vSphere Security

ESXi 5.5

vCenter Server 5.5

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-001164-04

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

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 security features available in the vSphere environment and the measures that you can take to safeguard your environment from attack.

Intended Audience

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

Updated Information

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

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

Revision	Description
EN-001164-04	■ Updated "Limit Log File Numbers in the vSphere Web Client," on page 125. It is no longer possible to change the log file size for individual virtual machines. ■ Updated "Uploading an SSH Key to Your ESXi Host," on page 94 to include a link to a KB article that describes how to generate the key on the host. ■ Updated "Active Directory LDAP Server and OpenLDAP Server Identity Source Settings," on page 29. Base DN for groups is not optional. For OpenLDAP configuration, the system adds the domain name in all caps as the domain alias if the user does not specify and alias. ■ Removed the topic that discusses how to configure a Windows NTP Client for Network Clock Synchronization. That information is available from the Microsoft Web site.
EN-001164-03	■ Added information about "Assigning Permissions for ESXi," on page 86 back in. This information was removed from this manual by mistake. ■ Clarified that ESXi processes do not start correctly if you use a password or pass phrase in "Modifying ESXi Web Proxy Settings," on page 107. ■ Changed Step 2 in "Configure a Host to Use Active Directory in the vSphere Web Client," on page 89 to more clearly illustrate the task. ■ Corrected the explanation of lockdown mode services for different users in "Lockdown Mode Behavior," on page 100. ■ In "General ESXi Security Recommendations," on page 77, corrected default certificate information to specify the PKCS#1 SHA-256 With RSA encryption signature algorithm.
EN-001164-02	Updated "Replacing ESXi SSL Certificates and Keys," on page 91 to explain when certificate replacement is recommended.
EN-001164-01	■ Moved "Enable SSL Certificate Validation Over Network File Copy," on page 74 from the Securing ESXi Hosts section to the Securing vCenter Server Systems section. ■ Added topic "Removing Expired or Revoked Certificates and Logs from Failed Installations," on page 73 ■ Added information on RDP hardening to "Hardening the vCenter Server Host Operating System," on page 71 ■ Added information about case matching requirements to "Assign Permissions in the vSphere Web Client," on page 66
EN-001164-00	Initial release.

1 Security in the vSphere Environment

To secure your vSphere environment, you must become familiar with many aspects of security including authentication, authorization, users and permissions, and aspects of 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:

Security and the Virtualization Layer

VMware designed the virtualization layer, or VMkernel, to run virtual machines. It controls the hardware that hosts use and schedules the allocation of hardware resources among the virtual machines. Because the VMkernel is fully dedicated to supporting virtual machines and is not used for other purposes, the interface to the VMkernel is strictly limited to the API required to manage virtual machines.

ESXi provides additional VMkernel protection with the following features:

Memory Hardening — The ESXi kernel, user-mode applications, and executable components such as drivers and libraries are located at random, non-predictable memory addresses. Combined with the non-executable memory protections made available by microprocessors, this provides protection that makes it difficult for malicious code to use memory exploits to take advantage of vulnerabilities.

Kernel Module Integrity — Digital signing ensures the integrity and authenticity of modules, drivers and applications as they are loaded by the VMkernel. Module signing allows ESXi to identify the providers of modules, drivers, or applications and whether they are VMware-certified. VMware software and certain third-party drivers are signed by VMware.

Trusted Platform Module (TPM) — vSphere uses Intel Trusted Platform Module/Trusted Execution Technology (TPM/TXT) to provide remote attestation of the hypervisor image based on hardware root of trust. The hypervisor image consists of the following elements:

- ESXi software (hypervisor) in VIB (package) format
- Third-party VIBs

- Third-party drivers

To leverage this capability, your ESXi system must have TPM and TXT enabled.

When TPM and TXT are enabled, ESXi measures the entire hypervisor stack when the system boots and stores these measurements in the Platform Configuration Registers (PCR) of the TPM. The measurements include the VMkernel, kernel modules, drivers, native management applications that run on ESXi, and any boot-time configuration options. All VIBs that are installed on the system are measured.

Third-party solutions can use this feature to build a verifier that detects tampering of the hypervisor image, by comparing the image with an image of the expected known good values. vSphere does not provide a user interface to view these measurements.

The measurements are exposed in a vSphere API. An event log is provided as part of the API, as specified by the Trusted Computing Group (TCG) standard for TXT.

Security and the Virtual Networking Layer

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

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 provide a substantial degree of protection when used with other common security practices, such as installing firewalls.

ESXi also 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.

Security Resources and Information

You can find additional information about security on the VMware Web site.

The table lists security topics and the location of additional information about these topics.

Table 1-1. 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/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 1-1. 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.
General information about virtualization and security	VMware Virtual Security Technical Resource Center http://www.vmware.com/go/security
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 VMware vCloud networking and security.	http://www.vmware.com/go/vmsafe
Hardening guides for different versions of vSphere and other VMware products.	https://www.vmware.com/support/support-resources/hardening-guides.html
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

vSphere Authentication with vCenter Single Sign-On

2

vCenter Single Sign-On is an authentication broker and security token exchange. When a user is authenticated with vCenter Single Sign-On, that user can access all installed vCenter services to which the user has been granted access. Because traffic is encrypted for all communications and only authenticated users can be granted access, your environment is secure.

Install or upgrade vCenter Single Sign-On before you install or upgrade any other vSphere components. See the *vSphere Installation and Setup* or the *vSphere Upgrade* documentation.

For information on replacing certificates for services that use vCenter Single Sign-On, see Chapter 3, "vSphere Security Certificates and Encryption," on page 43.

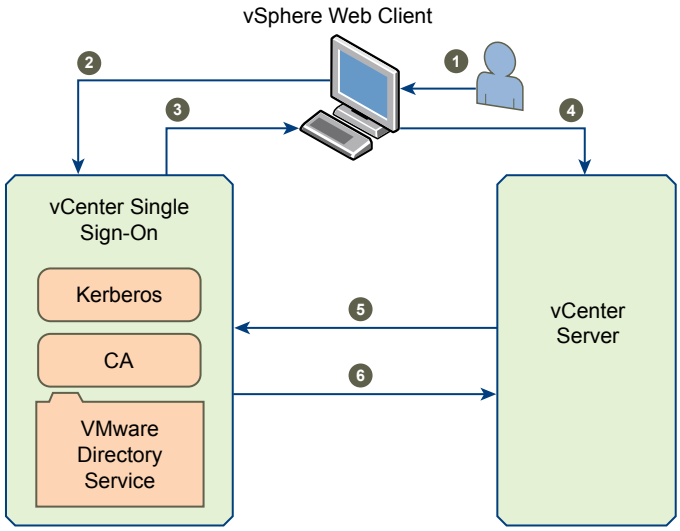
This chapter includes the following topics:

How vCenter Single Sign-On Protects Your Environment

vCenter Single Sign-On allows vSphere components to communicate with each other through a secure token mechanism 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 through Active Directory or OpenLDAP, as shown in the following illustration.

Figure 2-1. vCenter Single Sign-On Handshake



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. The checkbox becomes available after you install the VMware Client Integration Plugin.

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), vCenter Single Sign-On checks that domain.

3 If the user is in 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 The vCenter Single Sign-On server returns the token to the vCenter Server system.

The user can now authenticate to vCenter Server and view and modify any objects that the user has permissions for..

NOTE Initially, each user is assigned the No Access permission. A vCenter Server administrator must assign the user at least Read Only permissions before the user can log in. See "Assign Permissions in the vSphere Web Client," on page 66 and Chapter 5, "vCenter User Management Tasks," on page 65.

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 components are deployed as part of installation.

STS (Security Token Service)	STS certificates enable a user who has logged on through vCenter Single Sign-On to use any vCenter service that vCenter Single Sign-On supports without authenticating to each one. The STS service issues Security Assertion Markup Language (SAML) tokens. These security tokens represent the identity of a user in one of the identity source types supported by vCenter Single Sign-On.
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@vsphere.local has these privileges.
vCenter Lookup Service	vCenter Lookup Service contains topology information about the vSphere infrastructure, enabling vSphere components to connect to each other securely. Unless you are using Simple Install, you are prompted for the Lookup Service URL when you install other vSphere components. For example, the Inventory Service and the vCenter Server installers ask for the Lookup Service URL and then contact the Lookup Service to find vCenter Single Sign-On. After installation, the Inventory Service and vCenter Server system are registered in vCenter Lookup Service so other vSphere components, like the vSphere Web Client, can find them.
VMware Directory Service	Directory service associated with the vsphere.local domain. This service is a multi-tenanted, multi-mastered directory service that makes an LDAP directory available on port 11711. In multisite mode, an update of VMware Directory Service content in one VMware Directory Service instance results in the automatic update of the VMware Directory Service instances associated with all other vCenter Single Sign-On nodes.

How vCenter Single Sign-On Affects vCenter Server Installation

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

Authentication by vCenter Single Sign-On makes the VMware cloud infrastructure platform more secure by allowing the vSphere software components to communicate with each other through a secure token exchange mechanism.

For the first installation of vCenter Server, you must install all components. In subsequent installations in the same environment, or if you add services, you do not have to install vCenter Single Sign-On. One vCenter Single Sign-On server can serve your entire vSphere environment. After you install vCenter Single Sign-On once, you can connect all new vCenter Server instances to the same vCenter Single Sign-On service. You must install an Inventory Service instance for each vCenter Server instance.

Simple Install

The Simple Install option installs vCenter Single Sign-On, the vSphere Web Client, vCenter Inventory Service, and vCenter Server on the same host or virtual machine. Simple Install is appropriate for most deployments.

Custom Install

If you want to customize the location and setup of each component, you can install the components separately by performing a custom install and selecting the individual installation options, in the following order:

1 vCenter Single Sign-On

2 vSphere Web Client

3 vCenter Inventory Service

4 vCenter Server

You can install each component on a different host or virtual machine.

