Platform Services Controller Administration

Update 1
Modified 03 NOV 2017
VMware vSphere 6.5
VMware ESXi 6.5
vCenter Server 6.5

vmware®

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

https://docs.vmware.com/

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

docfeedback@vmware.com

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

Contents

About *Platform Services Controller Administration*

The *Platform Services Controller Administration* documentation explains how the VMware® Platform Services Controller™ fits into your vSphere environment and helps you perform common tasks such as certificate management and vCenter Single Sign-On configuration.

Platform Services Controller Administration explains how you can set up authentication with vCenter Single Sign-On and how to manage certificates for vCenter Server and related services.

Table 1. *Platform Services Controller Administration* Highlights

Topics	Content Highlights
Getting Started with Platform Services Controller	■ vCenter Server and Platform Services Controller deployment models. NOTE: This information changes with each release of the product. ■ Platform Services Controller services on Linux and Windows. ■ Managing Platform Services Controller services. ■ Managing the Platform Services Controller appliance using VAMI.
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.
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.

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 a *Hardening Guide* for each release of vSphere, accessible at http://www.vmware.com/security/hardening-guides.html. The *Hardening Guide* is a spreadsheet with entries for different potential security issues. It includes items for three different risk profiles.

Intended Audience

This information is intended for administrators who want to configure Platform Services Controller and associated services. The information is written for experienced Windows or Linux system administrators who are familiar with virtual machine technology and data center operations.

vSphere Web Client and vSphere Client

Task instructions in this guide are based on the vSphere Web Client. You can also perform most of the tasks in this guide by using the new vSphere Client, also called the HTML 5 client. The new vSphere Client user interface terminology, topology, and workflow are closely aligned with the same aspects and elements of the vSphere Web Client user interface. You can apply the vSphere Web Client instructions to the new vSphere Client unless otherwise instructed.

Note Not all functionality in the vSphere Web Client has been implemented for the vSphere Client in the vSphere 6.5 release. For an up-to-date list of unsupported functionality, see *Functionality Updates for the vSphere Client Guide* at http://www.vmware.com/info?id=1413.

Updated Information

This *Platform Services Controller Administration* documentation is updated with each release of the product or when necessary.

This table provides the update history of *Platform Services Controller Administration*.

Revision	Description
03 NOV 2017	■ Clarification in Understanding Stopping and Starting of Services ■ Include steps for stopping and starting reverse proxy on Windows in Configure the Reverse Proxy to Request Client Certificates.
EN-002010-04	Initial release.

Getting Started with Platform Services Controller

1

The Platform Services Controller provides common infrastructure services to the vSphere environment. Services include licensing, certificate management, and authentication with vCenter Single Sign-On.

This section includes the following topics:

vCenter Server and Platform Services Controller Deployment Types

You can deploy the vCenter Server Appliance or install vCenter Server for Windows with an embedded or external Platform Services Controller. You can also deploy a Platform Services Controller as an appliance or install it on Windows. If necessary, you can use a mixed operating systems environment.

Before you deploy the vCenter Server Appliance or install vCenter Server for Windows, you must determine the deployment model that is suitable for your environment. For each deployment or installation, you must select one of the three deployment types.

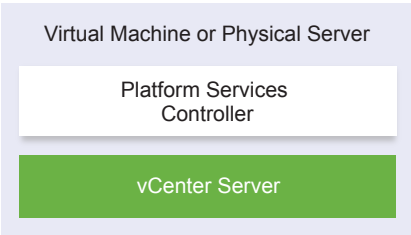
Table 1-1. vCenter Server and Platform Services Controller Deployment Types

Deployment Type	Description
vCenter Server with an embedded Platform Services Controller	All services that are bundled with the Platform Services Controller are deployed together with the vCenter Server services on the same virtual machine or physical server.
Platform Services Controller	Only the services that are bundled with the Platform Services Controller are deployed on the virtual machine or physical server.
vCenter Server with an external Platform Services Controller (Requires external Platform Services Controller)	Only the vCenter Server services are deployed on the virtual machine or physical server. You must register such a vCenter Server instance with a Platform Services Controller instance that you previously deployed or installed.

vCenter Server with an Embedded Platform Services Controller

Using an embedded Platform Services Controller results in a standalone deployment that has its own vCenter Single Sign-On domain with a single site. vCenter Server with an embedded Platform Services Controller is suitable for small environments. You cannot join other vCenter Server or Platform Services Controller instances to this vCenter Single Sign-On domain.

Figure 1-1. vCenter Server with an Embedded Platform Services Controller



Installing vCenter Server with an embedded Platform Services Controller has the following advantages:

- The connection between vCenter Server and the Platform Services Controller is not over the network, and vCenter Server is not prone to outages caused by connectivity and name resolution issues between vCenter Server and the Platform Services Controller.
- If you install vCenter Server on Windows virtual machines or physical servers, you need fewer Windows licenses.
- You manage fewer virtual machines or physical servers.

Installing vCenter Server with an embedded Platform Services Controller has the following disadvantages:

- There is a Platform Services Controller for each product which might be more than required and which consumes more resources.
- The model is suitable only for small-scale environments.

You can configure the vCenter Server Appliance with an embedded Platform Services Controller in vCenter High Availability configuration. For information, see *vSphere Availability*.

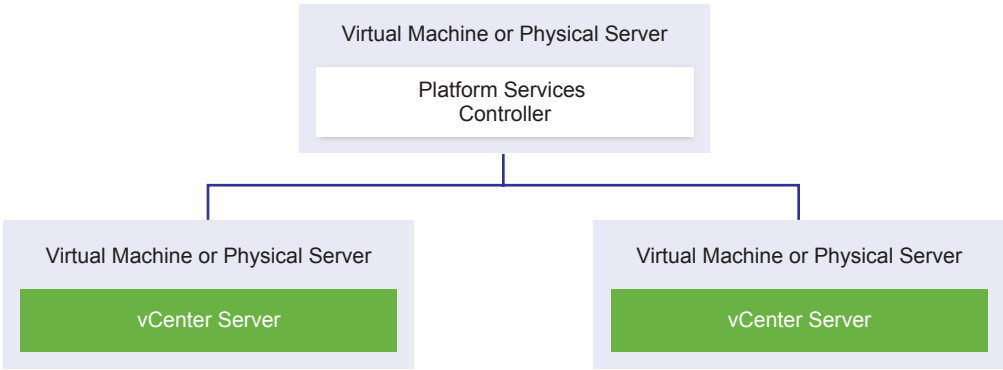
Note After you deploy or install vCenter Server with an embedded Platform Services Controller, you can reconfigure the deployment type and switch to vCenter Server with an external Platform Services Controller.

Platform Services Controller and vCenter Server with an External Platform Services Controller

When you deploy or install a Platform Services Controller instance, you can create a vCenter Single Sign-On domain or join an existing vCenter Single Sign-On domain. Joined Platform Services Controller instances replicate their infrastructure data, such as authentication and licensing information, and can span multiple vCenter Single Sign-On sites. For information, see Understanding vSphere Domains, Domain Names, and Sites.

You can register multiple vCenter Server instances with one common external Platform Services Controller instance. The vCenter Server instances assume the vCenter Single Sign-On site of the Platform Services Controller instance with which they are registered. All vCenter Server instances that are registered with one common or different joined Platform Services Controller instances are connected in Enhanced Linked Mode.

Figure 1-2. Example of Two vCenter Server Instances with a Common External Platform Services Controller



Installing vCenter Server with an external Platform Services Controller has the following advantages:

- Fewer resources consumed by the shared services in the Platform Services Controller instances.
- The model is suitable for large-scale environments.

Installing vCenter Server with an external Platform Services Controller has the following disadvantages:

- The connection between vCenter Server and Platform Services Controller might have connectivity and name resolution issues.
- If you install vCenter Server on Windows virtual machines or physical servers, you need more Microsoft Windows licenses.
- You must manage more virtual machines or physical servers.

For information about the Platform Services Controller and vCenter Server maximums, see the *Configuration Maximums* documentation.

For information about configuring the vCenter Server Appliance with an external Platform Services Controller in vCenter High Availability configuration, see *vSphere Availability*.

Mixed Operating Systems Environment

A vCenter Server instance installed on Windows can be registered with either a Platform Services Controller installed on Windows or a Platform Services Controller appliance. A vCenter Server Appliance can be registered with either a Platform Services Controller installed on Windows or a Platform Services Controller appliance. Both vCenter Server and the vCenter Server Appliance can be registered with the same Platform Services Controller.

Figure 1-3. Example of a Mixed Operating Systems Environment with an External Platform Services Controller on Windows

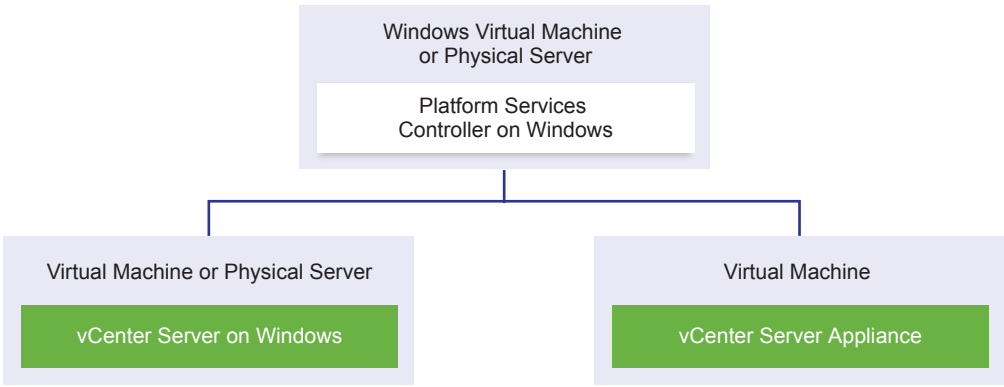
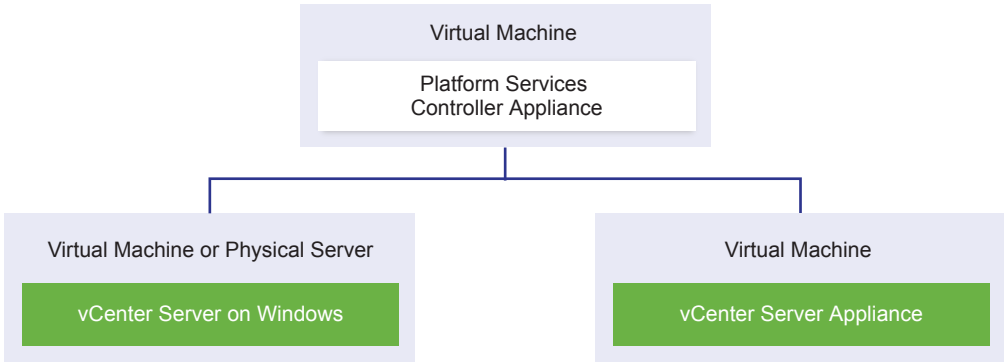


Figure 1-4. Example of a Mixed Operating Systems Environment with an External Platform Services Controller Appliance



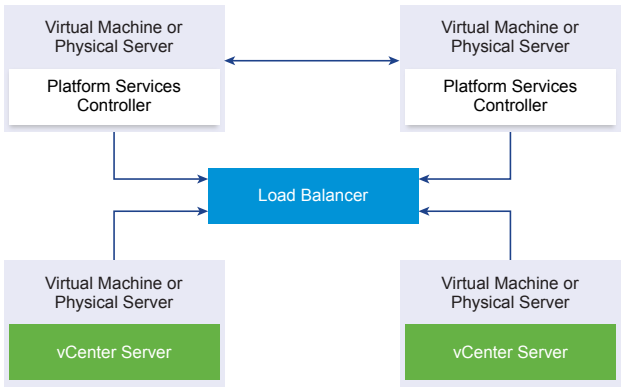
Note To ensure easy manageability and maintenance, use only appliances or only Windows installations of vCenter Server and Platform Services Controller.

Deployment Topologies with External Platform Services Controller Instances and High Availability

To ensure Platform Services Controller high availability in external deployments, you must install or deploy at least two joined Platform Services Controller instances in your vCenter Single Sign-On domain. When you use a third-party load balancer, you can ensure an automatic failover without downtime.

Platform Services Controller with a Load Balancer

Figure 1-5. Example of a Load Balanced Pair of Platform Services Controller Instances



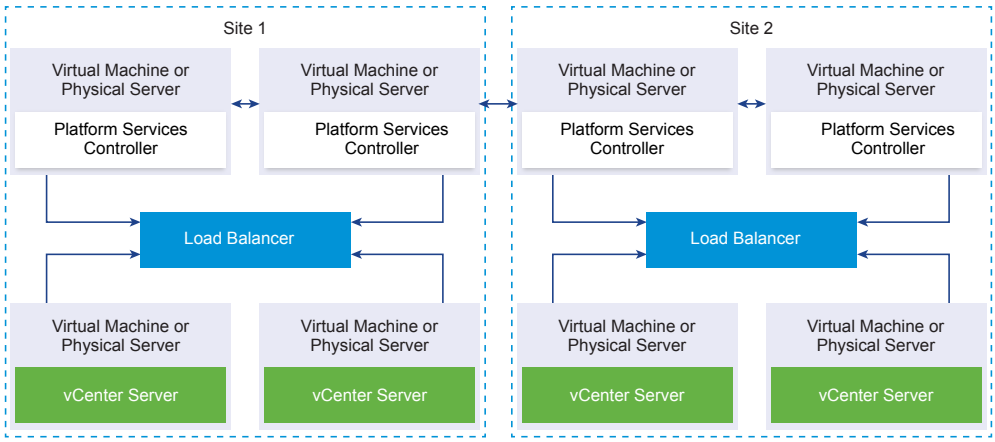
You can use a third-party load balancer per site to configure Platform Services Controller high availability with automatic failover for this site. For information about the maximum number of Platform Services Controller instances behind a load balancer, see the *Configuration Maximums* documentation.

Important To configure Platform Services Controller high availability behind a load balancer, the Platform Services Controller instances must be of the same operating system type. Mixed operating systems Platform Services Controller instances behind a load balancer are unsupported.

The vCenter Server instances are connected to the load balancer. When a Platform Services Controller instance stops responding, the load balancer automatically distributes the load among the other functional Platform Services Controller instances without downtime.

Platform Services Controller with Load Balancers Across vCenter Single Sign-On Sites

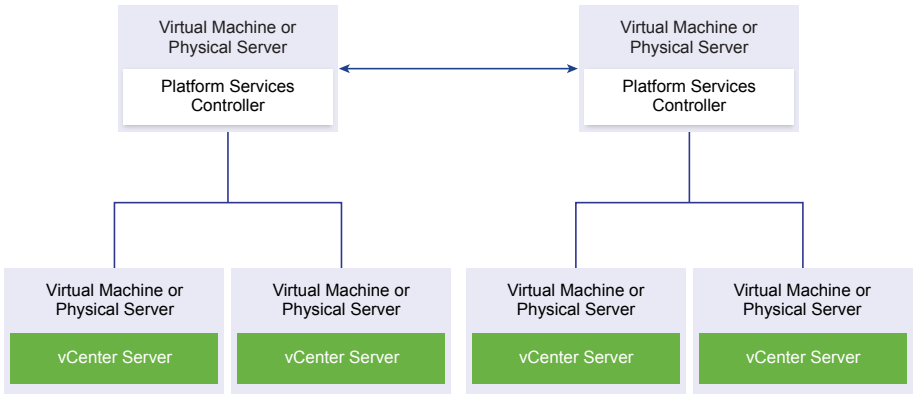
Figure 1-6. Example of Two Load Balanced Pairs of Platform Services Controller Instances Across Two Sites



Your vCenter Single Sign-On domain might span multiple sites. To ensure Platform Services Controller high availability with automatic failover throughout the domain, you must configure a separate load balancer in each site.

Platform Services Controller with No Load Balancer

Figure 1-7. Example of Two Joined Platform Services Controller Instances with No a Load Balancer

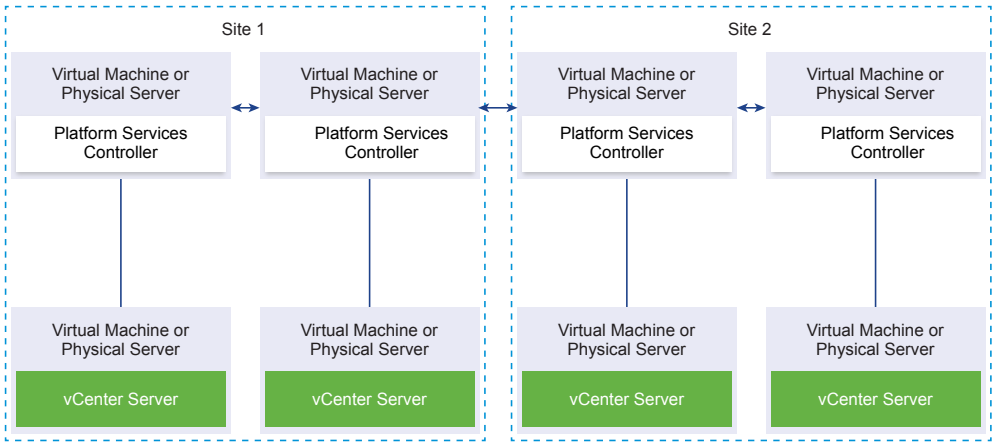


When you join two or more Platform Services Controller instances in the same site with no load balancer, you configure Platform Services Controller high availability with a manual failover for this site.

Note If your vCenter Single Sign-On domain includes three or more Platform Services Controller instances, you can manually create a ring topology. A ring topology ensures Platform Services Controller reliability when one of the instances fails. To create a ring topology, run the `/usr/lib/vmware-vmdir/bin/vdcrepadmin -f createagreement` command against the first and last Platform Services Controller instance that you have deployed.

Platform Services Controller with No Load Balancer Across vCenter Single Sign-On Sites

Figure 1-8. Example of Two Joined Pairs of Platform Services Controller Instances Across Two Sites with No Load Balancer



Important Repointing vCenter Server between sites and domains is unsupported. If no functional Platform Services Controller instance is available in the site, you must deploy or install a new Platform Services Controller instance in this site. This new Platform Services Controller instance becomes the replication partner of the existing Platform Services Controller instance.

Understanding vSphere Domains, Domain Names, and Sites

Each Platform Services Controller is associated with a vCenter Single Sign-On domain. The domain name defaults to vsphere.local, but you can change it during installation of the first Platform Services Controller. The domain determines the local authentication space. You can split a domain into multiple sites, and assign each Platform Services Controller and vCenter Server instance to a site. Sites are logical constructs, but usually correspond to geographic location.

Platform Services Controller Domain

When you install a Platform Services Controller, you are prompted to create a vCenter Single Sign-On domain or join an existing domain.

The domain name is used by the VMware Directory Service (vmdir) for all Lightweight Directory Access Protocol (LDAP) internal structuring.

With vSphere 6.0 and later, you can give your vSphere domain a unique name. To prevent authentication conflicts, use a name that is not used by OpenLDAP, Microsoft Active Directory, and other directory services.

Note You cannot change the domain to which a Platform Services Controller or vCenter Server instance belongs.

If you are upgrading from vSphere 5.5, your vSphere domain name remains the default (vsphere.local). For all versions of vSphere, you cannot change the name of a domain.

After you specify the name of your domain, you can add users and groups. It usually makes more sense to add an Active Directory or LDAP identity source and allow the users and groups in that identity source to authenticate. You can also add vCenter Server or Platform Services Controller instances, or other VMware products, such as vRealize Operations, to the domain.

Platform Services Controller Sites

You can organize Platform Services Controller domains into logical sites. A site in the VMware Directory Service is a logical container for grouping Platform Services Controller instances within a vCenter Single Sign-On domain.

Starting with vSphere 6.5, sites become important. During Platform Services Controller failover, the vCenter Server instances are affinitized to a different Platform Services Controller in the same site. To prevent your vCenter Server instances from being affinitized to a Platform Services Controller in a distant geographic location, you can use multiple sites.

You are prompted for the site name when you install or upgrade a Platform Services Controller. See the *vSphere Installation and Setup* documentation.

Platform Services Controller Capabilities

Platform Services Controller supports services such as identity management, certificate management, and license management in vSphere.

Key Capabilities

Platform Services Controller includes several services, discussed in Platform Services Controller Services, and has the following key capabilities.

- Authentication through vCenter Single Sign-On
- Provisioning of vCenter Server components and ESXi hosts with VMware Certificate Manager (VMCA) certificates by default
- Use of custom certificates, which are stored in the VMware Endpoint Certificate Store (VECS)
- Starting with vSphere 6.5, support for Platform Services Controller Services high availability

Deployment Models

You can install Platform Services Controller on a Windows system or deploy the Platform Services Controller appliance.

