vSphere Security

ESXi 6.0

vCenter Server 6.0

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

EN-001466-04

vmware®

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

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

The VMware Web site also provides the latest product updates.

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

docfeedback@vmware.com

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

Contents

About vSphere Security 7

Updated Information 9

1 Security in the vSphere Environment 11
- Securing the ESXi Hypervisor 11
- Securing vCenter Server Systems and Associated Services 13
- Securing Virtual Machines 14
- Securing the Virtual Networking Layer 15
- Passwords in Your vSphere Environment 16
- Security Best Practices and Resources 17

2 vSphere Authentication with vCenter Single Sign-On 19
- Understanding vCenter Single Sign-On 20
- Configuring vCenter Single Sign-On Identity Sources 29
- Managing the Security Token Service (STS) 35
- Managing vCenter Single Sign-On Policies 38
- Managing vCenter Single Sign-On Users and Groups 40
- vCenter Single Sign-On Security Best Practices 46
- Troubleshooting vCenter Single Sign-On 46

3 vSphere Security Certificates 51
- Certificate Management Overview 52
- Certificate Replacement Overview 53
- Managing Certificates in vSphere 6 56
- Using the vSphere Certificate Manager Utility 63
- Generate Certificate Signing Requests with vSphere Certificate Manager 69
- Manual Certificate Replacement 69
- Managing Certificates and Services with CLI Commands 96
- View vCenter Certificates with the vSphere Web Client 111
- Set the Threshold for vCenter Certificate Expiration Warnings 111

4 vSphere Permissions and User Management Tasks 113
- Understanding Authorization in vSphere 114
- Understanding the vCenter Server Permission Model 114
- Hierarchical Inheritance of Permissions 116
- Multiple Permission Settings 117
- Managing Permissions for vCenter Components 119
- Global Permissions 122
- Add a Global Permission 123
- Using Roles to Assign Privileges 123

Best Practices for Roles and Permissions 127
Required Privileges for Common Tasks 127

5 Securing ESXi Hosts 131
Use Scripts to Manage Host Configuration Settings 132
Configure ESXi Hosts with Host Profiles 133
General ESXi Security Recommendations 133
Certificate Management for ESXi Hosts 137
Customizing Hosts with the Security Profile 150
Assigning Permissions for ESXi 164
Using Active Directory to Manage ESXi Users 166
Using vSphere Authentication Proxy 169
Configuring Smart Card Authentication for ESXi 173
ESXi SSH Keys 175
Using the ESXi Shell 177
Modifying ESXi Web Proxy Settings 181
vSphere Auto Deploy Security Considerations 182
Managing ESXi Log Files 182
ESXi Security Best Practices 185

6 Securing vCenter Server Systems 187
vCenter Server Security Best Practices 187
Verify Thumbprints for Legacy ESXi Hosts 191
Verify that SSL Certificate Validation Over Network File Copy Is Enabled 192
vCenter Server TCP and UDP Ports 192
Control CIM-Based Hardware Monitoring Tool Access 193

7 Securing Virtual Machines 195
Limit Informational Messages from Virtual Machines to VMX Files 195
Prevent Virtual Disk Shrinking 196
Virtual Machine Security Best Practices 196

8 Securing vSphere Networking 205
Introduction to vSphere Network Security 205
Securing the Network with Firewalls 206
Secure the Physical Switch 210
Securing Standard Switch Ports With Security Policies 210
Securing vSphere Standard Switches 211
Secure vSphere Distributed Switches and Distributed Port Groups 212
Securing Virtual Machines with VLANs 213
Creating a Network DMZ on a Single ESXi Host 215
Creating Multiple Networks Within a Single ESXi Host 216
Internet Protocol Security 218
Ensure Proper SNMP Configuration 221
Use Virtual Switches with the vSphere Network Appliance API Only If Required 222
vSphere Networking Security Best Practices 222

9 Best Practices Involving Multiple vSphere Components 225
Synchronizing Clocks on the vSphere Network 225
Storage Security Best Practices 228
Verify That Sending Host Performance Data to Guests is Disabled 230
Setting Timeouts for the ESXi Shell and vSphere Web Client 230

10 Defined Privileges 233
Alarms Privileges 234
Auto Deploy and Image Profile Privileges 235
Certificates Privileges 235
Content Library Privileges 236
Datastore Privileges 237
Datastore Cluster Privileges 238
Distributed Switch Privileges 238
ESX Agent Manager Privileges 239
Extension Privileges 239
Folder Privileges 239
Global Privileges 240
Host CIM Privileges 240
Host Configuration Privileges 241
Host Inventory 242
Host Local Operations Privileges 242
Host vSphere Replication Privileges 243
Host Profile Privileges 243
Inventory Service Provider Privileges 244
Inventory Service Tagging Privileges 244
Network Privileges 245
Performance Privileges 245
Permissions Privileges 245
Profile-driven Storage Privileges 246
Resource Privileges 246
Scheduled Task Privileges 247
Sessions Privileges 247
Storage Views Privileges 248
Tasks Privileges 248
Transfer Service Privileges 248
VRM Policy Privileges 248
Virtual Machine Configuration Privileges 248
Virtual Machine Guest Operations Privileges 250
Virtual Machine Interaction Privileges 251
Virtual Machine Inventory Privileges 253
Virtual Machine Provisioning Privileges 253
Virtual Machine Service Configuration Privileges 255
Virtual Machine Snapshot Management Privileges 255
Virtual Machine vSphere Replication Privileges 256
dvPort Group Privileges 256
vApp Privileges 257
vServices Privileges 258

Index 259

About vSphere Security

vSphere Security provides information about securing your vSphere® environment for VMware® vCenter® Server and VMware ESXi.

To help you protect your vSphere environment, this documentation describes available security features and the measures that you can take to safeguard your environment from attack.

In addition to this document, 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. This *vSphere Security* document does not include information for Risk Profile 1 (highest security environment such as top-secret government).

Intended Audience

This information is for experienced Windows or Linux system administrators who are familiar with virtual machine technology and data center operations.

Updated Information

This *vSphere Security* documentation is updated with each release of the product or when necessary.

This table provides the update history of the *vSphere Security* documentation.

Revision	Description
EN-001466-04	Added pointer to KB article that explains use of script in deployments with external solutions to "Certificate Replacement in Large Deployments," on page 61.
EN-001466-03	■ Added some ports to "vCenter Server TCP and UDP Ports," on page 192. ■ Details and corrections for "Configuring Time Synchronization Settings in the vCenter Server Appliance," on page 226. ■ Added "PCI and PCIe Devices and ESXi," on page 185. ■ Added note that you should not delete groups in the vsphere.local domain to "Groups in the vsphere.local Domain," on page 27. ■ Clarified that the Certificate Manager utility requires keys in PEM format in the topics in the section "Using the vSphere Certificate Manager Utility," on page 63. ■ Updated "Use Custom Certificates with Auto Deploy," on page 148 to use **`custom`** instead of **`Custom`**.
EN-001466-02	■ Added additional recommendation to "General Networking Security Recommendations," on page 222 ■ Added VLAN ID recommendations to "Secure vSphere Distributed Switches and Distributed Port Groups," on page 212. ■ Added information about verifying trunk links to "Document and Check the vSphere VLAN Environment," on page 223. ■ Updated "Add Members to a vCenter Single Sign-On Group," on page 44. Groups are not displayed in the **Groups** tab. ■ Added information on stopping and starting service on Windows to "Replace the VMware Directory Service Certificate," on page 88. ■ Updated "Storage Views Privileges," on page 248. Storage Views are deprecated in vSphere 6.0. These privileges now control only access to the Storage Monitoring Services APIs.

Revision	Description
EN-001466-01	■ Updated the following topics to include instructions to select option 2 for certificate replacement. ■ "Replace Machine SSL Certificate with Custom Certificate," on page 64 ■ "Replace VMCA Root Certificate with Custom Signing Certificate and Replace All Certificates," on page 65 ■ "Replace Solution User Certificates with Custom Certificates," on page 67 ■ Added new topic "Generate Certificate Signing Requests with vSphere Certificate Manager," on page 69 ■ Fixed a technical inaccuracy in "Ensure Proper SNMP Configuration," on page 221. ■ Some clarifications in "ESXi Passwords, ESXi Pass Phrases, and Account Lockout," on page 135. ■ In "Replace the Root Certificate (Intermediate CA)," on page 80, changed `service-control --start vmca` to `service-control --start vmcad`. ■ Changed first step in "Change Certificate Default Settings," on page 142. This task is performed on the vCenter Server system, not on individual hosts. ■ Updated "vCenter Server TCP and UDP Ports," on page 192. Ports 11711 and 11712 are used only if vCenter Single Sign-On was upgraded from vSphere 5.5. In vSphere 6.0, vCenter Single Sign-On uses port 389 (LDAP) and 636 (LDAPS). ■ Updated "Use VMCA as an Intermediate Certificate Authority," on page 80. Replacing the VMCA before installing or upgrading other components in an environment with an external Platform Services Controller is no longer recommended.
EN-001466-00	Initial release.

1 Security in the vSphere Environment

The components of a vSphere environment are secured out of the box by a number of features such as certificates, authorization, a firewall on each ESXi, limited access, and so on. You can modify the default setup in many ways - for example, you can set permissions on vCenter objects, open firewall ports, or change the default certificates. This results in maximum flexibility in securing vCenter Server systems, ESXi hosts, and virtual machines.

A high level overview of different areas of vSphere that require attention helps you plan your security strategy. You also benefit from additional vSphere Security resources on the VMware website.

This chapter includes the following topics:

- "Securing the ESXi Hypervisor," on page 11
- "Securing vCenter Server Systems and Associated Services," on page 13
- "Securing Virtual Machines," on page 14
- "Securing the Virtual Networking Layer," on page 15
- "Passwords in Your vSphere Environment," on page 16
- "Security Best Practices and Resources," on page 17

Securing the ESXi Hypervisor

The ESXi hypervisor is secured out of the box. You can further protect ESXi hosts by using lockdown mode, and other built-in features. If you set up a reference host and make changes to all hosts based on that host's host profiles, or if you perform scripted management, you further protect your environment by assuring changes apply to all hosts.

Use the following features, discussed in detail in this guide, to enhance protection of ESXi hosts that are managed by vCenter Server. See also the *Security of the VMware vSphere Hypervisor* white paper.

Limit ESXi Access By default, the ESXi Shell and SSH services are not running and only the root user can log in to the Direct Console User Interface (DCUI). If you decide to enable ESXi or SSH access, you can set timeouts to limit the risk of unauthorized access.

	Users who can access the ESXi host must have permissions to manage the host. You set permissions on the host object from vCenter Server that manages the host.
Use Named Users and Least Privilege	Many tasks can be performed by the root user by default. Instead of allowing administrators to log in to the ESXi host using the root user account, you can apply different host configuration privileges to different named users from the vCenter Server permissions management interface. You can create a custom roles, assign privileges to the role, and associate the role with a named user and an ESXi host object from the vSphere Web Client. In a single host scenario, you manage users directly. See the *vSphere Single Host Management* documentation.
Minimize the Number of Open ESXi Firewall Ports	By default, firewall ports on your ESXi host are opened only when you start a corresponding service. You can use the vSphere Web Client or ESXCLI or PowerCLI commands to check and manage firewall port status. See "ESXi Firewall Configuration," on page 150.
Automate ESXi Host Management	Because it is often important that different hosts in the same data center are in sync, use scripted installation or vSphere Auto Deploy to provision hosts. You can manage the hosts using scripts. An alternative to scripted management are host profiles. You set up a reference host, export the host profile, and apply the host profile to your host. You can apply the host profile directly or as part of provisioning with Auto Deploy. See "Use Scripts to Manage Host Configuration Settings," on page 132 and see the *vSphere Installation and Setup* for information about vSphere Auto Deploy.
Take Advantage of Lockdown Mode	In lockdown mode, ESXi hosts can be accessed only through vCenter Server by default. Starting with vSphere 6.0, you can select strict lockdown mode or normal lockdown mode, and you can define Exception Users to allow direct access to service accounts such as backup agents. See "Lockdown Mode," on page 157.
Check VIB Package Integrity	Each VIB package has an associated acceptance level. You can add a VIB to an ESXi host only if the acceptance level is the same or better than the acceptance level of the host. You cannot add a CommunitySupported or PartnerSupported VIB to a host unless you explicitly change the host's acceptance level. See "Check the Acceptance Levels of Hosts and VIBs," on page 163.
Manage ESXi Certificates	In vSphere 6.0 and later, the VMware Certificate Authority (VMCA) provisions each ESXi host with a signed certificate that has VMCA as the root certificate authority by default. If company policy requires it, you can replace the existing certificates with certificates that are signed by a third-party CA. See "Certificate Management for ESXi Hosts," on page 137
Smart Card Authentication	Starting with vSphere 6.0, ESXi supports smart card authentication as an option instead of user name and password authentication.

See "Configuring Smart Card Authentication for ESXi," on page 173.

ESXi Account Lockout

Starting with vSphere 6.0, account locking is supported for access through SSH and through the vSphere Web Services SDK. The Direct Console Interface (DCUI) and the ESXi Shell do not support account lockout. By default, a maximum of ten failed attempts is allowed before the account is locked. The account is unlocked after two minutes by default.

See "ESXi Passwords, ESXi Pass Phrases, and Account Lockout," on page 135.

Security considerations for standalone hosts are similar, though the management tasks might differ. See the *vSphere Single Host Management* documentation.

Securing vCenter Server Systems and Associated Services

Your vCenter Server system and associated services are protected by authentication through vCenter Single Sign-On and by authorization through the vCenter Server permissions model. You can modify the default behavior, and you can take additional steps to protect access to your environment.

As you protect your vSphere environment, consider that all services that are associated with the vCenter Server instances must be protected. In some environments, you might protect several vCenter Server instances and one or more Platform Services Controller instances.

Harden All vCenter Host Machines

The first step in protecting your vCenter environment is hardening each machine on which vCenter Server or an associated service runs. Similar considerations apply to a physical machine or a virtual machine. Always install the latest security patches for your operating system and follow industry standard best practices to protect the host machine.

Learn about the vCenter Certificate Model

By default, the VMware Certificate Authority provisions each ESXi host, each machine in the environment, and each solution user with a certificate signed by VMCA. The environment works out of the box, but if company policy requires it, you can change the default behavior. See Chapter 3, "vSphere Security Certificates," on page 51.

For additional protection, be sure to explicitly remove expired or revoked certificates and failed installations.

Configure vCenter Single Sign-On

vCenter Server and associated services are protected by the vCenter Single Sign-On authentication framework. When you first install the software, you specify a password for the administrator@vsphere.local user, and only that domain is available as an identity source. You can add other identity sources, either Active Directory or LDAP, and set a default identity source. Going forward, users who can authenticate to an identity source can view objects and perform tasks if they are authorized to do so. See Chapter 2, "vSphere Authentication with vCenter Single Sign-On," on page 19.

Assign Roles to Users or Groups

For better logging, associate each permission you give on an object with a named user or group and a predefined role or custom role. The vSphere 6.0 permissions model allows great flexibility through multiple ways of authorizing users or groups. See "Understanding Authorization in vSphere," on page 114 and "Required Privileges for Common Tasks," on page 127.

Be sure to restrict administrator privileges and the use of the administrator role. If possible, do not use the anonymous Administrator user.

Set up NTP

Set up NTP for each node in your environment. The certificate infrastructure requires an accurate time stamp and does not work correctly if the nodes are out of sync.

See "Synchronizing Clocks on the vSphere Network," on page 225.

Securing Virtual Machines

To secure your virtual machines, keep the guest operating systems patched and protect your environment just as you would protect a physical machine. Consider disabling unnecessary functionality, minimize the use of the virtual machine console, and follow other best practices.

Protect the Guest Operating System

To protect your guest operating system, make sure that it uses the most recent patches and, if appropriate, anti-spyware and anti-malware programs. See the documentation from your guest operating system vendor and, potentially, other information available in books or on the Internet.

Disable Unnecessary Functionality

Check that unnecessary functionality is disabled to minimize potential points of attack. Many of the features that are used infrequently are disabled by default. Remove unnecessary hardware and disable certain features such as HFSG or copy and paste between the virtual machine and a remote console.

See "Disable Unnecessary Functions Inside Virtual Machines," on page 199.

Use Templates and Scripted Management

Virtual machine templates allow you to set up the operating system so it meets your requirements, and to then create additional virtual machines with the same settings.

If you want to change settings after initial deployment, consider using scripts, for example, PowerCLI. This documentation explains many tasks by using the vSphere Web Client to better illustrate the process, but scripts help you keep your environment consistent. In large environments, you can group virtual machines into folders to optimize scripting.

See "Use Templates to Deploy Virtual Machines," on page 197. See *vSphere Virtual Machine Administration* for details.

Minimize Use of the Virtual Machine Console

The virtual machine console provides the same function for a virtual machine that a monitor on a physical server provides. Users with access to the virtual machine console have access to virtual machine power management and removable device connectivity controls, which might allow a malicious attack on a virtual machine.

Securing the Virtual Networking Layer

The virtual networking layer includes virtual network adapters, virtual switches, distributed virtual switches, and ports and port groups. ESXi relies on the virtual networking layer to support communications between virtual machines and their users. In addition, ESXi uses the virtual networking layer to communicate with iSCSI SANs, NAS storage, and so forth.

vSphere includes the full array of features necessary for a secure networking infrastructure. You can secure each element of the infrastructure, such as virtual switches, distributed virtual switches, virtual network adapters, and so on separately. In addition, consider the following guidelines, discussed in more detail in Chapter 8, "Securing vSphere Networking," on page 205.

Isolate Network Traffic

Isolation of network traffic is essential to a secure ESXi environment. Different networks require different access and level of isolation. A management network isolates client traffic, command-line interface (CLI) or API traffic, and third-party software traffic from normal traffic. This network should be accessible only by system, network, and security administrators.

See "ESXi Networking Security Recommendations," on page 136.

Use Firewalls to Secure Virtual Network Elements

You can open and close firewall ports and secure each element in the virtual network separately. Firewall rules associate services with corresponding firewalls and can open and close the ESXi firewall according to the status of the service.

See "ESXi Firewall Configuration," on page 150.

Consider Network Security Policies

Networking security policy provides protection of traffic against MAC address impersonation and unwanted port scanning. The security policy of a standard or distributed switch is implemented in Layer 2 (Data Link Layer) of the network protocol stack. The three elements of the security policy are promiscuous mode, MAC address changes, and forged transmits.

See the *vSphere Networking* documentation for instructions.

Secure Virtual Machine Networking

The methods you use to secure a virtual machine network depend on which guest operating system is installed, whether the virtual machines operate in a trusted environment, and a variety of other factors. Virtual switches and distributed virtual switches provide a substantial degree of protection when used with other common security practices, such as installing firewalls.

See Chapter 8, "Securing vSphere Networking," on page 205.

Consider VLANs to Protect Your Environment

ESXi supports IEEE 802.1q VLANs, which you can use to further protect the virtual machine network or storage configuration. VLANs let you segment a physical network so that two machines on the same physical network cannot send packets to or receive packets from each other unless they are on the same VLAN.

See "Securing Virtual Machines with VLANs," on page 213.

Secure Connections to Virtualized Storage

A virtual machine stores operating system files, program files, and other data on a virtual disk. Each virtual disk appears to the virtual machine as a SCSI drive that is connected to a SCSI controller. A virtual machine is isolated from storage details and cannot access the information about the LUN where its virtual disk resides.

The Virtual Machine File System (VMFS) is a distributed file system and volume manager that presents virtual volumes to the ESXi host. You are responsible for securing the connection to storage. For example, if you are using iSCSI storage, you can set up your environment to use CHAP and, if required by company policy, mutual CHAP by using the vSphere Web Client or CLIs.

See "Storage Security Best Practices," on page 228.

Evaluate the Use of IPSec

ESXi supports IPSec over IPv6. You cannot use IPSec over IPv4.

See "Internet Protocol Security," on page 218.

In addition, evaluate whether VMware NSX for vSphere is a good solution for securing the networking layer in your environment.

Passwords in Your vSphere Environment

Password restrictions, lockout, and expiration in your vSphere environment depend on the system that the user targets, who the user is, and how policies are set.

ESXi Passwords

ESXi password restrictions are determined by the Linux PAM module pam_passwdqc. See "ESXi Passwords, ESXi Pass Phrases, and Account Lockout," on page 135.

Passwords for vCenter Server and Other vCenter Services

vCenter Single Sign-On manages authentication for all users who log in to vCenter Server and other vCenter services. The password restrictions, lockout, and expiration depend on the user's domain and on who the user is.

administrator@vsphere.local

The password for administrator@vsphere.local user, or the administrator@*mydomain* user if you selected a different domain during installation, does not expire and is not subject to the lockout policy. In all other regards, the password must follows the restrictions set in the vCenter Single Sign-On password policy. See "Edit the vCenter Single Sign-On Password Policy," on page 38.

If you forget the password for this users, search the VMware Knowledge Base system for information on resetting this password.

Other vsphere.local users

The passwords for other vsphere.local users, or users of the local domain you specified during installation, must follow the restrictions set by the vCenter Single Sign-On password policy and lockout policy. See "Edit the vCenter Single Sign-On Password Policy," on page 38 and "Edit the vCenter Single Sign-On Lockout Policy," on page 39. These passwords expire after 90 days by default, though administrators can change the expiration as part of the password policy.

If a user forgets their vsphere.local password, an administrator user can reset the password using the `dir-cli` command.

Other Users

Password restrictions, lockout, and expiration for all other users are determined by the domain (identity source) to which the user can authenticate.

vCenter Single Sign-On supports one default identity source, and users can log in to the vSphere Client with just their user names. The domain determines the password parameters. If users want to log in as a user in a non-default domain, they can include the domain name, that is, specify *user@domain* or *domain\user*. The domains password parameters apply in this case as well.

Passwords for vCenter Server Appliance Direct Console User Interface Users

The vCenter Server Appliance is a preconfigured Linux-based virtual machine, which is optimized for running vCenter Server and the associated services on Linux.

When you deploy the vCenter Server Appliance, you specify a password for the root user of the appliance Linux operating system and a password for the administrator@vsphere.local user. You can change the root user password and perform other vCenter Server Appliance local user management tasks from the Direct Console User Interface. See *vCenter Server Appliance Configuration*.

Security Best Practices and Resources

If you follow best practices, your ESXi and vCenter Server can be as secure as or even more secure than an environment that does not include virtualization.

This manual includes best practices for the different components of your vSphere infrastructure.

Table 1-1. Security Best Practices

vSphere component	Resource
ESXi host	"ESXi Security Best Practices," on page 185
vCenter Server system	"vCenter Server Security Best Practices," on page 187
Virtual machine	"Virtual Machine Security Best Practices," on page 196
vSphere Networking	"vSphere Networking Security Best Practices," on page 222

This manual is only one of the sources you need to ensure a secure environment.

VMware security resources, including security alerts and downloads, are available on the Web.

Table 1-2. VMware Security Resources on the Web

Topic	Resource
VMware security policy, up-to-date security alerts, security downloads, and focus discussions of security topics.	http://www.vmware.com/go/security
Corporate security response policy	http://www.vmware.com/support/policies/security_response.html VMware is committed to helping you maintain a secure environment. Security issues are corrected in a timely manner. The VMware Security Response Policy states our commitment to resolve possible vulnerabilities in our products.

Table 1-2. VMware Security Resources on the Web (Continued)

Topic	Resource
Third-party software support policy	http://www.vmware.com/support/policies/ VMware supports a variety of storage systems, software agents such as backup agents, system management agents, and so forth. You can find lists of agents, tools, and other software that supports ESXi by searching http://www.vmware.com/vmtn/resources/ for ESXi compatibility guides. The industry offers more products and configurations than VMware can test. If VMware does not list a product or configuration in a compatibility guide, Technical Support will attempt to help you with any problems, but cannot guarantee that the product or configuration can be used. Always evaluate security risks for unsupported products or configurations carefully.
Compliance and security standards, as well as partner solutions and in-depth content about virtualization and compliance	http://www.vmware.com/go/compliance
Information on security certifications and validations such as CCEVS and FIPS for different versions of the components of vSphere.	https://www.vmware.com/support/support-resources/certifications.html
Hardening guides for different versions of vSphere and other VMware products.	https://www.vmware.com/support/support-resources/hardening-guides.html
Security of the VMware vSphere Hypervisor white paper	http://www.vmware.com/files/pdf/techpaper/vmw-wp-secrty-vsphr-hyprvsr-uslet-101.pdf

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 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, License Service, and Lookup 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," on page 51.

After a user can authenticate with vCenter Single Sign-On, you can authorize the user to perform certain tasks. In most cases, you assign vCenter Server privileges, but vSphere includes other permission models. See "Understanding Authorization in vSphere," on page 114.

This chapter includes the following topics:

- "Understanding vCenter Single Sign-On," on page 20
- "Configuring vCenter Single Sign-On Identity Sources," on page 29
- "Managing the Security Token Service (STS)," on page 35
- "Managing vCenter Single Sign-On Policies," on page 38
- "Managing vCenter Single Sign-On Users and Groups," on page 40
- "vCenter Single Sign-On Security Best Practices," on page 46
- "Troubleshooting vCenter Single Sign-On," on page 46

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.

How vCenter Single Sign-On Protects Your Environment

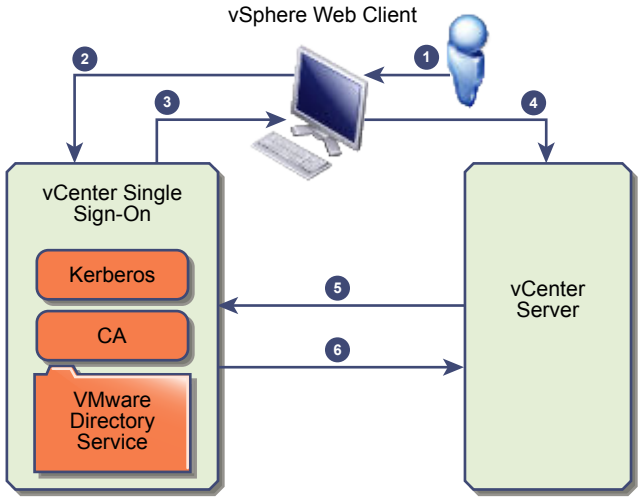
vCenter Single Sign-On allows vSphere components to communicate with each other through a secure token mechanism instead of requiring users to authenticate separately with each component.

vCenter Single Sign-On uses a combination of STS (Security Token Service), SSL for secure traffic, and authentication of human users through Active Directory or OpenLDAP and 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** checkbox.

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, leveraging thevCenter Server Authorization Framework to allow user access.

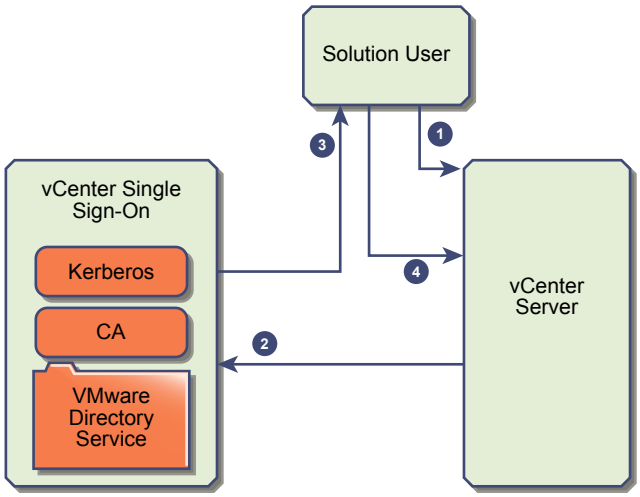
The user can now authenticate, and can view and modify any objects that the user's role has privileges for.

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 "Add a Permission to an Inventory Object," on page 120.

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 Third-Party Certificates With vSphere," on page 90.

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 eight 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 eight 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.

For detailed information about the deployment models, the advantages and disadvantages of each deployment type, see *vSphere Installation and Setup*.

How vCenter Single Sign-On Affects Upgrades

If you upgrade a Simple Install environment to a vCenter Server 6 embedded deployment, upgrade is seamless. If you upgrade a custom installation, the vCenter Single Sign-On service is part of the Platform Services Controller after the upgrade. Which users can log in to vCenter Server after an upgrade depends on the version that you are upgrading from and the deployment configuration.

As part of the upgrade, you can define a different vCenter Single Sign-On domain name to be used instead of vsphere.local.

Upgrade Paths

The result of the upgrade depends on what installation options you had selected, and what deployment model you are upgrading to.

Table 2-1. Upgrade Paths

Source	Result
vSphere 5.5 and earlier Simple Install	vCenter Server with embedded Platform Services Controller.
vSphere 5.5 and earlier Custom Install	If vCenter Single Sign-On was on a different node than vCenter Server, an environment with an external Platform Services Controller results. If vCenter Single Sign-On was on the same node as vCenter Server, but other services are on different nodes, an environment with an embedded Platform Services Controller results. If the custom installation included multiple replicating vCenter Single Sign-On servers, an environment with multiple replicating Platform Services Controller instances results.

Who Can Log In After Upgrade of a Simple Install

If you upgrade an environment that you provisioned using the Simple Install option, the result is always an installation with an embedded Platform Services Controller. Which users are authorized to log in depends on whether the source environment includes vCenter Single Sign-On.

Table 2-2. Login Privileges After Upgrade of Simple Install Environment

Source version	Login access for	Notes
vSphere 5.0	Local operating system users administrator@vsphere.local	You might be prompted for the administrator of the root folder in the vSphere inventory hierarchy during installation because of changes in user stores. If your previous installation supported Active Directory users, you can add the Active Directory domain as an identity source.
vSphere 5.1	Local operating system users administrator@vsphere.local Admin@SystemDomain	Starting with vSphere 5.5, vCenter Single Sign-On supports only one default identity source. You can set the default identity source. See "Set the Default Domain for vCenter Single Sign-On," on page 30. Users in a non-default domain can specify the domain when they log in (*DOMAIN**user* or user@*DOMAIN*).
vSphere 5.5	administrator@vsphere.local or the administrator of the domain that you specified during upgrade. All users from all identity sources can log in as before.	

If you upgrade from vSphere 5.0, which does not include vCenter Single Sign-On, to a version that includes vCenter Single Sign-On, local operating system users become far less important than the users in a directory service such as Active Directory. As a result, it is not always possible, or even desirable, to keep local operating system users as authenticated users.

Who Can Log In After Upgrade of a Custom Installation

If you upgrade an environment that you provisioned using the Custom Install option, the result depends on your initial choices:

- If vCenter Single Sign-On was on the same node as the vCenter Server system, the result is an installation with an embedded Platform Services Controller.
- If vCenter Single Sign-On was on a different node than the vCenter Server system, the result is an installation with an external Platform Services Controller.
- If you upgrade from vSphere 5.0, you can select an external or embedded Platform Services Controller as part of the upgrade process.

Login privileges after the upgrade depend on several factors.

Table 2-3. Login Privileges After Upgrade of Custom Install Environment

Source version	Login access for	Notes
vSphere 5.0	vCenter Single Sign-On recognizes local operating system users for the machine where the Platform Services Controller is installed, but not for the machine where vCenter Server is installed. NOTE Using local operating users for administration is not recommended, especially in federated environments. administrator@vsphere.local can log in to vCenter Single Sign-On and each vCenter Server instance as an administrator user.	If your 5.0 installation supported Active Directory users, those users no longer have access after the upgrade. You can add the Active Directory domain as an identity source.
vSphere 5.1 or vSphere 5.5	vCenter Single Sign-On recognizes local operating system users for the machine where the Platform Services Controller is installed, but not for the machine where vCenter Server is installed. NOTE Using local operating users for administration is not recommended, especially in federated environments. administrator@vsphere.localcan log in to vCenter Single Sign-On and each vCenter Server instance as an administrator user. For upgrades from vSphere 5.1 Admin@SystemDomain has the same privileges as administrator@vsphere.local.	Starting with vSphere 5.5, vCenter Single Sign-On supports only one default identity source. You can set the default identity source. See "Set the Default Domain for vCenter Single Sign-On," on page 30. Users in a non-default domain can specify the domain when they log in (*DOMAIN**user* or user@*DOMAIN*).

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 **Manage > Permissions** interface in the vSphere Web Client, not through vCenter Single Sign-On. See Chapter 4, "vSphere Permissions and User Management Tasks," on page 113.

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. See Chapter 4, "vSphere Permissions and User Management Tasks," on page 113.

After installation, the administrator@vsphere.local user 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).

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," on page 45. 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.

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," on page 29.

NOTE You cannot rename the administrator@vsphere.local user. For improved security, consider creating additional named users in the vsphere.local domain and assigning them administrative privileges. You can then stop using administrator@vsphere.local.

Authentication in Different Versions of vSphere

If a user connects to a vCenter Server system version 5.0.x or earlier, vCenter Server authenticates the user by validating the user against an Active Directory domain or against the list of local operating system users. In vCenter Server 5.1 and later, users authenticate through vCenter Single Sign-On.

NOTE You cannot use the vSphere Web Client to manage vCenter Server version 5.0 or earlier. Upgrade vCenter Server to version 5.1 or later.

ESXi Users

ESXi is not integrated with vCenter Single Sign-On. You add the ESXi host to an Active Directory domain explicitly. See "Configure a Host to Use Active Directory," on page 167.

You can still create local ESXi users with the vSphere Client, vCLI, or PowerCLI. vCenter Server is not aware of users that are local to ESXi and ESXi is not aware of vCenter Server users.

NOTE Manage permissions for ESXi hosts through vCenter Server if possible.

How to Log In to vCenter Server Components

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 default domain, that is, 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.

NOTE If your environment includes an Active Directory hierarchy, see VMware Knowledge Base article 206250 for details on supported and unsupported setups.

Groups in the vsphere.local Domain

The vsphere.local domain includes several predefined groups. Assign users to one of those groups to be able to perform the corresponding actions.

For all objects in the vCenter Server hierarchy, permissions are assigned 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 by giving them the corresponding role.

For some services that are not managed by vCenter Server directly, privileges are determined by membership to one of the vCenter Single Sign-On groups. 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.

NOTE 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 2-4. Groups in the vsphere.local Domain

Privilege	Description
Users	Users in the vsphere.local domain.
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. Adding members to these groups is not usually recommended.
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.
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 actas tokens from vCenter Single Sign-On.
ExternalIPDUsers	This group is not used by vSphere. This group is needed in conjunction with VMware vCloud Air.

Table 2-4. Groups in the vsphere.local Domain (Continued)

Privilege	Description
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 licensing service.
Administrators	Administrators of the VMware Directory Service (vmdir). Members of this group can perform vCenter Single Sign-On administration tasks. Adding members to this group is not usually recommended.

vCenter Server Password Requirements and Lockout Behavior

To manage your environment, you must be aware of the vCenter Single Sign-On password policy, of vCenter Server passwords, and of lockout behavior.

vCenter Single Sign-On Administrator Password

The password for administrator@vsphere.local must meet the following requirements:

- At least 8 characters
- At least one lowercase character
- At least one numeric character
- At least one special character

The password for administrator@vsphere.local cannot be more than 20 characters long. Only visible ASCII characters are allowed. That means, for example, that you cannot use the space character.

vCenter Server Passwords

In vCenter Server, password requirements are dictated by vCenter Single Sign-On or by the configured identity source, which can be Active Directory, OpenLDAP, or the local operating system for the vCenter Single Sign-On server (not recommended).

Lockout Behavior

By default, any user, including users with Administrator privileges, are locked out after a preset number of consecutive failed attempts. By default, users are locked out after five consecutive failed attempt in three minutes. A locked account is unlocked automatically after five minutes. You can change these defaults using the lockout policy. See "Edit the vCenter Single Sign-On Lockout Policy," on page 39.

Any user can change their password by using the `dir-cli password change` command. If a user forgets the password, the administrator can reset the password by using the `dir-cli password reset` command.

See "ESXi Passwords, ESXi Pass Phrases, and Account Lockout," on page 135 for a discussion of passwords of ESXi local users.

Configuring vCenter Single Sign-On Identity Sources

When a user logs in, vCenter Single Sign-On checks in the default identity source whether that user can authenticate. You can add identity sources, remove identity sources, and change the default.

You configure vCenter Single Sign-On from the vSphere Web Client. To configure vCenter Single Sign-On, you must have vCenter Single Sign-On administrator privileges. Having vCenter Single Sign-On administrator privileges is different from having the Administrator role on vCenter Server or ESXi. By default, only the user administrator@vsphere.local has administrator privileges on the vCenter Single Sign-On server in a new installation.

- Identity Sources for vCenter Server with vCenter Single Sign-On on page 29

  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 on page 30

  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 on page 31

  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.

- Edit a vCenter Single Sign-On Identity Source on page 34

  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 on page 35

  vSphere users are defined in an identity source. You can remove an identity source from the list of registered identity sources.

- Use vCenter Single Sign-On with Windows Session Authentication on page 35

  You can use vCenter Single Sign-On with Windows Session Authentication (SSPI). To make the checkbox on the login page available, the Client Integration Plug-in must be installed.

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 could always 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 named vsphere.local is created when you install vCenter Single Sign-On. Shown as **vsphere.local** in the vSphere Web Client.

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 default domain, that is, the domain that is set as the default identity source.

- Users who are in the default domain can log in with their user name and password.
- Users who are in a domain that has been added to vCenter Single Sign-On as an identity source but is not the default domain can log in to vCenter Server but must specify the domain in one of the following ways.
  - Including a domain name prefix, for example, MYDOMAIN\user1

- Including the domain, for example, user1@mydomain.com

- Users who are in a domain that is not a vCenter Single Sign-On identity source cannot log in to vCenter Server. If the domain that you add to vCenter Single Sign-On is part of a domain hierarchy, Active Directory determines whether users of other domains in the hierarchy are authenticated or not.

Procedure

1 Log in 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 vsphere.local domain.

2 Browse to **Administration > Single Sign-On > Configuration**.

3 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.

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," on page 29

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

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

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 vsphere.local domain.

2 Browse to **Administration > Single Sign-On > Configuration**.

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

4 Select the type of identity source and enter the identity source settings.

Option	Description
Active Directory (Integrated Windows Authentication)	Use this option for native Active Directory implementations. The machine on which the vCenter Single Sign-Onservice is running must be in an Active Directory domain if you want to use this option. See "Active Directory Identity Source Settings," on page 32.
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," on page 33.

Option	Description
OpenLDAP	Use this option for an OpenLDAP identity source. See "Active Directory LDAP Server and OpenLDAP Server Identity Source Settings," on page 33.
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 will 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. This is the default Active Directory domain configuration for authentication permissions. VMware recommends using a special service user.

5 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.

6 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 "Add a Permission to an Inventory Object," on page 120.

Active Directory Identity Source Settings

If you select the Active Directory (Integrated Windows Authentication) identity source type, you can either 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.

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 2-5. Add Identity Source Settings

Field	Description
Domain name	FDQN of the domain. Do not provide an IP address in this field.
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.

Table 2-5. Add Identity Source Settings (Continued)

Field	Description
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. You might have to run `setspn -S` to add the user you want to use. See the Microsoft documentation for information on `setspn`. The SPN must be unique across the domain. Running `setspn -S` checks that no duplicate is created.
User Principal Name (UPN)	Name 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).
Password	Password for the user who is used to authenticate with this identity source, which is the user who is specified in User Principal Name. Include the domain name, for example, jdoe@example.com.

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 2-6. Active Directory as an LDAP Server and OpenLDAP Settings

Field	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 field.
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: connections and 3269 for ldaps: connections. 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.

Table 2-6. Active Directory as an LDAP Server and OpenLDAP Settings (Continued)

Field	Description
Choose certificate	If you want to use LDAPS with your Active Directory LDAP Server or OpenLDAP Server identity source, a Choose certificate button becomes available after you type **`ldaps://`** in the URL field. 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 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 vsphere.local domain.

2 Browse to **Administration > Single Sign-On > Configuration**.

3 Click the **Identity Sources** tab.

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

5 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-Onservice is running must be in an Active Directory domain if you want to use this option. See "Active Directory Identity Source Settings," on page 32.
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," on page 33.
OpenLDAP	Use this option for an OpenLDAP identity source. See "Active Directory LDAP Server and OpenLDAP Server Identity Source Settings," on page 33.
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.

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

7 Click **OK**.

Remove a vCenter Single Sign-On Identity Source

vSphere users are defined in an identity source. You can remove an identity source from the list of registered identity sources.

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 vsphere.local domain.

2 Browse to **Administration > Single Sign-On > Configuration**.

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

4 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). To make the checkbox on the login page available, the Client Integration Plug-in must be installed.

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

Prerequisites

Your Windows domain must be set up properly. See VMware Knowledge Base article 2064250.

Procedure

1 Navigate to the vSphere Web Client login page.

2 If the **Use Windows session authentication** check box is not available, click **Download the Client Integration Plug-in** at the bottom of the login page.

3 If the browser blocks the installation by issuing certificate errors or by running a pop-up blocker, follow the Help instructions for your browser to resolve the problem.

4 Close other browsers if you are prompted to do so.

After installation, the plug-in is available for all browsers. If your browser requires it, you might have to allow the plug-in for individual sessions or for all sessions.

5 Exit and restart your browser.

After the restart, you can select the **Use Windows session authentication** check box.

Managing the Security Token Service (STS)

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

To acquire SAML tokens, users present their primary credentials to the STS interface. The primary credentials depend 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 Client.

After a user has a SAML token, the SAML token is sent as part of that user 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 (STS) Root 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.

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

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 vsphere.local domain.

2 Browse to **Administration > Single Sign-On > Configuration**.

3 Select the **Certificates** tab, then the **STS Signing** subtab, and click the **Add STS Signing Certificate** icon.

4 Click **Browse** to browse to the key store JKS file that contains the new certificate and click **Open**.

   If the key store file is valid, the STS certificate table is populated with the certificate information.

5 Click **OK**.

The new certificate information appears on the **STS Signing** tab.

What to do next

Restart the vSphere Web Client service. You can find all services in the **System Configuration** area of **Administration**.

Determine the Expiration Date of an LDAPS SSL Certificate

If you select a Active Directory LDAP Server and OpenLDAP Server 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 and 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 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 vsphere.local domain.

2 Browse to **Administration > Single Sign-On > Configuration**.

3 Click the **Certificates** tab, and then the **Identity Sources TrustStore** subtab.

4 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.

Add a SAML Service Provider

If you have an external SAML service provider in your environment, you can add your provider metadata to the VMware Identity Provider that is included with vCenter Single Sign-On. Going forward, your SAML service provider can be used.

The process involves importing the metadata from your SAML service provider into vCenter Single Sign-On, and importing the vCenter Single Sign-On metadata into your SAML service provider so the two providers share all data.

Prerequisites

Retrieve the metadata from your SAML service provider. Your provider must be a SAML 2.0 service provider.

Procedure

1 Export the metadate from your service provider to a file.

2 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 vsphere.local domain.

3 Browse to **Administration > Sign-On > Configuration**.

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

5 In the Metadata from your SAML service provider field, click **Import** and paste the XML strings into the dialog, or click **Import from File** to import a file and then click **Import**.

6 In the Metadata for your SAML service provider field, click **Download** and specify a file location.

7 Follow the instructions for your SAML service provider to add the vCenter Single Sign-On metadata to that service provider.

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 passwords, lockout policies, and token policies.

Edit the vCenter Single Sign-On Password Policy

The vCenter Single Sign-On password policy is a set of rules and restrictions on 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. You can reset an expired password if you know the old password.

NOTE Password policies apply only to user accounts, not to system accounts such as administrator@vsphere.local.

See "Change Your vCenter Single Sign-On Password," on page 45.

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 vsphere.local domain.

2 Browse to **Administration > Single Sign-On > Configuration**.

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

4 Click **Edit**.

5 Edit the password policy parameters.

Option	Description
Description	Password policy description.
Maximum lifetime	Maximum number of days that a password can exist before the user must change it.
Restrict reuse	Number of the user's previous passwords that cannot be selected. For example, if a user cannot reuse any of the last six passwords, type 6.
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.

Option	Description
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 requirements. 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. The number must be greater than 0. For example, if you enter 1, the following password is not allowed: p@$$word.

6 Click **OK**.

Edit the vCenter Single Sign-On Lockout Policy

A vCenter Single Sign-On lockout policy specifies the conditions under which a user's vCenter Single Sign-On account is locked when the user attempts to log in with incorrect credentials. You 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 you to specify the maximum number of failed login attempts and how much time can elapse between failures. The policy also specifies how much time must elapse before the account is automatically unlocked.

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

Procedure

1 Log in 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 vsphere.local domain.

2 Browse to **Administration > Single Sign-On > Configuration**.

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

4 Click **Edit**.

5 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.

6 Click **OK**.

Edit the vCenter Single Sign-On Token Policy

ThevCenter Single Sign-On token policy specifies the clock tolerance, renewal count, and other token properties. You can edit the vCenter Single Sign-On token policy to ensure that the token specification conforms to your corporation's security standards.

Procedure

1 Log in to the vSphere Web Client.

2 Select **Administration > Single Sign-On**, and select **Configuration**.

3 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.

4 Edit the token policy configuration parameters.

Option	Description
Clock tolerance	Time difference, in milliseconds, that vCenter Single Sign-On tolerates between a client clock and the domain controller clock. If the time difference is greater than the specified value, vCenter Single Sign-On declares the token invalid.
Maximum token renewal count	Maximum number of times that a token can be renewed. After the maximum number of renewal attempts, a new security token is required.
Maximum token delegation count	Holder-of-key tokens can be delegated to services in the vSphere environment. A service that uses a delegated token performs the service on behalf of the principal that provided the token. A token request specifies a DelegateTo identity. The DelegateTo value can either be a solution token or a reference to a solution token. This value specifies how many times a single holder-of-key token can be delegated.
Maximum bearer token lifetime	Bearer tokens provide authentication based only on possession of the token. Bearer tokens are intended for short-term, single-operation use. A bearer token does not verify the identity of the user or entity that is sending the request. This value specifies the lifetime value of a bearer token before the token has to be reissued.
Maximum holder-of-key token lifetime	Holder-of-key tokens provide authentication based on security artifacts that are embedded in the token. Holder-of-key tokens can be used for delegation. A client can obtain a holder-of-key token and delegate that token to another entity. The token contains the claims to identify the originator and the delegate. In the vSphere environment, a vCenter Server system obtains delegated tokens on a user's behalf and uses those tokens to perform operations. This value determines the lifetime of a holder-of-key token before the token is marked invalid.

5 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 on page 41

  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.

- Disable and Enable vCenter Single Sign-On Users on page 42

  When a vCenter Single Sign-Onuser account is disabled, the user cannot log in to the vCenter Single Sign-On server until the account is enabled by an administrator. You can disable and enable users from the vSphere Web Client interface.

- Delete a vCenter Single Sign-On User on page 42

  You can delete users that are in the vsphere.local domain from the vCenter Single Sign-On. You cannot delete local operating system users or users in another domain from the vSphere Web Client.

- Edit a vCenter Single Sign-On User on page 43

  You can change the password or other details of a vCenter Single Sign-On user from the vSphere Web Client. You cannot rename users in the vsphere.local domain. That means you cannot rename administrator@vsphere.local.

- Add a vCenter Single Sign-On Group on page 43

  In the vCenter Single Sign-On, groups listed on the **Groups** tab are internal to vCenter Single Sign-On. A group lets you create a container for a collection of group members (principals).

- Add Members to a vCenter Single Sign-On Group on page 44

  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 on page 44

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

- Delete vCenter Single Sign-On Solution Users on page 45

  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 on page 45

  Users in the vsphere.local domain can change their vCenter Single Sign-On passwords from the vSphere Web Client. Users in other domains change their passwords following the rules for that domain. You can change a vCenter Single Sign-On password or reset an expired password from the vSphere Web Client or using the `dir-cli password reset` command.

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 can select other domains and view information about the users in those domains, but you cannot add users to other domains from the vCenter Single Sign-On management interface of the vSphere Web Client.

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 vsphere.local domain.

2. Click **Home**, and browse to **Administration > Single Sign-On > Users and Groups**.

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

   You cannot add users to other domains.

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

5 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.

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

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

8 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 administrator 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," on page 44.

Disable and Enable vCenter Single Sign-On Users

When a vCenter Single Sign-Onuser account is disabled, the user cannot log in to the vCenter Single Sign-On server until the account is enabled by an administrator. You can disable and enable users from the vSphere Web Client interface.

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 users from the vCenter Users and Groups page.

Prerequisites

You must be a member of the vCenter Single Sign-On Administrators group to disable and enable vCenter Single Sign-On users.

Procedure

1 Log in 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 vsphere.local domain.

2 Click **Home**, and browse to **Administration > Single Sign-On > Users and Groups**.

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

4 To enable the user again, right-click the user, 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 the vCenter Single Sign-On. You cannot delete local operating system users or users in another domain from the vSphere Web Client.

CAUTION If you delete the administrator user in the vsphere.local domain, you can no longer log in to vCenter Single Sign-On. Reinstall vCenter Server and its components.

Procedure

1 Log in 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 vsphere.local domain.

2 Click **Home**, and browse to **Administration > Single Sign-On > Users and Groups**.

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

4 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 the vSphere Web Client. 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**.

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 vsphere.local domain.

2 Click **Home**, and browse to **Administration > Single Sign-On > Users and Groups**.

3 Click the **Users** tab.

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

5 Make changes to the user.

You cannot change the user name of the user.

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

6 Click **OK**.

Add a vCenter Single Sign-On Group

In the vCenter Single Sign-On, groups listed on the **Groups** tab are internal to vCenter Single Sign-On. A group lets you create a container for a collection of group members (principals).

When you add a vCenter Single Sign-On group from the vSphere Web Client administration interface, the group is added to the vsphere.local domain.

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 vsphere.local domain.

2 Click **Home**, and browse to **Administration > Single Sign-On > Users and Groups**.

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

4 Enter a name and description for the group.

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

5 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.

You can add members of Microsoft Active Directory or OpenLDAP groups to a vCenter Single Sign-On group. You cannot add groups from external identity sources to a vCenter Single Sign-On group.

Groups listed on the **Groups** tab in the vSphere Web Client are part of the vsphere.local domain. See "Groups in the vsphere.local Domain," on page 27.

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 vsphere.local domain.

2 Click **Home**, and browse to **Administration > Single Sign-On > Users and Groups**.

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

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

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

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

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

You can simultaneously add multiple members.

8 Click **OK**.

Remove Members from a vCenter Single Sign-On Group

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

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 vsphere.local domain.

2 Click **Home**, and browse to **Administration > Single Sign-On > Users and Groups**.

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

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

5 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 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 vsphere.local domain.

2 Click **Home**, and browse to **Administration > Single Sign-On > Users and Groups**.

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

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

5 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 vsphere.local domain can change their vCenter Single Sign-On passwords from the vSphere Web Client. Users in other domains change their passwords following the rules for that domain. You can change a vCenter Single Sign-On password or reset an expired password from the vSphere Web Client or using the `dir-cli password reset` command.

The password policy that is defined in the vCenter Single Sign-On configuration interface 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. The vSphere Web Client reminds you when your password is about to expire. You can reset an expired password if you know the old password.

This procedure explains how you can change a password. If your password is expired, you are prompted to change it. In that case, you must supply the old password. If you no longer remember your password, administrator@vsphere.local or another member of the Administrators group in vsphere.local can reset the password by using the `dir-cli password reset` command.