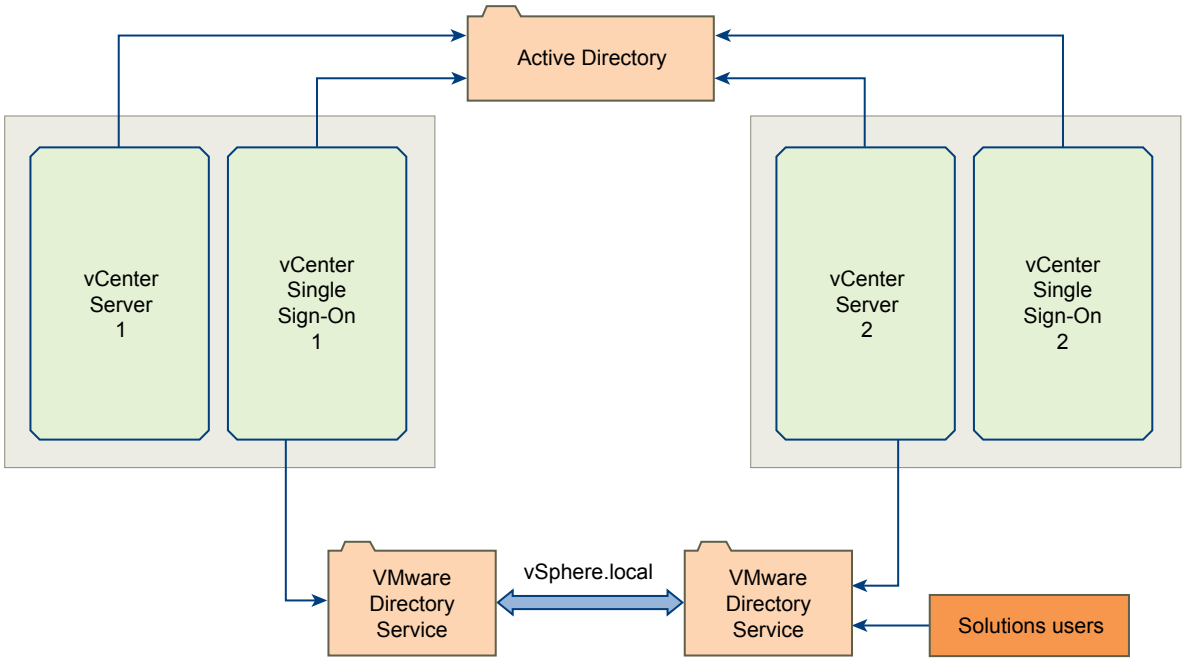
If you decide on installing multiple vCenter Server systems, you can point to the same vCenter Single Sign-On service for each vCenter Server.

Installing in Multiple Locations

Unlike vCenter Single Sign-On version 5.1, vCenter Single Sign-On 5.5 synchronizes authentication data across locations.

If you install vCenter Server systems in multiple locations, you can install a vCenter Single Sign-On server in each location. When you install the second and subsequent instances of vCenter Single Sign-On, you can point it to the first vCenter Single Sign-On instance during installation. The two instances synchronize their VMware Directory Service instances. Changes to one instance are propagated to the other instance.

Figure 2-2. Installing vCenter Single Sign-On in Multiple Locations



How vCenter Single Sign-On Affects vCenter Server Upgrades

Which users can log in to vCenter Server after an upgrade depends on the version that you are upgrading from and the deployment configuration.

In upgrades to vCenter Server 5.0 and earlier, which do not include a vCenter Single Sign-On service, both the local operating system users and Active Directory users that are registered with vCenter Server continue to work with the upgraded vCenter Server.

This behavior changes if you are upgrading from a version that does not include vCenter Single Sign-On to a version that does include vCenter Single Sign-On: vCenter Server version 5.1 or vCenter Server version 5.5.

NOTE With 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.

After the upgrade from a version earlier than version 5.1, you might be prompted for the administrator of the root folder in the vSphere inventory hierarchy during installation. This might happen because of changes in user stores from pre-5.1 versions to 5.1 and later versions of vSphere. See "Hierarchical Inheritance of Permissions," on page 57.

Simple Install Upgrade

A Simple Install upgrade installs or upgrades a single vCenter Server and related components.

If you upgrade to vCenter Server 5.5 from a vCenter Server version that does not include vCenter Single Sign-On, vCenter Single Sign-On recognizes existing local operating system users. In addition, the user administrator@vsphere.local can log in as an administrator user to vCenter Single Sign-On and vCenter Server. If your previous installation supported Active Directory users, you can add the Active Directory domain as an identity source.

If you upgrade vCenter Single Sign-On and vCenter Server, vCenter Single Sign-On recognizes existing local operating system users. In addition, the user administrator@vsphere.local can log in to vCenter Single Sign-On and vCenter Server as an administrator user. If your previous installation included an Active Directory domain as an identity source, that identity source is still available after the upgrade. Because vCenter Server supports only one default identity source, users might have to specify the domain when they log in (*DOMAIN**user*).

Custom Upgrade

A custom upgrade might install different vCenter Server components on different machines or install a second vCenter Server system on the same machine. You also use Custom Install to upgrade an environment that is installed in different locations.

If you upgrade to vCenter Server 5.5 from a vCenter Server version that does not include vCenter Single Sign-On, and you install vCenter Single Sign-On on a different machine than vCenter Server, vCenter Single Sign-On does not recognize existing local operating system users. The user administrator@vsphere.local can log in to vCenter Single Sign-On and vCenter Server as an administrator user. If your previous installation supported Active Directory users, you can add the Active Directory domain as an identity source.

If you are upgrading vCenter Server from a version that includes vCenter Single Sign-On in multisite mode, and if the different vCenter Server systems use Linked mode, you must resynchronize first. You can then upgrade all vCenter Single Sign-On instances and maintain Linked Mode functionality. Linked Mode is required for a single view of all vCenter Server systems. Multisite vCenter Single Sign-On is supported only if all nodes are the same version.

If you are upgrading vCenter Server from a version that includes vCenter Single Sign-On in high availability mode, you must upgrade all of the vCenter Single Sign-On high availability instances. Perform the upgrade first, and configure high availability by protecting both vCenter Server and vCenter Single Sign-On with VMware HA or VMware Heartbeat after the upgrade is complete.

NOTE When you install the vCenter Single Sign-On component that is included with vCenter Server version 5.5 in multiple locations, the VMware Directory Service is updated for all vCenter Single Sign-On instances if you make a change in one location.

Using vCenter Single Sign-On with vSphere

When a user logs in to a vSphere component, vCenter Single Sign-On is used for authentication. Users must be authenticated with vCenter Single Sign-On and must have been granted vCenter Server permissions to view and manage vSphere objects.

When users log in to the vSphere Web Client, they are first authenticated by vCenter Single Sign-On. For authenticated users, vCenter Server checks the permissions. What a user can see, and what a user can do, is determined by vSphere permission settings for vCenter Server and ESXi and by the applications in the environment. 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 Users and Permissions," on page 57 and Chapter 5, "vCenter User Management Tasks," on page 65.

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 of the vCenter Server instances or other vSphere services for which they have permissions. No further authentication is required. The actions that authenticated users can perform on objects depend on the user's vCenter Server permissions on those objects. See Chapter 4, "vSphere Users and Permissions," on page 57 and Chapter 5, "vCenter User Management Tasks," on page 65.

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).

While most vCenter Single Sign-On management tasks require vCenter Single Sign-On administrator credentials, all users that can authenticate to vCenter Single Sign-On can reset their password, even if the password has expired. See "Reset an Expired vCenter Single Sign-On Password," on page 22.

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 with vCenter Single Sign-On administrator privileges must log in to the vSphere Web Client. Upon authentication, that user can access the vCenter Single Sign-On administration interface to manage identity sources and default domains, specify password policies, and perform other administrative tasks. See "Configuring vCenter Single Sign-On," on page 21.

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 5.1 is not integrated with vCenter Single Sign-On. You add the ESXi host to an Active Directory domain explicitly. See "Add an ESXi Host to an Active Directory Domain," on page 81.

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.

Login Behavior

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.

- 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.

Configuring vCenter Single Sign-On

vCenter Single Sign-On lets you add identity sources, manage default domains, configure a password policy, and edit the lockout policy.

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.

- Reset an Expired vCenter Single Sign-On Password on page 22

  By default, vCenter Single Sign-On passwords, including the password for administrator@vsphere.local, expire after 90 days. The vSphere Web Client provides a warning when a password is about to expire. You can reset an expired password from the vSphere Web Client.

- Edit the vCenter Single Sign-On Password Policy on page 23

  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).

- Edit the vCenter Single Sign-On Lockout Policy on page 24

  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.

- Edit the vCenter Single Sign-On Token Policy on page 24

  The vCenter 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.

- Identity Sources for vCenter Server with vCenter Single Sign-On on page 25

  Identity sources allow you 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 26

  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 27

  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 30

  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 30

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

- Remove a Security Token Service (STS) Certificate on page 30

  vCenter Single Sign-On provides a Security Token Service (STS). The Security Token Service is a Web service that issues, validates, and renews security tokens. You can remove existing vCenter Single Sign-On STS certificates when they expire or change.

- Refresh the Security Token Service (STS) Root Certificate on page 31

  vCenter Single Sign-On provides 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 when it expires or changes.

- Determine the Expiration Date of an SSL Certificate on page 32

  CA-signed SSL certificates expire after a predefined lifespan. Knowing when a certificate expires lets you replace or renew the certificate before the expiration date.

- Determine Whether a Certificate is Being Used on page 32

  Before you start with certificate replacement, you can check whether the certificates you have are already being used. You can use the **Compute Usage** feature to determine whether or not the system is using a certificate.

- Use vCenter Single Sign-On with Windows Session Authentication on page 32

  You can use vCenter Single Sign-On with Windows Session Authentication (SSPI). Before the checkbox on the login page becomes available, you must install the Client Integration Plug-in.

Reset an Expired vCenter Single Sign-On Password

By default, vCenter Single Sign-On passwords, including the password for administrator@vsphere.local, expire after 90 days. The vSphere Web Client provides a warning when a password is about to expire. You can reset an expired password from the vSphere Web Client.

In vSphere 5.5 and later, a user with an expired password is prompted to reset the password upon login. To reset passwords for earlier versions of vCenter Single Sign-On, see the documentation for that version of the product.

Prerequisites

You must know the current, expired password corresponding to the user name.

Procedure

1 Go to the vSphere Web Client URL.

2 When prompted, provide the user name, the current password, and the new password.

If you are unable to log in, contact a vCenter Single Sign-On system administrator for assistance.

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 "Reset an Expired vCenter Single Sign-On Password," on page 22.

Procedure

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

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. Required.
Maximum lifetime	Maximum number of days that a password can exist before the user must change it.
Restrict re-use	Number of the user's previous passwords that cannot be selected. For example, if a user cannot reuse any of the last five passwords, type 5.
Maximum length	Maximum number of characters that are allowed in the password.
Minimum length	Minimum number of characters required in the password. The minimum length must be no less than the combined minimum of alphabetic, numeric, and special character requirements.
Character requirements	Minimum number of different character types that are required in the password. ■ 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. The following characters are not supported in passwords: non-ASCII characters, semicolon (;), double quotation mark ("), single quotation mark ('), circumflex (^), and backslash.
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.

Procedure

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

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	Description of the lockout policy. Currently a required field.
Max number of failed login attempts	Maximum number of failed login attempts that are allowed before the account is locked.
Time interval between failures (seconds)	Time period in which failed login attempts must occur to trigger a lockout.
Unlock time (seconds)	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

The vCenter 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 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**.

Identity Sources for vCenter Server with vCenter Single Sign-On

Identity sources allow you 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. Upon installation, every instance of vCenter Single Sign-On has the Local OS identity source identity source vpshere.local. This identity source is internal to vCenter Single Sign-On.

A vCenter Single Sign-On administrator user can create vCenter Single Sign-On users and groups.

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. 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. Shown as **Active Directory (Integrated Windows Authentication)** in the vSphere Web Client.

- 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.
- 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.

Login Behavior

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.