The deployment model depends on the version of Platform Services Controller that you are using. See vCenter Server and Platform Services Controller Deployment Types.

If you install more than one external Platform Services Controller in the same site in vSphere 6.5 and later, high availability for the Platform Services Controller instances is turned on automatically.

Managing Platform Services Controller Services

You manage Platform Services Controller services from the Platform Services Controller Web interface, from the vSphere Web Client, or by using one of the available scripts and CLIs.

Different Platform Services Controller services support different interfaces.

Table 1-2. Interfaces for Managing Platform Services Controller Services

Interface	Description
Platform Services Controller Web interface	Web interface for managing all services including vCenter Single Sign-On and Common Access Card. Connect to https://*psc_hostname_or_IP*/psc.
vSphere Web Client	Web interface for managing some of the services. Some services, such as smart card authentication, are configurable only from the Platform Services Controller Web interface.
Certificate Management utility	Command-line tool that supports CSR generation and certificate replacement. See Managing Certificates with the vSphere Certificate Manager Utility.
CLIs for managing Platform Services Controller services	Set of commands for managing certificates, the VMware Endpoint Certificate Store (VECS), and VMware Directory Service (vmdir). See Chapter 4 Managing Services and Certificates With CLI Commands.

Platform Services Controller Services

With Platform Services Controller, all VMware products within the same environment can share the authentication domain and other services. Services include certificate management, authentication, and licensing.

Platform Services Controller includes the following core infrastructure services.

Table 1-3. Platform Services Controller Services

Service	Description
`applmgmt` (VMware Appliance Management Service)	Handles appliance configuration and provides public API endpoints for appliance lifecycle management. Included on the Platform Services Controller appliance.
`vmware-cis-license` (VMware License Service)	Each Platform Services Controller includes VMware License Service, which delivers centralized license management and reporting functionality to VMware products in your environment. The license service inventory replicates across all Platform Services Controller in the domain at 30-second intervals.
`vmware-cm` (VMware Component Manager)	Component manager provides service registration and lookup functionalities.
`vmware-psc-client` (VMware Platform Services Controller Client)	Backend to the Platform Services Controller Web interface.

`vmware-sts-idmd`
(VMware Identity Management Service)
`vmware-stsd`
(VMware Security Token Service)
	Services behind the vCenter Single Sign-On feature, which provide secure authentication services to VMware software components and users.
	By using vCenter Single Sign-On, the VMware components communicate using a secure SAML token exchange mechanism. vCenter Single Sign-On constructs an internal security domain (vsphere.local by default) where the VMware software components are registered during installation or upgrade.

`vmware-rhttpproxy` (VMware HTTP Reverse Proxy)	The reverse proxy runs on each Platform Services Controller node and each vCenter Server system. It is a single entry point into the node and enables services that run on the node to communicate securely.
`vmware-sca` (VMware Service Control Agent)	Manages service configurations. You can use the `service-control` CLI to manage individual service configurations.
`vmware-statsmonitor` (VMware Appliance Monitoring Service)	Monitor the vCenter Server Appliance guest operating system resource consumption.
`vmware-vapi-endpoint` (VMware vAPI Endpoint)	The vSphere Automation API endpoint provides a single point of access to vAPI services. You can change the properties of the vAPI Endpoint service from the vSphere Web Client. See the *vSphere Automation SDKs Programming Guide* for details on vAPI endpoints.
`vmafdd` VMware Authentication Framework	Service that provides a client-side framework for vmdir authentication and serves the VMware Endpoint Certificate Store (VECS).

Table 1-3. Platform Services Controller Services (Continued)

Service	Description
`vmcad` VMware Certificate Service	Provisions each VMware software component that has the vmafd client libraries and each ESXi host with a signed certificate that has VMCA as the root certificate authority. You can change the default certificates by using the Certificate Manager utility or Platform Services Controller Web interface. VMware Certificate Service uses the VMware Endpoint Certificate Store (VECS) to serve as a local repository for certificates on every Platform Services Controller instance. Although you can decide not to use VMCA and instead can use custom certificates, you must add the certificates to VECS.
`vmdird` VMware Directory Service	Provides a multitenant, multimastered LDAP directory service that stores authentication, certificate, lookup, and license information. Do not update data in `vmdird` by using an LDAP browser. If your domain contains more than one Platform Services Controller instance, an update of vmdir content in one vmdir instance is propagated to all other instances of vmdir.
`vmdnsd` VMware Domain Name Service	Not used in vSphere 6.x. Used by the Platform Services Controller High Availability feature to ensure that authentication and other services remain available if one Platform Services Controller node cannot be reached.

`vmonapi`
VMware Lifecycle Manager API
`vmware-vmon`
VMware Service Lifecycle Manager
	Start and stop vCenter Server services and monitor service API health. The `vmware-vmon` service is a centralized platform-independent service that manages the lifecycle of Platform Services Controller and vCenter Server. Exposes APIs and CLIs to third-party applications.

`lwsmd` Likewise Service Manager	Likewise facilitates joining the host to an Active Directory domain and subsequent user authentication.

Access the Platform Services Controller Web Interface

You can use the Platform Services Controller Web interface to set up vCenter Single Sign-On, manage certificates, and configure two-factor authentication.

Note This interface includes some configuration options, such as Login Banner configuration and Smart Cart Authentication configuration, that are not available from the vSphere Web Client.

Procedure

1. From your Web browser, connect to https://*psc_ip_or_hostname*/psc.

   In environments that use an embedded Platform Services Controller, use https://*vc_ip_or_hostname*/psc

2. Log in as an administrator user in the local vCenter Single Sign-On domain (vsphere.local by default).

Manage Platform Services Controller Services From the vSphere Web Client

You can manage vCenter Single Sign-On and the Licensing service from the vSphere Web Client.

Use the Platform Services Controller Web interface or CLIs instead of the vSphere Web Client to manage the following services.

- Certificates
- VMware Endpoint Certificate Store (VECS)
- Two-factor authentication such as Common Access Card authentication
- Login banner

Procedure

1. Log in to a vCenter Server associated with the Platform Services Controller as a user with administrator privileges in the local vCenter Single Sign-On domain (vsphere.local by default).
2. Select **Administration** and click the item that you want to manage.

Option	Description
Single Sign-On	Configure vCenter Single Sign-On. ■ Set policies. ■ Manage identity sources. ■ Manage the STS Signing certificate. ■ Manage SAML service providers. ■ Manage users and groups.
Licensing	Configure licensing.

Use Scripts to Manage Platform Services Controller Services

Platform Services Controller includes scripts for generating CSRs, managing certificates and managing services.

For example, you can use the `certool` utility to generate CSRs and to replace certificates, both for scenarios with embedded Platform Services Controller and for scenarios with external Platform Services Controller. See Managing Certificates with the vSphere Certificate Manager Utility.

Use the CLIs for management tasks that the Web interfaces do 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 VMCA.	certool Initialization Commands Reference
`vecs-cli`	Manage the contents of VMware Certificate Store instances. Part of VMAFD.	vecs-cli Command Reference
`dir-cli`	Create and update certificates in VMware Directory Service. Part of VMAFD.	dir-cli Command Reference
`sso-config`	Utility for configuring smart card authentication.	vCenter Server Two-Factor Authentication
`service-control`	Command for starting, stopping, and listing services.	Run this command to stop services before running other CLI commands.

Procedure

1 Log in to the Platform Services Controller shell.

In most cases, 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. In some cases, you are prompted for the password twice to safeguard sensitive information.

Windows

`C:\Program Files\VMware\vCenter Server\vmafdd\vecs-cli.exe`

`C:\Program Files\VMware\vCenter Server\vmafdd\dir-cli.exe`

`C:\Program Files\VMware\vCenter Server\vmcad\certool.exe`

`C:\Program Files\VMware\VCenter server\VMware Identity Services\sso-config`

`VCENTER_INSTALL_PATH``\bin\service-control`

Linux

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

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

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

`/opt/vmware/bin`

On Linux, the `service-control` command does not require that you specify the path.

Managing the Platform Services Controller Appliance

You can manage the Platform Services Controller appliance from the virtual appliance management interface or from the appliance shell.

If you are using an environment with an embedded Platform Services Controller, you manage the one appliance that includes both Platform Services Controller and vCenter Server. See *vCenter Server Appliance Configuration*.

Table 1-5. Interfaces for Managing the Platform Services Controller Appliance

Interface	Description
Platform Services Controller virtual appliance management interface (VAMI)	Use this interface to reconfigure the system settings of a Platform Services Controller deployment.
Platform Services Controller appliance 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 4 Managing Services and Certificates With CLI Commands.

Manage the Appliance with the Platform Services Controller Virtual Appliance Management Interface

In an environment with an external Platform Services Controller, you can use the Platform Services Controller virtual appliance management interface (VAMI) to configure the appliance 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.

In an environment with an embedded Platform Services Controller, you manage the appliances that include both Platform Services Controller and vCenter Server.

Procedure

1. In a Web browser, go to the Platform Services Controller Web interface at https://*platform_services_controller_ip*:5480.
2. If a warning message about an untrusted SSL certificate appears, resolve the issue based on company security policy and the Web browser that you are using.
3. Log in as root.

   The default root password is the virtual appliance root password that you set when deploying the virtual appliance.

You can see the System Information page of the Platform Services Controller Appliance Management Interface.

Manage the Appliance from the Appliance Shell

You can use service management utilities and CLIs from the appliance 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 appliance management interface (VAMI).
   b. In the Navigator, select **Access** and click **Edit**.
   c. Click the **Enable SSH Login** check box and click **OK**.

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

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

Add a Platform Services Controller Appliance to an Active Directory Domain

If you want to add an Active Directory identity source to Platform Services Controller, you must join the Platform Services Controller appliance to an Active Directory domain.

If you are using a Platform Services Controller instance that is installed on Windows, you can use the domain to which that machine belongs.

Procedure

1. Log in to the Platform Services Controller Web interface at http://*psc_ip_or_dns*/psc as an administrator user.
2. Click **Appliance Settings** and click **Manage**.
3. Click **Join**, specify the domain, optional organizational unit, and user name and password, and click **OK**.

vSphere Authentication with vCenter Single Sign-On

2

vCenter Single Sign-On is an authentication broker and security token exchange infrastructure. When a user or a solution user can authenticate to vCenter Single Sign-On, that user receives a SAML token. Going forward, the user can use the SAML token to authenticate to vCenter 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.

Starting with vSphere 6.0, vCenter Single Sign-On is part of the Platform Services Controller. The Platform Services Controller contains the shared services that support vCenter Server and vCenter Server components. These services include vCenter Single Sign-On, VMware Certificate Authority, and License Service. See *vSphere Installation and Setup* for details on the Platform Services Controller.

For the initial handshake, users authenticate with a user name and password, and solution users authenticate with a certificate. For information on replacing solution user certificates, see Chapter 3 vSphere Security Certificates.

The next step is authorizing the users who can authenticate to perform certain tasks. In most cases, you assign vCenter Server privileges, usually 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 section includes the following topics:

Understanding vCenter Single Sign-On

To effectively manage vCenter Single Sign-On, you need to understand the underlying architecture and how it affects installation and upgrades.

vCenter Single Sign-On 6.0 Domains and Sites (http://link.brightcove.com/services/player/bcpid2296383276001?bctid=ref:video_sso_6_domains_sites)

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 instead of requiring users to authenticate separately with each component.

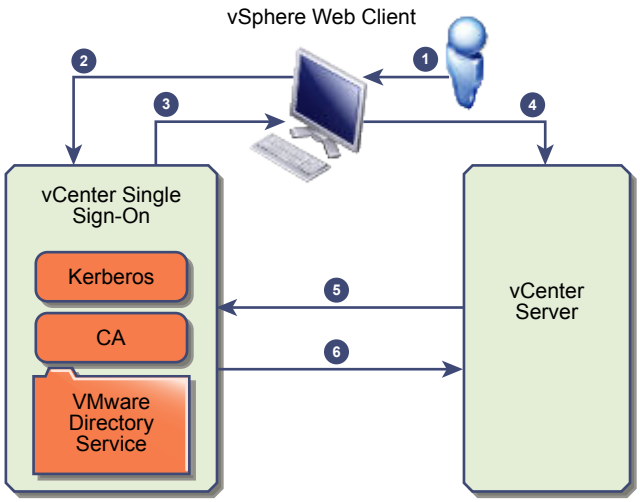
vCenter Single Sign-On uses the following services.

- STS (Security Token Service).
- SSL for secure traffic.
- Authentication of human users through Active Directory or OpenLDAP.
- Authentication of solution users through certificates.

vCenter Single Sign-On Handshake for Human Users

The following illustration shows the handshake for human users.

Figure 2-1. vCenter Single Sign-On Handshake for Human Users



1 A user logs in to the vSphere Web Client with a user name and password to access the vCenter Server system or another vCenter service.

   The user can also log in without a password and check the **Use Windows session authentication** check box.

2 The vSphere Web Client passes the login information to the vCenter Single Sign-On service, which checks the SAML token of the vSphere Web Client. If the vSphere Web 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 Web Client.
4 The vSphere Web 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 ThevCenter Single Sign-On server returns the token to the vCenter Server system, using thevCenter Server Authorization Framework to allow user access.

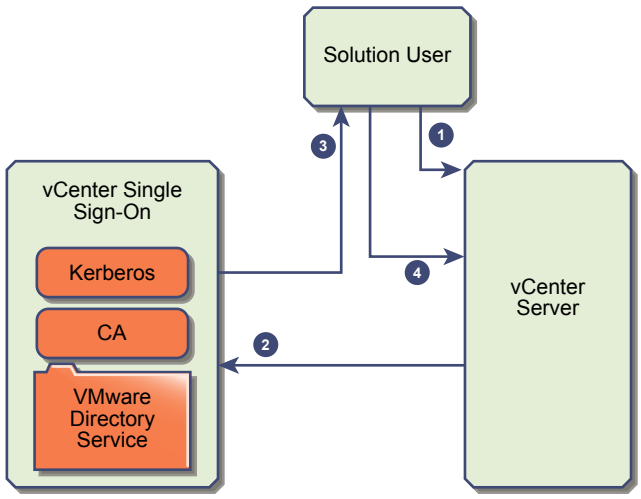
The user can now authenticate, and can view and modify any objects that the user's role has privileges for.

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.

vCenter Single Sign-On Handshake for Solution Users

Solution users are sets of services that are used in the vCenter Server infrastructure, for example, the vCenter Server or vCenter Server extensions. VMware extensions and potentially third-party extensions might also authenticate to vCenter Single Sign-On.

Figure 2-2. vCenter Single Sign-On Handshake for Solution Users



For solution users, the interaction proceeds as follows:

1 The solution user attempts to connect to a vCenter 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.

5 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 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 any time an ESXi host or vCenter Server is joined to Active Directory. It also affects security when vCenter Single Sign-On uses Active Directory as an identity source.

vCenter Single Sign-On Components

vCenter Single Sign-On includes the Security Token Service (STS), an administration server, and vCenter Lookup Service, as well as the VMware Directory Service (vmdir). The VMware Directory Service is also used for certificate management.

During installation, the components are deployed as part an embedded deployment, or as part of the Platform Services Controller.

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 byvCenter Single Sign-On. The SAML tokens allow both human users and 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 Web Client. Initially, only the user administrator@*your_domain_name* has these privileges. In vSphere

	5.5, this user was administrator@vsphere.local. With vSphere 6.0, you can change the vSphere domain when you install vCenter Server or deploy the vCenter Server Appliance with a new Platform Services Controller. Do not name the domain name with your Microsoft Active Directory or OpenLDAP domain name.
VMware Directory Service (vmdir)	The VMware Directory service (vmdir) is associated with the domain you specify during installation and is included in each embedded deployment and on each Platform Services Controller. This service is a multi-tenanted, multi-mastered directory service that makes an LDAP directory available on port 389. The service still uses port 11711 for backward compatibility with vSphere 5.5 and earlier systems. If your environment includes more than one instance of the Platform Services Controller, an update of vmdir content in one vmdir instance is propagated to all other instances of vmdir. Starting with vSphere 6.0, 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.

How vCenter Single Sign-On Affects Installation

Starting with version 5.1, vSphere includes a vCenter Single Sign-On service as part of the vCenter Server management infrastructure. This change affects vCenter Server installation.

Authentication with vCenter Single Sign-On makes vSphere more secure because the vSphere software components communicate with each other by using a secure token exchange mechanism, and all other users also authenticate with vCenter Single Sign-On.

Starting with vSphere 6.0, vCenter Single Sign-On is either included in an embedded deployment, or part of the Platform Services Controller. The Platform Services Controller contains all of the services that are necessary for the communication between vSphere components including vCenter Single Sign-On, VMware Certificate Authority, VMware Lookup Service, and the licensing service.

The order of installation is important.

First installation	If your installation is distributed, you must install the Platform Services Controller before you install vCenter Server or deploy the vCenter Server Appliance. For an embedded deployment the correct installation order happens automatically.
Subsequent installations	For approximately up to four vCenter Server instances, one Platform Services Controller can serve your entire vSphere environment. You can connect the new vCenter Server instances to the same Platform Services Controller. For more than approximately four

vCenter Server instances, you can install an additional Platform Services Controller for better performance. The vCenter Single Sign-On service on each Platform Services Controller synchronizes authentication data with all other instances. The precise number depends on how heavily the vCenter Server instances are being used and on other factors.

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 Web 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 Web Client, not through vCenter Single Sign-On. See the *vSphere Security* documentation.

vCenter Single Sign-On and vCenter Server Users

Using the vSphere Web Client, users authenticate to vCenter Single Sign-On by entering their credentials on the vSphere Web Client 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 (vsphere.local by default).

All users that can authenticate to vCenter Single Sign-On can reset their password, even if the password has expired, as long as they know the 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 Web Client and from the Platform Services Controller web interface.

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 Web Client. Upon authentication, that user can access the vCenter Single Sign-On administration interface from the vSphere Web Client and manage identity sources and default domains, specify password policies, and perform other administrative tasks. See Configuring vCenter Single Sign-On Identity Sources.

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.

ESXi Users

Standalone ESXi hosts are not integrated with vCenter Single Sign-On or with the Platform Services Controller. 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, vCLI, or PowerCLI. vCenter Server is not aware 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 Web Client or the Platform Services Controller Web interface.

When a user logs in to a vCenter Server system from the vSphere Web 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.

Note Starting with vSphere 6.0 Update 2, two-factor authentication is supported. See vCenter Server Two-Factor Authentication.

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 Administrator 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.

Note 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.

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 2-1. 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 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 vSphere Web Client to perform corresponding tasks.

Table 2-1. Groups in the vsphere.local Domain (Continued)

Privilege	Description
SystemConfiguration.BashShellAdministrators	This group is available only for vCenter Server Appliance deployments. A user in this group can enable and disable access to the BASH shell. By default a user who connects to the vCenter Server Appliance 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.
ExternalIPDUsers	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 Web 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.
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.

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 Web Client or Platform Services Controller Web interface. 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.

- 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.

- Add 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 from the vSphere Web Client or the Platform Services Controller interface.

- Edit a vCenter Single Sign-On Identity Source

  vSphere users are defined in an identity source. You can edit the details of an identity source that is associated with vCenter Single Sign-On.

- Remove a vCenter Single Sign-On Identity Source

  You can remove an identity source from the list of registered identity sources. When you do, users from that identity source can no longer authenticate to vCenter Single Sign-On.

- 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 Platform Services Controller to an Active Directory domain before you can use SSPI.

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.

An identity source is a collection of user and group data. 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. A vCenter Single Sign-On administrator can add identity sources, set the default identity source, and create users and groups in the vsphere.local identity source.

Types of Identity Sources

vCenter Server versions earlier than version 5.1 supported Active Directory and local operating system users as user repositories. As a result, local operating system users were always able to authenticate to the vCenter Server system. vCenter Server version 5.1 and version 5.5 uses vCenter Single Sign-On for authentication. See the vSphere 5.1 documentation for a list of supported identity sources with vCenter Single Sign-On 5.1. vCenter Single Sign-On 5.5 supports the following types of user repositories as identity sources, but supports only one default identity source.

- Active Directory versions 2003 and later. Shown as **Active Directory (Integrated Windows Authentication)** in the vSphere Web Client. 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.
- Active Directory over LDAP. vCenter Single Sign-On supports multiple Active Directory over LDAP identity sources. This identity source type is included for compatibility with the vCenter Single Sign-On service included with vSphere 5.1. Shown as **Active Directory as an LDAP Server** in the vSphere Web Client.
- OpenLDAP versions 2.4 and later. vCenter Single Sign-On supports multiple OpenLDAP identity sources. Shown as **OpenLDAP** in the vSphere Web Client.
- Local operating system users. Local operating system users are local to the operating system where the vCenter Single Sign-On server is running. The local operating system identity source exists only in basic vCenter Single Sign-On server deployments and is not available in deployments with multiple vCenter Single Sign-On instances. Only one local operating system identity source is allowed. Shown as **localos** in the vSphere Web Client.