Procedure

1 Log in to the vSphere Web Client using your vCenter Single Sign-On credentials.

2 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 **Administration > Single Sign-On > Users and Groups** and select **Edit User** from the right-button menu.

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

4 Type a new password and confirm it.

The password must conform to the password policy.

5 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.

Troubleshooting vCenter Single Sign-On

Configuring vCenter Single Sign-On can be a complex process.

The following topics provide a starting point for troubleshooting vCenter Single Sign-On. Search this documentation center and the VMware Knowledge Base system for additional pointers.

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) and 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	IThe 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 is an uncommon error. It indicates that the provided IP address or FQDN that resolves to vCenter Single Sign-On host was not the one 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 username 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 and that the PTR record information matches the DNS name of the controller. When using the vCenter Server Appliance, you can 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 log in as a user from the system domain (vsphere.local), ask your vCenter Single Sign-On administrator to unlock your account. As an alternative, you can wait until your account is unlocked, if the lock is set to expire in the password policy. 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.

vSphere Security Certificates

3

vSphere components 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 their certificates for their initial authentication to vCenter Single Sign-On. vCenter Single Sign-On provisions each component with a SAML token that the component uses for authentication going forward.

In vSphere 6.0 and later, the VMware Certificate Authority (VMCA) provisions each ESXi host and each vCenter Server service with certificates that are signed by VMCA by default. You can use the vSphere Certificate Manager command-line utility to perform certificate replacement operations. In special cases, you can replace certificates manually.

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

This chapter includes the following topics:

- "Certificate Management Overview," on page 52
- "Certificate Replacement Overview," on page 53
- "Managing Certificates in vSphere 6," on page 56
- "Using the vSphere Certificate Manager Utility," on page 63
- "Generate Certificate Signing Requests with vSphere Certificate Manager," on page 69
- "Manual Certificate Replacement," on page 69
- "Managing Certificates and Services with CLI Commands," on page 96
- "View vCenter Certificates with the vSphere Web Client," on page 111
- "Set the Threshold for vCenter Certificate Expiration Warnings," on page 111

Certificate Management Overview

The impact of the new 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

If you are an administrator who does not currently replace VMware certificates, VMCA can handle all certificate management for you. 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.

Administrators Who Replace VMware Certificates with Custom Certificates

For a fresh installation, administrators have these choices if company policy requires certificates that are signed by a third-party or enterprise certificate authority or requires custom certificate information.

- Replace the VMCA root certificate with a CA-signed certificate. In this scenario, the VMCA certificate is an intermediate certificate of this third-party CA. 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 have to explicitly replace certificates. You can use the 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 vCenter Server upgrade, administrators can set the certificate mode to Custom (see "Change the Certificate Mode," on page 144). 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.
  - If you upgrade a simple installation to an embedded deployment, vCenter Server custom certificates are retained. After the upgrade, your environment will work as before.
  - If you upgrade a multi-site deployment where vCenter Single Sign-On is on a different machine than other vCenter Server components, the upgrade process creates a multi-node deployment that includes a Platform Services Controller node and one or more management nodes.

    In this scenario, the existing vCenter Server and vCenter Single Sign-On certificates are retained and used as machine SSL certificates. VMCA assigns a VMCA-signed certificate to each solution user (collection of vCenter services). A solution user uses this certificate only to authenticate to vCenter Single Sign-On, so it might be unnecessary to replace solution user certificates.

  You can no longer use the vSphere 5.5 certificate replacement tool, which was available for vSphere 5.5 installations, because 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.

vCenter Certificate Interfaces

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

vSphere Certificate Manager utility	Perform all common certificate replacement tasks from the command-line.
Certificate management CLIs	Perform all certificate management tasks with `dir-cli`, `certool`, and `vecs-cli`.
vSphere Web Client certificate management	View certificates, including expiration information.

For ESXi, you perform certificate management from the vSphere Web Client. Certificates are provisioned by VMCA and are stored only locally on the ESXi host, not in vmdir or VECS. See "Certificate Management for ESXi Hosts," on page 137.

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 each replacement with the vSphere Certificate Manager utility or manually by using the CLIs included with your installation.

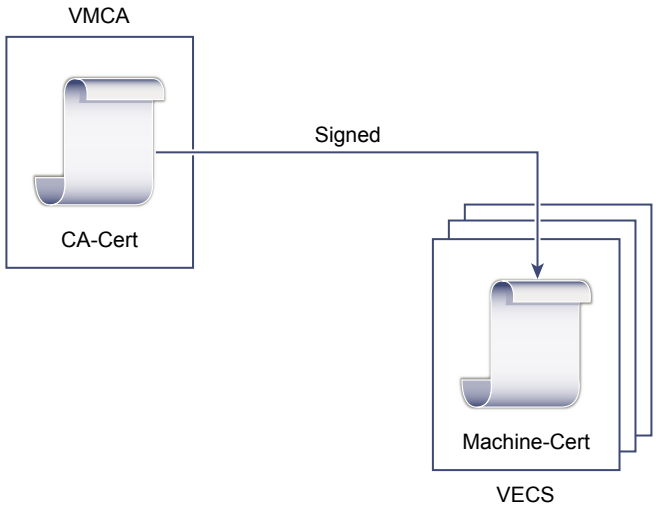
VMCA is included in each Platform Services Controller and in each embedded deployment. VMCA provisions each node, each vCenter Server solution user, and each ESXi host with a certificate that is signed by VMCA as the certificate authority. vCenter Server solution users are groups of vCenter Server services.

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



You can use the following vSphere Certificate Manager options:

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

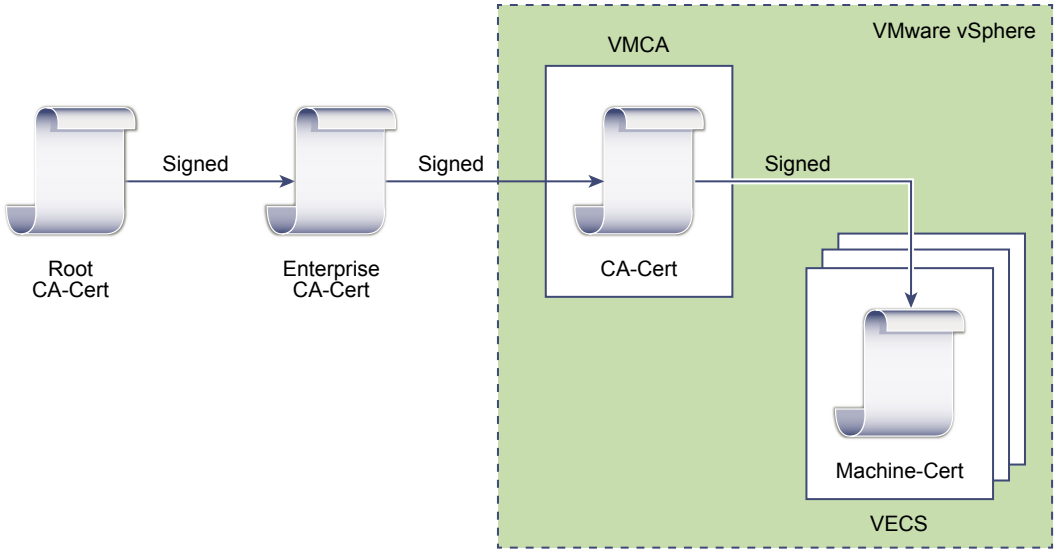
For manual certificate replacement, see "Replace Existing VMCA-Signed Certificates With New VMCA-Signed Certificates," on page 70.

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, all certificates are signed by 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



You can use the following vSphere Certificate Manager options:

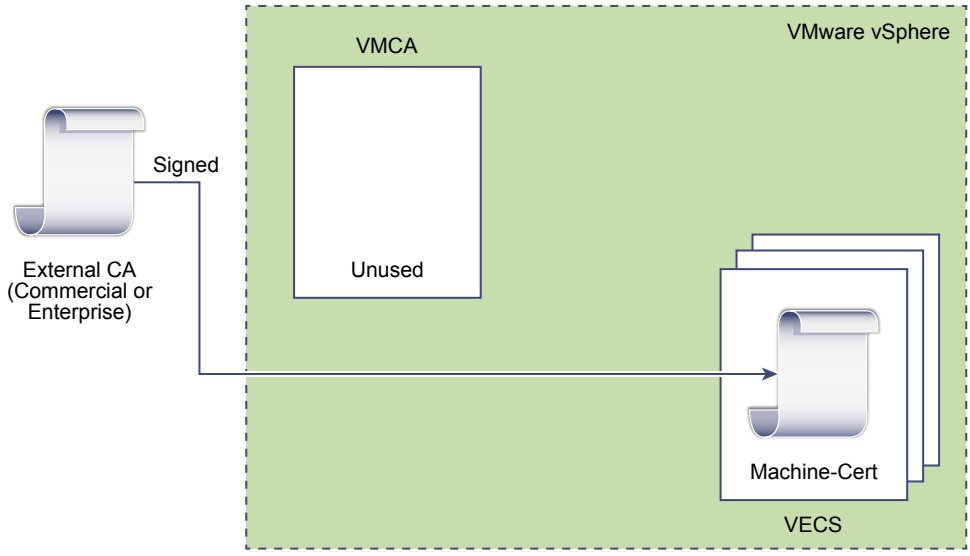
- Replace VMCA Root Certificate with Custom Signing Certificate and Replace All Certificates
- Replace Machine SSL Certificate with VMCA Certificate (multi-node deployment)
- Replace Solution User Certificate with VMCA Certificate (multi-node deployment)

For manual certificate replacement, see "Use VMCA as an Intermediate Certificate Authority," on page 80.

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



You can use the following vSphere Certificate Manager options:

- Replace Machine SSL Certificate with Custom Certificate

- Replace Solution User Certificates with Custom Certificates

For manual certificate replacement, see "Use Third-Party Certificates With vSphere," on page 90.

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.

ESXi Certificate Replacement

For ESXi hosts, you can change certificate provisioning behavior from the vSphere Web Client.

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.

See "Certificate Management for ESXi Hosts," on page 137.

Managing Certificates in vSphere 6

Starting with vSphere 6.0, the VMware Certificate Authority (VMCA) provisions vCenter Server components and ESXi hosts with certificates by default. Understanding the components and concepts of certificate management helps you make good decisions.

Where vSphere 6.0 Uses Certificates

In vSphere 6.0 and later, the VMware Certificate Authority (VMCA) provisions your environment with certificates. This includes machine SSL certificates for secure connections, solution user certificates for authentication to vCenter Single Sign-On, and certificates for ESXi hosts that are added to vCenter Server.

The following certificates are in use.

Table 3-1. Certificates in vSphere 6.0

Certificate	Provisioned by	Stored
ESXi certificates	VMCA (default)	Locally on ESXi host
Machine SSL certificates	VMCA (default)	VECS
Solution user certificates	VMCA (default)	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.	In certain corner cases, you might have to replace this certificate. See "Replace the VMware Directory Service Certificate," on page 88.

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 to which SSL clients connect. The certificate is used for server verification and for secure communication such as HTTPS or LDAPS.

All services communicate through the reverse proxy. For compatibility, services that were available in earlier versions of vSphere also use specific ports. For example, the vpxd service uses the MACHINE_SSL_CERT to expose its endpoint.

Every node (embedded deployment, management node, or Platform Services Controller), has its own machine SSL certificate. All services that are running on that node use this machine SSL certificate to expose their SSL endpoints.

The machine SSL certificate is used as follows:

- By 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.
- By the vCenter service (vpxd) on management nodes and embedded nodes.
- By 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 that is sent over SSL between components.

Solution User Certificates

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

Solution user certificates are used for authentication tovCenter Single Sign-On. 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 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.

The machine store is also included on each Platform Services Controller node.

vCenter Single Sign-On 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 (STS) Root Certificate," on page 36.

VMware Directory Service SSL Certificate

If you are using custom certificates, you might have to replace the VMware Directory Service SSL certificate explicitly. See "Replace the VMware Directory Service Certificate," on page 88.

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 3-2. 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," on page 103.

VECS includes the following stores.

Table 3-3. 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 3-3. 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. The machine store is also included on each Platform Services Controller node.
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 artoc;e instructs you to do so. **NOTE** CRLS are not supported in vSphere 6.0 Nevertheless, 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.

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

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.

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 node 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," on page 72
- "Replace Machine SSL Certificates (Intermediate CA)," on page 82
- "Replace Machine SSL Certificates With Custom Certificates," on page 92

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 "Using the vSphere Certificate Manager Utility," on page 63

See the following topics for details:

- "Replace Solution User Certificates With New VMCA-Signed Certificates," on page 75
- "Replace Solution User Certificates (Intermediate CA)," on page 84
- "Replace Solution User Certificates With Custom Certificates," on page 93

If company policy requires that you replace all certificates, you also have to replace the VMware Directory Service (vmdir) certificate on the Platform Services Controller. See "Replace the VMware Directory Service Certificate," on page 88.

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.

Using 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.

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 Replace Machine SSL Certificate with Custom Certificate on page 64

The machine SSL certificate is used by the reverse proxy service on every management node, Platform Services Controller, and embedded deployment. You can replace the certificate on each node with a custom certificate.

2 Replace VMCA Root Certificate with Custom Signing Certificate and Replace All Certificates on page 65

You can replace the VMCA root certificate with a CA-signed certificate that includes VMCA as an intermediate certificate in the certificate chain. Going forward, all certificates that VMCA generates include the full chain. You can use vSphere Certificate Manager to supply a custom signing certificate to VMCA, and to replace all certificates in your deployment.

3 Replace Machine SSL Certificate with VMCA Certificate on page 66

If any of the machine SSL certificates in your environment is corrupt or about to expire, you can replace it with a VMCA-signed machine SSL certificate. If you use vSphere Certificate Manager for this task, you are prompted for information and vSphere Certificate Manager performs starting and stopping of services and certificate replacement for you.

4 Regenerate a New VMCA Root Certificate and Replace All Certificates on page 66

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`.

5 Replace Solution User Certificates with Custom Certificates on page 67

When you select this option, vSphere Certificate Manager prompts you for replacement certificates for the existing solution user certificates. In multi-node deployments, run vSphere Certificate Manager with this option to replace the machine solution user certificate on the Platform Services Controller and the full set of solution users on each management node.

6 Replace Solution User Certificates with VMCA Certificates on page 68

If solution user certificates in your multi-node deployment are expired or compromised, you can generate a full set of new VMCA-signed certificates and then replace the existing solution user certificates.

7 Revert Last Performed Operation by Republishing Old Certificates on page 68

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.

8 Reset All Certificates on page 68

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

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. You can replace the certificate on each node with a custom certificate.

Each machine must have a machine SSL certificate for secure communication with other services.

When you replace the default VMCA-signed certificate with a custom certificate, the 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.

Prerequisites

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

Procedure

1 Start vSphere Certificate Manager and select option 1.

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

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

You can replace the VMCA root certificate with a CA-signed certificate that includes VMCA as an intermediate certificate in the certificate chain. Going forward, all certificates that VMCA generates include the full chain. You can use vSphere Certificate Manager to supply a custom signing certificate to VMCA, and to replace all certificates in your deployment.

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.

vSphere Certificate Manager prompts you for the following information:

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

Prerequisites

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
- For root certificates CA extension must be set to true, and cert sign must be in the list of requirements.
- Make sure that all nodes in your environment are time synchronized.
- No explicit limit to the length of the certificate chain. VMCA uses the OpenSSL default, which is ten certificates.
- VMCA does not support using certificates with wildcards or more than one DNS name.
- You cannot create subsidiary CAs of VMCA.

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

- 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 PKS8.
- x509 version 3
- Key Usage: Certificate Sign, CRL Sign
- Basic Constraint: Subject Type CA

Procedure

1 Start vSphere Certificate Manager and select option 2.

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

What to do next

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 Machine SSL Certificate with VMCA Certificate

If any of the machine SSL certificates in your environment is corrupt or about to expire, you can replace it with a VMCA-signed machine SSL certificate. If you use vSphere Certificate Manager for this task, you are prompted for information and vSphere Certificate Manager performs starting and stopping of services and certificate replacement for you.

You can replace the machine SSL certificate of individual machines, or use the option `Regenerate a new VMCA Root Certificate and replace all certificates` to replace all certificates with VMCA-signed certificates.

When you replace the existing machine SSL certificate with a new VMCA-signed certificate, vSphere Certificate Manager prompts you for the following information. vSphere Certificate Manager 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 FDQN 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. The IP address is optional.

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 run this command, vSphere Certificate Manager prompts you for the password and for certificate information and stores all information, except for the password, in the `certool.cfg` file. After that, stopping services, replacing all certificates, and restarting processes is automatic. You are prompted for the following information:

- 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
- IP address of Platform Services Controller if you are running the command on a management node

Prerequisites

You must know the FQDN of the machine for which you want to generate a new VMCA-signed certificate. All other properties default to the predefined values. The IP address is optional.

What to do next

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 Custom Certificates

When you select this option, vSphere Certificate Manager prompts you for replacement certificates for the existing solution user certificates. In multi-node deployments, run vSphere Certificate Manager with this option to replace the machine solution user certificate on the Platform Services Controller and the full set of solution users on each management node.

When you replace the existing machine solution user certificates with custom certificates, 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.

Prerequisites

Request a replacement certificate for each solution user.

- 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 Start vSphere Certificate Manager and select option 5.

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

Replace Solution User Certificates with VMCA Certificates

If solution user certificates in your multi-node deployment are expired or compromised, you can generate a full set of new VMCA-signed certificates and then replace the existing solution user certificates.

The following tasks are involved:

1 First you regenerate a new root certificate using option 4, `Regenerate a New VMCA Root Certificate and Replace All Certificates` on the Platform Services Controller.

   In an embedded deployment, no additional action is required.

2 Next, in a multi-node deployment, you run vSphere Certificate Manager with option 3 to replace all machine SSL certificates.

3 Finally, you run Certificate Manager again with this option to replace solution user certificates.

Prerequisites

You must know the password for administrator@vsphere.local.

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.

Generate Certificate Signing Requests with vSphere Certificate Manager

You can use vSphere Certificate Manager to generate Certificate Signing Requests (CSRs) that you can then send to your third-party or external certificate authority. You can use the returned certificates with vSphere Certificate Manager or with the manual certificate replacement using CLIs.

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 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 Start vSphere Certificate Manager and select the option that corresponds to the task that you want to perform.

Option	Option
Replace Machine SSL Certificate with Custom Certificate	1
Replace VMCA Root Certificate with Custom Signing Certificate	2
Replace Solution User Certificates with Custom Certificates	5

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.

What to do next

Send the CSR to your third-party or enterprise CA. After you receive the certificates from your CA, you can either make VMCA an intermediate CA or use the custom certificate as is. Run vSphere Certificate Manager again to perform certificate replacement.

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 Starting and Stopping 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.

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," on page 44.

Procedure

1 Generate a New VMCA-Signed Root Certificate on page 71

You generate new VMCA-signed certificates with the `certool` CLI and publish them to vmdir.

2 Replace Machine SSL Certificates with VMCA-Signed Certificates on page 72

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 on page 75

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 on page 79

During upgrade, your environment might temporarily include both vCenter Single Sign-On version 5.5 and vCenter Single Sign-On version 6.0, 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 and publish them 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
```

When you run this command, all instances of vmdir are updated immediately. Otherwise, propagation to all instances might take a while.

5 Restart all services.

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

Example: Generate a New VMCA-Signed Root Certificate

The following example shows the full set of steps for verifying the current root CA information, and 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 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 certificate is added 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 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:

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
```

- Output on Platform Services Controller:

```
MACHINE_SSL_CERT
TRUSTED_ROOTS
TRUSTED_ROOT_CRLS
machine
```

- 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 "Certificate Management for ESXi Hosts," on page 137.

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.

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 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, for example vpxd or vpxd-extension makes it easy to see which certificate maps to which solution user.

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 6.0, 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 required only if:

- Your environment includes both vCenter Single Sign-On 5.5 and vCenter Single Sign-On 6.0 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 6.0 service runs.

NOTE In most other cases, upgrading the complete environment before restarting the services is best practice. Teplacing the VMware Directory Service certificate is not usually recommended.

Procedure

1 On the node on which the vCenter Single Sign-On 6.0 service runs, replace the vmdird SSL certificate and key.

See "Replace the VMware Directory Service Certificate," on page 88.

2 On the node on which the vCenter Single Sign-On 5.5 service runs, set up the environment so the vCenter Single Sign-On 6.0 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 6.0 node, and rename it to `<sso_node2.domain.com>.pem`, where `<sso_node2.domain.com>` is the FQDN of the 6.0 node.

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

3 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. This approach combines the security of third-party CA-signed certificate with the convenience of automated certificate management.

Procedure

1 Replace the Root Certificate (Intermediate CA) on page 80

The first step in replacing the VMCA certificates with custom certificates is generating a CSR and adding the certificate that is returned to VMCA as a root certificate.

2 Replace Machine SSL Certificates (Intermediate CA) on page 82

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) on page 84

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

4 Replace the VMware Directory Service Certificate on page 88

If you decide to use a new VMCA root certificate, and you unpublish the VMCA root certificate that was used when you provisioned your environment, you must replace the machine SSL certificates, solution user certificates, and certificates for some internal services.

5 Replace the VMware Directory Service Certificate in Mixed Mode Environments on page 89

During upgrade, your environment might temporarily include both vCenter Single Sign-On version 5.5 and vCenter Single Sign-On version 6.0, 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 and adding the certificate that is returned to VMCA as a root certificate.

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
- For root certificates CA extension must be set to true, and cert sign must be in the list of requirements.
- Make sure that all nodes in your environment are time synchronized.
- No explicit limit to the length of the certificate chain. VMCA uses the OpenSSL default, which is ten certificates.
- VMCA does not support using certificates with wildcards or more than one DNS name.
- You cannot create subsidiary CAs of VMCA.

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, and 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 have to start with the VMCA certificate root and end 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 refresh these internal certificates:

- Replace the vCenter Single Sign-On Signing certificate. See "Refresh the Security Token Service (STS) Root Certificate," on page 36.
- Replace the VMware Directory Service certificate. See "Replace the VMware Directory Service Certificate," on page 88.

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
```

- Output on Platform Services Controller:

```
MACHINE_SSL_CERT
TRUSTED_ROOTS
TRUSTED_ROOT_CRLS
machine
```

- 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 "Certificate Management for ESXi Hosts," on page 137.

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 (Intermediate CA)

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

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, for example vpxd or vpxd-extension makes it easy to see which certificate maps to which solution user.

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

If you decide to use a new VMCA root certificate, and you unpublish the VMCA root certificate that was used when you provisioned your environment, you must replace the machine SSL certificates, solution user certificates, and certificates for some internal services.

If you unpublish the VMCA root certificate, you must replace the SSL Signing Certificate that is used by vCenter Single Sign-On. See "Refresh the Security Token Service (STS) Root Certificate," on page 36. You must also replace the VMware Directory Service (vmdir) certificate.

Prerequisites

Request a certificate for vmdir for your third-party or enterprise CA.

Procedure

1 Stop vmdir.

Linux

```
service-control --stop vmdird
```

Windows

```
service-control --stop VMWareDirectoryService
```

2 Copy the certificate and key that you just generated to the vmdir location.

Linux

```
cp vmdir.crt /usr/lib/vmware-vmdir/share/config/vmdircert.pem
cp vmdir.priv /usr/lib/vmware-vmdir/share/config/vmdirkey.pem
```

Windows

```
copy vmdir.crt
C:\programdata\vmware\vCenterServer\cfg\vmdird\vmdircert.pem
copy vmdir.priv
C:\programdata\vmware\vCenterServer\cfg\vmdird\vmdirkey.pem
```

3 Restart vmdir from the vSphere Web Client or using the `service-control` command.

Linux

```
service-control --start vmdird
```

Windows

```
service-control --start VMWareDirectoryService
```

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 6.0, 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 required only if:

- Your environment includes both vCenter Single Sign-On 5.5 and vCenter Single Sign-On 6.0 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 6.0 service runs.

NOTE In most other cases, upgrading the complete environment before restarting the services is best practice. Teplacing the VMware Directory Service certificate is not usually recommended.

Procedure

1 On the node on which the vCenter Single Sign-On 6.0 service runs, replace the vmdird SSL certificate and key.

See "Replace the VMware Directory Service Certificate," on page 88.

2 On the node on which the vCenter Single Sign-On 5.5 service runs, set up the environment so the vCenter Single Sign-On 6.0 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 6.0 node, and rename it to `<sso_node2.domain.com>.pem`, where `<sso_node2.domain.com>` is the FQDN of the 6.0 node.

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

3 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 Third-Party Certificates With vSphere

If company policy requires it, you can replace all certificates used in vSphere with third-party CA-signed certificates. If you do that, VMCA is not in your certificate chain but all vCenter certificates have to be stored 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, in place.

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.

Procedure

1 Request Certificates and Import a Custom Root Certificate on page 91

   If company policy does not allow an intermediate CA, VMCA cannot generate the certificates for you. You use custom certificates from an enterprise or third-party CA.

2 Replace Machine SSL Certificates With Custom Certificates on page 92

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

3 Replace Solution User Certificates With Custom Certificates on page 93

   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 on page 95

   If you decide to use a new VMCA root certificate, and you unpublish the VMCA root certificate that was used when you provisioned your environment, you must replace the machine SSL certificates, solution user certificates, and certificates for some internal services.

5 Replace the VMware Directory Service Certificate in Mixed Mode Environments on page 95

   During upgrade, your environment might temporarily include both vCenter Single Sign-On version 5.5 and vCenter Single Sign-On version 6.0, 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

If company policy does not allow an intermediate CA, VMCA cannot generate the certificates for you. You use custom certificates from an enterprise or third-party CA.

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

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.

   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 certificat, which is the signing certificate from the third-party CA.

```
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 these internal certificates:

- Replace the vCenter Single Sign-On Signing certificate. See "Refresh the Security Token Service (STS) Root Certificate," on page 36.
- Replace the VMware Directory Service certificate. See "Replace the VMware Directory Service Certificate," on page 88.

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 Certificate Authority.

- 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
```

What to do next

You can also replace the certificates for your ESXi hosts. See "Certificate Management for ESXi Hosts," on page 137.

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 Custom Certificates

After you replace the machine SSL certificates, you can replace the VMCA-signed solution user certificates with third-party or enterprise certificates.

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.

Consider whether replacement of solution user certificates is necessary in your environment. Because solution users are located behind a proxy server and the machine SSL certificate is used to secure SSL traffic, the solution user certificates might be less of a security concern.

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

If you decide to use a new VMCA root certificate, and you unpublish the VMCA root certificate that was used when you provisioned your environment, you must replace the machine SSL certificates, solution user certificates, and certificates for some internal services.

If you unpublish the VMCA root certificate, you must replace the SSL Signing Certificate that is used by vCenter Single Sign-On. See "Refresh the Security Token Service (STS) Root Certificate," on page 36. You must also replace the VMware Directory Service (vmdir) certificate.

Prerequisites

Request a certificate for vmdir for your third-party or enterprise CA.

Procedure

1 Stop vmdir.

Linux

```
service-control --stop vmdird
```

Windows

```
service-control --stop VMWareDirectoryService
```

2 Copy the certificate and key that you just generated to the vmdir location.

Linux

```
cp vmdir.crt /usr/lib/vmware-vmdir/share/config/vmdircert.pem
cp vmdir.priv /usr/lib/vmware-vmdir/share/config/vmdirkey.pem
```

Windows

```
copy vmdir.crt
C:\programdata\vmware\vCenterServer\cfg\vmdird\vmdircert.pem
copy vmdir.priv
C:\programdata\vmware\vCenterServer\cfg\vmdird\vmdirkey.pem
```

3 Restart vmdir from the vSphere Web Client or using the `service-control` command.

Linux

```
service-control --start vmdird
```

Windows

```
service-control --start VMWareDirectoryService
```

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 6.0, 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 required only if:

- Your environment includes both vCenter Single Sign-On 5.5 and vCenter Single Sign-On 6.0 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 6.0 service runs.

NOTE In most other cases, upgrading the complete environment before restarting the services is best practice. Teplacing the VMware Directory Service certificate is not usually recommended.

Procedure

1 On the node on which the vCenter Single Sign-On 6.0 service runs, replace the vmdird SSL certificate and key.

See "Replace the VMware Directory Service Certificate," on page 88.

2 On the node on which the vCenter Single Sign-On 5.5 service runs, set up the environment so the vCenter Single Sign-On 6.0 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 6.0 node, and rename it to `<sso_node2.domain.com>.pem`, where `<sso_node2.domain.com>` is the FQDN of the 6.0 node.

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

3 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 Certificates and Services with CLI Commands

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.

Table 3-4. CLI Tools for Managing Certificates and Associated Services

CLI	Description	See
`certool`	Generate and manage certificates and keys. Part of VMCA.	"Managing Certificates in vSphere 6," on page 56 "certool Initialization Commands Reference," on page 98
`vecs-cli`	Manage the contents of VMware Certificate Store instances. Part of VMAFD.	"vecs-cli Command Reference," on page 103
`dir-cli`	Create and update certificates in VMware Directory Service. Part of VMAFD.	"dir-cli Command Reference," on page 106

Certificate Management Tool Locations

By default, you find the tools 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
```

Linux

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

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

If you run commands from a management node with an external Platform Services Controller, you can specify the Platform Services Controller with the `--server` parameter.

Required Privileges for Certificate Management Operations

For most vCenter certificate management operations, you have to be in the CAAdmins group in the vsphere.local domain. The administrator@vsphere.local user is in the CAAdmins group. Some operations are allowed for all users.

If you run the vCenter Certificate Manager utility, you are prompted for the password of administrator@vsphere.local. If you replace certificates manually, different options for the different certificate management CLIs require different privileges.

dir-cli

You must be a member of the CAAdmins group in the vsphere.local domain. You are prompted for a user name and password each time you run a `dir-cli` command.

vecs-cli

Initially, only the store owner has access to a store. The store owner is the Administrator user on Windows systems and the root user on Linux systems. The store owner can provide access to other users.

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 CAAdmins group. The administrator@vsphere.local user is in the CAAdmins group. All users can run the following commands:

- `genselfcacert`
- `initscr`
- `getdc`
- `waitVMDIR`
- `waitVMCA`
- `genkey`
- `viewcert`

For certificate management for ESXi hosts, you must have the **Certificates. Manage Certificates** privilege. You can set that privilege from the vSphere Web Client.

Changing certool Configuration

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

The configuration 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 in the configuration as follows:

- Create a backup of the configuration file and then edit the file. If you are using the default configuration file, you do not have to specify it. Otherwise, for example, if you changed the configuration file name, use the `--config` command-line option.
- Override the configuration file value 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 because the SSL client checks the CN field of the Subject name of the certificate when verifying the machine's host name. Because a machine can have more than one alias, certificates have the Subject Alternative Name field extension where you can specify other names (DNS names, IP addresses, and so on). However, 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.

The `--Hostname` parameter is used to specify the DNSName of 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 certool Configuration," on page 97. See "Replace Existing VMCA-Signed Certificates With New VMCA-Signed Certificates," on page 70 for some usage examples.

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," on page 80.

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 available. 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>`	Optional name of the configuration file. Defaults to `certool.cfg`.
`--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. You can use the certificate to provision machines or solution users.

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.

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

Example:

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

certool --getrootca

Prints the current root CA certificate in human-readable form. 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 VMware Certificate Store (VECS) instances. Use these commands together with `dir-cli` and `certool` to manage your certificate infrastructure.

vecs-cli store create

Creates a certificate store.

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

Example:

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

vecs-cli store delete

Deletes a certificate store. You cannot delete certificate stores that are predefined by the system.

Option	Description
`--name <name>`	Name of the certificate store to delete.

Example:

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

vecs-cli store list

List certificate stores.

VECS includes the following stores.

Table 3-5. 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.
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. The machine store is also included on each Platform Services Controller node.

Table 3-5. Stores in VECS (Continued)

Store	Description
vSphere Certificate Manager Utility backup store (BACKUP_STORE)	Used by VMCA (VMware Certificate Manager) to support certificate revert. Only the most recent state is stored as a backup, you cannot go back more than one step.
Other stores	Other stores might be added by solutions. For example, the Virtual Volumes solution adds an SMS store. Do not modify the certificates in those stores unless VMware documentation or a VMware Knowledge Base artoc;e instructs you to do so. **NOTE** CRLS are not supported in vSphere 6.0 Nevertheless, 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 has all control of its store, including granting and revoking permissions. The administrator 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 entry create

Create 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.

vecs-cli entry list

List all entries in a specified store.

Option	Description
`--store <NameOfStore>`	Name of the certificate store.
`--text`	Displays a human-readable version of the certificate.

vecs-cli entry getcert

Retrieve 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.

vecs-cli entry getkey

Retrieve a key that is stored in 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 for the key.
`--output <output_file_path>`	Output file to write the key to.
`--text`	Displays a human-readable version of the key.

vecs-cli entry delete

Delete 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.

vecs-cli force-refresh

Forces a refresh of `vecs-cli`. When that happens, `vecs-cli` is updated to use the most recent information in vmdir. By default, VECS polls vmdir for new root certificate files every 5 minutes. Use this command for an immediate update of VECS from vmdir.

dir-cli Command Reference

The `dir-cli` utility allows you to create and update solution users, create other user accounts, and manage certificates and passwords in vmdir. Use this utility together with `vecs-cli` and `certool` to manage your certificate infrastructure.

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.
`--login <admin_user_id>`	By default, administrator@vsphere.local. That administrator can add other users to the CAAdmins vCenter Single Sign-On group to give them administrator privileges.
`--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>`	By default, administrator@vsphere.local. That administrator can add other users to the CAAdmins vCenter Single Sign-On group to give them administrator privileges.
`--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>`	By default, administrator@vsphere.local. That administrator can add other users to the CAAdmins vCenter Single Sign-On group to give them administrator privileges.
`--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>`	By default, administrator@vsphere.local. That administrator can add other users to the CAAdmins vCenter Single Sign-On group to give them administrator privileges.
`--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>`	By default, administrator@vsphere.local. That administrator can add other users to the CAAdmins vCenter Single Sign-On group to give them administrator privileges.
`--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>`	By default, administrator@vsphere.local. That administrator can add other users to the CAAdmins vCenter Single Sign-On group to give them administrator privileges.
`--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>`	By default, administrator@vsphere.local. That administrator can add other users to the CAAdmins vCenter Single Sign-On group to give them administrator privileges.
`--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 group exists.
`--login <admin_user_id>`	By default, administrator@vsphere.local. That administrator can add other users to the CAAdmins vCenter Single Sign-On group to give them administrator privileges.
`--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.
`--login <admin_user_id>`	By default, administrator@vsphere.local. That administrator can add other users to the CAAdmins vCenter Single Sign-On group to give them administrator privileges.
`--password <admin_password>`	Password of the administrator user. If you do not specify the password, you are prompted.

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
`--crl <file>`	Path to the CRL file associated with this certificate. Not currently used.
`--login <admin_user_id>`	By default, administrator@vsphere.local. That administrator can add other users to the CAAdmins vCenter Single Sign-On group to give them administrator privileges.
`--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>`	By default, administrator@vsphere.local. That administrator can add other users to the CAAdmins vCenter Single Sign-On group to give them administrator privileges.
`--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 ID is displayed in the `dir-cli trustedcert list` command.
`--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>`	By default, administrator@vsphere.local. That administrator can add other users to the CAAdmins vCenter Single Sign-On group to give them administrator privileges.
`--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>`	By default, administrator@vsphere.local. That administrator can add other users to the CAAdmins vCenter Single Sign-On group to give them administrator privileges.
`--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>`	By default, administrator@vsphere.local. That administrator can add other users to the CAAdmins vCenter Single Sign-On group to give them administrator privileges.
`--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.

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 Select **Administration**, click **Deployment**, and click **System Configuration**.

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, the select the **Manage** tab and the **Settings** subtab.

3 Click **Advanced Settings**, select **Edit**, and filter for threshold.

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

vSphere Permissions and User Management Tasks

4

vCenter Single Sign-On supports authentication, which means it determines whether a user can access vSphere components at all. In addition, each user must be authorized to view or manipulate vSphere objects.

vSphere supports several different authorization mechanisms, discussed in "Understanding Authorization in vSphere," on page 114. The focus of the information in this section is the vCenter Server permission model and how to perform user management tasks.

vCenter Server allows fine-grained control over authorization with permissions and roles. When you assign a permission to an object in the vCenter Server object hierarchy, you specify which user or group has which privileges on that object. To specify the privileges, you use roles, which are sets of privileges.

Initially, only the user administrator@vsphere.local is authorized to log in to the vCenter Server system. That user can then proceed as follows:

1 Add an identity source in which additional users and groups are defined to vCenter Single Sign-On. See "Add a vCenter Single Sign-On Identity Source," on page 31.

2 Give privileges to a user or group by selecting an object such as a virtual machine or a vCenter Server system and assigning a role on that object to the user or group.

Roles, Privileges, and Permissions (http://link.brightcove.com/services/player/bcpid2296383276001?bctid=ref:video_roles_privileges_permissions_vsphere_web_client)

This chapter includes the following topics:

- "Understanding Authorization in vSphere," on page 114
- "Understanding the vCenter Server Permission Model," on page 114
- "Hierarchical Inheritance of Permissions," on page 116
- "Multiple Permission Settings," on page 117
- "Managing Permissions for vCenter Components," on page 119
- "Global Permissions," on page 122
- "Add a Global Permission," on page 123
- "Using Roles to Assign Privileges," on page 123
- "Best Practices for Roles and Permissions," on page 127
- "Required Privileges for Common Tasks," on page 127

Understanding Authorization in vSphere

The primary way of authorizing a user or group in vSphere is the vCenter Server permissions. Depending on the task you want to perform, you might require other authorization.

vSphere 6.0 and later allows privileged users to give other users permissions to perform tasks in the following ways. These approaches are, for the most part, mutually exclusive; however, you can assign use global permissions to authorize certain users for all solution, and local vCenter Server permissions to authorize other users for individual vCenter Server systems.

vCenter Server Permissions

The permission model for vCenter Server systems relies on assigning permissions to objects in the object hierarchy of that vCenter Server. Each permission gives one user or group a set of privileges, that is, a role for a selected object. For example, you can select an ESXi host and assign a role to a group of users to give those users the corresponding privileges on that host.

Global Permissions

Global permissions are applied to a global root object that spans solutions. For example, if both vCenter Server and vCenter Orchestrator are installed, you can give permissions to all objects in both object hierarchies using global permissions.

Global permissions are replicated across the vsphere.local domain. Global permissions to not provide authorization for services managed through vsphere.local groups. See "Global Permissions," on page 122.

Group Membership in vsphere.local Groups

The user administrator@vsphere.local can perform tasks that are associated with services included with the Platform Services Controller. In addition, members of a vsphere.local group can perform the corresponding task. For example, you can perform license management if you are a member of the LicenseService.Administrators group. See "Groups in the vsphere.local Domain," on page 27.

ESXi Local Host Permissions

If you are managing a standalone ESXi host that is not managed by a vCenter Server system, you can assign one of the predefined roles to users. See the *vSphere Single Host Management* documentation.

Understanding the vCenter Server Permission Model

The permission model for vCenter Server systems relies on assigning permissions to objects in the vSphere object hierarchy. Each permission gives one user or group a set of privileges, that is, a role for the selected object.

You need to understand the following concepts:

Permissions

Each object in the vCenter Server object hierarchy has associated permissions. Each permission specifies for one group or user which privileges that group or user has on the object.

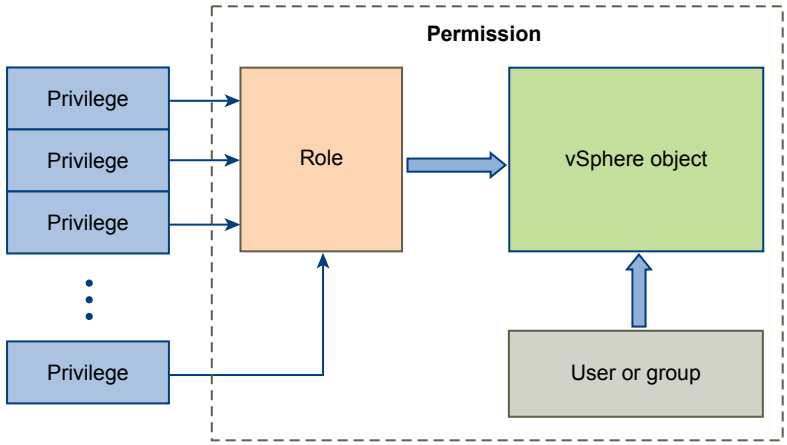
Users and Groups

On vCenter Server systems, you can assign privileges only to authenticated users or groups of authenticated users. Users are authenticated through vCenter Single Sign-On. The users and groups must be defined in the identity source that vCenter Single Sign-On is using to authenticate. Define users and groups using the tools in your identity source, for example, Active Directory.

Roles Roles allow you to assign permissions on an object based on a typical set of tasks that users perform. Default roles, such as Administrator, are predefined on vCenter Server and cannot be changed. Other roles, such as Resource Pool Administrator, are predefined sample roles. You can create custom roles either from scratch or by cloning and modifying sample roles.

Privileges Privileges are fine-grained access controls. You can group those privileges into roles, that you can then map to users or groups.

Figure 4-1. vSphere Permissions



To assign permissions to an object, you follow these steps:

1 Select the object in the vCenter object hierarchy to which you want to apply the permission.

2 Select the group or user that should have privileges on the object.

3 Select the role, that is the set of privileges, that the group or user should have on the object. By default, permissions propagate, that is the group or user has the selected role on the selected object and its child objects.

The permissions model makes it easy to get things done quickly by offering predefined roles. You can also combine privileges to create custom roles. See Chapter 10, "Defined Privileges," on page 233 for a reference to all privileges and the objects to which you can apply the privileges. See "Required Privileges for Common Tasks," on page 127 for some examples of the sets of privileges you need to perform these tasks.

In many cases, permissions must be defined on both a source object and a destination object. For example, if you move a virtual machine, you need some privileges on that virtual machine, but also privileges on the destination data center.

The permissions model for standalone ESXi hosts is simpler. See "Assigning Permissions for ESXi," on page 164

vCenter Server User Validation

vCenter Server systems that use a directory service regularly validate users and groups against the user directory domain. Validation occurs at regular intervals specified in the vCenter Server settings. For example, if user Smith was assigned a role on several objects, and the user's name was changed to Smith2 in the domain , the host concludes that Smith no longer exists and removes permissions associated with that user from the vSphere objects when the next validation occurs.

Similarly, if user Smith is removed from the domain, all permissions associated with that user are removed when the next validation occurs. If a new user Smith is added to the domain before the next validation occurs, the new user Smith is replaces the old user Smith in permissions on any object.

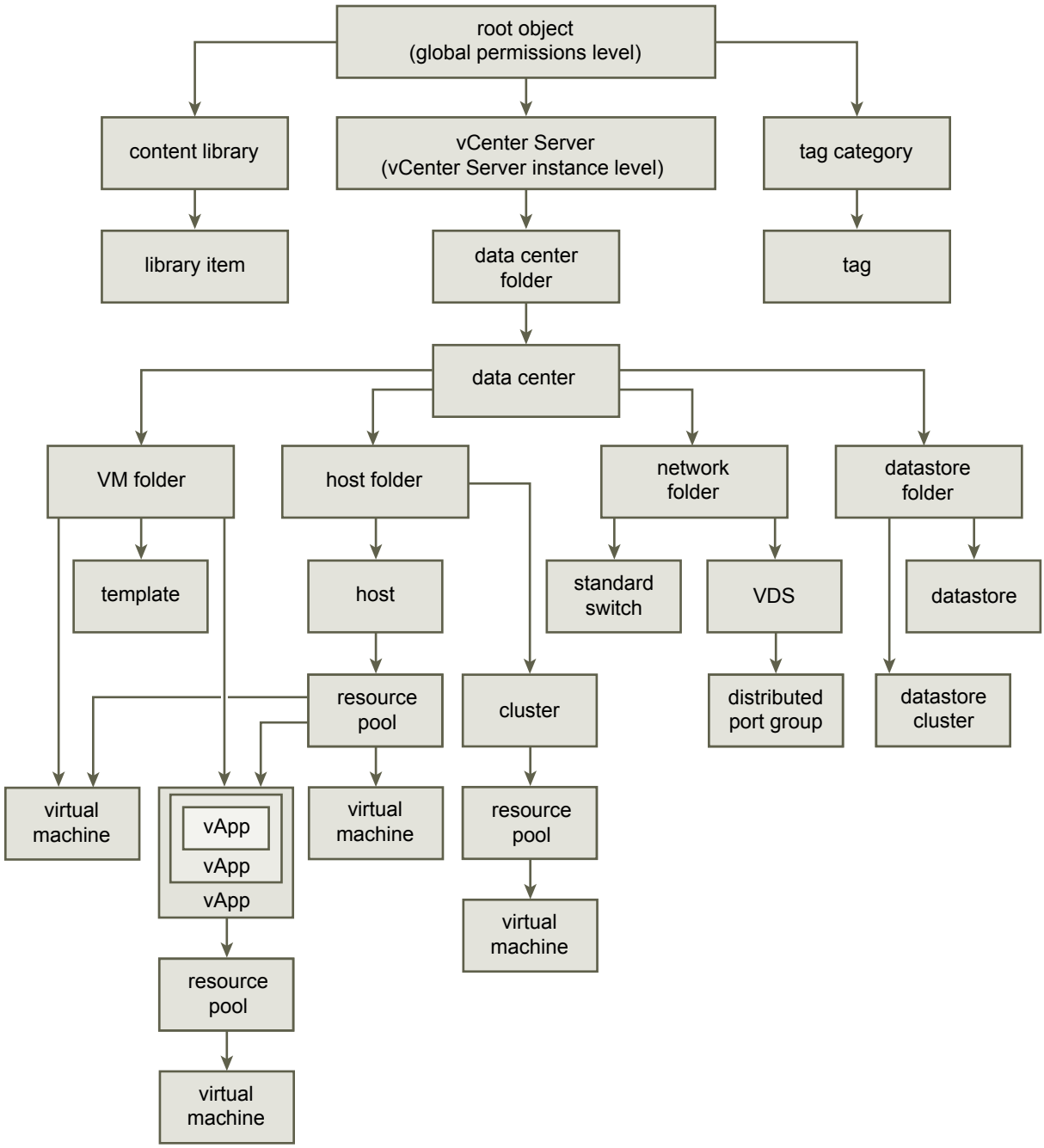
Hierarchical Inheritance of Permissions

When you assign a permission to an object, you can choose whether the permission propagates down the object hierarchy. You set propagation for each permission. Propagation is not universally applied. Permissions defined for a child object always override the permissions that are propagated from parent objects.

The figure illustrates the inventory hierarchy and the paths by which permissions can propagate.

NOTE Global permissions support assigning privileges across solutions from a global root object. See "Global Permissions," on page 122.

Figure 4-2. vSphere Inventory Hierarchy



Most inventory objects inherit permissions from a single parent object in the hierarchy. For example, a datastore inherits permissions from either its parent datastore folder or parent data center. Virtual machines inherit permissions from both the parent virtual machine folder and the parent host, cluster, or resource pool simultaneously.

For example, you can set permissions for a distributed switch and its associated distributed port groups, by setting permissions on a parent object, such as a folder or data center. You must also select the option to propagate these permissions to child objects.

Permissions take several forms in the hierarchy:

Managed entities

Privileged users can define permissions on managed entities.

- Clusters
- Data centers
- Datastores
- Datastore clusters
- Folders
- Hosts
- Networks (except vSphere Distributed Switches)
- Distributed port groups
- Resource pools
- Templates
- Virtual machines
- vSphere vApps

Global entities

You cannot modify permissions on entities that derive permissions from the root vCenter Server system.

- Custom fields
- Licenses
- Roles
- Statistics intervals
- Sessions

Multiple Permission Settings

Objects might have multiple permissions, but only one permission for each user or group. For example, one permission might specify that Group B has Administrator privileges on the object, and another permission might specify that Group B might have Virtual Machine Administrator privileges on the same object.

If an object inherits permissions from two parent objects, the permissions on one object are added to the permissions on the other object. For example, if a virtual machine is in a virtual machine folder and also belongs to a resource pool, that virtual machine inherits all permission settings from both the virtual machine folder and the resource pool.

Permissions applied on a child object always override permissions that are applied on a parent object. See "Example 2: Child Permissions Overriding Parent Permissions," on page 118.

If multiple group permissions are defined on the same object and a user belongs to two or more of those groups, two situations are possible:

- If no permission is defined for the user on that object, the user is assigned the set of privileges assigned to the groups for that object.
- If a permission is defined for the user on that object, the user's permission takes precedence over all group permissions.

Example 1: Inheritance of Multiple Permissions

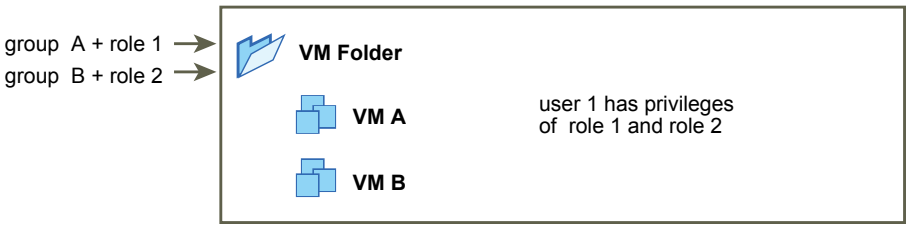
This example illustrates how an object can inherit multiple permissions from groups that are granted permission on a parent object.

In this example, two permissions are assigned on the same object for two different groups.

- Role 1 can power on virtual machines.
- Role 2 can take snapshots of virtual machines.
- Group A is granted Role 1 on VM Folder, with the permission set to propagate to child objects.
- Group B is granted Role 2 on VM Folder, with the permission set to propagate to child objects.
- User 1 is not assigned specific privileges.

User 1, who belongs to groups A and B, logs on. User 1 can both power on and take snapshots of VM A and VM B.

Figure 4-3. Example 1: Inheritance of Multiple Permissions



Example 2: Child Permissions Overriding Parent Permissions

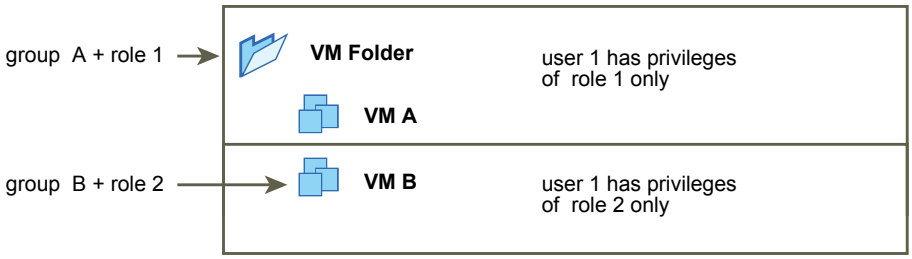
This example illustrates how permissions that are assigned on a child object can override permissions that are assigned on a parent object. You can use this overriding behavior to restrict user access to particular areas of the inventory.

In this example, permissions are defined on two different objects for two different groups.

- Role 1 can power on virtual machines.
- Role 2 can take snapshots of virtual machines.
- Group A is granted Role 1 on VM Folder, with the permission set to propagate to child objects.
- Group B is granted Role 2 on VM B.

User 1, who belongs to groups A and B, logs on. Because Role 2 is assigned at a lower point in the hierarchy than Role 1, it overrides Role 1 on VM B. User 1 can power on VM A, but not take snapshots. User 1 can take snapshots of VM B, but not power it on.

