a token when a user authenticates. The user can use the token to authenticate to vCenter Server services. The user can then perform the actions that user has privileges for.

Because traffic is encrypted for all communications, and because only authenticated users can perform the actions that they have privileges for, your environment is secure.

Users and service accounts authenticate with a token, or a user name and password. Solution users authenticate with a certificate. For information on replacing solution user certificates, see Chapter 2 vSphere Security Certificates.

The next step is authorizing the users who can authenticate to perform certain tasks. Usually, you assign vCenter Server privileges, typically by assigning the user to a group that has a role. vSphere includes other permission models such as global permissions. See the *vSphere Security* documentation.

This chapter includes the following topics:

How vCenter Single Sign-On Protects Your Environment

vCenter Single Sign-On allows vSphere components to communicate with each other through a secure token mechanism.

vCenter Single Sign-On uses the following services.

- Authentication of users through either external identity provider federation or the vCenter Server built-in identity provider. The built-in identity provider supports local accounts, Active Directory or OpenLDAP, Integrated Windows Authentication (IWA), and miscellaneous authentication mechanisms (smart card, RSA SecurID, and Windows Session Authentication).
- Authentication of solution users through certificates.
- Security Token Service (STS).
- SSL for secure traffic.

Identity Provider Overview

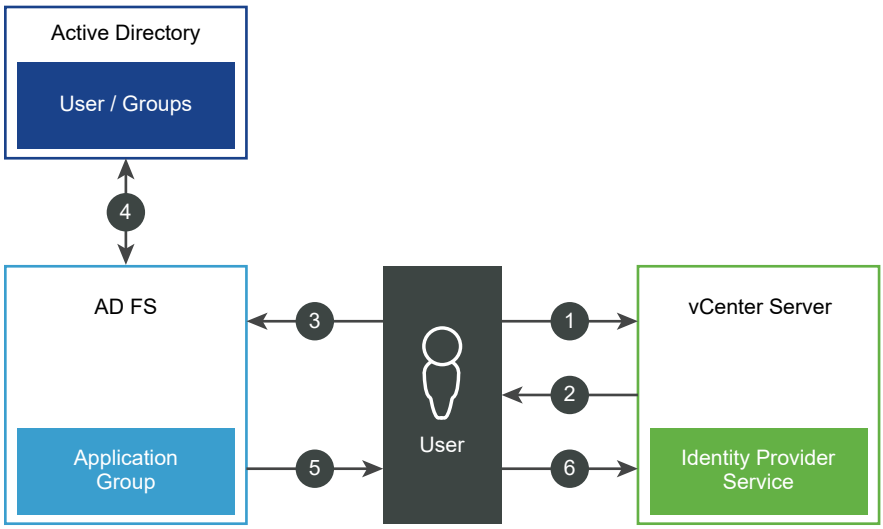
Before vSphere 7.0, vCenter Server includes a built-in identity provider. By default, vCenter Server uses the vsphere.local domain as the identity source (but you can change it during installation). You can configure the vCenter Server built-in identity provider to use Active Directory (AD) as its identity source using LDAP/S, OpenLDAP/S, and Integrated Windows Authentication (IWA). Such configurations allow customers to log in to vCenter Server using their AD accounts.

Starting with vSphere 7.0, you can configure vCenter Server for an external identity provider using federated authentication. In such a configuration, you replace vCenter Server as the identity provider. Currently, vSphere supports Active Directory Federation Services (AD FS) as the external identity provider. In this configuration, AD FS interacts with the identity sources on behalf of vCenter Server.

User Login with vCenter Server Identity Provider Federated Authentication

The following figure shows the user login flow for vCenter Server Identity Provider Federation.

Figure 4-1. vCenter Server Identity Provider Federation User Login



vCenter Server, AD FS, and Active Directory interact as follows:

1 The user starts on the vCenter Server landing page by entering a user name.

2 If the user name is for a federated domain, vCenter Server redirects the authentication request to AD FS.

3 If needed, AD FS prompts the user to log in with Active Directory credentials.

4 AD FS authenticates the user with Active Directory.

5 AD FS issues a security token with group information from Active Directory.

6 vCenter Server uses the token to log in the user.

The user is now authenticated, and can view and modify any objects that the user's role has privileges for.

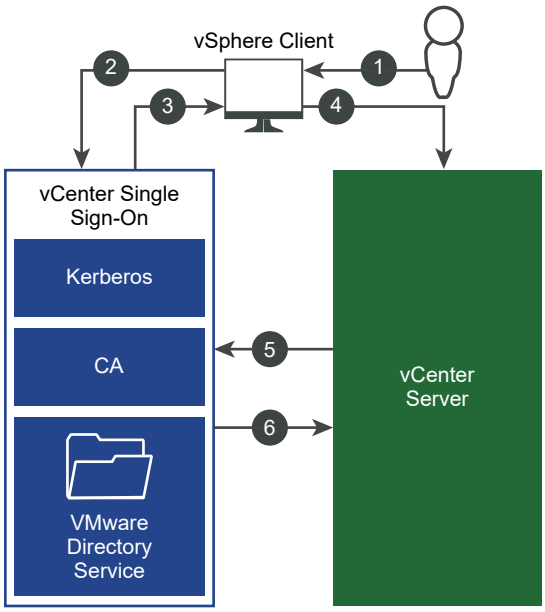
Note Initially, each user is assigned the No Access role. A vCenter Server administrator must assign the user at least to the Read Only role before the user can log in. See the *vSphere Security* documentation.

In case the external identity provider is unreachable, the login process falls back to the vCenter Server landing page, showing an appropriate information message. Users can still log in using their local accounts in the vsphere.local identity source.

User Login with the vCenter Server Built-In Identity Provider

The following figure shows the user login flow when vCenter Server acts as the identity provider.

Figure 4-2. User Login with the vCenter Server Built-In Identity Provider



1 A user logs in to the vSphere Client with a user name and password to access the vCenter Server system or another vCenter service.

   When Integrated Windows Authentication (IWA) has been configured, users can also log in without having to reenter their Windows password by checking the **Use Windows session authentication** check box.

2 The vSphere Client passes the login information to the vCenter Single Sign-On service, which checks the SAML token of the vSphere Client. If the vSphere Client has a valid token, vCenter Single Sign-On then checks whether the user is in the configured identity source (for example Active Directory).

   - If only the user name is used, vCenter Single Sign-On checks in the default domain.
   - If a domain name is included with the user name (*DOMAIN*\user1 or user1@*DOMAIN*), vCenter Single Sign-On checks that domain.

3 If the user can authenticate to the identity source, vCenter Single Sign-On returns a token that represents the user to the vSphere Client.

4 The vSphere Client passes the token to the vCenter Server system.

5 vCenter Server checks with the vCenter Single Sign-On server that the token is valid and not expired.

6 The vCenter Single Sign-On server returns the token to the vCenter Server system, using the vCenter Server Authorization Framework to allow user access.

The user is now authenticated, and can view and modify any objects that the user's role has privileges for.

Note Initially, each user is assigned the No Access role. A vCenter Server administrator must assign the user at least to the Read Only role before the user can log in. See the *vSphere Security* documentation.

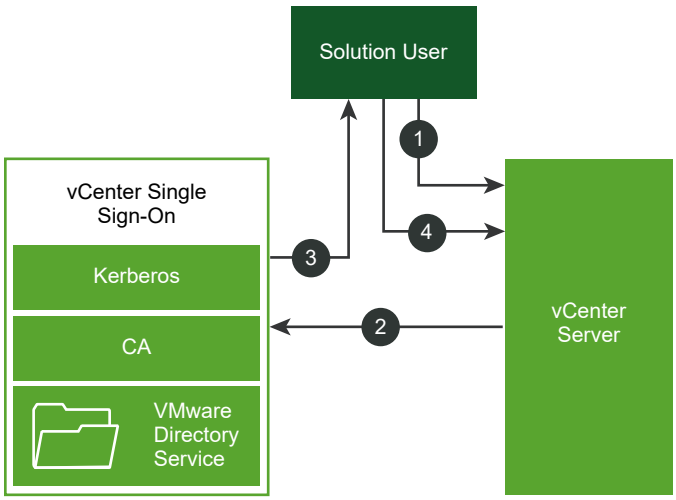
Login for Solution Users

Solution users are sets of services that are used in the vCenter Server infrastructure, for example, vCenter Server extensions. VMware extensions and potentially third-party extensions might also authenticate to vCenter Single Sign-On.

Note vCenter Server uses solution user certificates for internal communication only. Solution user certificates are not used for external communication.

The following figure shows the login flow for solution users.

Figure 4-3. Login for Solution Users



1 The solution user attempts to connect to a vCenter Server service.

2 The solution user is redirected to vCenter Single Sign-On. If the solution user is new to vCenter Single Sign-On, it has to present a valid certificate.

3 If the certificate is valid, vCenter Single Sign-On assigns a SAML token (bearer token) to the solution user. The token is signed by vCenter Single Sign-On.

4 The solution user is then redirected to vCenter Single Sign-On and can perform tasks based on its permissions.

   The next time the solution user has to authenticate, it can use the SAML token to log in to vCenter Server.

By default, this handshake is automatic because VMCA provisions solution users with certificates during startup. If your company policy requires third-party CA-signed certificates, you can replace the solution user certificates with third-party CA-signed certificates. If those certificates are valid, vCenter Single Sign-On assigns a SAML token to the solution user. See Use Custom Certificates with vSphere.

Supported Encryption

AES encryption, which is the highest level of encryption, is supported. The supported encryption affects security when vCenter Single Sign-On uses Active Directory as an identity source.

It also affects security anytime an ESXi host or vCenter Server is joined to Active Directory.

Understanding vCenter Server Identity Provider Federation

Starting in vSphere 7.0, vCenter Server supports federated authentication to sign in to vCenter Server.

To enable federated authentication to vCenter Server, you configure a connection to an external identity provider. The identity provider instance that you configure replaces vCenter Server as the identity provider. Currently, vCenter Server supports only Active Directory Federation Services (AD FS) as an external identity provider.

Note VMware encourages you to use federated authentication as vSphere moves towards token-based authentication. vCenter Server continues to have local accounts, for administrative access and error recovery.

How vCenter Server Identity Provider Federation Works

vCenter Server Identity Provider Federation enables you to configure an external identity provider for federated authentication. In this configuration, the external identity provider interacts with the identity source on behalf of vCenter Server.

vCenter Server Identity Provider Federation Basics

Starting in vSphere 7.0, vCenter Server supports federated authentication. In this scenario, when a user logs in to vCenter Server, vCenter Server redirects the user login to the external identity provider. The user credentials are no longer provided to vCenter Server directly. Instead, the user provides credentials to the external identity provider. vCenter Server trusts the external identity provider to perform the authentication. In the federation model, users never provide credentials directly to any service or application but only to the identity provider. As a result, you "federate" your applications and services, such as vCenter Server, with your identity provider.

vCenter Server Identity Provider Federation Benefits

vCenter Server Identity Provider Federation provides the following benefits.

- You can use Single Sign-On with existing federated infrastructure and applications.

- You can improve data center security because vCenter Server never handles the user's credentials.
- You can use the authentication mechanisms, such as multi-factor authentication, supported by the external identity provider.

vCenter Server Identity Provider Federation Components

The following components comprise a vCenter Server Identity Provider Federation configuration that uses Microsoft Active Directory Federation Services (AD FS):

- A vCenter Server
- An identity provider service configured on the vCenter Server
- An AD FS server and associated Microsoft Active Directory domain
- An AD FS Application Group
- Active Directory groups and users that map to vCenter Server groups and users

Note Currently, vCenter Server supports only AD FS as an external identity provider.

vCenter Server Identity Provider Federation Architecture

In vCenter Server Identity Provider Federation, vCenter Server uses the OpenID Connect (OIDC) protocol to receive an identity token that authenticates the user with vCenter Server.

To establish a relying party trust between vCenter Server and an identity provider, you must establish the identifying information and a shared secret between them. In AD FS, you do so by creating an OIDC configuration known as an Application Group, which consists of a Server application and a Web API. The two components specify the information that vCenter Server uses to trust and communicate with the AD FS server. You also create a corresponding identity provider in vCenter Server. Finally, you configure group memberships in vCenter Server to authorize logins from users in the AD FS domain.

The AD FS administrator must provide the following information to create the vCenter Server identity provider configuration:

- Client Identifier: The UUID string that is generated by the AD FS Application Group wizard and that identifies the Application Group itself.
- Shared Secret: The secret that is generated by the AD FS Application Group wizard and that is used to authenticate vCenter Server with AD FS.
- OpenID Address: The OpenID Provider Discovery endpoint URL of the AD FS server, specifying a well-known address that is typically the issuer endpoint concatenated with the path "`/.well-known/openid-configuration`". For example: `https://webserver.example.com/adfs/.well-known/openid-configuration`.

vCenter Server Identity Provider Federation and Enhanced Linked Mode

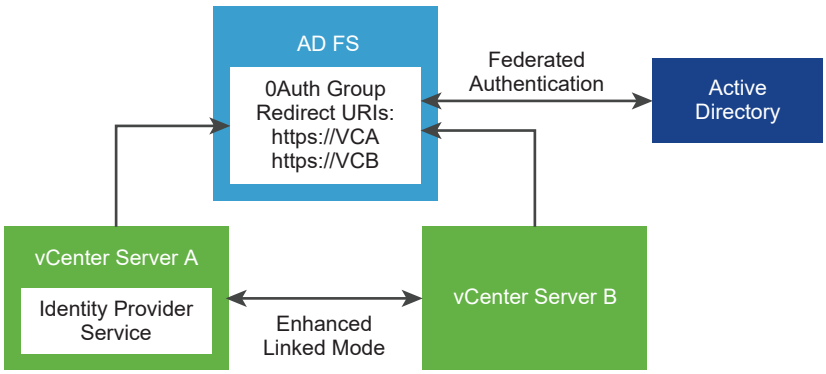
When you enable Identity Provider Federation in vCenter Server environments using enhanced linked mode, authentication and workflows continue to work as before.

If you use Enhanced Linked Mode configuration, note the following when logging in to vCenter Server using federated authentication.

- Users continue to see the same inventory, and can perform the same actions, based on the vCenter Server permissions and roles model.
- vCenter Server hosts in enhanced linked mode are not required to have access to each other's identity providers. For example, consider two vCenter Server systems A and B, and that use enhanced linked mode. After vCenter Server A authorizes a user, then the user is authorized on vCenter Server B as well.

The following illustration shows the authentication workflow with enhanced linked mode and vCenter Server Identity Provider Federation.