- 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.

vCenter Single Sign-On does not propagate permissions that result from nested groups from dissimilar identity sources. For example, if you add the Domain Administrators group to the Local Administrators group, the permissions is not propagated because Local OS and Active Directory are separate identity sources.

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.

- 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.

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.

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

localos	All local operating system users. These users can be granted permissions to vCenter Server. If you are upgrading, those users who already have permissions keep those permissions.
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.

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. See "Active Directory Identity Source Settings," on page 28.
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 29.

Option	Description
OpenLDAP	Use this option for an OpenLDAP identity source. See "Active Directory LDAP Server and OpenLDAP Server Identity Source Settings," on page 29.
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 user 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** permission. A user with vCenter Server **Modify.permissions** privileges can assign permissions to users or groups of users to enable them to log in to vCenter Server. See "Assign Permissions in the vSphere Web Client," on page 66.

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.

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.

Table 2-1. 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 SPN	Select this option if you expect to rename the local machine. You must specify an SPN, a user who can authenticate with the identity source, and a password for the user.
Service Principal	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.

Table 2-1. Add Identity Source Settings (Continued)

Field	Description
User Principal Name	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 2-2. Active Directory as an LDAP Server and OpenLDAP Settings

Field	Description
Name	Name of the identity source.
Base DN for users	Base domain 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 domain 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.
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.

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. See "Active Directory Identity Source Settings," on page 28.
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 29.
OpenLDAP	Use this option for an OpenLDAP identity source. See "Active Directory LDAP Server and OpenLDAP Server Identity Source Settings," on page 29.
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.

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.

Remove a Security Token Service (STS) Certificate

vCenter Single Sign-On provides a Security Token Service (STS). The Security Token Service is a Web service that issues, validates, and renews security tokens. You can remove existing vCenter Single Sign-On STS certificates when they expire or change.

Procedure

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

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

3 Select the **Certificates** tab.

4 Select the **STS Signing** tab and select the certificate that you want to remove.

5 Click the **Delete STS Signing Certificate** icon.

6 Click **Yes**.

The certificate is removed from the vCenter Single Sign-On server and no longer appears on the **STS Signing** tab.

What to do next

Restart the vSphere Web Client.

Refresh the Security Token Service (STS) Root Certificate

vCenter Single Sign-On provides 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 when it expires or changes.

STS certificates expire or change periodically and must be updated or refreshed. In some environments, your system administrator might implement automatic updates of the certificate. Otherwise, you can update the certificate manually.

NOTE The vCenter Certificate Automation Tool can only replace the SSL certificates. The tool cannot be used to replace the STS certificates.

Procedure

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

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

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

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.

Determine the Expiration Date of an SSL Certificate

CA-signed SSL certificates expire after a predefined lifespan. Knowing when a certificate expires lets you replace or renew the certificate before the expiration date.

Procedure

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

What to do next

Renew or replace SSL certificates that are getting close to their expiration date.

Determine Whether a Certificate is Being Used

Before you start with certificate replacement, you can check whether the certificates you have are already being used. You can use the **Compute Usage** feature to determine whether or not the system is using a certificate.

Procedure

1. Log in to the vSphere Web Client as administrator@vsphere.local or as another user with vCenter Single Sign-On administrator privileges.
2. Browse to **Administration > Single Sign-On > Configuration**.
3. Click the **Certificates** tab, and then the **Identity Sources TrustStore** subtab.
4. Click **Compute Usage**.

   For each certificate in the list, the vSphere Web Client communicates with each registered LDAPS identity source to determine whether a valid connection exists.
5. The Used By Domain column shows whether a certificate is in use, and helps you determine whether you can safely remove a certificate.

Use vCenter Single Sign-On with Windows Session Authentication

You can use vCenter Single Sign-On with Windows Session Authentication (SSPI). Before the checkbox on the login page becomes available, you must install the Client Integration Plug-in.

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.

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 pp-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.

5 Exit and restart your browser.

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

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 34

  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 34

  When a vCenter Single Sign-On user 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 35

  You can delete users that are in the vsphere.local domain from the vSphere Web Client. 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 35

  You can change the password or other details of a vCenter Single Sign-On user from the vSphere Web Client. You cannot change the user name of a user.

- Add a vCenter Single Sign-On Group on page 35

  In the vSphere Web Client, 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).

- Edit a vCenter Single Sign-On Group on page 36

  You can change the description of a vCenter Single Sign-On group in the vSphere Web Client. You cannot change the name of the group.

- Add Members to a vCenter Single Sign-On Group on page 36

  Members of a vCenter Singe 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 37

  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 Application Users on page 37

  vCenter Single Sign-On recognizes vCenter services such as vCenter Server, vCenter Inventory Server, and the vSphere Web Client and grants privileges to those services as application users.

- Change Your vCenter Single Sign-On Password on page 37

  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.

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.

2 Browse to **Administration > Single Sign-On > Users and Groups**.

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

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

You cannot add users to other domains.

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 permissions to perform management operations.

What to do next

Add the user to a group in the vsphere.local domain, for example, to the administrator group. See "Add Members to a vCenter Single Sign-On Group," on page 36.

Disable and Enable vCenter Single Sign-On Users

When a vCenter Single Sign-On user account is disabled, the user cannot log in to the vCenter Single Sign-On server until 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.

2 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 vSphere Web Client. 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.
2. 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 change the user name of a user.

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.
2. 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 vSphere Web Client, 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 vCenter Single Sign-On 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.
2. 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.

Edit a vCenter Single Sign-On Group

You can change the description of a vCenter Single Sign-On group in the vSphere Web Client. You cannot change the name of the group.

vCenter Single Sign-On groups are stored in the vCenter Single Sign-On database, which runs on the system where vCenter Single Sign-On is installed. These groups are part of 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.

2 Browse to **Administration > Single Sign-On > Users and Groups**.

3 Click the **Groups** tab.

4 Right-click the group to edit and select **Edit Group**.

5 Edit the description for the group.

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

6 Click **OK**.

Add Members to a vCenter Single Sign-On Group

Members of a vCenter Singe 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.

Groups listed on the **Groups** tab in the vSphere Web Client are internal to vCenter Single Sign-On and are part of the vsphere.local domain. You can add group members from other domains to a local group. You can also nest groups.

Procedure

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

2 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 principal to add to the group.

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

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

You can simultaneously add multiple principals.

8 Click **OK**.

The principal (user or group) is a member of the group and appears in the lower panel of the Groups tab.

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.
2. 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 Application Users

vCenter Single Sign-On recognizes vCenter services such as vCenter Server, vCenter Inventory Server, and the vSphere Web Client and grants privileges to those services as application users.

When you uninstall an vCenter service, the service is removed from the list of vCenter Single Sign-On application users as part of uninstallation by default. If you forcefully remove an application, or if the system becomes unrecoverable while the application user is still in the system, you can remove the application user explicitly from the vSphere Web Client.

IMPORTANT If you remove an application, the application no longer has access 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.
2. Browse to **Administration > Single Sign-On > Users and Groups**.
3. Click the **Applications Users** tab, and click the application user name.
4. Click the **Delete Application User** icon.
5. Click **Yes**.

The application (or solution) no longer has access to vCenter Server and cannot function as a vCenter service.

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.

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 passwords expire after 90 days, but your system administrator might change this default depending on the policy of your organization. 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.

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 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**.

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.

vCenter Single Sign-On Installation Fails

In a Windows environment, vCenter Single Sign-On installation might fail for several reasons.

Problem

The vCenter Single Sign-On installation fails in a Windows environment.

Cause

Multiple causes of an installation failure.

Solution

1 Verify that all installation setup prerequisites are met.

At the time the installation fails, the installer displays a message similar to `####: Installation failed due to....`

2 At a command line, run the following command to gather a vCenter Single Sign-On support bundle.

```
C:\Windows\System32\cscript.exe "SSO Server\scripts\sso-support.wsf" /z
```

3 Click **OK**

4 View the logs in `%TEMT%\vminst.log` for details about the failure and possible solutions.

For a complete list of logs, see VMware Knowledge Base article 2033430.

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 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.

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.

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.

4 Restart vCenter Single Sign-On.

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.
- 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.

vSphere Security Certificates and Encryption 3

ESXi and vCenter Server components communicate securely over SSL to ensure confidentiality, data integrity and authentication. Data is private, protected, and cannot be modified in transit without detection.

By default, vSphere services use the certificates that are created as part of the installation process and stored on each system. These default certificates are unique and make it possible to begin using the software, but they are not signed by a trusted certificate authority (CA).

To receive the full benefit of certificate checking, particularly if you intend to use SSL connections over the Internet, install new certificates that are signed by a valid internal certificate authority or purchase a certificate from a trusted security authority.

This chapter includes the following topics:

Certificates Used in vSphere

Different types of certificates are used for different purposes in your vSphere environment.

SAML Tokens Issued by vCenter Single Sign-On STS Service

STS certificates enable a user who has logged on through vCenter Single Sign-On to use any vCenter Service that vCenter Single Sign-On supports without authenticating to each one. The STS service issues Security Assertion Markup Language (SAML) tokens. These security tokens represent the identity of a user in one of the of the identity source types supported by vCenter Single Sign-On. See "How vCenter Single Sign-On Protects Your Environment," on page 15.

The vCenter Single Sign-On service deploys an Identity Provider which issues SAML Tokens used throughout the vSphere for authentication purposes. A SAML token is a piece of XML that represents the user's identity (user name, first, last name). In addition the SAML token contains group membership information so that the SAML token could be used for authorization operations. When vCenter Single Sign-On issues SAML tokens, it signs each token are signed with the certificate chain so that clients of vCenter Single Sign-On can verify that the SAML token comes from a trusted source.

SSL Certificates

SSL certificates secure communication throughout your vSphere environment. The client verifies the authenticity of the certificate presented during the SSL handshake phase, before encryption. This verification protects against man-in-the-middle attacks.

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

vSphere components include default certificates. You can replace the default certificates with self-signed or CA-signed certificates. For the vCenter core components, you can use the Certificate Automation Tool.

SSH Keys

SSH keys are used to control access to the ESXi hosts that are using the Secure Shell (SSH) protocol. See "Uploading an SSH Key to Your ESXi Host," on page 94.

Cipher Strength

To encrypt data, the sending component, such as a gateway or redirector, applies cryptographic algorithms, or ciphers, to alter the data before transmitting it. The receiving component uses a key to decrypt the data, returning it to its original form. Several ciphers are in use, and the level of security that each provides is different. One measure of a cipher's ability to protect data is its cipher strength—the number of bits in the encryption key. The larger the number, the more secure the cipher.

256-bit AES encryption and 1024-bit RSA for key exchange are the default for the following connections.

- vSphere Web Client connections to vCenter Server and to ESXi through the management interface.
- SDK connections to vCenter Server and to ESXi.
- Connections to the virtual machine virtual machine console.
- Direct SSH connections to ESXi.

Certificate Replacement Overview

For the core vCenter components, you can generate certificate requests and replace the default certificates with self-signed or CA-signed certificates by using the Certificate Automation Tool. You can also generate the requests, create the certificates, and replace the certificates from the command line without the tool.