Figure 4-4. Example 2: Child Permissions Overriding Parent Permissions



Example 3: User Role Overriding Group Role

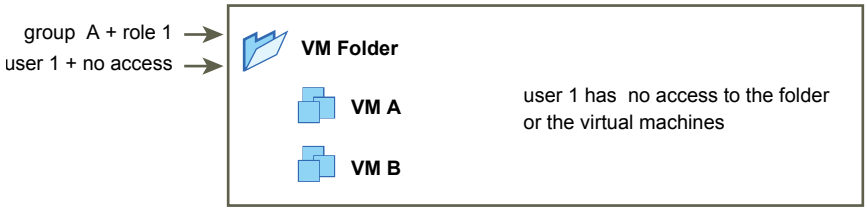
This example illustrates how the role assigned directly to an individual user overrides the privileges associated with a role assigned to a group.

In this example, permissions are defined on the same object. One permission associates a group with a role, the other permission associates an individual user with a role. The user is a member of the group.

- Role 1 can power on virtual machines.
- Group A is granted Role 1 on VM Folder.
- User 1 is granted No Access role on VM Folder.

User 1, who belongs to group A, logs on. The No Access role granted to User 1 on VM Folder overrides the role assigned to the group. User 1 has no access to VM Folder or VMs A and B.

Figure 4-5. Example 3: User Permissions Overriding Group Permissions



Managing Permissions for vCenter Components

A permission is set on an object in the vCenter object hierarchy. Each permission associates the object with a group or user and the group's or user's access roles. For example, you can select a virtual machine object, add one permission that gives the ReadOnly role to Group 1, and add a second permission that gives the Administrator role to User 2.

By assigning a different role to a group of users on different objects, you control the tasks that those users can perform in your vSphere environment. For example, to allow a group to configure memory for the host, select that host and add a permission that grants a role to that group that includes the **Host.Configuration.Memory Configuration** privilege.

To manage permissions from the vSphere Web Client, you need to understand the following concepts:

Permissions	Each object in the vCenter Server object hierarchy has associated permissions. Each permission specifies for one group or user which privileges that group or user has on the object.
Users and Groups	On vCenter Server systems, you can assign privileges only to authenticated users or groups of authenticated users. Users are authenticated through vCenter Single Sign-On. The users and groups must be defined in the identity source that vCenter Single Sign-On is using to authenticate. Define users and groups using the tools in your identity source, for example, Active Directory.
Roles	Roles allow you to assign permissions on an object based on a typical set of tasks that users perform. Default roles, such as Administrator, are predefined on vCenter Server and cannot be changed. Other roles, such as Resource Pool Administrator, are predefined sample roles. You can create custom roles either from scratch or by cloning and modifying sample roles.
Privileges	Privileges are fine-grained access controls. You can group those privileges into roles, that you can then map to users or groups.

You can assign permissions to objects at different levels of the hierarchy, for example, you can assign permissions to a host object or to a folder object that includes all host objects. See "Hierarchical Inheritance of Permissions," on page 116. You can also assign permissions to a global root object to apply the permissions to all object in all solutions. See "Global Permissions," on page 122.

Add a Permission to an Inventory Object

After you create users and groups and define roles, you must assign the users and groups and their roles to the relevant inventory objects. You can assign the same permissions to multiple objects simultaneously by moving the objects into a folder and setting the permissions on the folder.

When you assign permissions from the vSphere Web Client, user and group names must match Active Directory precisely, including case. If you upgraded from earlier versions of vSphere, check for case inconsistencies if you experience problems with groups.

Prerequisites

On the object whose permissions you want to modify, you must have a role that includes the **Permissions.Modify permission** privilege.

Procedure

1. Browse to the object for which you want to assign permissions in the vSphere Web Client object navigator.
2. Click the **Manage** tab and select **Permissions**.
3. Click the Add icon, and click **Add**.
4. Identify the user or group that will have the privileges defined by the selected role.
   a. From the **Domain** drop-down menu, select the domain where the user or group is located.
   b. Type a name in the Search box or select a name from the list.

      The system searches user names, group names, and descriptions.
   c. Select the user or group and click **Add**.

      The name is added to either the **Users** or **Groups** list.

d (Optional) Click **Check Names** to verify that the user or group exists in the identity source.

e Click **OK**.

5 Select a role from the **Assigned Role** drop-down menu.

The roles that are assigned to the object appear in the menu. The privileges contained in the role are listed in the section below the role title.

6 (Optional) To limit propagation, deselect the **Propagate to Child Objects** check box.

The role is applied only to the selected object and does not propagate to the child objects.

7 Click **OK** to add the permission.

Change Permissions

After a user or group and role pair is set for an inventory object, you can change the role paired with the user or group or change the setting of the **Propagate** check box. You can also remove the permission setting.

Procedure

1 Browse to the object in the vSphere Web Client object navigator.

2 Click the **Manage** tab and select **Permissions**.

3 Click the line item to select the user or group and role pair.

4 Click **Change role on permission**.

5 Select a role for the user or group from the **Assigned Role** drop-down menu.

6 To propagate the privileges to the children of the assigned inventory object, click the **Propagate** check box and click **OK**.

Remove Permissions

You can remove permissions on an object in the object hierarchy for individual users or for groups. When you do, the user no longer has the privileges associated with the role on the object.

Procedure

1 Browse to the object in the vSphere Web Client object navigator.

2 Click the **Manage** tab and select **Permissions**.

3 Click the appropriate line item to select the user or group and role pair.

4 Click **Remove permission**.

vCenter Server removes the permission setting.

Change Permission Validation Settings

vCenter Server periodically validates its user and group lists against the users and groups in the user directory. It then removes users or groups that no longer exist in the domain. You can disable validation or change the interval between validations. If you have domains with thousands of users or groups, or if searches take a long time to complete, consider adjusting the search settings.

For vCenter Server versions before vCenter Server 5.0, these settings apply to an Active Directory associated with vCenter Server. For vCenter Server 5.0 and later, these settings apply to vCenter Single Sign-On identity sources.

NOTE This procedure applies only to vCenter Server user lists. ESXi user lists cannot be searched in the same way.

Procedure

1 Browse to the vCenter Server system in the vSphere Web Client object navigator.

2 Select the **Manage** tab and click **Settings**.

3 Click **General** and click **Edit**.

4 Select **User directory**.

5 Change the values as needed.

Option	Description
User directory timeout	Timeout interval in seconds for connecting to the Active Directory server. This value specifies the maximum amount of time vCenter Server allows a search to run on the selected domain. Searching large domains can take a long time.
Query limit	Select the checkbox to set a maximum number of users and groups that vCenter Server displays.
Query limit size	Specifies the maximum number of users and groups that vCenter Server displays from the selected domain in the **Select Users or Groups** dialog box. If you enter 0 (zero), all users and groups appear.

6 Click **OK**.

Global Permissions

Global permissions are applied to a global root object that spans solutions, for example, both vCenter Server and vCenter Orchestrator. Use global permissions to give a user or group privileges for all objects in all object hierarchies.

Each solution has a root object in its own object hierarchy. The global root object acts as a parent object to each solution object. You can assign global permissions to users or groups, and decide on the role for each user or group. The role determines the set of privileges. You can assign a predefined role or create custom roles. See "Using Roles to Assign Privileges," on page 123. It is important to distinguish between vCenter Server permissions and global permissions.

vCenter Server permissions In most cases, you apply a permission to a vCenter Server inventory object such as an ESXi host or a virtual machine. When you do, you specify that a user or group has a set of privileges, called a role, on the object.

Global permissions Global permissions give a user or group privileges to view or manage all objects in each of the inventory hierarchies in your deployment.

If you assign a global and do not select Propagate, the users or groups associated with this permission do not have access to the objects in the hierarchy. They only have access to some global functionality such as creating roles.

IMPORTANT Use global permissions with care. Verify that you really want to assign permissions to all objects in all inventory hierarchies.

Add a Global Permission

You can use global permissions to give a user or group privileges for all objects in all inventory hierarchies in your deployment.

Use global permissions with care. Verify that you really want to assign permissions to all objects in all inventory hierarchies.

Prerequisites

To perform this task, you must have **.Permissions.Modify permission** privileges on the root object for all inventory hierarchies.

Procedure

1 Click **Administration** and select **Global Permissions** in the Access Control area.

2 Click **Manage**, and click the Add permission icon.

3 Identify the user or group that will have the privileges defined by the selected role.

   a From the **Domain** drop-down menu, select the domain where the user or group is located.

   b Type a name in the Search box or select a name from the list.

      The system searches user names, group names, and descriptions.

   c Select the user or group and click **Add**.

      The name is added to either the **Users** or **Groups** list.

   d (Optional) Click **Check Names** to verify that the user or group exists in the identity source.

   e Click **OK**.

4 Select a role from the **Assigned Role** drop-down menu.

   The roles that are assigned to the object appear in the menu. The privileges contained in the role are listed in the section below the role title.

5 Leave the Propagate to children check box selected in most cases.

   If you assign a global and do not select Propagate, the users or groups associated with this permission do not have access to the objects in the hierarchy. They only have access to some global functionality such as creating roles.

6 Click **OK**.

Using Roles to Assign Privileges

A role is a predefined set of privileges. Privileges define rights to perform actions and read properties. For example, the Virtual Machine Administrator role consists of read properties and of a set of rights to perform actions. The role allows a user to read and change virtual machine attributes.

When you assign permissions, you pair a user or group with a role and associate that pairing with an inventory object. A single user or group can have different roles for different objects in the inventory.

For example, if you have two resource pools in your inventory, Pool A and Pool B, you can assign a particular user the Virtual Machine User role on Pool A and the Read Only role on Pool B. These assignments allow that user to turn on virtual machines in Pool A, but to only view virtual machines in Pool B.

vCenter Server provides system roles and sample roles by default:

System roles — System roles are permanent. You cannot edit the privileges associated with these roles.

Sample roles — VMware provides sample roles for certain frequently performed combination of tasks. You can clone, modify or remove these roles.

NOTE To avoid losing the predefined settings in a sample role, clone the role first and make modifications to the clone. You cannot reset the sample to its default settings.

Users can schedule only tasks if they have a role that includes privileges to perform that task at the time the tasks are created.

NOTE Changes to roles and privileges take effect immediately, even if the users involved are logged in. The exception is searches, where changes take effect after the user has logged out and logged back in.

Custom Roles in vCenter Server and ESXi

You can create custom roles for vCenter Server and all object it manages, or for individual hosts.

vCenter Server Custom Roles (Recommended) — Create custom roles by using the role-editing facilities in the vSphere Web Client to create privilege sets that match your needs.

ESXi Custom Roles — You can create custom roles for individual hosts by using a CLI or the vSphere Client. See the *vSphere Single Host Management* documentation. Custom host roles are not accessible from vCenter Server.

If you manage ESXi hosts through vCenter Server, maintaining custom roles in both the host and vCenter Server can result in confusion and misuse. In most cases, defining vCenter Server roles is recommended.

When you manage a host using vCenter Server, the permissions associated with that host are created through vCenter Server and stored on vCenter Server. If you connect directly to a host, only the roles that are created directly on the host are available.

NOTE When you add a custom role and do not assign any privileges to it, the role is created as a Read Only role with three system-defined privileges: **System.Anonymous**, **System.View**, and **System.Read**.

Creating Roles in the vSphere Web Client (http://link.brightcove.com/services/player/bcpid2296383276001?bctid=ref:video_creating_role_in_vsphere_webclient)

vCenter Server System Roles

A role is a predefined set of privileges. When you add permissions to an object, you pair a user or group with a role. vCenter Server includes several system roles, which you cannot change.

vCenter Server System Roles

vCenter Server provides a small number of default roles. You cannot change the privileges associated with the default roles. The default roles are organized as a hierarchy; each role inherits the privileges of the previous role. For example, the Administrator role inherits the privileges of the Read Only role. Roles that you create do not inherit privileges from any of the system roles.

Administrator Role

Users assigned the Administrator role for an object are allowed to view and perform all actions on the object. This role also includes all privileges inherent in the Read Only role. If you are acting in the Administrator role on an object, you can assign privileges to individual users and groups. If you are acting in the Administrator role in vCenter Server, you can assign privileges to users and groups in the default vCenter Single Sign-On identity source. Supported identity services include Windows Active Directory and OpenLDAP 2.4.

By default, the administrator@vsphere.local user has the Administrator role on both vCenter Single Sign-On and vCenter Server after installation. That user can then associate other users with the Administrator role on vCenter Server.

No Access Role

Users assigned the No Access role for an object cannot view or change the object in any way. New users and groups are assigned this role by default. You can change the role on an object-by-object basis.

The administrator@vsphere.local user, the root user, and vpxuser are the only users not assigned the No Access role by default. Instead, they are assigned the Administrator role. You can remove the root user from any permissions or change its role to No Access as long as you first create a replacement permission at the root level with the Administrator role and associate this permission with a different user.

Read Only Role

Users assigned the Read Only role for an object are allowed to view the state of the object and details about the object. With this role, a user can view virtual machine, host, and resource pool attributes. The user cannot view the remote console for a host. All actions through the menus and toolbars are disallowed.

Create a Custom Role

You can create vCenter Server custom roles to suit the access control needs of your environment.

If you create or edit a role on a vCenter Server system that is part of the same vCenter Single Sign-On domain as other vCenter Server systems, the VMware Directory Service (vmdir) propagates the changes that you make to all other vCenter Server systems in the group. Assignments of roles to specific users and objects are not shared across vCenter Server systems.

Prerequisites

Verify that you are logged in as a user with Administrator privileges.

Procedure

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

2 Select Home, click **Administration**, and click **Roles**.

3 Click the **Create role action** (+) button.

4 Type a name for the new role.

5 Select privileges for the role and click **OK**.

Clone a Role

You can make a copy of an existing role, rename it, and edit it. When you make a copy, the new role is not applied to any users or groups and objects. You must assign the role to users or groups and objects.

If you create or edit a role on a vCenter Server system that is part of the same vCenter Single Sign-On domain as other vCenter Server systems, the VMware Directory Service (vmdir) propagates the changes that you make to all other vCenter Server systems in the group. Assignments of roles to specific users and objects are not shared across vCenter Server systems.

Prerequisites

Verify that you are logged in as a user with Administrator privileges.

Procedure

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

2 Select Home, click **Administration**, and click **Roles**.

3 Select a role, and click the **Clone role action** icon.

4 Type a name for the cloned role.

5 Select or deselect privileges for the role and click **OK**.

Edit a Role

When you edit a role, you can change the privileges selected for that role. When completed, these privileges are applied to any user or group that is assigned the edited role.

If you create or edit a role on a vCenter Server system that is part of the same vCenter Single Sign-On domain as other vCenter Server systems, the VMware Directory Service (vmdir) propagates the changes that you make to all other vCenter Server systems in the group. Assignments of roles to specific users and objects are not shared across vCenter Server systems.

Prerequisites

Verify that you are logged in as a user with Administrator privileges.

Procedure

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

2 Select Home, click **Administration**, and click **Roles**.

3 Select a role and click the **Edit role action** button.

4 Select or deselect privileges for the role and click **OK**.

Best Practices for Roles and Permissions

Use best practices for roles and permissions to maximize the security and manageability of your vCenter Server environment.

VMware recommends the following best practices when configuring roles and permissions in your vCenter Server environment:

- Where possible, assign a role to a group rather than individual users to grant privileges to that group.
- Grant permissions only on the objects where they are needed, and assign privileges only to users or groups that must have them. Using the minimum number of permissions makes it easier to understand and manage your permissions structure.
- If you assign a restrictive role to a group, check that the group does not contain the Administrator user or other users with administrative privileges. Otherwise, you could unintentionally restrict administrators' privileges in parts of the inventory hierarchy where you have assigned that group the restrictive role.
- Use folders to group objects. For example, if you want to grant modify permission on one set of hosts and view permission on another set of hosts, place each set of hosts in a folder.
- Use caution when adding a permission to the root vCenter Server objects. Users with privileges at the root level have access to global data on vCenter Server, such as roles, custom attributes, vCenter Server settings.
- In most cases, enable propagation when you assign permissions to an object. This ensures that when new objects are inserted in to the inventory hierarchy, they inherit permissions and are accessible to users.
- Use the No Access role to mask specific areas of the hierarchy if you do not want for certain users or groups to have access to the objects in that part of the object hierarchy.
- Changes to licenses propagate to all vCenter Server systems that are linked to the same Platform Services Controller or to Platform Services Controllers in the same vCenter Single Sign-On domain, even if the user does not have privileges on all of the vCenter Server systems.

Required Privileges for Common Tasks

Many tasks require permissions on more than one object in the inventory. You can review the privileges that are required to perform the tasks and, where applicable, the appropriate sample roles.

The table below lists common tasks that require more than one privilege. You can add permissions to inventory objects by pairing a user with one of the predefined roles, or you can create custom roles with the set of privileges that you expect to use multiple times.

If the task that you want to perform is not in this table, the following rules can help you determine where you must assign permissions to allow particular operations:

- Any operation that consumes storage space, such as creating a virtual disk or taking a snapshot, requires the **Datastore.Allocate Space** privilege on the target datastore, as well as the privilege to perform the operation itself.
- Moving an object in the inventory hierarchy requires appropriate privileges on the object itself, the source parent object (such as a folder or cluster), and the destination parent object.
- Each host and cluster has its own implicit resource pool that contains all the resources of that host or cluster. Deploying a virtual machine directly to a host or cluster requires the **Resource.Assign Virtual Machine to Resource Pool** privilege.

Table 4-1. Required Privileges for Common Tasks

Task	Required Privileges	Applicable Role
Create a virtual machine	On the destination folder or data center: ■ **Virtual machine.Inventory.Create new** ■ **Virtual machine.Configuration.Add new disk** (if creating a new virtual disk) ■ **Virtual machine.Configuration.Add existing disk** (if using an existing virtual disk) ■ **Virtual machine.Configuration.Raw device** (if using an RDM or SCSI pass-through device)	Administrator
	On the destination host, cluster, or resource pool: **Resource.Assign virtual machine to resource pool**	Resource pool administrator or Administrator
	On the destination datastore or folder containing a datastore: **Datastore.Allocate space**	Datastore Consumer or Administrator
	On the network that the virtual machine will be assigned to: **Network.Assign network**	Network Consumer or Administrator
Deploy a virtual machine from a template	On the destination folder or data center: ■ **Virtual machine .Inventory.Create from existing** ■ **Virtual machine.Configuration.Add new disk**	Administrator
	On a template or folder of templates: **Virtual machine.Provisioning.Deploy template**	Administrator
	On the destination host, cluster or resource pool: **Resource.Assign virtual machine to resource pool**	Administrator
	On the destination datastore or folder of datastores: **Datastore.Allocate space**	Datastore Consumer or Administrator
	On the network that the virtual machine will be assigned to: **Network.Assign network**	Network Consumer or Administrator
Take a virtual machine snapshot	On the virtual machine or a folder of virtual machines: **Virtual machine.Snapshot management. Create snapshot**	Virtual Machine Power User or Administrator
	On the destination datastore or folder of datastores: **Datastore.Allocate space**	Datastore Consumer or Administrator
Move a virtual machine into a resource pool	On the virtual machine or folder of virtual machines: ■ **Resource.Assign virtual machine to resource pool** ■ **Virtual machine.Inventory.Move**	Administrator
	On the destination resource pool: **Resource.Assign virtual machine to resource pool**	Administrator

Table 4-1. Required Privileges for Common Tasks (Continued)

Task	Required Privileges	Applicable Role
Install a guest operating system on a virtual machine	On the virtual machine or folder of virtual machines: ■ **Virtual machine.Interaction.Answer question** ■ **Virtual machine.Interaction.Console interaction** ■ **Virtual machine.Interaction.Device connection** ■ **Virtual machine.Interaction.Power Off** ■ **Virtual machine.Interaction.Power On** ■ **Virtual machine.Interaction.Reset** ■ **Virtual machine.Interaction.Configure CD media** (if installing from a CD) ■ **Virtual machine.Interaction.Configure floppy media** (if installing from a floppy disk) ■ **Virtual machine.Interaction.VMware Tools install**	Virtual Machine Power User or Administrator
	On a datastore containing the installation media ISO image: **Datastore.Browse datastore** (if installing from an ISO image on a datastore) On the datastore to which you upload the installation media ISO image: ■ **Datastore.Browse datastore** ■ **Datastore.Low level file operations**	Virtual Machine Power User or Administrator
Migrate a virtual machine with vMotion	On the virtual machine or folder of virtual machines: ■ **Resource.Migrate powered on virtual machine** ■ **Resource.Assign Virtual Machine to Resource Pool** (if destination is a different resource pool from the source)	Resource Pool Administrator or Administrator
	On the destination host, cluster, or resource pool (if different from the source): **Resource.Assign virtual machine to resource pool**	Resource Pool Administrator or Administrator
Cold migrate (relocate) a virtual machine	On the virtual machine or folder of virtual machines: ■ **Resource.Migrate powered off virtual machine** ■ **Resource.Assign virtual machine to resource pool** (if destination is a different resource pool from the source)	Resource Pool Administrator or Administrator
	On the destination host, cluster, or resource pool (if different from the source): **Resource.Assign virtual machine to resource pool**	Resource Pool Administrator or Administrator
	On the destination datastore (if different from the source): **Datastore.Allocate space**	Datastore Consumer or Administrator
Migrate a virtual machine with Storage vMotion	On the virtual machine or folder of virtual machines: **Resource.Migrate powered on virtual machine**	Resource Pool Administrator or Administrator
	On the destination datastore: **Datastore.Allocate space**	Datastore Consumer or Administrator
Move a host into a cluster	On the host: **Host.Inventory.Add host to cluster**	Administrator
	On the destination cluster: **Host.Inventory.Add host to cluster**	Administrator

Securing ESXi Hosts

5

The ESXi hypervisor architecture has many built-in security features such as CPU isolation, memory isolation, and device isolation. You can configure additional features such as lockdown mode, certificate replacement, and smart card authentication for enhanced security.

An ESXi host is also protected with a firewall. You can open ports for incoming and outgoing traffic as needed, but should restrict access to services and ports. Using the ESXi lockdown mode and limiting access to the ESXi Shell can further contribute to a more secure environment. Starting with vSphere 6.0, ESXi hosts participate in the certificate infrastructure. Hosts are provisioned with certificate that are signed by the VMware Certificate Authority (VMCA) by default.

See the VMware white paper *Security of the VMware vSphere Hypervisor* for additional information on ESXi security.

This chapter includes the following topics:

- "Use Scripts to Manage Host Configuration Settings," on page 132
- "Configure ESXi Hosts with Host Profiles," on page 133
- "General ESXi Security Recommendations," on page 133
- "Certificate Management for ESXi Hosts," on page 137
- "Customizing Hosts with the Security Profile," on page 150
- "Assigning Permissions for ESXi," on page 164
- "Using Active Directory to Manage ESXi Users," on page 166
- "Using vSphere Authentication Proxy," on page 169
- "Configuring Smart Card Authentication for ESXi," on page 173
- "ESXi SSH Keys," on page 175
- "Using the ESXi Shell," on page 177
- "Modifying ESXi Web Proxy Settings," on page 181
- "vSphere Auto Deploy Security Considerations," on page 182
- "Managing ESXi Log Files," on page 182
- "ESXi Security Best Practices," on page 185

Use Scripts to Manage Host Configuration Settings

In environments with many hosts, managing hosts with scripts is faster and less error prone than managing the hosts from the vSphere Web Client.

vSphere includes several scripting languages for host management. See the *vSphere Command-Line Documentation* and the *vSphere API/SDK Documentation* for reference information and programming tips and VMware Communities for additional tips about scripted management. The vSphere Administrator documentation focuses on using the vSphere Web Client for management.

vSphere PowerCLI

VMware vSphere PowerCLI provides a Windows PowerShell interface to the vSphere API. vSphere PowerCLI includes PowerShell cmdlets for administering vSphere components.

vSphere PowerCLI includes more than 200 cmdlets, a set of sample scripts, and a function library for management and automation. See the *vSphere PowerCLI Documentation*.

vSphere Command-Line Interface (vCLI)

vCLI includes a set of commands for managing ESXi hosts and virtual machines. The installer, which also installs the vSphere SDK for Perl, runs Windows or Linux systems and installs ESXCLI commands, vicfg- commands, and a set of other vCLI commands. See *vSphere Command-Line Interface Documentation*.

Starting with vSphere 6.0, you can also use one of the scripting interfaces to the vCloud Suite SDK such as the vCloud Suite SDK for Python. Functionality of those interfaces is fairly limited in vSphere 6.0.

Procedure

1 Create a custom role that has limited privileges.

   For example, consider creating a role that has a set of privileges for managing hosts but no privileges for managing virtual machines, storage, or networking. If the script you want to use only extracts information, you can create a role with read-only privileges for the host.

2 From the vSphere Web Client, create a service account and assign it the custom role.

   You can create multiple custom roles with different levels of access if you want access to certain hosts to be fairly limited.

3 Write scripts to perform parameter checking or modification, and run them.

For example, you can check or set the shell interactive timeout of a host as follows:

Language	Commands
vCLI (ESXCLI)	`esxcli <conn_options> system settings advanced get /UserVars/ESXiShellTimeOut` `esxcli --formatter=csv --format-param=fields="Path,Int Value" system settings advanced list | grep /UserVars/ESXiShellTimeOut`

PowerCLI	`List UserVars.ESXiShellInteractiveTimeOut for each host`
	`Get-VMHost | Select Name, @{N="UserVars.ESXiShellInteractiveTimeOut";E={$_ | Get-VMHostAdvancedConfiguration UserVars.ESXiShellInteractiveTimeOut | Select -ExpandProperty Values}}`
	`# Set UserVars.ESXiShellTimeOut to 900 on all hosts`
	`Get-VMHost | Foreach { Set-VMHostAdvancedConfiguration -VMHost $_ -Name UserVars.ESXiShellTimeOut -Value 900 }`

4 In large environments, create roles with different access privileges and group hosts into folders according to the tasks you want to perform, then run different scripts over different folders from different service accounts.

5 Be sure to verify that the changes happened as needed after you run the command.

Configure ESXi Hosts with Host Profiles

Host profiles allow you to set up standard configurations for your ESXi hosts and automate compliance to these configuration settings. Host profiles allow you to control many aspects of host configuration including memory, storage, networking, and so on.

You can configure host profiles for a reference host from the vSphere Web Client and apply the host profile to all hosts that share the characteristics of the reference host. You can also use host profiles to monitor hosts for host configuration changes. See the *vSphere Host Profiles* documentation.

You can attach the host profile to a cluster to apply it to all hosts in the cluster.

Procedure

1 Set up the reference host to specification and create a host profile.

2 Attach the profile to a host or cluster.

3 Apply the host profile of the reference host to other hosts or clusters.

General ESXi Security Recommendations

To protect an ESXi host against unauthorized intrusion and misuse, VMware imposes constraints on several parameters, settings, and activities. You can loosen the constraints to meet your configuration needs. If you do, make sure that you are working in a trusted environment and that you have taken enough other security measures to protect the network as a whole and the devices connected to the host.

Built-in Security Features

Risks to the hosts are mitigated out of the box as follows:

■

- ESXi Shell and SSH disabled by default.
- Only a limited number of firewall ports are open by default. You can explicitly open additional firewall ports that are associated with specific services.
- ESXi runs only services that are essential to managing its functions. The distribution is limited to the features required to run ESXi.
- By default, all ports not specifically required for management access to the host are closed. You must specifically open ports if you need additional services.
- By default, weak ciphers are disabled and communications from clients are secured by SSL. The exact algorithms used for securing the channel depend on the SSL handshake. Default certificates created on ESXi use PKCS#1 SHA-256 With RSA encryption as the signature algorithm.
- The Tomcat Web service, used internally by ESXi to support access by Web clients, has been modified to run only those functions required for administration and monitoring by a Web client. As a result, ESXi is not vulnerable to the Tomcat security issues reported in broader use.
- VMware monitors all security alerts that could affect ESXi security and issues a security patch if needed.
- Insecure services such as FTP and Telnet are not installed, and the ports for these services are closed by default. Because more secure services such as SSH and SFTP are easily available, avoid using these insecure services in favor of their safer alternatives. For example, use Telnet with SSL to access virtual serial ports if SSH is unavailable and you must use Telnet.

  If you must use insecure services and have implemented sufficient protection for the host, you can explicitly open ports to support them.

Additional Security Measures

Consider the following recommendations when evaluating host security and administration.

Limit access

If you decide to enable access to the Direct Console User Interface (DCUI) the ESXi Shell, or SSH, enforce strict access security policies.

The ESXi Shell has privileged access to certain parts of the host. Provide only trusted users with ESXi Shell login access.

Do not access managed hosts directly

Use the vSphere Web Client to administer ESXi hosts that are managed by a vCenter Server. Do not access managed hosts directly with the vSphere Client, and do not make changes to managed hosts from the host's DCUI.

If you manage hosts with a scripting interface or API, do not target the host directly. Instead, target the vCenter Server system that manages the host and specify the host name.

Use the vSphere Client or VMware CLIs or APIs to administer standalone ESXi hosts

Use the vSphere Client, one of the VMware CLIs or APIs to administer your ESXi hosts. Access the host from the DCUI or the ESXi Shell as the root user only for troubleshooting. If you decide to use the ESXi Shell, limit the accounts with access and set timeouts.

Use only VMware sources to upgrade ESXi components.

The host runs a variety of third-party packages to support management interfaces or tasks that you must perform. VMware does not support upgrading these packages from anything other than a VMware source. If you use a download or patch from another source, you might compromise management interface security or functions. Regularly check third-party vendor sites and the VMware knowledge base for security alerts.

NOTE Follow the VMware security advisories at http://www.vmware.com/security/.

ESXi Passwords, ESXi Pass Phrases, and Account Lockout

For ESXi hosts, you can use a password or a pass phrase. In each case, you must make sure the password or pass phrase meets the requirements.

ESXi uses the Linux PAM module `pam_passwdqc` for password management and control. See the manpages for `pam_passwdqc` for detailed information.

ESXi Passwords

ESXi enforces password requirements for direct access from the Direct Console User Interface, the ESXi Shell, SSH, or the vSphere Client. When you create a password, include a mix of characters from four character classes: lowercase letters, uppercase letters, numbers, and special characters such as underscore or dash.

Starting with vSphere 6.0, your user password must meet the following requirements. See *Example ESXi Passwords* below.

- Passwords must contain characters from at least three character classes.
- Passwords containing characters from three character classes must be at least seven characters long.
- Passwords containing characters from all four character classes must be at least seven characters long.

NOTE An uppercase character that begins a password does not count toward the number of character classes used. A number that ends a password does not count toward the number of character classes used.

The password cannot contain a dictionary word or part of a dictionary word.

Example ESXi Passwords

The following password candidates meet ESXi requirements.

- xQaTEhb!: Contains eight characters from three character classes.
- xQaT3#A: Contains seven characters from four character classes.

The following password candidates do not meet ESXi requirements.

- Xqat3h?: Begins with an uppercase character, reducing the effective number of character classes to two. The minimum number of supported character classes is three.
- xQaTEh2: Ends with a number, reducing the effective number of character classes to two. The minimum number of supported character classes is three.

ESXi Pass Phrase

Instead of a password, you can also use a pass phrase, however, pass phrases are disabled by default. You can change this default or other settings, by using the `Security.PasswordQualityControl` advanced option for your ESXi host from the vSphere Web Client.

For example, you can change the option to the following:

```
retry=3 min=disabled,disabled,16,7,7
```

This example allows pass phrases of at least 16 characters and at least 3 words, separated by spaces.

Making changes to the `/etc/pamd/passwd` file is still supported for legacy hosts but is deprecated for future releases.

Changing Default Password or Pass Phrase Restrictions

You can change the default restriction on passwords or pass phrases by using the `Security.PasswordQualityControl` advanced option for your ESXi host. By default, this option is set as follows:

```
retry=3 min=disabled,disabled,disabled,7,7
```

You can change the default, for example, to require a minimum of 15 characters and a minimum number of four words, as follows:

```
retry=3 min=disabled,disabled,15,7,7 passphrase=4
```

See the manpage for `pam_passwdqc` for more information.

NOTE Not all possible combinations of the options for `pam_passwdqc` have been tested. Perform additional testing after you make changes to the default password settings.

See the *vCenter Server and Host Management* documentation for information on setting ESXi advanced options.

ESXi Account Lockout Behavior

Starting with vSphere 6.0, account locking is supported for access through SSH and through the vSphere Web Services SDK. The Direct Console Interface (DCUI) and the ESXi Shell do not support account lockout. By default, a maximum of ten failed attempts is allowed before the account is locked. The account is unlocked after two minutes by default.

You can configure the login behavior with the following advanced options:

- `Security.AccountLockFailures`. Maximum number of failed login attempts before a user's account is locked. Zero disables account locking.
- `Security.AccountUnlockTime`. Number of seconds that a user is locked out.

See the *vCenter Server and Host Management* documentation for information on setting advanced options.

ESXi Networking Security Recommendations

Isolation of network traffic is essential to a secure ESXi environment. Different networks require different access and level of isolation.

Your ESXi host uses several networks. Use appropriate security measures for each network, and isolate traffic for specific applications and functions. For example, ensure that vSphere vMotion traffic does not travel over networks where virtual machines are located. Isolation prevents snooping. Having separate networks also is recommended for performance reasons.

- vSphere infrastructure networks are used for features such as VMware vSphere vMotion®, VMware vSphere Fault Tolerance, and storage. These networks are considered to be isolated for their specific functions and often are not routed outside a single physical set of server racks.
- A management network isolates client traffic, command-line interface (CLI) or API traffic, and third-party software traffic from normal traffic. This network should be accessible only by system, network, and security administrators. Use jump box or virtual private network (VPN) to secure access to the management network. Strictly control access within this network to potential sources of malware.
- Virtual machine traffic can flow over one or many networks. You can enhance the isolation of virtual machines by using virtual firewall solutions that set firewall rules at the virtual network controller. These settings travel with a virtual machine as it migrates from host to host within your vSphere environment.

Disable the Managed Object Browser (MOB)

The managed object browser provides a way to explore the VMkernel object model. However, attackers can use this interface to perform malicious configuration changes or actions because ou can change the host configuration by using the managed object browser. Use the Managed Object Browser only for debugging, and ensure that it is disabled in production systems.

Procedure

1 Select the host in the vSphere Web Client and go to **Advanced System Settings**.

2 Check the value of **Config.HostAgent.plugins.solo.enableMob**, and change it as appropriate.

Using `vim-cmd` from the ESXi Shell is no longer recommended.

Disable Authorized (SSH) Keys

Authorized keys allow you to enable access to an ESXi host through SSH without requiring user authentication. To increase host security, do not allow users to access a host using authorized keys.

A user is considered trusted if their public key is in the `/etc/ssh/keys-root/authorized_keys` file on a host. Trusted remote users are allowed to access the host without providing a password.

Procedure

- For day-to-day operations, disable SSH on ESXi hosts.
- If SSH is enabled, even temporarily, monitor the contents of the `/etc/ssh/keys-root/authorized_keys` file to ensure that no users are allowed to access the host without proper authentication.
- Monitor the `/etc/ssh/keys-root/authorized_keys` file to verify that it is empty and no SSH keys have been added to the file.
- If you find that the `/etc/ssh/keys-root/authorized_keys` file is not empty, remove any keys.

Disabling remote access with authorized keys might limit your ability to run commands remotely on a host without providing a valid login. For example, this can prevent you from running an unattended remote script.

Certificate Management for ESXi Hosts

In vSphere 6.0 and later, the VMware Certificate Authority (VMCA) provisions each new ESXi host with a signed certificate that has VMCA as the root certificate authority by default. Provisioning happens when the host is added to vCenter Server explicitly or as part of installation or upgrade to ESXi 6.0 or later.

You can view and manage these certificates from the vSphere Web Client and by using the `vim.CertificateManager` API in the vSphere Web Services SDK. You cannot view or manage ESXi certificates by using certificate managment CLIs that are available for managing vCenter Server certificates.

Certificates in vSphere 5.5 and in vSphere 6.0

When ESXi and vCenter Server communicate, they use SSL for almost all management traffic.

In vSphere 5.5 and earlier, the SSL endpoints are secured only by a combination of user name, password, and thumbprint. Users can replace the corresponding self-signed certificates with their own certificates. See the vSphere 5.5 Documentation Center.

In vSphere 6.0 and later, vCenter Server supports the following certificate modes for ESXi hosts.

Table 5-1. Certificate Modes for ESXi Hosts

Certificate Mode	Description
VMware Certificate Authority (default)	Use this mode if VMCA provisions all ESXi hosts, either as the top-level CA or as an intermediary CA. By default, VMCA provisions ESXi hosts with certificates. In this mode, you can refresh and renew certificates from the vSphere Web Client.
Custom Certificate Authority	Use this mode if you want to use only custom certificates that are signed by a third-party CA. In this mode, you are responsible for managing the certificates. You cannot refresh and renew certificates from the vSphere Web Client. NOTE Unless you change the certificate mode to Custom Certificate Authority, VMCA might replace custom certificates, for example, when you select **Renew** in the vSphere Web Client.
Thumbprint Mode	vSphere 5.5 used thumbprint mode, and this mode is still available as a fallback option for vSphere 6.0. In this mode, vCenter Server checks that the certificate is formatted correctly, but does not check the validity of the certificate. Even expired certificates are accepted. Do not use this mode unless you encounter problems that you cannot resolve with one of the other two modes. Some vCenter 6.0 and later services might not work correctly in thumbprint mode.

Certificate Expiration

Starting with vSphere 6.0, you can view information about certificate expiration for certificates that are signed by VMCA or a third-party CA in the vSphere Web Client. You can view the information for all hosts that are managed by a vCenter Server or for individual hosts. A yellow alarm is raised if the certificate is in the **Expiring Shortly** state (less than 8 months). A red alarm is raised if the certificate is in the **Expiration Imminent** state (less than 2 months).

ESXi Provisioning and VMCA

When you boot an ESXi host from installation media, the host initially has an autogenerated certificate. When the host is added to the vCenter Server system, it is provisioned with a certificate that is signed by VMCA as the root CA.

The process is similar for hosts that are provisioned with Auto Deploy. However, because those host do not store any state, the signed certificate is stored by the Auto Deploy server in its local certificate store. The certificate is reused upon subsequent boots of the ESXi hosts. An Auto Deploy server is part of any embedded deployment or management node.

If VMCA is not available when an Auto Deploy host boots the first time, the host first attempts to connect, and then cycles through shut down and reboot until VMCA becomes available and the host can be provisioned with a signed certificate.

Host Name and IP Address Changes

In vSphere 6.0 and later, a host name or IP address change might affect whether vCenter Server considers a host's certificate valid. How you added the host to vCenter Server affects whether manual intervention is necessary. Manual intervention means that you either reconnect the host, or you remove the host from vCenter Server and add it back.

Table 5-2. When Host Name or IP Address Changes Require Manual Intervention

Host added to vCenter Server using...	Host name changes	IP address changes
Host name	vCenter Server connectivity problem. Manual intervention required.	No intervention required.
IP address	No intervention required.	vCenter Server connectivity problem. Manual intervention required.

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

Host Upgrades and Certificates

If you upgrade an ESXi host to ESXi 6.0 or later, the upgrade process replaces self-signed certificates with VMCA-signed certificates. The process retains custom certificates even if those certificates are expired or invalid.

The recommended upgrade workflow depends on the current certificates.

Host Provisioned with Thumbprint Certificates

If your host is currently using thumbprint certificates, it is automatically assigned VMCA certificates as part of the upgrade process.

NOTE You cannot provision legacy hosts with VMCA certificates. You must upgrade to ESXi 6.0 or later.

Host Provisioned with Custom Certificates

If your host is provisioned with custom certificates, usually third-party CA-signed certificates, those certificates remain in place. Change the certificate mode to Custom to ensure that the certificates are not replaced accidentally.

NOTE If your environment is in VMCA mode, and you refresh the certificates from the vSphere Web Client, any existing certificates are replaced with certificates that are signed by VMCA.

Going forward, vCenter Server monitors the certificates and displays information, for example, about certificate expiration, in the vSphere Web Client.

If you decide not to upgrade your hosts to vSphere 6.0 or later, the hosts retain the certificates that they are currently using even if the host is managed by a vCenter Server system that uses VMCA certificates.

Hosts that are being provisioned by Auto Deploy are always assigned new certificates when they are first booted with ESXi 6.0 software. When you upgrade a host that is provisioned by Auto Deploy, the Auto Deploy server generates a certificate signing request (CSR) for the host and submits it to VMCA. VMCA stores the signed certificate for the host. When the Auto Deploy server provisions the host, it retrieves the certificate from VMCA and includes it as part of the provisioning process.

You can use Auto Deploy with custom certificates.

See "Use Custom Certificates with Auto Deploy," on page 148.

ESXi Certificate Default Settings

When vCenter Server requests a Certificate Signing Request (CSR) from an ESXi host, it uses default settings. Most of the default values are well suited for many situations, but company-specific information can be changed.

Consider changing the organization, and location information. You can change many of the default settings using the vSphere Web Client. See "Change Certificate Default Settings," on page 142.

Table 5-3. CSR Settings

Parameter	Default Value	Advanced Option
Key Size	2048	N.A.
Key Algorithm	RSA	N.A.
Certificate Signature Algorithm	sha256WithRSAEncryption	N.A.
Common Name	Name of the host if the host was added to vCenter Server by host name. IP address of the host if the host was added to vCenter Server by IP address.	N.A.
Country	USA	vpxd.certmgmt.certs.cn.country
Email address	vmca@vmware.com	vpxd.certmgmt.certs.cn.email
Locality (City)	Palo Alto	vpxd.certmgmt.certs.cn.localityName
Organization Unit Name	VMware Engineering	vpxd.certmgmt.certs.cn.organizationalUnitName
Organization Name	VMware	vpxd.certmgmt.certs.cn.organizationName
State or province	California	vpxd.certmgmt.certs.cn.state
Number of days the certificate is valid.	1825	vpxd.certmgmt.certs.cn.daysValid
Hard threshold for certificate expiration. vCenter Server raises a red alarm when this threshold is reached.	30 days	vpxd.certmgmt.certs.cn.hardThreshold
Poll interval for vCenter Server certificate validity checks.	5 days	vpxd.certmgmt.certs.cn.pollIntervalDays
Soft Threshold for certificate expiration. vCenter Server raises an event when this threshold is reached.	240 days	vpxd.certmgmt.certs.cn.softThreshold
Mode that vCenter Server users to determine whether existing certificates are replaced. Change this mode to retain custom certificates during upgrade. See "Host Upgrades and Certificates," on page 139.	Default is vmca You can also specify thumbprint or custom. See "Change the Certificate Mode," on page 144.	vpxd.certmgmt.mode

View Certificate Expiration Information for Multiple ESXi Hosts

If you are using ESXi 6.0 and later, you can view the certificate status of all hosts that are managed by your vCenter Server system. The display allows you to determine whether any of the certificates expire soon.

You can view certificate status information for hosts that are using VMCA mode and for hosts that are using custom mode in the vSphere Web Client. You cannot view certificate status information for hosts in thumbprint mode.

Procedure

1 Browse to the host in the vSphere Web Client inventory hierarchy.

By default, the Hosts display does not include the certificate status.

2 Right-click the Name field and select **Show/Hide Columns**.

3 Select **Certificate Valid To**, click **OK**, and scroll to the right if necessary.

The certificate information displays when the certificate expires.

If a host is added to vCenter Server or reconnected after a disconnect, vCenter Server renews the certificate if the status is Expired, Expiring, Expiring shortly, or Expiration imminent. The status is Expiring if the certificate is valid for less than eight months, Expiring shortly if the certificate is valid for less than two months, and Expiration imminent if the certificate is valid for less than one month.

4 (Optional) Deselect other columns to make it easier to see what you are interested in.

What to do next

Renew the certificates that are about to expire. See "Renew or Refresh ESXi Certificates," on page 141.

View Certificate Details for a Single ESXi Host

For ESXi 6.0 and later hosts that are in VMCA mode or custom mode, you can view certificate details from the vSphere Web Client. The information about the certificate can be helpful for debugging.

Procedure

1 Browse to the host in the vSphere Web Client inventory.

2 Click the **Manage** tab and click **Settings**.

3 Select **System**, and click **Certificate**.

You can examine the following information. This information is available only in the single-host view.

Field	Description	
Subject	The subject used during certificate generation.	
Issuer	The issuer of the certificate.	
Valid From	Date on which the certificate was generated.	
Valid To	Date on which the certificate expires.	
Status	Status of the certificate, one of the following.	
	Good	Normal operation.
	Expiring	Certificate will expire soon.
	Expiring shortly	Certificate is 8 months or less away from expiration (Default).
	Expiration imminent	Certificate is 2 months or less away from expiration (Default).
	Expired	Certificate is not valid because it expired.

Renew or Refresh ESXi Certificates

If VMCA assigns certificates to your ESXi hosts (6.0 and later), you can renew those certificates from the vSphere Web Client. You can also refresh all certificates from the TRUSTED_ROOTS store associated with vCenter Server.

You can renew your certificates when they are about to expire, or if you want to provision the host with a new certificate for other reasons. If the certificate is already expired, you must disconnect the host and reconnect it.

By default, vCenter Server renews the certificates of a host with status Expired, Expiring immediately, or Expiring each time the host is added to the inventory, or reconnected.

Procedure

1 Browse to the host in the vSphere Web Client inventory.

2 Click the **Manage** tab and click **Settings**.

3 Select **System**, and click **Certificate**.

You can view detailed information about the selected host's certificate.

4 Click **Renew** or **Refresh CA Certificates**.

Option	Description
Renew	Retrieves a fresh signed certificate for the host from VMCA.
Refresh CA Certificates	Pushes all certificates in the TRUSTED_ROOTS store in the vCenter Server VECS store to the host.

5 Click **Yes** to confirm.

Change Certificate Default Settings

When a host is added to a vCenter Server system, vCenter Server sends a Certificate Signing Request (CSR) for the host to VMCA. You can change some of the default settings in the CSR using the vCenter Server Advanced Settings in the vSphere Web Client.

Change company-specific default certificate settings. See "ESXi Certificate Default Settings," on page 139 for a complete list of default settings. Some of the defaults cannot be changed.

Procedure

1 In the vSphere Web Client, select the vCenter Server system that manages the hosts.

2 Click the **Manage** tab and click **Settings**.

3 Click **Advanced Settings** and click **Edit**.

4 In the Filter box, enter `certmgmt` to display only certificate management parameters.

5 Change the value of the existing parameters to follow company policy and click **OK**.

The next time you add a host to vCenter Server, the new settings are used in the CSR that vCenter Server sends to VMCA and in the certificate that is assigned to the host.

What to do next

Changes to certificate metadata only affect new certificates. If you want to change the certificates of hosts that are already managed by the vCenter Server system, you can disconnect and reconnect the hosts.

Understanding Certificate Mode Switches

Starting with vSphere 6.0, ESXi hosts are provisioned with certificates by VMCA by default. You can instead use custom certificate mode or, for debugging purposes, thumbprint mode. In most cases, mode switches are disruptive and not necessary. If you do require a mode switch, review the potential impact before you start.

In vSphere 6.0 and later, vCenter Server supports the following certificate modes for ESXi hosts.

Table 5-4. Certificate Modes for ESXi Hosts

Certificate Mode	Description
VMware Certificate Authority (default)	By default, the VMware Certificate Authority is used as the CA for ESXi host certificates. VMCA is the root CA by default, but it can be set up as the intermediary CA to another CA. In this mode, users can manage certificates from the vSphere Web Client. Also used if VMCA is a subordinate certificate.
Custom Certificate Authority	Some customers might prefer to manage their own external certificate authority. In this mode, customers are responsible for managing the certificates and cannot manage them from the vSphere Web Client.
Thumbprint Mode	vSphere 5.5 used thumbprint mode, and this mode is still available as a fallback option for vSphere 6.0. Do not use this mode unless you encounter problems with one of the other two modes that you cannot resolve. Some vCenter 6.0 and later services might not work correctly in thumbprint mode.

Using Custom ESXi Certificates

If your company policy requires that you use a different root CA than VMCA, you can switch the certificate mode in your environment after careful planning. The recommended workflow is as follows.

1 Obtain the certificates that you want to use.

2 Remove all hosts from vCenter Server.

3 Add the custom CA's root certificate to VECS.

4 Deploy the custom CA certificates to each host and restart services on that host.

5 Switch to Custom CA mode. See "Change the Certificate Mode," on page 144.

6 Add the hosts to the vCenter Server system.

Switching from Custom CA Mode to VMCA Mode

If you are using custom CA mode and decide that using VMCA works better in your environment, you can perform the mode switch after careful planning. The recommended workflow is as follows.

1 Remove all hosts from the vCenter Server system.

2 On the vCenter Server system, remove the third-party CA's root certificate from VECS.

3 Switch to VMCA mode. See "Change the Certificate Mode," on page 144.

4 Add the hosts to the vCenter Server system.

NOTE Any other workflow for this mode switch might result in unpredictable behavior.

Retaining Thumbprint Mode Certificates During Upgrade

The switch from VMCA mode to thumbprint mode might be necessary if you encounter problems with the VMCA certificates. In thumbprint mode, the vCenter Server system checks only whether a certificate exists and is formatted correctly, and does not check whether the certificate is valid. See "Change the Certificate Mode," on page 144 for instructions.

Switching from Thumbprint Mode to VMCA Mode

If you use thumbprint mode and you want to start using VMCA-signed certificates, the switch requires some planning. The recommended workflow is as follows.

1 Remove all hosts from the vCenter Server system.

2 Switch to VMCA certificate mode. See "Change the Certificate Mode," on page 144.

3 Add the hosts to the vCenter Server system.

NOTE Any other workflow for this mode switch might result in unpredictable behavior.

Switching from Custom CA Mode to Thumbprint Mode

If you are encountering problems with your custom CA, consider switching to thumbprint mode temporarily. The switch works seamlessly if you follow the instructions in "Change the Certificate Mode," on page 144. After the mode switch, the vCenter Server system checks only the format of the certificate and no longer checks the validity of the certificate itself.

Switching from Thumbprint Mode to Custom CA Mode

If you set your environment to thumbprint mode during troubleshooting, and you want to start using custom CA mode, you must first generate the required certificates. The recommended workflow is as follows.

1 Remove all hosts from the vCenter Server system.

2 Add the custom CA root certificate to TRUSTED_ROOTS store on VECS on the vCenter Server system. See "Update the vCenter Server TRUSTED_ROOTS Store (Custom Certificates)," on page 147.

3 For each ESXi host:

   a Deploy the custom CA certificate and key.

   b Restart services on the host.

4 Switch to custom mode. See "Change the Certificate Mode," on page 144.

5 Add the hosts to the vCenter Server system.

Change the Certificate Mode

In most cases, using VMCA to provision the ESXi hosts in your environment is the best solution. If corporate policy requires that you use custom certificates with a different root CA, you can edit the vCenter Server advanced options so that the hosts are not automatically provisioned with VMCA certificates when you refresh certificates. You are then responsible for the certificate management in your environment.

You can use the vCenter Server advanced settings to change to thumbprint mode or to custom CA mode. Use thumbprint mode only as a fallback option.