Figure 4-4. Enhanced Linked Mode and vCenter Server Identity Provider Federation



1 Two vCenter Server nodes are deployed in Enhanced Linked Mode configuration.

2 The AD FS setup has been configured on vCenter Server A using the Change Identity Provider wizard in the vSphere Client. Group memberships and permissions have also been established for AD FS users or groups.

3 vCenter Server A replicates the AD FS configuration to vCenter Server B.

4 All Redirect URIs for both vCenter Server nodes are added to the OAuth Application Group in AD FS. Only one OAuth Application Group is created.

5 When a user logs into and is authorized by vCenter Server A, the user is also authorized on vCenter Server B. If the user logs in to vCenter Server B first, the same holds true.

vCenter Server enhanced linked mode supports the following configuration scenarios for identity provider federation. In this section, the terms "AD FS settings" and "AD FS configuration" refer to the settings that you configure in the vSphere Client using the Change Identity Provider wizard, and any group memberships or permissions that you have established for AD FS users or groups.

Enable AD FS on an existing Enhanced Linked Mode configuration

High-level steps:

1. Deploy N vCenter Server nodes in Enhanced Linked Mode configuration.
2. Configure AD FS on one of the linked vCenter Server nodes.
3. The AD FS configuration is replicated to all other (N-1) vCenter Server nodes.
4. Add all Redirect URIs for all N vCenter Server nodes to the configured OAuth Application Group in AD FS.

Link a new vCenter Server to an existing Enhanced Linked Mode AD FS configuration

High-level Steps:

1. (Prerequisite) Set up AD FS on a vCenter Server N-node Enhanced Linked Mode configuration.
2. Deploy a new independent vCenter Server node.
3. Repoint the new vCenter Server to the N-node AD FS enhanced linked mode domain, using one of the *N* nodes as its replication partner.
4. All AD FS settings in the existing Enhanced Linked Mode configuration are replicated to the new vCenter Server.

   The AD FS settings that are in the N-node AD FS enhanced linked mode domain overwrite any existing AD FS settings on the newly linked vCenter Server.
5. Add all Redirect URIs for the new vCenter Server to the existing configured OAuth Application Group in AD FS.

Unlink a vCenter Server from an Enhanced Linked Mode AD FS configuration

High-level steps:

1. (Prerequisite) Set up AD FS on an N-node vCenter Server Enhanced Linked Mode configuration.
2. Unregister one of the vCenter Server hosts in the N-node configuration and repoint it to a new domain to unlink it from the N-node configuration.

3 The domain repointing process does not preserve SSO settings, so all AD FS settings on the unlinked vCenter Server node are reverted and lost. To continue using AD FS on this vCenter Server unlinked node, you must reconfigure AD FS from the beginning or you must relink the vCenter Server to an Enhanced Linked Mode configuration where AD FS is already set up.

vCenter Server Identity Provider Federation Caveats and Interoperability

vCenter Server Identity Provider Federation can interoperate with many other VMware features.

As you are planning your vCenter Server Identity Provider Federation strategy, consider possible interoperability limitations.

Authentication Mechanisms

In a vCenter Server Identity Provider Federation configuration, the external identity provider handles the authentication mechanisms (passwords, MFA, biometrics, and so on).

vCenter Server Policies

When vCenter Server acts as the identity provider, you control vCenter Server password, lockout, and token policies for the vsphere.local domain. When using federated authentication with vCenter Server, the external identity provider controls the password, lockout, and token policies for the accounts stored in the identity source such as Active Directory.

Auditing and Compliance

When using vCenter Server Identity Provider Federation, vCenter Server continues to create log entries for successful user logins. However, the external identity provider is responsible for tracking and logging actions such as failed password-entry attempts and user account lockouts. vCenter Server does not log such events because they are no longer visible to vCenter Server. For example, when AD FS is the identity provider, AD FS tracks and logs errors for federated logins. When vCenter Server is the identify provider for local logins, vCenter Server tracks and logs errors for local logins. In a federated configuration, vCenter Server does continue to log user actions post-login.

Existing VMware Product Integration

VMware products integrated with vCenter Server (for example, vROps, vSAN, NSX, and so on) continue to work as before.

Products That Integrate Post-Login

Products that integrate post-login (that is, they do not require a separate login) continue to work as before.

Simple Authentication for API, SDK, and CLI Access

Existing scripts, products, and other functionality that rely on API, SDK, or CLI commands that use Simple Authentication (that is, user name and password) continue to work as before. Internally, authentication occurs by passing the user name and password. This passing of the user name and password compromises some of the benefits of using identity federation, because it exposes the password to vCenter Server (and your scripts). Consider migrating to token-based authentication where possible.

vCenter Server Management Interface

If the user is a member of the Administrators group, accessing the vCenter Server Management Interface (formerly called vCenter Server Appliance Management Interface or VAMI) is supported.

Entering User Name Text on the AD FS Login Page

The AD FS login page does not support passing text to pre-populate the user name text box. As a result, during federated logins with AD FS, after entering your user name on the vCenter Server landing page and redirecting to the AD FS login page, you must reenter your user name on the AD FS login page. The user name that you enter on the vCenter Server landing page is necessary to redirect the login to the appropriate identity provider, and the user name on the AD FS login page is necessary to authenticate with AD FS. This inability to pass the user name to the AD FS login page is a limitation of AD FS. You cannot configure or change this behavior directly from vCenter Server.

vCenter Server Identity Provider Federation Life Cycle

When managing the life cycle of vCenter Server Identity Provider Federation, there are some specific considerations.

You can manage your vCenter Server Identity Provider Federation life cycle in the following ways.

Migrating from Using Active Directory to AD FS

If you are using Active Directory as your identity source for vCenter Server, migrating to using AD FS is straight forward. If your Active Directory groups and roles match your AD FS groups and roles, you do not need to take any additional action. When the groups and roles do not match, then you must perform some additional work. If vCenter Server is a domain member, consider removing it from the domain as it is not needed or used for identity federation.

Cross-Domain Repointing and Migration

vCenter Server Identity Provider Federation supports cross-domain repointing, that is, moving a vCenter Server from one vSphere SSO domain to another. The repointed vCenter Server receives the replicated AD FS configuration from the vCenter Server system, or systems, to which it was pointed.

In general, you do not need to perform any additional AD FS reconfiguration for a cross-domain repoint, unless one of the following is true.

1 The AD FS configuration of the repointed vCenter Server differs from the AD FS configuration of the vCenter Server to which it was pointed.

2 This is the first time the repointed vCenter Server is receiving an AD FS configuration.

In these cases, you must add the vCenter Server system's Redirect URIs to the corresponding Application Group on the AD FS server. For example, if vCenter Server 1 with AD FS Application Group A (or no AD FS configuration) is repointed to vCenter Server 2 with AD FS Application Group B, you must add the Redirect URIs of vCenter Server 1 to Application Group B.

Configuring vCenter Server Identity Provider Federation

After you deploy vCenter Server initially, you can configure an external identity provider for federated authentication.

You configure vCenter Server Identity Provider Federation from the vSphere Client or the API. You also must perform some configuration on your external identity provider. To configure vCenter Server Identity Provider Federation, you must have vCenter Single Sign-On administrator privileges. Having vCenter Single Sign-On administrator privileges is different from having the Administrator role on vCenter Server or ESXi. In a new installation, only the vCenter Single Sign-On administrator (administrator@vsphere.local by default) can authenticate to vCenter Single Sign-On.

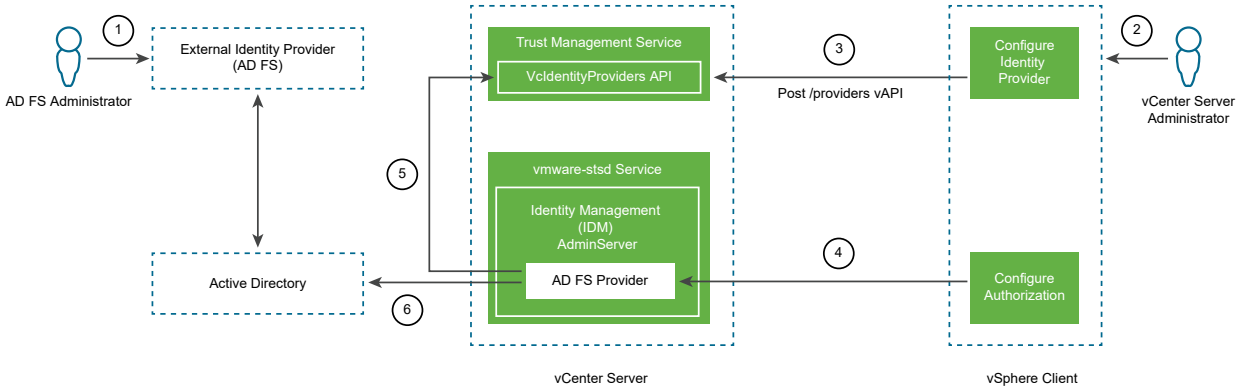
vCenter Server Identity Provider Federation Configuration Process Flow

To configure vCenter Server Identity Provider Federation effectively, you must understand the communication flows that take place.

vCenter Server Identity Provider Federation Configuration Process Flow

The following figure shows the process flow that occurs when configuring vCenter Server Identity Provider Federation.

Figure 4-5. vCenter Server Identity Provider Federation Configuration Process Flow



vCenter Server, AD FS, and Active Directory interact as follows.

1 The AD FS administrator configures an AD FS OAuth Application for vCenter Server.

2 The vCenter Server administrator logs in to the vCenter Server using the vSphere Client.

3 The vCenter Server administrator adds an AD FS identity provider to vCenter Server, and also enters information about the Active Directory domain.

   vCenter Server needs this information to make an LDAP connection to the Active Directory domain of the AD FS server. Using this connection, vCenter Server searches for users and groups, and adds them to vCenter Server local groups in the next step. See the section titled "Searching the Active Directory Domain" that follows for more information.

4 The vCenter Server administrator configures authorization permissions in vCenter Server for AD FS users.

5 The AD FS Provider queries the VcIdentityProviders API to get the LDAP connection information for the Active Directory source.

6 The AD FS Provider searches Active Directory for the queried users or groups to finish the Authorization configuration.

Searching the Active Directory Domain

You configure AD FS as the external identity provider in vCenter Server by using the Configure Main Identity Provider wizard in the vSphere Client. As part of the configuration process, you must enter information about your Active Directory domain, including user and group distinguished name information. Configuration of AD FS for authentication requires this Active Directory connection information. This connection is necessary to search for and map Active Directory user names and groups to roles and permissions in vCenter Server, whereas AD FS is used for the authentication of the user. This step of the Configure Main Identity Provider wizard does not create an Active Directory Over LDAP identity source. Rather, vCenter Server uses this information to establish a valid search-capable connection to your Active Directory domain to find users and groups there.

Consider an example using the following distinguished name entries:

- Base distinguished name for users: cn=Users,dc=corp,dc=local
- Base distinguished name for groups: dc=corp,dc=local
- User name: cn=Administrator,cn=Users,dc=corp,dc=local

If the AdfsUser@corp.local user is a member of the ADGroup@corp.local group, entering this information in the wizard allows a vCenter Server administrator to search for and find the ADGroup@corp.local group and add it to the vCenter Server Administrators@vsphere.local group. As a result, the AdfsUser@corp.local user is granted administrative privileges in vCenter Server upon logging in.

vCenter Server also uses this search process when you configure global permissions for Active Directory users and groups. In both cases, either configuring global permissions, or adding a user or group, you select the domain you entered for your AD FS identify provider from the **Domain** drop-down menu to search for and select users and groups from your Active Directory domain.

Use the Trusted Root Certificates Store Instead of the JRE truststore

If you imported a root CA certificate issued by your own internal Certificate Authority to the JRE truststore in vSphere 7.0, starting in vSphere 7.0 Update 1, you can register the certificate to the Trusted Root Certificates Store.

To configure vCenter Server Identity Provider Federation in vSphere 7.0 with a root CA certificate that was issued by your own internal Certificate Authority, you had to import it to the JRE truststore. Starting in vSphere 7.0 Update 1, you can register the certificate to the Trusted Root Certificates Store. This change means that you should add the root CA certificate that was issued by your own internal Certificate Authority to the Trusted Root Certificates Store (also called the VMware Endpoint Certificate Store, or VECS). Certificates in the JRE truststore continue to function, however, vCenter Server is standardizing on using the Trusted Root Certificates Store.

Procedure

1. Log in with the vSphere Client to the vCenter Server.
2. Navigate to **Administration > Certificates > Certificate Management**.
3. Next to **Trusted Root Certificates**, click **Add**.
4. Browse for the AD FS root certificate and click **Add**.

   The certificate is added in a panel under **Trusted Root Certificates**.

Configure vCenter Server Identity Provider Federation for AD FS

After installing or upgrading to vSphere 7.0 or later, you can configure vCenter Server Identity Provider Federation.

vCenter Server supports only one configured external identity provider (one source), and the vsphere.local identity source. You cannot use multiple external identity providers. vCenter Server Identity Provider Federation uses OpenID Connect (OIDC) for user login to vCenter Server.

This task describes how to add an AD FS group to the vSphere Administrators group as the way to control permissions. You can also configure privileges using AD FS Authorization through global or object permissions in vCenter Server. See the *vSphere Security* documentation for details about adding permissions.

Caution If you use an Active Directory identity source that you previously added to vCenter Server for your AD FS identity source, do not delete that existing identity source from vCenter Server. Doing so causes a regression with previously assigned roles and group memberships. Both the AD FS user with global permissions and users that were added to the Administrators group will not be able to log in.

Workaround: If you do not need the previously assigned roles and group memberships, and want to remove the previous Active Directory identity source, remove the identity source before creating the AD FS provider and configuring group memberships in vCenter Server.

Prerequisites

Active Directory Federation Services requirements:

- AD FS for Windows Server 2016 or later must already be deployed.
- AD FS must be connected to Active Directory.
- An Application Group for vCenter Server must be created in AD FS as part of the configuration process. See the VMware knowledge base article at https://kb.vmware.com/s/article/78029.
- An AD FS root CA certificate added to the Trusted Root Certificates Store (also called the VMware Certificate Store).
- You have created a vCenter Server administrators group in AD FS that contains the users you want to grant vCenter Server administrator privileges to.

For more information about configuring AD FS, see the Microsoft documentation.

vCenter Server and other requirements:

- vSphere 7.0 or later
- vCenter Server must be able to connect to the AD FS discovery endpoint, and the authorization, token, logout, JWKS, and any other endpoints advertised in the discovery endpoint metadata.
- You need the **VcIdentityProviders.Manage** privilege to create, update, or delete a vCenter Server Identity Provider that is required for federated authentication. To limit a user to view the Identity Provider configuration information only, assign the **VcIdentityProviders.Read** privilege.