Where to Find Information

How you want to replace certificates determines where you can find information. You can perform certificate replacement in several ways.

- Use the Certificate Replacement tool in your Windows environment, as described in this document.
- Replace certificates on Windows explicitly, as explained in VMware Knowledge Base article 2058519.
- Replace certificates on the vCenter Server Appliance, as explained in VMware Knowledge Base article 2057223.

If want to use certificates that are signed by a CA, you must generate a certificate request (CSR) for each component. You can use the tool to generate the CSRs. See "Preparing Your Environment," on page 48 for a list of certificate requirements.

Certificate Replacement Tool Overview

The Certificate Automation Tool is a command-line tool that helps you replace the certificates. In most cases, you replace the default certificates with custom certificates. You use the tool after you install all vCenter components. If you add a new component to your vSphere environment, you can run the tool again to perform certificate replacement for the new component. When you run the tool on a vCenter component such as the vCenter Server system or the vCenter Single Sign-On server, it performs the following tasks.

- Prompts you for required input.
- Validates the input (x.509 certificate and URL formats).
- Updates the SSL certificate of a component and the corresponding LookupService entries of the services that are exposed by the components if necessary.
- Restarts the corresponding service if necessary.
- Updates the trust of the component to all other components that it connects to. Restarts the component if necessary.
- Provides the next steps to the user where necessary.

NOTE Certificate replacement with the tool has been tested with vCenter Single Sign-On, vCenter Inventory Service, vCenter Server, vSphere Web Client, vSphere Update Manager, vCenter Log Browser and vCenter Orchestrator. If you have to perform a certificate replacement with another vSphere component, the instructions in VMware documentation or the VMware Knowledge base for that product. You might have to update certificates on one of the supported components as part of the process.

The tool supports the following vCenter components:

- vCenter Single Sign-On
- vCenter Inventory Service
- vCenter Server
- vSphere Web Client
- vSphere Update Manager
- vCenter Log Browser
- vCenter Orchestrator

Each component must have an SSL certificate and a solution user certificate. Most components use the same certificate for both purposes. On Windows, the solution user certificates must be unique, so a unique SSL certificate for each component is required.

Upgrades

If you replaced the default certificates in vSphere version 5.0 or version 5.1, and you upgrade to vSphere version 5.5, the certificates are migrated. If you are upgrading and you want to replace the default certificates, you can run the Certificate Automation Tool after the upgrade.

Certificate Automation Tool Deployment Options

The vCenter Certificate Automation Tool automates certificate renewal for core vCenter components on Windows operating systems.

The tool supports several deployment options. How the tool interacts with the user depends on the deployment option. See "Certificate Replacement Overview," on page 44

All Services on One Machine

You can edits the `ssl-environment.bat` file and enter environment-specific information, and run the tool on the machine without being prompted. As an alternative, you can run the tool and provide input when prompted.

Each Service on a Separate Machine

If each service runs on a separate machine or virtual machine in your environment, follow the steps below to update certificates. If some of these services run on the same machine, follow the information in the Update Planner list that is generated by the Certificate Automation Tool. If you are not including some of the services in your environment, you can skip the corresponding steps.

1. Install and run the tool on one machine. The tool generates the update planner list.
2. Install and run the tool on the machine on which vCenter Single Sign-on is running to update the vCenter Single Sign-On SSL certificate.
3. Install and run the tool on the Inventory Service machine. The tool performs these tasks:
   a. Updates the trust from vCenter Inventory Service to vCenter Single Sign-On.
   b. Updates the vCenter Inventory Service SSL certificate.
4. Install and run the tool on the machine on which vCenter Server is running. The tool performs these tasks:
   a. Updates the trust from the vCenter Server service to the vCenter Single Sign-On service.
   b. Updates the vCenter Server SSL certificate.
   c. Updates the trust from the vCenter Server to the vCenter Inventory Service.
   d. Updates the trust from the vCenter Server to the vSphere Update Manager.
5. Install and run the tool on the vCenter Orchestrator machine. The tool performs these tasks:
   a. Updates the trust from the vCenter Orchestrator service to the vCenter Single Sign-On service.
   b. Updates the trust from the vCenter Orchestrator service to the vCenter Server service.
   c. Updates the vCenter Orchestrator SSL certificate.
6. Install and run the tool on the vSphere Web Client machine. The tool performs these tasks:
   a. Updates the trust from the vSphere Web Client to the vCenter Single Sign-On service.
   b. Updates the trust from the vSphere Web Client to the vCenter Inventory Service and restarts the service.
   c. Updates the trust from the vSphere Web Client to the vCenter Server service and restarts the service.
   d. Updates the trust from the vSphere Web Client to the vCenter Orchestrator service and restarts the service.
   e. Updates the vSphere Web Client SSL certificate.

   You have to restart the vSphere Web Client to complete the updates of the trust relationships.
7. Install and run the tool on the Log Browser machine. The vSphere Web Client and the vCenter Log Browser always run on the same machine. The tool performs these tasks.
   a. Updates the trust from the Log Browser service to the vCenter Single Sign-On service.
   b. Updates the Log Browser SSL certificate.

8 Install and run the tool on the vSphere Update Manager machine.

The tool updates the vSphere Update Manager SSL certificate. As part of the certificate update, the vCenter Server trust to vSphere Update manger is updated.

Mixed Mode Deployment

In a mixed mode deployment, for example, when two services are on one machine and three services are on a second machine, you can run the tool as if each service were on a different machine.

Replacing vCenter Certificates With the vCenter Certificate Automation Tool

You can replace the default vCenter SSL certificates with CA-signed or self-signed certificates if company policy requires it. The vCenter Certificate Automation Tool is a command-line tool that helps you replace certificates in the correct order for the core vCenter services in your environment. You can use the tool to generate certificate requests, generate an update plan, and perform the update.

Each vSphere service has an identity, which is used to create an x509 certificate. You can replace the certificates for the core vCenter components with the vCenter Certificate Automation Tool. You can replace certificates for other vCenter components manually.

- Use the vCenter Certificate Automation Tool to replace SSL certificates for vCenter components that are installed on supported Windows operating systems. The tool helps you generate certificate requests and to plan the process of replacing certificates. The tool supports vCenter Single Sign-On, vCenter Inventory Service, vCenter Server, vSphere Web Client, vSphere Update Manager, vCenter Log Browser and vCenter Orchestrator.
- If you are using other vSphere components, see VMware documentation or the VMware Knowledge Base for certificate replacement information.
- If you are using a third-party component, you must replace the certificates manually. See VMware Knowledge Base article 2058519.
- If you are using the vCenter Server Appliance, replace SSL certificates manually. Some services share certificates. See VMware Knowledge Base article 2057223.

Replacing the certificates consists of several tasks.

1 Preparing Your Environment on page 48

Before you run the vCenter Certificate Automation Tool, verify that you are running on one of the supported operating systems and verify that you have the correct platform, that the certificates meet requirement, and that your system setup meets requirements.

2 Install the vCenter Certificate Automation Tool on page 50

You install the vCenter Certificate Automation Tool on each machine on which a vCenter core component resides. To do the initial planning, you can install the tool on a single machine.

3 Predefine Default Values for vCenter Certificate Automation Tool on page 50

Predefining default values in a configuration file for the tool helps prevent typing errors and saves time. With default values predefined, the tool no longer prompts you for those values. You cannot specify default passwords.

4 Generate Certificate Requests and Set Up CA Signed Certificates on page 51

If you want to use trusted certificates that are generated by a CA (Certificate Authority), you must create certificate requests and submit them to a CA.

5 Run the Update Planner on page 52

The update planner, part of the vCenter Certificate Automation Tool, allows you to determine the correct order for certificate replacement. Follow the steps in the order that the tool recommends for best results.

6 Run the Tool to Update SSL Certificates and Trusts on page 53

After you obtain the SSL certificates and you generate the list of update steps, you can run the tool to replace the existing certificates, reestablish trust, and optionally restart some of the services.

7 Rolling Back Your Updates on page 54

Each update operation successfully performs the update for one certificate and key, or fails in a way that preserves the original state. If an update fails, you might need to roll back the failed step.

Preparing Your Environment

Before you run the vCenter Certificate Automation Tool, verify that you are running on one of the supported operating systems and verify that you have the correct platform, that the certificates meet requirement, and that your system setup meets requirements.

Review the Known Issues listed in VMware Knowledge Base Article 2057340.

Supported Platforms

The tool has been tested on the following Windows operating systems.

- Windows 2008 R2 SP1
- Windows 2012 Standard

Tool and Product Versions

Different versions of the tool are supported with different versions of vSphere.

- Version 1.0 of the tool is supported with vSphere 5.1
- Version 1.0.1 of the tool is supported with vSphere 5.1 Update 1
- Version 5.5 of the tool is supported with vSphere 5.5

Certificate Requirements

You can obtain the CA-signed certificates before you run the tool, or you can have the tool generate the certificate requests for you. Before you run the tool to replace certificates, make sure that certificates meet the following requirements:

- The SSL certificate for each vSphere component has a unique base DN.
- The certificates and private keys meet these requirements:
  - Private key algorithm: RSA
  - Private key length >= 1024
  - Private key standard: PKCS#1 or PKCS#8
  - Private key storage: PEM
- Recommended certificate signature algorithm:
  - sha256WithRSAEncryption 1.2.840.113549.1.1.11
  - sha384WithRSAEncryption 1.2.840.113549.1.1.12

- sha512WithRSAEncryption 1.2.840.113549.1.1.13

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

- The certificate chain format meets these requirements:
  - Single PEM file that does not contain any comments.
  - The file starts with the header of the first certificate, that is, `-----BEGIN CERTIFICATE-----`.
  - Self-signed certificates are ordered from the leaf to the root.
  - No extra certificates are in the file.
  - The certificate chain is complete.
- The path or file name for certificates and keys does not contain any of the following special characters:
  - ^ (caret)
  - % (percent)
  - & (ampersand)
  - ; (semicolon)
  -) (closing parenthesis)

  The tool exits, throws an exception, or reports that certificate or key files are not found if it encounters those characters.

System Requirements

Install all vCenter components, obtain administrator permissions, and shut down dependent solutions, as follows:

- Verify that all vCenter components that require certificate updates are installed and running, and that you have access to the server for each component.
- Verify that you have administrative privileges on the server or servers that you are running the tool on. Although nonadministrator users can download and launch the tool, all operations fail without the proper permissions.
- Shut down the following dependent solutions that are running in the environment:
  - VMware Site Recovery Manager
  - vSphere Data Recovery
  - vCloud Director
  - Any third-party solution which might be connecting to vCenter Server

Install the vCenter Certificate Automation Tool

You install the vCenter Certificate Automation Tool on each machine on which a vCenter core component resides. To do the initial planning, you can install the tool on a single machine.

Install the tool on each physical or virtual machine on which a service is running whose certificate update is planned. You can install the tool in several configurations. See "Certificate Automation Tool Deployment Options," on page 45.

NOTE Different versions of the tool are supported with different versions of vSphere.