  Note Do not use local operating system users if the Platform Services Controller is on a different machine than the vCenter Server system. Using local operating system users might make sense in an embedded deployment but is not recommended.

- vCenter Single Sign-On system users. Exactly one system identity source is created when you install 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 (*DOMAIN\user*) to authenticate successfully.

vCenter Single Sign-On identity sources are managed by vCenter Single Sign-On administrator users.

You can add identity sources to a vCenter Single Sign-On server instance. Remote identity sources are limited to Active Directory and OpenLDAP server implementations.

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 Web 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 From a Web browser, connect to the vSphere Web Client or the Platform Services Controller.

Option	Description
vSphere Web Client	`https://vc_hostname_or_IP/vsphere-client`
Platform Services Controller	`https://psc_hostname_or_IP/psc` In an embedded deployment, the Platform Services Controller host name or IP address is the same as the vCenter Server host name or IP address.

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 configuration UI.

Option	Description
vSphere Web Client	a From the **Home** menu, select **Administration**. b Under **Single Sign-On**, click **Configuration**.
Platform Services Controller	Click **Single Sign-On** and click **Configuration**.

4 On the **Identity Sources** tab, select an identity source and click the **Set as Default Domain** icon.

In the domain display, the default domain shows (default) in the Domain column.

Add 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 from the vSphere Web Client or the Platform Services Controller interface.

An identity source can be a native Active Directory (Integrated Windows Authentication) domain or an OpenLDAP directory service. For backward compatibility, Active Directory as an LDAP Server is also available. See Identity Sources for vCenter Server with vCenter Single Sign-On

Immediately after installation, the following default identity sources and users are available:

localos	All local operating system users. If you are upgrading, those localos users who can already authenticate can continue to authenticate. Using the localos identity source does not make sense in environments that use an embedded Platform Services Controller.
vsphere.local	Contains the vCenter Single Sign-On internal users.

Prerequisites

If you are adding an Active Directory identity source, the vCenter Server Appliance or the Windows machine on which vCenter Server is running must be in the Active Directory domain. See Add a Platform Services Controller Appliance to an Active Directory Domain.

Procedure

1 From a Web browser, connect to the vSphere Web Client or the Platform Services Controller.

Option	Description
vSphere Web Client	`https://vc_hostname_or_IP/vsphere-client`
Platform Services Controller	`https://psc_hostname_or_IP/psc` In an embedded deployment, the Platform Services Controller host name or IP address is the same as the vCenter Server host name or IP address.

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 configuration UI.

Option	Description
vSphere Web Client	a From the **Home** menu, select **Administration**. b Under **Single Sign-On**, click **Configuration**.
Platform Services Controller	Click **Single Sign-On** and click **Configuration**.

4 On the **Identity Sources** tab, click the **Add Identity Source** icon.

5 Select the identity source type 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 as an LDAP Server	This option is available for backward compatibility. It requires that you specify the domain controller and other information. See Active Directory LDAP Server and OpenLDAP Server Identity Source Settings.
OpenLDAP	Use this option for an OpenLDAP identity source. See Active Directory LDAP Server and OpenLDAP Server Identity Source Settings.
LocalOS	Use this option to add the local operating system as an identity source. You are prompted only for the name of the local operating system. If you select this option, all users on the specified machine are visible to vCenter Single Sign-On, even if those users are not part of another domain.

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 If you configured an Active Directory as an LDAP Server or an OpenLDAP identity source, click **Test Connection** to ensure that you can connect to the identity source.

7 Click **OK**.

What to do next

When an identity source is added, all users can be authenticated but have the **No access** role. A user with vCenter Server **Modify.permissions** privileges can assign give users or groups of users privileges that enable them to log in to vCenter Server and view and manage objects. See the *vSphere Security* 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 Identity Source

You can set up vCenter Single Sign-On to use an Active Directory identity source only if that identity source is available.

- For a Windows installation, join the Windows machine to the Active Directory domain.

- For a vCenter Server Appliance, follow the instructions in the *vCenter Server Appliance 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 VMware Knowledge Base article 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.

Note In vSphere 5.5, vCenter Single Sign-On uses the machine account even if you specify the SPN. See VMware Knowledge Base article 2087978.

Table 2-2. 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. If you are using a vCenter Server Appliance, use the information on configuring network settings to update the DNS server settings.
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 `setspn –S` 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).

Active Directory LDAP Server and OpenLDAP Server Identity Source Settings

The Active Directory as an LDAP Server identity source is available for backward compatibility. Use the Active Directory (Integrated Windows Authentication) option for a setup that requires less input. The OpenLDAP Server identity source is available for environments that use OpenLDAP.

If you are configuring an OpenLDAP identity source, see VMware Knowledge Base article 2064977 for additional requirements.

Table 2-3. Active Directory as an LDAP Server and OpenLDAP Settings

Option	Description
Name	Name of the identity source.
Base DN for users	Base Distinguished Name for users.
Domain name	FDQN of the domain, for example, example.com. Do not provide an IP address in this text box.
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.
Base DN for groups	The base Distinguished Name for 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.
Choose certificate	If you want to use LDAPS with your Active Directory LDAP Server or OpenLDAP Server identity source, a **`Choose certificate`** button appears after you type **`ldaps://`** in the URL text box. A secondary URL is not required.
Username	ID of a user in the domain who has a minimum of read-only access to Base DN for users and groups.
Password	Password of the user who is specified by **Username**.

Edit a vCenter Single Sign-On Identity Source

vSphere users are defined in an identity source. You can edit the details of an identity source that is associated with vCenter Single Sign-On.

Procedure

1 From a Web browser, connect to the vSphere Web Client or the Platform Services Controller.

Option	Description
vSphere Web Client	**`https://`*`vc_hostname_or_IP`*`/vsphere-client`**
Platform Services Controller	**`https://`*`psc_hostname_or_IP`*`/psc`** In an embedded deployment, the Platform Services Controller host name or IP address is the same as the vCenter Server host name or IP address.

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 configuration UI.

Option	Description
vSphere Web Client	a From the **Home** menu, select **Administration**. b Under **Single Sign-On**, click **Configuration**.
Platform Services Controller	Click **Single Sign-On** and click **Configuration**.

4 Click the **Identity Sources** tab.

5 Right-click the identity source in the table and select **Edit Identity Source**.

6 Edit the identity source settings. The available options depend on the type of identity source you selected.

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 as an LDAP Server	This option is available for backward compatibility. It requires that you specify the domain controller and other information. See Active Directory LDAP Server and OpenLDAP Server Identity Source Settings.
OpenLDAP	Use this option for an OpenLDAP identity source. See Active Directory LDAP Server and OpenLDAP Server Identity Source Settings.
LocalOS	Use this option to add the local operating system as an identity source. You are prompted only for the name of the local operating system. If you select this option, all users on the specified machine are visible to vCenter Single Sign-On, even if those users are not part of another domain.

7 Click **Test Connection** to ensure that you can connect to the identity source.

8 Click **OK**.

Remove a vCenter Single Sign-On Identity Source

You can remove an identity source from the list of registered identity sources. When you do, users from that identity source can no longer authenticate to vCenter Single Sign-On.

Procedure

1 From a Web browser, connect to the vSphere Web Client or the Platform Services Controller.

Option	Description
vSphere Web Client	`https://vc_hostname_or_IP/vsphere-client`
Platform Services Controller	`https://psc_hostname_or_IP/psc` In an embedded deployment, the Platform Services Controller host name or IP address is the same as the vCenter Server host name or IP address.

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 configuration UI.

Option	Description
vSphere Web Client	a From the **Home** menu, select **Administration**. b Under **Single Sign-On**, click **Configuration**.
Platform Services Controller	Click **Single Sign-On** and click **Configuration**.

4 On the **Identity Sources** tab, select an identity source and click the **Delete Identity Source** icon.

5 Click **Yes** when prompted to confirm.

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 Platform Services Controller to an Active Directory domain before you can use SSPI.

Using SSPI speeds up the login process for the user who is currently logged in to a machine.

Prerequisites

- Join the Platform Services Controller appliance or the Windows machine on which Platform Services Controller is running to an Active Directory domain. See Add a Platform Services Controller Appliance to an Active Directory Domain.
- Verify that the domain is set up properly. See VMware Knowledge Base article 2064250.
- If you are using vSphere 6.0 and earlier, verify that the Client Integration Plug-in is installed.
- If you are using vSphere 6.5 and later, verify that the Enhanced Authentication Plug-In is installed. See *vSphere Installation and Setup*.

Procedure

1. Navigate to the vSphere Web 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.

vCenter Server Two-Factor Authentication

vCenter Single Sign-On allows you to authenticate as a user in an identity source that is known to vCenter Single Sign-On, or by using Windows session authentication. Starting with vSphere 6.0 Update 2, you can also authenticate 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.

Smart card authentication

Smart card authentication allows access only to users who attach a physical card to the USB drive of 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 Platform Services Controller 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 Platform Services Controller Web interface, or by using the `sso-config` script.

- For smart card authentication, you can perform the vCenter Single Sign-On setup from the Platform Services Controller Web interface 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 Web interface. However, if you enable RSA SecurID, that authentication method appears in the Web interface.

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.

When you configure smart card authentication for vCenter Single Sign-On, you must set up your environment before users can log in using smart card authentication.

- If you are using vSphere 6.0 and earlier, verify that the Client Integration Plug-in is installed.
- If you are using vSphere 6.5 and later, verify that the Enhanced Authentication Plug-In is installed. See *vSphere Installation and Setup*.

Users who log in to a vCenter Server or Platform Services Controller system are then prompted to authenticate with a smart card and PIN combination, as follows.

1. When the user inserts the smart card into the smart card reader, vCenter Single Sign-On reads the certificates on the card.
2. vCenter Single Sign-On prompts the user to select a certificate, and 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 and whether the PIN is correct. If revocation checking is turned on, vCenter Single Sign-On also checks whether the certificate is revoked.

4 If the certificate is known, and is not a revoked certificate, the user is authenticated and can then perform tasks that the user has permissions for.

Note It usually makes sense to leave user name and password authentication enabled during testing. After testing is complete, disable user name and password authentication and enable smart card authentication. Subsequently, the vSphere Web Client allows only smart card login. Only users with root or administrator privileges on the machine can reenable user name and password authentication by logging in to thePlatform Services Controller 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 or associated Platform Services Controller from the vSphere Web Client.

How you set up smart card authentication depends on the version of vSphere that you are using.

vSphere Version	Procedure	Links
6.0 Update 2 Later versions of vSphere 6.0	1 Set up the Tomcat server. 2 Enable and configure smart card authentication.	vSphere 6.0 documentation center.
6.5 and later	1 Set up the reverse proxy. 2 Enable and configure smart card authentication.	Configure the Reverse Proxy to Request Client Certificates Use the Command Line to Manage Smart Card Authentication Use the Platform Services Controller Web Interface to Manage Smart Card Authentication

Configure the Reverse Proxy to Request Client Certificates

Before you enable smart card authentication, you have to configure the reverse proxy on the Platform Services Controller system. If your environment uses an embedded Platform Services Controller, you perform this task on the system where both vCenter Server and Platform Services Controller run.

Reverse proxy configuration is required in vSphere 6.5 and later.

Prerequisites

Copy the CA certificates to the Platform Services Controller system.

Procedure

1 Log in to the Platform Services Controller.

OS	Description
Appliance	Log in to the appliance shell as the root user.
Windows	Log in to a Windows command prompt as an Administrator user.

2 Create a trusted client CA store.

This store will contain 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 Platform Services Controller appliance.

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
```

Note On Platform Services Controller on Windows, use `C:\ProgramData\VMware\vCenterServer\runtime\VMwareSTSService\conf\` and change the command to use backward slash.

3 Make a backup of the `config.xml` file that includes the reverse proxy definition, and open `config.xml` in an editor.

OS	Description
Appliance	`/etc/vmware-rhttpproxy/config.xml`
Windows	`C:\ProgramData\VMware\vCenterServer\cfg\vmware-rhttpproxy\config.xml`

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.

OS	Description
Appliance	`/usr/lib/vmware-vmon/vmon-cli --restart rhttpproxy`

Windows	Restart the operating system, or restart the VMware HTTP Reverse Proxy from the Service Manager or by following these steps:
	a Open an elevated command prompt.
	b Run the following commands:
	`cd C:\Program Files\VMware\vCenter Server\bin`
	`--stop vmware-rhttpproxy service-control`
	`--start vmware-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 locations:

Windows	`C:\Program Files\VMware\VCenter server\VMware Identity Services\sso-config.bat`
Linux	`/opt/vmware/bin/sso-config.sh`

Configuration of supported authentication types and revocation settings is stored in VMware Directory Service and replicated across all Platform Services Controller 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 Platform Services Controller command line. The following command enables user name and password authentication.

OS	Command
Windows	`sso-config.bat -set_authn_policy -pwdAuthn true -t <tenant_name>` If you use the default tenant, use vsphere.local as the tenant name.
Linux	`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 your environment uses Platform Services Controller version 6.5, and that you use vCenter Server version 6.0 or later. Platform Services Controller version 6.0 Update 2 supports smart card authentication, but the setup procedure is different.
- 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 Enhanced Key Usage field or the browser does not show the certificate.
- Verify that the Platform Services Controller Web interface certificate is trusted by the end user's workstation. Otherwise, the browser does not attempt the 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.

  Note The administrator of the vCenter Single Sign-On domain, administrator@vsphere.local by default, cannot perform smart card authentication.

- Set up the reverse proxy and restart the physical or virtual machine.

Procedure

1 Obtain the certificates and copy them to a folder that the `sso-config` utility can see.

Option	Description
Windows	Log in to the Platform Services Controller Windows installation and use WinSCP or a similar utility to copy the files.

Appliance	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 Platform Services Controller.
	d Optionally disable the appliance shell, as follows.
	`chsh -s "bin/appliancesh" root`

2 To enable smart cart authentication for VMware Directory Service (vmdir), run the following command.

```
sso-config.[bat|sh] -set_authn_policy -certAuthn true -cacerts
first_trusted_cert.cer,second_trusted_cert.cer  -t tenant
```

For example:

```
sso-config.[bat|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.[bat|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 white list, run the following command.

```
sso-config.[bat|sh] -set_authn_policy -certPolicies policies
```

To specify multiple policies, separate them with a command, for example:

```
sso-config.bat -set_authn_policy -certPolicies 2.16.840.1.101.2.1.11.9,2.16.840.1.101.2.1.11.19
```

This white list 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.[bat|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.[bat|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.[bat|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 reponder 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.[bat|sh] -t tenantName -get_alt_ocsp]
```

d To remove the current alternative OCSP responder settings, run this command.

```
sso-config.[bat|sh] -t tenantName -delete_alt_ocsp [-allSite] [-siteID
pscSiteID_for_the_configuration]
```

6 (Optional) To list configuration information, run the following command.

```
sso-config.[bat|sh] -get_authn_policy -t tenantName
```

Use the Platform Services Controller Web Interface to Manage Smart Card Authentication

You can enable and disable smart card authentication, customize the login banner, and set up the revocation policy from the Platform Services Controller Web interface.

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 Platform Services Controller command line. The following command enables user name and password authentication.

OS	Command
Windows	`sso-config.bat -set_authn_policy -pwdAuthn true -t <tenant_name>` If you use the default tenant, use vsphere.local as the tenant name.
Linux	`sso-config.sh -set_authn_policy -pwdAuthn true -t <tenant_name>` If you use the default tenant, use vsphere.local as the tenant name.

Prerequisites

- Verify that your environment uses Platform Services Controller version 6.5, and that you use vCenter Server version 6.0 or later. Platform Services Controller version 6.0 Update 2 supports smart card authentication, but the setup procedure is different.
- 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 Enhanced Key Usage field or the browser does not show the certificate.
- Verify that the Platform Services Controller Web interface certificate is trusted by the end user's workstation. Otherwise, the browser does not attempt the 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.

  Note The administrator of the vCenter Single Sign-On domain, administrator@vsphere.local by default, cannot perform smart card authentication.

- Set up the reverse proxy and restart the physical or virtual machine.

Procedure

1 Obtain the certificates and copy them to a folder that the `sso-config` utility can see.

Option	Description
Windows	Log in to the Platform Services Controller Windows installation and use WinSCP or a similar utility to copy the files.

Appliance	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`
	`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` on the Platform Services Controller.
	d Optionally disable the appliance shell, as follows.
	`chsh -s "bin/appliancesh" root`

2 From a Web browser, connect to the vSphere Web Client or the Platform Services Controller.

Option	Description
vSphere Web Client	**`https://`*`vc_hostname_or_IP`*`/vsphere-client`**
Platform Services Controller	**`https://`*`psc_hostname_or_IP`*`/psc`** In an embedded deployment, the Platform Services Controller host name or IP address is the same as the vCenter Server host name or IP address.

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 vCenter Single Sign-On configuration UI.

Option	Description
vSphere Web Client	a From the **Home** menu, select **Administration**. b Under **Single Sign-On**, click **Configuration**.
Platform Services Controller	Click **Single Sign-On** and click **Configuration**.

5 Click **Smart Card Configuration**, and select the **Trusted CA certificates** tab.

6 To add one or more trusted certificates, click **Add Certificate**, click **Browse**, select all certificates from trusted CAs, and click **OK**.

7 To specify the authentication configuration, click **Edit** next to **Authentication Configuration** and select or deselect authentication methods.

   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.

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 Platform Services Controller 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 Platform Services Controller Web interface 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 recommended 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. You can explicitly specify a location if the Authority Information Access extension is absent from the certificate or if you want to override it.
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 your environment uses Platform Services Controller version 6.5, and that you use vCenter Server version 6.0 or later. Platform Services Controller version 6.0 Update 2 supports smart card authentication, but the setup procedure is different.
- 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 Enhanced Key Usage field or the browser does not show the certificate.
- Verify that the Platform Services Controller Web interface certificate is trusted by the end user's workstation. Otherwise, the browser does not attempt the 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.

  Note The administrator of the vCenter Single Sign-On domain, administrator@vsphere.local by default, cannot perform smart card authentication.

Procedure

1 From a Web browser, connect to the vSphere Web Client or the Platform Services Controller.

Option	Description
vSphere Web Client	`https://vc_hostname_or_IP/vsphere-client`
Platform Services Controller	`https://psc_hostname_or_IP/psc` In an embedded deployment, the Platform Services Controller host name or IP address is the same as the vCenter Server host name or IP address.

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 configuration UI.

Option	Description
vSphere Web Client	a From the **Home** menu, select **Administration**. b Under **Single Sign-On**, click **Configuration**.
Platform Services Controller	Click **Single Sign-On** and click **Configuration**.

4 Click **Certificate Revocation Settings** and enable or disable revocation checking.

5 If certificate policies are in effect in your environment, you can add a policy in the **Certificate policies accepted** 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 uses Platform Services Controller version 6.5, and that you use vCenter Server version 6.0 or later. Platform Services Controller version 6.0 Update 2 supports smart card authentication, but the setup procedure is different.
- 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 a vCenter Single Sign-On Identity Source.

- Verify that the RSA Authentication Manager system can resolve the Platform Services Controller host name, and that the Platform Services Controller 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**. Decompress the resulting `AM_Config.zip` file to find the `sdconf.rec` file.
- Copy the `sdconf.rec` file to the Platform Services Controller node.

Procedure

1 Change to the directory where the `sso-config` script is located.

Option	Description
Windows	`C:\Program Files\VMware\VCenter server\VMware Identity Services`
Appliance	`/opt/vmware/bin`

2 To enable RSA SecurID authentication, run the following command.

```
sso-config.[sh|bat]  -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|bat] -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|bat] -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.

The userID attribute determines which LDAP attribute is used as the RSA userID.

```
sso-config.[sh|bat] -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
```

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***.

Manage the Login Banner

Starting with vSphere 6.0 Update 2, you can include a login banner with your environment. You can enable and disable the login banner, and you can require that users click an explicit consent check box.

Procedure

1 From a Web browser, connect to the vSphere Web Client or the Platform Services Controller.

Option	Description
vSphere Web Client	`https://vc_hostname_or_IP/vsphere-client`
Platform Services Controller	`https://psc_hostname_or_IP/psc` In an embedded deployment, the Platform Services Controller host name or IP address is the same as the vCenter Server host name or IP address.

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 Click **Single Sign-On**, click **Configuration**, and click the **Login Banner** tab.