Procedure

1 Log in with the vSphere Client to the vCenter Server.

2 Add your AD FS root CA certificate to the Trusted Root Certificates Store.

   a Navigate to **Administration > Certificates > Certificate Management**.

   b Next to **Trusted Root Store**, click **Add**.

   c Browse for the AD FS root certificate and click **Add**.

   The certificate is added in a panel under **Trusted Root Certificates**.

3 Navigate to the Configuration UI.

   a From the **Home** menu, select **Administration**.

   b Under **Single Sign On**, click **Configuration**.

4 Select the **Identity Provider** tab and obtain the Redirect URIs.

   a Click the informational “i” **icon** next to the “Change identity provider” link.

   Two Redirect URIs are displayed in the pop-up banner.

   b Copy both URIs to a file or write them down for later use in subsequent steps to configure the AD FS server.

   c Close the pop-up banner.

5 Create an OpenID Connect configuration in AD FS and configure it for vCenter Server.

   To establish a relying party trust between vCenter Server and an identity provider, you must establish the identifying information and a shared secret between them. In AD FS, you do so by creating an OpenID Connect configuration known as an Application Group, which consists of a Server application and a Web API. The two components specify the information that vCenter Server uses to trust and communicate with the AD FS server. To enable OpenID Connect in AD FS, see the VMware knowledge base article at https://kb.vmware.com/s/article/78029.

   Note the following when you create the AD FS Application Group.

   - You need the two Redirect URIs you obtained and saved from the prior step.
   - Copy the following information to a file or write it down for use when configuring the vCenter Server Identity Provider in the next step.
     - Client Identifier
     - Shared secret
     - OpenID address of the AD FS server

6 Create an identity provider on vCenter Server.

a Return to the **Identity Provider** tab in the vSphere Client.

b Click the "Change identity provider" link.

The Configure Main Identity Provider wizard opens.

c Select **Microsoft ADFS** and click **Next**.

Enter the information that you have gathered previously for the following text boxes:

- Client Identifier
- Shared Secret
- OpenID Address of the AD FS server

d Click **Next**.

e Enter user and group information for the Active Directory over LDAP connection to search for users and groups.

Option	Description
Base distinguished name for users	Base Distinguished Name for users.
Base distinguished name for groups	The base Distinguished Name for groups.
Username	ID of a user in the domain who has a minimum of read-only access to Base DN for users and groups.
Password	ID of a user in the domain who has a minimum of read-only access to Base DN for users and groups.
Primary server URL	Primary domain controller LDAP server for the domain. Use the format **`ldap://hostname:port`** or **`ldaps://hostname:port`**. The port is typically 389 for LDAP connections and 636 for LDAPS connections. For Active Directory multi-domain controller deployments, the port is typically 3268 for LDAP and 3269 for LDAPS. A certificate that establishes trust for the LDAPS endpoint of the Active Directory server is required when you use **`ldaps://`** in the primary or secondary LDAP URL.
Secondary server URL	Address of a secondary domain controller LDAP server that is used for failover.
SSL certificates	If you want to use LDAPS with your Active Directory LDAP Server or OpenLDAP Server identity source, click **`Browse`** to select a certificate.

f Click **Next**, review the information, and click **Finish**.

7 Navigate to the vCenter Single Sign-On user configuration UI.

a From the **Home** menu, select **Administration**.

b Under **Single Sign On**, click **Users and Groups**.

8 Configure group membership vCenter Server for AD FS Authorization.

   a Click the **Groups** tab.

   b Click the **Administrators** group and click **Add Members**.

   c Select the domain from the drop-down menu.

   d In the text box below the drop-down menu, enter the first few characters of AD FS group that you want to add then wait for the drop-down selection to appear.

      It might take several seconds for the selection to appear as vCenter Server establishes the connection to and searches Active Directory.

   e Select the AD FS group and add it to the Administrators group.

   f Click **Save**.

9 Verify logging in to vCenter Server with an Active Directory user.

Understanding vCenter Single Sign-On

If you are not using an external identity provider, you must understand the underlying architecture of the built-in identity provider, vCenter Single Sign-On, and how it affects installation and upgrades.

vCenter Single Sign-On Components

vCenter Single Sign-On includes the Security Token Service (STS), an administration server, the vCenter Lookup Service, and the VMware Directory Service (vmdir). The VMware Directory Service is also used for certificate management.

During installation, the following components are deployed as part of a vCenter Server deployment.

STS (Security Token Service)

The STS service issues Security Assertion Markup Language (SAML) tokens. These security tokens represent the identity of a user in one of the identity source types supported by vCenter Server. The SAML tokens allow interactive, scripted, and service users (including solution users) who authenticate successfully to vCenter Single Sign-On to use any vCenter service that vCenter Single Sign-On supports without authenticating again to each service.

The vCenter Single Sign-On service signs all tokens with a signing certificate, and stores the token signing certificate on disk. The certificate for the service itself is also stored on disk.

Administration server

The administration server allows users with administrator privileges to vCenter Single Sign-On to configure the vCenter Single Sign-On server and manage users and groups from the vSphere Client. Initially, only the user administrator@*your_domain_name* has these privileges. You can change the vSphere domain when you install vCenter Server. Do not name the domain name with your Microsoft Active Directory or OpenLDAP domain name.

VMware Directory Service (vmdir)

A VMware Directory Service (vmdir) is associated with the domain you specify during installation and is included in each vCenter Server deployment. This service is a multi-tenanted, peer-replicating directory service that makes an LDAP directory available on port 389. It also stores and manages vCenter Single Sign-On user accounts and passwords, which are secured by the SHA-512 hashing algorithm.

If your environment includes multiple instances of vCenter Server configured in linked mode, an update of vmdir content in one vmdir instance is propagated to all other instances of vmdir.

The VMware Directory Service stores not only vCenter Single Sign-On information but also certificate information.

Identity Management Service

Handles identity sources and STS authentication requests.

Using vCenter Single Sign-On with vSphere

When a user logs in to a vSphere component, or when a vCenter Server solution user accesses another vCenter Server service, vCenter Single Sign-On performs authentication. Users must be authenticated with vCenter Single Sign-On and have the necessary privileges for interacting with vSphere objects.

vCenter Single Sign-On authenticates both solution users and other users.

- Solution users represent a set of services in your vSphere environment. During installation, VMCA assigns a certificate to each solution user by default. The solution user uses that certificate to authenticate to vCenter Single Sign-On. vCenter Single Sign-On gives the solution user a SAML token, and the solution user can then interact with other services in the environment.
- When other users log in to the environment, for example, from the vSphere Client, vCenter Single Sign-On prompts for a user name and password. If vCenter Single Sign-On finds a user with those credentials in the corresponding identity source, it assigns the user a SAML token. The user can now access other services in the environment without being prompted to authenticate again.

  Which objects the user can view, and what a user can do, is usually determined by vCenter Server permission settings. vCenter Server administrators assign those permissions from the **Permissions** interface in the vSphere Client, not through vCenter Single Sign-On. See the *vSphere Security* documentation.

vCenter Single Sign-On and vCenter Server Users

Users authenticate to vCenter Single Sign-On by entering their credentials on the login page. After connecting to vCenter Server, authenticated users can view all vCenter Server instances or other vSphere objects for which their role gives them privileges. No further authentication is required.

After installation, the administrator of the vCenter Single Sign-On domain, administrator@vsphere.local by default, has administrator access to both vCenter Single Sign-On and vCenter Server. That user can then add identity sources, set the default identity source, and manage users and groups in the vCenter Single Sign-On domain.

All users that can authenticate to vCenter Single Sign-On can reset their password. See Change Your vCenter Single Sign-On Password . Only vCenter Single Sign-On administrators can reset the password for users who no longer have their password.

vCenter Single Sign-On Administrator Users

The vCenter Single Sign-On administrative interface is accessible from the vSphere Client.

To configure vCenter Single Sign-On and manage vCenter Single Sign-On users and groups, the user administrator@vsphere.local or a user in the vCenter Single Sign-On Administrators group must log in to the vSphere Client. Upon authentication, that user can access the vCenter Single Sign-On administration interface from the vSphere Client and manage identity sources and default domains, specify password policies, and perform other administrative tasks.

Note You cannot rename the vCenter Single Sign-On administrator user, which is administrator@vsphere.local by default or administrator@*mydomain* if you specified a different domain during installation. For improved security, consider creating additional named users in the vCenter Single Sign-On domain and assigning them administrative privileges. You can then stop using the administrator account.

Other User Accounts

The following user accounts are created automatically within vCenter Server in the vsphere.local domain (or the default domain that you created at installation). These user accounts are shell accounts. The vCenter Single Sign-On password policy does not apply to these accounts.

Table 4-1. Other vSphere User Accounts

Account	Description
K/M	For Kerberos key management.
krbtgt/VSPHERE.LOCAL	For Integrated Windows Authentication compatibility.
waiter-*random_string*	For Auto Deploy.

ESXi Users

Standalone ESXi hosts are not integrated with vCenter Single Sign-On. See *vSphere Security* for information on adding an ESXi host to Active Directory.

If you create local ESXi users for a managed ESXi host with the VMware Host Client, ESXCLI, or PowerCLI, vCenter Server is not aware of those users. Creating local users can therefore result in confusion, especially if you use the same user names. Users who can authenticate to vCenter Single Sign-On can view and manage ESXi hosts if they have the corresponding permissions on the ESXi host object.

Note Manage permissions for ESXi hosts through vCenter Server if possible.

How to Log In to vCenter Server Components

You can log in by connecting to the vSphere Client.

When a user logs in to a vCenter Server system from the vSphere Client, the login behavior depends on whether the user is in the domain that is set as the default identity source.

- Users who are in the default domain can log in with their user name and password.
- Users who are in a domain that has been added to vCenter Single Sign-On as an identity source but is not the default domain can log in to vCenter Server but must specify the domain in one of the following ways.
  - Including a domain name prefix, for example, MYDOMAIN\user1
  - Including the domain, for example, user1@mydomain.com
- Users who are in a domain that is not a vCenter Single Sign-On identity source cannot log in to vCenter Server. If the domain that you add to vCenter Single Sign-On is part of a domain hierarchy, Active Directory determines whether users of other domains in the hierarchy are authenticated or not.

If your environment includes an Active Directory hierarchy, see VMware Knowledge Base article 2064250 for details on supported and unsupported setups.

Groups in the vCenter Single Sign-On Domain

The vCenter Single Sign-On domain (vsphere.local by default) includes several predefined groups. Add users to one of those groups to enable them to perform the corresponding actions.

See Managing vCenter Single Sign-On Users and Groups.

For all objects in the vCenter Server hierarchy, you can assign permissions by pairing a user and a role with the object. For example, you can select a resource pool and give a group of users read privileges to that resource pool object by giving them the corresponding role.

For some services that are not managed by vCenter Server directly, membership in one of the vCenter Single Sign-On groups determines the privileges. For example, a user who is a member of the Administrators group can manage vCenter Single Sign-On. A user who is a member of the CAAdmins group can manage the VMware Certificate Authority, and a user who is in the LicenseService.Administrators group can manage licenses.

The following groups are predefined in vsphere.local. Many of these groups are internal to vsphere.local or give users high-level administrative privileges. Add users to any of these groups only after careful consideration of the risks.

Caution Do not delete any of the predefined groups in the vsphere.local domain. If you do, errors with authentication or certificate provisioning might result.

Table 4-2. Groups in the vsphere.local Domain

Privilege	Description
Users	Users in the vCenter Single Sign-On domain (vsphere.local by default).
SolutionUsers	Solution users group for vCenter services. Each solution user authenticates individually to vCenter Single Sign-On with a certificate. By default, VMCA provisions solution users with certificates. Do not add members to this group explicitly.
CAAdmins	Members of the CAAdmins group have administrator privileges for VMCA. Do not add members to this group unless you have compelling reasons.
DCAdmins	Members of the DCAdmins group can perform Domain Controller Administrator actions on VMware Directory Service. **Note** Do not manage the domain controller directly. Instead, use the `vmdir` CLI or the vSphere Client to perform corresponding tasks.
SystemConfiguration.BashShellAdministrators	A user in this group can enable and disable access to the BASH shell. By default a user who connects to the vCenter Server with SSH can access only commands in the restricted shell. Users who are in this group can access the BASH shell.
ActAsUsers	Members of Act-As Users are allowed to get Act-As tokens from vCenter Single Sign-On.
ExternalIDPUsers	This internal group is not used by vSphere. VMware vCloud Air requires this group.
SystemConfiguration.Administrators	Members of the SystemConfiguration.Administrators group can view and manage the system configuration in the vSphere Client. These users can view, start and restart services, troubleshoot services, see the available nodes, and manage those nodes.
DCClients	This group is used internally to allow the management node access to data in VMware Directory Service. **Note** Do not modify this group. Any changes might compromise your certificate infrastructure.
ComponentManager.Administrators	Members of the ComponentManager.Administrators group can invoke component manager APIs that register or unregister services, that is, modify services. Membership in this group is not necessary for read access on the services.
LicenseService.Administrators	Members of LicenseService.Administrators have full write access to all licensing-related data and can add, remove, assign, and unassign serial keys for all product assets registered in the licensing service.

Table 4-2. Groups in the vsphere.local Domain (continued)

Privilege	Description
Administrators	Administrators of the VMware Directory Service (vmdir). Members of this group can perform vCenter Single Sign-On administration tasks. Do not add members to this group unless you have compelling reasons and understand the consequences.
TrustedAdmins	Members of this group can perform VMware® vSphere Trust Authority™ configuration and administration tasks. By default, this group does not contain any members. You must add a member to this group so that you can perform vSphere Trust Authority tasks.
AutoUpdate	This group is used internally for vCenter Cloud Gateway.
SyncUsers	This group is used internally for vCenter Cloud Gateway.
vSphereClientSolutionUsers	This group is used internally for the vSphere Client.
ServiceProviderUsers	Members of this group can manage the vSphere with Tanzu and VMware Cloud on AWS infrastructure.
NsxAdministrators	This group is used for NSX.
WorkloadStorage	Workload storage group.
RegistryAdministrators	Members of this group can manage the registry.
NsxAuditors	This group is used for NSX.
NsxViAdministrators	This group is used for NSX.
SystemConfiguration.SupportUsers	Members of the SystemConfiguration.SupportUsers group can access the support bundle API.
SystemConfiguration.ReadOnly	Members of this group can access vCenter Server Appliance read-only operations.

Configuring vCenter Single Sign-On Identity Sources

When a user logs in with just a user name, vCenter Single Sign-On checks in the default identity source whether that user can authenticate. When a user logs in and includes the domain name in the login screen, vCenter Single Sign-On checks the specified domain if that domain has been added as an identity source. You can add identity sources, remove identity sources, and change the default.