Procedure

1 Select the vCenter Server that manages the hosts and click **Settings**.

2 Click **Advanced Settings**, and click **Edit**.

3 In the Filter box, enter **`certmgmt`** to display only certificate management keys.

4 Change the value of vpxd.certmgmt.mode to **custom** if you intend to manage your own certificates, and to **thumbprint** if you temporarily want to use thumbprint mode, and click **OK**.

5 Restart the vCenter Server service.

Replacing ESXi SSL Certificates and Keys

Your company's security policy might require that you replace the default ESXi SSL certificate with a third-party CA-signed certificate on each host.

By default, vSphere components use the VMCA-signed certificate and key that are created during installation. If you accidentally delete the VMCA-signed certificate, remove the host from its vCenter Server system, and add it back. When you add the host, vCenter Server requests a new certificate from VMCA and provisions the host with it.

Replace VMCA-signed certificates with certificates from a trusted CA, either a commercial CA or an organizational CA, if company policy requires it.

The default certificates are in the same location as the vSphere 5.5 certificates. You can replace the default certificates with trusted certificates in a number of ways.

NOTE You can also use the `vim.CertificateManager` and `vim.host.CertificateManager` managed objects in the vSphere Web Services SDK. See the vSphere Web Services SDK documentation.

After you replace the certificate, you have to update the TRUSTED_ROOTS store in VECS on the vCenter Server system that manages the host to ensure that the vCenter Server and the ESXi host have a trust relationship.

- Requirements for ESXi Certificate Signing Requests on page 145

  If you want to use a third-party CA-signed certificate, either with VMCA as a subordinate authority or with a custom certificate authority, you have to send a Certificate Signing Request (CSR) to the CA.

- Replace the Default Certificate and Key from the ESXi Shell on page 146

  You can replace the default VMCA-signed ESXi certificates from the ESXi Shell.

- Replace a Default Certificate and Key With the vifs Command on page 146

  You can replace the default VMCA-signed ESXi certificates with the `vifs` command.

- Replace a Default Certificate Using HTTPS PUT on page 147

  You can use third-party applications to upload certificates and key. Applications that support HTTPS PUT operations work with the HTTPS interface that is included with ESXi.

- Update the vCenter Server TRUSTED_ROOTS Store (Custom Certificates) on page 147

  If you set up your ESXi hosts to use custom certificates, you have to update the `TRUSTED_ROOTS` store on the vCenter Server system that manages the hosts.

Requirements for ESXi Certificate Signing Requests

If you want to use a third-party CA-signed certificate, either with VMCA as a subordinate authority or with a custom certificate authority, you have to send a Certificate Signing Request (CSR) to the CA.

Use a CSR with these characteristics:

- 2048 bits
- PKCS1
- No wildcards
- 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.

Replace the Default Certificate and Key from the ESXi Shell

You can replace the default VMCA-signed ESXi certificates from the ESXi Shell.

Prerequisites

- If you want to use third-party CA-signed certificates, generate the certificate request, send it to the certificate authority, and store the certificates on each ESXi host.
- If necessary, enable the ESXi Shell or enable SSH traffic from the vSphere Web Client. See "Use the vSphere Web Client to Enable Access to the ESXi Shell," on page 178.
- All file transfers and other communications occur over a secure HTTPS session. The user who is used to authenticate the session must have the privilege **Host.Config.AdvancedConfig** on the host. For more information on assigning privileges through roles, see "Managing Permissions for vCenter Components," on page 119.

Procedure

1. Log in to the ESXi Shell, either directly from the DCUI or from an SSH client, as a user with administrator privileges.
2. In the directory `/etc/vmware/ssl`, rename the existing certificates using the following commands.

   ```
   mv rui.crt orig.rui.crt
   mv rui.key orig.rui.key
   ```

3. Copy the certificates that you want to use to `/etc/vmware/ssl`.
4. Rename the new certificate and key to `rui.crt` and `rui.key`.
5. Restart the host after you install the new certificate.

   Alternatively, you can put the host into maintenance mode, install the new certificate, use the Direct Console User Interface (DCUI) to restart the management agents, and set the host to exit maintenance mode.

What to do next

Update the vCenter Server TRUSTED_ROOTS store. See "Update the vCenter Server TRUSTED_ROOTS Store (Custom Certificates)," on page 147.

Replace a Default Certificate and Key With the vifs Command

You can replace the default VMCA-signed ESXi certificates with the `vifs` command.

Prerequisites

- If you want to use third-party CA-signed certificates, generate the certificate request, send it to the certificate authority, and store the certificates on each ESXi host.
- If necessary, enable the ESXi Shell or enable SSH traffic from the vSphere Web Client. See "Use the vSphere Web Client to Enable Access to the ESXi Shell," on page 178.
- All file transfers and other communications occur over a secure HTTPS session. The user who is used to authenticate the session must have the privilege **Host.Config.AdvancedConfig** on the host. For more information on assigning privileges through roles, see "Managing Permissions for vCenter Components," on page 119.

Procedure

1. Back up the existing certificates.
2. Generate a certificate request following the instructions from the certificate authority.

3 When you have the certificate, use the `vifs` command to upload the certificate to the appropriate location on the host from an SSH connection to the host.

```
vifs --server hostname --username username --put rui.crt /host/ssl_cert
vifs --server hostname --username username --put rui.key /host/ssl_key
```

4 Restart the host.

What to do next

Update the vCenter Server TRUSTED_ROOTS store. See "Update the vCenter Server TRUSTED_ROOTS Store (Custom Certificates)," on page 147.

Replace a Default Certificate Using HTTPS PUT

You can use third-party applications to upload certificates and key. Applications that support HTTPS PUT operations work with the HTTPS interface that is included with ESXi.

Prerequisites

- If you want to use third-party CA-signed certificates, generate the certificate request, send it to the certificate authority, and store the certificates on each ESXi host.
- If necessary, enable the ESXi Shell or enable SSH traffic from the vSphere Web Client. See "Use the vSphere Web Client to Enable Access to the ESXi Shell," on page 178.
- All file transfers and other communications occur over a secure HTTPS session. The user who is used to authenticate the session must have the privilege **Host.Config.AdvancedConfig** on the host. For more information on assigning privileges through roles, see "Managing Permissions for vCenter Components," on page 119.

Procedure

1 Back up the existing certificates.

2 In your upload application, process each file as follows:

   a Open the file.

   b Publish the file to one of these locations.

Option	Description
Certificates	`https://hostname/host/ssl_cert`
Keys	`https://hostname/host/ssl_key`

   The location `/host/ssl_cert` and `host/ssl_key` link to the certificate files in `/etc/vmware/ssl`.

3 Restart the host.

What to do next

Update the vCenter Server TRUSTED_ROOTS store. See "Update the vCenter Server TRUSTED_ROOTS Store (Custom Certificates)," on page 147.

Update the vCenter Server TRUSTED_ROOTS Store (Custom Certificates)

If you set up your ESXi hosts to use custom certificates, you have to update the `TRUSTED_ROOTS` store on the vCenter Server system that manages the hosts.

Prerequisites

Replace the certificates on each host with custom certificates.

Procedure

1 Log in to the vCenter Server system that manages the ESXi hosts.

Log in to the Windows system on which you installed the software, or log in to the vCenter Server Appliance shell.

2 Run `vecs-cli` to add the new certificates to the `TRUSTED_ROOTS` store, for example:

```
/usr/lib/vmware-vmafd/bin/vecs-cli entry create --store TRUSTED_ROOTS --alias custom1.crt --
cert /etc/vmware/ssl/custom1.crt
```

What to do next

Set certificate mode to Custom. If certificate mode is VMCA, the default, and you perform a certificate refresh, your custom certificates are replaced with VMCA-signed certificates. See "Change the Certificate Mode," on page 144.

Use Custom Certificates with Auto Deploy

By default, the Auto Deploy server provisions each host with certificates that are signed by VMCA. You can set up the Auto Deploy server to provision all hosts with custom certificates that are not signed by VMCA. In that scenario, the Auto Deploy server becomes a subordinate certificate authority of your third-party CA.

Prerequisites

- Request a certificate that meets your requirements from your CA.
  - 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
- Name the certificate and key files `rbd-ca.crt` and `rbd-ca.key`.

Procedure

1 Back up the default ESXi certificates.

The certificates are located at `/etc/vmware-rbd/ssl/`.

2 From the vSphere Web Client, stop the Auto Deploy service.

a Select **Administration**, and click **System Configuration** under **Deployment**.

b Click **Services**.

c Right-click the service you want to stop and select **Stop**.

3 On the system where the Auto Deploy service runs, replace `rbd-ca.crt` and `rbd-ca.key` in `/etc/vmware-rbd/ssl/` with your custom certificate and key file.

4 On the system where the Auto Deploy service runs, update the TRUSTED_ROOTS store in VECS to use your new certificates.

```
vecs-cli entry delete --store TRUSTED_ROOTS --alias
                rbd_cert
vecs-cli entry create --store TRUSTED_ROOTS --alias
                rbd_cert --cert /etc/vmware-rbd/ssl/rbd-ca.crt
```

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

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

5 Create a `castore.pem` file that contains what's in TRUSTED_ROOTS and place the file in the `/etc/vmware-rbd/ssl/` directory.

In custom mode, you are responsible for maintaining this file.

6 Change the certificate mode for the vCenter Server system to **`custom`**.

See "Change the Certificate Mode," on page 144.

7 Restart the vCenter Server service and start the Auto Deploy service.

The next time you provision a host that is set up to use Auto Deploy, the Auto Deploy server generates a certificate using the root certificate that you just added to the TRUSTED_ROOTS store.

Restore ESXi Certificate and Key Files

When you replace a certificate on an ESXi host by using the vSphere Web Services SDK, the previous certificate and key are appended to a `.bak` file. You can restore previous certificates by moving the information in the `.bak` file to the current certificate and key files.

The host certificate and key are located in `/etc/vmware/ssl/rui.crt` and `/etc/vmware/ssl/rui.key`. When you replace a host certificate and key by using the vSphere Web Services SDK `vim.CertificateManager` managed object, the previous key and certificate are appended to the file `/etc/vmware/ssl/rui.bak`.

NOTE If you replace the certificate by using HTTP PUT, `vifs`, or from the ESXi Shell, the existing certificates are not appended to the `.bak` file.

Procedure

1 On the ESXi host, locate the file `/etc/vmware/ssl/rui.bak`.

The file has the following format.

```
#
# Host private key and certificate backup from 2014-06-20 08:02:49.961
#

-----BEGIN PRIVATE KEY-----
previous key
-----END PRIVATE KEY-----

-----BEGIN CERTIFICATE-----
previous cert
-----END CERTIFICATE-----
```

2 Copy the text starting with `-----BEGIN PRIVATE KEY-----` and ending with `-----END PRIVATE KEY-----` into the `/etc/vmware/ssl/rui.key` file.

Include `-----BEGIN PRIVATE KEY-----` and `-----END PRIVATE KEY-----`.

3 Copy the text between -----BEGIN CERTIFICATE----- and -----END CERTIFICATE----- into the /etc/vmware/ssl/rui.crt file.

   Include -----BEGIN CERTIFICATE----- and -----END CERTIFICATE-----.

4 Restart the host or send ssl_reset events to all services that use the keys.

```
for s in /etc/init.d/*; do $s | grep ssl_reset > /dev/null; if [ $? == 0 ]; then $s
ssl_reset; fi; done
```

Customizing Hosts with the Security Profile

You can customize many of the essential security settings for your host through the Security Profile panel available in the vSphere Web Client. The Security Profile is especially useful for single host management. If you are managing multiple hosts, consider using one of the CLIs or SDKs and automating the customization.

ESXi Firewall Configuration

ESXi includes a firewall that is enabled by default.

At installation time, the ESXi firewall is configured to block incoming and outgoing traffic, except traffic for services that are enabled in the host's security profile.

As you open ports on the firewall, consider that unrestricted access to services running on an ESXi host can expose a host to outside attacks and unauthorized access. Reduce the risk by configuring the ESXi firewall to allow access only from authorized networks.

NOTE The firewall also allows Internet Control Message Protocol (ICMP) pings and communication with DHCP and DNS (UDP only) clients.

You can manage ESXi firewall ports as follows:

- Use the security profile for each host in the vSphere Web Client. See "Manage ESXi Firewall Settings," on page 151
- Use ESXCLI commands from the command line or in scripts. See "ESXi ESXCLI Firewall Commands," on page 155.
- Use a custom VIB if the port you want to open is not included in the security profile.

  You create custom VIBs with the vibauthor tool available from VMware Labs. To install the custom VIB, you have to change the acceptance level of the the ESXi host to CommunitySupported. See VMware Knowledge Base Article 2007381.

  NOTE If you engage VMware Technical Support to investigate a problem on an ESXi host with a CommunitySupported VIB installed, VMware Support might request that this CommunitySupported VIB be uninstalled as a troubleshooting step to determine if that VIB is related to the problem being investigated.

ESXi Firewall Concepts (http://link.brightcove.com/services/player/bcpid2296383276001?bctid=ref:video_esxi_firewall_concepts)

The behavior of the NFS Client rule set (nfsClient) is different from other rule sets. When the NFS Client rule set is enabled, all outbound TCP ports are open for the destination hosts in the list of allowed IP addresses. See "NFS Client Firewall Behavior," on page 154 for more information.

Manage ESXi Firewall Settings

You can configure incoming and outgoing firewall connections for a service or a management agent from the vSphere Web Client or at the command line.

NOTE If different services have overlapping port rules, enabling one service might implicitly enable other services. You can specify which IP addresses are allowed to access each service on the host to avoid this problem.

Procedure

1 Browse to the host in the vSphere Web Client inventory.

2 Click the **Manage** tab and click **Settings**.

3 Click **Security Profile**.

The vSphere Web Client displays a list of active incoming and outgoing connections with the corresponding firewall ports.

4 In the Firewall section, click **Edit**.

The display shows firewall rule sets, which include the name of the rule and the associated information.

5 Select the rule sets to enable, or deselect the rule sets to disable.

Column	Description
Incoming Ports and Outgoing Ports	The ports that the vSphere Web Client opens for the service
Protocol	Protocol that a service uses.
Daemon	Status of daemons associated with the service

6 For some services, you can manage service details.

- Use the **Start**, **Stop**, or **Restart** buttons to change the status of a service temporarily.
- Change the Startup Policy to have the service start with the host or with port usage.

7 For some services, you can explicitly specify IP addresses from which connections are allowed.

See "Add Allowed IP Addresses for an ESXi Host," on page 151.

8 Click **OK**.

Add Allowed IP Addresses for an ESXi Host

By default, the firewall for each service allows access to all IP addresses. To restrict traffic, change each service to allow traffic only from your management subnet. You might also deselect some services if your environment does not use them.

You can use the vSphere Web Client, vCLI, or PowerCLI to update the Allowed IP list for a service. By default, all IP addresses are allowed for a service.

Adding Allowed IP Addresses to the ESXi Firewall (http://link.brightcove.com/services/player/bcpid2296383276001?bctid=ref:video_adding_allowed_IP_to_esxi_firewall)

Procedure

1 Browse to the host in the vSphere Web Client inventory.

2 Click the **Manage** tab and click **Settings**.

3 Under System, click **Security Profile**.

4 In the Firewall section, click **Edit** and select a service from the list.

5 In the Allowed IP Addresses section, deselect **Allow connections from any IP address** and enter the IP addresses of networks that are allowed to connect to the host.

Separate IP addresses with commas. You can use the following address formats:

- 192.168.0.0/24
- 192.168.1.2, 2001::1/64
- fd3e:29a6:0a81:e478::/64

6 Click **OK**.

Incoming and Outgoing Firewall Ports for ESXi Hosts

The vSphere Web Client allows you to open and close firewall ports for each service or to allow traffic from selected IP addresses.

The following table lists the firewalls for services that are usually installed. If you install other VIBs on your host, additional services and firewall ports might become available.

Table 5-5. Incoming Firewall Connections

Service	Port	Comment
CIM Server	5988 (TCP)	Server for CIM (Common Information Model).
CIM Secure Server	5989 (TCP)	Secure server for CIM.
CIM SLP	427 (TCP, UDP)	The CIM client uses the Service Location Protocol, version 2 (SLPv2) to find CIM servers.
DHCPv6	546 (TCP, UDP)	DHCP client for IPv6.
DVSSync	8301, 8302 (UDP)	DVSSync ports are used for synchronizing states of distributed virtual ports between hosts that have VMware FT record/replay enabled. Only hosts that run primary or backup virtual machines must have these ports open. On hosts that are not using VMware FT these ports do not have to be open.
NFC	902 (TCP)	Network File Copy (NFC) provides a file-type-aware FTP service for vSphere components. ESXi uses NFC for operations such as copying and moving data between datastores by default.
Virtual SAN Clustering Service	12345, 23451 (UDP)	Virtual SAN Cluster Monitoring and Membership Directory Service. Uses UDP-based IP multicast to establish cluster members and distribute Virtual SAN metadata to all cluster members. If disabled, Virtual SAN does not work.
DHCP Client	68 (UDP)	DHCP client for IPv4.
DNS Client	53 (UDP)	DNS client.
Fault Tolerance	8200, 8100, 8300 (TCP, UDP)	Traffic between hosts for vSphere Fault Tolerance (FT).
NSX Distributed Logical Router Service	6999 (UDP)	NSX Virtual Distributed Router service. The firewall port associated with this service is opened when NSX VIBs are installed and the VDR module is created. If no VDR instances are associated with the host, the port does not have to be open. This service was called NSX Distributed Logical Router in earlier versions of the product.

Table 5-5. Incoming Firewall Connections (Continued)

Service	Port	Comment
Virtual SAN Transport	2233 (TCP)	Virtual SAN reliable datagram transport. Uses TCP and is used for Virtual SAN storage IO. If disabled, Virtual SAN does not work.
SNMP Server	161 (UDP)	Allows the host to connect to an SNMP server.
SSH Server	22 (TCP)	Required for SSH access.
vMotion	8000 (TCP)	Required for virtual machine migration with vMotion.
vSphere Web Client	902, 443 (TCP)	Client connections
vsanvp	8080 (TCP)	VSAN VASA Vendor Provider. Used by the Storage Management Service (SMS) that is part of vCenter to access information about Virtual SAN storage profiles, capabilities, and compliance. If disabled, Virtual SAN Storage Profile Based Management (SPBM) does not work.
vSphere Web Access	80 (TCP)	Welcome page, with download links for different interfaces.

Table 5-6. Outgoing Firewall Connections

Service	Port	Comment
CIM SLP	427 (TCP, UDP)	The CIM client uses the Service Location Protocol, version 2 (SLPv2) to find CIM servers.
DHCPv6	547 (TCP, UDP)	DHCP client for IPv6.
DVSSync	8301, 8302 (UDP)	DVSSync ports are used for synchronizing states of distributed virtual ports between hosts that have VMware FT record/replay enabled. Only hosts that run primary or backup virtual machines must have these ports open. On hosts that are not using VMware FT these ports do not have to be open.
HBR	44046, 31031 (TCP)	Used for ongoing replication traffic by vSphere Replication and VMware Site Recovery Manager.
NFC	902 (TCP)	Network File Copy (NFC) provides a file-type-aware FTP service for vSphere components. ESXi uses NFC for operations such as copying and moving data between datastores by default.
WOL	9 (UDP)	Used by Wake on LAN.
Virtual SAN Clustering Service	12345 23451 (UDP)	Cluster Monitoring, Membership, and Directory Service used by Virtual SAN.
DHCP Client	68 (UDP)	DHCP client.
DNS Client	53 (TCP, UDP)	DNS client.
Fault Tolerance	80, 8200, 8100, 8300 (TCP, UDP)	Supports VMware Fault Tolerance.
Software iSCSI Client	3260 (TCP)	Supports software iSCSI.
NSX Distributed Logical Router Service	6999 (UDP)	The firewall port associated with this service is opened when NSX VIBs are installed and the VDR module is created. If no VDR instances are associated with the host, the port does not have to be open.

Table 5-6. Outgoing Firewall Connections (Continued)

Service	Port	Comment
rabbitmqproxy	5671 (TCP)	A proxy running on the ESXi host that allows applications running inside virtual machines to communicate to the AMQP brokers running in the vCenter network domain. The virtual machine does not have to be on the network, that is, no NIC is required. The proxy connects to the brokers in the vCenter network domain. Therefore, the outgoing connection IP addresses should at least include the current brokers in use or future brokers. Brokers can be added if customer would like to scale up.
Virtual SAN Transport	2233 (TCP)	Used for RDT traffic (Unicast peer to peer communication) between Virtual SAN nodes.
vMotion	8000 (TCP)	Required for virtual machine migration with vMotion.
VMware vCenter Agent	902 (UDP)	vCenter Server agent.
vsanvp	8080 (TCP)	Used for Virtual SAN Vendor Provider traffic.

NFS Client Firewall Behavior

The NFS Client firewall rule set behaves differently than other ESXi firewall rule sets. ESXi configures NFS Client settings when you mount or unmount an NFS datastore. The behavior differs for different versions of NFS.

When you add, mount, or unmount an NFS datastore, the resulting behavior depends on the version of NFS.

NFS v3 Firewall Behavior

When you add or mount an NFS v3 datastore, ESXi checks the state of the NFS Client (`nfsClient`) firewall rule set.

- If the `nfsClient` rule set is disabled, ESXi enables the rule set and disables the Allow All IP Addresses policy by setting the `allowedAll` flag to `FALSE`. The IP address of the NFS server is added to the allowed list of outgoing IP addresses.
- If the `nfsClient` rule set is enabled, the state of the rule set and the allowed IP address policy are not changed. The IP address of the NFS server is added to the allowed list of outgoing IP addresses.

Note If you manually enable the `nfsClient` rule set or manually set the Allow All IP Addresses policy, either before or after you add an NFS v3 datastore to the system, your settings are overridden when the last NFS v3 datastore is unmounted. The `nfsClient` rule set is disabled when all NFS v3 datastores are unmounted.

When you remove or unmount an NFS v3 datastore, ESXi performs one of the following actions.

- If none of the remaining NFS v3 datastores are mounted from the server of the datastore being unmounted, ESXi removes the server's IP address from the list of outgoing IP addresses.
- If no mounted NFS v3 datastores remain after the unmount operation, ESXi disables the `nfsClient` firewall rule set.

NFS v4.1 Firewall Behavior

When you mount the first NFS v4.1 datastore, ESXi enables the `nfs41client` rule set and sets its `allowedAll` flag to TRUE. This action opens port 2049 for all IP addresses. Unmounting an NFS v4.1 datastore does not affect the firewall state. That is, the first NFS v4.1 mount opens port 2049 and that port remains enabled unless you close it explicitly.

ESXi ESXCLI Firewall Commands

If your environment includes multiple ESXi hosts, automating firewall configuration by using ESXCLI commands or the vSphere Web Services SDK is recommended.

You can use the ESXi Shell or vSphere CLI commands to configure ESXi at the command line to automate firewall configuration. See *Getting Started with vSphere Command-Line Interfaces* for an introduction, and *vSphere Command-Line Interface Concepts and Examples* for examples of using ESXCLI to manipulate firewalls and firewall rules.

Table 5-7. Firewall Commands

Command	Description
`esxcli network firewall get`	Return the enabled or disabled status of the firewall and lists default actions.
`esxcli network firewall set --default-action`	Set to true to set the default action to pass, set to fals to set the default action to drop.
`esxcli network firewall set --enabled`	Enable or disable the ESXi firewall.
`esxcli network firewall load`	Load the firewall module and rule set configuration files.
`esxcli network firewall refresh`	Refresh the firewall configuration by reading the rule set files if the firewall module is loaded.
`esxcli network firewall unload`	Destroy filters and unload the firewall module.
`esxcli network firewall ruleset list`	List rule sets information.
`esxcli network firewall ruleset set --allowed-all`	Set to true to allow all access to all IPs, set to false to use a list of allowed IP addresses.
`esxcli network firewall ruleset set --enabled --ruleset-id=<string>`	Set enabled to true or false to enable or disable the specified ruleset.
`esxcli network firewall ruleset allowedip list`	List the allowed IP addresses of the specified rule set.
`esxcli network firewall ruleset allowedip add`	Allow access to the rule set from the specified IP address or range of IP addresses.
`esxcli network firewall ruleset allowedip remove`	Remove access to the rule set from the specified IP address or range of IP addresses.
`esxcli network firewall ruleset rule list`	List the rules of each ruleset in the firewall.

Customizing ESXi Services from the Security Profile

An ESXi host includes several services that are running by default. Other services, for example SSH, are included in the host's security profile. You can enable and disable those services as needed if company policy allows it.

"Use the vSphere Web Client to Enable Access to the ESXi Shell," on page 178 is an example of how to enable a service.

NOTE Enabling services affects the security of your host. Do not enable a service unless strictly necessary.

Available services depend on the VIBs that are installed on the ESXi host. You cannot add services without installing a VIB. Some VMware products, for example, vSphere HA, install VIBs on hosts and make services and the corresponding firewall ports available.

In a default installation, you can modify the status of the following services from the vSphere Web Client.

Table 5-8. ESXi Services in the Security Profile

Service	Default	Description
Direct Console UI	Running	The Direct Console User Interface (DCUI) service allows you to interact with an ESXi host from the local console host using text-based menus.
ESXi Shell	Stopped	The ESXi Shell is available from the Direct Console User Interface and includes a set of fully supported commands and a set of commands for troubleshooting and remediation. You must enable access to the ESXi Shell from the direct console of each system. You can enable access to the local ESXi Shell or access to the ESXi Shell with SSH.
SSH	Stopped	The host's SSH client service that allows remote connections through Secure Shell.
Load-Based Teaming Daemon	Running	Load-Based Teaming.
Local Security Authentication Server (Active Directory Service)	Stopped	Part of Active Directory Service. When you configure ESXi for Active Directory, this service is started.
I/O Redirector (Active Directory Service)	Stopped	Part of Active Directory Service. When you configure ESXi for Active Directory, this service is started.
Network Login Server (Active Directory Service)	Stopped	Part of Active Directory Service. When you configure ESXi for Active Directory, this service is started.
NTP Daemon	Stopped	Network Time Protocol daemon.
CIM Server	Running	Service that can be used by Common Information Model (CIM) applications.
SNMP Server	Stopped	SNMP daemon. See *vSphere Monitoring and Performance* for information on configuring SNMP v1, v2, and v3.
Syslog Server	Stopped	Syslog daemon. You can enable syslog from the Advanced System Settings in the vSphere Web Client. See *vSphere Installation and Setup*.
vSphere High Availability Agent	Stopped	Supports vSphere High Availability functionality.
vProbe Daemon	Stopped	vProbe daemon.
VMware vCenter Agent	Running	vCenter Server agent. Allows a vCenter Server to connect to an ESXi host. Specifically, vpxa is the communication conduit to the host daemon, which in turn communicates with the ESXi kernel.
X.Org Server	Stopped	X.Org Server. This optional feature is used internally for 3D graphics for virtual machines.

Enable or Disable a Service in the Security Profile

You can enable or disable one of the services listed in the Security Profile from the vSphere Web Client.

After installation, certain services are running by default, while others are stopped. In some cases, additional setup is necessary before a service becomes available in the vSphere Web Client UI. For example, the NTP service is a way of getting accurate time information, but this service only works when required ports are opened in the firewall.

Prerequisites

Connect to vCenter Server with the vSphere Web Client.

Procedure

1 Browse to a host in the vSphere Web Client inventory, and select a host.

2 Click the **Manage** tab and click **Settings**.

3 Under System, select **Security Profile** and click **Edit**.

4 Scroll to the service that you wish to change.

5 In the Service Details pane, select **Start**, **Stop**, or **Restart** for a one-time change to the host's status, or select from the **Startup Policy** menu to change the status of the host across reboots.

- **Start automatically if any ports are open, and stop when all ports are closed**: The default setting for these services. If any port is open, the client attempts to contact the network resources for the service. If some ports are open, but the port for a particular service is closed, the attempt fails. If and when the applicable outgoing port is opened, the service begins completing its startup.
- **Start and stop with host**: The service starts shortly after the host starts, and closes shortly before the host shuts down. Much like **Start automatically if any ports are open, and stop when all ports are closed**, this option means that the service regularly attempts to complete its tasks, such as contacting the specified NTP server. If the port was closed but is subsequently opened, the client begins completing its tasks shortly thereafter.
- **Start and stop manually**: The host preserves the user-determined service settings, regardless of whether ports are open or not. When a user starts the NTP service, that service is kept running as long as the host is powered on. If the service is started and the host is powered off, the service is stopped as part of the shutdown process, but as soon as the host is powered on, the service is started again, preserving the user-determined state.

NOTE These settings apply only to service settings that are configured through the vSphere Web Client or to applications that are created with the vSphere Web Services SDK. Configurations made through other means, such as from the ESXi Shell or with configuration files, are not affected by these settings.

Lockdown Mode

To increase the security of your ESXi hosts, you can put them in lockdown mode. In lockdown mode, operations must be performed through vCenter Server by default.

Starting with vSphere 6.0, you can select normal lockdown mode or strict lockdown mode, which offer different degrees of lockdown. vSphere 6.0 also introduces the Exception User list. Exception users do not lose their privileges when the host enters lockdown mode. Use the Exception User list to add the accounts of third-party solutions and external applications that need to access the host directly when the host is in lockdown mode. See "Specify Lockdown Mode Exception Users," on page 163.

Lockdown Mode in vSphere 6 (http://link.brightcove.com/services/player/bcpid2296383276001?bctid=ref:video_lockdown_mode_vsphere)

Normal Lockdown Mode and Strict Lockdown Mode

Starting with vSphere 6.0, you can select normal lockdown mode or strict lockdown mode, which offer different degrees of lockdown.

Normal Lockdown Mode

In normal lockdown mode the DCUI service is not stopped. If the connection to the vCenter Server system is lost and access through the vSphere Web Client is no longer available, privileged accounts can log in to the ESXi host's Direct Console Interface and exit lockdown mode. Only the following accounts can access the Direct Console User Interface:

- Accounts in the Exception User list for lockdown mode who have administrative privileges on the host. The Exception Users list is meant for service accounts that perform very specific tasks. Adding ESXi administrators to this list defeats the purpose of lockdown mode.
- Users defined in the DCUI.Access advanced option for the host. This option is for emergency access to the Direct Console Interface in case the connection to vCenter Server is lost. These users do not require administrative privileges on the host.

Strict Lockdown Mode

In strict lockdown mode, which is new in vSphere 6.0, the DCUI service is stopped. If the connection to vCenter Server is lost and the vSphere Web Client is no longer available, the ESXi host becomes unavailable unless the ESXi Shell and SSH services are enabled and Exception Users are defined. If you cannot restore the connection to the vCenter Server system, you have to reinstall the host.

Lockdown Mode and the ESXi Shell and SSH Services

Strict lockdown mode stops the DCUI service. However, the ESXi Shell and SSH services are independent of lockdown mode. For lockdown mode to be an effective security measure, ensure that the ESXi Shell and SSH services are also disabled. Those services are disabled by default.

When a host is in lockdown mode, users on the Exception Users list can access the host from the ESXi Shell and through SSH if they have the Administrator role on the host. This access is possible even in strict lockdown mode. Leaving the ESXi Shell service and the SSH service disabled is the most secure option.

NOTE The Exception Users list is meant for service accounts that perform specific tasks such as host backups, and not for administrators. Adding administrator users to the Exception Users list defeats the purpose of lockdown mode.

Enabling and Disabling Lockdown Mode

Privileged users can enable lockdown mode in several ways:

- When using the Add Host wizard to add a host to a vCenter Server system.
- Using the vSphere Web Client. See "Enable Lockdown Mode Using the vSphere Web Client," on page 160. You can enable both normal lockdown mode and strict lockdown mode from the vSphere Web Client.
- Using the Direct Console User Interface (DCUI). See "Enable or Disable Normal Lockdown Mode from the Direct Console User Interface," on page 161.

Privileged users can disable lockdown mode from the vSphere Web Client. They can disable normal lockdown mode from the Direct Console Interface, but they cannot disable strict lockdown mode from the Direct Console Interface.

NOTE If you enable or disable lockdown mode using the Direct Console User Interface, permissions for users and groups on the host are discarded. To preserve these permissions, you can enable and disable lockdown mode using the vSphere Web Client.

Lockdown Mode Behavior

In lockdown mode, some services are disabled, and some services are accessible only to certain users.

Lockdown Mode Services for Different Users

When the host is running, available services depend on whether lockdown mode is enabled, and on the type of lockdown mode.

- In strict and normal lockdown mode, privileged users can access the host through vCenter Server, either from the vSphere Web Client or by using the vSphere Web Services SDK.
- Direct Console Interface behavior differs for strict lockdown mode and normal lockdown mode.
  - In strict lockdown mode, the Direct Console User Interface (DCUI) service is disabled.
  - In normal lockdown mode, accounts on the Exception User list who have administrator privileges and users who are specified in the DCUI.Access advanced system setting can access the Direct Console Interface.
- If the ESXi Shell or SSH are enabled and the host is placed in strict or normal lockdown mode, accounts on the Exception Users list who have administrator privileges can use these services. For all other users, ESXi Shell or SSH access is disabled. Starting with vSphere 6.0, ESXi or SSH sessions for users who do not have administrator privileges are terminated.

All access is logged for both strict and normal lockdown mode.

Table 5-9. Lockdown Mode Behavior

Service	Normal Mode	Normal Lockdown Mode	Strict Lockdown Mode
vSphere Web Services API	All users, based on permissions	vCenter (vpxuser) Exception users, based on permissions vCloud Director (vslauser, if available)	vCenter (vpxuser) Exception users, based on permissions vCloud Director (vslauser, if available)
CIM Providers	Users with administrator privileges on the host	vCenter (vpxuser) Exception users, based on permissions. vCloud Director (vslauser, if available)	vCenter (vpxuser) Exception, based on permissions. vCloud Director (vslauser, if available)
Direct Console UI (DCUI)	Users with administrator privileges on the host , and users in the DCUI.Access advanced option	Users defined in the DCUI.Access advanced option Exception users with administrator privileges on the host	DCUI service is stopped

Table 5-9. Lockdown Mode Behavior (Continued)

Service	Normal Mode	Normal Lockdown Mode	Strict Lockdown Mode
ESXi Shell (if enabled)	Users with administrator privileges on the host	Users defined in the DCUI.Access advanced option Exception users with administrator privileges on the host	Users defined in the DCUI.Access advanced option Exception users with administrator privileges on the host
SSH (if enabled)	Users with administrator privileges on the host	Users defined in the DCUI.Access advanced option Exception users with administrator privileges on the host	Users defined in the DCUI.Access advanced option Exception users with administrator privileges on the host

Users Logged in to the ESXi Shell When Lockdown Mode Is Enabled

If users are logged in to the ESXi Shell or access the host through SSH before lockdown mode is enabled, those users who are on the list of Exception Users and who have administrator privileges on the host remain logged in. Starting with vSphere 6.0, the session is terminated for all other users. This applies to both normal and strict lockdown mode.

Enable Lockdown Mode Using the vSphere Web Client

Enable lockdown mode to require that all configuration changes go through vCenter Server. vSphere 6.0 and later supports normal lockdown mode and strict lockdown mode.

To completely disallow all direct access to a host, you can select strict lockdown mode. Strict lockdown mode makes it impossible to access a host if the vCenter Server is unavailable and SSH and the ESXi Shell are disabled. See "Lockdown Mode Behavior," on page 159.

Procedure

1 Browse to the host in the vSphere Web Client inventory.

2 Click the **Manage** tab and click **Settings**.

3 Under System, select **Security Profile**.

4 In the Lockdown Mode panel, click **Edit**.

5 Click **Lockdown Mode** and select one of the lockdown mode options.

Option	Description
Normal	The host can be accessed through vCenter Server. Only users who are on the Exception Users list and have administrator privileges can log in to the Direct Console User Interface. If SSH or the ESXi Shell are enabled, access might be possible.
Strict	The host can only be accessed through vCenter Server. If SSH or the ESXi Shell are enabled, running sessions for accounts in the DCUI.Access advanced option and for Exception User accounts that have administrator privileges remain enabled. All other sessions are terminated.

6 Click **OK**.

Disable Lockdown Mode Using the vSphere Web Client

Disable lockdown mode to allow configuration changes from direct connections to the ESXi host. Leaving lockdown mode enabled results in a more secure environment.

In vSphere 6.0 you can disable lockdown mode as follows:

From the vSphere Web Client	Users can disable both normal lockdown mode and strict lockdown mode from the vSphere Web Client.
From the Direct Console User Interface	Users who can access the Direct Console User Interface on the ESXi host can disable normal lockdown mode. In strict lockdown mode, the Direct Console Interface service is stopped.

Procedure

1 Browse to the host in the vSphere Web Client inventory.

2 Click the **Manage** tab and click **Settings**.

3 Under System, select **Security Profile**.

4 In the Lockdown Mode panel, click **Edit**.

5 Click **Lockdown Mode** and select **None** to disable lockdown mode.

The system exits lockdown mode, vCenter Server displays an alarm, and an entry is added to the audit log.

Enable or Disable Normal Lockdown Mode from the Direct Console User Interface

You can enable and disable normal lockdown mode from the Direct Console User Interface (DCUI). You can enable and disable strict lockdown mode only from the vSphere Web Client.

When the host is in normal lockdown mode, the following accounts can access the Direct Console User Interface:

- Accounts in the Exception Users list who have administrator privileges on the host. The Exception Users list is meant for service accounts such as a backup agent.
- Users defined in the DCUI.Access advanced option for the host. This option can be used to enable access in case of catastrophic failure.

For ESXi 6.0 and later, user permissions are preserved when you enable lockdown mode, and are restored when you disable lockdown mode from the Direct Console Interface.

NOTE If you upgrade a host that is in lockdown mode to ESXi version 6.0 without exiting lockdown mode, and if you exit lockdown mode after the upgrade, all the permissions defined before the host entered lockdown mode are lost. The system assigns the administrator role to all users who are found in the DCUI.Access advanced option to guarantee that the host remains accessible.

To retain permissions, disable lockdown mode for the host from the vSphere Web Client before the upgrade.

Procedure

1 At the Direct Console User Interface of the host, press F2 and log in.

2 Scroll to the **Configure Lockdown Mode** setting and press Enter to toggle the current setting.

3 Press Esc until you return to the main menu of the Direct Console User Interface.

Specifying Accounts with Access Privileges in Lockdown Mode

You can specify service accounts that can access the ESXi host directly by adding them to the Exception Users list. You can specify a single user who can access the ESXi host in case of catastrophic vCenter Server failure.

What different accounts can do by default when lockdown mode is enabled, and how you can change the default behavior, depends on the version of the vSphere environment.

- In versions of vSphere earlier than vSphere 5.1, only the root user can log into the Direct Console User Interface on an ESXi host that is in lockdown mode.
- In vSphere 5.1 and later, you can add a user to the DCUI.Access advanced system setting for each host. The option is meant for catastrophic failure of vCenter Server, and the password for the user with this access is usually locked into a safe. A user in the DCUI.Access list does not need to have full administrative privileges on the host.
- In vSphere 6.0 and later, the DCUI.Access advanced system setting is still supported. In addition, vSphere 6.0 and later supports an Exception User list, which is for service accounts that have to log in to the host directly. Accounts with administrator privileges that are on the Exception Users list can log in to the ESXi Shell. In addition, those user can log in to a host's DCUI in normal lockdown mode and can exit lockdown mode.

  You specify Exception Users from the vSphere Web Client.

Add Users to the DCUI.Access Advanced Option

The main purpose of the DCUI.Access advanced option is to allow you to exit lockdown mode in case of catastrophic failure, when you cannot access the host from vCenter Server. You add users to the list by editing the Advanced Settings for the host from the vSphere Web Client.

NOTE Users in the DCUI.Access list can change lockdown mode settings regardless of their privileges. This can impact the security of your host. For service accounts that need direct access to the host, consider adding users to the Exception Users list instead. Exception user can only perform tasks for which they have privileges. See "Specify Lockdown Mode Exception Users," on page 163.

Procedure

1. Browse to the host in the vSphere Web Client object navigator.
2. Click the **Manage** tab and select **Settings**.
3. Click **Advanced System Settings** and select **DCUI.Access**.
4. Click **Edit** and enter the user names, separated by commas.

   By default, the root user is included. Consider removing root from the DCUI.Access, list and specifying a named account for better auditability.
5. Click **OK**.

Specify Lockdown Mode Exception Users

In vSphere 6.0 and later, you can add users to the Exception Users list from the vSphere Web Client. These users do not lose their permissions when the host enters lockdown mode. It makes sense to add service accounts such as a backup agent to the Exception Users list.

Exception users do not lose their privileges when the host enters lockdown mode. Usually these accounts represent third-party solutions and external applications that need to continue to function in lockdown mode.

NOTE The Exception Users list is meant for service accounts that perform very specific tasks, and not for administrators. Adding administrator users to the Exception Users list defeats the purpose of lockdown mode.

Exception users are host local users or Active Directory users with privileges defined locally for the ESXi host. They are not vCenter Server users. These users are allowed to perform operations on the host based on their privileges. That means, for example, that a read-only user cannot disable lockdown mode on a host.

Procedure

1 Browse to the host in the vSphere Web Client inventory.

2 Click the **Manage** tab and click **Settings**.

3 Under System, select **Security Profile**.

4 In the Lockdown Mode panel, click **Edit**.

5 Click **Exception Users** and click the plus icon to add exception users.

Check the Acceptance Levels of Hosts and VIBs

To protect the integrity of the ESXi host, do not allow users to install unsigned (community-supported) VIBs. An unsigned VIB contains code that is not certified by, accepted by, or supported by VMware or its partners. Community-supported VIBs do not have a digital signature.

You can use ESXCLI commands to set an acceptance level for a host. The host's acceptance level must be the same or less restrictive than the acceptance level of any VIB you want to add to the host. To protect the security and integrity of your ESXi hosts, do not allow unsigned (CommunitySupported) VIBs to be installed on hosts in production systems.

The following acceptance levels are supported.

VMwareCertified The VMwareCertified acceptance level has the most stringent requirements. VIBs with this level go through thorough testing fully equivalent to VMware in-house Quality Assurance testing for the same technology. Today, only IOVP drivers are published at this level. VMware takes support calls for VIBs with this acceptance level.

VMwareAccepted VIBs with this acceptance level go through verification testing, but the tests do not fully test every function of the software. The partner runs the tests and VMware verifies the result. Today, CIM providers and PSA plug-ins are among the VIBs published at this level. VMware directs support calls for VIBs with this acceptance level to the partner's support organization.

PartnerSupported VIBs with the PartnerSupported acceptance level are published by a partner that VMware trusts. The partner performs all testing. VMware does not verify the results. This level is used for a new or nonmainstream technology that partners want to enable for VMware systems. Today, driver VIB technologies such as Infiniband, ATAoE, and SSD are at this level with nonstandard hardware drivers. VMware directs support calls for VIBs with this acceptance level to the partner's support organization.

CommunitySupported The CommunitySupported acceptance level is for VIBs created by individuals or companies outside of VMware partner programs. VIBs at this level have not gone through any VMware-approved testing program and are not supported by VMware Technical Support or by a VMware partner.

Procedure

1 Connect to each ESXi host and verify that the acceptance level is set to VMwareCertified or VMwareAccepted by running the following command.

```
esxcli software acceptance get
```

2 If the host acceptance level is not VMwareCertified or VMwareAccepted, determine whether any of the VIBs are not at the VMwareCertified or VMwareAccepted level by running the following commands.

```
esxcli software vib list
esxcli software vib get –n vibname
```

3 Remove any VIBs that are at the PartnerSupported or CommunitySupported level by running the following command.

```
esxcli software vib remove ––vibname vib
```

4 Change the acceptance level of the host by running the following command.

```
esxcli software acceptance set ––level acceptance_level
```

Assigning Permissions for ESXi

In most cases, you give privileges to users by assigning permissions to ESXi host objects that are managed by a vCenter Server system. If you are using a standalone ESXi host, you can assign privileges directly.

Assiging Permissions to ESXi Hosts that Are Managed by vCenter Server

If your ESXi host is managed by a vCenter Server, perform management tasks through the vSphere Web Client.

You can select the ESXi host object in the vCenter Server object hierarchy and assing the administrator role to a limited number of users who might perform direct management on the ESXi host. See “Using Roles to Assign Privileges,” on page 123.

Best practice is to create at least one named user account, assign it full administrative privileges on the host, and use this account instead of the root account. Set a highly complex password for the root account and limit the use of the root account. (Do not remove the root account.)

Assigning Permissions to Standalone ESXi Hosts

If your environment does not include a vCenter Server system, the following users are predefined.

- root user. See “root User Privileges,” on page 165.
- vpxuser. See “vpxuser Privileges,” on page 165.
- dcui user. See “dcui User Privileges,” on page 166.

You can add local users and define custom roles from the Management tab of the vSphere Client. See the *vSphere Single Host Management* documentation.

The following roles are predefined:

Read Only	Allows a user to view objects associated with the ESXi host but not to make any changes to objects.
Administrator	Administrator role.
No Access	No access. This is the default. You can override the default as appropriate.

You can manage local users and groups and add local custom roles to an ESXi host using a vSphere Client connected directly to the ESXi host. See the *vSphere Single Host Management* documentation.

Starting with vSphere 6.0, you can use ESXCLI account management commands for managing ESXi local user accounts. You can use ESXCLI permission management commands for setting or removing permissions on both Active Directory accounts (users and groups) and on ESXi local accounts (users only).

NOTE If you define a user for the ESXi host by connecting to the host directly, and a user with the same name also exists in vCenter Server, those users are different. If you assign a role to one of the users, the other user is not assigned the same role.

root User Privileges

By default each ESXi host has a single root user account with the Administrator role. That root user account can be used for local administration and to connect the host to vCenter Server.

This common root account can make it easier to break into an ESXi host and make it harder to match actions to a specific administrator.

Set a highly complex password for the root account and limit the use of the root account, for example, for use when adding a host to vCenter Server. Do not remove the root account. In vSphere 5.1 and later, only the root user and no other named user with the Administrator role is permitted to add a host to vCenter Server.

Best practice is to ensure that any account with the Administrator role on an ESXi host is assigned to a specific user with a named account. Use ESXi Active Directory capabilities, which allow you to manage Active Directory credentials if possible.

IMPORTANT If you remove the access privileges for the root user, you must first create another permission at the root level that has a different user assigned to the Administrator role.

vpxuser Privileges

vCenter Server uses vpxuser privileges when managing activities for the host.

vCenter Server has Administrator privileges on the host that it manages. For example, vCenter Server can move virtual machines to and from hosts and perform configuration changes needed to support virtual machines.

The vCenter Server administrator can perform most of the same tasks on the host as the root user and also schedule tasks, work with templates, and so forth. However, the vCenter Server administrator cannot directly create, delete, or edit local users and groups for hosts. These tasks can only be performed by a user with Administrator permissions directly on each host.

NOTE You cannot manage the vpxuser using Active Directory.

CAUTION Do not change vpxuser in any way. Do not change its password. Do not change its permissions. If you do so, you might experience problems when working with hosts through vCenter Server.

dcui User Privileges

The dcui user runs on hosts and acts with Administrator rights. This user's primary purpose is to configure hosts for lockdown mode from the Direct Console User Interface (DCUI).

This user acts as an agent for the direct console and cannot be modified or used by interactive users.

Using Active Directory to Manage ESXi Users

You can configure ESXi to use a directory service such as Active Directory to manage users.

Creating local user accounts on each host presents challenges with having to synchronize account names and passwords across multiple hosts. Join ESXi hosts to an Active Directory domain to eliminate the need to create and maintain local user accounts. Using Active Directory for user authentication simplifies the ESXi host configuration and reduces the risk for configuration issues that could lead to unauthorized access.

When you use Active Directory, users supply their Active Directory credentials and the domain name of the Active Directory server when adding a host to a domain.

Install or Upgrade vSphere Authentication Proxy

Install vSphere Authentication Proxy to enable ESXi hosts to join a domain without using Active Directory credentials. vSphere Authentication Proxy enhances security for PXE-booted hosts and hosts that are provisioned using Auto Deploy by removing the need to store Active Directory credentials in the host configuration.

If an earlier version of the vSphere Authentication Proxy is installed on your system, this procedure upgrades the vSphere Authentication Proxy to the current version.

You can install vSphere Authentication Proxy on the same machine as the associated vCenter Server, or on a different machine that has network connection to the vCenter Server. vSphere Authentication Proxy is supported with vCenter Server versions 5.0 and later.

The vSphere Authentication Proxy service binds to an IPv4 address for communication with vCenter Server, and does not support IPv6. The vCenter Server instance can be on a host machine in an IPv4-only, IPv4/IPv6 mixed-mode, or IPv6-only network environment, but the machine that connects to the vCenter Server through the vSphere Web Client must have an IPv4 address for the vSphere Authentication Proxy service to work.

Prerequisites

- Install Microsoft .NET Framework 3.5 on the machine where you want to install vSphere Authentication Proxy.
- Verify that you have administrator privileges.
- Verify that the host machine has a supported processor and operating system.

- Verify that the host machine has a valid IPv4 address. You can install vSphere Authentication Proxy on a machine in an IPv4-only or IPv4/IPv6 mixed-mode network environment, but you cannot install vSphere Authentication Proxy on a machine in an IPv6-only environment.
- If you are installing vSphere Authentication Proxy on a Windows Server 2008 R2 host machine, download and install the Windows hotfix described in Windows KB Article 981506 on the support.microsoft.com Web site. If this hotfix is not installed, the vSphere Authentication Proxy Adapter fails to initialize. This problem is accompanied by error messages in `camadapter.log` similar to `Failed to bind CAM website with CTL` and `Failed to initialize CAMAdapter.`
- Download the vCenter Server installer.

Gather the following information to complete the installation or upgrade:

- The location to install vSphere Authentication Proxy, if you are not using the default location.
- The address and credentials for the vCenter Server that vSphere Authentication Proxy will connect to: IP address or name, HTTP port, user name, and password.
- The host name or IP address to identify vSphere Authentication Proxy on the network.

Procedure

1. Add the host machine where you will install the authentication proxy service to the domain.
2. Use the Domain Administrator account to log in to the host machine.
3. In the software installer directory, double-click the `autorun.exe` file to start the installer.
4. Select **VMware vSphere Authentication Proxy** and click **Install**.
5. Follow the wizard prompts to complete the installation or upgrade.

   During installation, the authentication service registers with the vCenter Server instance where Auto Deploy is registered.

When you install the vSphere Authentication Proxy service, the installer creates a domain account with appropriate privileges to run the authentication proxy service. The account name begins with the prefix `CAM–` and has a 32-character, randomly generated password associated with it. The password is set to never expire. Do not change the account settings.

Configure a Host to Use Active Directory

You can configure a host to use a directory service such as Active Directory to manage users and groups.

When you add an ESXi host to Active Directory the DOMAIN group **ESXi Admins** is assigned full administrative access to the host if it exists. If you do not want to make full administrative access available, see VMware Knowledge Base article 1025569 for a workaround.

If a host is provisioned with Auto Deploy, Active Directory credentials cannot be stored on the hosts. You can use the vSphere Authentication Proxy to join the host to an Active Directory domain. Because a trust chain exists between the vSphere Authentication Proxy and the host, the Authentication Proxy can join the host to the Active Directory domain. See "Using vSphere Authentication Proxy," on page 169.

NOTE When you define user account settings in Active Directory, you can limit the computers that a user can log in to by the computer name. By default, no equivalent restrictions are set on a user account. If you set this limitation, LDAP Bind requests for the user account fail with the message `LDAP binding not successful`, even if the request is from a listed computer. You can avoid this issue by adding the netBIOS name for the Active Directory server to the list of computers that the user account can log in to.