- Version 1.0 of the tool is supported with vSphere 5.1
- Version 1.0.1 of the tool is supported with vSphere 5.1 Update 1
- Version 5.5 of the tool is supported with vSphere 5.5

Prerequisites

- Verify that all requirements are met. See "Preparing Your Environment," on page 48.
- Obtain certificates for each machine on which a vSphere component resides before you install the tool, or use the tool to generate Certificate Signing Requests (CSRs) and obtain certificates from your Certificate Authority. See "Generate Certificate Requests and Set Up CA Signed Certificates," on page 51.

Procedure

1 Download the vCenter Certificate Automation Tool.

   The download is located in the Drivers and Tools section of the VMware vSphere download page.

2 For initial planning, copy the downloaded ZIP file to one machine and generate the Update Planner list.

3 Depending on your deployment, you might copy the downloaded ZIP file to each machine on which a vCenter core component resides.

4 Unzip the file into any directory, preserving the directory structure.

What to do next

You can predefine your preferred default values, see "Predefine Default Values for vCenter Certificate Automation Tool," on page 50, or respond to the prompts when you run the tool.

If a newer version of the tool becomes available, you can download and unzip that version of the tool to a different directory and delete the old version of the tool.

Predefine Default Values for vCenter Certificate Automation Tool

Predefining default values in a configuration file for the tool helps prevent typing errors and saves time. With default values predefined, the tool no longer prompts you for those values. You cannot specify default passwords.

Predefining default values is not required, but might help speed up the process later. If the tool does not encounter defaults, it prompts you.

Prerequisites

Verify that the vCenter Certificate Automation Tool is not running. The tool reads the values in `ssl-environment.bat` when you start it.

Procedure

1 Open `ssl-environment.bat` in a text editor.

2 Specify parameters that you want to change for each vSphere component that requires updated certificates.

For example, for vCenter Server, you can edit the `vc_cert_chain`, `vc_private_key`, and `vc_username` parameters.

3 Save and close `ssl-environment.bat`.

4 Start the tool.

The tool picks up your default values each time you start it.

The vCenter Certificate Automation Tool saves the information and uses it to automatically prefill required input.

What to do next

Generate certificate requests if necessary, or run the update planner if you deployed on multiple machines to plan your certificate update tasks. See "Run the Update Planner," on page 52.

Generate Certificate Requests and Set Up CA Signed Certificates

If you want to use trusted certificates that are generated by a CA (Certificate Authority), you must create certificate requests and submit them to a CA.

You can create the certificate requests manually, or use the vCenter Certificate Automation Tool to generate certificate requests for each component. See VMware KB article 2061934 for detailed instruction on manual generation and replacement.

For increased security, generate each certificate and private key on the machine where it will be used.

NOTE This procedure explains how to prepare your CA-signed certificates. The tool also works with self-signed certificates.

Procedure

1 You can use the tool to generate the certificate requests for each of the following services if you are using them in your environment.

- vCenter Single Sign-On service
- vCenter Inventory Service
- vCenter Server
- vCenter Orchestrator
- vSphere Web Client
- vCenter Log Browser
- vCenter Update Manager

2 Submit the certificate requests to the CA that you are using.

The CA returns the generated certificates and keys.

3 When you later supply the certificates and keys to the tool, the tool generates the PFX and JKS files that are required by the vCenter Single Sign-On infrastructure and places them in the correct location.

What to do next

- Run the tool to generate update planner information.

Run the Update Planner

The update planner, part of the vCenter Certificate Automation Tool, allows you to determine the correct order for certificate replacement. Follow the steps in the order that the tool recommends for best results.

Procedure

1. Log into a machine on which the vCenter Certificate Automation Tool is installed.
2. From a command line, navigate to the location to which you unzipped the tool and run the following command.

   ```
   ssl-updater.bat
   ```

3. When prompted, select `1. Plan your steps to update SSL certificates`.
4. Enter the numbers that correspond to the services that you want to update.
   - To update more than one SSL certificate, separate the numbers with a comma. For example, to update the SSL certificates on vCenter Single Sign-On, vCenter Server, and the vSphere Web Client, type:**`1,3,4`**
   - To update the certificate on all services that are supported by the tool, type 8.

   The vSphere Web Client and the vCenter Log Browser always run on the same machine.

   NOTE Enter all of the services you intend to update. If you leave out some services initially and run the Update Planner again later, the steps might be incorrect and the update might fail.

   The Update Planner displays the tasks to perform and the order to perform them in.
5. Save the Update Planner output to a text file.

   Sample output for an environment where all certificates will be replaced is shown below.

   ```
   1. Go to the machine with Single Sign-On installed and
   - Update the Single Sign-On SSL certificate.

   2. Go to the machine with Inventory Service installed and
   - Update Inventory Service trust to Single Sign-On.

   3. Go to the machine with Inventory Service installed and
   - Update the Inventory Service SSL certificate.

   4. Go to the machine with vCenter Server installed and
   - Update vCenter Server trust to Single Sign-On.

   5. Go to the machine with vCenter Server installed and
   - Update the vCenter Server SSL certificate.

   6. Go to the machine with vCenter Server installed and
   - Update vCenter Server trust to Inventory Service.

   7. Go to the machine with Inventory Service installed and
   - Update the Inventory Service trust to vCenter Server.

   8. Go to the machine with vCenter Orchestrator installed and
   - Update vCenter Orchestrator trust to Single Sign-On.
   ```

```
9. Go to the machine with vCenter Orchestrator installed and
- Update vCenter Orchestrator trust to vCenter Server.

10. Go to the machine with vCenter Orchestrator installed and
- Update the vCenter Orchestrator SSL certificate.

11. Go to the machine with vSphere Web Client installed and
- Update vSphere Web Client trust to Single Sign-On.

12. Go to the machine with vSphere Web Client installed and
- Update vSphere Web Client trust to Inventory Service.

13. Go to the machine with vSphere Web Client installed and
- Update vSphere Web Client trust to vCenter Server.

14. Go to the machine with vSphere Web Client installed and
- Update the vSphere Web Client SSL certificate.

15. Go to the machine with Log Browser installed and
- Update the Log Browser trust to Single Sign-On.

16. Go to the machine with Log Browser installed and
- Update the Log Browser SSL certificate.

17. Go to the machine with vSphere Update Manager installed and
- Update the vSphere Update Manager SSL certificate.

18. Go to the machine with vSphere Update Manager installed and
- Update vSphere Update Manager trust to vCenter Server.
```

6 Type **9** to return to the main menu.

What to do next

Update certificates and trusts. See "Run the Tool to Update SSL Certificates and Trusts," on page 53.

Run the Tool to Update SSL Certificates and Trusts

After you obtain the SSL certificates and you generate the list of update steps, you can run the tool to replace the existing certificates, reestablish trust, and optionally restart some of the services.

See "Certificate Automation Tool Deployment Options," on page 45 for an overview of how the tool proceeds in different deployments.

The tool gives you a list of update tasks and specifies the machine on which to perform each task. If you select a task, the tool prompts for input to perform that task. For example, to update the Inventory Service, you select Inventory Service from the menu. The tool prompts you for information that it requires to update the Inventory Service Trust to Single Sign-On, and to update the Inventory Service SSL Certificate options.

Perform the tasks in sequence. If the update planner instructs you to perform tasks on multiple machines, keep the tool running on each machine to avoid entering information again.

Procedure

1 Move to the first machine on the task list and start the tool by running `ssl-updater.bat`.

The tool does not list machines by name but points you to the machine on which a service is running.

2 Select `Update SSL certificate`.

3 When prompted, specify the service whose certificate you want to update.

If you prespecified the default, the tool does not prompt you.

To update multiple SSL certificates, update the certificate for one service and then proceed to the next service on the machine where it is deployed. The SSL certificate for each vSphere component must be unique.

4 When prompted, type the requested information, such as the locations of the new SSL chain and private key, passwords and so on.

5 Continue until you have provided all information.

6 Check the planner for the next step.

You might have to deploy and start the tool on a different machine to update some of the services.

7 After you have completed your update plan, you can close the command prompt window to end your session.

Rolling Back Your Updates

Each update operation successfully performs the update for one certificate and key, or fails in a way that preserves the original state. If an update fails, you might need to roll back the failed step.

Before beginning the update process, the vCenter Certificate Automation Tool saves a copy of the existing certificate information in a backup folder, ensuring that you can roll back to the previously used certificate to keep the entire system up and running.

You can use the tool's menu item to let you roll back to the original.

NOTE After rolling back the vCenter Server certificate, you must update the vCenter Server trust to VMware Update Manager again.

Replace vCenter Server Appliance Certificates

You can replace vCenter Server Appliance certificates. Because the Certificate Automation Tool is supported only on Windows, you must replace the certificates by hand.

Replacing the default SSL certificate and key with a self-signed or CA-signed certificate on vCenter Server Appliance is a manual process. You cannot use the Certificate Automation Tool to update the certificate and key on Linux.

Prerequisites

Obtain certificate files (including the certificate and private key).

Procedure

- Follow the steps in VMware Knowledge Base article 2057223.

Replace vCenter Server Heartbeat Certificates

If you have a problem with the current certificate, or if your corporate security policy requires doing so, you can replace default vCenter ServerHeartbeat certificates.

Prerequisites

- Install OpenSSL on the system where you intend to replace the certificate.
- Obtain the certificate files `rui.crt`, `rui.key`, and `rui.pfx`.

Procedure

1 Download the `SSLImport.jar` utility from the VMware Knowledge Base article Replacing SSL Certificates for vCenter Server Heartbeat 6.x (KB 2013041).

2 Follow the steps in the knowledge base article to replace the certificate.

vSphere Users and Permissions

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.

vCenter Server allows fine-grained control over authorization with permissions and roles. Review first the background information about hierachical inheritance of permissions, permission validation, and related topics. You can then move on to vCenter Server User Management Tasks (Chapter 5, "vCenter User Management Tasks," on page 65).