You configure vCenter Single Sign-On from the vSphere Client. To configure vCenter Single Sign-On, you must have vCenter Single Sign-On administrator privileges. Having vCenter Single Sign-On administrator privileges is different from having the Administrator role on vCenter Server or ESXi. In a new installation, only the vCenter Single Sign-On administrator (administrator@vsphere.local by default) can authenticate to vCenter Single Sign-On.

Identity Sources for vCenter Server with vCenter Single Sign-On

You can use identity sources to attach one or more domains to vCenter Single Sign-On. A domain is a repository for users and groups that the vCenter Single Sign-On server can use for user authentication.

Note In vSphere 7.0 Update 2 and later, you can enable FIPS on vCenter Server. See the *vSphere Security* documentation. AD over LDAP and IWA are not supported when FIPS is enabled. Use external identity provider federation when in FIPS mode. See Configuring vCenter Server Identity Provider Federation.

An administrator can add identity sources, set the default identity source, and create users and groups in the vsphere.local identity source.

The user and group data is stored in Active Directory, OpenLDAP, or locally to the operating system of the machine where vCenter Single Sign-On is installed. After installation, every instance of vCenter Single Sign-On has the identity source *your_domain_name*, for example vsphere.local. This identity source is internal to vCenter Single Sign-On.

Note At any time, only one default domain exists. If a user from a non-default domain logs in, that user must add the domain name to authenticate successfully. The domain name is in the form:

```
DOMAIN\user
```

The following identity sources are available.

- Active Directory over LDAP. vCenter Single Sign-On supports multiple Active Directory over LDAP identity sources.
- Active Directory (Integrated Windows Authentication) versions 2003 and later. vCenter Single Sign-On allows you to specify a single Active Directory domain as an identity source. The domain can have child domains or be a forest root domain. VMware KB article 2064250 discusses Microsoft Active Directory Trusts supported with vCenter Single Sign-On.
- OpenLDAP versions 2.4 and later. vCenter Single Sign-On supports multiple OpenLDAP identity sources.

Note A future update to Microsoft Windows will change the default behavior of Active Directory to require strong authentication and encryption. This change will impact how vCenter Server authenticates to Active Directory. If you use Active Directory as your identity source for vCenter Server, you must plan to enable LDAPS. For more information about this Microsoft security update, see https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/ADV190023 and https://blogs.vmware.com/vsphere/2020/01/microsoft-ldap-vsphere-channel-binding-signing-adv190023.html.

Set the Default Domain for vCenter Single Sign-On

Each vCenter Single Sign-On identity source is associated with a domain. vCenter Single Sign-On uses the default domain to authenticate a user who logs in without a domain name. Users who belong to a domain that is not the default domain must include the domain name when they log in.

When a user logs in to a vCenter Server system from the vSphere Client, the login behavior depends on whether the user is in the domain that is set as the default identity source.

- Users who are in the default domain can log in with their user name and password.
- Users who are in a domain that has been added to vCenter Single Sign-On as an identity source but is not the default domain can log in to vCenter Server but must specify the domain in one of the following ways.
  - Including a domain name prefix, for example, MYDOMAIN\user1
  - Including the domain, for example, user1@mydomain.com
- Users who are in a domain that is not a vCenter Single Sign-On identity source cannot log in to vCenter Server. If the domain that you add to vCenter Single Sign-On is part of a domain hierarchy, Active Directory determines whether users of other domains in the hierarchy are authenticated or not.

Procedure

1. Log in with the vSphere Client to the vCenter Server.
2. Specify the user name and password for administrator@vsphere.local or another member of the vCenter Single Sign-On Administrators group.

   If you specified a different domain during installation, log in as administrator@*mydomain*.
3. Navigate to the Configuration UI.
   a. From the **Home** menu, select **Administration**.
   b. Under **Single Sign On**, click **Configuration**.
4. Under the **Identity Provider** tab, click **Identity Sources**, select an identity source, and click **Set as Default**.
5. Click **OK**.

   In the domain display, the default domain shows (default) in the Type column.

Add or Edit a vCenter Single Sign-On Identity Source

Users can log in to vCenter Server only if they are in a domain that has been added as a vCenter Single Sign-On identity source. vCenter Single Sign-On administrator users can add identity sources, or change the settings for identity sources that they added.

An identity source can be an Active Directory over LDAP, a native Active Directory (Integrated Windows Authentication) domain, or an OpenLDAP directory service. See Identity Sources for vCenter Server with vCenter Single Sign-On.

Immediately after installation, the vsphere.local domain (or the domain you specified during installation) with the vCenter Single Sign-On internal users is available.

Note If you have updated or replaced your Active Directory SSL certificate, you must remove and re-add the identity source in vCenter Server.

Prerequisites

If you are adding an Active Directory (Integrated Windows Authentication) identity source, the vCenter Server must be in the Active Directory domain. See Add a vCenter Server to an Active Directory Domain.

Procedure

1. Log in with the vSphere Client to the vCenter Server.
2. Specify the user name and password for administrator@vsphere.local or another member of the vCenter Single Sign-On Administrators group.

   If you specified a different domain during installation, log in as administrator@*mydomain*.
3. Navigate to the Configuration UI.
   a. From the **Home** menu, select **Administration**.
   b. Under **Single Sign On**, click **Configuration**.
4. Under the **Identity Provider** tab, click **Identity Sources**, and click **Add**.
5. Select the identity source and enter the identity source settings.

Option	Description
Active Directory (Integrated Windows Authentication)	Use this option for native Active Directory implementations. The machine on which the vCenter Single Sign-On service is running must be in an Active Directory domain if you want to use this option. See Active Directory Identity Source Settings.
Active Directory over LDAP	This option requires that you specify the domain controller and other information. See Active Directory over LDAP and OpenLDAP Server Identity Source Settings.
OpenLDAP	Use this option for an OpenLDAP identity source. See Active Directory over LDAP and OpenLDAP Server Identity Source Settings.

Note If the user account is locked or disabled, authentications and group and user searches in the Active Directory domain fail. The user account must have read-only access over the User and Group OU, and must be able to read user and group attributes. Active Directory provides this access by default. Use a special service user for improved security.

6 Click **Add**.

What to do next

Initially, each user is assigned the No Access role. A vCenter Server administrator must assign the user at least to the Read Only role before the user can log in. See the *vSphere Security* documentation.

Active Directory over LDAP and OpenLDAP Server Identity Source Settings

The Active Directory over LDAP identity source is preferred over the Active Directory (Integrated Windows Authentication) option. The OpenLDAP Server identity source is available for environments that use OpenLDAP.

If you are configuring an OpenLDAP identity source, see the VMware knowledge base article at http://kb.vmware.com/kb/2064977 for additional requirements.

Note A future update to Microsoft Windows will change the default behavior of Active Directory to require strong authentication and encryption. This change will impact how vCenter Server authenticates to Active Directory. If you use Active Directory as your identity source for vCenter Server, you must plan to enable LDAPS. For more information about this Microsoft security update, see https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/ADV190023 and https://blogs.vmware.com/vsphere/2020/01/microsoft-ldap-vsphere-channel-binding-signing-adv190023.html.

Table 4-3. Active Directory over LDAP and OpenLDAP Server Settings

Option	Description
Name	Name of the identity source.
Base DN for users	Base Distinguished Name for users. Enter the DN from which to start user searches. For example, cn=Users,dc=myCorp,dc=com.
Base DN for groups	The Base Distinguished Name for groups. Enter the DN from which to start group searches. For example, cn=Groups,dc=myCorp,dc=com.
Domain name	The FQDN of the domain.
Domain alias	For Active Directory identity sources, the domain's NetBIOS name. Add the NetBIOS name of the Active Directory domain as an alias of the identity source if you are using SSPI authentications. For OpenLDAP identity sources, the domain name in capital letters is added if you do not specify an alias.

Table 4-3. Active Directory over LDAP and OpenLDAP Server Settings (continued)

Option	Description
User name	ID of a user in the domain who has a minimum of read-only access to Base DN for users and groups. The ID can be in any of these formats: ■ UPN (user@domain.com) ■ NetBIOS (DOMAIN\user) ■ DN (cn=user,cn=Users,dc=domain,dc=com) The user name must be fully-qualified. An entry of "user" does not work.
Password	Password of the user who is specified by **Username**.
Connect to	Domain controller to connect to. Can be any domain controller in the domain, or specific controllers.
Primary Server URL	Primary domain controller LDAP server for the domain. You can use either the host name or the IP address. Use the format **`ldap://hostname_or_IPaddress:port`** or **`ldaps://hostname_or_IPaddress:port`**. The port is typically 389 for LDAP connections and 636 for LDAPS connections. For Active Directory multi-domain controller deployments, the port is typically 3268 for LDAP and 3269 for LDAPS. A certificate that establishes trust for the LDAPS endpoint of the Active Directory server is required when you use **`ldaps://`** in the primary or the secondary LDAP URL.
Secondary server URL	Address of a secondary domain controller LDAP server that is used for failover. You can use either the host name or the IP address.
SSL certificates	If you want to use LDAPS with your Active Directory LDAP Server or OpenLDAP Server identity source, click **`Browse`** to select a certificate. To export the root CA certificate from Active Directory, consult the Microsoft documentation.

Active Directory Identity Source Settings

If you select the Active Directory (Integrated Windows Authentication) identity source type, you can use the local machine account as your SPN (Service Principal Name) or specify an SPN explicitly. You can use this option only if the vCenter Single Sign-On server is joined to an Active Directory domain.

Prerequisites for Using an Active Directory (Integrated Windows Authentication) Identity Source

You can set up vCenter Single Sign-On to use an Active Directory (Integrated Windows Authentication) identity source only if that identity source is available. Follow the instructions in the *vCenter Server Configuration* documentation.

Note Active Directory (Integrated Windows Authentication) always uses the root of the Active Directory domain forest. To configure your Integrated Windows Authentication identity source with a child domain within your Active Directory forest, see the VMware knowledge base article at http://kb.vmware.com/kb/2070433.

Select **Use machine account** to speed up configuration. If you expect to rename the local machine on which vCenter Single Sign-On runs, specifying an SPN explicitly is preferable.

If you have enabled diagnostic event logging in your Active Directory to identify where hardening might be needed, you might see a log event with Event ID 2889 on that directory server. Event ID 2889 is generated as an anomaly rather than a security risk when using Integrated Windows Authentication. For more information about Event ID 2889, see the VMware knowledge base article at https://kb.vmware.com/s/article/78644.

Table 4-4. Add Identity Source Settings

Text Box	Description
Domain name	FQDN of the domain name, for example, mydomain.com. Do not provide an IP address. This domain name must be DNS-resolvable by the vCenter Server system.
Use machine account	Select this option to use the local machine account as the SPN. When you select this option, you specify only the domain name. Do not select this option if you expect to rename this machine.
Use Service Principal Name (SPN)	Select this option if you expect to rename the local machine. You must specify an SPN, a user who can authenticate with the identity source, and a password for the user.
Service Principal Name (SPN)	SPN that helps Kerberos to identify the Active Directory service. Include the domain in the name, for example, `STS/example.com`. The SPN must be unique across the domain. Running the `setspn -S` command checks that no duplicate is created. See the Microsoft documentation for information on `setspn`.
User Principal Name (UPN) **Password**	Name and password of a user who can authenticate with this identity source. Use the email address format, for example, `jchin@mydomain.com`. You can verify the User Principal Name with the Active Directory Service Interfaces Editor (ADSI Edit).

Add or Remove an Identity Source Using the CLI

You can use the `sso-config` utility to add or remove an identity source.

An identity source can be a native Active Directory (Integrated Windows Authentication) domain, AD over LDAP, AD over LDAP using LDAPS (LDAP over SSL), or OpenLDAP. See Identity Sources for vCenter Server with vCenter Single Sign-On. You also use the `sso-config` utility to set up smart card and RSA SecurID authentication.

Prerequisites

If you are adding an Active Directory identity source, the vCenter Server must be in the Active Directory domain. See Add a vCenter Server to an Active Directory Domain.

Enable SSH login. See Manage vCenter Server from the vCenter Server Shell.

Procedure

1. Use SSH or another remote console connection to start a session on the vCenter Server system.
2. Log in as root.
3. Change to the directory where the `sso-config` utility is located.

   ```
   cd /opt/vmware/bin
   ```

4. Refer to the `sso-config` help by running `sso-config.sh -help`, or see the VMware knowledge base article at https://kb.vmware.com/s/article/67304 for usage examples.

Use vCenter Single Sign-On with Windows Session Authentication

You can use vCenter Single Sign-On with Windows Session Authentication (SSPI). You must join the vCenter Server to an Active Directory domain before you can use SSPI.

Prerequisites

- Join the vCenter Server to an Active Directory domain. See Add a vCenter Server to an Active Directory Domain.
- Verify that the domain is set up properly. See the VMware knowledge base article at http://kb.vmware.com/kb/2064250.
- Verify that the Enhanced Authentication Plug-In is installed. See *vCenter Server Installation and Setup*.

Note When you configure vCenter Server to use federated authentication with Active Directory Federation Services, the Enhanced Authentication Plug-in only applies to configurations where vCenter Server is the identity provider (Active Directory over LDAP, Integrated Windows Authentication, and OpenLDAP configurations).

Procedure

1. Navigate to the vSphere Client login page.
2. Select the **Use Windows session authentication** check box.
3. Log in using the Active Directory user name and password.
   - If the Active Directory domain is the default identity source, log in with your user name, for example jlee.
   - Otherwise, include the domain name, for example, jlee@example.com.

Managing the vCenter Server Security Token Service

The vCenter Server Security Token Service (STS) is a Web service that issues, validates, and renews security tokens.

As a token issuer, the Security Token Service (STS) uses a private key to sign the tokens and publishes the public certificates for services to verify the token signature. vCenter Server manages the STS signing certificates and stores them in the VMware Directory Service (vmdir). Tokens can have a significant lifetime, and historically might have been signed by any one of multiple keys.

Users present their primary credentials to the STS interface to acquire tokens. The primary credential depends on the type of user.

Solution user

Valid certificate.

Other users

User name and password available in a vCenter Single Sign-On identity source.

STS authenticates the user based on the primary credentials, and constructs a SAML token that contains user attributes.

By default, the VMware Certificate Authority (VMCA) generates the STS signing certificate. You can refresh the STS signing certificate with a new VMCA certificate. You can also import and replace the default STS signing certificate with a custom or third-party generated STS signing certificate. Do not replace the STS signing certificate unless the security policy of your company requires replacing all certificates.