4 Click **Edit** and configure the login banner.

Option	Description
Status	Click the **Enabled** check box to enable the login banner. You cannot make login banner changes unless you click this check box.
Explicit Consent	Click the **Explicit Consent** check box to require that the user clicks a check box before logging in. You can also display a message without a check box.
Title	Title of the banner. By default, the Login Banner text is `I agree to the`. You can add to that, for example `Terms and Conditions`.
Message	Message that the user sees when clicking the banner, for example, the text of the terms and conditions. The message is required if you use explicit consent.

Using vCenter Single Sign-On as the Identity Provider for Another Service Provider

The vSphere Web Client is automatically registered as trusted SAML 2.0 Service Provider (SP) to vCenter Single Sign-On. You can add other trusted service providers to an identity federation where vCenter Single Sign-On acting as the SAML Identity Provider (IDP). The service providers must conform to the SAML 2.0 protocol. After the federation is set up, the service provider grants access to a user if that user can authenticate to vCenter Single Sign-On.

Note vCenter Single Sign-On can be the IDP to other SPs.vCenter Single Sign-On cannot be an SP that uses another IDP.

A registered SAML service provider can grant access to a user that already has a live session, that is, a user that is logged in to the identity provider. For example, vRealize Automation 7.0 and later supports vCenter Single Sign-On as an identity provider. You can set up a federation from vCenter Single Sign-On and from vRealize Automation. After that, vCenter Single Sign-On can perform the authentication when you log in to vRealize Automation.

To join a SAML service provider to the identity federation, you have to set up trust between the SP and the IDP by exchanging SAML metadata between them.

You have to perform integration tasks for both vCenter Single Sign-On and the service that is using vCenter Single Sign-On.

1 Export IDP metadata to a file, then import it to the SP.

2 Export SP metadata and import it into the IDP.

You can use the vSphere Web Client interface to vCenter Single Sign-On to export the IDP metadata, and to import the metadate from the SP. If you are using vRealize Automation as the SP, see the vRealize Automation documentation for details on exporting the SP metadata and importing the IDP metadata.

Note The service must fully support the SAML 2.0 standard or integration does not work.

Join a SAML Service Provider to the Identity Federation

You add a SAML service provider to vCenter Single Sign-On, and add vCenter Single Sign-On as the identity provider to that service. Going forward, when users log in to the service provider, the service provider authenticates those users with vCenter Single Sign-On.

Prerequisites

The target service must fully support the SAML 2.0 standard and the SP metadata must have the `SPSSODescriptor` element.

If the metadata do not follow the SAML 2.0 metadata schema precisely, you might have to edit the metadata before you import it. For example, if you are using an Active Directory Federation Services (ADFS) SAML service provider, you have to edit the metadata before you can import them. Remove the following non-standard elements:

```
fed:ApplicationServiceType
fed:SecurityTokenServiceType
```

Procedure

1 Export the metadata from the service provider to a file.

2 From a Web browser, connect to the vSphere Web Client or the Platform Services Controller.

Option	Description
vSphere Web Client	`https://vc_hostname_or_IP/vsphere-client`
Platform Services Controller	`https://psc_hostname_or_IP/psc` In an embedded deployment, the Platform Services Controller host name or IP address is the same as the vCenter Server host name or IP address.

3 Import the SP metadata into vCenter Single Sign-On.

   a Select the **SAML Service Providers** tab.

   b In the **Metadata from your SAML service provider** dialog box, import the metadata by pasting the XML string or by importing a file.

4 Export the vCenter Single Sign-On IDP metadata.

   a In the **Metadata for your SAML service provider** text box, click **Download**.

   b Specify a file location.

5 Log in to the SAML SP, for example VMware vRealize Automation 7.0, and follow the SP instructions to add the vCenter Single Sign-On metadata to that service provider.

   See the vRealize Automation documentation for details on importing the metadata into that product.

Security Token Service STS

The vCenter Single Sign-On Security Token Service (STS) is a Web service that issues, validates, and renews security tokens.

Users present their primary credentials to the STS interface to acquire SAML tokens. The primary credential depends on the type of user.

User	User name and password available in a vCenter Single Sign-On identity source.
Application user	Valid certificate.

STS authenticates the user based on the primary credentials, and constructs a SAML token that contains user attributes. STS signs the SAML token with its STS signing certificate, and assigns the token to the user. By default, the STS signing certificate is generated by VMCA. You can replace the default STS signing certificate from the vSphere Web Client. Do not replace the STS signing certificate unless your company's security policy requires replacing all certificates.

After a user has a SAML token, the SAML token is sent as part of that user's HTTP requests, possibly through various proxies. Only the intended recipient (service provider) can use the information in the SAML token.

Refresh the Security Token Service Certificate

The vCenter Single Sign-On server includes a Security Token Service (STS). The Security Token Service is a Web service that issues, validates, and renews security tokens. You can manually refresh the existing Security Token Service certificate from the vSphere Web Client when the certificate expires or changes.

To acquire a SAML token, a user presents the primary credentials to the Secure Token Server (STS). The primary credentials depend on the type of user:

Solution user	Valid certificate
Other users	User name and password available in a vCenter Single Sign-On identity source.

The STS authenticates the user using the primary credentials, and constructs a SAML token that contains user attributes. The STS service signs the SAML token with its STS signing certificate, and then assigns the token to a user. By default, the STS signing certificate is generated by VMCA.

After a user has a SAML token, the SAML token is sent as part of that user's HTTP requests, possibly through various proxies. Only the intended recipient (service provider) can use the information in the SAML token.

You can replace the existing STS signing certificate vSphere Web Client if your company policy requires it, or if you want to update an expired certificate.

Caution Do not replace the file in the filesystem. If you do, errors that are unexpected and difficult to debug result.

Note After you replace the certificate, you must restart the node to restart both the vSphere Web Client service and the STS service.

Prerequisites

Copy the certificate that you just added to the java keystore from the Platform Services Controller to your local workstation.

Platform Services Controller appliance	*certificate_location*/keys/root-trust.jks For example: /keys/root-trust.jks For example: /root/newsts/keys/root-trust.jks
Windows installation	*certificate_location*\root-trust.jks For example: C:\Program Files\VMware\vCenter Server\jre\bin\root-trust.jks

Procedure

1. Log in to the vSphere Web Client as administrator@vsphere.local or as another user with vCenter Single Sign-On administrator privileges.

   Users with vCenter Single Sign-On administrator privileges are in the Administrators group in the local vCenter Single Sign-On domain, vsphere.local by default.
2. Select the **Certificates** tab, then the **STS Signing** subtab, and click the **Add STS Signing Certificate** icon.
3. Add the certificate.
   a. Click **Browse** to browse to the key store JKS file that contains the new certificate and click **Open**.
   b. Type the password when prompted.
   c. Click the top of the STS alias chain and click **OK**.
   d. Type the password again when prompted
4. Click **OK**.
5. Restart the Platform Services Controller node to start both the STS service and the vSphere Web Client.

   Before the restart, authentication does not work correctly so the restart is essential.

Generate a New STS Signing Certificate on the Appliance

If you want to replace the default vCenter Single Sign-On Security Token Service (STS) signing certificate, you have to generate a new certificate and add it to the Java key store. This procedure explains the steps on an embedded deployment appliance or an external Platform Services Controller appliance.

Note This certificate is valid for ten years and is not an external-facing certificate. Do not replace this certificate unless your company's security policy requires it.

See Generate a New STS Signing Certificate on a vCenter Windows Installation if you are running a Platform Services Controller Windows installation.

Procedure

1 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/newst
```

2 Copy the `certool.cfg` file into the new directory.

```
cp /usr/lib/vmware-vmca/share/config/certool.cfg /root/newsts
```

3 Open your copy of the `certool.cfg` file and edit it to use the local Platform Services Controller 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
```

4 Generate the key.

```
/usr/lib/vmware-vmca/bin/certool --server localhost --genkey --privkey=/root/newsts/sts.key --
pubkey=/root/newsts/sts.pub
```

5 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
```

6 Convert the certificate to PK12 format.

```
openssl pkcs12 -export -in /root/newsts/newsts.cer -inkey /root/newsts/sts.key -
certfile /etc/vmware-sso/keys/ssoserverRoot.crt -name "newstssigning" -passout pass:changeme -out
newsts.p12
```

7 Add the certificate to the Java key store (JKS).

```
/usr/java/jre-vmware/bin/keytool -v -importkeystore -srckeystore newsts.p12 -srcstoretype pkcs12 -
srcstorepass changeme -srcalias newstssigning -destkeystore root-trust.jks -deststoretype JKS -
deststorepass testpassword -destkeypass testpassword

/usr/java/jre-vmware/bin/keytool -v -importcert -keystore root-trust.jks -deststoretype JKS -
storepass testpassword -keypass testpassword -file /etc/vmware-sso/keys/ssoserverRoot.crt -alias
root-ca
```

8 When prompted, type **Yes** to accept the certificate into the keystore.

What to do next

You can now import the new certificate. See Refresh the Security Token Service Certificate.

Generate a New STS Signing Certificate on a vCenter Windows Installation

If you want to replace the default STS signing certificate, you have to first generate a new certificate and add it to the Java key store. This procedure explains the steps on a Windows installation.

Note This certificate is valid for ten years and is not an external-facing certificate. Do not replace this certificate unless your company's security policy requires it.

See Generate a New STS Signing Certificate on the Appliance if you are using a virtual appliance.

Procedure

1 Create a new directory to hold the new certificate.

```
cd C:\ProgramData\VMware\vCenterServer\cfg\sso\keys\
mkdir newsts
cd newsts
```

2 Make a copy of the `certool.cfg` file and place it in the new directory.

```
copy "C:\Program Files\VMware\vCenter Server\vmcad\certool.cfg" .
```

3 Open your copy of the `certool.cfg` file and edit it to use the local Platform Services Controller IP address and hostname.

The country is required and has to be two characters. The following sample illustrates this.

```
#
# 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
```

4 Generate the key.

```
"C:\Program Files\VMware\vCenter Server\vmcad\certool.exe" --server localhost --genkey --
privkey=sts.key --pubkey=sts.pub
```

5 Generate the certificate

```
"C:\Program Files\VMware\vCenter Server\vmcad\certool.exe" --gencert --cert=newsts.cer --
privkey=sts.key --config=certool.cfg
```

6 Convert the certificate to PK12 format.

```
"C:\Program Files\VMware\vCenter Server\openSSL\openssl.exe" pkcs12 -export -in newsts.cer -inkey
sts.key -certfile ..\ssoserverRoot.crt -name "newstssigning" -passout pass:changeme -out newsts.p12
```

7 Add the certificate to the Java key store (JKS).