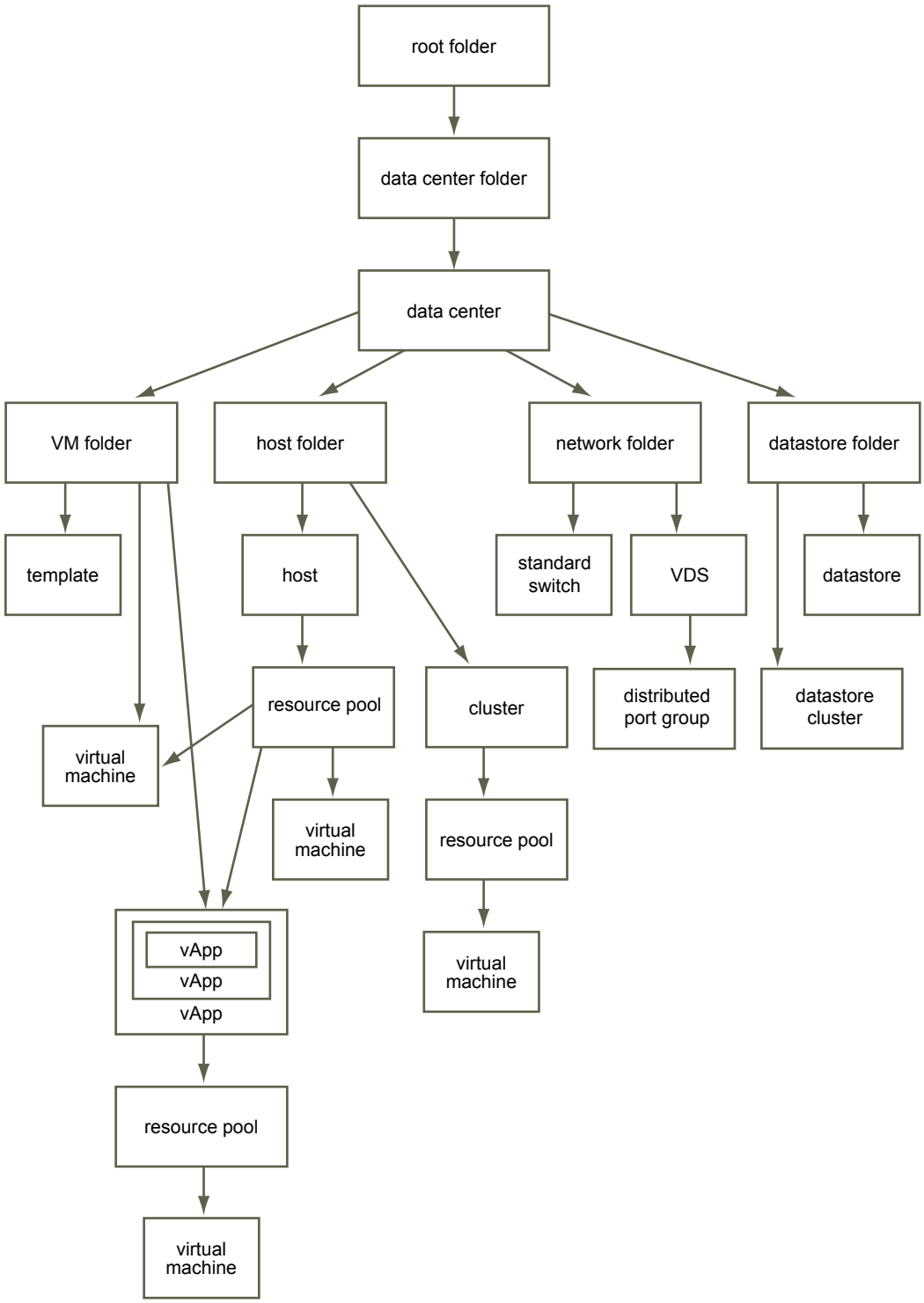
This chapter includes the following topics:

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 inventory hierarchy and the paths by which permissions can propagate.

Figure 4-1. 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 datacenter. Virtual machines inherit permissions from both the parent virtual machine folder and the parent host, cluster, or resource pool simultaneously. To restrict a user's privileges on a virtual machine, you must set permissions on both the parent folder and the parent host, cluster, or resource pool for that virtual machine.

To set permissions for a distributed switch and its associated distributed port groups, set permissions on a parent object, such a folder or datacenter. You must also select the option to propagate these permissions to child objects.

Permissions take several forms in the hierarchy:

Managed entities You can define permissions on managed entities.

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

Global entities Global entities derive permissions from the root vCenter Server system.

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

Permission Validation

vCenter Server and ESXi hosts that use Active Directory regularly validate users and groups against the Windows Active Directory domain. Validation occurs whenever the host system starts and at regular intervals specified in the vCenter Server settings.

For example, if user Smith was assigned permissions and in the domain the user's name was changed to Smith2, the host concludes that Smith no longer exists and removes permissions for that user when the next validation occurs.

Similarly, if user Smith is removed from the domain, all permissions 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 receives all the permissions the old user Smith was assigned.

Using Roles to Assign Privileges

A role is a predefined set of privileges. Privileges define individual rights that a user requires to perform actions and read properties.

When you assign permissions to a user or group, you pair the user or group with a role and associate that pairing with an inventory object. A single user might 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 might 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.

The roles created on a host are separate from the roles created on a vCenter Server system. When you manage a host using vCenter Server, the roles that are created through vCenter Server are available. If you connect directly to the host, the roles created directly on the host are available.

vCenter Server and ESXi hosts provide default system roles and sample roles:

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

Sample roles VMware provides sample roles for convenience as guidelines and suggestions. You can modify or remove these roles.

See "Roles in vCenter Server and ESXi," on page 68 for information on creating, cloning, and editing roles.

All roles permit the user to schedule tasks by default. Users can schedule only tasks they have permission to perform at the time the tasks are created.

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

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, grant permissions to groups rather than individual users.
- Grant permissions only where needed. 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 to correspond to the differing permissions you want to grant for them.
- Use caution when granting a permission at the root vCenter Server level. Users with permissions at the root level have access to global data on vCenter Server, such as roles, custom attributes, vCenter Server settings, and licenses. Changes to licenses and roles propagate to all vCenter Server systems in a Linked Mode group, even if the user does not have permissions on all of the vCenter Server systems in the group.

- In most cases, enable propagation on permissions. 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 masks specific areas of the hierarchy that you don't want particular users to have access to.

Required Privileges for Common Tasks

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

The following table lists common tasks that require more than one privilege. You can use the Applicable Roles on the inventory objects to grant permission to perform these tasks, or you can create your own roles with the equivalent required privileges.

Table 4-1. Required Privileges for Common Tasks

Task	Required Privileges	Applicable Role
Create a virtual machine	On the destination folder or datacenter: ■ **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 datacenter: ■ **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

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

Task	Required Privileges	Applicable Role
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
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

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

Task	Required Privileges	Applicable Role
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

Password Requirements

Password requirements differ for vCenter Server and for ESXi hosts.

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. See "Edit the vCenter Single Sign-On Password Policy," on page 23, or see the relevant Active Directory or OpenLDAP documentation.

ESXi Passwords

By default, ESXi enforces requirements for user passwords.

Your user password must meet the following length requirements.

- Passwords containing characters from one or two character classes must be at least eight characters long.
- 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 six characters long.

When you create a password, include a mix of characters from four character classes: lowercase letters, uppercase letters, numbers, and special characters such as an underscore or dash.

The password cannot contain the words root, admin, or administrator in any form.

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.

You can also use a passphrase, which is a phrase consisting of at least three words, each of which is 8 to 40 characters long.

Example: Creating Acceptable ESXi Passwords

The following password candidates meet the requirements of ESXi.

- xQaTEhbU: Contains eight characters from two character classes.
- xQaT3pb: Contains seven characters from three character classes.
- xQaT3#: Contains six characters from four character classes.

The following password candidates do not meet the requirements of ESXi.

- Xqat3hb: Begins with an uppercase character, reducing the effective number of character classes to two. Eight characters are required when you use only two character classes.
- xQaTEh2: Ends with a number, reducing the effective number of character classes to two. Eight characters are required when you use only two character classes.

vCenter Server User Directory Settings

You can limit the number of results returned when you search for users and groups and set a user directory timeout for vCenter Server.

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 permissions and in the domain the user's name was changed to Smith2, the host concludes that Smith no longer exists and removes permissions for that user when the next validation occurs.

Similarly, if user Smith is removed from the domain, all permissions 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 receives all the permissions the old user Smith was assigned.

vCenter User Management Tasks 5

Users in the vCenter environment must be authenticated, and they must be authorized to view and change vSphere objects. Administrators perform user management tasks from the vSphere Web Client.

This chapter includes the following topics:

Managing Permissions for vCenter Components

Permissions are access roles that consist of a user and the user's assigned role for an object such as a virtual machine or ESXi host. Permissions grant users the right to perform the activities specified by the role on the object to which the role is assigned.

For example, to configure memory for the host, you must grant a role to a user that includes the **Host.Configuration.Memory Configuration** privilege. By assigning different roles to users for different objects, you control the tasks that users can perform in your vSphere environment.

Users other than root and vpxuser initially have no permissions on any objects, which means they cannot view these objects or perform operations on them. A user with Administrator privileges must assign permissions to these users to allow them to perform tasks.

The list of privileges is the same for ESXi and vCenter Server. See Chapter 11, "Defined Privileges," on page 153 for a complete list of privileges.

Multiple Permissions

Many tasks require permissions on more than one object.

Permissions applied on a child object always override permissions that are applied on a parent object. Virtual machine folders and resource pools are equivalent levels in the hierarchy. If you assign propagating permissions to a user or group on a virtual machine's folder and its resource pool, the user has the privileges propagated from the resource pool and from the folder.

If multiple group permissions are defined on the same object and the 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.

Permission Examples

These 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.

Assign Permissions in the vSphere Web Client

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 at one time on multiple objects by moving the objects to a folder and setting the permissions on the folder.

Permissions assigned from the vSphere Web Client must match permissions, including case, in ActiveDirectory precisely. If you upgraded from earlier versions of vSphere, check for case inconsistencies if you experience problems with groups.

Prerequisites

Permissions.Modify permission on the parent object of the object whose permissions you want to modify.

Procedure

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

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

3 Click **Add Permission**.

4 Click **Add**.

5 Identify the user or group that will have the permission.

   a Select the domain where the user or group is located from the **Domain** drop-down menu.

   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 database.

   e Click **OK**.

6 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.

7 (Optional) 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.

8 Verify that the users and groups are assigned to the appropriate permissions and click **OK**.

The server adds the permission to the list of permissions for the object.

The list of permissions references all users and groups that have roles assigned to the object and indicates where in the vCenter Server hierarchy the role is assigned.

Change Permissions in the vSphere Web Client

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 in the vSphere Web Client

Removing a permission for a user or group does not remove the user or group from the list of those available. It also does not remove the role from the list of available items. It removes the user or group and role pair from the selected inventory 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 in the vSphere Web Client

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.

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 (Optional) Deselect the **Validation** check box to disable validation.

Validation is enabled by default. Users and groups are validated when vCenter Server system starts, even if validation is disabled.

6 (Optional) If validation is enabled, enter a validation period to specify a time, in minutes, between validations.

7 Click **OK**.

Roles in vCenter Server and ESXi

vCenter Server grants access to an object only to users who are assigned permissions for the object. When you assign a user permissions for the object, you pair the user with a role. A role is a predefined set of privileges.

vCenter Server provides three 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 default roles.

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

vCenter Server Custom Roles (Recommended)	You can create custom roles by using the role-editing facilities in the vSphere Web Client to create privilege sets that match your user needs.
ESXi Custom Roles	You can create custom roles for individual hosts by using a CLI or the vSphere Client. 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.

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**.

Create a Role in the vSphere Web Client

VMware recommends that you create 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 a connected group in Linked Mode, the changes that you make are propagated to all other vCenter Server systems in the group. Assignments of roles to specific users and objects are not shared across linked vCenter Server systems.