You can use the vSphere Client to:

- Refresh STS certificates
- Import and replace custom and third-party generated STS certificates
- View STS certificate details, such as the expiration date

You can also use the command line to replace custom and third-party generated STS certificates.

STS Certificate Duration and Expiration

A fresh installation of vSphere 7.0 Update 1 and later creates an STS signing certificate with a duration of 10 years. When an STS signing certificate is close to expiring, an alarm warns you starting at 90 days once per week, and then daily when seven days away.

Note In certain circumstances, replacing your STS signing certificates can change the duration of the certificates. When performing certificate replacement, pay attention to the issuing and expiration dates.

Refresh a vCenter Server STS Certificate Using the vSphere Client

You can refresh your vCenter Server STS signing certificates using the vSphere Client. The VMware Certificate Authority (VMCA) issues a new certificate and replaces the current certificate.

When you refresh STS signing certificates, the VMware Certificate Authority (VMCA) issues a new certificate and replaces the current certificate in the VMware Directory Service (vmdir). STS starts using the new certificate to issue new tokens. In an Enhanced Linked Mode configuration, vmdir uploads the new certificate from the issuing vCenter Server system to all linked vCenter Server systems. When you refresh STS signing certificates, you must restart the vCenter Server system, and any other vCenter Server system that is part of an Enhanced Linked Mode configuration.

If you are using a custom generated or third-party STS signing certificate, the refresh overwrites that certificate with a VMCA-issued certificate. To update custom generated or third-party STS signing certificates, use the import and replace option. See Import and Replace a vCenter Server STS Certificate Using the vSphere Client.

The VMCA-issued STS signing certificate is valid for 10 years and is not an external-facing certificate. Do not replace this certificate unless the security policy of your company requires it.

Prerequisites

For certificate management, you must supply the password of the administrator of the local domain (administrator@vsphere.local by default). If you are renewing certificates, you must also supply the vCenter Single Sign-On credentials for a user with administrator privileges on the vCenter Server system.

Procedure

1. Log in with the vSphere Client to the vCenter Server.
2. Specify the user name and password for administrator@vsphere.local or another member of the vCenter Single Sign-On Administrators group.

   If you specified a different domain during installation, log in as administrator@*mydomain*.

3 Navigate to the Certificate Management UI.

   a From the **Home** menu, select **Administration**.

   b Under **Certificates**, click **Certificate Management**.

4 If the system prompts you, enter the credentials of your vCenter Server.

5 Under **STS Signing Certificate**, click **Actions > Refresh with vCenter certificate**.

   If you are using a custom generated or third-party STS signing certificate, the refresh action overwrites that certificate with a VMCA-generated certificate.

   Note If you were using third-party certificates for compliance reasons, the refresh might cause your vCenter Server systems to go out of compliance. Also, if you are using a custom generated or third-party STS signing certificate, the Security Token Service no longer uses that custom or third-party certificate for token signing.

6 Click **Refresh**.

   The VMCA refreshes the STS signing certificate on this vCenter Server system and on any linked vCenter Server systems.

7 (Optional) If the **Force Refresh** button appears, vCenter Single Sign-On has detected a problem. Before clicking **Force Refresh**, consider the following potential results.

   - If all the impacted vCenter Server systems are not running at least vSphere 7.0 Update 3, they do not support the certificate refresh.
   - Selecting **Force Refresh** requires that you restart all vCenter Server systems and can render those systems inoperable until you do so.

   a If you are unsure of the impact, click **Cancel** and research your environment.

   b If you are sure of the impact, click **Force Refresh** to proceed with the refresh then manually restart your vCenter Server systems.

What to do next

To ensure that all the STS services in an Enhanced Linked Mode configuration validate the new tokens, you must restart the linked vCenter Server systems. See the topic about how to reboot vCenter Server in the *vCenter Server Configuration* documentation.

Import and Replace a vCenter Server STS Certificate Using the vSphere Client

You can import and replace the vCenter Server STS certificate with a custom generated or third-party certificate using the vSphere Client client.

To import and replace the default STS signing certificate, you must first generate a new certificate. When you import and replace STS signing certificates, the VMware Directory Service (vmdir) uploads the new certificate from the issuing vCenter Server system to all linked vCenter Server systems.

The STS certificate is not an external-facing certificate. Do not replace this certificate unless the security policy of your company requires it.

Prerequisites

For certificate management, you must supply the password of the administrator of the local domain (administrator@vsphere.local by default). You also must supply the vCenter Single Sign-On credentials for a user with administrator privileges on the vCenter Server system.

Procedure

1. Log in with the vSphere Client to the vCenter Server.
2. Specify the user name and password for administrator@vsphere.local or another member of the vCenter Single Sign-On Administrators group.

   If you specified a different domain during installation, log in as administrator@*mydomain*.
3. Navigate to the Certificate Management UI.
   a. From the **Home** menu, select **Administration**.
   b. Under **Certificates**, click **Certificate Management**.
4. If the system prompts you, enter the credentials of your vCenter Server.
5. Under **STS Signing Certificate**, click **Actions > Import and Replace**.
6. Select the PEM file.

   The PEM file includes the signing certificate chain and the private key.
7. Click **Replace**.

   The STS signing certificate is replaced on this vCenter Server system and on any linked vCenter Server systems.
8. Restart the vCenter Server system, and any other vCenter Server system that is part of an Enhanced Linked Mode configuration.

   See the topic about how to reboot vCenter Server in the *vCenter Server Configuration* documentation.

Replace a vCenter Server STS Certificate Using the Command Line

You can replace the vCenter Server STS certificate with a custom generated or third-party certificate using the CLI.

To use a company required certificate or to refresh a certificate that is near expiration, you can replace the existing STS signing certificate. To replace the default STS signing certificate, you must first generate a new certificate.

The STS certificate is not an external-facing certificate. Do not replace this certificate unless the security policy of your company requires it.

Caution You must use the procedures described here. Do not replace the certificate directly in the file system.

Prerequisites

Enable SSH login to vCenter Server. See Manage vCenter Server from the vCenter Server Shell.

Procedure

1. Log in to the vCenter Server shell as root.
2. Create a certificate.
   a. Create a top-level directory to hold the new certificate and verify the location of the directory.

```
mkdir newsts
cd newsts
pwd
#resulting output: /root/newsts
```

   b. Copy the `certool.cfg` file into the new directory.

```
cp /usr/lib/vmware-vmca/share/config/certool.cfg /root/newsts
```

   c. Using a command-line editor such as Vim, open your copy of the `certool.cfg` file and edit it to use the local vCenter Server IP address and hostname. The country is required and has to be two characters, as shown in the following example.

```
#
# Template file for a CSR request
#

# Country is needed and has to be 2 characters
Country = US
Name = STS
Organization = ExampleInc
OrgUnit = ExampleInc Dev
State = Indiana
Locality = Indianapolis
IPAddress = 10.0.1.32
Email = chen@exampleinc.com
Hostname = homecenter.exampleinc.local
```

   d. Generate the key.

```
/usr/lib/vmware-vmca/bin/certool --server localhost --genkey --privkey=/root/newsts/
sts.key --pubkey=/root/newsts/sts.pub
```

e Generate the certificate.

```
/usr/lib/vmware-vmca/bin/certool --gencert --cert=/root/newsts/newsts.cer --privkey=/
root/newsts/sts.key --config=/root/newsts/certool.cfg
```

f Create a PEM file with the certificate chain and private key.

```
cat newsts.cer /var/lib/vmware/vmca/root.cer sts.key > newsts.pem
```

3 Update the STS signing certificate, for example:

```
/opt/vmware/bin/sso-config.sh -set_signing_cert -t vsphere.local /root/newsts/newsts.pem
```

4 Restart the vCenter Server system, and any other vCenter Server system that is part of an Enhanced Linked Mode configuration. See the topic about how to reboot vCenter Server in the *vCenter Server Configuration* documentation.

For authentication to work correctly, you must restart vCenter Server. Both the STS service and the vSphere Client are restarted.

View the Active vCenter Server STS Signing Certificate Chain

You can use the vSphere Client to view the active vCenter Server STS signing certificate chain.

You can view the following information on the active STS certificate.

- "Valid until" date
- A green check for a valid certificate, and an orange check warning of an expired certificate
- A **View Details** link to show the active certificate chain

Procedure

1 Log in with the vSphere Client to the vCenter Server.

2 Enter the user name and password for a user that has at least Read privileges.

3 Navigate to the Certificate Management UI.

a From the **Home** menu, select **Administration**.

b Under **Certificates**, click **Certificate Management**.

4 If the system prompts you, enter the credentials of your vCenter Server.

5 To view details for the active STS certificate, click **View Details**.

Determine the Expiration Date of an LDAPS SSL Certificate

When using Active Directory over LDAPS, you can upload an SSL certificate for the LDAP traffic. SSL certificates expire after a predefined lifespan. You can view the certificate's expiration date so that you know to replace or renew the certificate before it expires.

vCenter Server alerts you when an active LDAP SSL certificate is close to its expiration date.

You see certificate expiration information only if you use Active Directory over LDAP or an OpenLDAP identity source and specify an `ldaps://` URL for the server.

Prerequisites

Enable SSH login to vCenter Server. See Manage vCenter Server from the vCenter Server Shell.

Procedure

1. Log in as root to the vCenter Server.
2. Run the following command.

   ```
   /opt/vmware/bin/sso-config.sh -get_identity_sources
   ```

   Ignore the SLF4J messages.
3. To determine the expiration date, view the SSL certificate's details and verify the `NotAfter` field.

Managing vCenter Single Sign-On Policies

vCenter Single Sign-On policies enforce the security rules for local accounts and tokens in general. You can view and edit the default vCenter Single Sign-On password policy, lockout policy, and token policy.

Edit the vCenter Single Sign-On Password Policy

The vCenter Single Sign-On password policy determines the password format and password expiration. Password policy applies only to users in the vCenter Single Sign-On domain (vsphere.local).

By default, vCenter Single Sign-On built-in user account passwords expire after 90 days. The vSphere Client reminds you when your password is about to expire.

See Change Your vCenter Single Sign-On Password .

Note The administrator account (administrator@vsphere.local) does not get locked out nor does its password expire. Proper security practice is to audit logins from this account and rotate the password regularly.

Procedure

1. Log in with the vSphere Client to the vCenter Server.
2. Specify the user name and password for administrator@vsphere.local or another member of the vCenter Single Sign-On Administrators group.

   If you specified a different domain during installation, log in as administrator@*mydomain*.

3 Navigate to the Configuration UI.

   a From the **Home** menu, select **Administration**.

   b Under **Single Sign On**, click **Configuration**.

4 Click the **Local Accounts** tab.

5 Click **Edit** for the **Password Policy** row.

6 Edit the password policy.

Option	Description
Description	Password policy description.
Maximum lifetime	Maximum number of days that a password is valid before the user must change it. The maximum number of days you can enter is 999999999. A value of zero (0) means that the password never expires.
Restrict reuse	Number of previous passwords that cannot be reused. For example, if you enter 6, the user cannot reuse any of the last six passwords.
Maximum length	Maximum number of characters that are allowed in the password.
Minimum length	Minimum number of characters required in the password. The minimum length must be no less than the combined minimum of alphabetic, numeric, and special character requirements.
Character requirements	Minimum number of different character types that are required in the password. You can specify the number of each type of character, as follows: ■ Special: & # % ■ Alphabetic: A b c D ■ Uppercase: A B C ■ Lowercase: a b c ■ Numeric: 1 2 3 ■ Identical Adjacent: The number must be greater than 0. For example, if you enter 1, the following password is not allowed: p@$$word. The minimum number of alphabetic characters must be no less than the combined uppercase and lowercase characters. Non-ASCII characters are supported in passwords. In earlier versions of vCenter Single Sign-On, limitations on supported characters exist.

7 Click **Save**.

Edit the vCenter Single Sign-On Lockout Policy

If a user attempts to log in with incorrect credentials, a vCenter Single Sign-On lockout policy specifies when the user's vCenter Single Sign-On account is locked. Administrators can edit the lockout policy.

If a user logs in to vsphere.local multiple times with the wrong password, the user is locked out. The lockout policy allows administrators to specify the maximum number of failed login attempts, and set the time interval between failures. The policy also specifies how much time must elapse before the account is automatically unlocked.

Note The lockout policy applies only to user accounts, not to system accounts such as administrator@vsphere.local.

Procedure

1 Log in with the vSphere Client to the vCenter Server.

2 Specify the user name and password for administrator@vsphere.local or another member of the vCenter Single Sign-On Administrators group.

   If you specified a different domain during installation, log in as administrator@*mydomain*.

3 Navigate to the Configuration UI.

   a From the **Home** menu, select **Administration**.

   b Under **Single Sign On**, click **Configuration**.

4 Click the **Local Accounts** tab.

5 Click **Edit** for the **Lockout Policy** row.

   You might need to scroll down to see the **Lockout Policy** row.

6 Edit the parameters.

Option	Description
Description	Optional description of the lockout policy.
Maximum number of failed login attempts	Maximum number of failed login attempts that are allowed before the account is locked.
Time interval between failures	Time period in which failed login attempts must occur to trigger a lockout.
Unlock time	Amount of time that the account remains locked. If you enter 0, the administrator must unlock the account explicitly.

7 Click **Save**.

Edit the vCenter Single Sign-On Token Policy

The vCenter Single Sign-On token policy specifies token properties such as the clock tolerance and renewal count. You can edit the token policy to ensure that the token specification conforms to security standards in your corporation.

Procedure

1 Log in with the vSphere Client to the vCenter Server.

2 Specify the user name and password for administrator@vsphere.local or another member of the vCenter Single Sign-On Administrators group.

   If you specified a different domain during installation, log in as administrator@*mydomain*.

3 Navigate to the Configuration UI.

   a From the **Home** menu, select **Administration**.

   b Under **Single Sign On**, click **Configuration**.

4 Click the **Local Accounts** tab.

5 Click **Edit** for the **Token Trustworthiness** row.

   You might need to scroll down to see the **Token Trustworthiness** row.