```
"C:\Program Files\VMware\vCenter Server\jre\bin\keytool.exe" -v -importkeystore -srckeystore
newsts.p12 -srcstoretype pkcs12 -srcstorepass changeme -srcalias newstssigning -destkeystore root-
trust.jks -deststoretype JKS -deststorepass testpassword -destkeypass testpassword
"C:\Program Files\VMware\vCenter Server\jre\bin\keytool.exe" -v -importcert -keystore root-
trust.jks -deststoretype JKS -storepass testpassword -keypass testpassword -
file ..\ssoserverRoot.crt -alias root-ca
```

What to do next

You can now import the new certificate. See Refresh the Security Token Service Certificate.

Determine the Expiration Date of an LDAPS SSL Certificate

If you select an LDAP identity source, and you decide to use LDAPS, you can upload an SSL certificate for the LDAP traffic. SSL certificates expire after a predefined lifespan. Knowing when a certificate expires lets you replace or renew the certificate before the expiration date.

You see certificate expiration information only if you use an Active Directory LDAP Server or OpenLDAP Server and specify an `ldaps://` URL for the server. The Identity Sources **TrustStore** tab remains empty for other types of identity sources or for `ldap://` traffic.

Procedure

1 From a Web browser, connect to the vSphere Web Client or the Platform Services Controller.

Option	Description
vSphere Web Client	`https://vc_hostname_or_IP/vsphere-client`
Platform Services Controller	`https://psc_hostname_or_IP/psc` In an embedded deployment, the Platform Services Controller host name or IP address is the same as the vCenter Server host name or IP address.

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 configuration UI.

Option	Description
vSphere Web Client	a From the **Home** menu, select **Administration**. b Under **Single Sign-On**, click **Configuration**.
Platform Services Controller	Click **Single Sign-On** and click **Configuration**.

4 Click the **Certificates** tab, and click **Identity Sources TrustStore**.

5 Find the certificate and verify the expiration date in the **Valid To** text box.

You might see a warning at the top of the tab which indicates that a certificate is about to expire.

Managing vCenter Single Sign-On Policies

vCenter Single Sign-On policies enforce the security rules in your environment. 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 governs the format and expiration of vCenter Single Sign-On user passwords. The password policy applies only to users in the vCenter Single Sign-On domain (vsphere.local).

By default, vCenter Single Sign-On passwords expire after 90 days. The vSphere Web Client reminds you when your password is about to expire.

Note The password policy applies only to user accounts, not to system accounts such as administrator@vsphere.local.

See Change Your vCenter Single Sign-On Password.

Procedure

1 From a Web browser, connect to the vSphere Web Client or the Platform Services Controller.

Option	Description
vSphere Web Client	`https://vc_hostname_or_IP/vsphere-client`
Platform Services Controller	`https://psc_hostname_or_IP/psc` In an embedded deployment, the Platform Services Controller host name or IP address is the same as the vCenter Server host name or IP address.

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 configuration UI.

Option	Description
vSphere Web Client	a From the **Home** menu, select **Administration**. b Under **Single Sign-On**, click **Configuration**.
Platform Services Controller	Click **Single Sign-On** and click **Configuration**.

4 Click the **Policies** tab and select **Password Policies**.

5 Click **Edit**.

6 Edit the password policy parameters.

Option	Description
Description	Password policy description.
Maximum lifetime	Maximum number of days that a password is valid before the user must change it.
Restrict reuse	Number of previous passwords that cannot be reused. For example, if you type 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 The minimum number of alphabetic characters must be no less than the combined uppercase and lowercase characters. In vSphere 6.0 and later, non-ASCII characters are supported in passwords. In earlier versions of vCenter Single Sign-On, limitations on supported characters exist.
Identical adjacent characters	Maximum number of identical adjacent characters that are allowed in the password. For example, if you enter 1, the following password is not allowed: p@$$word. The number must be greater than 0.

7 Click **OK**.

Edit the vCenter Single Sign-On Lockout Policy

A vCenter Single Sign-On lockout policy specifies when a user's vCenter Single Sign-On account is locked if the user attempts to log in with incorrect credentials. 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 From a Web browser, connect to the vSphere Web Client or the Platform Services Controller.

Option	Description
vSphere Web Client	`https://vc_hostname_or_IP/vsphere-client`
Platform Services Controller	`https://psc_hostname_or_IP/psc` In an embedded deployment, the Platform Services Controller host name or IP address is the same as the vCenter Server host name or IP address.

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 configuration UI.

Option	Description
vSphere Web Client	a From the **Home** menu, select **Administration**. b Under **Single Sign-On**, click **Configuration**.
Platform Services Controller	Click **Single Sign-On** and click **Configuration**.

4 Click the **Policies** tab and select **Lockout Policy**.

5 Click **Edit**.

6 Edit the parameters.

Option	Description
Description	Optional description of the lockout policy.
Max 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 **OK**.

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 From a Web browser, connect to the vSphere Web Client or the Platform Services Controller.

Option	Description
vSphere Web Client	`https://vc_hostname_or_IP/vsphere-client`
Platform Services Controller	`https://psc_hostname_or_IP/psc` In an embedded deployment, the Platform Services Controller host name or IP address is the same as the vCenter Server host name or IP address.

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 configuration UI.

Option	Description
vSphere Web Client	a From the **Home** menu, select **Administration**. b Under **Single Sign-On**, click **Configuration**.
Platform Services Controller	Click **Single Sign-On** and click **Configuration**.

4 Click the **Policies** tab and select **Token Policy**.

The vSphere Web Client displays the current configuration settings. If you have not modified the default settings, vCenter Single Sign-On uses them.

5 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.

Option	Description
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.

6 Click **OK**.

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 Web 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 Web 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.

- 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.

- 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.

- 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.

- 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).

- 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 Web Client.

- Remove Members From a vCenter Single Sign-On Group

  You can remove members from a vCenter Single Sign-On group by using the vSphere Web Client or the Platform Services Controller Web interface. When you remove a member (user or group) from a group, you do not delete the member from the system.

- Delete vCenter Single Sign-On Solution Users

  vCenter Single Sign-On displays solution users. A solution user is a collection of services. Several vCenter Server solution users are predefined and authenticate to vCenter Single Sign-On as part of installation. In troubleshooting situations, for example, if an uninstall did not complete cleanly, you can delete individual solution users from the vSphere Web Client.

- 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 a Web interface. Users in other domains change their passwords following the rules for that domain.

Add vCenter Single Sign-On Users

Users listed on the **Users** tab in the vSphere Web 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 From a Web browser, connect to the vSphere Web Client or the Platform Services Controller.

Option	Description
vSphere Web Client	`https://vc_hostname_or_IP/vsphere-client`
Platform Services Controller	`https://psc_hostname_or_IP/psc` In an embedded deployment, the Platform Services Controller host name or IP address is the same as the vCenter Server host name or IP address.

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.

Option	Description
vSphere Web Client	a From the **Home** menu, select **Administration**. b Under **Single Sign-On**, click **Users and Groups**.
Platform Services Controller	Click **Single Sign-On** and click **Users and Groups**.

4 If vsphere.local is not the currently selected domain, select it from the dropdown menu.

You cannot add users to other domains.

5 On the **Users** tab, click the **New User** icon.

6 Type a user name and password for the new user.

You cannot change the user name after you create a user.

The password must meet the password policy requirements for the system.

7 (Optional) Type the first name and last name of the new user.

8 (Optional) Enter an email address and description for the user.

9 Click **OK**.

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 From a Web browser, connect to the vSphere Web Client or the Platform Services Controller.

Option	Description
vSphere Web Client	`https://vc_hostname_or_IP/vsphere-client`
Platform Services Controller	`https://psc_hostname_or_IP/psc` In an embedded deployment, the Platform Services Controller host name or IP address is the same as the vCenter Server host name or IP address.

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.

Option	Description
vSphere Web Client	a From the **Home** menu, select **Administration**. b Under **Single Sign-On**, click **Users and Groups**.
Platform Services Controller	Click **Single Sign-On** and click **Users and Groups**.

4 Select a user account, click the **Disable** icon, and click **Yes** when prompted.

5 To enable the user again, right-click the user name, select **Enable**, and click **Yes** when prompted.

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 From a Web browser, connect to the vSphere Web Client or the Platform Services Controller.

Option	Description
vSphere Web Client	`https://vc_hostname_or_IP/vsphere-client`
Platform Services Controller	`https://psc_hostname_or_IP/psc` In an embedded deployment, the Platform Services Controller host name or IP address is the same as the vCenter Server host name or IP address.

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.

Option	Description
vSphere Web Client	a From the **Home** menu, select **Administration**. b Under **Single Sign-On**, click **Users and Groups**.
Platform Services Controller	Click **Single Sign-On** and click **Users and Groups**.

4 Select the **Users** tab, and select the vsphere.local domain.

5 In the list of users, select the user that you want to delete and click the **Delete** icon.

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 Web Client. Log in as administrator@vsphere.local and select **Configuration > Policies > Password Policies**.

See also Edit the vCenter Single Sign-On Password Policy.

Procedure

1 From a Web browser, connect to the vSphere Web Client or the Platform Services Controller.

Option	Description
vSphere Web Client	`https://vc_hostname_or_IP/vsphere-client`
Platform Services Controller	`https://psc_hostname_or_IP/psc` In an embedded deployment, the Platform Services Controller host name or IP address is the same as the vCenter Server host name or IP address.

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.

Option	Description
vSphere Web Client	a From the **Home** menu, select **Administration**. b Under **Single Sign-On**, click **Users and Groups**.
Platform Services Controller	Click **Single Sign-On** and click **Users and Groups**.

4 Click the **Users** tab.

5 Right-click the user and select **Edit User**.

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 From a Web browser, connect to the vSphere Web Client or the Platform Services Controller.

Option	Description
vSphere Web Client	`https://vc_hostname_or_IP/vsphere-client`
Platform Services Controller	`https://psc_hostname_or_IP/psc` In an embedded deployment, the Platform Services Controller host name or IP address is the same as the vCenter Server host name or IP address.

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.

Option	Description
vSphere Web Client	a From the **Home** menu, select **Administration**. b Under **Single Sign-On**, click **Users and Groups**.
Platform Services Controller	Click **Single Sign-On** and click **Users and Groups**.

4 Select the **Groups** tab and click the **New Group** icon.

5 Enter a name and description for the group.

You cannot change the group name after you create the group.

6 Click **OK**.

What to do next

- Add members to the 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 Web Client.

See VMware Knowledge Base article 2095342 for some 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 From a Web browser, connect to the vSphere Web Client or the Platform Services Controller.

Option	Description
vSphere Web Client	`https://vc_hostname_or_IP/vsphere-client`
Platform Services Controller	`https://psc_hostname_or_IP/psc` In an embedded deployment, the Platform Services Controller host name or IP address is the same as the vCenter Server host name or IP address.

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.

Option	Description
vSphere Web Client	a From the **Home** menu, select **Administration**. b Under **Single Sign-On**, click **Users and Groups**.
Platform Services Controller	Click **Single Sign-On** and click **Users and Groups**.

4 Click the **Groups** tab and click the group (for example, Administrators).

5 In the Group Members area, click the **Add Members** icon.

6 Select the identity source that contains the member to add to the group.

7 (Optional) Enter a search term and click **Search**.

8 Select the member and click **Add**.

You can add more than one member.

9 Click **OK**.

Remove Members From a vCenter Single Sign-On Group

You can remove members from a vCenter Single Sign-On group by using the vSphere Web Client or the Platform Services Controller Web interface. When you remove a member (user or group) from a group, you do not delete the member from the system.

Procedure

1 From a Web browser, connect to the vSphere Web Client or the Platform Services Controller.

Option	Description
vSphere Web Client	`https://vc_hostname_or_IP/vsphere-client`
Platform Services Controller	`https://psc_hostname_or_IP/psc` In an embedded deployment, the Platform Services Controller host name or IP address is the same as the vCenter Server host name or IP address.

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.

Option	Description
vSphere Web Client	a From the **Home** menu, select **Administration**. b Under **Single Sign-On**, click **Users and Groups**.
Platform Services Controller	Click **Single Sign-On** and click **Users and Groups**.

4 Select the **Groups** tab and click the group.

5 In the list of group members, select the user or group that you want to remove and click the **Remove Member** icon.

6 Click **OK**.

The user is removed from the group, but is still available in the system.

Delete vCenter Single Sign-On Solution Users

vCenter Single Sign-On displays solution users. A solution user is a collection of services. Several vCenter Server solution users are predefined and authenticate to vCenter Single Sign-On as part of installation. In troubleshooting situations, for example, if an uninstall did not complete cleanly, you can delete individual solution users from the vSphere Web Client.

When you remove the set of services associated with a vCenter Server solution user or a third-party solution user from your environment, the solution user is removed from the vSphere Web Client display. If you forcefully remove an application, or if the system becomes unrecoverable while the solution user is still in the system, you can remove the solution user explicitly from the vSphere Web Client.

Important If you delete a solution user, the corresponding services can no longer authenticate to vCenter Single Sign-On.

Procedure

1 From a Web browser, connect to the vSphere Web Client or the Platform Services Controller.

Option	Description
vSphere Web Client	`https://vc_hostname_or_IP/vsphere-client`
Platform Services Controller	`https://psc_hostname_or_IP/psc` In an embedded deployment, the Platform Services Controller host name or IP address is the same as the vCenter Server host name or IP address.

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.

Option	Description
vSphere Web Client	a From the **Home** menu, select **Administration**. b Under **Single Sign-On**, click **Users and Groups**.
Platform Services Controller	Click **Single Sign-On** and click **Users and Groups**.

4 Click the **Solution Users** tab, and click the solution user name.

5 Click the **Delete Solution User** icon.

6 Click **Yes**.

The services associated with the solution user no longer have access to vCenter Server and cannot function as vCenter Server services.

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 a Web interface. 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 user 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.

This procedure explains how you can change a valid password.

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 From a Web browser, connect to the vSphere Web Client or the Platform Services Controller.

Option	Description
vSphere Web Client	`https://vc_hostname_or_IP/vsphere-client`
Platform Services Controller	`https://psc_hostname_or_IP/psc` In an embedded deployment, the Platform Services Controller host name or IP address is the same as the vCenter Server host name or IP address.

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 left 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 User** from the right-button menu.

4 Select **Change Password** and type your current password.

5 Type a new password and confirm it.

The password must conform to the password policy.

6 Click **OK**.

vCenter Single Sign-On Security Best Practices

Follow vCenter Single Sign-On security best practices to protect your vSphere environment.

The vSphere 6.0 authentication and certificate 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 is expired and the ability to log is compromised. 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.

vSphere Security Certificates

3

vCenter services use SSL to communicate securely with each other and with ESXi. SSL communications ensure data confidentiality and integrity. Data is protected and cannot be modified in transit without detection.

vCenter Server services such as the vSphere Web Client also use certificates for initial authentication to vCenter Single Sign-On. vCenter Single Sign-On provisions each set of services (solution user) with a SAML token that the solution user can authenticate with.

In vSphere 6.0 and later, the VMware Certificate Authority (VMCA) provisions each ESXi host and each vCenter Server service with a certificate that is signed by VMCA by default.

You can replace the existing certificates with new VMCA-signed certificates, make VMCA a subordinate CA, or replace all certificates with custom certificates. You have several options:

Table 3-1. Different Approaches to Certificate Replacement

Option	See
Use the Platform Services Controller Web interface (vSphere 6.0 Update 1 and later).	Managing Certificates with the Platform Services Controller Web Interface
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 4 Managing Services and Certificates With CLI Commands

vSphere Certificate Management
(http://link.brightcove.com/services/player/bcpid2296383276001?bctid=ref:video_vsphere6_cert_infrastructure)

This section includes the following topics:

- Certificate Requirements for Different Solution Paths
- Certificate Management Overview
- Managing Certificates with the Platform Services Controller Web Interface
- Managing Certificates from the vSphere Web Client
- Managing Certificates with the vSphere Certificate Manager Utility
- Manual Certificate Replacement

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 and for solution user certificates.

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

Requirements for All Imported Certificates

- Key size: 2048 bits or more (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.
- Client Authentication and Server Authentication cannot be present under Enhanced Key Usage.

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.
- If you are generating a CSR in an environment with an external Platform Services Controller, you are prompted for the host name or IP address of the Platform Services Controller.
- 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 Platform Services Controller if you are running the command on a vCenter Server (management) node

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 or more
	  ■ PEM format. VMware supports PKCS8 and PKCS1 (RSA keys). When keys are added to VECS, they are converted to PKCS8
	  ■ x509 version 3
	  ■ If you are using custom certificates, the CA extension must be set to true for root certificates, and cert sign must be in the list of requirements.
	  ■ CRL signing must be enabled.
	  ■ Enhanced Key Usage must not contain Client Authentication or 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 VMware Knowledge Base Article 2112009, Creating a Microsoft Certificate Authority Template for SSL certificate creation in vSphere 6.0, for an example using Microsoft Certificate Authority.

Machine SSL certificate	You can use vSphere Certificate Manager to create the CSR or create the CSR manually. If you create the CSR manually, it must meet the requirements listed under *Requirements for All Imported Certificates* above. 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. 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*.

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 CSRs using vSphere Certificate Manager or create the CSR manually. The CSR must meet the requirements listed under *Requirements for All Imported Certificates* above. ■ 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 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 under *Requirements for All Imported Certificates* above. ■ 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. If you generate the certificate manually, this 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.

Note Do not use CRL Distribution Points, Authority Information Access, or Certificate Template Information in any custom certificates.

Certificate Management Overview

The work required for setting up or updating your certificate infrastructure depends on the requirements in your environment, on whether you are performing a fresh install or an upgrade, and on 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 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 company policy does not allow intermediate certificates in the chain, you can replace certificates explicitly. You can use thePlatform Services Controller Web interface, 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 certificate 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 certificate mode is VMCA, the default, and the user performs a certificate refresh from the vSphere Web Client, the VMCA-signed certificates replace the custom certificates.
- For vCenter Server components, what happens depends on the existing environment.
  - An upgrade of a simple installation to an embedded deployment, vCenter Server retains custom certificates. After the upgrade, your environment will work as before.
  - For an upgrade of a multi-site deployment, vCenter Single Sign-On can be on a different machine than other vCenter Server components. In that case, the upgrade process creates a multi-node deployment that includes a Platform Services Controller node and one or more management nodes.

This scenario retains the existing vCenter Server and vCenter Single Sign-On certificates. 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 company policy.

You can no longer use the vSphere 5.5 certificate replacement tool, which was available for vSphere 5.5 installations. The new architecture results in a different service distribution and placement. A new command-line utility, vSphere Certificate Manager, is available for most certificate management tasks.

vSphere Certificate Interfaces

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

Table 3-2. Interfaces for Managing vCenter Server Certificates

Interface	Use
Platform Services Controller Web Interface	Perform common certificate tasks with a graphical user interface.
vSphere 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`.
vSphere Web Client	View certificates, including expiration information.

For ESXi, you perform certificate management from the vSphere Web 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, the Platform Services Controller, 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

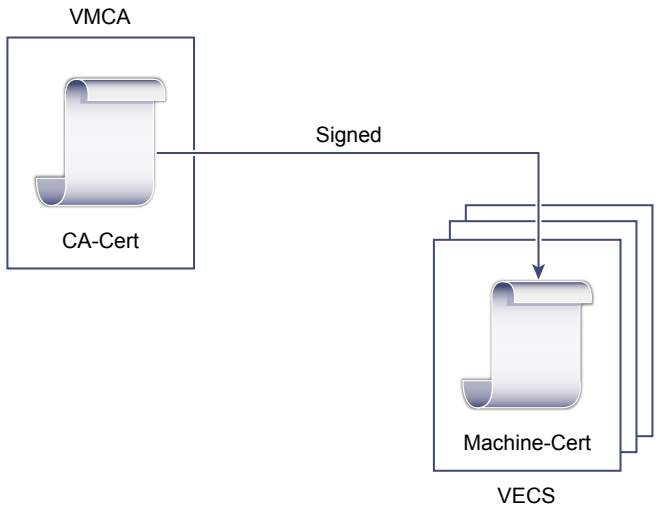
You can perform different types of certificate replacement depending on company policy and requirements for the system that you are configuring. You can perform certificate replacement from the Platform Services Controller, by using the vSphere Certificate Manager utility or manually by using the CLIs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

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 ten years, and all certificates that VMCA signs expire when the root certificate expires, that is, after a maximum of ten years.

Figure 3-1. Certificates Signed by VMCA Are Stored in VECS

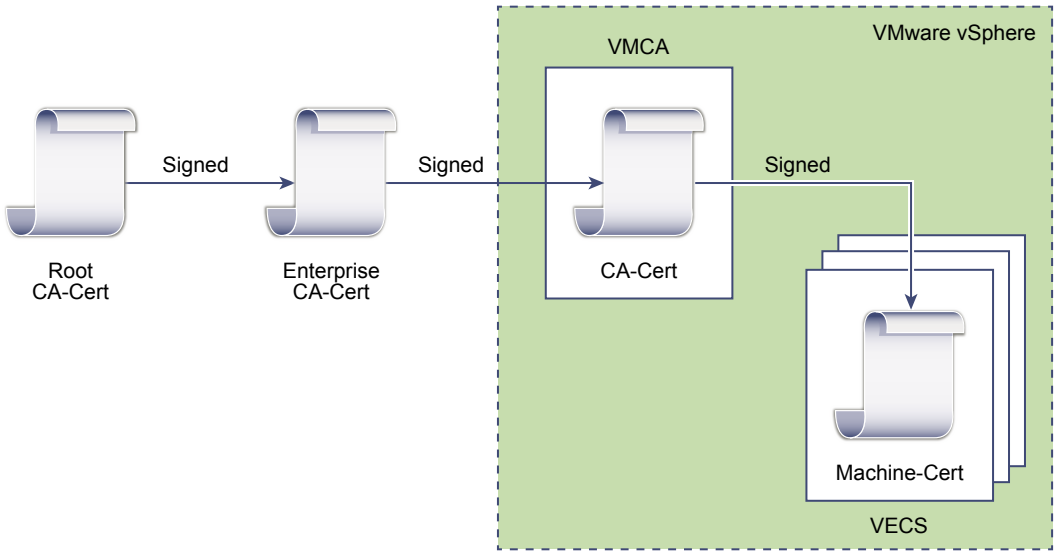


Make VMCA an Intermediate CA

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 that includes an external Platform Services Controller, install the Platform Services Controller first and replace the VMCA root certificate. Next, install other services or add ESXi hosts to your environment. If you perform a fresh install with an embedded Platform Services Controller, 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.

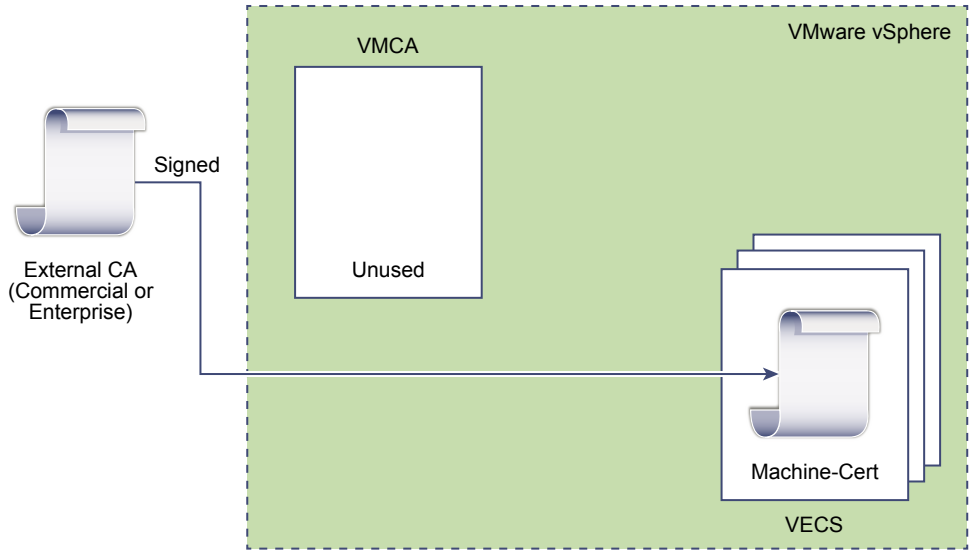
Figure 3-2. Certificates Signed by a Third-Party or Enterprise CA Use VMCA as an Intermediate CA



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 3-3. External Certificates are Stored Directly in VECS



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 Web Client. See the *vSphere Security*documentation for details.

Table 3-3. ESXi Certificate Replacement Options

Option	Description
VMware Certificate Authority mode (default)	When you renew certificates from the vSphere Web 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 manually update and use certificates 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

In vSphere 6.0 and later, 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 3-4. Certificates in vSphere 6.0

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 vSphere Web Client. 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 node has its own machine SSL certificate. Nodes include vCenter Server instance, Platform Services Controller instance, or embedded deployment instance. All services that are running on a node use the machine SSL certificate to expose their SSL endpoints.

The following services use the machine SSL certificate.

- The reverse proxy service on each Platform Services Controller node. SSL connections to individual vCenter services always go to the reverse proxy. Traffic does not go to the services themselves.
- The vCenter service (vpxd) on management nodes and embedded nodes.
- The VMware Directory Service (vmdir) on infrastructure nodes and embedded nodes.

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 Web Client or Platform Services Controller Web interface 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 on each management node and each embedded deployment:

- `machine`: Used by component manager, 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 on management nodes and embedded deployments. vpxd uses the solution user certificate that is stored in this store to authenticate to vCenter Single Sign-On.
- `vpxd-extensions`: vCenter extensions store. Includes the Auto Deploy service, inventory service, and other services that are not part of other solution users.

- `vsphere-webclient`: vSphere Web Client store. Also includes some additional services such as the performance chart service.

Each Platform Services Controller node includes a `machine` certificate.

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. vCenter Single Sign-On issues holder-of-key SAML tokens to solution users and bearer tokens other users, which log in with a user name and password. You can replace this certificate from the vSphere Web Client. See Refresh the Security Token Service Certificate.
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 embedded deployment and every platform services node. VMCA is part of every VMware core identity services group. Use the management CLIs and the vSphere Web Client to interact with these services.

VMware core identity services include several components.

Table 3-5. Core Identity Services

Service	Description	Included in
VMware Directory Service (vmdir)	Handles SAML certificate management for authentication in conjunction with vCenter Single Sign-On.	Platform Services Controller Embedded deployment
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.	Platform Services Controller Embedded deployment
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.	Platform Services Controller vCenter Server Embedded deployment

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 embedded deployment, Platform Services Controller node, and management node and holds the keystores that contain the certificates and keys.

VECS polls VMware Directory Service (vmdir) periodically for updates to the TRUSTED_ROOTS 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 3-6. 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 embedded deployments and on each Platform Services Controller node. All services in vSphere 6.0 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.
Trusted root store (TRUSTED_ROOTS)	Contains all trusted root certificates.

Table 3-6. Stores in VECS (Continued)

Store	Description
Solution user stores ■ machine ■ vpxd ■ vpxd-extensions ■ vsphere-webclient	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. In an embedded deployment, all solution user certificates are on the same system. The following solution user certificate stores are included in VECS on each management node and each embedded deployment: ■ machine: Used by component manager, 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 on management nodes and embedded deployments. vpxd uses the solution user certificate that is stored in this store to authenticate to vCenter Single Sign-On. ■ vpxd-extensions: vCenter extensions store. Includes the Auto Deploy service, inventory service, and other services that are not part of other solution users. ■ vsphere-webclient: vSphere Web Client store. Also includes some additional services such as the performance chart service. Each Platform Services Controller node includes a machine certificate.
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 vSphere Web Client.

Some certificates are stored on the filesystem, either temporarily during startup or permanently. Do not change the certificates on the file system. Use `vecs-cli` to perform operations on certificates that are stored in VECS.

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 6.0 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

Certificate replacement in deployments that include multiple management nodes and one or more Platform Services Controller nodes is similar to replacement in embedded deployments. In both cases, you can use the vSphere Certificate Management utility or replace certificates manually. Some best practices guide the replacement process.

Certificate Replacement in High Availability Environments That Include a Load Balancer

In environments with less than eight vCenter Server systems, VMware typically recommends a single Platform Services Controller instance and associated vCenter Single Sign-On service. In larger environments, consider using multiple Platform Services Controller instances, protected by a network load balancer. The white paper *vCenter Server 6.0 Deployment Guide* on the VMware website discusses this setup.

Replacement of Machine SSL Certificates in Environments with Multiple Management Nodes

If your environment includes multiple management nodes and a single Platform Services Controller, you can replace certificates with the vSphere Certificate Manager utility, or manually with vSphere CLI commands.

vSphere Certificate Manager

You run vSphere Certificate Manager on each machine. On management nodes, you are prompted for the IP address of the Platform Services Controller. 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. On management nodes, you must specify the Platform Services Controller with the `--server` parameter. 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 Management Nodes

If your environment includes multiple management nodes and a single Platform Services Controller, 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. On management nodes, you are prompted for the IP address of the Platform Services Controller. 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 the Platform Services Controller.
   - A certificate for the machine solution user on each management node.

- A certificate for each of the following solution users on each management node:
  - `vpxd solution` user
  - `vpxd-extension` solution user
  - `vsphere-webclient` 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 or Platform Services Controller. If you replace the default machine SSL certificate on the vCenter Server system or the Platform Services Controller, 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 VMware Knowledge Base article 2109074 for details.

Managing Certificates with the Platform Services Controller Web Interface

You can view and manage certificates by logging in to the Platform Services Controller web interface. You can perform many certificate management tasks either with the vSphere Certificate Manager utility or by using this web interface.

The Platform Services Controller web interface allows you to perform these management tasks.

- View the current certificate stores and add and remove certificate store entries.
- View the VMware Certificate Authority (VMCA) instance associated with this Platform Services Controller.
- View certificates that are generated by VMware Certificate Authority.
- Renew existing certificates or replace certificates.

Most parts of the certificate replacement workflows are supported fully from the Platform Services Controller web interface. For generating CSRs, you can use the vSphere Certificate Manage utility.

Supported Workflows

After you install a Platform Services Controller, the VMware Certificate Authority on that node provisions all other nodes in the environment with certificates by default. You can use one of the following workflows to renew or replace certificates.

Renew Certificates	You can have VMCA generate a new root certificate and renew all certificates in your environment from the Platform Services Controller web interface.
Make VMCA an Intermediate CA	You can generate a CSR using the vSphere Certificate Manager utility, edit the certificate you receive from the CSR to add VMCA to the chain, and then add the certificate chain and private key to your environment. When you then renew all certificates, VMCA provisions all machines and solution users with certificates that are signed by the full chain.
Replace Certificates with Custom Certificates	If you do not want to use 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 Platform Services Controller.

In a mixed-mode environment, you can use CLI commands to replace the vCenter Single Sign-On certificate after replacing the other certificates. See Replace the VMware Directory Service Certificate in Mixed Mode Environments.

Explore Certificate Stores from the Platform Services Controller Web Interface

A VMware Endpoint Certificate Store (VECS) instance is included on each Platform Services Controller node and each vCenter Server node. You can explore the different stores inside the VMware Endpoint Certificate Store from the Platform Services Controller web interface.

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 From a Web browser, connect to the vSphere Web Client or the Platform Services Controller.

Option	Description
vSphere Web Client	`https://vc_hostname_or_IP/vsphere-client`
Platform Services Controller	`https://psc_hostname_or_IP/psc` In an embedded deployment, the Platform Services Controller host name or IP address is the same as the vCenter Server host name or IP address.

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 Under Certificates, click **Certificate Store** and explore the store.

4 Select the store inside the VMware Endpoint Certificate Store (VECS) that you want to explore from the pulldown menu.

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

5 To view details for a certificate, select the certificate and click the **Show Details** icon.

6 To delete an entry from the selected store, click the **Delete Entry** icon.

   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.

Replace Certificates with New VMCA-Signed Certificates from the Platform Services Controller Web Interface

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 Platform Services Controller web interface.

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 From a Web browser, connect to the vSphere Web Client or the Platform Services Controller.

Option	Description
vSphere Web Client	`https://vc_hostname_or_IP/vsphere-client`
Platform Services Controller	`https://psc_hostname_or_IP/psc` In an embedded deployment, the Platform Services Controller host name or IP address is the same as the vCenter Server host name or IP address.

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 Log in as an administrator.

4 Renew the machine SSL certificate for the local system.
   a Click the **Machine Certificates** tab.
   b Select the certificate, click **Renew**, and answer **Yes** to the prompt.
5 (Optional) Renew the solution user certificates for the local system.
   a Click the **Solution User Certificates** tab.
   b Select a certificate and click **Renew** to renew individual selected certificates, or click **Renew All** to renew all solution user certificates.
   c Answer **Yes** at the prompt.
6 If your environment includes an external Platform Services Controller, you can then renew the certificates for each of the vCenter Server system.
   a Click the **Logout** button in the Certificate Management panel.
   b When prompted, specify the IP address or FQDN of the vCenter Server system and user name and password of a vCenter Server administrator who can authenticate to vCenter Single Sign-On.
   c Renew the machine SSL certificate on the vCenter Server and, optionally, each solution user certificate.
   d If you have multiple vCenter Server systems in your environment, repeat the process for each system.

What to do next

Restart services on the Platform Services Controller. You can either restart the Platform Services Controller, or run the following commands from the command line:

Windows

On Windows, the `service-control` command is located at *`VCENTER_INSTALL_PATH`*`\bin`.