Prerequisites

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

Procedure

1 Browse to **Administration > Role Manager** in the vSphere Web Client.

2 Select a vCenter Server system from the drop-down menu.

3 Click **Create role action**.

4 Type a name for the new role.

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

Edit a Role in the vSphere Web Client

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 a connected group in Linked Mode, the changes you make are propagated to all other vCenter Server systems in the group. Assignments of roles to specific users and objects are not shared across linked vCenter Server systems.

Prerequisites

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

Procedure

1 Browse to **Administration > Role Manager** in the vSphere Web Client.

2 Select a vCenter Server system from the drop-down menu.

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

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

Clone a Role in the vSphere Web Client

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 a connected group in Linked Mode, the changes you make are propagated to all other vCenter Server systems in the group. Assignments of roles to specific users and objects are not shared across linked vCenter Server systems.

Prerequisites

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

Procedure

1 Browse to **Administration > Role Manager** in the vSphere Web Client.

2 Select a vCenter Server system from the drop-down menu.

3 Click **Clone role action**.

4 Type a name for the cloned role.

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

Adjust the Search List in Large Domains in the vSphere Web Client

If you have domains with thousands of users or groups, or if searches take a long time to complete, adjust the search settings.

NOTE This procedure applies only to vCenter Server user lists. ESXi host 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 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**.

6 Securing vCenter Server Systems

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:

Hardening the vCenter Server Host Operating System

Protect the host where vCenter Server is running against vulnerabilities and attacks by ensuring that the operating system of the host (Windows or Linux) 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*.

Best Practices for vCenter Server Privileges

Strictly control vCenter Server administrator privileges to increase security for the system.

- Full administrative rights to vCenter Server should be removed from the local Windows administrator account and granted to a special-purpose local vCenter Server administrator account. Grant full vSphere 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.

- Avoid allowing users to log in directly to the vCenter Server system. Allow only those users who have legitimate tasks to perform to log into the system and ensure that these events are audited.
- Install vCenter Server using a service account instead of a Windows account. You can use a service account or a Windows account to run vCenter Server. Using a service account allows you to enable Windows authentication for SQL Server, which provides more security. The service account must be an administrator on the local machine.
- 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 of the server cannot be verified as a valid user or group, the Administrator privileges are removed and assigned to the local Windows Administrators group.
- Grant minimal privileges to the 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 can be removed after the product is installed or upgraded.

Restrict Use of the Administrator Privilege

By default, vCenter Server grants full administrator privileges to the administrator of the local system, which can be accessed by domain administrators. To minimize risk of this privilege being abused, remove administrative rights from the local operating system's administrator account and assign these rights to a special-purpose local vSphere administrator account. Use the local vSphere account to create individual user accounts.

Grant the Administrator privilege only to administrators who are required to have it. Do not grant the privilege to any group whose membership is not strictly controlled.

Procedure

1. Create a user account that you will use to manage vCenter Server (for example, vi-admin).

   Ensure that the user does not belong to any local groups, such as the Administrators group.
2. Log into the vCenter Server system as the local operating system administrator and grant the role of global vCenter Server administrator to the user account you created (for example, vi-admin).
3. Log out of vCenter Server and log in with the user account you created (vi-admin).
4. Verify that the user can perform all tasks available to a vCenter Server administrator.
5. Remove the administrator privileges that are assigned to the local operating system administrator user or group.

Restrict Use of the Administrator Role

Secure the vCenter Server Administrator role and assign it only to certain users.

Protect the vCenter Server administrator user from regular use by relying on user accounts associated with specific individuals.

Prerequisites

- Create a user account to manage vCenter Server and assign full vCenter Server administrator privileges to the user. See "Managing Permissions for vCenter Components," on page 65.
- Remove vCenter Server administrator privileges from the local operating system administrator.

Procedure

1. Log in to the vCenter Server system as the vCenter Server administrator you created (for example, vi-admin).
2. Grant full administrator privileges to the minimum number of individuals required.

3 Log out as the vCenter Server administrator.

What to do next

Protect the vCenter Server administrator account password. For example, create a password with two halves, each half of which is known to only one person, or lock a printout of the password in a safe.

Enable Certificate Checking and Verify Host Thumbprints in the vSphere Web Client

To prevent man-in-the-middle attacks and to fully use the security that certificates provide, certificate checking is enabled by default. You can verify that certificate checking is enabled in the vSphere Web Client.

NOTE vCenter Server certificates are preserved across upgrades.

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** and verify that **vCenter requires verified host SSL certificates** is selected.

5 If there are hosts that 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**.

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 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.

Enable SSL Certificate Validation Over Network File Copy

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. You can disable and reenable SSL certificate validation for NFC operations.

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 datacenter.

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**.

Limiting vCenter Server Network Connectivity

For improved security, avoid putting the vCenter Server system on any network other than the 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 the 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 (linked mode only)
- 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 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.

Restricting the Use of Linux Clients

Communications between client components and vCenter Server system or ESXi hosts are protected by SSL-based encryption by default. Linux versions of these components do not perform certificate validation, so you should restrict the use of these clients.

Even if you have replaced the self-signed certificates on the vCenter Server system and the ESXi hosts with legitimate certificates signed by your local root certificate authority or a third party CA, 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 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.

Verifying the Integrity of the vSphere Web Client

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, do not install any vSphere Web Client plug-ins that do not come from a trusted source.

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 server. 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.

Remove the tcdump Package from the vCenter Server Virtual Appliance

By default, the vCenter Server virtual appliance includes the tcdump package. You can remove that package if security considerations require it.

The tcpdump package allows administrators to analyze TCP packets for troubleshooting and testing. However, in some situations security considerations require a removal of the package. For example, you must remove the package to ensure compliance with GEN003865 in the DIS STIG, run the following command as root to remove the tcpdump package from the system:

Procedure

1 Log in to the vCenter Server Virtual Appliance as root.

2 Run the following command.

```
rpm –e tcpdump
```

Securing ESXi Hosts 7

Restricting access to the services and ports on an ESXi host is critical to protecting against unauthorized intrusion in your vSphere environment.

If a host is compromised, the virtual machines on that host are now threatened to be compromised as well. Restrict access to services and ports, an ESXi host is protected with a firewall. Using the ESXi lockdown mode and limiting access to the ESXi Shell can further contribute to a more secure environment.

This chapter includes the following topics:

General ESXi Security Recommendations

To protect the 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.

Consider the following recommendations when evaluating host security and administration.

- Limit user access.

To improve security, restrict user access to the Direct Console User Interface (DCUI) and the ESXi Shell and enforce access security policies, for example, by setting up password restrictions.

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

- Use the vSphere Client to administer standalone ESXi hosts.

  Whenever possible, use the vSphere Client or a third-party network management tool to administer your ESXi hosts instead of working though the command-line interface as the root user. Using the vSphere Client lets you limit the accounts with access to the ESXi Shell, safely delegate responsibilities, and set up roles that prevent administrators and users from using capabilities they do not need.

- 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.

- 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.

In addition to implementing the firewall, risks to the hosts are mitigated using other methods.

- ESXi runs only services essential to managing its functions, and 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 all 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, always avoid using these insecure services in favor of their safer alternatives. For example, use Telnet with SSL instead of Telnet to access virtual serial ports. If you must use insecure services and have implemented sufficient protection for the host, you must explicitly open ports to support them.

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

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. The managed object browser lets you change the host configuration. This interface is used primarily for debugging the vSphere Web Services SDK.

Procedure

1 Connect directly to the host using the ESXi Shell.

2 (Optional) Determine if the managed object browser (MOB) is enabled by running the following command.

```
vim-cmd proxysvc/service_list
```

If the service is running, the following text appears in the list of services:

```
...
serverNamespace = '/mob',
accessMode = "httpsWithRedirect",
pipeName = "/var/run/vmware/proxy-mob",
...
```

3 Disable the service by running the following command.

```
vim-cmd proxysvc/remove_service "/mob" "httpsWithRedirect"
```

Changes are effective immediately and persist across reboots.

The managed object browser is no longer available for diagnostics. Some third-party tools use this interface to gather information.

What to do next

After you disable the managed object browser, perform tests to verify that third-party applications still function as expected.

To reenable the service, run the following command.

```
vim-cmd proxysvc/add_np_service "/mob" httpsWithRedirect /var/run/vmware/proxy-mob
```

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.

Configure SSL Timeouts

You can configure SSL timeouts for ESXi by editing a configuration file on the ESXi host.

Timeout periods can be set for two types of idle connections:

- The Read Timeout setting applies to connections that have completed the SSL handshake process with port 443 of ESXi.

- The Handshake Timeout setting applies to connections that have not completed the SSL handshake process with port 443 of ESXi.

Both connection timeouts are set in milliseconds.

Idle connections are disconnected after the timeout period. By default, fully established SSL connections have a timeout of infinity.

Procedure

1 Log in to the ESXi Shell as a user with administrator privileges.

2 Change to the directory `/etc/vmware/rhttpproxy/`.

3 Use a text editor to open the `config.xml` file.

4 Enter the `<readTimeoutMs>` value in milliseconds.

For example, to set the Read Timeout to 20 seconds, add the following line.

```
<readTimeoutMs>20000</readTimeoutMs>
```

5 Enter the `<handshakeTimeoutMs>` value in milliseconds.

For example, to set the Handshake Timeout to 20 seconds, add the following line.

```
<handshakeTimeoutMs>20000</handshakeTimeoutMs>
```

6 Save your changes and close the file.

7 Restart the `rhttpproxy` process:

```
/etc/init.d/rhttpproxy restart
```

Example: Configuration File

The following section from the file `/etc/vmware/rhttpproxy/config.xml` shows where to add the SSL timeout settings.

```
<vmacore>
 ...
 <http>
    ...
  <readTimeoutMs>20000</readTimeoutMs>
    ...
 </http>
 ...
 <ssl>
  ...
  <handshakeTimeoutMs>20000</handshakeTimeoutMs>
  ...
    </ssl>
</vmacore>
```