6 Edit the token policy configuration parameters.

Option	Description
Clock Tolerance	Time difference, in milliseconds, that vCenter Single Sign-On tolerates between a client clock and the domain controller clock. If the time difference is greater than the specified value, vCenter Single Sign-On declares the token invalid.
Maximum Token Renewal Count	Maximum number of times that a token can be renewed. After the maximum number of renewal attempts, a new security token is required.
Maximum Token Delegation Count	Holder-of-key tokens can be delegated to services in the vSphere environment. A service that uses a delegated token performs the service on behalf of the principal that provided the token. A token request specifies a DelegateTo identity. The DelegateTo value can either be a solution token or a reference to a solution token. This value specifies how many times a single holder-of-key token can be delegated.
Maximum Bearer Token Lifetime	Bearer tokens provide authentication based only on possession of the token. Bearer tokens are intended for short-term, single-operation use. A bearer token does not verify the identity of the user or entity that is sending the request. This value specifies the lifetime value of a bearer token before the token has to be reissued.
Maximum Holder-of-Key Token Lifetime	Holder-of-key tokens provide authentication based on security artifacts that are embedded in the token. Holder-of-key tokens can be used for delegation. A client can obtain a holder-of-key token and delegate that token to another entity. The token contains the claims to identify the originator and the delegate. In the vSphere environment, a vCenter Server system obtains delegated tokens on a user's behalf and uses those tokens to perform operations. This value determines the lifetime of a holder-of-key token before the token is marked invalid.

7 Click **Save**.

Edit Password Expiration Notification for Active Directory (Integrated Windows Authentication) Users

The Active Directory password expiration notification is separate from the vCenter Server SSO password expiration. The default password expiration notification for an Active Directory user is 30 days but the actual password expiration depends on your Active Directory system.
The vSphere Client controls the expiration notification. You can change the default expiration notification to meet the security standards in your corporation.

Prerequisites

- Enable SSH login to vCenter Server. See Manage vCenter Server from the vCenter Server Shell.

Procedure

1. Log in to the vCenter Server shell as a user with administrator privileges.

   The default user with the super administrator role is root.
2. Change directory to the location of the vSphere Client `webclient.properties` file.

   ```
   cd /etc/vmware/vsphere-ui
   ```
3. Open the `webclient.properties` file with a text editor.
4. Edit the following variable.

   ```
   sso.pending.password.expiration.notification.days = 30
   ```
5. Restart the vSphere Client.

   ```
   service-control --stop vsphere-ui
   service-control --start vsphere-ui
   ```

Managing vCenter Single Sign-On Users and Groups

A vCenter Single Sign-On administrator user can manage users and groups in the vsphere.local domain from the vSphere Client.

The vCenter Single Sign-On administrator user can perform the following tasks.

Add vCenter Single Sign-On Users

Users listed on the **Users** tab in the vSphere Client are internal to vCenter Single Sign-On and belong to the vsphere.local domain. You add users to that domain from one of the vCenter Single Sign-On management interfaces.

You can select other domains and view information about the users in those domains, but you cannot add users to other domains from a vCenter Single Sign-On management interface.

Procedure

1. Log in with the vSphere Client to the vCenter Server.
2. Specify the user name and password for administrator@vsphere.local or another member of the vCenter Single Sign-On Administrators group.

   If you specified a different domain during installation, log in as administrator@*mydomain*.
3. Navigate to the vCenter Single Sign-On user configuration UI.
   a. From the **Home** menu, select **Administration**.
   b. Under **Single Sign On**, click **Users and Groups**.
4. If vsphere.local is not the currently selected domain, select it from the drop-down menu.

   You cannot add users to other domains.
5. On the **Users** tab, click **Add**.
6. Enter a user name and password for the new user.

   The maximum number of characters allowed for the user name is 300.

   You cannot change the user name after you create a user. The password must meet the password policy requirements for the system.
7. (Optional) Enter the first name and the last name of the new user.
8. (Optional) Enter an email address and description for the user.
9. Click **Add**.

Results

When you add a user, that user initially has no privileges to perform management operations.

What to do next

Add the user to a group in the vsphere.local domain, for example, to the group of users who can administer VMCA (CAAdmins) or to the group of users who can administer vCenter Single Sign-On (Administrators). See Add Members to a vCenter Single Sign-On Group.

Disable and Enable vCenter Single Sign-On Users

When a vCenter Single Sign-On user account is disabled, the user cannot log in to the vCenter Single Sign-On server until an administrator enables the account. You can disable and enable accounts from one of the vCenter Single Sign-On management interfaces.

Disabled user accounts remain available in the vCenter Single Sign-On system, but the user cannot log in or perform operations on the server. Users with administrator privileges can disable and enable accounts from the vCenter **Users and Groups** page.

Prerequisites

You must be a member of the vCenter Single Sign-On Administrators group to disable and enable vCenter Single Sign-On users.

Procedure

1. Log in with the vSphere Client to the vCenter Server.
2. Specify the user name and password for administrator@vsphere.local or another member of the vCenter Single Sign-On Administrators group.

   If you specified a different domain during installation, log in as administrator@*mydomain*.
3. Navigate to the vCenter Single Sign-On user configuration UI.
   a. From the **Home** menu, select **Administration**.
   b. Under **Single Sign On**, click **Users and Groups**.
4. Select a user name, click the vertical ellipsis icon, and click **Disable**.
5. Click **OK**.
6. To enable the user again, click the vertical ellipsis icon, click **Enable**, and click **OK**.

Delete a vCenter Single Sign-On User

You can delete users that are in the vsphere.local domain from a vCenter Single Sign-On management interface. You cannot delete local operating system users or users in another domain from a vCenter Single Sign-On management interface.

Caution If you delete the administrator user in the vsphere.local domain, you can no longer log in to vCenter Single Sign-On. Reinstall vCenter Server and its components.

Procedure

1. Log in with the vSphere Client to the vCenter Server.
2. Specify the user name and password for administrator@vsphere.local or another member of the vCenter Single Sign-On Administrators group.

   If you specified a different domain during installation, log in as administrator@*mydomain*.
3. Navigate to the vCenter Single Sign-On user configuration UI.
   a. From the **Home** menu, select **Administration**.
   b. Under **Single Sign On**, click **Users and Groups**.
4. Select **Users**, and select the vsphere.local domain from the drop-down menu.
5. In the list of users, select the user that you want to delete and click the vertical ellipsis icon.
6. Click **Delete**.

   Proceed with caution. You cannot undo this action.

Edit a vCenter Single Sign-On User

You can change the password or other details of a vCenter Single Sign-On user from a vCenter Single Sign-On management interface. You cannot rename users in the vsphere.local domain. That means you cannot rename administrator@vsphere.local.

You can create additional users with the same privileges as administrator@vsphere.local.

vCenter Single Sign-On users are stored in the vCenter Single Sign-On vsphere.local domain.

You can review the vCenter Single Sign-On password policies from the vSphere Client. Log in as administrator@vsphere.local and from the **Administration** menu, select **Configuration > Local Accounts > Password Policy**.

See also Edit the vCenter Single Sign-On Password Policy.

Procedure

1. Log in with the vSphere Client to the vCenter Server.
2. Specify the user name and password for administrator@vsphere.local or another member of the vCenter Single Sign-On Administrators group.

   If you specified a different domain during installation, log in as administrator@*mydomain*.
3. Navigate to the vCenter Single Sign-On user configuration UI.
   a. From the **Home** menu, select **Administration**.
   b. Under **Single Sign On**, click **Users and Groups**.
4. Click **Users**.
5. Click the vertical ellipsis icon and select **Edit**.
6. Edit the user attributes.

   You cannot change the user name of the user.

   The password must meet the password policy requirements for the system.
7. Click **OK**.

Add a vCenter Single Sign-On Group

The vCenter Single Sign-On **Groups** tab shows groups in the local domain, vsphere.local by default. You add groups if you need a container for group members (principals).

You cannot add groups to other domains, for example, the Active Directory domain, from the vCenter Single Sign-On **Groups** tab.

If you do not add an identity source to vCenter Single Sign-On, creating groups and adding users can help you organize the local domain.

Procedure

1. Log in with the vSphere Client to the vCenter Server.

2 Specify the user name and password for administrator@vsphere.local or another member of the vCenter Single Sign-On Administrators group.

   If you specified a different domain during installation, log in as administrator@*mydomain*.

3 Navigate to the vCenter Single Sign-On user configuration UI.

   a From the **Home** menu, select **Administration**.

   b Under **Single Sign On**, click **Users and Groups**.

4 Select **Groups**, and click **Add Group**.

5 Enter a name and description for the group.

   The maximum number of characters allowed for the group name is 300. You cannot change the group name after you create the group.

6 From the **Add Members** drop-down menu, select the identity source that contains the member to add to the group.

   If you have configured an external identity provider such as AD FS, the domain of that identity provider is available to select in the **Add Members** drop-down menu.

7 Enter a search term.

8 Select the member.

   You can add more than one member.

9 Click **Add**.

What to do next

See Add Members to a vCenter Single Sign-On Group.

Add Members to a vCenter Single Sign-On Group

Members of a vCenter Single Sign-On group can be users or other groups from one or more identity sources. You can add new members from the vSphere Client.

See the VMware knowledge base article at http://kb.vmware.com/kb/2095342 for the background information.

Groups listed on the **Groups** tab in the Web interface are part of the vsphere.local domain. See Groups in the vCenter Single Sign-On Domain.

Procedure

1 Log in with the vSphere Client to the vCenter Server.

2 Specify the user name and password for administrator@vsphere.local or another member of the vCenter Single Sign-On Administrators group.

   If you specified a different domain during installation, log in as administrator@*mydomain*.

3 Navigate to the vCenter Single Sign-On user configuration UI.

   a From the **Home** menu, select **Administration**.

   b Under **Single Sign On**, click **Users and Groups**.

4 Click **Groups** and click the group (for example, Administrators).

5 From the **Add Members** drop-down menu, select the identity source that contains the member to add to the group.

   If you have configured an external identity provider, such as AD FS, the domain of that identity provider is available to select in the **Add Members** drop-down menu.

6 Enter a search term.

7 Select the member.

   You can add more than one member.

8 Click **Save**.

Remove Members from a vCenter Single Sign-On Group

You can remove members from a vCenter Single Sign-On group by using the vSphere Client. When you remove a member (user or group) from a group, you do not delete the member from the system.

Procedure

1 Log in with the vSphere Client to the vCenter Server.

2 Specify the user name and password for administrator@vsphere.local or another member of the vCenter Single Sign-On Administrators group.

   If you specified a different domain during installation, log in as administrator@*mydomain*.

3 Navigate to the vCenter Single Sign-On user configuration UI.

   a From the **Home** menu, select **Administration**.

   b Under **Single Sign On**, click **Users and Groups**.

4 Select **Groups** and click a group.

5 In the list of group members, select the user or group that you want to remove and click the vertical ellipsis icon.

6 Click **Remove Member**.

7 Click **Remove**.

Results

The user is removed from the group, but is still available in the system.

Change Your vCenter Single Sign-On Password

Users in the local domain, vsphere.local by default, can change their vCenter Single Sign-On passwords from the vSphere Client. Users in other domains change their passwords following the rules for that domain.

The vCenter Single Sign-On lockout policy determines when your password expires. By default, vCenter Single Sign-On passwords expire after 90 days, but administrator passwords such as the password for administrator@vsphere.local do not expire. vCenter Single Sign-On management interfaces show a warning when your password is about to expire.

Note You can change a password only if it is not expired.

If the password is expired, the administrator of the local domain, administrator@vsphere.local by default, can reset the password by using the `dir-cli password reset` command. Only members of the Administrator group for the vCenter Single Sign-On domain can reset passwords.

Procedure

1. Log in with the vSphere Client to the vCenter Server.
2. Specify the user name and password for administrator@vsphere.local or another member of the vCenter Single Sign-On Administrators group.

   If you specified a different domain during installation, log in as administrator@*mydomain*.
3. In the upper navigation pane, to the right of the Help menu, click your user name to pull down the menu.

   As an alternative, you can select **Single Sign On > Users and Groups** and select **Edit** from the vertical ellipsis menu.
4. Enter your current password.
5. Enter a new password and confirm it.

   The password must conform to the password policy.
6. Click **Save**.

Understanding Other Authentication Options

Starting with vSphere 7.0, external identity provider federation is the preferred authentication method for vCenter Server. You can still authenticate by using Windows session Authentication (SSPI), by using a smart card (UPN-based Common Access Card or CAC), or by using an RSA SecurID token.

Two-Factor Authentication Methods

The two-factor authentication methods are often required by government agencies or large enterprises.

External Identity Provider Federation

External identity provider federation enables you to use the authentication mechanisms supported by the external identity provider, including multi-factor authentication.

Smart Card Authentication

Smart card authentication allows access only to users who attach a physical card reader to the computer that they log in to. An example is Common Access Card (CAC) authentication.

The administrator can deploy the PKI so that the smart card certificates are the only client certificates that the CA issues. For such deployments, only smart card certificates are presented to the user. The user selects a certificate, and is prompted for a PIN. Only users who have both the physical card and the PIN that matches the certificate can log in.

RSA SecurID Authentication

For RSA SecurID authentication, your environment must include a correctly configured RSA Authentication Manager. If the vCenter Server is configured to point to the RSA server, and if RSA SecurID Authentication is enabled, users can log in with their user name and token.

See the two vSphere Blog posts about RSA SecurID setup for details.

Note vCenter Single Sign-On supports only native SecurID. It does not support RADIUS authentication.

Specifying a Nondefault Authentication Method

Administrators can set up a nondefault authentication method from the vSphere Client, or by using the `sso-config` script.

- For smart card authentication, you can perform the vCenter Single Sign-On setup from the vSphere Client or by using `sso-config`. Setup includes enabling smart card authentication and configuring certificate revocation policies.
- For RSA SecurID, you use the `sso-config` script to configure RSA Authentication Manager for the domain, and to enable RSA token authentication. You cannot configure RSA SecurID authentication from the vSphere Client. However, if you enable RSA SecurID, that authentication method appears in the vSphere Client.

Combining Authentication Methods

You can enable or disable each authentication method separately by using `sso-config`. Leave user name and password authentication enabled initially, while you are testing a two-factor authentication method, and set only one authentication method to enabled after testing.

Smart Card Authentication Login

A smart card is a small plastic card with an embedded integrated circuit chip. Many government agencies and large enterprises use smart cards such as Common Access Card (CAC) to increase the security of their systems and to comply with security regulations. A smart card is used in environments where each machine includes a smart card reader. Smart card hardware drivers that manage the smart card are typically preinstalled.

Note In vSphere 7.0 Update 2 and later, you can enable FIPS on vCenter Server. See the *vSphere Security* documentation. RSA SecureID and CAC authentication are not supported when FIPS is enabled. Use external identity provider federation for MFA authentication. See Configuring vCenter Server Identity Provider Federation.

Users who log in to a vCenter Server system are prompted to authenticate with a smart card and PIN combination, as follows.

1. When a user inserts the smart card into the smart card reader, the browser reads the certificates on the card.
2. The browser prompts the user to select a certificate, then prompts the user for the PIN for that certificate.
3. vCenter Single Sign-On checks whether the certificate on the smart card is known. If revocation checking is turned on, vCenter Single Sign-On also checks whether the certificate is revoked.
4. If the certificate is known to vCenter Single Sign-On, and is not a revoked certificate, the user is authenticated and can perform tasks for which that the user has permissions.