```
service-control --stop --all
service-control --start VMWareAfdService
service-control --start VMWareDirectoryService
service-control --start VMWareCertificateService
```

vCenter Server Appliance

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

Make VMCA an Intermediate Certificate Authority from the Platform Services Controller Web Interface

You can have the VMCA certificate signed by another CA so that VMCA becomes an intermediate CA. Going forward, all certificates that VMCA generates include the full chain.

You can perform this setup by using the vSphere Certificate Manager utility, by using CLIs, or from the Platform Services Controller Web interface.

Prerequisites

1 Generate the CSR.

2 Edit the certificate that you receive, and place the current VMCA root certificate at the bottom.

Generate CSR with vSphere Certificate Manager and Prepare Root Certificate (Intermediate CA) explains both steps.

Procedure

1 From a Web browser, connect to the vSphere Web Client or the Platform Services Controller.

Option	Description
vSphere Web Client	`https://vc_hostname_or_IP/vsphere-client`
Platform Services Controller	`https://psc_hostname_or_IP/psc` In an embedded deployment, the Platform Services Controller host name or IP address is the same as the vCenter Server host name or IP address.

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 To replace the existing certificate with the chained certificate, follow these steps:

a Under Certificates, click **Certificate Authority** and select the **Root Certificate** tab.

b Click **Replace Certificate**, add the private key file and the certificate file (full chain), and click **OK**.

c In the **Replace Root Certificate** dialog box, click **Browse** and select the private key, click **Browse** again and select the certificate, and click **OK**.

Going forward, VMCA signs all certificates that it issues with the new chained root certificate.

4 Renew the machine SSL certificate for the local system.

a Under Certificates, click **Certificate Management** and click the **Machine Certificates** tab.

b Select the certificate, click **Renew**, and answer **Yes** to the prompt.

VMCA replaces the machine SSL certificate with the certificate that is signed by the new CA.

5 (Optional) Renew the solution user certificates for the local system.

   a Click the **Solution User Certificates** tab.

   b Select a certificate and click **Renew** to renew individual selected certificates, or click **Renew All** to replace all certificates and answer **Yes** to the prompt.

   VMCA replaces the solution user certificate or all solution user certificates with certificates that are signed by the new CA.

6 If your environment includes an external Platform Services Controller, you can then renew the certificates for each of the vCenter Server system.

   a Click the **Logout** button in the Certificate Management panel.

   b When prompted, specify the IP address or FQDN of the vCenter Server system and user name and password of a vCenter Server administrator.

   The administrator must be able to authenticate to vCenter Single Sign-On.

   c Renew the machine SSL certificate on the vCenter Server and, optionally, each solution user certificate.

   d If you have multiple vCenter Server systems in your environment, repeat the process for each system.

What to do next

Restart services on the Platform Services Controller. You can either restart the Platform Services Controller, or run the following commands from the command line:

Windows

On Windows, the `service-control` command is located at *`VCENTER_INSTALL_PATH`*`\bin`.

```
service-control --stop --all
service-control --start VMWareAfdService
service-control --start VMWareDirectoryService
service-control --start VMWareCertificateService
```

vCenter Server Appliance

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

Set up Your System to Use Custom Certificates from the Platform Services Controller

You can use the Platform Services Controller to 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. 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 Platform Services Controller UI.

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:

Windows

```
C:\Program Files\VMware\vCenter Server\vmcad\certificate-manager.bat
```

Linux

```
/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.
- If you are generating a CSR in an environment with an external Platform Services Controller, you are prompted for the host name or IP address of the Platform Services Controller.
- 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 Platform Services Controller 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 Platform Services Controller 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.

On each Platform Services Controller node, Certificate Manager generates one certificate and key pair. On each vCenter Server node, Certificate Manager generates four certificate and key pairs.

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 From a Web browser, connect to the vSphere Web Client or the Platform Services Controller.

Option	Description
vSphere Web Client	`https://vc_hostname_or_IP/vsphere-client`
Platform Services Controller	`https://psc_hostname_or_IP/psc` In an embedded deployment, the Platform Services Controller host name or IP address is the same as the vCenter Server host name or IP address.

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 Log in as an administrator.

4 Select **Trusted Root Certificates**, and click **Add certificate**.

5 Click **Browse** and select the location of the certificate chain.

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

What to do next

Replace the Machine SSL certificates and, optionally, the Solution User certificates with certificates that are signed by this CA.

Add Custom Certificates from the Platform Services Controller

You can add custom Machine SSL certificates and custom solution user certificates to the certificate store from the Platform Services Controller.

In most cases, replacing the machine SSL certificate for each component is sufficient. The solution user certificate remains behind a proxy.

Prerequisites

Generate certificate signing requests (CSRs) for each certificate that you want to replace. You can generate the CSRs with the Certificate Manager utility. Place the certificate and private key in a location that the Platform Services Controller can access.

Procedure

1 From a Web browser, connect to the vSphere Web Client or the Platform Services Controller.

Option	Description
vSphere Web Client	`https://vc_hostname_or_IP/vsphere-client`
Platform Services Controller	`https://psc_hostname_or_IP/psc` In an embedded deployment, the Platform Services Controller host name or IP address is the same as the vCenter Server host name or IP address.

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 Log in as an administrator.

4 To replace a machine certificate follow these steps:

a Select the **Machine Certificates** tab and click the certificate that you want to replace.

b Click **Replace**, and click **Browse** to replace the certificate chain, then click **Browse** to replace the private key.

5 To replace the solution user certificates, follow these steps:

a Select the **Solution User Certificates** tab and click the first of the four certificates for a component, for example, **machine**.

b Click **Replace**, and click **Browse** to replace the certificate chain, then click **Browse** to replace the private key.

c Repeat the process for the other three certificates for the same component.

What to do next

Restart services on the Platform Services Controller. You can either restart the Platform Services Controller, or run the following commands from the command line:

Windows

On Windows, the `service-control` command is located at *VCENTER_INSTALL_PATH*\bin.

```
service-control --stop --all
service-control --start VMWareAfdService
service-control --start VMWareDirectoryService
service-control --start VMWareCertificateService
```

vCenter Server Appliance

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

Managing Certificates from the vSphere Web Client

You can explore certificates from the vSphere Web Client, and you can set the threshold for expiration warnings. Perform all other management tasks from the Platform Services Controller Web interface.

See Managing Certificates with the Platform Services Controller Web Interface.

View vCenter Certificates with the vSphere Web Client

You can view the certificates known to the vCenter Certificate Authority (VMCA) to see whether active certificates are about to expire, to check on expired certificates, and to see the status of the root certificate. You perform all certificate management tasks using the certificate management CLIs.

You view certificates associated with the VMCA instance that is included with your embedded deployment or with the Platform Services Controller. Certificate information is replicated across instances of VMware Directory Service (vmdir).

When you attempt to view certificates in the vSphere Web Client, you are prompted for a user name and password. Specify the user name and password of a user with privileges for VMware Certificate Authority, that is, a user in the CAAdmins vCenter Single Sign-On group.

Procedure

1. Log in to vCenter Server as administrator@vsphere.local or another user of the CAAdmins vCenter Single Sign-On group.
2. From the Home menu, select **Administration**.
3. Click **Nodes**, and select the node for which you want to view or manage certificates.
4. Click the **Manage** tab, and click **Certificate Authority**.

5 Click the certificate type for which you want to view certificate information.

Option	Description
Active Certificates	Displays active certificates, including their validation information. The green Valid To icon changes when certificate expiration is approaching.
Revoked Certificates	Displays the list of revoked certificates. Not supported in this release.
Expired Certificates	Lists expired certificates.
Root Certificates	Displays the root certificates available to this instance of vCenter Certificate Authority.

6 Select a certificate and click the **Show Certificate Details** button to view certificate details.

Details include the Subject Name, Issuer, Validity, and Algorithm.

Set the Threshold for vCenter Certificate Expiration Warnings

Starting with vSphere 6.0, 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 Web Client.

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

3 Click **Advanced Settings** and filter for **`threshold`**.

4 Change the setting of `vpxd.cert.threshold` to the desired value and click **OK**.

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 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:

Windows

```
C:\Program Files\VMware\vCenter Server\vmcad\certificate-manager.bat
```

Linux

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

1 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.

2 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. In multi-node deployments, run vSphere Certificate Manager with this option on the Platform Services Controller and then run the utility again on all other nodes and select `Replace Machine SSL certificate with VMCA Certificate` and `Replace Solution user certificates with VMCA certificates`.

3 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.

4 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.

5 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.

6 Reset All Certificates

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

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 is a 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. It explains what to do in environments with embedded Platform Services Controller or external Platform Services Controller.

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 In a multi-node deployment, you have to 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. It explains what to do in environments with embedded Platform Services Controller or external Platform Services Controller.

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, in a multi-node deployment, you have to repeat the process on each node.

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

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. In multi-node deployments, run vSphere Certificate Manager with this option on the Platform Services Controller and then run the utility again on all other nodes and select `Replace Machine SSL certificate with VMCA Certificate` and `Replace Solution user certificates with VMCA certificates`.

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 Platform Services Controller, 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 Platform Services Controller if you are running the command on a management node

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 an embedded deployment or on a Platform Services Controller.

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. If you use an embedded deployment, the replacement process is complete after Certificate Manager has restarted the services.

4 If your environment includes an external Platform Services Controller, you have to replace certificates on each vCenter Server system.

a Log in to the vCenter Server system.

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

The service names differ on Windows and the vCenter Server Appliance.

Windows

```
service-control --stop --all
service-control --start VMWareAfdService
service-control --start VMWareDirectoryService
service-control --start VMWareCertificateService
```

vCenter Server Appliance

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

c Restart all services.

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

d To replace the machine SSL certificate, run vSphere Certificate Manager with option 3, `Replace Machine SSL certificate with VMCA Certificate`.

e 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.

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. It explains what to do in environments with embedded Platform Services Controller or external Platform Services Controller.

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.

4 In a multi-node deployment, you have to 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).

Procedure

1 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.

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

   You can use vSphere Certificate Manager to generate a CSR and sent 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.

3 Replace Machine SSL Certificate with VMCA Certificate (Intermediate CA)

   In a multi-node deployment that uses VMCA as an intermediate CA, you have to replace the machine SSL certificate explicitly. First you replace the VMCA root certificate on the Platform Services Controller node, and then you can replace the certificates on the vCenter Server nodes to have the certificates signed by the full chain. You can also use this option to replace machine SSL certificates that are corrupt or about to expire.

4 Replace Solution User Certificates with VMCA Certificates (Intermediate CA)

In a multi-node environment that uses VMCA as an intermediate CA, you can replace the solution user certificates explicitly. First you replace the VMCA root certificate on the Platform Services Controller node, and then you can replace the certificates on the vCenter Server nodes to have the certificates signed by the full chain. You can also use this option to replace solution user certificates that are corrupt or about to expire.

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 or more
  - PEM format. VMware supports PKCS8 and PKCS1 (RSA keys). When keys are added to VECS, they are converted to PKCS8
  - x509 version 3
  - If you are using custom certificates, the CA extension must be set to true for root certificates, and cert sign must be in the list of requirements.
  - CRL signing must be enabled.
  - Enhanced Key Usage must not contain Client Authentication or 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 VMware Knowledge Base Article 2112009, Creating a Microsoft Certificate Authority Template for SSL certificate creation in vSphere 6.0, 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. Start vSphere Certificate Manager and select Option 2.

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

2. Supply the password and the Platform Services Controller IP address or host name if prompted.
3. 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.

4. Send the certificate to the CA for signing to the enterprise or external CA and name the file `root_signing_cert.cer`.
5. 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-----
```

6. 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 sent 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 an embedded installation or on an external Platform Services Controller 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 will 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 an embedded installation or on an external Platform Services Controller 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.
3. If you replace the root certificate on the Platform Services Controller in a multi-node deployment, follow these steps for each vCenter Server node.
   a. Restart services on the vCenter Server node.
   b. Regenerate all certificates on the vCenter Server instance by using options 3 (`Replace Machine SSL certificate with VMCA Certificate`) and 6 (`Replace Solution user certificates with VMCA certificates`).

   When you replace the certificates, VMCA signs with the full chain.

What to do next

If you are upgrading from a vSphere 5.x environment, you might have to replace the vCenter Single Sign-On certificate inside vmdir. See Replace the VMware Directory Service Certificate in Mixed Mode Environments.

Replace Machine SSL Certificate with VMCA Certificate (Intermediate CA)

In a multi-node deployment that uses VMCA as an intermediate CA, you have to replace the machine SSL certificate explicitly. First you replace the VMCA root certificate on the Platform Services Controller node, and then you can replace the certificates on the vCenter Server nodes to have the certificates signed by the full chain. 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 Platform Services Controller, 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 Platform Services Controller if you are running the command on a management node

Prerequisites

- Restart all vCenter Server nodes explicitly if you replaced the VMCA root certificate in a multi-node deployment.
- 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 Platform Services Controller if you are running on a vCenter Server system with an external Platform Services Controller.

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.

vSphere Certificate Manager replaces the machine SSL certificate.

Replace Solution User Certificates with VMCA Certificates (Intermediate CA)

In a multi-node environment that uses VMCA as an intermediate CA, you can replace the solution user certificates explicitly. First you replace the VMCA root certificate on the Platform Services Controller node, and then you can replace the certificates on the vCenter Server nodes to have the certificates signed by the full chain. You can also use this option to replace solution user certificates that are corrupt or about to expire.

Prerequisites

- Restart all vCenter Server nodes explicitly if you replaced the VMCA root certificate in a multi-node deployment.

- 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 Platform Services Controller if you are running on a vCenter Server system with an external Platform Services Controller.

Procedure

1 Start vSphere Certificate Manager and select option 6.

2 Respond to the prompts.

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 Platform Services Controller Web interface, 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. It explains what to do in environments with embedded Platform Services Controller or external Platform Services Controller.

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, in a multi-node deployment, you have to repeat the process on each node.

Procedure

1 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.

2 Replace Machine SSL Certificate with Custom Certificate

   The machine SSL certificate is used by the reverse proxy service on every management node, Platform Services Controller, and embedded deployment. 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.

3 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 Web Client In multi-node deployments replace the machine solution user certificate on the Platform Services Controller and the full set of solution users on each management 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:

Windows

```
C:\Program Files\VMware\vCenter Server\vmcad\certificate-manager.bat
```

Linux

```
/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.
- If you are generating a CSR in an environment with an external Platform Services Controller, you are prompted for the host name or IP address of the Platform Services Controller.
- 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 Platform Services Controller 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 Platform Services Controller 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.

   On each Platform Services Controller node, Certificate Manager generates one certificate and key pair. On each vCenter Server node, Certificate Manager generates four certificate and key pairs.

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 management node, Platform Services Controller, and embedded deployment. 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 or more (PEM encoded)
   - CRT format
   - x509 version 3
   - SubjectAltName must contain DNS Name=<machine_FQDN>
   - Contains the following Key Usages: Digital Signature, Non Repudiation, Key Encipherment

Note Do not use CRL Distribution Points, Authority Information Access, or Certificate Template Information in any custom certificates.

See also VMware Knowledge Base article 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).
- If you are running the command on a management node in a multi-node deployment, IP address of the Platform Services Controller.

What to do next

If you are upgrading from a vSphere 5.x environment, you might have to replace the vCenter Single Sign-On certificate inside `vmdir`. See Replace the VMware Directory Service Certificate in Mixed Mode Environments.

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 Web Client In multi-node deployments replace the machine solution user certificate on the Platform Services Controller and the full set of solution users on each management node.

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

The format should be 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 or more (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, Non Repudiation, Key Encipherment

See also VMware Knowledge Base article 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.
- If you run vSphere Certificate Manager on a Platform Services Controller node, you are prompted for the certificate and key (`vpxd.crt` and `vpxd.key`) for the machine solution user.
- If you run vSphere Certificate Manager on a management node or an embedded deployment, you are prompted for the full set of certificates and keys (`vpxd.crt` and `vpxd.key`) for all solution users.

What to do next

If you are upgrading from a vSphere 5.x environment, you might have to replace the vCenter Single Sign-On certificate inside vmdir. See Replace the VMware Directory Service Certificate in Mixed Mode Environments.

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 if you want 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.

- On a Platform Services Controller node, vSphere Certificate Manager can regenerate the root certificate and replace the machine SSL certificate and the machine solution user certificate.
- On a management node, vSphere Certificate Manager can replace the machine SSL certificate and all solution user certificates.
- In an embedded deployment, vSphere Certificate Manager can replace all certificates.

Which certificates are replaced depends on which options you select.

Manual Certificate Replacement

For some special cases, for example, if you want to replace only one type of solution user certificate, you cannot use the vSphere Certificate Manager utility. In that case, 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.

- If your environment uses an embedded Platform Services Controller, you start and stop all services, as discussed in this document.
- If your environment uses an external Platform Services Controller, you do not have to stop and start VMware Directory Service (vmdird) and VMware Certificate Authority (vmcad) on the vCenter Server node. Those services run on the Platform Services Controller.

Follow these rules of thumb.

- 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 perform these tasks:
  - Delete a machine SSL certificate or any solution user certificate in VECS.
  - Replace a solution user certificate in vmdir (VMware Directory Service).

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.

Procedure

1. 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.

2. 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.

3. 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.

4. Replace the VMware Directory Service Certificate in Mixed Mode Environments

   During upgrade, your environment might temporarily include both vCenter Single Sign-On version 5.5 and vCenter Single Sign-On version 6.x. For that case, you have to perform additional steps to replace the VMware Directory Service SSL certificate if you replace the SSL certificate of the node on which the vCenter Single Sign-On service is running.

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.

In a multi-node deployment, you run root certificate generation commands on the Platform Services Controller.

Procedure

1 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.

The service names differ on Windows and the vCenter Server Appliance.

Windows

```
service-control --stop --all
service-control --start VMWareAfdService
service-control --start VMWareDirectoryService
service-control --start VMWareCertificateService
```

vCenter Server Appliance

```
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 don't 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) List the VMCA root certificate to make sure it is in the certificate store.

- On a Platform Services Controller node or embedded installation:

```
C:\>"C:\Program Files\VMware\vCenter Server\vmcad\"certool --getrootca
```

- On a management node (external installation):

  ```
  C:\>"C:\Program Files\VMware\vCenter Server\vmcad\"certool --getrootca --server=<psc-ip-or-fqdn>
  ```

  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.

  This command works on both Platform Services Controller nodes and management nodes because VECS polls vmdir.