Prerequisites

- Verify that you have an Active Directory domain. See your directory server documentation.

- Verify that the host name of ESXi is fully qualified with the domain name of the Active Directory forest.

  fully qualified domain name = host_name.domain_name

Procedure

1 Synchronize the time between ESXi and the directory service system using NTP.

  See "Synchronize ESXi Clocks with a Network Time Server," on page 225 or the VMware Knowledge Base for information about how to synchronize ESXi time with a Microsoft Domain Controller.

2 Ensure that the DNS servers that you configured for the host can resolve the host names for the Active Directory controllers.

  a Browse to the host in the vSphere Web Client object navigator.

  b Click the **Manage** tab and click **Networking**.

  c Click DNS, and verify that the host name and DNS server information for the host are correct.

What to do next

Use the vSphere Web Client to join a directory service domain. For hosts that are provisioned with Auto Deploy, set up the vSphere Authentication Proxy. See "Using vSphere Authentication Proxy," on page 169.

Add a Host to a Directory Service Domain

To have your host use a directory service, you must join the host to the directory service domain.

You can enter the domain name in one of two ways:

- **`name.tld`** (for example, **`domain.com`**): The account is created under the default container.
- **`name.tld/container/path`** (for example, **`domain.com/OU1/OU2`**): The account is created under a particular organizational unit (OU).

To use the vSphere Authentication Proxy service, see "Using vSphere Authentication Proxy," on page 169.

Procedure

1 Browse to the host in the vSphere Web Client inventory.

2 Click the **Manage** tab and click **Settings**.

3 Under System, select **Authentication Services**.

4 Click **Join Domain**.

5 Enter a domain.

  Use the form **`name.tld`** or **`name.tld/container/path`**.

6 Enter the user name and password of a directory service user who has permissions to join the host to the domain, and click **OK**.

7 (Optional) If you intend to use an authentication proxy, enter the proxy server IP address.

8 Click **OK** to close the Directory Services Configuration dialog box.

View Directory Service Settings

You can view the type of directory server, if any, that the host uses to authenticate users and the directory server settings.

Procedure

1 Browse to the host in the vSphere Web Client inventory.

2 Click the **Manage** tab and click **Settings**.

3 Under System, select **Authentication Services**.

The Authentication Services page displays the directory service and domain settings.

Using vSphere Authentication Proxy

When you use the vSphere Authentication Proxy, you do not need to transmit Active Directory credentials to the host. Users supply the domain name of the Active Directory server and the IP address of the authentication proxy server when they add a host to a domain.

vSphere Authentication Proxy is especially helpful when used in conjunction with Auto Deploy. You set up a reference host that points to Authentication Proxy and set up a rule that applies the reference host's profile to any ESXi host provisioned with Auto Deploy. Even you use vSphere Authentication Proxy in an environment that uses certificates that are provisioned by VMCA or third-party certificates, the process works seamlessly as long as you follow the instructions for using custom certificates with Auto Deploy. See "Use Custom Certificates with Auto Deploy," on page 148.

NOTE You cannot use vSphere Authentication Proxy in an environment that supports only IPv6.

Install or Upgrade vSphere Authentication Proxy

Install vSphere Authentication Proxy to enable ESXi hosts to join a domain without using Active Directory credentials. vSphere Authentication Proxy enhances security for PXE-booted hosts and hosts that are provisioned using Auto Deploy by removing the need to store Active Directory credentials in the host configuration.

If an earlier version of the vSphere Authentication Proxy is installed on your system, this procedure upgrades the vSphere Authentication Proxy to the current version.

You can install vSphere Authentication Proxy on the same machine as the associated vCenter Server, or on a different machine that has network connection to the vCenter Server. vSphere Authentication Proxy is supported with vCenter Server versions 5.0 and later.

The vSphere Authentication Proxy service binds to an IPv4 address for communication with vCenter Server, and does not support IPv6. The vCenter Server instance can be on a host machine in an IPv4-only, IPv4/IPv6 mixed-mode, or IPv6-only network environment, but the machine that connects to the vCenter Server through the vSphere Web Client must have an IPv4 address for the vSphere Authentication Proxy service to work.

Prerequisites

- Install Microsoft .NET Framework 3.5 on the machine where you want to install vSphere Authentication Proxy.
- Verify that you have administrator privileges.
- Verify that the host machine has a supported processor and operating system.
- Verify that the host machine has a valid IPv4 address. You can install vSphere Authentication Proxy on a machine in an IPv4-only or IPv4/IPv6 mixed-mode network environment, but you cannot install vSphere Authentication Proxy on a machine in an IPv6-only environment.
- If you are installing vSphere Authentication Proxy on a Windows Server 2008 R2 host machine, download and install the Windows hotfix described in Windows KB Article 981506 on the support.microsoft.com Web site. If this hotfix is not installed, the vSphere Authentication Proxy Adapter fails to initialize. This problem is accompanied by error messages in `camadapter.log` similar to `Failed to bind CAM website with CTL` and `Failed to initialize CAMAdapter.`
- Download the vCenter Server installer.

Gather the following information to complete the installation or upgrade:

- The location to install vSphere Authentication Proxy, if you are not using the default location.
- The address and credentials for the vCenter Server that vSphere Authentication Proxy will connect to: IP address or name, HTTP port, user name, and password.
- The host name or IP address to identify vSphere Authentication Proxy on the network.

Procedure

1. Add the host machine where you will install the authentication proxy service to the domain.
2. Use the Domain Administrator account to log in to the host machine.
3. In the software installer directory, double-click the `autorun.exe` file to start the installer.
4. Select **VMware vSphere Authentication Proxy** and click **Install**.
5. Follow the wizard prompts to complete the installation or upgrade.

   During installation, the authentication service registers with the vCenter Server instance where Auto Deploy is registered.

When you install the vSphere Authentication Proxy service, the installer creates a domain account with appropriate privileges to run the authentication proxy service. The account name begins with the prefix `CAM–` and has a 32-character, randomly generated password associated with it. The password is set to never expire. Do not change the account settings.

Configure a Host to Use the vSphere Authentication Proxy for Authentication

After you install the vSphere Authentication Proxy service (CAM service), you must configure the host to use the authentication proxy server to authenticate users.

Prerequisites

Install the vSphere Authentication Proxy service (CAM service) on a host. See "Install or Upgrade vSphere Authentication Proxy," on page 166.

Procedure

1. Use the IIS manager on the host to set up the DHCP range.

   Setting the range allows hosts that are using DHCP in the management network to use the authentication proxy service.

Option	Action
For IIS 6	a Browse to **Computer Account Management Web Site**. b Right-click the virtual directory **CAM ISAPI**. c Select **Properties > Directory Security > Edit IP Address and Domain Name Restrictions > Add Group of Computers**.
For IIS 7	a Browse to **Computer Account Management Web Site**. b Click the **CAM ISAPI** virtual directory in the left pane and open **IPv4 Address and Domain Restrictions**. c Select **Add Allow Entry > IPv4 Address Range**.

2 If a host is not provisioned by Auto Deploy, change the default SSL certificate to a self-signed certificate or to a certificate signed by a commercial certificate authority (CA).

Option	Description
VMCA certificate	If you are using the default VMCA-signed certificates, you have to ensure that the authentication proxy host trusts the VMCA certificate. a Manually add the VMCA certificate to the Trusted Root Certificate Authorities certificate store. b Add the VMCA-signed certificate (`root.cer`) to the local trust certificate store on the system where the authentication proxy service is installed. You can find the file in `C:\ProgramData\VMware\CIS\data\vmca`. c Restart the vSphere Authentication Proxy service.
Third-party CA-signed certificate	Add the CA-signed certificate (DER-encoded) to the local trust certificate store on the system where the authentication proxy service is installed and restart the vSphere Authentication Proxy service. ■ For Windows 2003, copy the certificate file to `C:\Documents and Settings\All Users\Application Data\VMware\vSphere Authentication Proxy\trust`. ■ For Windows 2008, copy the certificate file to `C:\Program Data\VMware\vSphere Authentication Proxy\trust`.

Setting up vSphere Authentication Proxy

Your ESXi hosts can use a vSphere Authentication proxy if they have the Authentication Proxy certificate information.

You need only authenticate the server once.

NOTE ESXi and the Authentication Proxy server must be able to authenticate. Make sure that this authentication functionality is enabled at all times. If you must disable authentication, you can use the Advanced Settings dialog box to set the `UserVars.ActiveDirectoryVerifyCAMCertifcate` attribute to 0.

Export vSphere Authentication Proxy Certificate

To authenticate the vSphere Authentication Proxy to ESXi, you must provide ESXi with the proxy server certificate.

Prerequisites

Install the vSphere Authentication Proxy service (CAM service) on a host. See "Install or Upgrade vSphere Authentication Proxy," on page 166.

Procedure

1 On the authentication proxy server system, use the IIS Manager to export the certificate.

Option	Action
For IIS 6	a Right-click **Computer Account Management Web Site**. b Select **Properties > Directory Security > View Certificate**.
For IIS 7	a Click **Computer Account Management Web Site** in the left pane. b Select **Bindings** to open the Site Bindings dialog box. c Select **https** binding. d Select **Edit > View SSL Certificate** .

2 Select **Details > Copy to File**.

3 Select the options **Do Not Export the Private Key** and **Base-64 encoded X.509 (CER)**.

What to do next

Import the certificate to ESXi.

Import a Proxy Server Certificate to ESXi

To authenticate the vSphere Authentication Proxy server to ESXi, upload the proxy server certificate to ESXi.

You use the vSphere Web Client user interface to upload the vSphere Authentication Proxy server certificate to ESXi.

Prerequisites

Install the vSphere Authentication Proxy service (CAM service) on a host. See "Install or Upgrade vSphere Authentication Proxy," on page 166.

Export the vSphere Authentication Proxy server certificate as described in "Export vSphere Authentication Proxy Certificate," on page 171.

Procedure

1 Browse to the host, click the **Manage** tab, and click **Authentication Services**.

2 Click **Import Certificate**.

3 Enter the full path to the authentication proxy server certificate file on the host and the IP address of the authentication proxy server.

Use the form [*datastore name*] *file path* to enter the path to the proxy server.

4 Click **OK**.

Use vSphere Authentication Proxy to Add a Host to a Domain

When you join a host to a directory service domain, you can use the vSphere Authentication Proxy server for authentication instead of transmitting user-supplied Active Directory credentials.

You can enter the domain name in one of two ways:

- **`name.tld`** (for example, **`domain.com`**): The account is created under the default container.
- **`name.tld/container/path`** (for example, **`domain.com/OU1/OU2`**): The account is created under a particular organizational unit (OU).

Prerequisites

- Connect to a vCenter Server system with the vSphere Web Client.
- If ESXi is configured with a DHCP address, set up the DHCP range.
- If ESXi is configured with a static IP address, verify that its associated profile is configured to use the vSphere Authentication Proxy service to join a domain so that the authentication proxy server can trust the ESXi IP address.
- If ESXi is using a VMCA-signed certificate, verify that the host has been added to vCenter Server. This allows the authentication proxy server to trust ESXi.
- If ESXi is using a CA-signed certificate and is not provisioned by Auto Deploy, verify that the CA certificate has been added to the local trust certificate store of the authentication proxy server as described in "Configure a Host to Use the vSphere Authentication Proxy for Authentication," on page 170.
- Authenticate the vSphere Authentication Proxy server to the host.

Procedure

1 Browse to the host in the vSphere Web Client and click the **Manage** tab.

2 Click **Settings** and select **Authentication Services**.

3 Click **Join Domain**.

4 Enter a domain.

Use the form `name.tld` or `name.tld/container/path`.

5 Select **Using Proxy Server**.

6 Enter the IP address of the authentication proxy server.

7 Click **OK**.

Replace the Authentication Proxy Certificate for the ESXi Host

You can import a certificate from a trusted certificate authority from the vSphere Web Client

Prerequisites

- Upload the authentication proxy certificate file to the ESXi host.

Procedure

1 In the vSphere Web Client, select the ESXi host.

2 In the **Settings** tab, select **Authentication Services** in the **System** area.

3 Click **Import Certificate**.

4 Enter the SSL certificate path and the vSphere Authentication Proxy server.

Configuring Smart Card Authentication for ESXi

You can use smart card authentication to log in to the ESXi Direct Console User Interface (DCUI) by using a Personal Identity Verification (PIV), Common Access Card (CAC) or SC650 smart card instead of the default prompt for a user name and password.

A smart card is a small plastic card with an embedded integrated circuit chip. Many government agencies and large enterprises use smart card based two-factor authentication to increase the security of their systems and comply with security regulations.

When smart card authentication is enabled on an ESXi host, the DCUI prompts you for a valid smart card and PIN combination instead of the default prompt for a user name and password.

1 When you insert the smart card into the smart card reader, the ESXi host reads the credentials on it.

2 The ESXi DCUI displays your login ID, and prompts you for your PIN.

3 After you enter your PIN, the ESXi host matches it with the PIN stored on the smart card and verifies the certificate on the smart card with Active Directory.

4 After a successful verification of the smart card certificate, ESXi logs you in to the DCUI.

You can switch to user name and password authentication from the DCUI by pressing F3.

The chip on the smart card locks after a few consecutive incorrect PIN entries, usually three. If a smart card is locked, only selected personnel can unlock it.

Enable Smart Card Authentication

Enable smart card authentication to prompt for smart card and PIN combination to log in to the ESXi DCUI.

Prerequisites

- Set up the infrastructure to handle smart card authentication, such as accounts in the Active Directory domain, smart card readers, and smart cards.
- Configure ESXi to join an Active Directory domain that supports smart card authentication. For more information, see "Using Active Directory to Manage ESXi Users," on page 166.
- Use the vSphere Web Client to add root certificates. See "Certificate Management for ESXi Hosts," on page 137.

Procedure

1. In the vSphere Web Client, browse to the host.
2. Click the **Manage** tab and click **Settings**.
3. Under System, select **Authentication Services**.

   You see the current smart card authentication status and a list with imported certificates.
4. In the Smart Card Authentication panel, click **Edit**.
5. In the Edit Smart Card Authentication dialog box, select the Certificates page.
6. Add trusted Certificate Authority (CA) certificates, for example, root and intermediary CA certificates.
7. Open the Smart Card Authentication page, select the **Enable Smart Card Authentication** check box, and click **OK**.

Disable Smart Card Authentication

Disable smart card authentication to return to the default user name and password authentication for ESXi DCUI login.

Procedure

1. In the vSphere Web Client, browse to the host.
2. Click the **Manage** tab and click **Settings**.
3. Under System, select **Authentication Services**.

   You see the current smart card authentication status and a list with imported certificates.
4. In the Smart Card Authentication panel, click **Edit**.
5. On the Smart Card Authentication page, deselect the **Enable Smart Card Authentication** check box, and click **OK**.

Authenticating User Credentials in Case of Connectivity Problems

If the Active Directory (AD) domain server is not reachable, you can log in to the ESXi DCUI by using user name and password authentication to perform emergency actions on the host.

In exceptional circumstances, the AD domain server is not reachable to authenticate the user credentials on the smart card because of connectivity problems, network outage, or disasters. If the connection to the AD server is lost, you can log in to the ESXi DCUI by using the credentials of a local ESXi user. This lets you preform diagnostics or other emergency actions. The fallback to user name and password login is logged. When the connectivity to AD is restored, smart card authentication is enabled again.

NOTE Loss of network connectivity to vCenter Server does not affect smart card authentication if the Active Directory (AD) domain server is available.

Using Smart Card Authentication in Lockdown Mode

When enabled, lockdown mode on the ESXi host increases the security of the host and limits access to the DCUI. Lockdown mode might disable the smart card authentication feature.

In normal lockdown mode, only users on the Exception Users list with administrator privileges can access the DCUI. Exception users are host local users or Active Directory users with permissions defined locally for the ESXi host. If you want to use smart card authentication in normal lockdown mode, you must add users to the Exception Users list from the vSphere Web Client. These users do not lose their permissions when the host enters normal lockdown mode and can log in to the DCUI. For more information, see "Specify Lockdown Mode Exception Users," on page 163.

In strict lockdown mode, the DCUI service is stopped. As a result, you cannot access the host by using smart card authentication.

ESXi SSH Keys

You can use SSH keys to restrict, control, and secure access to an ESXi host. By using an SSH key, you can allow trusted users or scripts to log in to a host without specifying a password.

You can copy the SSH key to the host by using the `vifs` vSphere CLI command. See *Getting Started with vSphere Command-Line Interfaces* for information on installing and using the vSphere CLI command set. It is also possible to use HTTPS PUT to copy the SSK key to the host.

Instead of generating the keys externally and uploading them, you can create the keys on the ESXi host and download them. See VMware Knowledge Base article 1002866.

Enabling SSH and adding SSH keys to the host has inherent risks and is not recommended in a hardened environment. See "Disable Authorized (SSH) Keys," on page 137.

NOTE For ESXi 5.0 and earlier, a user with an SSH key can access the host even when the host is in lockdown mode. This is fixed in ESXi 5.1.

SSH Security

You can use SSH to remotely log in to the ESXi Shell and perform troubleshooting tasks for the host.

SSH configuration in ESXi is enhanced to provide a high security level.

Version 1 SSH protocol disabled	VMware does not support Version 1 SSH protocol and uses Version 2 protocol exclusively. Version 2 eliminates certain security problems present in Version 1 and provides you with a safe way to communicate with the management interface.
Improved cipher strength	SSH supports only 256-bit and 128-bit AES ciphers for your connections.

These settings are designed to provide solid protection for the data you transmit to the management interface through SSH. You cannot change these settings.

Upload an SSH Key Using a vifs Command

You can use authorized keys to log in to a host with SSH. You can upload authorized keys with a `vifs` command.

Authorized keys allow you to authenticate remote access to a host. When users or scripts try to access a host with SSH, the key provides authentication without a password. With authorized keys you can automate authentication, which is useful when you write scripts to perform routine tasks.

You can upload the following types of SSH keys to a host:

- Authorized keys file for root user
- DSA key
- DSA public key
- RSA key
- RSA public key

IMPORTANT Do not modify the `/etc/ssh/sshd_config` file.

Procedure

- At the command line, use the `vifs` command to upload the SSH key to appropriate location.

  ```
  vifs --server hostname --username username --put filename /host/ssh_host_dsa_key_pub
  ```

Type of key	Location
Authorized key files for the root user	`/host/ssh_root_authorized keys` You must have full administrator privileges to upload this file.
DSA keys	`/host/ssh_host_dsa_key`
DSA public keys	`/host/ssh_host_dsa_key_pub`
RSA keys	`/host/ssh_host_rsa_key`
RSA public keys	`/host/ssh_host_rsa_key_pub`

Upload an SSH Key Using HTTPS PUT

You can use authorized keys to log in to a host with SSH. You can upload authorized keys with HTTPS PUT.

Authorized keys allow you to authenticate remote access to a host. When users or scripts try to access a host with SSH, the key provides authentication without a password. With authorized keys you can automate authentication, which is useful when you write scripts to perform routine tasks.

You can upload the following types of SSH keys to a host using HTTPS PUT:

- Authorized keys file for root user
- DSA key
- DSA public key
- RSA key
- RSA public key

IMPORTANT Do not modify the `/etc/ssh/sshd_config` file.

Procedure

1 In your upload application, open the key file.

2 Publish the file to the following locations.

Type of key	Location
Authorized key files for the root user	`https://hostname_or_IP_address/host/ssh_root_authorized_keys` You must have full administrator privileges on the host to upload this file.
DSA keys	`https://hostname_or_IP_address/host/ssh_host_dsa_key`
DSA public keys	`https://hostname_or_IP_address/host/ssh_host_dsa_key_pub`
RSA keys	`https://hostname_or_IP_address/host/ssh_host_rsa_key`
RSA public keys	`https://hostname_or_IP_address/host/ssh_host_rsa_key_pub`

Using the ESXi Shell

The ESXi Shell (formerly Tech Support Mode or TSM) is disabled by default on ESXi. You can enable local and remote access to the shell if necessary.

Enable the ESXi Shell for troubleshooting only. The ESXi Shell can be enabled and disabled whether or not the host is running in lockdown mode. See "Lockdown Mode Behavior," on page 159.

ESXi Shell — Enable this service to access the ESXi Shell locally.

SSH — Enable this service to access the ESXi Shell remotely using SSH. You can upload SSH keys to your hosts See "ESXi SSH Keys," on page 175.

Direct Console UI (DCUI) — When you enable this service while running in lockdown mode, you can log in locally to the direct console user interface as the root user and disable lockdown mode. You can then access the host using a direct connection to the vSphere Client or by enabling the ESXi Shell.

The root user and users with the Administrator role can access the ESXi Shell. Users who are in the Active Directory group ESX Admins are automatically assigned the Administrator role. By default, only the root user can execute system commands (such as `vmware -v`) using the ESXi Shell.

NOTE Do not enable the ESXi Shell until you actually need access.

- Use the vSphere Web Client to Enable Access to the ESXi Shell on page 178

  You can use the vSphere Web Client to enable local and remote (SSH) access to the ESXi Shell and to set the idle timeout and availability timeout.

- Use the Direct Console User Interface (DCUI) to Enable Access to the ESXi Shell on page 180

  The Direct Console User Interface (DCUI) allows you to interact with the host locally using text-based menus. Evaluate carefully whether the security requirements of your environment support enabling the Direct Console User Interface.

- Log in to the ESXi Shell for Troubleshooting on page 181

  Perform ESXi configuration tasks with the vSphere Web Client. the vSphere CLI, or vSphere PowerCLI. Log in to the ESXi Shell (formerly Tech Support Mode or TSM) for troubleshooting purposes only.

Use the vSphere Web Client to Enable Access to the ESXi Shell

You can use the vSphere Web Client to enable local and remote (SSH) access to the ESXi Shell and to set the idle timeout and availability timeout.

NOTE Access the host by using the vSphere Web Client, remote command-line tools (vCLI and PowerCLI), and published APIs. Do not enable remote access to the host using SSH unless special circumstances require that you enable SSH access.

Prerequisites

If you want to use an authorized SSH key, you can upload it. See "ESXi SSH Keys," on page 175.

Procedure

1. Browse to the host in the vSphere Web Client inventory.
2. Click the **Manage** tab and click **Settings**.
3. Under System, select **Security Profile**.
4. In the Services panel, click **Edit**.
5. Select a service from the list.
   - ESXi Shell
   - SSH
   - Direct Console UI
6. Click **Service Details** and select the startup policy **Start and stop manually**.

   When you select **Start and stop manually**, the service does not start when you reboot the host. If you want the service to start when you reboot the host, select **Start and stop with host**.
7. Select **Start** to enable the service.
8. Click **OK**.

What to do next

Set the availability and idle timeouts for the ESXi Shell. See "Create a Timeout for ESXi Shell Availability in the vSphere Web Client," on page 179 and "Create a Timeout for Idle ESXi Shell Sessions in the vSphere Web Client," on page 179

Create a Timeout for ESXi Shell Availability in the vSphere Web Client

The ESXi Shell is disabled by default. You can set an availability timeout for the ESXi Shell to increase security when you enable the shell.

The availability timeout setting is the amount of time that can elapse before you must log in after the ESXi Shell is enabled. After the timeout period, the service is disabled and users are not allowed to log in.

Procedure

1 Browse to the host in the vSphere Web Client inventory.

2 Click the **Manage** tab and click **Settings**.

3 Under System, select **Advanced System Settings**.

4 Select UserVars.ESXiShellTimeOut and click the **Edit** icon.

5 Enter the idle timeout setting.

   You must restart the SSH service and the ESXi Shell service for the timeout to take effect.

6 Click **OK**.

If you are logged in when the timeout period elapses, your session will persist. However, after you log out or your session is terminated, users are not allowed to log in.

Create a Timeout for Idle ESXi Shell Sessions in the vSphere Web Client

If a user enables the ESXi Shell on a host, but forgets to log out of the session, the idle session remains connected indefinitely. The open connection can increase the potential for someone to gain privileged access to the host. You can prevent this by setting a timeout for idle sessions.

The idle timeout is the amount of time that can elapse before a user is logged out of an idle interactive session. You can control the amount of time for both local and remote (SSH) session from the Direct Console Interface (DCUI) or from the vSphere Web Client.

Procedure

1 Browse to the host in the vSphere Web Client inventory.

2 Click the **Manage** tab and click **Settings**.

3 Under System, select **Advanced System Settings**.

4 Select UserVars.ESXiShellInteractiveTimeOut, click the **Edit** icon, and enter the timeout setting.

5 Restart the ESXi Shell service and the SSH service for the timeout to take effect.

If the session is idle, users are logged out after the timeout period elapses.

Use the Direct Console User Interface (DCUI) to Enable Access to the ESXi Shell

The Direct Console User Interface (DCUI) allows you to interact with the host locally using text-based menus. Evaluate carefully whether the security requirements of your environment support enabling the Direct Console User Interface.

You can use the Direct Console User Interface to enable local and remote access to the ESXi Shell.

NOTE Changes made to the host using the Direct Console User Interface, the vSphere Web Client, ESXCLI, or other administrative tools are committed to permanent storage every hour or upon graceful shutdown. Changes might be lost if the host fails before they are committed.

Procedure

1 From the Direct Console User Interface, press F2 to access the System Customization menu.

2 Select **Troubleshooting Options** and press Enter.

3 From the Troubleshooting Mode Options menu, select a service to enable.

- Enable ESXi Shell
- Enable SSH

4 Press Enter to enable the service.

5 Press Esc until you return to the main menu of the Direct Console User Interface.

What to do next

Set the availability and idle timeouts for the ESXi Shell. See "Create a Timeout for ESXi Shell Availability in the Direct Console User Interface," on page 180 and "Create a Timeout for Idle ESXi Shell Sessions," on page 181.

Create a Timeout for ESXi Shell Availability in the Direct Console User Interface

The ESXi Shell is disabled by default. You can set an availability timeout for the ESXi Shell to increase security when you enable the shell.

The availability timeout setting is the amount of time that can elapse before you must log in after the ESXi Shell is enabled. After the timeout period, the service is disabled and users are not allowed to log in.

Procedure

1 From the Troubleshooting Mode Options menu, select **Modify ESXi Shell and SSH timeouts** and press Enter.

2 Enter the availability timeout.

You must restart the SSH service and the ESXi Shell service for the timeout to take effect.

3 Press Enter and press Esc until you return to the main menu of the Direct Console User Interface.

4 Click **OK**.

If you are logged in when the timeout period elapses, your session will persist. However, after you log out or your session is terminated, users are not allowed to log in.

Create a Timeout for Idle ESXi Shell Sessions

If a user enables the ESXi Shell on a host, but forgets to log out of the session, the idle session remains connected indefinitely. The open connection can increase the potential for someone to gain privileged access to the host. You can prevent this by setting a timeout for idle sessions.

The idle timeout is the amount of time that can elapse before the user is logged out of an idle interactive sessions. Changes to the idle timeout apply the next time a user logs in to the ESXi Shell and do not affect existing sessions.

You can specify the timeout from the Direct Console User Interface in seconds, or from the vSphere Web Client in minutes.

Procedure

1 From the Troubleshooting Mode Options menu, select **Modify ESXi Shell and SSH timeouts** and press Enter.

2 Enter the idle timeout, in seconds.

You must restart the SSH service and the ESXi Shell service for the timeout to take effect.

3 Press Enter and press Esc until you return to the main menu of the Direct Console User Interface.

If the session is idle, users are logged out after the timeout period elapses.

Log in to the ESXi Shell for Troubleshooting

Perform ESXi configuration tasks with the vSphere Web Client. the vSphere CLI, or vSphere PowerCLI. Log in to the ESXi Shell (formerly Tech Support Mode or TSM) for troubleshooting purposes only.

Procedure

1 Log in to the ESXi Shell using one of the following methods.

- If you have direct access to the host, press Alt+F1 to open the login page on the machine's physical console.
- If you are connecting to the host remotely, use SSH or another remote console connection to start a session on the host.

2 Enter a user name and password recognized by the host.

Modifying ESXi Web Proxy Settings

When you modify Web proxy settings, you have several encryption and user security guidelines to consider.

NOTE Restart the host process after making any changes to host directories or authentication mechanisms.

- Do not set up certificates that use a password or pass phrases. ESXi does not support Web proxies that use passwords or pass phrases, also known as encrypted keys. If you set up a Web proxy that requires a password or pass phrase, ESXi processes cannot start correctly.
- To support encryption for user names, passwords, and packets, SSL is enabled by default for vSphere Web Services SDK connections. If you want to configure these connections so that they do not encrypt transmissions, disable SSL for your vSphere Web Services SDK connection by switching the connection from HTTPS to HTTP.

  Consider disabling SSL only if you created a fully trusted environment for these clients, where firewalls are in place and transmissions to and from the host are fully isolated. Disabling SSL can improve performance, because you avoid the overhead required to perform encryption.

- To protect against misuse of ESXi services, most internal ESXi services are accessible only through port 443, the port used for HTTPS transmission. Port 443 acts as a reverse proxy for ESXi. You can see a list of services on ESXi through an HTTP welcome page, but you cannot directly access the Storage Adapters services without proper authorization.

  You can change this configuration so that individual services are directly accessible through HTTP connections. Do not make this change unless you are using ESXi in a fully trusted environment.

- When you upgrade your environment, the certificate remains in place.

vSphere Auto Deploy Security Considerations

To best protect your environment, be aware of security risks that might exist when you use Auto Deploy with host profiles.

Networking Security

Secure your network as you would for any other PXE-based deployment method. vSphere Auto Deploy transfers data over SSL to prevent casual interference and snooping. However, the authenticity of the client or of the Auto Deploy server is not checked during a PXE boot.

You can greatly reduce the security risk of Auto Deploy by completely isolating the network where Auto Deploy is used.

Boot Image and Host Profile Security

The boot image that the vSphere Auto Deploy server downloads to a machine can have the following components.

- The VIB packages that the image profile consists of are always included in the boot image.
- The host profile and host customization are included in the boot image if Auto Deploy rules are set up to provision the host with a host profile or a host customization setting.
  - The administrator (root) password and user passwords that are included with host profile and host customization are MD5 encrypted.
  - Any other passwords associated with profiles are in the clear. If you set up Active Directory by using host profiles, the passwords are not protected.

    Use the vSphere Authentication Service for setting up Active Directory to avoid exposing the Active Directory passwords. If you set up Active Directory using host profiles, the passwords are not protected.
- The host's public and private SSL key and certificate are included in the boot image.

Managing ESXi Log Files

Log files are an important component of troubleshooting attacks and obtaining information about breaches of host security. Logging to a secure, centralized log server can help prevent log tampering. Remote logging also provides a long-term audit record.

Take the following measures to increase the security of the host.

- Configure persistent logging to a datastore. By default, the logs on ESXi hosts are stored in the in-memory file system. Therefore, they are lost when you reboot the host, and only 24 hours of log data is stored. When you enable persistent logging, you have a dedicated record of server activity available for the host.
- Remote logging to a central host allows you to gather log files onto a central host, where you can monitor all hosts with a single tool. You can also do aggregate analysis and searching of log data, which might reveal information about things like coordinated attacks on multiple hosts.

- Configure remote secure syslog on ESXi hosts using a remote command line such as vCLI or PowerCLI, or using an API client.
- Query the syslog configuration to make sure that a valid syslog server has been configured, including the correct port.

Configure Syslog on ESXi Hosts

All ESXi hosts run a syslog service (`vmsyslogd`), which logs messages from the VMkernel and other system components to log files. Up to 30 hosts are supported.

You can use the vSphere Web Client or the `esxcli system syslog` vCLI command to configure the syslog service.

For more information about using vCLI commands, see *Getting Started with vSphere Command-Line Interfaces*.

Procedure

1 In the vSphere Web Client inventory, select the host.

2 Click the **Manage** tab.

3 In the System panel, click **Advanced System Settings**.

4 Locate the **Syslog** section of the Advanced System Settings list.

5 To set up logging globally, select the setting to change and click the Edit icon.

Option	Description
Syslog.global.defaultRotate	Sets the maximum number of archives to keep. You can set this number globally and for individual subloggers.
Syslog.global.defaultSize	Sets the default size of the log, in KB, before the system rotates logs. You can set this number globally and for individual subloggers.
Syslog.global.LogDir	Directory where logs are stored. The directory can be located on mounted NFS or VMFS volumes. Only the `/scratch` directory on the local file system is persistent across reboots. The directory should be specified as [*datastorename*] *path_to_file* where the path is relative to the root of the volume backing the datastore. For example, the path `[storage1] /systemlogs` maps to the path `/vmfs/volumes/storage1/systemlogs`.
Syslog.global.logDirUnique	Selecting this option creates a subdirectory with the name of the ESXi host under the directory specified by **Syslog.global.LogDir**. A unique directory is useful if the same NFS directory is used by multiple ESXi hosts.
Syslog.global.LogHost	Remote host to which syslog messages are forwarded and port on which the remote host receives syslog messages. You can include the protocol and the port, for example, `ssl://hostName1:1514`. UDP (default), TCP, and SSL are supported. The remote host must have syslog installed and correctly configured to receive the forwarded syslog messages. See the documentation for the syslog service installed on the remote host for information on configuration.

6 (Optional) To overwrite the default log size and log rotation for any of the logs.

   a Click the name of the log you that want to customize.

   b Click the Edit icon and enter the number of rotations and log size you want.

7 Click **OK**.

Changes to the syslog options take effect immediately.

ESXi Log File Locations

ESXi records host activity in log files, using a syslog facility.

Component	Location	Purpose
VMkernel	`/var/log/vmkernel.log`	Records activities related to virtual machines and ESXi.
VMkernel warnings	`/var/log/vmkwarning.log`	Records activities related to virtual machines.
VMkernel summary	`/var/log/vmksummary.log`	Used to determine uptime and availability statistics for ESXi (comma separated).
ESXi host agent log	`/var/log/hostd.log`	Contains information about the agent that manages and configures the ESXi host and its virtual machines.
vCenter agent log	`/var/log/vpxa.log`	Contains information about the agent that communicates with vCenter Server (if the host is managed by vCenter Server).
Shell log	`/var/log/vpxa.log`	Contains a record of all commands typed into the ESXi Shell as well as shell events (for example, when the shell was enabled).
Authentication	`/var/log/auth.log`	Contains all events related to authentication for the local system.
System messages	`/var/log/syslog.log`	Contains all general log messages and can be used for troubleshooting. This information was formerly located in the messages log file.
Virtual machines	The same directory as the affected virtual machine's configuration files, named vmware.log and vmware*.log. For example, `/vmfs/volumes/`*`datastore/virtual machine`*`/vwmare.log`	Contains virtual machine power events, system failure information, tools status and activity, time sync, virtual hardware changes, vMotion migrations, machine clones, and so on.

Securing Fault Tolerance Logging Traffic

When you enable Fault Tolerance (FT), VMware vLockstep captures inputs and events that occur on a Primary VM and sends them to the Secondary VM, which is running on another host.

This logging traffic between the Primary and Secondary VMs is unencrypted and contains guest network and storage I/O data, as well as the memory contents of the guest operating system. This traffic can include sensitive data such as passwords in plaintext. To avoid such data being divulged, ensure that this network is secured, especially to avoid "man-in-the-middle" attacks. For example, use a private network for FT logging traffic.

ESXi Security Best Practices

Following ESXi security best practices helps ensure the integrity of your vSphere deployment.

Verify Installation Media

Always check the SHA1 hash after downloading an ISO, offline bundle, or patch to ensure integrity and authenticity of the downloaded files. If you obtain physical media from VMware and the security seal is broken, return the software to VMware for a replacement.

After downloading media, use the MD5 sum value to verify the integrity of the download. Compare the MD5 sum output with the value posted on the VMware website. Each operating system has a different method and tool for checking MD5 sum values. For Linux use the "md5sum" command. For Microsoft Windows, you can download an add-on product

Check CRLs Manually

By default, an ESXi host does not support CRL checking. You must search for and remove revoked certificates manually. These are typically custom generated certificates from a corporate certificate authority or 3rd party authority. Most corporations have scripts in place to find and replace revoked SSL certificates on your ESXi host.

Monitor the ESX Admins Active Directory Group

The Active Directory group used by vSphere is defined by the `plugins.hostsvc.esxAdminsGroup` advanced system setting. By default this option is set to ESX Admins. All members of the ESX Admins group are granted full administrative access to all ESXi hosts in the domain. Monitor Active Directory for the creation of this group and limit membership to highly trusted users and groups.

Configuration Files

Although most ESXi configuration settings are controlled with an API, a limited number of configuration files affects the host directly. These files are exposed through the vSphere file transfer API, which uses HTTPS. If you make any changes to these files, you must also perform the corresponding administrative action such as making a configuration change.

NOTE Do not attempt to monitor files that are NOT exposed via this file-transfer API, since this can result in a destabilized system.

Use vmkfstools to Erase Sensitive Data

When you delete a VMDK file with sensitive data, shut down or stop the virtual machine, and then issue the vCLI command `vmkfstools –writezeroes` on that file before you delete the file from the datastore.

PCI and PCIe Devices and ESXi

Using the VMware DirectPath I/O feature to pass through a PCI or PCIe device to a virtual machine results in a potential security vulnerability. The vulnerability can be triggered by buggy or malicious code, such as a device driver, running in privileged mode in the guest OS. Industry-standard hardware and firmware does not currently have sufficient error containment support to make it possible for ESXi to fully close the vulnerability.

VMware recommends that you use PCI or PCIe passthrough to a virtual machine only if the virtual machine is owned and administered by a trusted entity. You must be sure that this entity does not to attempt to crash or exploit the host from the virtual machine.

Your host might be compromised in one of the following ways.

- The guest OS might generate an unrecoverable PCI or PCIe error. Such an error does not corrupt data, but can crash the ESXi host. Such errors might occur because of bugs or incompatibilities in the hardware devices that are being passed through, or because of problems with drivers in the guest OS.
- The guest OS might generate a Direct Memory Access (DMA) operation that causes an IOMMU page fault on the ESXi host, for example, if the DMA operation targets an address outside the virtual machine's memory. On some machines, host firmware configures IOMMU faults to report a fatal error through a non-maskable interrupt (NMI), which causes the ESXi host to crash. This problem might occur because of problems with the drivers in the guest OS.
- If the operating system on the ESXi host is not using interrupt remapping, the guest OS might inject a spurious interrupt into the ESXi host on any vector. ESXi currently uses interrupt remapping on Intel platforms where it is available; interrupt mapping is part of the Intel VT-d feature set. ESXi does not use interrupt mapping on AMD platforms. A spurious interrupt most likely results in a crash of the ESXi host; however, other ways to exploit these interrupts might exist in theory.

Securing vCenter Server Systems 6

Securing vCenter Server includes ensuring security of the host where vCenter Server is running, following best practices for assigning privileges and roles, and verifying the integrity of the clients that connect to vCenter Server.

This chapter includes the following topics:

- "vCenter Server Security Best Practices," on page 187
- "Verify Thumbprints for Legacy ESXi Hosts," on page 191
- "Verify that SSL Certificate Validation Over Network File Copy Is Enabled," on page 192
- "vCenter Server TCP and UDP Ports," on page 192
- "Control CIM-Based Hardware Monitoring Tool Access," on page 193

vCenter Server Security Best Practices

Following vCenter Server security best practices helps you ensure the integrity of your vSphere environment.

Best Practices for vCenter Server Access Control

Strictly control access to different vCenter Server components to increase security for the system.

The following guidelines help ensure security of your environment.

Use named accounts

- If the local Windows administrator account currently has full administrative rights to vCenter Server, remove those access rights and grant those rights to one or more named vCenter Server administrator accounts. Grant full administrative rights only to those administrators who are required to have it. Do not grant this privilege to any group whose membership is not strictly controlled.

  NOTE Starting with vSphere 6.0, the local administrator no longer has full administrative rights to vCenter Server by default. Using local operating system users is not recommended.

- Install vCenter Server using a service account instead of a Windows account. The service account must be an administrator on the local machine.

- Make sure that applications use unique service accounts when connecting to a vCenter Server system.

Minimize access

Avoid allowing users to log directly in to the vCenter Server host machine. Users who are logged in to the vCenter Server can potentially cause harm, either intentionally or unintentionally, by altering settings and modifying processes. They also have potential access to vCenter credentials, such as the SSL certificate. Allow only those users who have legitimate tasks to perform to log in to the system and ensure that login events are audited.

Monitor privileges of vCenter Server administrator users

Not all administrator users must have the Administrator role. Instead, create a custom role with the appropriate set of privileges and assign it to other administrators.

Users with the vCenter Server Administrator role have privileges on all objects in the hierarchy. For example, by default the Administrator role allows users to interact with files and programs inside a virtual machine's guest operating system. Assigning that role to too many users can lessen virtual machine data confidentiality, availability, or integrity. Create a role that gives the administrators the privileges they need, but remove some of the virtual machine management privileges.

Grant minimal privileges to vCenter Server database user

The database user requires only certain privileges specific to database access. In addition, some privileges are required only for installation and upgrade. These privileges can be removed after the product is installed or upgraded.

Verify password policy for vpxuser

By default, vCenter Server changes the vpxuser password automatically every 30 days. Ensure that this setting meets your policies, or configure the policy to meet your company's password aging policies. See "Set the vCenter Server Password Policy," on page 188.

NOTE Make sure that password aging policy is not too short.

Check privileges after vCenter Server restart

Check for privilege reassignment when you restart vCenter Server. If the user or user group that is assigned the Administrator role on the root folder cannot be verified as a valid user or group during a restart, the role is removed from that user or group. In its place, vCenter Server grants the Administrator role to the vCenter Single Sign-On account administrator@vsphere.local. This account can then act as the administrator.

Reestablish a named administrator account and assign the Administrator role to that account to avoid using the anonymous administrator@vsphere.local account.

Set the vCenter Server Password Policy

By default, vCenter Server changes the vpxuser password automatically every 30 days. You can change that value from the vSphere Web Client.

Procedure

1. Select the vCenter Server in the vSphere Web Client object hierarchy.
2. Click the **Manage** tab and the **Settings** subtab.
3. Click **Advanced Settings** and enter **`VimPasswordExpirationInDays`** in the filter box.
4. Set `VirtualCenter.VimPasswordExpirationInDays` to comply with your requirements.

Hardening the vCenter Server Windows Host

Protect the Windows host where vCenter Server is running against vulnerabilities and attacks by ensuring that the host environment is as secure as possible.

- Maintain a supported operating system, database, and hardware for the vCenter Server system. If vCenter Server is not running on a supported operating system, it might not run properly, making vCenter Server vulnerable to attacks.
- Keep the vCenter Server system properly patched. By staying up-to-date with operating system patches, the server is less vulnerable to attack.
- Provide operating system protection on the vCenter Server host. Protection includes antivirus and anti-malware software.
- On each Windows computer in the infrastructure, ensure that Remote Desktop (RDP) Host Configuration settings are set to ensure the highest level of encryption according to industry-standard guidelines or internal guidelines.

For operating system and database compatibility information, see the *vSphere Compatibility Matrixes*.

Removing Expired or Revoked Certificates and Logs from Failed Installations

Leaving expired or revoked certificates or leaving vCenter Server installation logs for failed installation on your vCenter Server system can compromise your environment.

Removing expired or revoked certificates is required for the following reasons.

- If expired or revoked certificates are not removed from the vCenter Server system, the environment can be subject to a MiTM attack
- In certain cases, a log file that contains the database password in plain text is created on the system if vCenter Server installation fails. An attacker who breaks into the vCenter Server system, might gain access to this password and, at the same time, access to the vCenter Server database.

Limiting vCenter Server Network Connectivity

For improved security, avoid putting the vCenter Server system on any network other than a management network, and ensure that vSphere management traffic is on a restricted network. By limiting network connectivity, you limit certain types of attack.

vCenter Server requires access to a management network only. Avoid putting the vCenter Server system on other networks such as your production network or storage network, or on any network with access to the Internet. vCenter Server does not need access to the network where vMotion operates.

vCenter Server requires network connectivity to the following systems.

- All ESXi hosts.
- The vCenter Server database.
- Other vCenter Server systems (if the vCenter Server systems are part of a common vCenter Single Sign-On domain for purposes of replicating tags, permissions, and so on).
- Systems that are authorized to run management clients. For example, the vSphere Web Client, a Windows system where you use the PowerCLI, or any other SDK-based client.
- Systems that run add-on components such as VMware vSphere Update Manager.
- Infrastructure services such as DNS, Active Directory, and NTP.
- Other systems that run components that are essential to functionality of the vCenter Server system.

Use a local firewall on the Windows system where the vCenter Server system is running or use a network firewall. Include IP-based access restrictions so that only necessary components can communicate with the vCenter Server system.

Consider Restricting the Use of Linux Clients

Communications between client components and a vCenter Server system or ESXi hosts are protected by SSL-based encryption by default. Linux versions of these components do not perform certificate validation. Consider restricting the use of these clients.

Even if you have replaced the VMCA-signed certificates on the vCenter Server system and the ESXi hosts with certificates that are signed by a third party CA, certain communications with Linux clients are still vulnerable to man-in-the-middle attacks. The following components are vulnerable when they run on the Linux operating system.

- vCLI commands
- vSphere SDK for Perl scripts
- Programs written using the vSphere Web Services SDK

You can relax the restriction against using Linux clients if you enforce proper controls.

- Restrict management network access to authorized systems only.
- Use firewalls to ensure that only authorized hosts are allowed to access vCenter Server.
- Use jump-box systems to ensure that Linux clients are behind the jump.

Examine Installed Plug-Ins

vSphere Web Client extensions run at the same privilege level as the user who is logged in. A malicious extension can masquerade as a useful plug-in and perform harmful operations such as stealing credentials or changing the system configuration. To increase security, use a vSphere Web Client installation that includes only authorized extensions from trusted sources.

A vCenter installation includes the vSphere Web Client extensibility framework, which provides the ability to extend the vSphere Web Client with menu selections or toolbar icons that provide access to vCenter add-on components or external, Web-based functionality. This flexibility results in a risk of introducing unintended capabilities. For example, if an administrator installs a plug-in in an instance of the vSphere Web Client, the plug-in can then execute arbitrary commands with the privilege level of that administrator.

To protect against potential compromise of your vSphere Web Client you can periodically examine all installed plug-ins and make sure that all plug-ins come from a trusted source.

Prerequisites

You must have privileges to access the vCenter Single Sign-On service. These privileges differ from vCenter Server privileges.

Procedure

1. Log in to the vSphere Web Client as administrator@vsphere.local or a user with vCenter Single Sign-On privileges.
2. From the Home page, select **Administration**, and then select **Client Plug-Ins** under **Solutions**
3. Examine the list of client plug-ins.

vCenter Server Appliance Security Best Practices

Follow all best practices for securing a vCenter Server system to secure your vCenter Server Appliance. Additional steps help you make your environment more secure.

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 certificate validity. 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. See "Synchronize the Time in the vCenter Server Appliance with an NTP Server," on page 227.
Restrict vCenter Server Appliance network access	Restrict access to only those essential components required to communicate with the vCenter Server Appliance. Blocking access from unnecessary systems reduces the potential for general attacks on the operating system. Restricting access to only those essential components minimizes risk.

Verify Thumbprints for Legacy ESXi Hosts

In vSphere 6 and later, hosts are assigned VMCA certificates by default. If you change the certificate mode to thumbprint, you can continue to use thumbprint mode for legacy hosts. You can verify the thumbprints in the vSphere Web Client.

NOTE Certificates are preserved across upgrades by default.

Procedure

1. Browse to the vCenter Server system in the vSphere Web Client object navigator.
2. Select the **Manage** tab, click **Settings**, and click **General**.
3. Click **Edit**.
4. Click **SSL Settings**.
5. If any of your ESXi 5.5 or earlier hosts require manual validation, compare the thumbprints listed for the hosts to the thumbprints in the host console.

   To obtain the host thumbprint, use the Direct Console User Interface (DCUI).

   a. Log in to the direct console and press F2 to access the System Customization menu.

   b. Select **View Support Information**.

      The host thumbprint appears in the column on the right.
6. If the thumbprint matches, select the **Verify** check box next to the host.

   Hosts that are not selected will be disconnected after you click **OK**.
7. Click **OK**.

Verify that SSL Certificate Validation Over Network File Copy Is Enabled

Network File Copy (NFC) provides a file-type-aware FTP service for vSphere components. Starting with vSphere 5.5, ESXi uses NFC for operations such as copying and moving data between datastores by default, but you might have to enable it if it is disabled.

When SSL over NFC is enabled, connections between vSphere components over NFC are secure. This connection can help prevent man-in-the-middle attacks within a data center.

Because using NFC over SSL causes some performance degradation, you might consider disabling this advanced setting in some development environments.

Procedure

1 Connect to the vCenter Server with the vSphere Web Client.

2 Select the **Settings** tab, and click **Advanced Settings**.

3 Click **Edit**.

4 At the bottom of the dialog, enter the following Key and Value.

Field	Value
Key	nfc.useSSL
Value	true

5 Click **OK**.

vCenter Server TCP and UDP Ports

vCenter Server is accessed through predetermined TCP and UDP ports. If you manage network components from outside a firewall, you might be required to reconfigure the firewall to allow access on the appropriate ports.

The table lists TCP and UDP ports, and the purpose and the type of each. Ports that are open by default at installation time are indicated by (Default). For an up-to-date list of ports of all vSphere components for the different versions of vSphere, see VMware Knowledge Base Article 1012382.

Table 6-1. vCenter Server TCP and UDP Ports

Port	Purpose
80 (Default)	HTTP access vCenter Server requires port 80 for direct HTTP connections. Port 80 redirects requests to HTTPS port 443. This redirection is useful if you accidentally use http://server instead of https://server WS-Management (also requires port 443 to be open)
88, 2013	Control interface RPC for Kerberos, used by vCenter Single Sign-On.
123	NTP Client
161 (Default)	SNMP Server
389	vCenter Single Sign-On LDAP (6.0 and later)
636	vCenter Single Sign-On LDAPS (6.0 and later)

Table 6-1. vCenter Server TCP and UDP Ports (Continued)

Port	Purpose
443 (Default)	vCenter Server systems use port 443 to monitor data transfer from SDK clients. This port is also used for the following services: ■ WS-Management (also requires port 80 to be open) ■ Third-party network management client connections to vCenter Server ■ Third-party network management clients access to hosts
902 (Default)	The default port that the vCenter Server system uses to send data to managed hosts. Managed hosts also send a regular heartbeat over UDP port 902 to the vCenter Server system. This port must not be blocked by firewalls between the server and the hosts or between hosts.
903	MKS transactions (xinetd/vmware-authd-mks).
1234, 1235 (Default)	vSphere Replication.
2012	RPC port for VMware Directory Service (vmdir).
2014	RPC port for VMware Certificate Authority (VMCA) service.
2020	RPC port for VMware Authentication Framework Service (vmafd).
5900-5964	RFB protocol, which is used by management tools such as VNC.
7444	vCenter Single Sign-On HTTPS.
8000 (Default)	Requests from vMotion.
8109	VMware Syslog Collector.
9090	vSphere Web Client HTTPS access to virtual machine consoles. Allows a vCenter Server Appliance to communicate with vSphere Web Client Remote Console traffic.
9443	vSphere Web Client HTTP access to ESXi hosts.
10080	Inventory service.
11711	vCenter Single Sign-On LDAP (environments that are upgraded from vSphere 5.5)
11712	vCenter Single Sign-On LDAPS (environments that are upgraded from vSphere 5.5)
12721	VMware Identity Management service.
15005	ESX Agent Manager (EAM). An ESX Agent can be a virtual machine or an optional VIB. The agent extends the functions of an ESXi host to provide additional services that a vSphere solution such as NSX-v or vRealize Automation requires.
15007	vService Manager (VSM). This service registers vCenter Server extensions. Open this port only if required by extensions that you intend to use.