Note It usually makes sense to leave user name and password authentication enabled during testing. After testing is complete, deactivate user name and password authentication and activate smart card authentication. Subsequently, the vSphere Client allows only smart card login. Only users with root or administrator privileges on the machine can reactivate user name and password authentication by logging in to the vCenter Server directly.

Configuring and Using Smart Card Authentication

You can set up your environment to require smart card authentication when a user connects to a vCenter Server from the vSphere Client.

Configuring smart card authentication involves first setting up the reverse proxy then enabling and configuring the smart card authentication itself. You use the `sso-config` utility to manage smart card authentication.

Configure the Reverse Proxy to Request Client Certificates

Before you enable smart card authentication, you must configure the reverse proxy on the vCenter Server system.

Reverse proxy configuration is required in vSphere 6.5 and later.

Prerequisites

Copy the CA certificates to the vCenter Server system.

Note vCenter Server 7.0 supports the HTTP/2 protocol. All modern browsers and applications, including the vSphere Client, connect to vCenter Server using HTTP/2. However, smart card authentication requires use of the HTTP/1.1 protocol. Enabling smart card authentication disables Application-Layer Protocol Negotiation (ALPN, https://tools.ietf.org/html/rfc7301) for HTTP/2, effectively preventing the browser from using HTTP/2. Applications that use only HTTP/2, without relying on ALPN, continue to work.

Procedure

1. Log in to the vCenter Server shell as the root user.
2. Create a trusted client CA store.

   This store contains the trusted issuing CA's certificates for client certificate. The client here is the browser from which the smart card process prompts the end user for information.

   The following example shows how you create a certificate store on the vCenter Server.

   For a single certificate:

   ```
   cd /usr/lib/vmware-sso/
   openssl x509 -inform PEM -in xyzCompanySmartCardSigningCA.cer > /usr/lib/vmware-sso/vmware-sts/conf/clienttrustCA.pem
   ```

   For multiple certificates:

   ```
   cd /usr/lib/vmware-sso/
   openssl x509 -inform PEM -in xyzCompanySmartCardSigningCA.cer >> /usr/lib/vmware-sso/vmware-sts/conf/clienttrustCA.pem
   ```

3. Make a backup of the `/etc/vmware-rhttpproxy/config.xml` file that includes the reverse proxy definition, and open `config.xml` in an editor.
4. Make the following changes and save the file.

   ```
   <http>
   <maxConnections> 2048 </maxConnections>
   <requestClientCertificate>true</requestClientCertificate>
   <clientCertificateMaxSize>4096</clientCertificateMaxSize>
   <clientCAListFile>/usr/lib/vmware-sso/vmware-sts/conf/clienttrustCA.pem</clientCAListFile>
   </http>
   ```

   The `config.xml` file includes some of these elements. Uncomment, update, or add the elements as needed.
5. Restart the service.

   ```
   /usr/lib/vmware-vmon/vmon-cli --restart rhttpproxy
   ```

Use the Command Line to Manage Smart Card Authentication

You can use the `sso-config` utility to manage smart card authentication from the command line. The utility supports all smart card configuration tasks.

You can find the `sso-config` script at the following location:

```
/opt/vmware/bin/sso-config.sh
```

Configuration of supported authentication types and revocation settings is stored in VMware Directory Service and replicated across all vCenter Server instances in a vCenter Single Sign-On domain.

If user name and password authentication are disabled, and if problems occur with smart card authentication, users cannot log in. In that case, a root or administrator user can turn on user name and password authentication from the vCenter Server command line. The following command enables user name and password authentication.

```
sso-config.sh -set_authn_policy -pwdAuthn true -t tenant_name
```

If you use the default tenant, use vsphere.local as the tenant name.

If you use OCSP for revocation check, you can rely on the default OCSP specified in the smart card certificate AIA extension. You can also override the default and configure one or more alternative OCSP responders. For example, you can set up OCSP responders that are local to the vCenter Single Sign-On site to process the revocation check request.

Note If your certificate does not have OCSP defined, enable CRL (certificate revocation list) instead.

Prerequisites

- Verify that an enterprise Public Key Infrastructure (PKI) is set up in your environment, and that certificates meet the following requirements:
  - A User Principal Name (UPN) must correspond to an Active Directory account in the Subject Alternative Name (SAN) extension.
  - The certificate must specify Client Authentication in the Application Policy or Extended Key Usage field or the browser does not show the certificate.
- Add an Active Directory identity source to vCenter Single Sign-On.
- Assign the vCenter Server Administrator role to one or more users in the Active Directory identity source. Those users can then perform management tasks because they can authenticate and they have vCenter Server administrator privileges.
- Ensure that you have set up the reverse proxy and restarted the physical or virtual machine.

Procedure

1 Obtain the certificates and copy them to a folder that the `sso-config` utility can see.

   a Log in to the appliance console, either directly or by using SSH.

   b Enable the appliance shell, as follows.

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

   c Use WinSCP or a similar utility to copy the certificates to the `/usr/lib/vmware-sso/vmware-sts/conf` on the vCenter Server.

   d Optionally disable the shell, as follows.

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

2 To enable smart cart authentication, run the following command.

   ```
   sso-config.sh -set_authn_policy -certAuthn true -cacerts
   first_trusted_cert.cer,second_trusted_cert.cer  -t tenant
   ```

   For example:

   ```
   sso-config.sh -set_authn_policy -certAuthn true -cacerts MySmartCA1.cer,MySmartCA2.cer  -t
   vsphere.local
   ```

   Separate multiple certificates with commas, but do not put spaces after the comma.

3 To disable all other authentication methods, run the following commands.

   ```
   sso-config.sh -set_authn_policy -pwdAuthn false -t vsphere.local
   sso-config.sh -set_authn_policy -winAuthn false -t vsphere.local
   sso-config.sh -set_authn_policy -securIDAuthn false -t vsphere.local
   ```

4 (Optional) To set a certificate policies allowlist, run the following command.

   ```
   sso-config.sh -set_authn_policy -certPolicies policies
   ```

   To specify multiple policies, separate them with a comma, for example:

   ```
   sso-config.sh -set_authn_policy -certPolicies
   2.16.840.1.101.2.1.11.9,2.16.840.1.101.2.1.11.19
   ```

   This allowlist specifies object IDs of policies that are allowed in the certificate's certificate policy extension. An X509 certificate can have a Certificate Policy extension.

5 (Optional) Turn on and configure revocation checking using OCSP.

a Turn on revocation checking using OCSP.

```
sso-config.sh  -set_authn_policy -t tenantName  -useOcsp true
```

b If the OCSP responder link is not provided by the AIA extension of the certificates, provide the overriding OCSP responder URL and OCSP authority certificate.

The alternative OCSP is configured for each vCenter Single Sign-On site. You can specify more than one alternative OCSP responder for your vCenter Single Sign-On site to allow for failover.

```
sso-config.sh -t tenant -add_alt_ocsp  [-siteID yourPSCClusterID] -ocspUrl http://
ocsp.xyz.com/ -ocspSigningCert yourOcspSigningCA.cer
```

Note The configuration is applied to the current vCenter Single Sign-On site by default. Specify the `siteID` parameter only if you configure alternative OCSP for other vCenter Single Sign-On sites.

Consider the following example.

```
 .sso-config.sh -t vsphere.local -add_alt_ocsp
-ocspUrl http://failover.ocsp.nsn0.rcvs.nit.disa.mil/ -ocspSigningCert ./
DOD_JITC_EMAIL_CA-29__0x01A5__DOD_JITC_ROOT_CA_2.cer
 Adding alternative OCSP responder for tenant :vsphere.local
 OCSP responder is added successfully!
 [
 site::   78564172-2508-4b3a-b903-23de29a2c342
     [
     OCSP url::   http://ocsp.nsn0.rcvs.nit.disa.mil/
     OCSP signing CA cert:   binary value]
     ]
     [
     OCSP url::   http://failover.ocsp.nsn0.rcvs.nit.disa.mil/
     OCSP signing CA cert:   binary value]
     ]
 ]
```

c To display the current alternative OCSP responder settings, run this command.

```
sso-config.sh -t tenantName -get_alt_ocsp]
```

d To remove the current alternative OCSP responder settings, run this command.

```
sso-config.sh -t tenantName -delete_alt_ocsp [-allSite] [-siteID
pscSiteID_for_the_configuration]
```

6 (Optional) To list configuration information, run the following command.

```
sso-config.sh -get_authn_policy -t tenantName
```

Manage Smart Card Authentication

You can enable and disable smart card authentication, customize the login banner, and set up the revocation policy from the vSphere Client.

If smart card authentication is enabled and other authentication methods are disabled, users are then required to log in using smart card authentication.

If user name and password authentication are disabled, and if problems occur with smart card authentication, users cannot log in. In that case, a root or administrator user can turn on user name and password authentication from the vCenter Server command line. The following command enables user name and password authentication.

```
sso-config.sh -set_authn_policy -pwdAuthn true -t tenant_name
```

Prerequisites

- Verify that an enterprise Public Key Infrastructure (PKI) is set up in your environment, and that certificates meet the following requirements:
  - A User Principal Name (UPN) must correspond to an Active Directory account in the Subject Alternative Name (SAN) extension.
  - The certificate must specify Client Authentication in the Application Policy or Extended Key Usage field or the browser does not show the certificate.
- Add an Active Directory identity source to vCenter Single Sign-On.
- Assign the vCenter Server Administrator role to one or more users in the Active Directory identity source. Those users can then perform management tasks because they can authenticate and they have vCenter Server administrator privileges.
- Ensure that you have set up the reverse proxy and restarted the physical or virtual machine.

Procedure

1. Obtain the certificates and copy them to a folder that the `sso-config` utility can see.
   a. Log in to the vCenter Server console, either directly or by using SSH.
   b. Enable the shell, as follows.

      ```
      shell
      chsh -s "/bin/bash" root
      csh -s "bin/appliance/sh" root
      ```

   c. Use WinSCP or a similar utility to copy the certificates to the `/usr/lib/vmware-sso/vmware-sts/conf` directory on the vCenter Server.
   d. Optionally disable the appliance shell, as follows.

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

2. Log in with the vSphere Client to the vCenter Server.

3 Specify the user name and password for administrator@vsphere.local or another member of the vCenter Single Sign-On Administrators group.

   If you specified a different domain during installation, log in as administrator@*mydomain*.

4 Navigate to the Configuration UI.

   a From the **Home** menu, select **Administration**.

   b Under **Single Sign On**, click **Configuration**.

5 Under the **Identity Provider** tab, click **Smart Card Authentication**, then click **Edit**.

6 Select or deselect authentication methods, and click **Save**.

   You can choose smart card authentication by itself, or both smart card authentication and password and Windows session authentication.

   You cannot enable or disable RSA SecurID authentication from this Web interface. However, if RSA SecurID has been enabled from the command line, the status appears in the Web interface.

   The **Trusted CA certificates** appears.

7 Under the **Trusted CA certificates** tab, click **Add**, and click **Browse**.

8 Select all certificates from trusted CAs, and click **Add**.

What to do next

Your environment might require enhanced OCSP configuration.

- If your OCSP response is issued by a different CA than the signing CA of the smart card, provide the OCSP signing CA certificate.
- You can configure one or more local OCSP responders for each vCenter Server site in a multi-site deployment. You can configure these alternative OCSP responders using the CLI. See Use the Command Line to Manage Smart Card Authentication.

Set Revocation Policies for Smart Card Authentication

You can customize certificate revocation checking, and you can specify where vCenter Single Sign-On looks for information about revoked certificates.

You can customize the behavior by using the vSphere Client or by using the `sso-config` script. The settings that you select depend in part on what the CA supports.

- If revocation checking is disabled, vCenter Single Sign-On ignores any CRL or OCSP settings. vCenter Single Sign-On does not perform checks on any certificates.
- If revocation checking is enabled, the setup depends on the PKI setup.

  OCSP only

If the issuing CA supports an OCSP responder, enable **OCSP** and disable **CRL as failover for OCSP**.

CRL only

If the issuing CA does not support OSCP, enable **CRL checking** and disable **OSCP checking**.

Both OSCP and CRL

If the issuing CA supports both an OCSP responder and a CRL, vCenter Single Sign-On checks the OCSP responder first. If the responder returns an unknown status or is not available, vCenter Single Sign-On checks the CRL. For this case, enable both **OCSP checking** and **CRL checking**, and enable **CRL as failover for OCSP**.

- If revocation checking is enabled, advanced users can specify the following additional settings.

  OSCP URL

  By default, vCenter Single Sign-On checks the location of the OCSP responder that is defined in the certificate being validated. If the Authority Information Access extension is absent from the certificate or if you want to override it, you can explicitly specify a location.

  Use CRL from certificate

  By default, vCenter Single Sign-On checks the location of the CRL that is defined in the certificate being validated. Disable this option if the CRL Distribution Point extension is absent from the certificate or if you want to override the default.

  CRL location

  Use this property if you disable **Use CRL from certificate** and you want to specify a location (file or HTTP URL) where the CRL is located.

You can further limit which certificates vCenter Single Sign-On accepts by adding a certificate policy.

Prerequisites

- Verify that an enterprise Public Key Infrastructure (PKI) is set up in your environment, and that certificates meet the following requirements:
  - A User Principal Name (UPN) must correspond to an Active Directory account in the Subject Alternative Name (SAN) extension.
  - The certificate must specify Client Authentication in the Application Policy or Extended Key Usage field or the browser does not show the certificate.
- Verify that the vCenter Server certificate is trusted by the end user's workstation. Otherwise, the browser does not attempt authentication.
- Add an Active Directory identity source to vCenter Single Sign-On.

- Assign the vCenter Server Administrator role to one or more users in the Active Directory identity source. Those users can then perform management tasks because they can authenticate and they have vCenter Server administrator privileges.

Procedure

1. Log in with the vSphere Client to the vCenter Server.
2. Specify the user name and password for administrator@vsphere.local or another member of the vCenter Single Sign-On Administrators group.

   If you specified a different domain during installation, log in as administrator@*mydomain*.
3. Navigate to the Configuration UI.
   a. From the **Home** menu, select **Administration**.
   b. Under **Single Sign On**, click **Configuration**.
4. Under the **Identity Provider** tab, click **Smart Card Authentication**.
5. Click **Certificate revocation** and click **Edit** to enable or disable revocation checking.
6. If certificate policies are in effect in your environment, you can add a policy in the **Certificate policies** pane.

Set Up RSA SecurID Authentication

You can set up your environment to require that users log in with an RSA SecurID token. SecurID setup is supported only from the command line.