  ```
  "C:\Program Files\VMware\vCenter Server\vmafdd\"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).

  ```
  C:\>"C:\Program Files\VMware\vCenter Server\vmcad\"certool --selfca --config="C:\Program Files\VMware\vCenter Server\vmcad\certool.cfg"
  ```

  On Windows, `--config` is optional because the command uses the default `certool.cfg` file.

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. In a multi-node deployment, you must run the Machine SSL certificate generation commands on each node. Use the `--server` parameter to point to the Platform Services Controller from a vCenter Server with external Platform Services Controller.

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 `certool.cfg` in the following locations:

OS	Path
Windows	`C:\Program Files\VMware\vCenter Server\vmcad`
Linux	`/usr/lib/vmware-vmca/share/config/`

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

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.

The service names differ on Windows and the vCenter Server Appliance.

Windows

```
service-control --stop --all
service-control --start VMWareAfdService
service-control --start VMWareDirectoryService
service-control --start VMWareCertificateService
```

vCenter Server Appliance

```
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 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-<PSC-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. Run this command on each management node and Platform Services Controller node; it does not require a `--server` option.

```
C:\>"C:\Program Files\VMware\vCenter Server\vmcad\"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.

- On a Platform Services Controller node or embedded installation:

```
C:\>"C:\Program Files\VMware\vCenter Server\vmcad\"certool --gencert --cert=new-vmca-ssl.crt --
privkey=ssl-key.priv --config=ssl-config.cfg
```

- On a vCenter Server (external installation):

```
C:\>"C:\Program Files\VMware\vCenter Server\vmcad\"certool --gencert --cert=new-vmca-ssl.crt --
privkey=ssl-key.priv --config=ssl-config.cfg --server=<psc-ip-or-fqdn>
```

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

4 (Optional) List the content of VECS.

```
"C:\Program Files\VMware\vCenter Server\vmafdd\" vecs-cli store list
```

- Sample output on Platform Services Controller:

```
MACHINE_SSL_CERT
TRUSTED_ROOTS
TRUSTED_ROOT_CRLS
machine
```

- Sample output on vCenter Server:

```
output (on vCenter):
MACHINE_SSL_CERT
TRUSTED_ROOTS
TRUSTED_ROOT_CRLS
machine
vpxd
vpxd-extension
vsphere-webclient
sms
```

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 the Platform Services Controller, run the following command to update the Machine SSL certificate in the MACHINE_SSL_CERT store.

```
C:\>"C:\Program Files\VMware\vCenter Server\vmafdd\"vecs-cli entry delete --store
MACHINE_SSL_CERT --alias __MACHINE_CERT
C:\>"C:\Program Files\VMware\vCenter Server\vmafdd\"vecs-cli entry create --store
MACHINE_SSL_CERT --alias __MACHINE_CERT --cert new-vmca-ssl.crt --key ssl-key.priv
```

- On each management node or embedded deployment, run the following command 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.

```
C:\>"C:\Program Files\VMware\vCenter Server\vmafdd\"vecs-cli entry delete --store
MACHINE_SSL_CERT --alias __MACHINE_CERT
C:\>"C:\Program Files\VMware\vCenter Server\vmafdd\"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.

After replacing the root certificate in a multi-node deployment, you must restart services on all vCenter Server with external Platform Services Controller nodes.

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 on each management node and on each Platform Services Controller node. You replace the other solution user certificates only on each management node. Use the `--server` parameter to point to the Platform Services Controller when you run commands on a management node with an external Platform Services Controller.

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.

```
C:\Program Files\VMware\vCenter Server\vmafdd>dir-cli service list
Enter password for administrator@vsphere.local:
1. machine-1d364500-4b45-11e4-96c2-020011c98db3
2. vpxd-1d364500-4b45-11e4-96c2-020011c98db3
3. vpxd-extension-1d364500-4b45-11e4-96c2-020011c98db3
4. vsphere-webclient-1d364500-4b45-11e4-96c2-020011c98db3
```

When you list solution user certificates in multi-node 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.

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

The service names differ on Windows and the vCenter Server Appliance.

Windows

```
service-control --stop --all
service-control --start VMWareAfdService
service-control --start VMWareDirectoryService
service-control --start VMWareCertificateService
```

vCenter Server Appliance

```
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. That includes a pair for the machine solution user on each Platform Services Controller and each management node and a pair for each additional solution user (vpxd, vpxd-extension, vsphere-webclient) on each management node.

a Generate a key pair for the machine solution user of an embedded deployment or for the machine solution user of the Platform Services Controller.

```
C:\>"C:\Program Files\VMware\vCenter Server\vmcad\"certool --genkey --privkey=machine-key.priv
--pubkey=machine-key.pub
```

b (Optional) For deployments with an external Platform Services Controller, generate a key pair for the machine solution user on each management node.

```
C:\>"C:\Program Files\VMware\vCenter Server\vmcad\"certool --genkey --privkey=machine-key.priv
--pubkey=machine-key.pub
```

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

```
C:\>"C:\Program Files\VMware\vCenter Server\vmcad\"certool --genkey --privkey=vpxd-key.priv --
pubkey=vpxd-key.pub
```

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

```
C:\>"C:\Program Files\VMware\vCenter Server\vmcad\"certool --genkey --privkey=vpxd-extension-
key.priv --pubkey=vpxd-extension-key.pub
```

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

```
C:\>"C:\Program Files\VMware\vCenter Server\vmcad\"certool --genkey --privkey=vsphere-
webclient-key.priv --pubkey=vsphere-webclient-key.pub
```

2 Generate solution user certificates that are signed by the new VMCA root certificate for the machine solution user on each Platform Services Controller and each management node and for each additional solution user (vpxd, vpxd-extension, vsphere-webclient) on each management 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 on the Platform Services Controller node to generate a solution user certificate for the machine solution user on that node.

```
C:\>"C:\Program Files\VMware\vCenter Server\vmcad\"certool --gencert --cert=new-machine.crt --
privkey=machine-key.priv --Name=machine
```

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

```
C:\>"C:\Program Files\VMware\vCenter Server\vmcad\"certool --gencert --cert=new-machine.crt --
privkey=machine-key.priv --Name=machine --server=<psc-ip-or-fqdn>
```

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

```
C:\>"C:\Program Files\VMware\vCenter Server\vmcad\"certool --gencert --cert=new-vpxd.crt --
privkey=vpxd-key.priv --Name=vpxd --server=<psc-ip-or-fqdn>
```

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

```
C:\>"C:\Program Files\VMware\vCenter Server\vmcad\"certool --gencert --cert=new-vpxd-
extension.crt --privkey=vpxd-extension-key.priv --Name=vpxd-extension --server=<psc-ip-or-fqdn>
```

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

```
C:\>"C:\Program Files\VMware\vCenter Server\vmcad\"certool --gencert --cert=new-vsphere-
webclient.crt --privkey=vsphere-webclient-key.priv --Name=vsphere-webclient --server=<psc-ip-
or-fqdn>
```

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 On the Platform Services Controller node, run the following command to replace the machine solution user certificate:

```
C:\>"C:\Program Files\VMware\vCenter Server\vmafdd\"vecs-cli entry delete --store machine --
alias machine
C:\>"C:\Program Files\VMware\vCenter Server\vmafdd\"vecs-cli entry create --store machine --
alias machine --cert new-machine.crt --key machine-key.priv
```

b Replace the machine solution user certificate on each management node:

```
C:\>"C:\Program Files\VMware\vCenter Server\vmafdd\"vecs-cli entry delete --store machine --
alias machine
C:\>"C:\Program Files\VMware\vCenter Server\vmafdd\"vecs-cli entry create --store machine --
alias machine --cert new-machine-vc.crt --key machine-vc-key.priv
```

c Replace the vpxd solution user certificate on each management node.

```
C:\>"C:\Program Files\VMware\vCenter Server\vmafdd\"vecs-cli entry delete --store vpxd --alias
vpxd
C:\>"C:\Program Files\VMware\vCenter Server\vmafdd\"vecs-cli entry create --store vpxd --alias
vpxd --cert new-vpxd.crt --key vpxd-key.priv
```

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

```
C:\>"C:\Program Files\VMware\vCenter Server\vmafdd\"vecs-cli entry delete --store vpxd-
extension --alias vpxd-extension
C:\>"C:\Program Files\VMware\vCenter Server\vmafdd\"vecs-cli entry create --store vpxd-
extension --alias vpxd-extension --cert new-vpxd-extension.crt --key vpxd-extension-key.priv
```

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

```
C:\>"C:\Program Files\VMware\vCenter Server\vmafdd\"vecs-cli entry delete --store vsphere-
webclient --alias vsphere-webclient
C:\>"C:\Program Files\VMware\vCenter Server\vmafdd\"vecs-cli entry create --store vsphere-
webclient --alias vsphere-webclient --cert new-vsphere-webclient.crt --key vsphere-webclient-
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 can run this command on a Platform Services Controller or a vCenter Server system.

```
C:\>"C:\Program Files\VMware\vCenter Server\vmafdd\"dir-cli>dir-cli service list
output:
1. machine-29a45d00-60a7-11e4-96ff-00505689639a
2. machine-6fd7f140-60a9-11e4-9e28-005056895a69
3. vpxd-6fd7f140-60a9-11e4-9e28-005056895a69
4. vpxd-extension-6fd7f140-60a9-11e4-9e28-005056895a69
5. vsphere-webclient-6fd7f140-60a9-11e4-9e28-005056895a69
```

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 the Platform Services Controller. For example, if machine-29a45d00-60a7-11e4-96ff-00505689639a is the machine solution user on the Platform Services Controller, run this command:

```
C:\>"C:\Program Files\VMware\vCenter Server\vmafdd\"dir-cli service update --name
machine-29a45d00-60a7-11e4-96ff-00505689639a --cert new-machine-1.crt
```

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

```
C:\>"C:\Program Files\VMware\vCenter Server\vmafdd\"dir-cli service update --name
machine-6fd7f140-60a9-11e4-9e28-005056895a69 --cert new-machine-2.crt
```

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

```
C:\>"C:\Program Files\VMware\vCenter Server\vmafdd\"dir-cli service update --name
vpxd-6fd7f140-60a9-11e4-9e28-005056895a69 --cert new-vpxd.crt
```

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

```
C:\>"C:\Program Files\VMware\vCenter Server\vmafdd\"dir-cli service update --name vpxd-
extension-6fd7f140-60a9-11e4-9e28-005056895a69 --cert new-vpxd-extension.crt
```

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

```
C:\>"C:\Program Files\VMware\vCenter Server\vmafdd\"dir-cli service update --name vsphere-
webclient-6fd7f140-60a9-11e4-9e28-005056895a69 --cert new-vsphere-webclient.crt
```

What to do next

Restart all services on each Platform Services Controller node and each management node.

Replace the VMware Directory Service Certificate in Mixed Mode Environments

During upgrade, your environment might temporarily include both vCenter Single Sign-On version 5.5 and vCenter Single Sign-On version 6.x. For that case, you have to perform additional steps to replace the VMware Directory Service SSL certificate if you replace the SSL certificate of the node on which the vCenter Single Sign-On service is running.

The VMware Directory Service SSL certificate is used by vmdir to perform handshakes between Platform Services Controller nodes that perform vCenter Single Sign-On replication.

These steps are not required for a mixed mode environment that includes vSphere 6.0 and vSphere 6.5 nodes. These steps are required only if:

- Your environment includes both vCenter Single Sign-On 5.5 and vCenter Single Sign-On 6.x services.
- The vCenter Single Sign-On services are set up to replicate vmdir data.
- You plan to replace the default VMCA-signed certificates with custom certificates for the node on which the vCenter Single Sign-On 6.x service runs.

Note Upgrading the complete environment before restarting the services is best practice. Replacing the VMware Directory Service certificate is not usually recommended.

Procedure

1. On the node on which the vCenter Single Sign-On 5.5 service runs, set up the environment so the vCenter Single Sign-On 6.x service is known.
   a. Back up all files `C:\ProgramData\VMware\CIS\cfg\vmdird`.
   b. Make a copy of the `vmdircert.pem` file on the 6.x node, and rename it to `<sso_node2.domain.com>.pem`, where `<sso_node2.domain.com>` is the FQDN of the 6.x node.
   c. Copy the renamed certificate to `C:\ProgramData\VMware\CIS\cfg\vmdird` to replace the existing replication certificate.
2. Restart the VMware Directory Service on all machines where you replaced certificates.

   You can restart the service from the vSphere Web Client or use the `service-control` command.

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.

Procedure

1. Replace the Root Certificate (Intermediate CA)

   The first step in replacing the VMCA certificates with custom certificates is generating a CSR, sending the CSR to be signed. You then add the signed certificate to VMCA as a root certificate.
2. 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.
3. Replace Solution User Certificates (Intermediate CA)

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

4 Replace the VMware Directory Service Certificate in Mixed Mode Environments

During upgrade, your environment might temporarily include both vCenter Single Sign-On version 5.5 and vCenter Single Sign-On version 6.x. For that case, you have to perform additional steps to replace the VMware Directory Service SSL certificate if you replace the SSL certificate of the node on which the vCenter Single Sign-On service is running.

Replace the Root Certificate (Intermediate CA)

The first step in replacing the VMCA certificates with custom certificates is generating a CSR, 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 or more
- PEM format. VMware supports PKCS8 and PKCS1 (RSA keys). When keys are added to VECS, they are converted to PKCS8
- x509 version 3
- If you are using custom certificates, the CA extension must be set to true for root certificates, and cert sign must be in the list of requirements.
- CRL signing must be enabled.
- Enhanced Key Usage must not contain Client Authentication or 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 VMware Knowledge Base Article 2112009, Creating a Microsoft Certificate Authority Template for SSL certificate creation in vSphere 6.0, for an example using Microsoft Certificate Authority.

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

- Key size 2048 bits or more
- 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 along with the full CA chain of your third-party CA or enterprise CA. Save the file, for example as `rootca1.crt`.

You can accomplish this 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.

The service names differ on Windows and the vCenter Server Appliance.

Windows

```
service-control --stop --all
service-control --start VMWareAfdService
service-control --start VMWareDirectoryService
service-control --start VMWareCertificateService
```

vCenter Server Appliance

```
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:

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

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.

```
C:\>"C:\Program Files\VMware\vCenter Server\vmcad\certool" --rootca --cert=C:\custom-certs\root.pem --
privkey=C:\custom-certs\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 company policy requires it. If you do, you have to replace the vCenter Single Sign-On Signing certificate. See Refresh the Security Token Service Certificate

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. In a multi-node deployment, you must run the Machine SSL certificate generation commands on each node. Use the `--server` parameter to point to the Platform Services Controller from a vCenter Server with external Platform Services Controller.

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.

You can find `certool.cfg` in the following locations:

Windows	`C:\Program Files\VMware\vCenter Server\vmcad`
Linux	`/usr/lib/vmware-vmca/share/config/`

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

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.

The service names differ on Windows and the vCenter Server Appliance.

Windows

```
service-control --stop --all
service-control --start VMWareAfdService
service-control --start VMWareDirectoryService
service-control --start VMWareCertificateService
```

vCenter Server Appliance

```
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-<PSC-FQDN-example>
Organization = VMware
OrgUnit = VMware Engineering
State = California
Locality = Palo Alto
Hostname = <FQDN>
```

2 Generate a key pair for the machine SSL certificate. Run this command on each management node and Platform Services Controller node; it does not require a `--server` option.

```
C:\>"C:\Program Files\VMware\vCenter Server\vmcad\"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.

- On a Platform Services Controller node or embedded installation:

```
C:\>"C:\Program Files\VMware\vCenter Server\vmcad\"certool --gencert --cert=new-vmca-ssl.crt --
privkey=ssl-key.priv --config=ssl-config.cfg
```

- On a vCenter Server (external installation):

```
C:\>"C:\Program Files\VMware\vCenter Server\vmcad\"certool --gencert --cert=new-vmca-ssl.crt --
privkey=ssl-key.priv --config=ssl-config.cfg --server=<psc-ip-or-fqdn>
```

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

4 (Optional) List the content of VECS.

```
"C:\Program Files\VMware\vCenter Server\vmafdd\" vecs-cli store list
```

- Sample output on Platform Services Controller:

```
MACHINE_SSL_CERT
TRUSTED_ROOTS
TRUSTED_ROOT_CRLS
machine
```

- Sample output on vCenter Server:

```
output (on vCenter):
MACHINE_SSL_CERT
TRUSTED_ROOTS
TRUSTED_ROOT_CRLS
machine
vpxd
vpxd-extension
vsphere-webclient
sms
```

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 the Platform Services Controller, run the following command to update the Machine SSL certificate in the MACHINE_SSL_CERT store.

```
C:\>"C:\Program Files\VMware\vCenter Server\vmafdd\"vecs-cli entry delete --store
MACHINE_SSL_CERT --alias __MACHINE_CERT
C:\>"C:\Program Files\VMware\vCenter Server\vmafdd\"vecs-cli entry create --store
MACHINE_SSL_CERT --alias __MACHINE_CERT --cert new-vmca-ssl.crt --key ssl-key.priv
```

- On each management node or embedded deployment, run the following command 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.

```
C:\>"C:\Program Files\VMware\vCenter Server\vmafdd\"vecs-cli entry delete --store
MACHINE_SSL_CERT --alias __MACHINE_CERT
C:\>"C:\Program Files\VMware\vCenter Server\vmafdd\"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 on each management node and on each Platform Services Controller node. You replace the other solution user certificates only on each management node. Use the `--server` parameter to point to the Platform Services Controller when you run commands on a management node with an external Platform Services Controller.

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.

   ```
   C:\Program Files\VMware\vCenter Server\vmafdd>dir-cli service list
   Enter password for administrator@vsphere.local:
   1. machine-1d364500-4b45-11e4-96c2-020011c98db3
   2. vpxd-1d364500-4b45-11e4-96c2-020011c98db3
   3. vpxd-extension-1d364500-4b45-11e4-96c2-020011c98db3
   4. vsphere-webclient-1d364500-4b45-11e4-96c2-020011c98db3
   ```

   When you list solution user certificates in multi-node 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.

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

The service names differ on Windows and the vCenter Server Appliance.

Windows

```
service-control --stop --all
service-control --start VMWareAfdService
service-control --start VMWareDirectoryService
service-control --start VMWareCertificateService
```

vCenter Server Appliance

```
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 don't 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. That includes a pair for the machine solution user on each Platform Services Controller and each management node and a pair for each additional solution user (vpxd, vpxd-extension, vsphere-webclient) on each management node.

a Generate a key pair for the machine solution user of an embedded deployment or for the machine solution user of the Platform Services Controller.

```
C:\>"C:\Program Files\VMware\vCenter Server\vmcad\"certool --genkey --privkey=machine-key.priv
--pubkey=machine-key.pub
```

b (Optional) For deployments with an external Platform Services Controller, generate a key pair for the machine solution user on each management node.

```
C:\>"C:\Program Files\VMware\vCenter Server\vmcad\"certool --genkey --privkey=machine-key.priv
--pubkey=machine-key.pub
```

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

```
C:\>"C:\Program Files\VMware\vCenter Server\vmcad\"certool --genkey --privkey=vpxd-key.priv --
pubkey=vpxd-key.pub
```

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

```
C:\>"C:\Program Files\VMware\vCenter Server\vmcad\"certool --genkey --privkey=vpxd-extension-
key.priv --pubkey=vpxd-extension-key.pub
```

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

```
C:\>"C:\Program Files\VMware\vCenter Server\vmcad\"certool --genkey --privkey=vsphere-
webclient-key.priv --pubkey=vsphere-webclient-key.pub
```

2 Generate solution user certificates that are signed by the new VMCA root certificate for the machine solution user on each Platform Services Controller and each management node and for each additional solution user (vpxd, vpxd-extension, vsphere-webclient) on each management 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 on the Platform Services Controller node to generate a solution user certificate for the machine solution user on that node.

```
C:\>"C:\Program Files\VMware\vCenter Server\vmcad\"certool --gencert --cert=new-machine.crt --
privkey=machine-key.priv --Name=machine
```

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

```
C:\>"C:\Program Files\VMware\vCenter Server\vmcad\"certool --gencert --cert=new-machine.crt --
privkey=machine-key.priv --Name=machine --server=<psc-ip-or-fqdn>
```

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

```
C:\>"C:\Program Files\VMware\vCenter Server\vmcad\"certool --gencert --cert=new-vpxd.crt --
privkey=vpxd-key.priv --Name=vpxd --server=<psc-ip-or-fqdn>
```

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

```
C:\>"C:\Program Files\VMware\vCenter Server\vmcad\"certool --gencert --cert=new-vpxd-
extension.crt --privkey=vpxd-extension-key.priv --Name=vpxd-extension --server=<psc-ip-or-fqdn>
```

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

```
C:\>"C:\Program Files\VMware\vCenter Server\vmcad\"certool --gencert --cert=new-vsphere-webclient.crt --privkey=vsphere-webclient-key.priv --Name=vsphere-webclient --server=<psc-ip-or-fqdn>
```

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 On the Platform Services Controller node, run the following command to replace the machine solution user certificate:

```
C:\>"C:\Program Files\VMware\vCenter Server\vmafdd\"vecs-cli entry delete --store machine --alias machine
C:\>"C:\Program Files\VMware\vCenter Server\vmafdd\"vecs-cli entry create --store machine --alias machine --cert new-machine.crt --key machine-key.priv
```

b Replace the machine solution user certificate on each management node:

```
C:\>"C:\Program Files\VMware\vCenter Server\vmafdd\"vecs-cli entry delete --store machine --alias machine
C:\>"C:\Program Files\VMware\vCenter Server\vmafdd\"vecs-cli entry create --store machine --alias machine --cert new-machine-vc.crt --key machine-vc-key.priv
```

c Replace the vpxd solution user certificate on each management node.

```
C:\>"C:\Program Files\VMware\vCenter Server\vmafdd\"vecs-cli entry delete --store vpxd --alias vpxd
C:\>"C:\Program Files\VMware\vCenter Server\vmafdd\"vecs-cli entry create --store vpxd --alias vpxd --cert new-vpxd.crt --key vpxd-key.priv
```

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

```
C:\>"C:\Program Files\VMware\vCenter Server\vmafdd\"vecs-cli entry delete --store vpxd-extension --alias vpxd-extension
C:\>"C:\Program Files\VMware\vCenter Server\vmafdd\"vecs-cli entry create --store vpxd-extension --alias vpxd-extension --cert new-vpxd-extension.crt --key vpxd-extension-key.priv
```

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

```
C:\>"C:\Program Files\VMware\vCenter Server\vmafdd\"vecs-cli entry delete --store vsphere-webclient --alias vsphere-webclient
C:\>"C:\Program Files\VMware\vCenter Server\vmafdd\"vecs-cli entry create --store vsphere-webclient --alias vsphere-webclient --cert new-vsphere-webclient.crt --key vsphere-webclient-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 can run this command on a Platform Services Controller or a vCenter Server system.