In addition to these ports, you can configure other ports depending on your needs.

Control CIM-Based Hardware Monitoring Tool Access

The Common Information Model (CIM) system provides an interface that enables hardware-level management from remote applications using a set of standard APIs. To ensure that the CIM interface is secure, provide only the minimum access necessary to these applications. If an application has been provisioned with a root or full administrator account and the application is compromised, the full virtual environment might be compromised.

CIM is an open standard that defines a framework for agent-less, standards-based monitoring of hardware resources for ESXi. This framework consists of a CIM object manager, often called a CIM broker, and a set of CIM providers.

CIM providers are used as the mechanism to provide management access to device drivers and underlying hardware. Hardware vendors, including server manufacturers and specific hardware device vendors, can write providers to provide monitoring and management of their particular devices. VMware also writes providers that implement monitoring of server hardware, ESXi storage infrastructure, and virtualization-specific resources. These providers run inside the ESXi system and therefore are designed to be extremely lightweight and focused on specific management tasks. The CIM broker takes information from all CIM providers, and presents it to the outside world via standard APIs, the most common one being WS-MAN.

Do not provide root credentials to remote applications to access the CIM interface. Instead, create a service account specific to these applications and grant read-only access to CIM information to any local account defined on the ESXi system, as well as any role defined in vCenter Server.

Procedure

1 Create a service account specific to CIM applications.

2 Grant read-only access to CIM information to any local account defined on the ESXi system, as well as any role defined in vCenter Server.

3 (Optional) If the application requires write access to the CIM interface, create a role to apply to the service account with only two privileges:

- **Host.Config.SystemManagement**
- **Host.CIM.CIMInteraction**

  This role can be local to the host or centrally defined on vCenter Server, depending on how the monitoring application works.

When a user logs into the host with the service account you created for CIM applications, the user has only the privileges **SystemManagement** and **CIMInteraction**, or read-only access.

7 Securing Virtual Machines

The guest operating system that runs in the virtual machine is subject to the same security risks as a physical system. Secure virtual machines as you would secure physical machines.

This chapter includes the following topics:

- "Limit Informational Messages from Virtual Machines to VMX Files," on page 195
- "Prevent Virtual Disk Shrinking," on page 196
- "Virtual Machine Security Best Practices," on page 196

Limit Informational Messages from Virtual Machines to VMX Files

Limit informational messages from the virtual machine to the VMX file to avoid filling the datastore and causing a Denial of Service (DoS). A Denial of Service can occur when you do not control the size of a virtual machine's VMX file and the amount of information exceeds the datastore's capacity.

The configuration file containing the informational name-value pairs is limited to 1MB by default. This capacity is sufficient in most cases, but you can change this value if necessary. For example, you might increase the limit if large amounts of custom information are being stored in the configuration file.

NOTE Consider carefully how much information you require. If the amount of information exceeds the datastore's capacity, a Denial of Service might result.

The default limit of 1MB is applied even when the `tools.setInfo.sizeLimit` parameter is not listed in the advanced options.

Procedure

1. Find the virtual machine in the vSphere Web Client inventory.
   a. Select a data center, folder, cluster, resource pool, or host.
   b. Click the **Related Objects** tab and click **Virtual Machines**.
2. Right-click the virtual machine and click **Edit Settings**.
3. Select **VM Options**.
4. Click **Advanced** and click **Edit Configuration**.
5. Add or edit the `tools.setInfo.sizeLimit` parameter.

Prevent Virtual Disk Shrinking

Nonadministrative users in the guest operating system are able to shrink virtual disks. Shrinking a virtual disk reclaims the disk's unused space. However, if you shrink a virtual disk repeatedly, the disk can become unavailable and cause a denial of service. To prevent this, disable the ability to shrink virtual disks.

Prerequisites

- Turn off the virtual machine.
- Verify that you have root or administrator privileges on the virtual machine.

Procedure

1 Find the virtual machine in the vSphere Web Client inventory.

   a Select a data center, folder, cluster, resource pool, or host.

   b Click the **Related Objects** tab and click **Virtual Machines**.

2 Right-click the virtual machine and click **Edit Settings**.

3 Select **VM Options**.

4 Click **Advanced** and click **Edit Configuration**.

5 Add or edit the following parameters.

Name	Value
isolation.tools.diskWiper.disable	TRUE
isolation.tools.diskShrink.disable	TRUE

6 Click **OK**.

When you disable this feature, you cannot shrink virtual machine disks when a datastore runs out of space.

Virtual Machine Security Best Practices

Following virtual machine security best practices helps ensure the integrity of your vSphere deployment.

- General Virtual Machine Protection on page 197

  A virtual machine is, in most respects, the equivalent of a physical server. Employ the same security measures in virtual machines that you do for physical systems.

- Use Templates to Deploy Virtual Machines on page 197

  When you manually install guest operating systems and applications on a virtual machine, you introduce a risk of misconfiguration. By using a template to capture a hardened base operating system image with no applications installed, you can ensure that all virtual machines are created with a known baseline level of security.

- Minimize Use of Virtual Machine Console on page 198

  The virtual machine console provides the same function for a virtual machine that a monitor on a physical server provides. Users with access to the virtual machine console have access to virtual machine power management and removable device connectivity controls, which might allow a malicious attack on a virtual machine.

- Prevent Virtual Machines from Taking Over Resources on page 198

  When one virtual machine consumes so much of the host resources that other virtual machines on the host cannot perform their intended functions, a Denial of Service (DoS) might occur. To prevent a virtual machine from causing a DoS, use host resource management features such as setting Shares and using resource pools.

- Disable Unnecessary Functions Inside Virtual Machines on page 199

  Any service running in a virtual machine provides the potential for attack. By disabling unnecessary system components that are not necessary to support the application or service running on the system, you reduce the number of components that can be attacked.

General Virtual Machine Protection

A virtual machine is, in most respects, the equivalent of a physical server. Employ the same security measures in virtual machines that you do for physical systems.

Follow these best practices to protect your virtual machine:

Patches and other protection

Keep all security measures up-to-date, including applying appropriate patches. It is especially important to keep track of updates for dormant virtual machines that are powered off, because it can be easy to overlook them. For example, ensure that anti-virus software, anti-spy ware, intrusion detection, and other protection are enabled for every virtual machine in your virtual infrastructure. You should also ensure that you have enough space for the virtual machine logs.

Anti-virus scans

Because each virtual machine hosts a standard operating system, you must protect it from viruses by installing anti-virus software. Depending on how you are using the virtual machine, you might also want to install a software firewall.

Stagger the schedule for virus scans, particularly in deployments with a large number of virtual machines. Performance of systems in your environment degrades significantly if you scan all virtual machines simultaneously. Because software firewalls and antivirus software can be virtualization-intensive, you can balance the need for these two security measures against virtual machine performance, especially if you are confident that your virtual machines are in a fully trusted environment.

Serial ports

Serial ports are interfaces for connecting peripherals to the virtual machine. They are often used on physical systems to provide a direct, low-level connection to the console of a server, and a virtual serial port allows for the same access to a virtual machine. Serial ports allow for low-level access, which often does not have strong controls like logging or privileges.

Use Templates to Deploy Virtual Machines

When you manually install guest operating systems and applications on a virtual machine, you introduce a risk of misconfiguration. By using a template to capture a hardened base operating system image with no applications installed, you can ensure that all virtual machines are created with a known baseline level of security.

You can use templates that can contain a hardened, patched, and properly configured operating system to create other, application-specific templates, or you can use the application template to deploy virtual machines.

Procedure

- Provide templates for virtual machine creation that contain hardened, patched, and properly configured operating system deployments.

  If possible, deploy applications in templates as well. Ensure that the applications do not depend on information specific to the virtual machine to be deployed.

What to do next

For more information about templates, see the *vSphere Virtual Machine Administration* documentation.

Minimize Use of Virtual Machine Console

The virtual machine console provides the same function for a virtual machine that a monitor on a physical server provides. Users with access to the virtual machine console have access to virtual machine power management and removable device connectivity controls, which might allow a malicious attack on a virtual machine.

Procedure

1. Use native remote management services, such as terminal services and SSH, to interact with virtual machines.

   Grant access to the virtual machine console only when necessary.

2. Limit the connections to the console to as few connections as necessary.

   For example, in a highly secure environment, limit the connection to one. In some environments, you can increase that limit depending on how many concurrent connections are necessary to accomplish normal tasks.

Prevent Virtual Machines from Taking Over Resources

When one virtual machine consumes so much of the host resources that other virtual machines on the host cannot perform their intended functions, a Denial of Service (DoS) might occur. To prevent a virtual machine from causing a DoS, use host resource management features such as setting Shares and using resource pools.

By default, all virtual machines on an ESXi host share resources equally. You can use Shares and resource pools to prevent a denial of service attack that causes one virtual machine to consume so much of the host's resources that other virtual machines on the same host cannot perform their intended functions.

Do not use Limits unless you fully understand the impact.

Procedure

1. Provision each virtual machine with just enough resources (CPU and memory) to function properly.
2. Use Shares to guarantee resources to critical virtual machines.
3. Group virtual machines with similar requirements into resource pools.
4. In each resource pool, leave Shares set to the default to ensure that each virtual machine in the pool receives approximately the same resource priority.

   With this setting, a single virtual machine cannot use more than other virtual machines in the resource pool.

What to do next

See the *vSphere Resource Management* documentation for information about shares and limits.

Disable Unnecessary Functions Inside Virtual Machines

Any service running in a virtual machine provides the potential for attack. By disabling unnecessary system components that are not necessary to support the application or service running on the system, you reduce the number of components that can be attacked.

Virtual machines do not usually require as many services or functions as physical servers. When you virtualize a system, evaluate whether a particular service or function is necessary.

Procedure

- Disable unused services in the operating system.

  For example, if the system runs a file server, turn off any Web services.
- Disconnect unused physical devices, such as CD/DVD drives, floppy drives, and USB adaptors.
- Disable unused functionality, such as unused display features or HGFS (Host Guest File System).
- Turn off screen savers.
- Do not run the X Window system on Linux, BSD, or Solaris guest operating systems unless it is necessary.

Remove Unnecessary Hardware Devices

Any enabled or connected device represents a potential attack channel. Users and processes without privileges on a virtual machine can connect or disconnect hardware devices, such as network adapters and CD-ROM drives. Attackers can use this capability to breach virtual machine security. Removing unnecessary hardware devices can help prevent attacks.

An attacker with access to a virtual machine can connect a disconnected hardware device and access sensitive information on the media left in the drive, or disconnect a network adapter to isolate the virtual machine from its network, resulting in a denial of service.

- Ensure that unauthorized devices are not connected and remove any unneeded or unused hardware devices.
- Disable unnecessary virtual devices from within a virtual machine.
- Ensure that no device is connected to a virtual machine if it is not required. Serial and parallel ports are rarely used for virtual machines in a data center, and CD/DVD drives are usually connected only temporarily during software installation.

Procedure

1. Log into a vCenter Server system using the vSphere Web Client.
2. Right-click the virtual machine and click **Edit Settings**.
3. Check each hardware device and ensure that you want it connected.

   Include checks for the following devices:

   - Floppy drives
   - Serial ports
   - Parallel ports
   - USB controllers
   - CD-ROM drives

Disable Unused Display Features

Attackers can use an unused display feature as a vector for inserting malicious code into your environment. Disable features that are not in use in your environment.

Procedure

1 Find the virtual machine in the vSphere Web Client inventory.

   a Select a data center, folder, cluster, resource pool, or host.

   b Click the **Related Objects** tab and click **Virtual Machines**.

2 Right-click the virtual machine and click **Edit Settings**.

3 Select **VM Options**.

4 Click **Advanced** and click **Edit Configuration**.

5 If appropriate, set the following parameters by adding or editing them if appropriate.

Option	Description
svga.vgaonly	If you set this parameter to TRUE, advanced graphics functions no longer work. Only character-cell console mode will be available. If you use this setting, `mks.enable3d` has no effect. NOTE Apply this settings only to virtual machines that do not need a virtualized video card.
mks.enable3d	Set this parameter to FALSE on virtual machines that do not require 3D functionality.

Disable Unexposed Features

VMware virtual machines are designed to work on both vSphere systems and hosted virtualization platforms such as Workstation and Fusion. Certain virtual machine parameters do not need to be enabled when you run a virtual machine on a vSphere system. Disable these parameters to reduce the potential for vulnerabilities.

Prerequisites

Turn off the virtual machine.

Procedure

1 Find the virtual machine in the vSphere Web Client inventory.

   a Select a data center, folder, cluster, resource pool, or host.

   b Click the **Related Objects** tab and click **Virtual Machines**.

2 Right-click the virtual machine and click **Edit Settings**.

3 Select **VM Options**.

4 Click **Advanced** and click **Edit Configuration**.

5 Set the following parameters to TRUE by adding or editing them.

   - `isolation.tools.unity.push.update.disable`
   - `isolation.tools.ghi.launchmenu.change`
   - `isolation.tools.memSchedFakeSampleStats.disable`
   - `isolation.tools.getCreds.disable`

- `isolation.tools.ghi.autologon.disable`
- `isolation.bios.bbs.disable`
- `isolation.tools.hgfsServerSet.disable`

6 Click **OK**.

Disable HGFS File Transfers

Certain operations such as automated tools upgrades use a component in the hypervisor called host guest file system (HGFS). You can disable this component to minimize the risk that an attacker can use HGFS to transfer files inside the guest operating system.

Procedure

1 Find the virtual machine in the vSphere Web Client inventory.

   a Select a data center, folder, cluster, resource pool, or host.

   b Click the **Related Objects** tab and click **Virtual Machines**.

2 Right-click the virtual machine and click **Edit Settings**.

3 Select **VM Options**.

4 Click **Advanced** and click **Edit Configuration**.

5 Verify that the `isolation.tools.hgfsServerSet.disable` parameter is set to TRUE.

When you make this change, the VMX process no longer responds to commands from the tools process. APIs that use HGFS to transfer files to and from the guest operating system, such as some VIX commands or the VMware Tools auto-upgrade utility, no longer work.

Disable Copy and Paste Operations Between Guest Operating System and Remote Console

Copy and paste operations between the guest operating system and remote console are disabled by default. For a secure environment, retain the default setting. If you require copy and paste operations, you must enable them using the vSphere Client.

Prerequisites

Turn off the virtual machine.

Procedure

1 Log into a vCenter Server system using the vSphere Web Client.

2 Right-click the virtual machine and click **Edit Settings**.

3 Click **VM Options**, and click **Edit Configuration**.

4 Ensure that the following values are in the Name and Value columns, or click **Add Row** to add them.

Name	Value
isolation.tools.copy.disable	true
isolation.tools.paste.disable	true

   These options override any settings made in the guest operating system's VMware Tools control panel.

5 Click **OK**.

6 (Optional) If you made changes to the configuration parameters, restart the virtual machine.

Limiting Exposure of Sensitive Data Copied to the Clipboard

Copy and paste operations are disabled by default for hosts to prevent exposing sensitive data that has been copied to the clipboard.

When copy and paste is enabled on a virtual machine running VMware Tools, you can copy and paste between the guest operating system and remote console. As soon as the console window gains focus, non-privileged users and processes running in the virtual machine can access the clipboard for the virtual machine console. If a user copies sensitive information to the clipboard before using the console, the user—perhaps unknowingly—exposes sensitive data to the virtual machine. To prevent this problem, copy and paste operations for the guest operating system are disabled by default.

It is possible to enable copy and paste operations for virtual machines if necessary.

Restrict Users from Running Commands Within a Virtual Machine

By default, a user with vCenter Server Administrator role can interact with files and programs within a virtual machine's guest operating system. To reduce the risk of breaching guest confidentiality, availability, or integrity, create a nonguest access role without the **Guest Operations** privilege.

For security, be as restrictive about allowing access to the virtual data center as you are to the physical data center. To avoid giving users full administrator access, create a custom role that disables guest access and apply that role to users who require administrator privileges, but who are not authorized to interact with files and programs within a guest operating system.

For example, a configuration might include a virtual machine on the infrastructure that has sensitive information on it. Tasks such as migration with vMotion and Storage vMotion require that the IT role has access to the virtual machine. In this case, disable some remote operations within a guest OS to ensure that the IT role cannot access the sensitive information.

Prerequisites

Verify that you have **Administrator** privileges on the vCenter Server system where you create the role.

Procedure

1 Log in to the vSphere Web Client as a user who has **Administrator** privileges on the vCenter Server system where you will create the role.

2 Click **Administration** and select **Roles**.

3 Click the **Create role action** icon and type a name for the role.

For example, type `Administrator No Guest Access`.

4 Select **All Privileges**.

5 Deselect **All Privileges.Virtual machine.Guest Operations** to remove the Guest Operations set of privileges.

6 Click **OK**.

What to do next

Select the vCenter Server system or the host and assign a permission that pairs the user or group that should have the new privileges to the newly created role. Remove those users from the default Administrator role.

Prevent a Virtual Machine User or Process from Disconnecting Devices

Users and processes without root or administrator privileges within virtual machines have the capability to connect or disconnect devices, such as network adaptors and CD-ROM drives, and the ability to modify device settings. To increase virtual machine security, remove these devices. If you do not want to permanently remove a device, you can prevent a virtual machine user or process from connecting or disconnecting the device from within the guest operating system.

Prerequisites

Turn off the virtual machine.

Procedure

1 Find the virtual machine in the vSphere Web Client inventory.

   a Select a data center, folder, cluster, resource pool, or host.

   b Click the **Related Objects** tab and click **Virtual Machines**.

2 Right-click the virtual machine and click **Edit Settings**.

3 Select **VM Options**.

4 Click **Advanced** and click **Edit Configuration**.

5 Verify that the following values are in the Name and Value columns, or click **Add Row** to add them.

Name	Value
isolation.device.connectable.disable	true
isolation.device.edit.disable	true

   These options override any settings made in the guest operating system's VMware Tools control panel.

6 Click **OK** to close the Configuration Parameters dialog box, and click **OK** again.

Modify Guest Operating System Variable Memory Limit

You can increase the guest operating system variable memory limit if large amounts of custom information are being stored in the configuration file.

Prerequisites

Turn off the virtual machine.

Procedure

1 Find the virtual machine in the vSphere Web Client inventory.

   a Select a data center, folder, cluster, resource pool, or host.

   b Click the **Related Objects** tab and click **Virtual Machines**.

2 Right-click the virtual machine and click **Edit Settings**.

3 Select **VM Options > Advanced** and click **Edit Configuration** .

4 Add or edit the parameter `tools.setInfo.sizeLimit` and set the value to the number of bytes.

5 Click **OK**.

Prevent Guest Operating System Processes from Sending Configuration Messages to the Host

You can prevent guests from writing any name-value pairs to the configuration file. This is appropriate when guest operating systems must be prevented from modifying configuration settings.

Prerequisites

Turn off the virtual machine.

Procedure

1 Find the virtual machine in the vSphere Web Client inventory.

   a Select a data center, folder, cluster, resource pool, or host.

   b Click the **Related Objects** tab and click **Virtual Machines**.

2 Right-click the virtual machine and click **Edit Settings**.

3 Select **VM Options**.

4 Click **Advanced** and click **Edit Configuration**.

5 Click **Add Row** and type the following values in the Name and Value columns.

   - In the Name column: `isolation.tools.setinfo.disable`
   - In the Value column: `true`

6 Click **OK** to close the Configuration Parameters dialog box, and click **OK** again.

Avoid Using Independent Nonpersistent Disks

When you use independent nonpersistent disks, successful attackers can remove any evidence that the machine was compromised by shutting down or rebooting the system. Without a persistent record of activity on a virtual machine, administrators might be unaware of an attack. Therefore, you should avoid using independent nonpersistent disks.

Procedure

◆ Ensure that virtual machine activity is logged remotely on a separate server, such as a syslog server or equivalent Windows-based event collector.

   If remote logging of events and activity is not configured for the guest, scsiX:Y.mode should be one of the following settings:

   - Not present
   - Not set to independent nonpersistent

When nonpersistent mode is not enabled, you cannot roll a virtual machine back to a known state when you reboot the system.

8 Securing vSphere Networking

Securing vSphere Networking is an essential part of protecting your environment. You secure different vSphere components in different ways. See the *vSphere Networking* documentation for detailed information about networking in the vSphere environment.

This chapter includes the following topics:

- "Introduction to vSphere Network Security," on page 205
- "Securing the Network with Firewalls," on page 206
- "Secure the Physical Switch," on page 210
- "Securing Standard Switch Ports With Security Policies," on page 210
- "Securing vSphere Standard Switches," on page 211
- "Secure vSphere Distributed Switches and Distributed Port Groups," on page 212
- "Securing Virtual Machines with VLANs," on page 213
- "Creating a Network DMZ on a Single ESXi Host," on page 215
- "Creating Multiple Networks Within a Single ESXi Host," on page 216
- "Internet Protocol Security," on page 218
- "Ensure Proper SNMP Configuration," on page 221
- "Use Virtual Switches with the vSphere Network Appliance API Only If Required," on page 222
- "vSphere Networking Security Best Practices," on page 222

Introduction to vSphere Network Security

Network security in the vSphere environment shares many characteristics of securing a physical network environment, but also includes some characteristics that apply only to virtual machines.

Firewalls

Add firewall protection to your virtual network by installing and configuring host-based firewalls on some or all of its virtual machines.

For efficiency, you can set up private virtual machine Ethernet networks or virtual networks. With virtual networks, you install a host-based firewall on a virtual machine at the head of the virtual network. This firewall serves as a protective buffer between the physical network adapter and the remaining virtual machines in the virtual network.

Because host-based firewalls can slow performance, balance your security needs against performance goals before you install host-based firewalls on virtual machines elsewhere in the virtual network.

See "Securing the Network with Firewalls," on page 206.

Segmentation

Keep different virtual machine zones within a host on different network segments. If you isolate each virtual machine zone on its own network segment, you minimize the risk of data leakage from one virtual machine zone to the next. Segmentation prevents various threats, including Address Resolution Protocol (ARP) spoofing, in which an attacker manipulates the ARP table to remap MAC and IP addresses, thereby gaining access to network traffic to and from a host. Attackers use ARP spoofing to generate man in the middle (MITM) attacks, perform denial of service (DoS) attacks, hijack the target system, and otherwise disrupt the virtual network.

Planning segmentation carefully lowers the chances of packet transmissions between virtual machine zones, which prevents sniffing attacks that require sending network traffic to the victim. Also, an attacker cannot use an insecure service in one virtual machine zone to access other virtual machine zones in the host. You can implement segmentation by using either of two approaches. Each approach has different benefits.

- Use separate physical network adapters for virtual machine zones to ensure that the zones are isolated. Maintaining separate physical network adapters for virtual machine zones is probably the most secure method and is less prone to misconfiguration after the initial segment creation.
- Set up virtual local area networks (VLANs) to help safeguard your network. Because VLANs provide almost all of the security benefits inherent in implementing physically separate networks without the hardware overhead, they offer a viable solution that can save you the cost of deploying and maintaining additional devices, cabling, and so forth. See "Securing Virtual Machines with VLANs," on page 213.

Preventing Unauthorized Access

If your virtual machine network is connected to a physical network, it can be subject to breaches just like a network that consists of physical machines. Even if the virtual machine network is isolated from any physical network, virtual machines in the network can be subject to attacks from other virtual machines in the network. The requirements for securing virtual machines are often the same as those for securing physical machines.

Virtual machines are isolated from each other. One virtual machine cannot read or write another virtual machine's memory, access its data, use its applications, and so forth. However, within the network, any virtual machine or group of virtual machines can still be the target of unauthorized access from other virtual machines and might require further protection by external means.

Securing the Network with Firewalls

Security administrators use firewalls to safeguard the network or selected components in the network from intrusion.

Firewalls control access to devices within their perimeter by closing all communication pathways, except for those that the administrator explicitly or implicitly designates as authorized. The pathways, or ports, that administrators open in the firewall allow traffic between devices on different sides of the firewall.

IMPORTANT The ESXi firewall in ESXi 5.5 does not allow per-network filtering of vMotion traffic. Therefore, you must install rules on your external firewall to ensure that no incoming connections can be made to the vMotion socket.

In a virtual machine environment, you can plan the layout for firewalls between components.

- Firewalls between physical machines such as vCenter Server systems and ESXi hosts.

- Firewalls between one virtual machine and another—for example, between a virtual machine acting as an external Web server and a virtual machine connected to your company's internal network.
- Firewalls between a physical machine and a virtual machine, such as when you place a firewall between a physical network adapter card and a virtual machine.

How you use firewalls in your ESXi configuration is based on how you plan to use the network and how secure any given component needs to be. For example, if you create a virtual network where each virtual machine is dedicated to running a different benchmark test suite for the same department, the risk of unwanted access from one virtual machine to the next is minimal. Therefore, a configuration where firewalls are present between the virtual machines is not necessary. However, to prevent interruption of a test run from an outside host, you might set up the configuration so that a firewall is present at the entry point of the virtual network to protect the entire set of virtual machines.

Firewalls for Configurations with vCenter Server

If you access ESXi hosts through vCenter Server, you typically protect vCenter Server using a firewall. This firewall provides basic protection for your network.

A firewall might lie between the clients and vCenter Server. Alternatively, depending on your deployment, vCenter Server and the clients can both be behind the firewall. The main point is to ensure that a firewall is present at what you consider to be an entry point for the system.

For a comprehensive list of TCP and UDP ports, including those for vSphere vMotion™ and vSphere Fault Tolerance, see "vCenter Server TCP and UDP Ports," on page 192.

Networks configured with vCenter Server can receive communications through the vSphere Web Client or third-party network management clients that use the SDK to interface with the host. During normal operation, vCenter Server listens for data from its managed hosts and clients on designated ports. vCenter Server also assumes that its managed hosts listen for data from vCenter Server on designated ports. If a firewall is present between any of these elements, you must ensure that the firewall has open ports to support data transfer.

You might also include firewalls at a variety of other access points in the network, depending on how you plan to use the network and the level of security various devices require. Select the locations for your firewalls based on the security risks that you have identified for your network configuration. The following is a list of firewall locations common to ESXi implementations.

- Between the vSphere Web Client or a third-party network-management client and vCenter Server.
- If your users access virtual machines through a Web browser, between the Web browser and the ESXi host.
- If your users access virtual machines through the vSphere Web Client, between the vSphere Web Client and the ESXi host. This connection is in addition to the connection between the vSphere Web Client and vCenter Server, and it requires a different port.
- Between vCenter Server and the ESXi hosts.
- Between the ESXi hosts in your network. Although traffic between hosts is usually considered trusted, you can add firewalls between them if you are concerned about security breaches from machine to machine.

  If you add firewalls between ESXi hosts and plan to migrate virtual machines between the servers, perform cloning, or use vMotion, you must also open ports in any firewall that divides the source host from the target hosts so that the source and targets can communicate.
- Between the ESXi hosts and network storage such as NFS or iSCSI storage. These ports are not specific to VMware, and you configure them according to the specifications for your network.

Connecting to vCenter Server Through a Firewall

vCenter Server uses TCP port 443 to listen for data transfer from its clients. If you have a firewall between vCenter Server and its clients, you must configure a connection through which vCenter Server can receive data from the clients.

Open TCP port 443 in the firewall to enable vCenter Server to receive data from the vSphere Web Client. Firewall configuration depends on what is used at your site, ask your local firewall system administrator for information.

If you do not want to use port 443 as the port for vSphere Web Client-to-vCenter Server communication, you can switch to another port by changing the vCenter Server settings from the vSphere Web Client. See the *vCenter Server and Host Management* documentation.

If you are still using the vSphere Client, see the *vSphere Administration with vSphere Client documentation*.

Firewalls for Configurations Without vCenter Server

You can connect clients directly to your ESXi network instead of using vCenter Server.

Networks configured without vCenter Server receive communications through the vSphere Client, one of the vSphere command-line interfaces, the vSphere Web Services SDK, or third-party clients. For the most part, the firewall needs are the same as when a vCenter Server is present, but several key differences exist.

- As you would for configurations that include vCenter Server, be sure a firewall is present to protect your ESXi layer or, depending on your configuration, your clients and ESXi layer. This firewall provides basic protection for your network.
- Licensing in this type of configuration is part of the ESXi package that you install on each of the hosts. Because licensing is resident to the server, a separate license server is not required. This eliminates the need for a firewall between the license server and the ESXi network.

You can configure firewall ports using ESXCLI, using the vSphere Client, or using firewall rules. See "ESXi Firewall Configuration," on page 150.

Connecting ESXi Hosts Through Firewalls

If you have a firewall between two ESXi hosts and you want to allow transactions between the hosts or use vCenter Server to perform any source or target activities, such as vSphere High Availability (vSphere HA) traffic, migration, cloning, or vMotion, you must configure a connection through which the managed hosts can receive data.

To configure a connection for receiving data, open ports for traffic from services such as vSphere High Availability, vMotion, and vSphere Fault Tolerance. See "ESXi Firewall Configuration," on page 150 for a discussion of configuration files, vSphere Web Client access, and firewall commands. See "Incoming and Outgoing Firewall Ports for ESXi Hosts," on page 152 for a list of ports. Refer to the firewall system administrator for additional information on configuring the ports.

Connecting to the Virtual Machine Console Through a Firewall

When you connect your client to ESXi hosts through vCenter Server, certain ports must be open for user and administrator communication with virtual machine consoles. These ports support different client functions, interface with different layers on ESXi, and use different authentication protocols.

How you connect to the virtual machine console depends on whether you are using the vSphere Web Client or whether you are using a different client such as the vSphere Web Services SDK.

Connecting by Using the vSphere Web Client

When you are connecting with the vSphere Web Client, you always connect to the vCenter Server that manages the host, and access the virtual machine console from there.

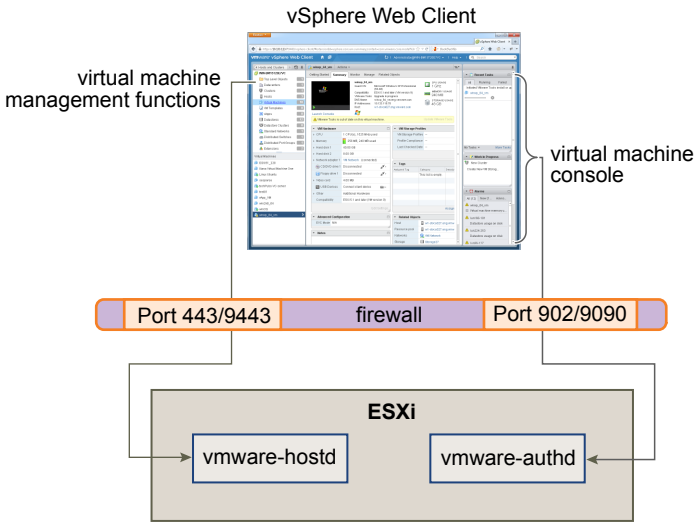
The following ports are involved.

Port 9443 and Port 9090 The vSphere Web Client uses port 9443 for HTTPS communication with vCenter Server and port 9090 for HTTP communication with vCenter Server. Once users can access vCenter Server, they can also access individual ESXi hosts and virtual machines.

These ports can be changed during vSphere Web Client installation.

Port 443 and Port 902 Open ports 443 and 902 in the firewall to allow data transfer to ESXi hosts from vCenter Server if you have a firewall between your vCenter Server system and the ESXi host managed by vCenter Server.

Figure 8-1. Port Use for vSphere Web Client Communications with an ESXi Host Managed by vCenter Server



For additional information on configuring the ports, see the firewall system administrator.

Connecting to ESXi Hosts Directly with the vSphere Client

You can connect directly to an ESXi host. with the vSphere Client.

NOTE Do not connect directly to hosts that are managed by a vCenter Server system. If you make changes to such hosts from the vSphere Client, instability in your environment results.

Port 902 The vSphere Client uses this port to provide a connection for guest operating system MKS activities on virtual machines. It is through this port that users interact with the guest operating systems and applications of the virtual machine. VMware does not support configuring a different port for this function.

Secure the Physical Switch

Secure the physical switch on each ESXi host to prevent attackers from gaining access to the host and its virtual machines.

For best protection of your hosts, ensure that physical switch ports are configured with spanning tree disabled and ensure that the non-negotiate option is configured for trunk links between external physical switches and virtual switches in Virtual Switch Tagging (VST) mode.

Procedure

1 Log in to the physical switch and ensure that spanning tree protocol is disabled or that Port Fast is configured for all physical switch ports that are connected to ESXi hosts.

2 For virtual machines that perform bridging or routing, check periodically that the first upstream physical switch port is configured with BPDU Guard and Port Fast disabled and with spanning tree protocol enabled.

   In vSphere 5.1 and later, to prevent the physical switch from potential Denial of Service (DoS) attacks, you can turn on the guest BPDU filter on the ESXi hosts.

3 Log in to the physical switch and ensure that Dynamic Trunking Protocol (DTP) is not enabled on the physical switch ports that are connected to the ESXi hosts.

4 Routinely check physical switch ports to ensure that they are properly configured as trunk ports if connected to virtual switch VLAN trunking ports.

Securing Standard Switch Ports With Security Policies

As with physical network adapters, a virtual machine network adapter can send frames that appear to be from a different machine or impersonate another machine so that it can receive network frames that are intended for that machine. Also, like physical network adapters, a virtual machine network adapter can be configured so that it receives frames targeted for other machines. Both scenarios present a security risk.

When you create a standard switch for your network, you add port groups in the vSphere Web Client to impose a policy for the virtual machines and VMkernel adapters for system traffic attached to the switch.

As part of adding a VMkernel port group or virtual machine port group to a standard switch, ESXi configures a security policy for the ports in the group. You can use this security policy to ensure that the host prevents the guest operating systems of its virtual machines from impersonating other machines on the network. This security feature is implemented so that the guest operating system responsible for the impersonation does not detect that the impersonation was prevented.

The security policy determines how strongly you enforce protection against impersonation and interception attacks on virtual machines. To correctly use the settings in the security profile, you must understand how virtual machine network adapters control transmissions and how attacks are staged at this level. See the Security Policy section in the *vSphere Networking* publication.

.

Securing vSphere Standard Switches

You can secure standard switch traffic against Layer 2 attacks by restricting some of the MAC address modes by using the security settings of the switches.

Each virtual machine network adapter has an initial MAC address and an effective MAC address.

Initial MAC address The initial MAC address is assigned when the adapter is created. Although the initial MAC address can be reconfigured from outside the guest operating system, it cannot be changed by the guest operating system.

Effective MAC address Each adapter has an effective MAC address that filters out incoming network traffic with a destination MAC address that is different from the effective MAC address. The guest operating system is responsible for setting the effective MAC address and typically matches the effective MAC address to the initial MAC address.

Upon creating a virtual machine network adapter, the effective MAC address and initial MAC address are the same. The guest operating system can alter the effective MAC address to another value at any time. If an operating system changes the effective MAC address, its network adapter receives network traffic that is destined for the new MAC address.

When sending packets through a network adapter, the guest operating system typically places its own adapter effective MAC address in the source MAC address field of the Ethernet frames. It places the MAC address for the receiving network adapter in the destination MAC address field. The receiving adapter accepts packets only if the destination MAC address in the packet matches its own effective MAC address.

An operating system can send frames with an impersonated source MAC address. This means an operating system can stage malicious attacks on the devices in a network by impersonating a network adapter that the receiving network authorizes.

Protect virtual traffic against impersonation and interception Layer 2 attacks by configuring a security policy on port groups or ports.

The security policy on distributed port groups and ports includes the following options:

- Promiscuous mode (see "Promiscuous Mode Operation," on page 212)
- MAC address changes (see "MAC Address Changes," on page 211)
- Forged transmits (see "Forged Transmits," on page 212)

You can view and change the default settings by selecting the virtual switch associated with the host from the vSphere Web Client. See the *vSphere Networking* documentation.

MAC Address Changes

The security policy of a virtual switch includes a **MAC address changes** option. This option affects traffic that a virtual machine receives.

When the **Mac address changes** option is set to **Accept**, ESXi accepts requests to change the effective MAC address to a different address than the initial MAC address.

When the **Mac address changes** option is set to **Reject**, ESXi does not honor requests to change the effective MAC address to a different address than the initial MAC address. This setting protects the host against MAC impersonation. The port that the virtual machine adapter used to send the request is disabled and the virtual machine adapter does not receive any more frames until the effective MAC address matches the initial MAC address. The guest operating system does not detect that the MAC address change request was not honored.

Note The iSCSI initiator relies on being able to get MAC address changes from certain types of storage. If you are using ESXi iSCSI with iSCSI storage, set the **MAC address changes** option to **Accept**.

In some situations, you might have a legitimate need for more than one adapter to have the same MAC address on a network—for example, if you are using Microsoft Network Load Balancing in unicast mode. When Microsoft Network Load Balancing is used in the standard multicast mode, adapters do not share MAC addresses.

Forged Transmits

The **Forged transmits** option affects traffic that is transmitted from a virtual machine.

When the **Forged transmits** option is set to **Accept**, ESXi does not compare source and effective MAC addresses.

To protect against MAC impersonation, you can set the **Forged transmits** option to **Reject**. If you do, the host compares the source MAC address being transmitted by the guest operating system with the effective MAC address for its virtual machine adapter to see if they match. If the addresses do not match, the ESXi host drops the packet.

The guest operating system does not detect that its virtual machine adapter cannot send packets by using the impersonated MAC address. The ESXi host intercepts any packets with impersonated addresses before they are delivered, and the guest operating system might assume that the packets are dropped.

Promiscuous Mode Operation

Promiscuous mode eliminates any reception filtering that the virtual machine adapter performs so that the guest operating system receives all traffic observed on the wire. By default, the virtual machine adapter cannot operate in promiscuous mode.

Although promiscuous mode can be useful for tracking network activity, it is an insecure mode of operation, because any adapter in promiscuous mode has access to the packets even if some of the packets are received only by a particular network adapter. This means that an administrator or root user within a virtual machine can potentially view traffic destined for other guest or host operating systems.

Note In some situations, you might have a legitimate reason to configure a standard or a distributed virtual switch to operate in promiscuous mode, for example, if you are running network intrusion detection software or a packet sniffer.

Secure vSphere Distributed Switches and Distributed Port Groups

Administrators have several options for securing a vSphere Distributed Switches in their vSphere environment.

Procedure

1 For distributed port groups with static binding, verify that the Auto Expand feature is disabled.

  Auto Expand is enabled by default in vSphere 5.1 and later.

To disable Auto Expand, configure the `autoExpand` property under the distributed port group with the vSphere Web Services SDK or with a command-line interface. See the *vSphere Web Services SDK* documentation.

2 Ensure that all private VLAN IDs of any vSphere Distributed Switch are fully documented.

3 If you are using VLAN tagging on a dvPortgroup, VLAN IDs must correspond to the IDs on external VLAN-aware upstream switches. If VLAN IDs are not tracked completely, mistaken reuse of IDs could allow traffic between inappropriate physical and virtual machines. Similarly, wrong or missing VLAN IDs may lead to traffic not passing between physical and virtual machines.

4 Ensure that no unused ports exist on a virtual port group associated with a vSphere Distributed Switch.

5 Label all vSphere Distributed Switches.

vSphere Distributed Switches associated with an ESXi host require a field for the name of the switch. This label serves as a functional descriptor for the switch, just as the host name associated with a physical switch. The label on the vSphere Distributed Switch indicates the function or the IP subnet of the switch. For example, you can label the switch as internal to indicate that it is only for internal networking between a virtual machine's private virtual switch with no physical network adaptors bound to it.

6 Disable network healthcheck for your vSphere Distributed Switches if you are not actively using it.

Network healthcheck is disabled by default. Once enabled, the healthcheck packets contain information about the host, switch, and port that an attacker can potentially use. Use network healthcheck only for troubleshooting, and turn it off when troubleshooting is finished.

7 Protect virtual traffic against impersonation and interception Layer 2 attacks by configuring a security policy on port groups or ports.

The security policy on distributed port groups and ports includes the following options:

- Promiscuous mode (see "Promiscuous Mode Operation," on page 212)
- MAC address changes (see "MAC Address Changes," on page 211)
- Forged transmits (see "Forged Transmits," on page 212)

You can view and change the current settings by selecting **Manage Distributed Port Groups** from the right-button menu of the distributed switch and selecting **Security** in the wizard. See the *vSphere Networking* documentation.

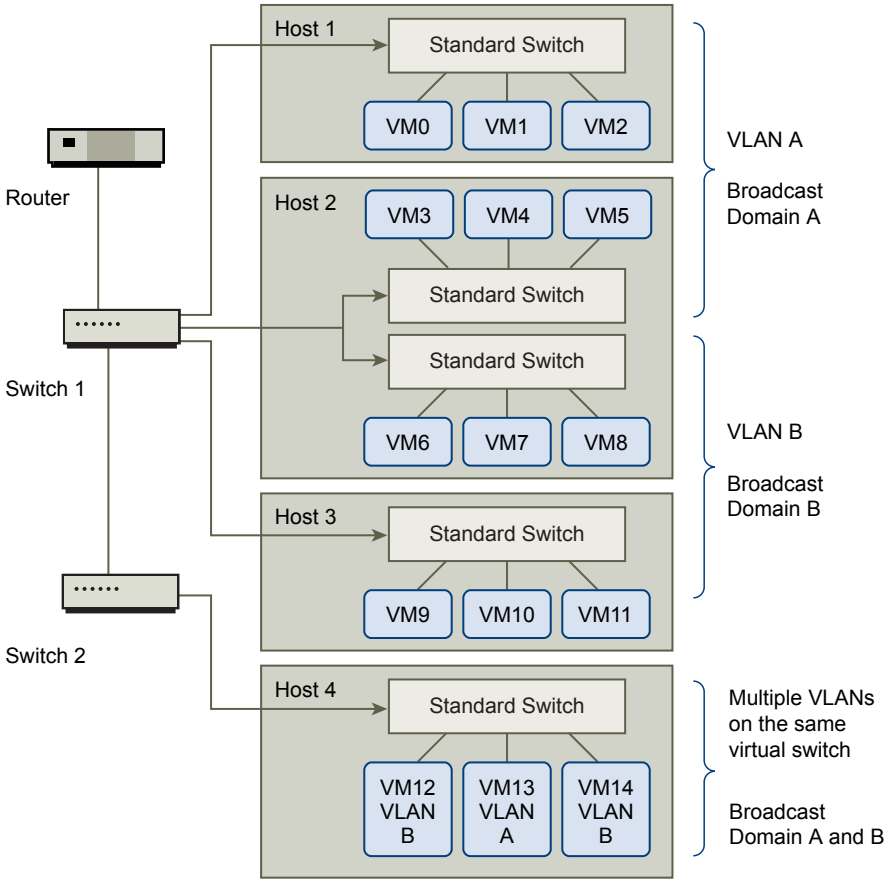
Securing Virtual Machines with VLANs

The network can be one of the most vulnerable parts of any system. Your virtual machine network requires as much protection as your physical network. Using VLANs can improve networking security in your environment.

VLANs are an IEEE standard networking scheme with specific tagging methods that allow routing of packets to only those ports that are part of the VLAN. When properly configured, VLANs provide a dependable means for you to protect a set of virtual machines from accidental or malicious intrusions.

VLANs let you segment a physical network so that two machines in the network are unable to transmit packets back and forth unless they are part of the same VLAN. For example, accounting records and transactions are among a company's most sensitive internal information. In a company whose sales, shipping, and accounting employees all use virtual machines in the same physical network, you might protect the virtual machines for the accounting department by setting up VLANs.

Figure 8-2. Sample VLAN Layout



In this configuration, all employees in the accounting department use virtual machines in VLAN A and the employees in sales use virtual machines in VLAN B.

The router forwards packets containing accounting data to the switches. These packets are tagged for distribution to VLAN A only. Therefore, the data is confined to Broadcast Domain A and cannot be routed to Broadcast Domain B unless the router is configured to do so.

This VLAN configuration prevents the sales force from intercepting packets destined for the accounting department. It also prevents the accounting department from receiving packets intended for the sales group. The virtual machines serviced by a single virtual switch can be in different VLANs.

Security Considerations for VLANs

The way you set up VLANs to secure parts of a network depends on factors such as the guest operating system and the way your network equipment is configured.

ESXi features a complete IEEE 802.1q-compliant VLAN implementation. VMware cannot make specific recommendations on how to set up VLANs, but there are factors to consider when using a VLAN deployment as part of your security enforcement policy.

Secure VLANs

Administrators have several options for securing the VLANs in their vSphere environment.

Procedure

1 Ensure that port groups are not configured to VLAN values that are reserved by upstream physical switches

Do not set VLAN IDs to values reserved for the physical switch.

2 Ensure that port groups are not configured to VLAN 4095 unless you are using for Virtual Guest Tagging (VGT).

Three types of VLAN tagging exist in vSphere:

- External Switch Tagging (EST)
- Virtual Switch Tagging (VST) - The virtual switch tags with the configured VLAN ID the traffic that is incoming to the attached virtual machines and removes the VLAN tag from the traffic that is leaving them. To set up VST mode, assign a VLAN ID between 1 and 4095.
- Virtual Guest Tagging (VGT) - Virtual machines handle VLAN traffic. To activate VGT mode, set the VLAN ID to 4095. On a distributed switch, you can also allow virtual machine traffic based on its VLAN by using the **VLAN Trunking** option.

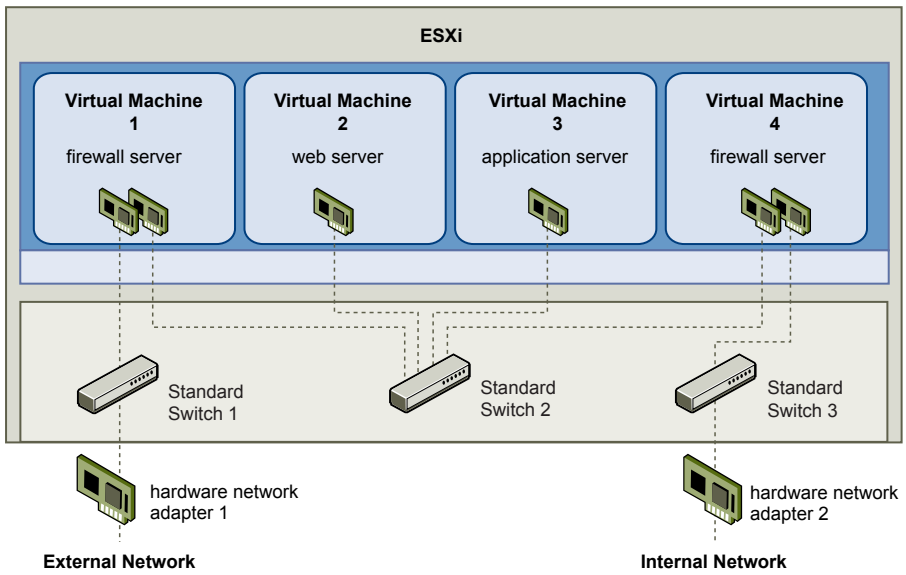
On a standard switch you can configure VLAN networking mode at switch or port group level, and on a distributed switch at distributed port group or port level.

3 Ensure that all VLANs on each virtual switch are fully documented and that each virtual switch has all required VLANs and only required VLANs.

Creating a Network DMZ on a Single ESXi Host

One example of how to use ESXi isolation and virtual networking features to configure a secure environment is the creation of a network demilitarized zone (DMZ) on a single host.

Figure 8-3. DMZ Configured on a Single ESXi Host



In this example, four virtual machines are configured to create a virtual DMZ on Standard Switch 2:

- Virtual Machine 1 and Virtual Machine 4 run firewalls and are connected to physical network adapters through standard switches. Both of these virtual machines are using multiple switches.

- Virtual Machine 2 runs a Web server, and Virtual Machine 3 runs as an application server. Both of these virtual machines are connected to one virtual switch.

The Web server and application server occupy the DMZ between the two firewalls. The conduit between these elements is Standard Switch 2, which connects the firewalls with the servers. This switch has no direct connection with any elements outside the DMZ and is isolated from external traffic by the two firewalls.

From an operational viewpoint, external traffic from the Internet enters Virtual Machine 1 through Hardware Network Adapter 1 (routed by Standard Switch 1) and is verified by the firewall installed on this machine. If the firewall authorizes the traffic, it is routed to the standard switch in the DMZ, Standard Switch 2. Because the Web server and application server are also connected to this switch, they can serve external requests.

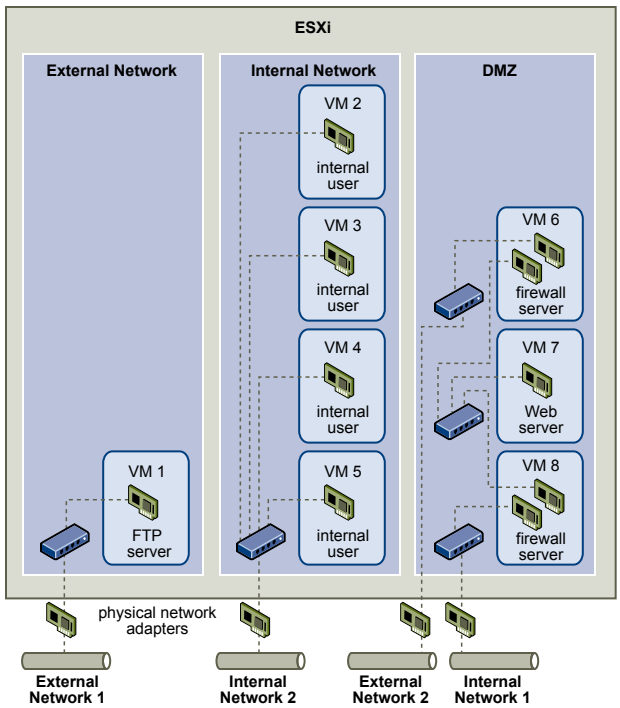
Standard Switch 2 is also connected to Virtual Machine 4. This virtual machine provides a firewall between the DMZ and the internal corporate network. This firewall filters packets from the Web server and application server. If a packet is verified, it is routed to Hardware Network Adapter 2 through Standard Switch 3. Hardware Network Adapter 2 is connected to the internal corporate network.

When creating a DMZ on a single host, you can use fairly lightweight firewalls. Although a virtual machine in this configuration cannot exert direct control over another virtual machine or access its memory, all the virtual machines are still connected through a virtual network. This network could be used for virus propagation or targeted for other types of attacks. The security of the virtual machines in the DMZ is equivalent to separate physical machines connected to the same network.

Creating Multiple Networks Within a Single ESXi Host

The ESXi system is designed so that you can connect some groups of virtual machines to the internal network, others to the external network, and still others to both—all on the same host. This capability is an outgrowth of basic virtual machine isolation coupled with a well-planned use of virtual networking features.

Figure 8-4. External Networks, Internal Networks, and a DMZ Configured on a Single ESXi Host



In the figure, the system administrator configured a host into three distinct virtual machine zones: FTP server, internal virtual machines, and DMZ. Each zone serves a unique function.

FTP server

Virtual Machine 1 is configured with FTP software and acts as a holding area for data sent to and from outside resources such as forms and collateral localized by a vendor.