See the two vSphere Blog posts about RSA SecurID setup for details.

Note RSA Authentication Manager requires that the user ID is a unique identifier that uses 1 to 255 ASCII characters. The characters ampersand (&), percent (%), greater than (>), less than (<), and single quote (`) are not allowed.

Prerequisites

- Verify that your environment has a correctly configured RSA Authentication Manager and that users have RSA tokens. RSA Authentication Manager version 8.0 or later is required.
- Verify that the identity source that RSA Manager uses has been added to vCenter Single Sign-On. See Add or Edit a vCenter Single Sign-On Identity Source.
- Verify that the RSA Authentication Manager system can resolve the vCenter Server host name, and that the vCenter Server system can resolve the RSA Authentication Manager host name.
- Export the `sdconf.rec` file from the RSA Manager by selecting **Access > Authentication Agents > Generate configuration file**. To find `sdconf.rec` file, decompress the resulting `AM_Config.zip` file.
- Copy the `sdconf.rec` file to the vCenter Server node.

Procedure

1 Change to the directory where the `sso-config` script is located.

```
/opt/vmware/bin
```

2 To enable RSA SecurID authentication, run the following command.

```
sso-config.sh -t tenantName -set_authn_policy -securIDAuthn true
```

tenantName is the name of the vCenter Single Sign-On domain, vsphere.local by default.

3 (Optional) To disable other authentication methods, run the following command.

```
sso-config.sh -set_authn_policy -pwdAuthn false -winAuthn false -certAuthn false -t
vsphere.local
```

4 To configure the environment so that the tenant at the current site uses the RSA site, run the following command.

```
sso-config.sh -set_rsa_site [-t tenantName] [-siteID Location] [-agentName Name] [-
sdConfFile Path]
```

For example:

```
sso-config.sh -set_rsa_site -agentName SSO_RSA_AUTHSDK_AGENT -sdConfFile /tmp/sdconf.rec
```

You can specify the following options.

Option	Description
siteID	Optional Platform Services Controller site ID. Platform Services Controller supports one RSA Authentication Manager instance or cluster per site. If you do not explicitly specify this option, the RSA configuration is for the current Platform Services Controller site. Use this option only if you are adding a different site.
agentName	Defined in RSA Authentication Manager.
sdConfFile	Copy of the `sdconf.rec` file that was downloaded from RSA Manager and includes configuration information for the RSA Manager, such as the IP address.

5 (Optional) To change the tenant configuration to nondefault values, run the following command.

```
sso-config.sh -set_rsa_config [-t tenantName] [-logLevel Level] [-logFileSize Size]
[-maxLogFileCount Count] [-connTimeOut Seconds] [-readTimeOut Seconds] [-encAlgList
Alg1,Alg2,...]
```

The default is usually appropriate, for example:

```
sso-config.sh -set_rsa_config -t vsphere.local -logLevel DEBUG
```

6 (Optional) If your identity source is not using the User Principal Name as the user ID, set up the identity source userID attribute. (Supported with Active Directory over LDAP identity sources only.)

The userID attribute determines which LDAP attribute is used as the RSA userID.

```
sso-config.sh -set_rsa_userid_attr_map [-t tenantName] [-idsName Name] [-ldapAttr
AttrName] [-siteID Location]
```

For example:

```
sso-config.sh -set_rsa_userid_attr_map -t vsphere.local -idsName ssolabs.com -ldapAttr
userPrincipalName
```

7 To display the current settings, run the following command.

```
sso-config.sh -t tenantName -get_rsa_config
```

Results

If user name and password authentication is disabled and RSA authentication is enabled, users must log in with their user name and RSA token. User name and password login is no longer possible.

Note Use the user name format ***userID@domainName*** or ***userID@domain_upn_suffix***.

Managing the Login Message to the vSphere Client Login Page

You can create a message that is displayed on the vSphere Client login page.

You can set a message, disclaimer, or terms and conditions. Also, you can configure the message to require acknowledgment of the message before login.

Manage the Login Message to the vSphere Client Login Page

You can add a login message to the vSphere Client login page. You can also configure a custom login message and provide a check box for user consent.

Procedure

1 Log in with the vSphere Client to the vCenter Server.

2 Specify the user name and password for administrator@vsphere.local or another member of the vCenter Single Sign-On Administrators group.

If you specified a different domain during installation, log in as administrator@*mydomain*.

3 Navigate to the Configuration UI.

   a From the **Home** menu, select **Administration**.

   b Under **Single Sign On**, click **Configuration**.

4 Click the **Login Message** tab.

5 Click **Edit** and configure the login message.

Option	Description
Show login message	Toggle on **Show login message** to enable the login message. You cannot make changes to the login message unless you toggle on this switch.
Login message	Title of the message. By default, when **Consent checkbox** is toggled on, the login message text is `I agree to Terms and Conditions`. You must replace `Terms and Conditions` with your own text. If the **Consent checkbox** is toggled off, then `Login message` appears, over which you enter your message.
Consent checkbox	Toggle on **Consent checkbox** to require that the user clicks a check box before logging in. You can also display a message without a check box.
Details of login message	Message that the user sees when clicking the login message, for example, the text of the terms and conditions. You must enter some details in this text box.

6 Click **Save**.

vCenter Single Sign-On Security Best Practices

Follow vCenter Single Sign-On security best practices to protect your vSphere environment.

The vSphere authentication infrastructure enhances security in your vSphere environment. To make sure that infrastructure is not compromised, follow vCenter Single Sign-On best practices.

Check password expiration

The default vCenter Single Sign-On password policy has a password lifetime of 90 days. After 90 days, the password expires and you can no longer log in. Check the expiration and refresh passwords in a timely fashion.

Configure NTP

Ensure that all systems use the same relative time source (including the relevant localization offset), and that the relative time source can be correlated to an agreed-upon time standard (such as Coordinated Universal Time—UTC). Synchronized systems are essential for vCenter Single Sign-On certificate validity, and for the validity of other vSphere certificates.

NTP also makes it easier to track an intruder in log files. Incorrect time settings can make it difficult to inspect and correlate log files to detect attacks, and can make auditing inaccurate.

Troubleshooting Authentication 5

The following topics provide a starting point for troubleshooting vCenter Server authentication problems. Search this documentation center and the VMware Knowledge Base system for additional pointers.

This chapter includes the following topics:

Determining the Cause of a Lookup Service Error

vCenter Single Sign-On installation displays an error referring to the vCenter Server or the vSphere Client.

Problem

vCenter Server and Web Client installers show the error `Could not contact Lookup Service. Please check VM_ssoreg.log....`

Cause

This problem has several causes, including unsynchronized clocks on the host machines, firewall blocking, and services that must be started.

Solution

1. Verify that the clocks on the host machines running vCenter Single Sign-On, vCenter Server, and the Web Client are synchronized.
2. View the specific log file found in the error message.

   In the message, system temporary folder refers to `%TEMP%`.

3 Within the log file, search for the following messages.

The log file contains output from all installation attempts. Locate the last message that shows `Initializing registration provider...`

Message	Cause and solution
`java.net.ConnectException: Connection timed out: connect`	The IP address is incorrect, a firewall is blocking access to vCenter Single Sign-On, or vCenter Single Sign-On is overloaded. Ensure that a firewall is not blocking the vCenter Single Sign-On port (by default 7444). Ensure also that the machine on which vCenter Single Sign-On is installed has adequate free CPU, I/O, and RAM capacity.
`java.net.ConnectException: Connection refused: connect`	The IP address or FQDN is incorrect and the vCenter Single Sign-On service has not started or has started within the past minute. Verify that vCenter Single Sign-On is working by checking the status of vCenter Single Sign-On vmware-sso daemon. Restart the service. If restarting does not correct the problem, see the recovery section of the *vSphere Troubleshooting Guide*.
`Unexpected status code: 404. SSO Server failed during initialization`	Restart vCenter Single Sign-On. If restarting does not correct the problem, see the Recovery section of the *vSphere Troubleshooting Guide*.
The error shown in the UI begins with `Could not connect to vCenter Single Sign-On`	You also see the return code `SslHandshakeFailed`. This error indicates that the provided IP address or FQDN that resolves to vCenter Single Sign-On host was not the address used when you installed vCenter Single Sign-On. In the `VM_ssoreg.log`, find the line that contains the following message. `host name in certificate did not match: <install-configured FQDN or IP> != <A> or <B> or <C>` where A was the FQDN you entered during the vCenter Single Sign-On installation, and B and C are system-generated allowable alternatives. Correct the configuration to use the FQDN on the right of the `!=` sign in the log file. In most cases, use the FQDN that you specified during vCenter Single Sign-On installation. If none of the alternatives are possible in your network configuration, recover your vCenter Single Sign-On SSL configuration.

Unable to Log In Using Active Directory Domain Authentication

You log in to a vCenter Server component from the vSphere Client. You use your Active Directory user name and password. Authentication fails.

Problem

You add an Active Directory identity source to vCenter Single Sign-On, but users cannot log in to vCenter Server.

Cause

Users use their user name and password to log in to the default domain. For all other domains, users must include the domain name (user@domain or DOMAIN\user).

Solution

For all vCenter Single Sign-On deployments, you can change the default identity source. After that change, users can log in to the default identity source with user name and password only.

To configure your Integrated Windows Authentication identity source with a child domain within your Active Directory forest, see the VMware knowledge base article at http://kb.vmware.com/kb/2070433. By default, Integrated Windows Authentication uses the root domain of your Active Directory forest.

If changing the default identity source does not resolve the issue, perform the following additional troubleshooting steps.

1 Synchronize the clocks between the vCenter Server and the Active Directory domain controllers.

2 Verify that each domain controller has a pointer record (PTR) in the Active Directory domain DNS service.

   Verify that the PTR record information for the domain controller matches the DNS name of the controller. When using the vCenter Server, run the following commands to perform the task:

   a To list the domain controllers, run the following command:

   ```
   # dig SRV _ldap._tcp.my-ad.com
   ```

   The relevant addresses are in the answer section, as in the following example:

   ```
   ;; ANSWER SECTION:
   _ldap._tcp.my-ad.com. (...) my-controller.my-ad.com
   ...
   ```

   b For each domain controller, verify forward and reverse resolution by running the following command:

   ```
   # dig my-controller.my-ad.com
   ```

   The relevant addresses are in the answer section, as in the following example:

   ```
   ;; ANSWER SECTION:
   my-controller.my-ad.com (...) IN A controller IP address
   ...
   ```

   ```
   # dig -x <controller IP address>
   ```

The relevant addresses are in the answer section, as in the following example:

```
;; ANSWER SECTION:
IP-in-reverse.in-addr.arpa. (...) IN PTR my-controller.my-ad.com
...
```

3 If that does not resolve the problem, remove the vCenter Server from the Active Directory domain and then rejoin the domain. See the *vCenter Server Configuration* documentation.

4 Close all browser sessions connected to the vCenter Server and restart all services.

```
/bin/service-control --restart --all
```

vCenter Server Login Fails Because the User Account Is Locked

When you log in to vCenter Server from the vSphere Client login page, an error indicates that the account is locked.

Problem

After several failed attempts, you cannot log in to the vSphere Client using vCenter Single Sign-On. You see the message that your account is locked.

Cause

You exceeded the maximum number of failed login attempts.

Solution

- If you attempted log in as a user from the system domain (vsphere.local by default), ask your vCenter Single Sign-On administrator to unlock your account. If the lock is set to expire in the lockout policy, you can wait until your account is unlocked. vCenter Single Sign-On administrators can use CLI commands to unlock your account.
- If you log in as a user from an Active Directory or LDAP domain, ask your Active Directory or LDAP administrator to unlock your account.

VMware Directory Service Replication Can Take a Long Time

If your environment includes multiple vCenter Server instances connected through enhanced linked mode, and if one of the vCenter Server instances becomes unavailable, your environment continues to function. When the vCenter Server becomes available again, user data and other information are usually replicated within 30 seconds with partners connected through enhanced linked mode. In certain circumstances, however, replication might take a long time.

Problem

In certain situations, for example, when your environment includes multiple vCenter Server instances in different locations, and you make significant changes while one vCenter Server is unavailable, you do not see replication across VMware Directory Service instances right away. For example, you do not see a new user that was added to the available vCenter Server instance in the other instance until replication is complete. Replication might take a long time, depending on your enhanced linked mode topology.

Cause

During normal operation, changes to a VMware Directory Service (vmdir) instance in one vCenter Server instance (node) show up in its direct replication partner within about 30 seconds. Depending on the replication topology, changes in one node might have to propagate through intermediate nodes before they arrive at each vmdir instance in each node. Information that is replicated includes user information, certificate information, license information for virtual machines that are created, cloned, or migrated with VMware vMotion, and more.

When the replication link is broken, for example, because of a network outage or because a node becomes unavailable, changes in the federation do not converge. After the unavailable node is restored, each node tries to catch up with all changes. Eventually, all vmdir instances converge to a consistent state but it might take a while to reach that consistent state if many changes occurred while one node was unavailable.

Solution

Your environment functions normally while replication happens. Do not attempt to solve the problem unless it persists for over an hour.

Export a vCenter Server Support Bundle

You can export a support bundle that contains the log files for the vCenter Server services from the vSphere Client, or by using an API. After the export, you can explore the logs locally or send the bundle to VMware Support.

For more information about the API, see *vCenter Server Management Programming Guide*.

Prerequisites

Verify that the vCenter Server is successfully deployed and running.

Procedure

1. From a Web browser, connect to the vCenter Server configuration management interface at https://*vcenter_server_ip*:5480.
2. Log in as the root user for the vCenter Server.
3. From the **Actions** menu, select **Create Support Bundle**.

4 Unless browser settings prevent an immediate download, the support bundle is saved to your local machine.

Authentication Services Logs Reference

The vCenter Server authentication services use syslog for logging. You can examine the log files to determine the reasons for failures.

Table 5-1. Service Logs

Service	Description
VMware Directory Service	By default, vmdir logging goes to `/var/log/messages` or `/var/log/vmware/vmdird/`. For issues at deployment time, `/var/log/vmware/vmdir/vmafdvmdirclient.log` might also contain useful troubleshooting data.
VMware Single Sign-On	vCenter Single Sign-On logging goes to `/var/log/vmware/sso/`.
VMWare Certificate Authority (VMCA)	VMCA service log is located in `/var/log/vmware/vmcad/vmcad-syslog.log`.
VMware Endpoint Certificate Store (VECS)	VECS service log is located in `/var/log/vmware/vmafdd/vmafdd-syslog.log`.
VMware Lookup Service	Lookup service log is located in `/var/log/vmware/sso/lookupServer.log`.