```
C:\>"C:\Program Files\VMware\vCenter Server\vmafdd\"dir-cli>dir-cli service list
output:
1. machine-29a45d00-60a7-11e4-96ff-00505689639a
2. machine-6fd7f140-60a9-11e4-9e28-005056895a69
3. vpxd-6fd7f140-60a9-11e4-9e28-005056895a69
4. vpxd-extension-6fd7f140-60a9-11e4-9e28-005056895a69
5. vsphere-webclient-6fd7f140-60a9-11e4-9e28-005056895a69
```

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 the Platform Services Controller. For example, if machine-29a45d00-60a7-11e4-96ff-00505689639a is the machine solution user on the Platform Services Controller, run this command:

```
C:\>"C:\Program Files\VMware\vCenter Server\vmafdd\"dir-cli service update --name
machine-29a45d00-60a7-11e4-96ff-00505689639a --cert new-machine-1.crt
```

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

```
C:\>"C:\Program Files\VMware\vCenter Server\vmafdd\"dir-cli service update --name
machine-6fd7f140-60a9-11e4-9e28-005056895a69 --cert new-machine-2.crt
```

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

```
C:\>"C:\Program Files\VMware\vCenter Server\vmafdd\"dir-cli service update --name
vpxd-6fd7f140-60a9-11e4-9e28-005056895a69 --cert new-vpxd.crt
```

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

```
C:\>"C:\Program Files\VMware\vCenter Server\vmafdd\"dir-cli service update --name vpxd-
extension-6fd7f140-60a9-11e4-9e28-005056895a69 --cert new-vpxd-extension.crt
```

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

```
C:\>"C:\Program Files\VMware\vCenter Server\vmafdd\"dir-cli service update --name vsphere-
webclient-6fd7f140-60a9-11e4-9e28-005056895a69 --cert new-vsphere-webclient.crt
```

Replace the VMware Directory Service Certificate in Mixed Mode Environments

During upgrade, your environment might temporarily include both vCenter Single Sign-On version 5.5 and vCenter Single Sign-On version 6.x. For that case, you have to perform additional steps to replace the VMware Directory Service SSL certificate if you replace the SSL certificate of the node on which the vCenter Single Sign-On service is running.

The VMware Directory Service SSL certificate is used by vmdir to perform handshakes between Platform Services Controller nodes that perform vCenter Single Sign-On replication.

These steps are not required for a mixed mode environment that includes vSphere 6.0 and vSphere 6.5 nodes. These steps are required only if:

- Your environment includes both vCenter Single Sign-On 5.5 and vCenter Single Sign-On 6.x services.
- The vCenter Single Sign-On services are set up to replicate vmdir data.
- You plan to replace the default VMCA-signed certificates with custom certificates for the node on which the vCenter Single Sign-On 6.x service runs.

Note Upgrading the complete environment before restarting the services is best practice. Replacing the VMware Directory Service certificate is not usually recommended.

Procedure

1 On the node on which the vCenter Single Sign-On 5.5 service runs, set up the environment so the vCenter Single Sign-On 6.x service is known.

   a Back up all files `C:\ProgramData\VMware\CIS\cfg\vmdird`.

   b Make a copy of the `vmdircert.pem` file on the 6.x node, and rename it to `<sso_node2.domain.com>.pem`, where `<sso_node2.domain.com>` is the FQDN of the 6.x node.

   c Copy the renamed certificate to `C:\ProgramData\VMware\CIS\cfg\vmdird` to replace the existing replication certificate.

2 Restart the VMware Directory Service on all machines where you replaced certificates.

   You can restart the service from the vSphere Web Client or use the `service-control` command.

Use Custom Certificates With vSphere

If 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.

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 keeping track of 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 VMware Knowledge Base Article 2000888.

Procedure

1 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 CA and importing the root certificates into VECS.

2 Replace Machine SSL Certificates With Custom Certificates

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

3 Replace Solution User Certificates With Custom Certificates

   After you replace the machine SSL certificates, you can replace the VMCA-signed solution user certificates with third-party or enterprise certificates.

4 Replace the VMware Directory Service Certificate in Mixed Mode Environments

   During upgrade, your environment might temporarily include both vCenter Single Sign-On version 5.5 and vCenter Single Sign-On version 6.x. For that case, you have to perform additional steps to replace the VMware Directory Service SSL certificate if you replace the SSL certificate of the node on which the vCenter Single Sign-On service is running.

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 CA and importing the root certificates into VECS.

Prerequisites

The certificate must meet the following requirements:

- Key size: 2048 bits or more (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, Non Repudiation, 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 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, four solution user certificates for each embedded system or management node. Solution user certificates should not include IP address, host name, or email address. Each certificate must have a different certificate Subject.
   - Optionally, a machine solution user certificate for external Platform Services Controller instances. This certificate differs from the machine SSL certificate for the Platform Services Controller.

   Typically, the result is a PEM file for the trusted chain, plus the signed SSL certificates for each Platform Services Controller or management node.
2. List the TRUSTED_ROOTS and 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 a HTTPS connection to a node where the certificate will be replaced, check 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.

The service names differ on Windows and the vCenter Server Appliance.

Windows

```
service-control --stop --all
service-control --start VMWareAfdService
service-control --start VMWareDirectoryService
service-control --start VMWareCertificateService
```

vCenter Server Appliance

```
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 company policy requires it. If you do, you have to refresh the vCenter Single Sign-On certificate. See Refresh the Security Token Service Certificate.

Replace Machine SSL Certificates With Custom Certificates

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

Each machine must have a machine SSL certificate for secure communication with other services. In a multi-node deployment, you must run the Machine SSL certificate generation commands on each node. Use the `--server` parameter to point to the Platform Services Controller from a vCenter Server with external Platform Services Controller.

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).
- If you are running the command on a vCenter Server with external Platform Services Controller in a multi-node deployment, IP address of the Platform Services Controller.

Prerequisites

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

- Key size: 2048 bits or more (PEM encoded)
- CRT format
- x509 version 3
- SubjectAltName must contain DNS Name=<machine_FQDN>
- Contains the following Key Usages: Digital Signature, Non Repudiation, Key Encipherment

Procedure

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

The service names differ on Windows and the vCenter Server Appliance.

Windows

```
service-control --stop --all
service-control --start VMWareAfdService
service-control --start VMWareDirectoryService
service-control --start VMWareCertificateService
```

vCenter Server Appliance

```
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 Restart all services.

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

Example: Replace Machine SSL Certificates with Custom Certificates

You can replace the machine SSL certificate on each node the same way.

1 First, delete the existing certificate in VECS.

```
"C:\Program Files\VMware\vCenter Server\vmafdd\"vecs-cli entry delete --store MACHINE_SSL_CERT --
alias __MACHINE_CERT
```

2 Next, add the replacement certificate.

```
"C:\Program Files\VMware\vCenter Server\vmafdd\"vecs-cli entry create --store MACHINE_SSL_CERT --
alias __MACHINE_CERT --cert E:\custom-certs\ms-ca\signed-ssl\custom-w1-vim-cat-
dhcp-094.eng.vmware.com.crt --key E:\custom-certs\ms-ca\signed-ssl\custom-x3-vim-cat-
dhcp-1128.vmware.com.priv
```

Replace Solution User Certificates With Custom Certificates

After you replace the machine SSL certificates, you can replace the VMCA-signed solution user certificates with third-party or enterprise 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.

Solution users use certificates only to authenticate to vCenter Single Sign-On. If the certificate is valid, vCenter Single Sign-On assigns a SAML token to the solution user, and the solution user uses the SAML token to authenticate to other vCenter components.

You replace the machine solution user certificate on each management node and on each Platform Services Controller node. You replace the other solution user certificates only on each management node. Use the `--server` parameter to point to the Platform Services Controller when you run commands on a management node with an external Platform Services Controller.

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

- Key size: 2048 bits or more (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, Non Repudiation, 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 vmca
```

2 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.

```
C:\Program Files\VMware\vCenter Server\vmafdd>dir-cli service list
Enter password for administrator@vsphere.local:
1. machine-1d364500-4b45-11e4-96c2-020011c98db3
2. vpxd-1d364500-4b45-11e4-96c2-020011c98db3
3. vpxd-extension-1d364500-4b45-11e4-96c2-020011c98db3
4. vsphere-webclient-1d364500-4b45-11e4-96c2-020011c98db3
```

When you list solution user certificates in multi-node 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.

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

You must add the certificates in that order.

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

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

4 Restart all services.

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

Replace the VMware Directory Service Certificate in Mixed Mode Environments

During upgrade, your environment might temporarily include both vCenter Single Sign-On version 5.5 and vCenter Single Sign-On version 6.x. For that case, you have to perform additional steps to replace the VMware Directory Service SSL certificate if you replace the SSL certificate of the node on which the vCenter Single Sign-On service is running.

The VMware Directory Service SSL certificate is used by vmdir to perform handshakes between Platform Services Controller nodes that perform vCenter Single Sign-On replication.

These steps are not required for a mixed mode environment that includes vSphere 6.0 and vSphere 6.5 nodes. These steps are required only if:

- Your environment includes both vCenter Single Sign-On 5.5 and vCenter Single Sign-On 6.x services.
- The vCenter Single Sign-On services are set up to replicate vmdir data.
- You plan to replace the default VMCA-signed certificates with custom certificates for the node on which the vCenter Single Sign-On 6.x service runs.

Note Upgrading the complete environment before restarting the services is best practice. Replacing the VMware Directory Service certificate is not usually recommended.

Procedure

1. On the node on which the vCenter Single Sign-On 5.5 service runs, set up the environment so the vCenter Single Sign-On 6.x service is known.
   a. Back up all files `C:\ProgramData\VMware\CIS\cfg\vmdird`.
   b. Make a copy of the `vmdircert.pem` file on the 6.x node, and rename it to `<sso_node2.domain.com>.pem`, where `<sso_node2.domain.com>` is the FQDN of the 6.x node.
   c. Copy the renamed certificate to `C:\ProgramData\VMware\CIS\cfg\vmdird` to replace the existing replication certificate.
2. Restart the VMware Directory Service on all machines where you replaced certificates.

   You can restart the service from the vSphere Web Client or use the `service-control` command.

Managing Services and Certificates With CLI Commands

4

A set of CLIs allows you to manage VMCA (VMware Certificate Authority), VECS (VMware Endpoint Certificate Store), and VMware Directory Service (vmdir). 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.

Table 4-1. 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 VMAFD.	vecs-cli Command Reference
`dir-cli`	Create and update certificates in VMware Directory Service. Part of VMAFD.	dir-cli Command Reference
`sso-config`	Some vCenter Single Sign-On configuration. In most cases, using the Platform Services Controller Web interface is recommended. Use this command for two-factor authentication setup.	Command-line help. vCenter Server Two-Factor Authentication
`service-control`	Start or stop services, for example as part of a certificate replacement workflow	

CLI Locations

By default, you find the CLIs in the following locations on each node.

Windows

```
C:\Program Files\VMware\vCenter Server\vmafdd\vecs-cli.exe
C:\Program Files\VMware\vCenter Server\vmafdd\dir-cli.exe
C:\Program Files\VMware\vCenter Server\vmcad\certool.exe
C:\Program Files\VMware\VCenter server\VMware Identity Services\sso-config
```

	VCENTER_INSTALL_PATH\bin\service-control
Linux	/usr/lib/vmware-vmafd/bin/vecs-cli /usr/lib/vmware-vmafd/bin/dir-cli /usr/lib/vmware-vmca/bin/certool /opt/vmware/bin On Linux, the service-control command does not require that you specify the path.

If you run commands from a vCenter Server system with an external Platform Services Controller, you can specify the Platform Services Controller with the --server parameter.

This section includes the following topics:

- Required Privileges for Running CLIs
- Changing the certool Configuration Options
- certool Initialization Commands Reference
- certool Management Commands Reference
- vecs-cli Command Reference
- dir-cli Command Reference

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 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 on Windows and root users on Linux 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 at the following location by default.

OS	Location
Linux	/usr/lib/vmware-vmca/config
Windows	C:\Program Files\VMware\vCenter Server\vmcad\

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.
- ```
  certool --gencert --config C:\Temp\myconfig.cfg
  ```
- Override individual values on the command line. For example, to override Locality, run this command:

  ```
  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
`--initcsr`	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 --initcsr --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.
`--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 in conjunction 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.

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:

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

certool --getrootca

Prints the current root CA certificate in human-readable form. If you are running this command from a management node, use the machine name of the Platform Services Controller node to retrieve the root CA. 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 other Platform Services Controller 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 4-2. 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 embedded deployments and on each Platform Services Controller node. All services in vSphere 6.0 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.
Trusted root store (TRUSTED_ROOTS)	Contains all trusted root certificates.

Table 4-2. Stores in VECS (Continued)

Store	Description
Solution user stores ■ machine ■ vpxd ■ vpxd-extensions ■ vsphere-webclient	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. In an embedded deployment, all solution user certificates are on the same system. The following solution user certificate stores are included in VECS on each management node and each embedded deployment: ■ machine: Used by component manager, 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 on management nodes and embedded deployments. vpxd uses the solution user certificate that is stored in this store to authenticate to vCenter Single Sign-On. ■ vpxd-extensions: vCenter extensions store. Includes the Auto Deploy service, inventory service, and other services that are not part of other solution users. ■ vsphere-webclient: vSphere Web Client store. Also includes some additional services such as the performance chart service. Each Platform Services Controller node includes a machine certificate.
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.

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.

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-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.

Option	Description
`--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 also use `dir-cli` to manage and query the domain functional level of Platform Services Controller instances.

dir-cli nodes list

Lists all vCenter Server system for the specified Platform Services Controller instance.

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 if you do not want to target the affinitized Platform Services Controller. Specify the IP address or FQDN of the Platform Services Controller;

dir-cli domain-functional-level get

Retrieve the domain functional level for the specified Platform Services Controller.

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 if you do not want to target the affinitized Platform Services Controller. Specify the IP address or FQDN of the Platform Services Controller;
`--domain-name <domain_name>`	Optional name of the domain in which the Platform Services Controller is running.

dir-cli domain-functional-level set

Explicitly set the domain functional level for the specified Platform Services Controller. The domain functional level is set set automatically as part of installation. If you are upgrading your environment, run this command to set the level to 2. Run the command on one of the Platform Services Controller instances after all nodes are upgraded to vSphere 6.5.

Note You cannot change the domain functional level of a Platform Services Controller 6.0 or earlier instance to 2.

Option	Description
`--level <level>`	Level for the Platform Services Controller. Use 2 to explicitly set the level after an upgrade, for example, because you want to use Platform Services Controller high availability.
`--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 if you do not want to target the affinitized Platform Services Controller. Specify the IP address or FQDN of the Platform Services Controller;
`--domain-name <domain_name>`	Optional name of the domain in which the Platform Services Controller is running.

dir-cli list-domain-versions

Lists the domain functional level of each Platform Services Controller in the current domain or in the domain that is specified by `--domain-name <domain_name>`. Also lists the highest domain functional level that is possible that domain.

Run this command before you run `dir-cli domain-functional-level set` to make sure it is possible to change the DFL.

Option	Description
`--level <level>`	Level for the Platform Services Controller. Use 2 to explicitly set the level after an upgrade. Use 1 if you explicitly want to downgrade your environment, for example, because you want to use an external Platform Services Controller.
`--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 if you do not want to target the affinitized Platform Services Controller. Specify the IP address or FQDN of the Platform Services Controller;
`--domain-name <domain_name>`	Optional name of the domain in which the Platform Services Controller is running.

dir-cli computer password-reset

Enables you to reset the password of the machine account in the domain. This option is useful if you have to restore a Platform Services Controller instance.

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 Platform Services Controller 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>`	
`--wstrustrole <ActAsUser>`	
`--ssoadminrole <Administrator/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 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

Deletes the specified user inside vmdir.

Option	Description
`--account <name>`	Name of the vCenter Single Sign-On user to delete.
`--password-never-expires`	Set this option to true if you are creating a user account for automated tasks that have to authenticate to Platform Services Controller, 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.
`--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 already 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.

Troubleshooting Platform Services Controller 5

The following topics provide a starting point for troubleshooting Platform Services Controller. Search this documentation center and the VMware Knowledge Base system for additional pointers.

This section 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 Web 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 service (Windows) and vmware-sso daemon (Linux). Restart the service. If this 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 this 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 `%TEMP%\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 Web 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).

If you are using the vCenter Server Appliance, other problems might exist.

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 VMware Knowledge Base article 2070433. By default, Integrated Windows Authentication uses the root domain of your Active Directory forest.

If you are using the vCenter Server Appliance, and changing the default identity source does not resolve the issue, perform the following additional troubleshooting steps.

1 Synchronize the clocks between the vCenter Server Appliance 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 Appliance, 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 Appliance from the Active Directory domain and then rejoin the domain. See the *vCenter Server Appliance Configuration* documentation.

4 Close all browser sessions connected to the vCenter Server Appliance 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 Web Client login page, an error indicates that the account is locked.

Problem

After several failed attempts, you cannot log in to the vSphere Web 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 Platform Services Controller instances, and if one of the Platform Services Controller instances becomes unavailable, your environment continues to function. When the Platform Services Controller becomes available again, user data and other information are usually replicated within 60 seconds. In certain special circumstances, however, replication might take a long time.

Problem

In certain situations, for example, when your environment includes multiple Platform Services Controller instances in different locations, and you make significant changes while one Platform Services Controller 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 Platform Services Controller instance in the other instance until replication is complete.

Cause

During normal operation, changes to a VMware Directory Service (vmdir) instance in one Platform Services Controller instance (node) show up in its direct replication partner within about 60 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 Platform Services Controller Support Bundle

You can export a support bundle that contains the log files for the Platform Services Controller services. After the export, you can explore the logs locally or send the bundle to VMware Support.

Prerequisites

Verify that the Platform Services Controller virtual appliance is successfully deployed and running.

Procedure

1. From a Web browser, connect to the Platform Services Controller management interface at https://*platform_services_controller_ip*:5480
2. Log in as the root user for the virtual appliance.
3. Click **Create support bundle**.
4. Unless browser settings prevent an immediate download, the support bundle is saved to your local machine.

Platform Services Controller Service Logs Reference

The Platform Services Controller 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`.