This virtual machine is associated with an external network only. It has its own virtual switch and physical network adapter that connect it to External Network 1. This network is dedicated to servers that the company uses to receive data from outside sources. For example, the company uses External Network 1 to receive FTP traffic from vendors and allow vendors access to data stored on externally available servers though FTP. In addition to servicing Virtual Machine 1, External Network 1 services FTP servers configured on different ESXi hosts throughout the site.

Because Virtual Machine 1 does not share a virtual switch or physical network adapter with any virtual machines in the host, the other resident virtual machines cannot transmit packets to or receive packets from the Virtual Machine 1 network. This restriction prevents sniffing attacks, which require sending network traffic to the victim. More importantly, an attacker cannot use the natural vulnerability of FTP to access any of the host's other virtual machines.

Internal virtual machines

Virtual Machines 2 through 5 are reserved for internal use. These virtual machines process and store company-private data such as medical records, legal settlements, and fraud investigations. As a result, the system administrators must ensure the highest level of protection for these virtual machines.

These virtual machines connect to Internal Network 2 through their own virtual switch and network adapter. Internal Network 2 is reserved for internal use by personnel such as claims processors, in-house lawyers, or adjustors.

Virtual Machines 2 through 5 can communicate with one another through the virtual switch and with internal virtual machines elsewhere on Internal Network 2 through the physical network adapter. They cannot communicate with externally facing machines. As with the FTP server, these virtual machines cannot send packets to or receive packets from the other virtual machines' networks. Similarly, the host's other virtual machines cannot send packets to or receive packets from Virtual Machines 2 through 5.

DMZ

Virtual Machines 6 through 8 are configured as a DMZ that the marketing group uses to publish the company's external Web site.

This group of virtual machines is associated with External Network 2 and Internal Network 1. The company uses External Network 2 to support the Web servers that use the marketing and financial department to host the corporate Web site and other Web facilities that it hosts to outside users. Internal Network 1 is the conduit that the marketing department uses to publish content to the corporate Web site, post downloads, and maintain services like user forums.

Because these networks are separate from External Network 1 and Internal Network 2, and the virtual machines have no shared points of contact (switches or adapters), there is no risk of attack to or from the FTP server or the internal virtual machine group.

By capitalizing on virtual machine isolation, correctly configuring virtual switches, and maintaining network separation, the system administrator can house all three virtual machine zones in the same ESXi host and be confident that there will be no data or resource breaches.

The company enforces isolation among the virtual machine groups by using multiple internal and external networks and making sure that the virtual switches and physical network adapters for each group are completely separate from those of other groups.

Because none of the virtual switches straddle virtual machine zones, the system administrator succeeds in eliminating the risk of packet leakage from one zone to another. A virtual switch, by design, cannot leak packets directly to another virtual switch. The only way for packets to travel from one virtual switch to another is under the following circumstances:

- The virtual switches are connected to the same physical LAN.
- The virtual switches connect to a common virtual machine, which could be used to transmit packets.

Neither of these conditions occur in the sample configuration. If system administrators want to verify that no common virtual switch paths exist, they can check for possible shared points of contact by reviewing the network switch layout in the vSphere Web Client.

To safeguard the virtual machines' resources, the system administrator lowers the risk of DoS and DDoS attacks by configuring a resource reservation and a limit for each virtual machine. The system administrator further protects the ESXi host and virtual machines by installing software firewalls at the front and back ends of the DMZ, ensuring that the host is behind a physical firewall, and configuring the networked storage resources so that each has its own virtual switch.

Internet Protocol Security

Internet Protocol Security (IPsec) secures IP communications coming from and arriving at a host. ESXi hosts support IPsec using IPv6.

When you set up IPsec on a host, you enable authentication and encryption of incoming and outgoing packets. When and how IP traffic is encrypted depends on how you set up the system's security associations and security policies.

A security association determines how the system encrypts traffic. When you create a security association, you specify the source and destination, encryption parameters, and a name for the security association.

A security policy determines when the system should encrypt traffic. The security policy includes source and destination information, the protocol and direction of traffic to be encrypted, the mode (transport or tunnel) and the security association to use.

List Available Security Associations

ESXi can provide a list of all security associations available for use by security policies. The list includes both user created security associations and any security associations the VMkernel installed using Internet Key Exchange.

You can get a list of available security associations using the `esxcli` vSphere CLI command.

Procedure

- At the command prompt, enter the command **`esxcli network ip ipsec sa list`**.

ESXi displays a list of all available security associations.

Add an IPsec Security Association

Add a security association to specify encryption parameters for associated IP traffic.

You can add a security association using the `esxcli` vSphere CLI command.

Procedure

- At the command prompt, enter the command **`esxcli network ip ipsec sa add`** with one or more of the following options.

Option	Description
`--sa-source=` ***source address***	Required. Specify the source address.
`--sa-destination=` ***destination address***	Required. Specify the destination address.
`--sa-mode=` ***mode***	Required. Specify the mode, either `transport` or `tunnel`.
`--sa-spi=` ***security parameter index***	Required. Specify the security parameter index. The security parameter index identifies the security association to the host. It must be a hexadecimal with a 0x prefix. Each security association you create must have a unique combination of protocol and security parameter index.
`--encryption-algorithm=` ***encryption algorithm***	Required. Specify the encryption algorithm using one of the following parameters. ■ `3des-cbc` ■ `aes128-cbc` ■ `null` (provides no encryption)
`--encryption-key=` ***encryption key***	Required when you specify an encryption algorithm. Specify the encryption key. You can enter keys as ASCII text or as a hexadecimal with a 0x prefix.
`--integrity-algorithm=` ***authentication algorithm***	Required. Specify the authentication algorithm, either `hmac-sha1` or `hmac-sha2-256`.
`--integrity-key=` ***authentication key***	Required. Specify the authentication key. You can enter keys as ASCII text or as a hexadecimal with a 0x prefix.
`--sa-name=`***name***	Required. Provide a name for the security association.

Example: New Security Association Command

The following example contains extra line breaks for readability.

```
esxcli network ip ipsec sa add
--sa-source 3ffe:501:ffff:0::a
--sa-destination 3ffe:501:ffff:0001:0000:0000:0000:0001
--sa-mode transport
--sa-spi 0x1000
--encryption-algorithm 3des-cbc
--encryption-key 0x697076367265616479 6c6f676f336465736362636f757432
--integrity-algorithm hmac-sha1
--integrity-key 0x69707636726561647 96c6f67736861316f757432
--sa-name sa1
```

Remove an IPsec Security Association

You can remove a security association using the ESXCLI vSphere CLI command.

Prerequisites

Verify that the security association you want to use is not currently in use. If you try to remove a security association that is in use, the removal operation fails.

Procedure

- At the command prompt, enter the command
  `esxcli network ip ipsec sa remove --sa-name` ***`security_association_name`***

List Available IPsec Security Policies

You can list available security policies using the ESXCLI vSphere CLI command.

Procedure

- At the command prompt, enter the command **`esxcli network ip ipsec sp list`**

The host displays a list of all available security policies.

Create an IPSec Security Policy

Create a security policy to determine when to use the authentication and encryption parameters set in a security association. You can add a security policy using the ESXCLI vSphere CLI command.

Prerequisites

Before creating a security policy, add a security association with the appropriate authentication and encryption parameters as described in "Add an IPsec Security Association," on page 218.

Procedure

- At the command prompt, enter the command **`esxcli network ip ipsec sp add`** with one or more of the following options.

Option	Description
`--sp-source=` ***source address***	Required. Specify the source IP address and prefix length.
`--sp-destination=` ***destination address***	Required. Specify the destination address and prefix length.
`--source-port=` ***port***	Required. Specify the source port. The source port must be a number between 0 and 65535.
`--destination-port=` ***port***	Required. Specify the destination port. The source port must be a number between 0 and 65535.
`--upper-layer-protocol=` ***protocol***	Specify the upper layer protocol using one of the following parameters. ■ `tcp` ■ `udp` ■ `icmp6` ■ `any`
`--flow-direction=` ***direction***	Specify the direction in which you want to monitor traffic using either `in` or `out`.
`--action=` ***action***	Specify the action to take when traffic with the specified parameters is encountered using one of the following parameters. ■ `none`: Take no action ■ `discard`: Do not allow data in or out. ■ `ipsec`: Use the authentication and encryption information supplied in the security association to determine whether the data comes from a trusted source.
`--sp-mode=` ***mode***	Specify the mode, either `tunnel` or `transport`.
`--sa-name=`***security association name***	Required. Provide the name of the security association for the security policy to use.
`--sp-name=`***name***	Required. Provide a name for the security policy.

Example: New Security Policy Command

The following example includes extra line breaks for readability.

```
esxcli network ip ipsec add
--sp-source=2001:db8:1::/64
--sp-destination=2002:db8:1::/64
--source-port=23
--destination-port=25
--upper-layer-protocol=tcp
--flow-direction=out
--action=ipsec
--sp-mode=transport
--sa-name=sa1
--sp-name=sp1
```

Remove an IPsec Security Policy

You can remove a security policy from the ESXi host using the ESXCLI vSphere CLI command.

Prerequisites

Verify that the security policy you want to use is not currently in use. If you try to remove a security policy that is in use, the removal operation fails.

Procedure

- At the command prompt, enter the command **`esxcli network ip ipsec sp remove --sa-name`** ***`security policy name`***.

  To remove all security policies, enter the command **`esxcli network ip ipsec sp remove --remove-all`**.

Ensure Proper SNMP Configuration

If SNMP is not properly configured, monitoring information can be sent to a malicious host. The malicious host can then use this information to plan an attack.

Procedure

1. Run `esxcli system snmp get` to determine whether SNMP is currently used.
2. If your system does require SNMP, make sure that it is running by running the `esxcli system snmp set --enable true` command.
3. If your system uses SNMP, see the *Monitoring and Performance* publication for setup information for SNMP 3.

   SNMP must be configured on each ESXi host. You can use vCLI, PowerCLI, or the vSphere Web Services SDK for configuration.

Use Virtual Switches with the vSphere Network Appliance API Only If Required

If you are not using products that make use of the vSphere Network Appliance API (DvFilter), do not configure your host to send network information to a virtual machine. If the vSphere Network Appliance API is enabled, an attacker might attempt to connect a virtual machine to the filter. This connection might provide access to the network of other virtual machines on the host.

If you are using a product that makes use of this API, verify that the host is configured correctly. See the sections on DvFilter in *Developing and Deploying vSphere Solutions, vServices, and ESX Agents*. If your host is set up to use the API, make sure that the value of the `Net.DVFilterBindIpAddress` parameter matches the product that uses the API.

Procedure

1 To ensure that the `Net.DVFilterBindIpAddress` kernel parameter has the correct value, locate the parameter by using the vSphere Web Client.

   a Select the host and click the **Manage** tab.

   b Under System, select **Advanced System Settings**.

   c Scroll down to `Net.DVFilterBindIpAddress` and verify that the parameter has an empty value.

   The order of parameters is not strictly alphabetical. Type **`DVFilter`** in the Filter field to display all related parameters.

2 If you are not using DvFilter settings, make sure that the value is blank.

3 If you are using DvFilter settings, make sure the value of the parameter matches the value that the product that uses the DvFilter is using.

vSphere Networking Security Best Practices

Following networking security helps ensure the integrity of your vSphere deployment.

General Networking Security Recommendations

Following general network security recommendations is the first step in securing your networking environment. You can then move on to special areas, such as securing the network with firewalls or using IPsec.

- Ensure that physical switch ports are configured with Portfast if spanning tree is enabled. Because VMware virtual switches do not support STP, physical switch ports connected to an ESXi host must have Portfast configured if spanning tree is enabled to avoid loops within the physical switch network. If Portfast is not set, potential performance and connectivity issues might arise.
- Ensure that Netflow traffic for a Distributed Virtual Switch is only being sent to authorized collector IP addresses. Netflow exports are not encrypted and can contain information about the virtual network, increasing the potential for a successful man-in-the-middle attack. If Netflow export is required, verify that all Netflow target IP addresses are correct.
- Ensure that only authorized administrators have access to virtual networking components by using the role-based access controls. For example, virtual machine administrators should have access only to port groups in which their virtual machines reside. Network administrators should have permissions to all virtual networking components but no access to virtual machines. Limiting access reduces the risk of misconfiguration, whether accidental or malicious, and enforces key security concepts of separation of duties and least privilege.

- Ensure that port groups are not configured to the value of the native VLAN. Physical switches use VLAN 1 as their native VLAN. Frames on a native VLAN are not tagged with a 1. ESXi does not have a native VLAN. Frames with VLAN specified in the port group have a tag, but frames with VLAN not specified in the port group are not tagged. This can cause an issue because irtual machines that are tagged with a 1 end up as belonging to native VLAN of the physical switch.

  For example, frames on VLAN 1 from a Cisco physical switch are untagged because VLAN1 is the native VLAN on that physical switch. However, frames from the ESXi host that are specified as VLAN 1 are tagged with a 1; therefore, traffic from the ESXi host that is destined for the native VLAN is not routed correctly because it is tagged with a 1 instead of being untagged. Traffic from the physical switch that is coming from the native VLAN is not visible because it is not tagged. If the ESXi virtual switch port group uses the native VLAN ID, traffic from virtual machines on that port is not be visible to the native VLAN on the switch because the switch is expecting untagged traffic.

- Ensure that port groups are not configured to VLAN values reserved by upstream physical switches. Physical switches reserve certain VLAN IDs for internal purposes and often disallow traffic configured to these values. For example, Cisco Catalyst switches typically reserve VLANs 1001–1024 and 4094. Using a reserved VLAN might result in a denial of service on the network.

- Ensure that port groups are not configured to VLAN 4095 except for Virtual Guest Tagging (VGT). Setting a port group to VLAN 4095 activates VGT mode. In this mode, the virtual switch passes all network frames to the virtual machine without modifying the VLAN tags, leaving it to the virtual machine to deal with them.

- Restrict port-level configuration overrides on a distributed virtual switch. Port-level configuration overrides are disabled by default. Once enabled, overrides allow different security settings for a virtual machine than the settings at the port-group level. Certain virtual machines require unique configurations, but monitoring is essential. If overrides are not monitored, anyone who gains access to a virtual with a less secure distributed virtual switch configuration might attempt to exploit that access.

- Ensure that distributed virtual switch port mirror traffic is sent only to authorized collector ports or VLANs. A vSphere Distributed Switch can mirror traffic from one port to another to allow packet capture devices to collect specific traffic flows. Port mirroring sends a copy of all specified traffic in un-encrypted format. This mirrored traffic contains the full data in the packets captured and can result in total compromise of that data if misdirected. If port mirroring is required, verify that all port mirror destination VLAN, port and uplink IDs are correct.

Document and Check the vSphere VLAN Environment

Check your VLAN environment regularly to avoid addressing problems. Fully document the VLAN environment and ensure that VLAN IDs are used only once. Your documentation can help with troubleshooting and is essential when you want to expand the environment.

Procedure

1 Ensure that all vSwitch and VLANS IDs are fully documented

  If you are using VLAN tagging on a virtual switch, the IDs must correspond to the IDs on external VLAN-aware upstream switches. If VLAN IDs are not tracked completely, mistaken reuse of IDs might allow for traffic between the wrong physical and virtual machines. Similarly, if VLAN IDs are wrong or missing, traffic between physical and virtual machines might be blocked where you want traffic to pass.

2 Ensure that VLAN IDs for all distributed virtual port groups (dvPortgroup instances) are fully documented

  If you are using VLAN tagging on a dvPortgroup the IDs must correspond to the IDs on external VLAN-aware upstream switches. If VLAN IDs are not tracked completely, mistaken reuse of IDs might allow for traffic between the wrong physical and virtual machines. Similarly, if VLAN IDs are wrong or missing, traffic between physical and virtual machines might be blocked where you want traffic to pass.

3 Ensure that private VLAN IDs for all distributed virtual switches are fully documented

Private VLANs (PVLANs) for distributed virtual switches require primary and secondary VLAN IDs. These IDs must correspond to the IDs on external PVLAN-aware upstream switches. If VLAN IDs are not tracked completely, mistaken reuse of IDs might allow for traffic between the wrong physical and virtual machines. Similarly, if PVLAN IDs are wrong or missing, traffic between physical and virtual machines might be blocked where you want traffic to pass.

4 Verify that VLAN trunk links are connected only to physical switch ports that function as trunk links.

When connecting a virtual switch to a VLAN trunk port, you must properly configure both the virtual switch and the physical switch at the uplink port. If the physical switch is not properly configured, frames with the VLAN 802.1q header are forwarded to a switch that not expecting their arrival.

Adopting Sound Network Isolation Practices

Adapting sound network isolation practices significantly bolsters network security in your vSphere environment.

Isolate the Management Network

The vSphere management network provides access to the vSphere management interface on each component. Services running on the management interface provide an opportunity for an attacker to gain privileged access to the systems. Remote attacks are likely to begin with gaining access to this network. If an attacker gains access to the management network, it provides the staging ground for further intrusion.

Strictly control access to management network by protecting it at the security level of the most secure virtual machine running on an ESXi host or cluster. No matter how the management network is restricted, administrators must have access to this network to configure the ESXi hosts and vCenter Server system. Enable access to management functionality in a strictly controlled manner by using one of the following approaches.

- For especially sensitive environments, configure a controlled gateway or other controlled method to access the management network. For example, require that administrators connect to the management network through a VPN, and allow access only to trusted administrators.
- Configure jump boxes that run management clients.

Isolate Storage Traffic

Ensure that IP-based storage traffic is isolated. IP-based storage includes iSCSI and NFS. Virtual machines might share virtual switches and VLANs with the IP-based storage configurations. This type of configuration might expose IP-based storage traffic to unauthorized virtual machine users.

IP-based storage frequently is not encrypted; anyone with access to this network can view it. To restrict unauthorized users from viewing the IP-based storage traffic, logically separate the IP-based storage network traffic from the production traffic. Configure the IP-based storage adapters on separate VLANs or network segments from the VMkernel management network to limit unauthorized users from viewing the traffic.

Isolate VMotion Traffic

VMotion migration information is transmitted in plain text. Anyone with access to the network over which this information flows can view it. Potential attackers can intercept vMotion traffic to obtain the memory contents of a virtual machine. They might also stage a MiTM attack in which the contents are modified during migration.

Separate vMotion traffic from production traffic on an isolated network. Set up the network to be nonroutable, that is, make sure that no layer-3 router is spanning this and other networks, to prevent outside access to the network.

Best Practices Involving Multiple vSphere Components

9

Some security best practices, such as setting up NTP in your environment, affect more than one vSphere component. Consider these recommendations when configuring your environment.

See Chapter 5, "Securing ESXi Hosts," on page 131 and Chapter 7, "Securing Virtual Machines," on page 195 for related information.

This chapter includes the following topics:

- "Synchronizing Clocks on the vSphere Network," on page 225
- "Storage Security Best Practices," on page 228
- "Verify That Sending Host Performance Data to Guests is Disabled," on page 230
- "Setting Timeouts for the ESXi Shell and vSphere Web Client," on page 230

Synchronizing Clocks on the vSphere Network

Make sure that components on the vSphere network have their clocks synchronized. If the clocks on the machines in your vSphere network are not synchronized, SSL certificates, which are time-sensitive, might not be recognized as valid in communications between network machines.

Unsynchronized clocks can result in authentication problems, which can cause the installation to fail or prevent the vCenter Server Appliance vpxd service from starting.

Make sure any Windows host machine on which a vCenter component runs is synchronized with the NTP server. See the Knowledge Base article Timekeeping best practices for Windows, including NTP.

- Synchronize ESXi Clocks with a Network Time Server on page 225

  Before you install vCenter Server or deploy the vCenter Server Appliance, make sure all machines on your vSphere network have their clocks synchronized.

- Configuring Time Synchronization Settings in the vCenter Server Appliance on page 226

  You can change the time synchronization settings in the vCenter Server Appliance after deployment.

Synchronize ESXi Clocks with a Network Time Server

Before you install vCenter Server or deploy the vCenter Server Appliance, make sure all machines on your vSphere network have their clocks synchronized.

This task explains how to set up NTP from the vSphere Client. You can instead use the `vicfg-ntp` vCLI command. See the *vSphere Command-Line Interface Reference*.

Procedure

1 Start the vSphere Client, and connect to the ESXi host.

2 On the **Configuration** tab, click **Time Configuration**.

3 Click **Properties**, and click **Options**.

4 Select **NTP Settings**.

5 Click **Add**.

6 In the Add NTP Server dialog box, enter the IP address or fully qualified domain name of the NTP server to synchronize with.

7 Click **OK**.

The host time synchronizes with the NTP server.

Configuring Time Synchronization Settings in the vCenter Server Appliance

You can change the time synchronization settings in the vCenter Server Appliance after deployment.

When you deploy the vCenter Server Appliance, you can choose the time synchronization method to be either by using an NTP server or by using VMware Tools. In case the time settings in your vSphere network change, you can edit the vCenter Server Appliance and configure the time synchronization settings by using the commands in the appliance shell.

When you enable periodic time synchronization, VMware Tools sets the time of the guest operating system to be the same as the time of the host.

After time synchronization occurs, VMware Tools checks once every minute to determine whether the clocks on the guest operating system and the host still match. If not, the clock on the guest operating system is synchronized to match the clock on the host.

Native time synchronization software, such as Network Time Protocol (NTP), is typically more accurate than VMware Tools periodic time synchronization and is therefore preferred. You can use only one form of periodic time synchronization in the vCenter Server Appliance. If you decide to use native time synchronization software, vCenter Server Appliance VMware Tools periodic time synchronization is disabled, and the reverse.

Use VMware Tools Time Synchronization

You can set up the vCenter Server Appliance to use VMware Tools time synchronization.

Procedure

1 Access the appliance shell and log in as a user who has the administrator or super administrator role.

The default user with super administrator role is root.

2 Run the command to enable VMware Tools time synchronization.

```
timesync.set --mode host
```

3 (Optional) Run the command to verify that you successfully applied the VMware Tools time synchronization.

```
timesync.get
```

The command returns that the time synchronization is in host mode.

The time of the appliance is synchronized with the time of the ESXi host.

Add or Replace NTP Servers in the vCenter Server Appliance Configuration

To set up the vCenter Server Appliance to use NTP-based time synchronization, first add the NTP servers to the vCenter Server Appliance configuration.

Procedure

1 Access the appliance shell and log in as a user who has the administrator or super administrator role.

The default user with super administrator role is root.

2 Add NTP servers to the vCenter Server Appliance configuration by running the `ntp.server.add` command.

For example, run the following command:

```
ntp.server.add --servers IP-addresses-or-host-names
```

Here *IP-addresses-or-host-names* is a comma-separated list of IP addresses or host names of the NTP servers.

This command adds NTP servers to the configuration. If the time synchronization is based on an NTP server, then the NTP daemon is restarted to reload the new NTP servers. Otherwise, this command just adds the new NTP servers to the existing NTP configuration.

3 (Optional) To delete old NTP servers and add new ones to the vCenter Server Appliance configuration, run the `ntp.server.set` command.

For example, run the following command:

```
ntp.server.set --servers IP-addresses-or-host-names
```

Here *IP-addresses-or-host-names* is a comma-separated list of IP addresses or host names of the NTP servers.

This command deletes old NTP servers from the configuration and sets the input NTP servers in the configuration. If the time synchronization is based on an NTP server, the NTP daemon is restarted to reload the new NTP configuration. Otherwise, this command just replaces the servers in NTP configuration with the servers that you provide as input.

Synchronize the Time in the vCenter Server Appliance with an NTP Server

You can configure the time synchronization settings in the vCenter Server Appliance to be based on an NTP server.

Prerequisites

Set up one or more Network Time Protocol (NTP) servers in the vCenter Server Appliance configuration. See "Add or Replace NTP Servers in the vCenter Server Appliance Configuration," on page 227.

Procedure

1 Access the appliance shell and log in as a user who has the administrator or super administrator role.

The default user with super administrator role is root.

2 Run the command to enable NTP-based time synchronization.

```
timesync.set --mode NTP
```

3 (Optional) Run the command to verify that you successfully applied the NTP synchronization.

```
timesync.get
```

The command returns that the time synchronization is in NTP mode.

Storage Security Best Practices

Follow best practices for storage security, as outlined by your storage security provider. You can also take advantage of CHAP and mutual CHAP to secure iSCSI storage, mask and zone SAN resources, and configure Kerberos credentials for NFS 4.1.

See also the *VMware Virtual SAN* documentation.

Securing iSCSI Storage

The storage you configure for a host might include one or more storage area networks (SANs) that use iSCSI. When you configure iSCSI on a host, you can take several measures to minimize security risks.

iSCSI is a means of accessing SCSI devices and exchanging data records by using TCP/IP over a network port rather than through a direct connection to a SCSI device. In iSCSI transactions, blocks of raw SCSI data are encapsulated in iSCSI records and transmitted to the requesting device or user.

iSCSI SANs let you make efficient use of existing Ethernet infrastructures to provide hosts access to storage resources that they can dynamically share. iSCSI SANs provide an economical storage solution for environments that rely on a common storage pool to serve numerous users. As with any networked system, your iSCSI SANs can be subject to security breaches.

NOTE The requirements and procedures for securing an iSCSI SAN are similar for the hardware iSCSI adapters you can use with hosts and for iSCSI configured directly through the host.

Securing iSCSI Devices

One means of securing iSCSI devices from unwanted intrusion is to require that the host, or initiator, be authenticated by the iSCSI device, or target, whenever the host attempts to access data on the target LUN.

The goal of authentication is to prove that the initiator has the right to access a target, a right granted when you configure authentication.

ESXi does not support Secure Remote Protocol (SRP), or public-key authentication methods for iSCSI. You can use Kerberos only with NFS 4.1.

ESXi supports both CHAP and Mutual CHAP authentication. the *vSphere Storage* documentation explains how to select the best authentication method for your iSCSI device and how to set up CHAP.

Ensure uniqueness of CHAP secrets. The mutual authentication secret for each host should be different; if possible, the secret should be different for each client authenticating to the server as well. This ensures that if a single host is compromised, an attacker cannot create another arbitrary host and authenticate to the storage device. With a single shared secret, compromise of one host can allow an attacker to authenticate to the storage device.

Protecting an iSCSI SAN

When you plan your iSCSI configuration, take measures to improve the overall security of the iSCSI SAN. Your iSCSI configuration is only as secure as your IP network, so by enforcing good security standards when you set up your network, you help safeguard your iSCSI storage.

The following are some specific suggestions for enforcing good security standards.

Protect Transmitted Data

A primary security risk in iSCSI SANs is that an attacker might sniff transmitted storage data.

Take additional measures to prevent attackers from easily seeing iSCSI data. Neither the hardware iSCSI adapter nor ESXi iSCSI initiator encrypts the data that they transmit to and from the targets, making the data more vulnerable to sniffing attacks.

Allowing your virtual machines to share standard switches and VLANs with your iSCSI configuration potentially exposes iSCSI traffic to misuse by a virtual machine attacker. To help ensure that intruders cannot listen to iSCSI transmissions, make sure that none of your virtual machines can see the iSCSI storage network.

If you use a hardware iSCSI adapter, you can accomplish this by making sure that the iSCSI adapter and ESXi physical network adapter are not inadvertently connected outside the host by virtue of sharing a switch or some other means. If you configure iSCSI directly through the ESXi host, you can accomplish this by configuring iSCSI storage through a different standard switch than the one used by your virtual machines.

In addition to protecting the iSCSI SAN by giving it a dedicated standard switch, you can configure your iSCSI SAN on its own VLAN to improve performance and security. Placing your iSCSI configuration on a separate VLAN ensures that no devices other than the iSCSI adapter have visibility into transmissions within the iSCSI SAN. Also, network congestion from other sources cannot interfere with iSCSI traffic.

Secure iSCSI Ports

When you run iSCSI devices, ESXi does not open any ports that listen for network connections. This measure reduces the chances that an intruder can break into ESXi through spare ports and gain control over the host. Therefore, running iSCSI does not present any additional security risks at the ESXi end of the connection.

Any iSCSI target device that you run must have one or more open TCP ports to listen for iSCSI connections. If any security vulnerabilities exist in the iSCSI device software, your data can be at risk through no fault of ESXi. To lower this risk, install all security patches that your storage equipment manufacturer provides and limit the devices connected to the iSCSI network.

Masking and Zoning SAN Resources

You can use zoning and LUN masking to segregate SAN activity and restrict access to storage devices.

You can protect access to storage in your vSphere environment by using zoning and LUN masking with your SAN resources. For example, you might manage zones defined for testing independently within the SAN so they do not interfere with activity in the production zones. Similarly, you might set up different zones for different departments.

When you set up zones, take into account any host groups that are set up on the SAN device.

Zoning and masking capabilities for each SAN switch and disk array and the tools for managing LUN masking are vendor specific.

See your SAN vendor's documentation and the *vSphere Storage* documentation.

Using Kerberos Credentials for NFS 4.1

With NFS version 4.1, ESXi supports Kerberos authentication mechanism.

Kerberos is an authentication service that allows an NFS 4.1 client installed on ESXi to prove its identity to an NFS server before mounting an NFS share. Kerberos uses cryptography to work across an insecure network connection. The vSphere implementation of Kerberos for NFS 4.1 supports only identity verification for the client and server, but does not provide data integrity or confidentiality services.

When you use Kerberos authentication, the following considerations apply:

- ESXi uses Kerberos version 5 with Active Directory domain and Key Distribution Center (KDC).
- As a vSphere administrator, you specify Active Directory credentials to provide an access to NFS 4.1 Kerberos datastores to an NFS user. A single set of credentials is used to access all Kerberos datastores mounted on that host.

- When multiple ESXi hosts share the same NFS 4.1 datastore, you must use the same Active Directory credentials for all hosts that access the shared datastore. You can automate this by setting the user in host profiles and applying the profile to all ESXi hosts.
- NFS 4.1 does not support simultaneous AUTH_SYS and Kerberos mounts.
- NFS 4.1 with Kerberos does not support IPv6. Only IPv4 is supported.

See the *vSphere Storage* documentation for step-by-step instructions.

Verify That Sending Host Performance Data to Guests is Disabled

vSphere includes virtual machine performance counters on Windows operating systems where VMware Tools is installed. Performance counters allow virtual machine owners to do accurate performance analysis within the guest operating system. By default, vSphere does not expose host information to the guest virtual machine.

The ability to send host performance data to a guest virtual machine is disabled by default. This default setting prevents a virtual machine from obtaining detailed information about the physical host, and does not make host data available if a breach of security of the virtual machine occurs.

Note The procedure below illustrates the basic process. Use the vSphere or one of the vSphere command-line interfaces (vCLI, PowerCLI, and so on) for performing this task on all hosts simultaneously instead.

Procedure

1 On the ESXi system that hosts the virtual machine, browse to the VMX file.

Virtual machine configuration files are located in the `/vmfs/volumes/datastore` directory, where *datastore* is the name of the storage device where the virtual machine files are stored.

2 In the VMX file, verify that the following parameter is set.

```
tools.guestlib.enableHostInfo=FALSE
```

3 Save and close the file.

You cannot retrieve performance information about the host from inside the guest virtual machine.

Setting Timeouts for the ESXi Shell and vSphere Web Client

To prevent intruders from using an idle session, be sure to set timeouts for the ESXi Shell and vSphere Web Client

ESXi Shell Timeout

For the ESXi Shell, you can set the following timeouts from the vSphere Web Client and from the Direct Console User Interface (DCUI).

Availability Timeout The availability timeout setting is the amount of time that can elapse before you must log in after the ESXi Shell is enabled. After the timeout period, the service is disabled and users are not allowed to log in.

Idle Timeout The idle timeout is the amount of time that can elapse before the user is logged out of an idle interactive sessions. Changes to the idle timeout apply the next time a user logs in to the ESXi Shell and do not affect existing sessions.

vSphere Web Client Timeout

vSphere Web Client sessions terminate after 120 minutes by default. You can change this default in the `webclient.properties` file, as discussed in the *vCenter Server and Host Management* documentation.

10 Defined Privileges

The following tables list the default privileges that, when selected for a role, can be paired with a user and assigned to an object. The tables in this appendix use VC to indicate vCenter Server and HC to indicate host client, a standalone ESXi or Workstation host.

When setting permissions, verify all the object types are set with appropriate privileges for each particular action. Some operations require access permission at the root folder or parent folder in addition to access to the object being manipulated. Some operations require access or performance permission at a parent folder and a related object.

vCenter Server extensions might define additional privileges not listed here. Refer to the documentation for the extension for more information on those privileges.

This chapter includes the following topics:

- "Alarms Privileges," on page 234
- "Auto Deploy and Image Profile Privileges," on page 235
- "Certificates Privileges," on page 235
- "Content Library Privileges," on page 236
- "Datastore Privileges," on page 237
- "Datastore Cluster Privileges," on page 238
- "Distributed Switch Privileges," on page 238
- "ESX Agent Manager Privileges," on page 239
- "Extension Privileges," on page 239
- "Folder Privileges," on page 239
- "Global Privileges," on page 240
- "Host CIM Privileges," on page 240
- "Host Configuration Privileges," on page 241
- "Host Inventory," on page 242
- "Host Local Operations Privileges," on page 242
- "Host vSphere Replication Privileges," on page 243
- "Host Profile Privileges," on page 243
- "Inventory Service Provider Privileges," on page 244
- "Inventory Service Tagging Privileges," on page 244

- "Network Privileges," on page 245
- "Performance Privileges," on page 245
- "Permissions Privileges," on page 245
- "Profile-driven Storage Privileges," on page 246
- "Resource Privileges," on page 246
- "Scheduled Task Privileges," on page 247
- "Sessions Privileges," on page 247
- "Storage Views Privileges," on page 248
- "Tasks Privileges," on page 248
- "Transfer Service Privileges," on page 248
- "VRM Policy Privileges," on page 248
- "Virtual Machine Configuration Privileges," on page 248
- "Virtual Machine Guest Operations Privileges," on page 250
- "Virtual Machine Interaction Privileges," on page 251
- "Virtual Machine Inventory Privileges," on page 253
- "Virtual Machine Provisioning Privileges," on page 253
- "Virtual Machine Service Configuration Privileges," on page 255
- "Virtual Machine Snapshot Management Privileges," on page 255
- "Virtual Machine vSphere Replication Privileges," on page 256
- "dvPort Group Privileges," on page 256
- "vApp Privileges," on page 257
- "vServices Privileges," on page 258

Alarms Privileges

Alarms privileges control the ability to create, modify, and respond to alarms on inventory objects.

You can set this privilege at different levels in the hierarchy. For example, if you set a privilege at the folder level, you can propagate the privilege to one or more objects within the folder. The object listed in the Required On column must have the privilege set, either directly or inherited.

Table 10-1. Alarms Privileges

Privilege Name	Description	Required On
Alarms.Acknowledge alarm	Allows suppression of all alarm actions on all triggered alarms.	Object on which an alarm is defined
Alarms.Create alarm	Allows creation of a new alarm. When creating alarms with a custom action, privilege to perform the action is verified when the user creates the alarm.	Object on which an alarm is defined
Alarms.Disable alarm action	Allows stopping an alarm action from occurring after an alarm has been triggered. This does not disable the alarm.	Object on which an alarm is defined
Alarms.Modify alarm	Allows changing the properties of an alarm.	Object on which an alarm is defined

Table 10-1. Alarms Privileges (Continued)

Privilege Name	Description	Required On
Alarms.Remove alarm	Allows deletion of an alarm.	Object on which an alarm is defined
Alarms.Set alarm status	Allows changing the status of the configured event alarm. The status can change to **Normal**, **Warning**, or **Alert**.	Object on which an alarm is defined

Auto Deploy and Image Profile Privileges

Auto Deploy privileges control who can perform different tasks on Auto Deploy rules, and who can associate a host. Auto Deploy privileges also allow you to control who can create or edit an image profile.

The table describes privileges that determine who can manage Auto Deploy rules and rule sets and who can create and edit image profiles. See *vSphere Installation and Setup*.

You can set this privilege at different levels in the hierarchy. For example, if you set a privilege at the folder level, you can propagate the privilege to one or more objects within the folder. The object listed in the Required On column must have the privilege set, either directly or inherited.

Table 10-2. Auto Deploy Privileges

Privilege Name	Description	Required On
Auto Deploy.Host.AssociateMachine	Allows users to run a PowerCLI command that associates a host with a machine.	vCenter Server
Auto Deploy.Image Profile .Create	Allows creation of image profiles.	vCenter Server
Auto Deploy.Image Profile .Edit	Allows editing of image profiles.	vCenter Server
Auto Deploy.Rule .Create	Allows creation of Auto Deploy rules.	vCenter Server
Auto Deploy.Rule .Delete	Allows deletion of Auto Deploy rules.	vCenter Server
Auto Deploy.Rule .Delete	Allows editing of Auto Deploy rules.	vCenter Server
Auto Deploy.RuleSet .Activate	Allows activation of Auto Deploy rule sets.	vCenter Server
Auto Deploy.RuleSet .Edit	Allows editing of Auto Deploy rule sets.	vCenter Server

Certificates Privileges

Certificates privileges control which users can manage ESXi certificates.

This privilege determines who can perform certificate management for ESXi hosts. See "Required Privileges for Certificate Management Operations," on page 97 for information on vCenter Server certificate management.

You can set this privilege at different levels in the hierarchy. For example, if you set a privilege at the folder level, you can propagate the privilege to one or more objects within the folder. The object listed in the Required On column must have the privilege set, either directly or inherited.

Table 10-3. Host Certificates Privileges

Privilege Name	Description	Required On
Certificates. Manage Certificates	Allows certificate management for ESXi hosts.	vCenter Server

Content Library Privileges

Content Libraries provide simple and effective management for virtual machine templates and vApps. Content library privileges control who can view or manage different aspects of content libraries.

You can set this privilege at different levels in the hierarchy. For example, if you set a privilege at the folder level, you can propagate the privilege to one or more objects within the folder. The object listed in the Required On column must have the privilege set, either directly or inherited.

Table 10-4. Content Library Privileges

Privilege Name	Description	Required On
Content library. Add library item	Allows addition of items in a library.	Library
Content library. Configure settings	Allows changes to settings for a content library. No vSphere Web Client user interface elements are associated with this privilege.	Library
Content library. Create local library	Allows creation of local libraries on the specified vCenter Server system.	vCenter Server
Content library. Create subscribed library	Allows creation of subscribed libraries.	vCenter Server
Content library. Delete library item	Allows deletion of library items.	Library. Set this permission to propagate to all library items.
Content library. Delete local library	Allows deletion of a local library.	Library
Content library. Delete subscribed library	Allows deletion of a subscribed library.	Library
Content library. Download files	Allows download of files from the content library.	Library
Content library. Evict library item	Allows eviction of items. The content of a subscribed library can be cached or not cached. If the content is cached, you can release a library item by evicting it if you have this privilege.	Library. Set this permission to propagate to all library items.
Content library. Evict subscribed library	Allows eviction of a subscribed library. The content of a subscribed library can be cached or not cached. If the content is cached, you can release a library by evicting it if you have this privilege.	Library
Content library. Import Storage	Allows a user to import a library item if the source file URL starts with ds:// or file://. This privilege is disabled for content library administrator by default, Because an import from a storage URL implies import of content , enable this privilege only if necessary and if now security concern exists for the user who will perform the import.	Library
Content library. Probe subscription information	This privilege allows solution users and APIs to probe a remote library's subscription info including URL, SSL certificate and password. The resulting structure describes whether the subscription configuration is successful or whether there are problems such as SSL errors.	Library
Content library. Read storage	Allows reading of content library storage.	Library
Content library. Sync library item	Allows synchronization of library items.	Library. Set this permission to propagate to all library items.
Content library. Sync subscribed library	Allows synchronization of subscribed libraries.	Library

Table 10-4. Content Library Privileges (Continued)

Privilege Name	Description	Required On
Content library. Type introspection	Allows a solution user or API to introspect the type support plugins for the content library service.	Library
Content library. Update configuration settings	Allows you to update the configuration settings. No vSphere Web Client user interface elements are associated with this privilege.	Library
Content library. Update files	Allows you to upload content into the content library. Also allows you to remove files from a library item.	Library
Content library. Update library	Allows updates to the content library.	Library
Content library. Update library item	Allows updates to library items.	Library. Set this permission to propagate to all library items.
Content library. Update local library	Allows updates of local libraries.	Library
Content library. Update subscribed library	Allows you to update the properties of a subscribed library.	Library
Content library. View configuration settings	Allows you to view the configuration settings. No vSphere Web Client user interface elements are associated with this privilege.	Library

Datastore Privileges

Datastore privileges control the ability to browse, manage, and allocate space on datastores.

You can set this privilege at different levels in the hierarchy. For example, if you set a privilege at the folder level, you can propagate the privilege to one or more objects within the folder. The object listed in the Required On column must have the privilege set, either directly or inherited.

Table 10-5. Datastore Privileges

Privilege Name	Description	Required On
Datastore.Allocate space	Allows allocating space on a datastore for a virtual machine, snapshot, clone, or virtual disk.	Data stores
Datastore.Browse datastore	Allows browsing files on a datastore.	Data stores
Datastore.Configure datastore	Allows configuration of a datastore.	Data stores
Datastore.Low level file operations	Allows performing read, write, delete, and rename operations in the datastore browser.	Data stores
Datastore.Move datastore	Allows moving a datastore between folders. Privileges must be present at both the source and destination.	Datastore, source and destination
Datastore.Remove datastore	Allows removal of a datastore. This privilege is deprecated. To have permission to perform this operation, a user or group must have this privilege assigned in both the object and its parent object.	Data stores
Datastore.Remove file	Allows deletion of files in the datastore. This privilege is deprecated. Assign the **Low level file operations** privilege.	Data stores
Datastore.Rename datastore	Allows renaming a datastore.	Data stores

Table 10-5. Datastore Privileges (Continued)

Privilege Name	Description	Required On
Datastore.Update virtual machine files	Allows updating file paths to virtual machine files on a datastore after the datastore has been resignatured.	Data stores
Datastore.Update virtual machine metadata	Allows updating virtual machine metadata associated with a datastore.	Data stores

Datastore Cluster Privileges

Datastore cluster privileges control the configuration of datastore clusters for Storage DRS.

You can set this privilege at different levels in the hierarchy. For example, if you set a privilege at the folder level, you can propagate the privilege to one or more objects within the folder. The object listed in the Required On column must have the privilege set, either directly or inherited.

Table 10-6. Datastore Cluster Privileges

Privilege Name	Description	Required On
Datastore cluster.Configure a datatstore cluster	Allows creation of and configuration of settings for datastore clusters for Storage DRS.	Datastore clusters

Distributed Switch Privileges

Distributed Switch privileges control the ability to perform tasks related to the management of Distributed Switch instances.

You can set this privilege at different levels in the hierarchy. For example, if you set a privilege at the folder level, you can propagate the privilege to one or more objects within the folder. The object listed in the Required On column must have the privilege set, either directly or inherited.

Table 10-7. vSphere Distributed Switch Privileges

Privilege Name	Description	Required On
Distributed switch.Create	Allows creation of a distributed switch.	Data centers, Network folders
Distributed switch.Delete	Allows removal of a distributed switch. To have permission to perform this operation, a user or group must have this privilege assigned in both the object and its parent object.	Distributed switches
Distributed switch.Host operation	Allows changing the host members of a distributed switch.	Distributed switches
Distributed switch.Modify	Allows changing the configuration of a distributed switch.	Distributed switches
Distributed switch.Move	Allows moving a vSphere Distributed Switch to another folder.	Distributed switches
Distributed switch.Network I/O control operation	Allow changing the resource settings for a vSphere Distributed Switch.	Distributed switches
Distributed switch.Policy operation	Allows changing the policy of a vSphere Distributed Switch.	Distributed switches
Distributed switch .Port configuration operation	Allow changing the configuration of a port in a vSphere Distributed Switch.	Distributed switches
Distributed switch.Port setting operation	Allows changing the setting of a port in a vSphere Distributed Switch.	Distributed switches
Distributed switch.VSPAN operation	Allows changing the VSPAN configuration of a vSphere Distributed Switch.	Distributed switches

ESX Agent Manager Privileges

ESX Agent Manager privileges control operations related to ESX Agent Manager and agent virtual machines. The ESX Agent Manager is a service that lets you install management virtual machines, which are tied to a host and not affected by VMware DRS or other services that migrate virtual machines.

You can set this privilege at different levels in the hierarchy. For example, if you set a privilege at the folder level, you can propagate the privilege to one or more objects within the folder. The object listed in the Required On column must have the privilege set, either directly or inherited.

Table 10-8. ESX Agent Manager

Privilege Name	Description	Required On
ESX Agent Manager.Config	Allows deployment of an agent virtual machine on a host or cluster.	Virtual machines
ESX Agent Manager.Modify	Allows modifications to an agent virtual machine such as powering off or deleting the virtual machine.	Virtual machines
ESX Agent View.View	Allows viewing of an agent virtual machine.	Virtual machines

Extension Privileges

Extension privileges control the ability to install and manage extensions.

You can set this privilege at different levels in the hierarchy. For example, if you set a privilege at the folder level, you can propagate the privilege to one or more objects within the folder. The object listed in the Required On column must have the privilege set, either directly or inherited.

Table 10-9. Extension Privileges

Privilege Name	Description	Required On
Extension.Register extension	Allows registration of an extension (plug-in).	Root vCenter Server
Extension.Unregister extension	Allows unregistering an extension (plug-in).	Root vCenter Server
Extension.Update extension	Allows updates to an extension (plug-in).	Root vCenter Server

Folder Privileges

Folder privileges control the ability to create and manage folders.

You can set this privilege at different levels in the hierarchy. For example, if you set a privilege at the folder level, you can propagate the privilege to one or more objects within the folder. The object listed in the Required On column must have the privilege set, either directly or inherited.

Table 10-10. Folder Privileges

Privilege Name	Description	Required On
Folder.Create folder	Allows creation of a new folder.	Folders
Folder.Delete folder	Allows deletion of a folder. To have permission to perform this operation, a user or group must have this privilege assigned in both the object and its parent object.	Folders
Folder.Move folder	Allows moving a folder. Privilege must be present at both the source and destination.	Folders
Folder.Rename folder	Allows changing the name of a folder.	Folders

Global Privileges

Global privileges control global tasks related to tasks, scripts, and extensions.

You can set this privilege at different levels in the hierarchy. For example, if you set a privilege at the folder level, you can propagate the privilege to one or more objects within the folder. The object listed in the Required On column must have the privilege set, either directly or inherited.

Table 10-11. Global Privileges

Privilege Name	Description	Required On
Global.Act as vCenter Server	Allows preparation or initiation of a vMotion send operation or a vMotion receive operation.	Root vCenter Server
Global.Cancel task	Allows cancellation of a running or queued task.	Inventory object related to the task
Global.Capacity planning	Allows enabling the use of capacity planning for planning consolidation of physical machines to virtual machines.	Root vCenter Server
Global.Diagnostics	Allows retrieval of a list of diagnostic files, log header, binary files, or diagnostic bundle. To avoid potential security breaches, limit this privilege to the vCenter Server Administrator role.	Root vCenter Server
Global.Disable methods	Allows servers for vCenter Server extensions to disable certain operations on objects managed by vCenter Server.	Root vCenter Server
Global.Enable methods	Allows servers for vCenter Server extensions to enable certain operations on objects managed byvCenter Server.	Root vCenter Server
Global.Global tag	Allows adding or removing global tags.	Root host or vCenter Server
Global.Health	Allows viewing the health of vCenter Server components.	Root vCenter Server
Global.Licenses	Allows viewing installed licenses and adding or removing licenses.	Root host or vCenter Server
Global.Log event	Allows logging a user-defined event against a particular managed entity.	Any object
Global.Manage custom attributes	Allows adding, removing, or renaming custom field definitions.	Root vCenter Server
Global.Proxy	Allows access to an internal interface for adding or removing endpoints to or from the proxy.	Root vCenter Server
Global.Script action	Allows scheduling a scripted action in conjunction with an alarm.	Any object
Global.Service managers	Allows use of the `resxtop` command in the vSphere CLI.	Root host or vCenter Server
Global.Set custom attribute	Allows viewing, creating, or removing custom attributes for a managed object.	Any object
Global.Settings	Allows reading and modifying runtime vCenter Server configuration settings.	Root vCenter Server
Global.System tag	Allows adding or removing system tags.	Root vCenter Server

Host CIM Privileges

Host CIM privileges control the use of CIM for host health monitoring.

You can set this privilege at different levels in the hierarchy. For example, if you set a privilege at the folder level, you can propagate the privilege to one or more objects within the folder. The object listed in the Required On column must have the privilege set, either directly or inherited.

Table 10-12. Host CIM Privileges

Privilege Name	Description	Required On
Host.CIM.CIM Interaction	Allow a client to obtain a ticket to use for CIM services.	Hosts

Host Configuration Privileges

Host configuration privileges control the ability to configure hosts.

You can set this privilege at different levels in the hierarchy. For example, if you set a privilege at the folder level, you can propagate the privilege to one or more objects within the folder. The object listed in the Required On column must have the privilege set, either directly or inherited.

Table 10-13. Host Configuration Privileges

Privilege Name	Description	Required On
Host.Configuration.Advanced Settings	Allows setting advanced host configuration options.	Hosts
Host.Configuration.Authentication Store	Allows configuring Active Directory authentication stores.	Hosts
Host.Configuration.Change PciPassthru settings	Allows changes to PciPassthru settings for a host.	Hosts
Host.Configuration.Change SNMP settings	Allows changes to SNMP settings for a host.	Hosts
Host.Configuration.Change date and time settings	Allows changes to date and time settings on the host.	Hosts
Host.Configuration.Change settings	Allows setting of lockdown mode on ESXi hosts.	Hosts
Host.Configuration.Connection	Allows changes to the connection status of a host (connected or disconnected).	Hosts
Host.Configuration.Firmware	Allows updates to the ESXi host's firmware.	Hosts
Host.Configuration.Hyperthreading	Allows enabling and disabling hyperthreading in a host CPU scheduler.	Hosts
Host.Configuration.Image configuration	Allows changes to the image associated with a host.	
Host.Configuration.Maintenance	Allows putting the host in and out of maintenance mode and shutting down and restarting the host.	Hosts
Host.Configuration.Memory configuration	Allows modifications to the host configuration.	Hosts
Host.Configuration.Network configuration	Allows configuration of network, firewall, and vMotion network.	Hosts
Host.Configuration.Power	Allows configuration of host power management settings.	Hosts
Host.Configuration.Query patch	Allows querying for installable patches and installing patches on the host.	Hosts
Host.Configuration.Security profile and firewall	Allows configuration of Internet services, such as SSH, Telnet, SNMP, and of the host firewall.	Hosts
Host.Configuration.Storage partition configuration	Allows VMFS datastore and diagnostic partition management. Users with this privilege can scan for new storage devices and manage iSCSI.	Hosts
Host.Configuration.System Management	Allows extensions to manipulate the file system on the host.	Hosts

Table 10-13. Host Configuration Privileges (Continued)

Privilege Name	Description	Required On
Host.Configuration.System resources	Allows updates to the configuration of the system resource hierarchy.	Hosts
Host.Configuration.Virtual machine autostart configuration	Allows changes to the auto-start and auto-stop order of virtual machines on a single host.	Hosts

Host Inventory

Host inventory privileges control adding hosts to the inventory, adding hosts to clusters, and moving hosts in the inventory.

The table describes the privileges required to add and move hosts and clusters in the inventory.

You can set this privilege at different levels in the hierarchy. For example, if you set a privilege at the folder level, you can propagate the privilege to one or more objects within the folder. The object listed in the Required On column must have the privilege set, either directly or inherited.

Table 10-14. Host Inventory Privileges

Privilege Name	Description	Required On
Host.Inventory.Add host to cluster	Allows addition of a host to an existing cluster.	Clusters
Host.Inventory.Add standalone host	Allows addition of a standalone host.	Host folders
Host.Inventory.Create cluster	Allows creation of a new cluster.	Host folders
Host.Inventory.Modify cluster	Allows changing the properties of a cluster.	Clusters
Host.Inventory.Move cluster or standalone host	Allows moving a cluster or standalone host between folders. Privilege must be present at both the source and destination.	Clusters
Host.Inventory.Move host	Allows moving a set of existing hosts into or out of a cluster. Privilege must be present at both the source and destination.	Clusters
Host.Inventory.Remove cluster	Allows deletion of a cluster or standalone host. To have permission to perform this operation, a user or group must have this privilege assigned in both the object and its parent object.	Clusters, Hosts
Host.Inventory.Remove host	Allows removal of a host. To have permission to perform this operation, a user or group must have this privilege assigned in both the object and its parent object.	Hosts plus parent object
Host.Inventory.Rename cluster	Allows renaming a a cluster.	Clusters

Host Local Operations Privileges

Host local operations privileges control actions performed when the vSphere Client is connected directly to a host.

You can set this privilege at different levels in the hierarchy. For example, if you set a privilege at the folder level, you can propagate the privilege to one or more objects within the folder. The object listed in the Required On column must have the privilege set, either directly or inherited.

Table 10-15. Host Local Operations Privileges

Privilege Name	Description	Required On
Host.Local operations.Add host to vCenter	Allows installation and removal of vCenter agents, such as vpxa and aam, on a host.	Root host
Host.Local operations.Create virtual machine	Allows creation of a new virtual machine from scratch on a disk without registering it on the host.	Root host
Host.Local operations.Delete virtual machine	Allows deletion of a virtual machine on disk. Supported for registered and unregistered virtual machines.	Root host
Host.Local operations.Extract NVRAM content	Allows extraction of the NVRAM content of a host.	
Host.Local operations.Manage user groups	Allows management of local accounts on a host.	Root host
Host.Local operations.Reconfigure virtual machine	Allows reconfiguring a virtual machine.	Root host
Host.Local operations.Relayout snapshots	Allows changes to the layout of a virtual machine's snapshots.	Root host

Host vSphere Replication Privileges

Host vSphere replication privileges control the use of virtual machine replication by VMware vCenter Site Recovery Manager™ for a host.

You can set this privilege at different levels in the hierarchy. For example, if you set a privilege at the folder level, you can propagate the privilege to one or more objects within the folder. The object listed in the Required On column must have the privilege set, either directly or inherited.

Table 10-16. Host vSphere Replication Privileges

Privilege Name	Description	Required On
Host.vSphere Replication.Manage Replication	Allows management of virtual machine replication on this host.	Hosts

Host Profile Privileges

Host Profile privileges control operations related to creating and modifying host profiles.

You can set this privilege at different levels in the hierarchy. For example, if you set a privilege at the folder level, you can propagate the privilege to one or more objects within the folder. The object listed in the Required On column must have the privilege set, either directly or inherited.

Table 10-17. Host Profile Privileges

Privilege Name	Description	Required On
Host profile.Clear	Allows clearing of profile related information.	Root vCenter Server
Host profile.Create	Allows creation of a host profile.	Root vCenter Server
Host profile.Delete	Allows deletion of a host profile.	Root vCenter Server
Host profile.Edit	Allows editing a host profile.	Root vCenter Server

Table 10-17. Host Profile Privileges (Continued)

Privilege Name	Description	Required On
Host profile.Export	Allows exporting a host profile	Root vCenter Server
Host profile.View	Allows viewing a host profile.	Root vCenter Server

Inventory Service Provider Privileges

Inventory Service Provider privileges are internal only. Do not use.

Inventory Service Tagging Privileges

Inventory Service Tagging privileges control the ability to create and delete tags and tag categories, and assign and remove tags on vSphere inventory objects.

You can set this privilege at different levels in the hierarchy. For example, if you set a privilege at the folder level, you can propagate the privilege to one or more objects within the folder. The object listed in the Required On column must have the privilege set, either directly or inherited.

Table 10-18. vCenter Inventory Service Privileges

Privilege Name	Description	Required On
Inventory Service.vSphere Tagging.Assign or Unassign vSphere Tag	Allows assignment or unassignment of a tag for an object in the vCenter Server inventory.	Any object
Inventory Service.vSphere Tagging.Create vSphere Tag	Allows creation of a tag.	Any object
Inventory Service.vSphere Tagging.Create vSphere Tag Category	Allows creation of a tag category.	Any object
Inventory Service.vSphere Tagging.Create vSphere Tag Scope	Allows creation of a tag scope.	Any object
Inventory Service.vSphere Tagging.Delete vSphere Tag	Allows deletion of a tag category.	Any object
Inventory Service.vSphere Tagging.Delete vSphere Tag Category	Allows deletion of a tag category..	Any object
Inventory Service.vSphere Tagging.Delete vSphere Tag Scope	Allows deletion of a tag scope.	Any object
Inventory Service.vSphere Tagging.Edit vSphere Tag	Allows editing of a tag.	Any object
Inventory Service.vSphere Tagging.Edit vSphere Tag Category	Allows editing of a tag category.	Any object
Inventory Service.vSphere Tagging.Edit vSphere Tag Scope	Allows editing of a tag scope.	Any object
Inventory Service.vSphere Tagging.Modify UsedBy Field for Category	Allows changing the UsedBy field for a tag category.	Any object
Inventory Service.vSphere Tagging.Modify UsedBy Field for Tag	Allows changing the UsedBy field for a tag.	Any object

Network Privileges

Network privileges control tasks related to network management.

You can set this privilege at different levels in the hierarchy. For example, if you set a privilege at the folder level, you can propagate the privilege to one or more objects within the folder. The object listed in the Required On column must have the privilege set, either directly or inherited.

Table 10-19. Network Privileges

Privilege Name	Description	Required On
Network.Assign network	Allows assigning a network to a virtual machine.	Networks, Virtual Machines
Network.Configure	Allows configuring a network.	Networks, Virtual Machines
Network.Move network	Allows moving a network between folders. Privilege must be present at both the source and destination.	Networks
Network.Remove	Allows removal of a network. This privilege is deprecated. To have permission to perform this operation, a user or group must have this privilege assigned in both the object and its parent object.	Networks

Performance Privileges

Performance privileges control modifying performance statistics settings.

You can set this privilege at different levels in the hierarchy. For example, if you set a privilege at the folder level, you can propagate the privilege to one or more objects within the folder. The object listed in the Required On column must have the privilege set, either directly or inherited.

Table 10-20. Performance Privileges

Privilege Name	Description	Required On
Performance.Modify intervals	Allows creating, removing, and updating performance data collection intervals.	Root vCenter Server

Permissions Privileges

Permissions privileges control the assigning of roles and permissions.

You can set this privilege at different levels in the hierarchy. For example, if you set a privilege at the folder level, you can propagate the privilege to one or more objects within the folder. The object listed in the Required On column must have the privilege set, either directly or inherited.

Table 10-21. Permissions Privileges

Privilege Name	Description	Required On
Permissions.Modify permission	Allows defining one or more permission rules on an entity, or updating rules if rules are already present for the given user or group on the entity. To have permission to perform this operation, a user or group must have this privilege assigned in both the object and its parent object.	Any object plus parent object
Permissions.Modify privilege	Allows modifying a privilege's group or description. No vSphere Web Client user interface elements are associated with this privilege.	

Table 10-21. Permissions Privileges (Continued)

Privilege Name	Description	Required On
Permissions.Modify role	Allows updating a role's name and the privileges that are associated with the role.	Any object
Permissions.Reassign role permissions	Allows reassigning all permissions of a role to another role.	Any object

Profile-driven Storage Privileges

Profile-driven storage privileges control operations related to storage profiles.

You can set this privilege at different levels in the hierarchy. For example, if you set a privilege at the folder level, you can propagate the privilege to one or more objects within the folder. The object listed in the Required On column must have the privilege set, either directly or inherited.

Table 10-22. Profile-driven Storage Privileges

Privilege Name	Description	Required On
Profile-driven storage.Profile-driven storage update	Allows changes to be made to storage profiles, such as creating and updating storage capabilities and virtual machine storage profiles.	Root vCenter Server
Profile-driven storage.Profile-driven storage view	Allows viewing of defined storage capabilities and storage profiles.	Root vCenter Server

Resource Privileges

Resource privileges control the creation and management of resource pools, as well as the migration of virtual machines.

You can set this privilege at different levels in the hierarchy. For example, if you set a privilege at the folder level, you can propagate the privilege to one or more objects within the folder. The object listed in the Required On column must have the privilege set, either directly or inherited.

Table 10-23. Resource Privileges

Privilege Name	Description	Required On
Resource.Apply recommendation	Allows accepting a suggestion by the server to perform a migration with vMotion.	Clusters
Resource.Assign vApp to resource pool	Allows assignment of a vApp to a resource pool.	Resource pools
Resource.Assign virtual machine to resource pool	Allows assignment of a virtual machine to a resource pool.	Resource pools
Resource.Create resource pool	Allows creation of resource pools.	Resource pools, clusters
Resource.Migrate	Allows cold migration of a virtual machine's execution to a specific resource pool or host.	Virtual machines
Resource.Migrate powered off virtual machine	Allows migration of a powered off virtual machine to a different resource pool or host.	Virtual machines
Resource.Migrate powered on virtual machine	Allows migration with vMotion of a powered on virtual machine to a different resource pool or host.	
Resource.Modify resource pool	Allows changes to the allocations of a resource pool.	Resource pools
Resource.Move resource pool	Allows moving a resource pool. Privilege must be present at both the source and destination.	Resource pools

Table 10-23. Resource Privileges (Continued)

Privilege Name	Description	Required On
Resource.Query vMotion	Allows querying the general vMotion compatibility of a virtual machine with a set of hosts.	Root vCenter Server
Resource.Remove resource pool	Allows deletion of a resource pool. To have permission to perform this operation, a user or group must have this privilege assigned in both the object and its parent object.	Resource pools
Resource.Rename resource pool	Allows renaming of a resource pool.	Resource pools

Scheduled Task Privileges

Scheduled task privileges control creation, editing, and removal of scheduled tasks.

You can set this privilege at different levels in the hierarchy. For example, if you set a privilege at the folder level, you can propagate the privilege to one or more objects within the folder. The object listed in the Required On column must have the privilege set, either directly or inherited.

Table 10-24. Scheduled Task Privileges

Privilege Name	Description	Required On
Scheduled task.Create tasks	Allows scheduling of a task. Required in addition to the privileges to perform the scheduled action at the time of scheduling.	Any object
Scheduled task.Modify task	Allows reconfiguration of the scheduled task properties.	Any object
Scheduled task.Remove task	Allows removal of a scheduled task from the queue.	Any object
Scheduled task.Run task	Allows running the scheduled task immediately. Creating and running a scheduled task also requires permission to perform the associated action.	Any object

Sessions Privileges

Sessions privileges control the ability of extensions to open sessions on the vCenter Server system.

You can set this privilege at different levels in the hierarchy. For example, if you set a privilege at the folder level, you can propagate the privilege to one or more objects within the folder. The object listed in the Required On column must have the privilege set, either directly or inherited.

Table 10-25. Session Privileges

Privilege Name	Description	Required On
Sessions.Impersonate user	Allow impersonation of another user. This capability is used by extensions.	Root vCenter Server
Sessions.Message	Allow setting of the global log in message.	Root vCenter Server
Sessions.Validate session	Allow verification of session validity.	Root vCenter Server
Sessions.View and stop sessions	Allow viewing sessions and forcing log out of one or more logged-on users.	Root vCenter Server

Storage Views Privileges

Storage Views privileges control privileges for Storage Monitoring Service APIs. Starting with vSphere 6.0, storage views are deprecated and these privileges no longer apply to them.

You can set this privilege at different levels in the hierarchy. For example, if you set a privilege at the folder level, you can propagate the privilege to one or more objects within the folder. The object listed in the Required On column must have the privilege set, either directly or inherited.

Table 10-26. Storage Views Privileges

Privilege Name	Description	Required On
Storage views.Configure service	Allows privileged users to use all Storage Monitoring Service APIs. Use **Storage views.View** for privileges to read-only Storage Monitoring Service APIs.	Root vCenter Server
Storage views.View	Allows privileged users to use read-only Storage Monitoring Service APIs.	Root vCenter Server

Tasks Privileges

Tasks privileges control the ability of extensions to create and update tasks on the vCenter Server.

You can set this privilege at different levels in the hierarchy. For example, if you set a privilege at the folder level, you can propagate the privilege to one or more objects within the folder. The object listed in the Required On column must have the privilege set, either directly or inherited.

Table 10-27. Tasks Privileges

Privilege Name	Description	Required On
Tasks.Create task	Allows an extension to create a user-defined task. No vSphere Web Client user interface elements are associated with this privilege.	Root vCenter Server
Tasks.Update task	Allows an extension to updates a user-defined task. No vSphere Web Client user interface elements are associated with this privilege.	Root vCenter Server

Transfer Service Privileges

Transfer service privileges are VMware internal. Do not use these privileges.

VRM Policy Privileges

VRM policy privileges are VMware internal. Do not use these privileges.

Virtual Machine Configuration Privileges

Virtual Machine Configuration privileges control the ability to configure virtual machine options and devices.

You can set this privilege at different levels in the hierarchy. For example, if you set a privilege at the folder level, you can propagate the privilege to one or more objects within the folder. The object listed in the Required On column must have the privilege set, either directly or inherited.

Table 10-28. Virtual Machine Configuration Privileges

Privilege Name	Description	Required On
Virtual machine.Configuration.Add existing disk	Allows adding an existing virtual disk to a virtual machine.	Virtual machines
Virtual machine.Configuration.Add new disk	Allows creation of a new virtual disk to add to a virtual machine.	Virtual machines
Virtual machine.Configuration.Add or remove device	Allows addition or removal of any non-disk device.	Virtual machines
Virtual machine.Configuration.Advanced	Allows addition or modification of advanced parameters in the virtual machine's configuration file.	Virtual machines
Virtual machine.Configuration.Change CPU count	Allows changing the number of virtual CPUs.	Virtual machines
Virtual machine.Configuration.Change resource	Allows changing the resource configuration of a set of virtual machine nodes in a given resource pool.	Virtual machines
Virtual machine.Configuration.Configure managedBy	Allows an extension or solution to mark a virtual machine as being managed by that extension or solution.	Virtual machines
Virtual machine.Configuration.Disk change tracking	Allows enabling or disabling of change tracking for the virtual machine's disks.	Virtual machines
Virtual machine.Configuration.Disk lease	Allows disk lease operations for a virtual machine.	Virtual machines
Virtual machine.Configuration.Display connection settings	Allows configuration of virtual machine remote console options.	Virtual machines
Virtual machine.Configuration.Extend virtual disk	Allows expansion of the size of a virtual disk.	Virtual machines
Virtual machine.Configuration.Host USB device	Allows attaching a host-based USB device to a virtual machine.	Virtual machines
Virtual machine.Configuration.Memory	Allows changing the amount of memory allocated to the virtual machine.	Virtual machines
Virtual machine.Configuration.Modify device settings	Allows changing the properties of an existing device.	Virtual machines
Virtual machine.Configuration.Query Fault Tolerance compatibility	Allows checking if a virtual machine is compatible for Fault Tolerance.	Virtual machines
Virtual machine.Configuration.Query unowned files	Allows querying of unowned files.	Virtual machines

Table 10-28. Virtual Machine Configuration Privileges (Continued)

Privilege Name	Description	Required On
Virtual machine.Configuration.Raw device	Allows adding or removing a raw disk mapping or SCSI pass through device. Setting this parameter overrides any other privilege for modifying raw devices, including connection states.	Virtual machines
Virtual machine.Configuration.Reload from path	Allows changing a virtual machine configuration path while preserving the identity of the virtual machine. Solutions such as VMware vCenter Site Recovery Manager use this operation to maintain virtual machine identity during failover and failback.	Virtual machines
Virtual machine.Configuration.Remove disk	Allows removal of a virtual disk device.	Virtual machines
Virtual machine.Configuration.Rename	Allows renaming a virtual machine or modifying the associated notes of a virtual machine.	Virtual machines
Virtual machine.Configuration.Reset guest information	Allows editing the guest operating system information for a virtual machine.	Virtual machines
Virtual machine.Configuration.Set annotation	Allows adding or editing a virtual machine annotation.	Virtual machines
Virtual machine.Configuration.Settings	Allows changing general virtual machine settings.	Virtual machines
Virtual machine.Configuration.Swapfile placement	Allows changing the swapfile placement policy for a virtual machine.	Virtual machines
Virtual machine.Configuration.Unlock virtual machine	Allows decrypting a virtual machine.	Virtual machines
Virtual machine.Configuration.Upgrade virtual machine compatibility	Allows upgrade of the virtual machine's virtual machine compatibility version.	Virtual machines

Virtual Machine Guest Operations Privileges

Virtual Machine Guest Operations privileges control the ability to interact with files and programs inside a virtual machine's guest operating system with the API.

See the *VMware vSphere API Reference* documentation for more information on these operations.

You can set this privilege at different levels in the hierarchy. For example, if you set a privilege at the folder level, you can propagate the privilege to one or more objects within the folder. The object listed in the Required On column must have the privilege set, either directly or inherited.

Table 10-29. Virtual Machine Guest Operations

Privilege Name	Description	Effective on Object
Virtual machine.Guest Operations.Guest Operation Alias modification	Allows virtual machine guest operations that involve modifying the alias for the virtual machine.	Virtual machines
Virtual machine.Guest Operations.Guest Operation Alias query	Allows virtual machine guest operations that involve querying the alias for the virtual machine.	Virtual machines

Table 10-29. Virtual Machine Guest Operations (Continued)

Privilege Name	Description	Effective on Object
Virtual machine.Guest Operations.Guest Operation Modifications	Allows virtual machine guest operations that involve modifications to a guest operating system in a virtual machine, such as transferring a file to the virtual machine. No vSphere Web Client user interface elements are associated with this privilege.	Virtual machines
Virtual machine.Guest Operations.Guest Operation Program Execution	Allows virtual machine guest operations that involve executing a program in the virtual machine. No vSphere Web Client user interface elements are associated with this privilege.	Virtual machines
Virtual machine.Guest Operations.Guest Operation Queries	Allows virtual machine guest operations that involve querying the guest operating system, such as listing files in the guest operating system. No vSphere Web Client user interface elements are associated with this privilege.	Virtual machines

Virtual Machine Interaction Privileges

Virtual Machine Interaction privileges control the ability to interact with a virtual machine console, configure media, perform power operations, and install VMware Tools.

You can set this privilege at different levels in the hierarchy. For example, if you set a privilege at the folder level, you can propagate the privilege to one or more objects within the folder. The object listed in the Required On column must have the privilege set, either directly or inherited.

Table 10-30. Virtual Machine Interaction

Privilege Name	Description	Required On
Virtual machine.Interaction.Answer question	Allows resolution of issues with virtual machine state transitions or runtime errors.	Virtual machines
Virtual machine.Interaction.Backup operation on virtual machine	Allows performance of backup operations on virtual machines.	Virtual machines
Virtual machine.Interaction.Configure CD media	Allows configuration of a virtual DVD or CD-ROM device.	Virtual machines
Virtual machine.Interaction.Configure floppy media	Allows configuration of a virtual floppy device.	Virtual machines
Virtual machine.Interaction.Console interaction	Allows interaction with the virtual machine's virtual mouse, keyboard, and screen.	Virtual machines
Virtual machine.Interaction.Create screenshot	Allows creation of a virtual machine screen shot.	Virtual machines
Virtual machine.Interaction.Defragment all disks	Allows defragment operations on all disks of the virtual machine.	Virtual machines
Virtual machine.Interaction.Device connection	Allows changing the connected state of a virtual machine's disconnectable virtual devices.	Virtual machines

Table 10-30. Virtual Machine Interaction (Continued)

Privilege Name	Description	Required On
Virtual machine.Interaction.Disable Fault Tolerance	Allows disabling the Secondary virtual machine for a virtual machine using Fault Tolerance.	Virtual machines
Virtual machine.Interaction.Drag and Drop	Allows drag and drop of files between a virtual machine and a remote client.	Virtual machines
Virtual machine.Interaction.Enable Fault Tolerance	Allows enabling the Secondary virtual machine for a virtual machine using Fault Tolerance.	Virtual machines
Virtual machine.Interaction.Guest operating system management by VIX API	Allows management of the virtual machine's operating system through the VIX API.	Virtual machines
Virtual machine.Interaction.Inject USP HID scan codes	Allows injection of USP HID scan codes.	Virtual machines
Virtual machine.Interaction.Pause/Unpause	Allows pausing or unpausing of the virtual machine.	Virtual machines
Virtual machine.Interaction.Perform wipe or shrink operations	Allows performing wipe or shrink operations on the virtual machine.	Virtual machines
Virtual machine.Interaction.Power Off	Allows powering off a powered-on virtual machine. This operation powers down the guest operating system.	Virtual machines
Virtual machine.Interaction.Power On	Allows powering on a powered-off virtual machine, and resuming a suspended virtual machine.	Virtual machines
Virtual machine.Interaction.Record session on Virtual Machine	Allows recording a session on a virtual machine.	Virtual machines
Virtual machine.Interaction.Replay session on Virtual Machine	Allows replaying of a recorded session on a virtual machine.	Virtual machines
Virtual machine.Interaction.Reset	Allows resetting of a virtual machine and reboots the guest operating system.	Virtual machines
Virtual machine.Interaction.Suspend	Allows suspending a powered-on virtual machine. This operation puts the guest in standby mode.	Virtual machines
Virtual machine.Interaction.Test failover	Allows testing of Fault Tolerance failover by making the Secondary virtual machine the Primary virtual machine.	Virtual machines
Virtual machine.Interaction.Test restart Secondary VM	Allows termination of a Secondary virtual machine for a virtual machine using Fault Tolerance.	Virtual machines
Virtual machine.Interaction.Turn Off Fault Tolerance	Allows turning off Fault Tolerance for a virtual machine.	Virtual machines

Table 10-30. Virtual Machine Interaction (Continued)

Privilege Name	Description	Required On
Virtual machine.Interaction.Turn On Fault Tolerance	Allows turning on Fault Tolerance for a virtual machine.	Virtual machines
Virtual machine.Interaction.VMware Tools install	Allows mounting and unmounting the VMware Tools CD installer as a CD-ROM for the guest operating system.	Virtual machines

Virtual Machine Inventory Privileges

Virtual Machine Inventory privileges control adding, moving, and removing virtual machines.

You can set this privilege at different levels in the hierarchy. For example, if you set a privilege at the folder level, you can propagate the privilege to one or more objects within the folder. The object listed in the Required On column must have the privilege set, either directly or inherited.

Table 10-31. Virtual Machine Inventory Privileges

Privilege Name	Description	Required On
Virtual machine .Inventory.Create from existing	Allows creation of a virtual machine based on an existing virtual machine or template, by cloning or deploying from a template.	Clusters, Hosts, Virtual machine folders
Virtual machine.Inventory.Create new	Allows creation of a virtual machine and allocation of resources for its execution.	Clusters, Hosts, Virtual machine folders
Virtual machine.Inventory.Move	Allows relocating a virtual machine in the hierarchy. The privilege must be present at both the source and destination.	Virtual machines
Virtual machine.Inventory.Register	Allows adding an existing virtual machine to a vCenter Server or host inventory.	Clusters, Hosts, Virtual machine folders
Virtual machine.Inventory.Remove	Allows deletion of a virtual machine. Deletion removes the virtual machine's underlying files from disk. To have permission to perform this operation, a user or group must have this privilege assigned in both the object and its parent object.	Virtual machines
Virtual machine.Inventory.Unregister	Allows unregistering a virtual machine from a vCenter Server or host inventory. To have permission to perform this operation, a user or group must have this privilege assigned in both the object and its parent object.	Virtual machines

Virtual Machine Provisioning Privileges

Virtual Machine Provisioning privileges control activities related to deploying and customizing virtual machines.

You can set this privilege at different levels in the hierarchy. For example, if you set a privilege at the folder level, you can propagate the privilege to one or more objects within the folder. The object listed in the Required On column must have the privilege set, either directly or inherited.

Table 10-32. Virtual Machine Provisioning Privileges

Privilege Name	Description	Required On
Virtual machine.Provisioning.Allow disk access	Allows opening a disk on a virtual machine for random read and write access. Used mostly for remote disk mounting.	Virtual machines
Virtual machine.Provisioning.Allow read-only disk access	Allows opening a disk on a virtual machine for random read access. Used mostly for remote disk mounting.	Virtual machines
Virtual machine.Provisioning.Allow virtual machine download	Allows read operations on files associated with a virtual machine, including vmx, disks, logs, and nvram.	Root host or vCenter Server
Virtual machine.Provisioning.Allow virtual machine files upload	Allows write operations on files associated with a virtual machine, including vmx, disks, logs, and nvram.	Root host or vCenter Server
Virtual machine.Provisioning.Clone template	Allows cloning of a template.	Templates
Virtual machine.Provisioning.Clone virtual machine	Allows cloning of an existing virtual machine and allocation of resources.	Virtual machines
Virtual machine.Provisioning.Create template from virtual machine	Allows creation of a new template from a virtual machine.	Virtual machines
Virtual machine.Provisioning.Customize	Allows customization of a virtual machine's guest operating system without moving the virtual machine.	Virtual machines
Virtual machine.Provisioning.Deploy template	Allows deployment of a virtual machine from a template.	Templates
Virtual machine.Provisioning.Mark as template	Allows marking an existing powered off virtual machine as a template.	Virtual machines
Virtual machine.Provisioning.Mark as virtual machine	Allows marking an existing template as a virtual machine.	Templates
Virtual machine.Provisioning.Modify customization specification	Allows creation, modification, or deletion of customization specifications.	Root vCenter Server
Virtual machine.Provisioning.Promote disks	Allows promote operations on a virtual machine's disks.	Virtual machines
Virtual machine.Provisioning.Read customization specifications	Allows reading a customization specification.	Virtual machines

Virtual Machine Service Configuration Privileges

Virtual machine service configuration privileges control who can perform monitoring and management task on service configuration.

You can set this privilege at different levels in the hierarchy. For example, if you set a privilege at the folder level, you can propagate the privilege to one or more objects within the folder. The object listed in the Required On column must have the privilege set, either directly or inherited.

NOTE In vSphere 6.0, do not assign or remove this privilege by using the vSphere Web Client.

Table 10-33. Virtual machine Service Configuration Privileges

Privilege Name	Description
Virtual Machine. Service configuration. Allow notifications	Allows generating and consuming notification about service status.
Virtual Machine. Service configuration. Allow polling of global event notifications	Allows querying whether any notifications are present.
Virtual Machine. Service configuration. Manage service configurations	Allows creating, modifying, and deleting virtual machine services.
Virtual Machine. Service configuration. Modify service configuration	Allows modification of existing virtual machine service configuration.
Virtual Machine. Service configuration. Query service configurations	Allows retrieval of list of virtual machine services.
Virtual Machine. Service configuration. Read service configuration	Allows retrieval of existing virtual machine service configuration.

Virtual Machine Snapshot Management Privileges

Virtual machine snapshot management privileges control the ability to take, delete, rename, and restore snapshots.

You can set this privilege at different levels in the hierarchy. For example, if you set a privilege at the folder level, you can propagate the privilege to one or more objects within the folder. The object listed in the Required On column must have the privilege set, either directly or inherited.

Table 10-34. Virtual Machine State Privileges

Privilege Name	Description	Required On
Virtual machine.Snapshot management. Create snapshot	Allows creation of a snapshot from the virtual machine's current state.	Virtual machines
Virtual machine.Snapshot management.Remove Snapshot	Allows removal of a snapshot from the snapshot history.	Virtual machines

Table 10-34. Virtual Machine State Privileges (Continued)

Privilege Name	Description	Required On
Virtual machine.Snapshot management.Rename Snapshot	Allows renaming a snapshot with a new name, a new description, or both.	Virtual machines
Virtual machine.Snapshot management.Revert to snapshot	Allows setting the virtual machine to the state it was in at a given snapshot.	Virtual machines

Virtual Machine vSphere Replication Privileges

Virtual Machine vSphere replication privileges control the use of replication by VMware vCenter Site Recovery Manager™ for virtual machines.

You can set this privilege at different levels in the hierarchy. For example, if you set a privilege at the folder level, you can propagate the privilege to one or more objects within the folder. The object listed in the Required On column must have the privilege set, either directly or inherited.

Table 10-35. Virtual Machine vSphere Replication

Privilege Name	Description	Required On
Virtual machine.vSphere Replication.Configure Replication	Allows configuration of replication for the virtual machine.	Virtual machines
Virtual machine.vSphere Replication.Manage Replication	Allows triggering of full sync, online sync or offline sync on a replication.	Virtual machines
Virtual machine.vSphere Replication.Monitor Replication	Allows monitoring of replication.	Virtual machines

dvPort Group Privileges

Distributed virtual port group privileges control the ability to create, delete, and modify distributed virtual port groups.

The table describes the privileges required to create and configure distributed virtual port groups.

You can set this privilege at different levels in the hierarchy. For example, if you set a privilege at the folder level, you can propagate the privilege to one or more objects within the folder. The object listed in the Required On column must have the privilege set, either directly or inherited.

Table 10-36. Distributed Virtual Port Group Privileges

Privilege Name	Description	Required On
dvPort group.Create	Allows creation of a distributed virtual port group.	Virtual port groups
dvPort group.Delete	Allows deletion of distributed virtual port group. To have permission to perform this operation, a user or group must have this privilege assigned in both the object and its parent object.	Virtual port groups
dvPort group.Modify	Allows modification of a distributed virtual port group configuration.	Virtual port groups
dvPort group.Policy operation	Allows setting the policy of a distributed virtual port group.	Virtual port groups
dvPort group.Scope operation	Allows setting the scope of a distributed virtual port group.	Virtual port groups

vApp Privileges

vApp privileges control operations related to deploying and configuring a vApp.

You can set this privilege at different levels in the hierarchy. For example, if you set a privilege at the folder level, you can propagate the privilege to one or more objects within the folder. The object listed in the Required On column must have the privilege set, either directly or inherited.

Table 10-37. vApp Privileges

Privilege Name	Description	Required On
vApp.Add virtual machine	Allows adding a virtual machine to a vApp.	vApps
vApp.Assign resource pool	Allows assigning a resource pool to a vApp.	vApps
vApp.Assign vApp	Allows assigning a vApp to another vApp	vApps
vApp.Clone	Allows cloning of a vApp.	vApps
vApp.Create	Allows creation of a vApp.	vApps
vApp.Delete	Allows deletion a vApp. To have permission to perform this operation, a user or group must have this privilege assigned in both the object and its parent object.	vApps
vApp.Export	Allows export of a vApp from vSphere.	vApps
vApp.Import	Allows import of a vApp into vSphere.	vApps
vApp.Move	Allows moving a vApp to a new inventory location.	vApps
vApp.Power Off	Allows power off operations on a vApp.	vApps
vApp.Power On	Allows power on operations on a vApp.	vApps
vApp.Rename	Allows renaming a vApp.	vApps
vApp.Suspend	Allows suspension of a vApp.	vApps
vApp.Unregister	Allows unregistering a vApp. To have permission to perform this operation, a user or group must have this privilege assigned in both the object and its parent object.	vApps
vApp.View OVF Environment	Allows viewing the OVF environment of a powered-on virtual machine within a vApp.	vApps
vApp.vApp application configuration	Allows modification of a vApp's internal structure, such as product information and properties.	vApps
vApp.vApp instance configuration	Allows modification of a vApp's instance configuration, such as policies.	vApps
vApp.vApp managedBy configuration	Allows an extension or solution to mark a vApp as being managed by that extension or solution. No vSphere Web Client user interface elements are associated with this privilege.	vApps
vApp.vApp resource configuration	Allows modification of a vApp's resource configuration. To have permission to perform this operation, a user or group must have this privilege assigned in both the object and its parent object.	vApps

vServices Privileges

vServices privileges control the ability to create, configure, and update vService dependencies for virtual machines and vApps.

You can set this privilege at different levels in the hierarchy. For example, if you set a privilege at the folder level, you can propagate the privilege to one or more objects within the folder. The object listed in the Required On column must have the privilege set, either directly or inherited.

Table 10-38. vServices

Privilege Name	Description	Required On
vService.Create dependency	Allows creation of a vService dependency for a virtual machine or vApp.	vApps and virtual machines
vService.Destroy dependency	Allows removal of a vService dependency for a virtual machine or vApp.	vApps and virtual machines
vService.Reconfigure dependency configuration	Allows reconfiguration of a dependency to update the provider or binding.	vApps and virtual machines
vService.Update dependency	Allows updates of a dependence to configure the name or description.	vApps and virtual machines

Index

Numerics

3D features **200**
3rd party root certificate **79, 89, 95**

A

access, privileges **233**
Active Directory **166–168, 170, 172**
Active Directory domain, authentication with vCenter Server Appliance **47**
Active Directory identity source **32**
Active Directory LDAP Server identity source **33**
Administrator role **125**
administrator user, setting for vCenter Server **22**
alarms, privileges **234**
allowed IP addresses, firewall **151**
anti-spyware **14**
antivirus software, installing **197**
assign global permissions **123**
authenticating, vSphere Authentication Proxy **171**
authentication
  iSCSI storage **228**
  smart card **173, 174**
  with Active Directory domain **47**
authentication proxy **166, 170, 172**
authentication proxy server **171, 172**
authorization **113, 114**
authorized keys, disabling **137**
Auto Deploy
  privileges **235**
  security **182**
  vSphere Authentication Proxy **169**
availability timeout for the ESXi Shell **180**

B

back up ESXi certificates **149**
best practices
  permissions **127**
  roles **127**
  security **225**

C

CA-signed certificates **146**
CAM server **171**
CAM service **170**
categories, privileges **244**
certificate authority **56**
certificate details **142**
certificate expiration **140**
certificate information **140**
Certificate Manager, CSRs **69**
certificate replacement
  large deployments **61**
  SSO HA **61**
  stopping services **70**
certificate requests, generating **71, 80, 82**
certificate signing request **69**
certificate management **52**
certificate management tools **96**
certificate replacement options **53**
certificates
  checking **191**
  disabling SSL for vSphere SDK **181**
  expiration warning **111**
  expired **189**
  generate certificates **56**
  host upgrades **139**
  privilege **235**
  refresh STS for vCenter Single Sign-On **36**
  revoked **189**
  uploading **147**
  VMCA root certificates **80**
certificates; replace machine SSL certificate **92**
certool **98**
certool --rootca **70**
certool configuration options **97**
certool management commands **101**
certool.cfg file **97**
CIM tool access, limiting **193**
content library, privileges **236**
copy and paste
  disabled for guest operating systems **201**
  guest operating systems **202**
  virtual machines **202**
CSR **69**
custom certificates
  auto deploy **148**
  ESXi **147**
custom roles **123**

D

datastore clusters, privileges **238**
datastores, privileges **237**
dcui **166**
DCUI Access **162**
dcui user privileges, dcui **166**
DCUI.Access **162**
DCUI.Access advanced system setting **162**
default domain **29**
default domains, vCenter Single Sign-On **30**
default certificates, replacing with CA-signed certificates **146**
delete identity source **35**
delete Single Sign-On users **42**
delete vCenter Single Sign-On users **42**
device disconnection, preventing in the vSphere Web Client **203**
dir-cli, certificate replacement **37**
Direct Console User Interface access **162**
Direct Console User Interface (DCUI) **162**
directory server, viewing **168**
directory service
  Active Directory **167**
  configuring a host **167**
disable remote operations in a virtual machine **202**
disable user, Single Sign-On **42**
disabling
  logging for guest operating systems **204**
  SSL for vSphere SDK **181**
  variable information size **203**
distributed switch **212**
distributed switches, permission **116**
Distributed Switches, privileges **238**
distributed virtual port group privileges **256**
DMZ **216**
DvFilter **222**

E

edit user, Single Sign-On **43**
ESX Agent Manager, privileges **239**
esxcli firewall **155**
ESXi
  log files **184**
  syslog service **183**
ESXi certificate details **141**
ESXi certificates
  replacing **145**
  restore **149**
ESXi certificates, backup **149**
ESXi certificates, default settings **139**
ESXi CSR requirements **145**
esxi custom certificate mode **144**
ESXi incoming firewall ports **152**
ESXi log files **182**
ESXi networking **136**
ESXi outgoing firewall ports **152**
ESXi passwords **16**
ESXi security best practices **185**
ESXi Shell
  configuring **177**
  direct connections **181**
  enabling **177, 178, 180**
  enabling with vSphere Web Client **178**
  logging in **181**
  remote connections **181**
  setting availability timeout **178**
  setting idle timeout **178**
  setting timeout **180**
  SSH connections **176**
  timeouts **179, 181**
esxi thumbprint certificate mode **144**
exception user list **157**
exit automation tool **164**
expiration warning, certificates **111**
expiration of certificate **37**
expired certificates **189**
extensions, privileges **239**

F

Fault Tolerance (FT)
  logging **184**
  security **184**
firewall
  commands **155**
  configuring **155**
  NFS client **154**
firewall ports
  configuring with vCenter Server **207**
  configuring without vCenter Server **208**
  connecting to vCenter Server **208**
  host to host **208**
  overview **206**
  vSphere Client direct connection **208**
  vSphere Web Client and vCenter Server **207**
firewall settings **151**
firewalls
  access for management agents **151**
  access for services **151**
floppy disks **199**
folders, privileges **239**
forged transmissions **211, 212**

G

generating CSRs **69**

generating certificate requests **71, 80, 82**
genselfcacert **70**
global permissions, assign **123**
global privileges **240**
groups
  add members **44**
  adding **43**
  local **43**
  searching **122**
guest operating systems
  copy and paste **202**
  disabling logging **204**
  enabling copy and paste **201**
  limiting variable information size **203**

H

hardening the vCenter Server Host OS **189**
hardware devices **199**
HGFS File Transfers **201**
host name, configuring **167**
host profiles, privileges **243, 246**
host upgrades and certificates **139**
host configuration with scripts **132**
host management privileges, user **166**
host security
  authorized keys **137**
  CIM tools **193**
  disabling MOB **137**
  logging **182**
  managed object browser **137**
  performance data **230**
  resource management **198**
  unsigned VIBs **163**
  using templates **197**
  virtual machine console **198**
  virtual disk shrinking **196**
host-to-host firewall ports **208**
hosts
  CIM privileges **240**
  configuration privileges **241**
  inventory privileges **242**
  local operations privileges **242**
  thumbprints **191**
  vSphere replication privileges **243**
HTTPS PUT, uploading certificates and keys **147, 177**
Hypervisor security **11**

I

identity source
  adding to vCenter Single Sign-On **31**
  editing for vCenter Single Sign-On **34**
identity sources for vCenter Single Sign-On **29**
idle session timeout **179, 181**
image profile privileges **235**
Image Builder security **163**
informational messages, limiting **195**
intermediate CA **65, 84**
Internet Protocol Security (IPsec) **218**
inventory service, privileges **244**
IP addresses, adding allowed **151**
IPsec, *See* Internet Protocol Security (IPsec)
iSCSI
  authentication **228**
  protecting transmitted data **228**
  QLogic iSCSI adapters **228**
  securing ports **228**
  security **228**
isolation
  standard switches **15**
  virtual networking layer **15**
  VLANs **15**

J

join domain **170**

K

keys
  authorized **176, 177**
  SSH **176, 177**
  uploading **147, 176, 177**

L

Linux-based clients, restricting use with vCenter Server **190**
load balancer **49**
lockdown mode
  behavior **159**
  catastrophic vCenter Server failure **162**
  DCUI access **162**
  DCUI.Access **162**
  different product versions **162**
  direct console user interface **161**
  enabling **160, 161**
  vSphere Web Client **160**
lockdown mode exception users **157**
lockdown mode, disable **161**
lockdown mode,vSphere 6.0 and later **163**
lockout policy, vCenter Single Sign-On **39**
log files
  ESXi **182, 184**
  locating **184**
logging
  disabling for guest operating systems **204**
  host security **182**
logs for failed installation **189**

Lookup Service error **46**
Lookup Service, *See* vCenter Lookup Service
Lotus replication **49**
LUN masking **229**

M

MAC address changes **211**
machine SSL certificate **66**
machine SSL certificates **72**
manage certificates **235**
managed entities, permissions **116**
managed object browser, disabling **137**
management access
  firewalls **151**
  TCP and UDP ports **192**
management interface
  securing **131**
  securing with VLANs and virtual switches **214**
management network **136**
managing Single Sign-On users **40**
manual certificate replacement **69**

N

Netflow **222**
network connectivity, limiting **189**
network isolation **224**
network file copy (NFC) **192**
network security **205**
networking security **222**
networks
  privileges **245**
  security **213**
NFC, enabling SSL **192**
NFS 4.1, Kerberos credentials **229**
NFS client, firewall rule set **154**
No Access role **125**
NTP **167**
NTP servers, adding **227**
NTP-based time synchronization **227**

O

OpenLDAP Server identity source **33**

P

password policies, vCenter Single Sign-On **38**
password policy **29**
password policy vCenter Server **188**
password requirements **28, 135**
passwords
  changing vCenter Single Sign-On **45**
  overview **16**
  vCenter Single Sign-On policies **38**
PCI devices **185**
PCIe devices **185**
performance, privileges **245**
performance data, disable sending **230**
permissions
  administrator **119**
  and privileges **119**
  assigning **120, 123, 173**
  best practices **127**
  changing **121**
  distributed switches **116**
  inheritance **116, 118, 119**
  overriding **118, 119**
  overview **119**
  privileges **245**
  removing **121**
  root user **119**
  settings **117**
  user **165**
  vpxuser **119**
plug-ins, privileges **239**
policies
  lockout in vCenter Single Sign-On **39**
  security **220**
  Single Sign-On **38, 40**
  vCenter Single Sign-On passwords **38**
portfast **222**
Portfast **222**
PowerCLI **14**
PowerCLI host management **132**
principals, remove from group **44**
privileges
  alarms **234**
  assigning **123**
  Auto Deploy **235**
  categories **244**
  certificate **235**
  certificate management **97**
  configuration **241**
  content library **236**
  datastore clusters **238**
  datastores **237**
  Distributed Switches **238**
  dvPort group **256**
  ESX Agent Manager **239**
  extension **239**
  folder **239**
  global **240**
  host CIM **240**
  host inventory **242**
  host local operations **242**
  host profiles **243, 246**
  host vSphere replication **243**

image profile **235**
inventory service **244**
network **245**
performance **245**
permission **245**
plug-ins **239**
resource **246**
scheduled tasks **247**
sessions **247**
storage views **248**
tags **244**
tasks **248**
Transfer Service **248**
vApps **257**
vCenter Inventory Service **244**
vCenter Server **187**
virtual machine **253**
virtual machine configuration **248**
virtual machine interaction **251**
virtual machine provisioning **253**
virtual machine guest operations **250**
virtual machine service configuration **255**
virtual machine snapshot management **255**
virtual machine vSphere replication **256**
VRM policy **248**
vServices **258**
privileges and permissions **119**
privileges, required, for common tasks **127**
promiscuous mode **211, 212**

R

Read Only role **125**
remote operations, disabling in virtual machine **202**
removing users from groups **44**
renew ESXi certificates **141**
replace machine SSL certificateValid **64**
replace solution user certificates **84**
replace VMCA root certificate **66**
replacing, default certificates **146**
replacing certificates manually **69**
replacing VMCA-signed certificates **72**
request certificates **91**
required privileges, for common tasks **127**
Reset All Certificates **68**
resources, privileges **246**
restore ESXi certificates **149**
restrict Guest Operations privileges **202**
restricting use of Linux-based clients with vCenter Server **190**
revert certificate management operation **68**
revoked certificates **189**
revoking certificates, securing **61**
roles
Administrator **125**
and permissions **125**
best practices **127**
creating **125, 126**
default **125**
No Access **125**
privileges, lists of **233**
Read Only **125**
removing **121**
security **125**
root certificates **80**
root login, permissions **119, 165**

S

SAML token **20**
sample roles **123**
SAN **229**
scheduled tasks, privileges **247**
SDK, firewall ports and virtual machine console **208**
search lists, adjusting for large domains **122**
securing networking **205**
securing vCenter Server Appliance **191**
security
best practices **225**
certification **17**
DMZ in single host **215, 216**
host **133**
iSCSI storage **228**
permissions **119**
standard switch ports **210, 211**
vCenter Server **13**
virtual machines with VLANs **213**
virtual networking layer **15**
virtualization layer **11**
VLAN hopping **214**
VMware policy **17**
security policies
available **220**
creating **220**
listing **220**
removing **221**
security profile **150, 156**
security token service (STS), vCenter Single Sign-On **36**
security and PCI devices **185**
security associations
adding **218**
available **218**

listing **218**
removing **219**
security policy **210**
security recommendations **157, 222**
Security Token Service **20, 22, 35**
services
stopping **70**
syslogd **183**
sessions, privileges **247**
shares limits, host security **198**
Single Sign-On
about **25**
benefits **20**
disabling users **42**
editing users **43**
effect on vCenter Server installation and upgrades **22**
login fails because user account is locked **48**
Lookup Service Error **46**
policies **38**
troubleshooting **46**
unable to log in using Active Directory domain **47**
upgrades **23**
Single Sign-On identity source, deleting **35**
Single Sign-On solution users **45**
smart card authentication
configuring **173**
disable **174**
enable **174**
fallback **175**
in lockdown mode **175**
SMS API privileges **248**
SNMP **221**
solution user sso handshake **20**
solution users **45**
solution user certificates **67, 75**
spanning **222**
SSH
ESXi Shell **176**
security settings **176**
SSH keys **175**
SSL
enable over NFC **192**
enabling and disabling **51**
encryption and certificates **51**
SSL certificate **37**
SSO, *See* Single Sign On *See* Single Sign-On
SSO HA **49**
SSO passwords **16**
SSPI **35**
standard switch ports, security **210, 211**
standard switch security **214**
standard switches
and iSCSI **228**
forged transmissions **211**
MAC address changes **211**
promiscuous mode **211**
storage, securing with VLANs and virtual switches **214**
Storage Monitoring Service API privileges **248**
storage views, privileges **248**
storage security best practices **228**
stp **210**
strict lockdown mode **157**
STS, *See* security token service (STS)
STS (Security Token Service) **22**
subordinate certificate **84**
switch **210**
synchronize ESXi clocks on vSphere network **225**
synchronizing clocks on the vSphere network **225**
syslog **183**

T

tags, privileges **244**
tasks, privileges **248**
TCP ports **192**
templates, host security **197**
third-party CA **91**
third-party certificates **90**
third-party root certificate **79, 89, 95**
third-party software support policy **17**
thumbprint certificates **139**
thumbprints, hosts **191**
time synchronization
NTP-based **227**
VMware Tools-based **226**
time synchronization settings **226**
timeout, ESXi Shell **179, 181**
timeout for ESXi Shell availability **180**
timeouts
ESXi Shell **178**
setting **178**
token policy, Single Sign-On **40**
TRUSTED_ROOTS **147**

U

UDP ports **192**
understanding passwords **16**
understanding Single Sign-On **20**
unexposed features, disable **200**
updated information **9**
updating trusts **93**
user management **113**

user permissions, vpxuser **165**
user account locked, SSO fails **48**
user directory timeout **122**
user repositories for vCenter Single Sign-On **29**
users
  adding local **41**
  disabling Single Sign-On **42**
  editing Single Sign-On **43**
  remove from group **44**
  searching **122**
users and groups **44**
users and permissions **113**
UserVars.ActiveDirectoryVerifyCAMCertifcate **171**

V

vApps, privileges **257**
variable information size for guest operating systems
  disabling **203**
  limiting **203**
vCenter Server
  connecting through firewall **208**
  firewall ports **207**
  privileges **187**
vCenter Inventory Service
  privileges **244**
  tagging **244**
vCenter Lookup Service **22**
vCenter Server security **187, 189**
vCenter Server Appliance
  adding NTP servers **227**
  NTP-based time synchronization **227**
  security best practices **191**
  time synchronization settings **226**
  unable to log in **47**
  VMware Tools-based time synchronization **226**
vCenter Server administrator user, setting **22**
vCenter Server Host OS, hardening **189**
vCenter Server security best practices **187**
vCenter Sever Appliance, replacing NTP servers **227**
vCenter Single Sign-On
  Active Directory **31, 34**
  changing password **45**
  domains **30**
  identity sources **29, 31, 34**
  LDAP **31, 34**
  locked users **39**
  OpenLDAP **31, 34**
  password policy **38**
  security token service (STS) **36**
  user repositories **29**
vCenter Single Sign-On best practices **46**
VECS **59**
vecs-cli, certificate replacement **37**
VGA-Only Mode **200**
VGT **215**
view certificates **111**
vifs, uploading certificates and keys **176**
virtual disks, shrinking **196**
virtual guest tagging **215**
virtual machine console, host security **198**
virtual machine security
  best practices **196**
  disable features **200**
  VMX parameters **200**
virtual machine service configuration, privileges **255**
virtual machines
  configuration privileges **248**
  copy and paste **202**
  disable copy and paste **201**
  disabling logging **204**
  guest operations privileges **250**
  interaction privileges **251**
  inventory privileges **253**
  isolation **215, 216**
  limiting variable information size **203**
  preventing device disconnection in the vSphere Web Client **203**
  provisioning privileges **253**
  securing **195, 204**
  snapshot management privileges **255**
  vSphere replication privileges **256**
virtual network, security **213**
virtual networking layer and security **15**
VirtualCenter.VimPasswordExpirationInDays **188**
VLAN **215**
VLAN documentation **223**
VLAN security **214**
VLANs
  and iSCSI **228**
  Layer 2 security **214**
  security **213**
  VLAN hopping **214**
VMCA
  certool **98**
  root certificates **80**
  view certificates **111**
vmca root certificate **70**
VMCA mode switches **142**
VMCA root certificate **79, 89, 95**
VMCA-signed certificates **66, 68, 72**
vmca-signed certificates **75**

vmdir certificate **88, 95**
vmdir replication **49**
vmdircert.pem **88, 95**
vmdirkey.pem **88, 95**
vMotion, securing with VLANs and virtual switches **214**
VMware Certificate Authority **58**
VMware Directory Service **22**
VMware Endpoint Certificate Store **59**
VMware Tools-based time synchronization **226**
vmx files, editing **195**
vpxd.cert.threshold **111**
vpxd.certmgmt.mode **144**
vpxuser **165**
VRM policy, privileges **248**
vServices, privileges **258**
vSphere Authentication Proxy
  authenticating **171**
  install or upgrade **166, 169**
vSphere Authentication Proxy Server **171, 172**
vSphere Certificate Manager **66**
vSphere Certificate Manager utility **63**
vSphere Client, firewall ports for direct connection **208**
vSphere Distributed Switch **212**
vSphere Network Appliance **222**
vSphere security overview **11**
vSphere Web Client security **230**
vsphere.local groups **27**

W

Windows session authentication **35**

Z

zoning **229**