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 plugins 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 Community Supported 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
```

Add an ESXi Host to an Active Directory Domain

Because ESXi does not support vCenter Single Sign-On, it does not support the identity sources you set up with vCenter Single Sign-On. You can add an ESXi host to an Active Directory Domain from the vSphere Web Client.

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 **Join Domain**, supply the domain settings, and click **OK**.

ESXi Firewall Configuration

ESXi includes a firewall between the management interface and the network. The firewall is enabled by default.

At installation time, the ESXi firewall is configured to block incoming and outgoing traffic, except traffic for the default services listed in "TCP and UDP Ports," on page 132.

NOTE The firewall also allows Internet Control Message Protocol (ICMP) pings and communication with DHCP and DNS (UDP only) clients.

Supported services and management agents that are required to operate the host are described in a rule set configuration file in the ESXi firewall directory `/etc/vmware/firewall/`. The file contains firewall rules and lists each rule's relationship with ports and protocols.

You cannot add a rule to the ESXi firewall unless you create and install a VIB that contains the rule set configuration file. The VIB authoring tool is available to VMware partners.

NOTE 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 Rule Set Behavior," on page 84 for more information.

Rule Set Configuration Files

A rule set configuration file contains firewall rules and describes each rule's relationship with ports and protocols. The rule set configuration file can contain rule sets for multiple services.

Rule set configuration files are located in the `/etc/vmware/firewall/` directory. To add a service to the host security profile, VMware partners can create a VIB that contains the port rules for the service in a configuration file. VIB authoring tools are available to VMware partners.

A VMware Fling of the `vibauthor` tool allows all users to create VIBs. To add a VIB at the customer-supported acceptance level to your ESXi host, you must first lower the host's acceptance level. A lowered host acceptance level might affect your support contract. See the *Installation and Setup* documentation.

The ESXi 5.x ruleset.xml format is the same as in ESX and ESXi 4.x, but has two additional tags: enabled and required. The ESXi 5.x firewall continues to support the 4.x ruleset.xml format.

Each set of rules for a service in the rule set configuration file contains the following information.

- A numeric identifier for the service, if the configuration file contains more than one service.
- A unique identifier for the rule set, usually the name of the service.
- For each rule, the file contains one or more port rules, each with a definition for direction, protocol, port type, and port number or range of port numbers.
- A flag indicating whether the service is enabled or disabled when the rule set is applied.
- An indication of whether the rule set is required and cannot be disabled.

Example: Rule Set Configuration File

```
<ConfigRoot>
<service id='0000'>
 <id>serviceName</id>
  <rule id = '0000'>
   <direction>inbound</direction>
   <protocol>tcp</protocol>
   <porttype>dst</porttype>
   <port>80</port>
```

```
  </rule>
  <rule id='0001'>
   <direction>inbound</direction>
   <protocol>tcp</protocol>
   <porttype>src</porttype>
   <port>
    <begin>1020</begin>
    <end>1050</end>
   </port>
 </rule>
 <enabled>true</enabled>
    <required>false</required>
</service>
</ConfigRoot>
```

Allow or Deny Access to an ESXi Service or Management Agent with the vSphere Web Client

You can configure firewall properties to allow or deny access for a service or management agent.

You add information about allowed services and management agents to the host configuration file. You enable or disable these services and agents in the vSphere Web Client or at the command line.

NOTE If different services have overlapping port rules, enabling one service might implicitly enable overlapping services. To minimize the effects of this behavior, you can specify which IP addresses are allowed to access each service on the host.

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**.

5 Select the rule sets to enable, or deselect the rule sets to disable.

The Incoming Ports and Outgoing Ports columns indicate the ports that the vSphere Web Client opens for the service. The Protocol column indicates the protocol that the service uses. The Daemon column indicates the status of daemons associated with the service.

6 Click **OK**.

Add Allowed IP Addresses in the vSphere Web Client

You can specify which networks are allowed to connect to each service that is running on the host.

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.

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**.

NFS Client Rule Set Behavior

The NFS Client rule set behaves differently than other ESXi firewall rule sets. ESXi configures NFS Client settings when you mount or unmount an NFS datastore.

When you add or mount an NFS datastore, ESXi checks the state of the NFS Client (`nfsClient`) firewall rule set.

- If the NFS Client 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 NFS Client 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.

When you remove or unmount an NFS datastore, ESXi performs one of the following actions.

- If ESXi is mounted on any NFS datastore, the IP address of the unmounted NFS server is removed from the list of allowed outgoing IP addresses and the NFS Client rule set remains enabled.
- If ESXi is not mounted on any NFS datastore, the IP address of the unmounted NFS server is removed from the list of allowed outgoing IP addresses and the NFS Client rule set is disabled.

NOTE If you manually enable the NFS Client rule set or manually set the Allow All IP Addresses policy, either before or after you add an NFS datastore to the system, your settings are overridden when the last NFS datastore is unmounted. The NFS Client rule set is disabled when all NFS datastores are unmounted.

Automating Service Behavior Based on Firewall Settings

ESXi can automate whether services start based on the status of firewall ports.

Automation helps ensure that services start if the environment is configured to enable their function. For example, starting a network service only if some ports are open can help avoid the situation where services are started, but are unable to complete the communications required to complete their intended purpose.

In addition, having accurate information about the current time is a requirement for some protocols, such as Kerberos. The NTP service is a way of getting accurate time information, but this service only works when required ports are opened in the firewall. The service cannot achieve its goal if all ports are closed. The NTP services provide an option to configure the conditions when the service starts or stops. This configuration includes options that account for whether firewall ports are opened, and then start or stop the NTP service based on those conditions. Several possible configuration options exist, all of which are also applicable to the SSH server.

NOTE The settings described in this section only apply to service settings configured through the vSphere Web Client or applications created with the vSphere Web services SDK. Configurations made through other means, such as the ESXi Shell or configuration files in `/etc/init.d/`, are not affected by these settings.

- **Start automatically if any ports are open, and stop when all ports are closed**: The default setting for these services that VMware recommends. If any port is open, the client attempts to contact the network resources pertinent to the service in question. If some ports are open, but the port for a particular service is closed, the attempt fails, but there is little drawback to such a case. If and when the applicable outgoing port is opened, the service begins completing its tasks.
- **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 ESXi firewall automates when rule sets are enabled or disabled based on the service startup policy. When a service starts, its corresponding rule set is enabled. When a service stops, the rule set is disabled.

ESXi Firewall Commands

You can configure the ESXi firewall at the command line.

Firewall Configuration Using the ESXi Shell

The vSphere Web Client graphical user interface provides the preferred means of performing many configuration tasks. However, you can use the ESXi Shell or vSphere CLI commands to configure ESXi at the command line if necessary. See *Getting Started with vSphere Command-Line Interfaces*

Table 7-1. Firewall Commands

Command	Description
`esxcli network firewall get`	Returns 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.

Table 7-1. Firewall Commands (Continued)

Command	Description
`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.

Assigning Permissions for ESXi

ForESXi, permissions are defined as access roles that consist of a user and the user's assigned role for an object such as a virtual machine or ESXi host. Permissions grant users the right to perform the activities specified by the role on the object to which the role is assigned.

The *vSphere Single Host Management* document explains how you can perform permission validation and assign and remove permissions with the vSphere Client. This document discusses the different types of permissions.

Specify Users with DCUI Access in Lockdown Mode

You can specify which users can log into a host that is lockdown mode. DCUI Access users do not need to have full administrative privileges on the host. You grant the DCUI Access privilege in Advanced Settings in the vSphere Web Client.

In versions of vSphere earlier than vSphere 5.1, the root user can log into the DCUI on a host that is in lockdown mode. In vSphere 5.1, you can specify which local ESXi users are allowed to log in to the DCUI when the host is in lockdown mode. These special users do not need to have full administrative privileges on the host. Specifying users other than the anonymous root user allows you to log which users have performed operations on the host while it is in lockdown mode.

IMPORTANT When you disable lockdown mode using the DCUI, all users with the DCUI Access privilege are granted the Administrator role on the host.

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 the setting **DCUI.Access**.

4 Click **Edit** and enter the user names, separated by commas.

By default, the root user is specified. You can remove root from the list of DCUI access users, as long as you specified at least one other user.

5 Click **OK**.

Multiple Permission Settings

Objects might have multiple permissions, but only one permission for each user or group.

Permissions applied on a child object always override permissions that are applied on a parent object. Virtual machine folders and resource pools are equivalent levels in the hierarchy. If you assign propagating permissions to a user or group on a virtual machine's folder and its resource pool, the user has the privileges propagated from the resource pool and from the folder.

If multiple group permissions are defined on the same object and the 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

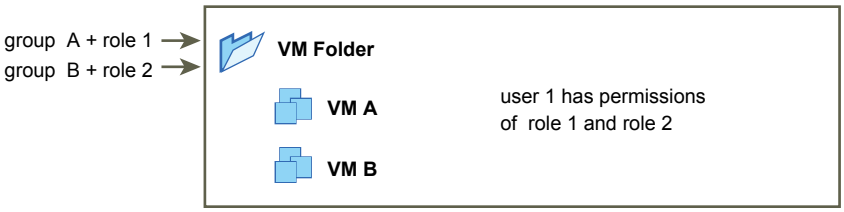
This example illustrates how an object can inherit multiple permissions from groups that are granted permission on a parent object.

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 permission.

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 7-1. Example 1: Inheritance of Multiple Permissions



Example 2: Child Permissions Overriding Parent Permissions

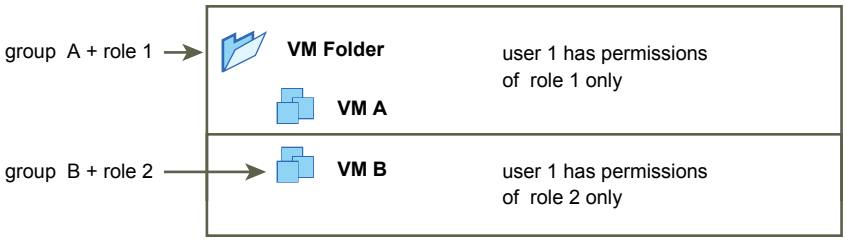
This example illustrates how permissions that are assigned on a child object can override permissions that are assigned on a parent object. You can use this overriding behavior to restrict user access to particular areas of the inventory.

In this example, permissions are assigned to two different groups on two different objects.

- 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 7-2. Example 2: Child Permissions Overriding Parent Permissions



Example 3: User Permissions Overriding Group Permissions

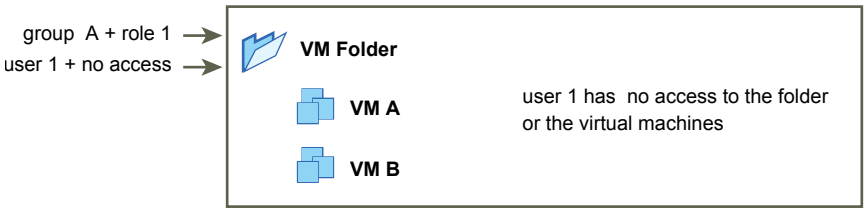
This example illustrates how permissions assigned directly to an individual user override permissions assigned to a group that the user is a member of.

In this example, permissions are assigned to a user and to a group on the same object.

- 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 group permission. User 1 has no access to VM Folder or VMs A and B.

Figure 7-3. Example 3: User Permissions Overriding Group Permissions



root User Permissions

Create a non-root user account for local admin access.

By default each ESXi host has a single root user account with full administrator privileges that can be used for local administration and to connect the host to vCenter Server. Sharing a common root account can make it easier to break into an ESXi host.

Create at least one named user account and assign it full administrative privileges 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 user itself.)

IMPORTANT If you remove the access permissions for the root user, you must first create another permission at the root level that has a different user assigned to the Administrator role.

NOTE In vSphere 5.1 and later, only the root user and no other user with administrator privileges is permitted to add a host to vCenter Server.

Assigning the Administrator role to a different user helps you maintain security through traceability. The vSphere Client logs all actions that the Administrator role user initiates as events, providing you with an audit trail. If all administrators log in as the root user, you cannot tell which administrator performed an action. If you create multiple permissions at the root level—each associated with a different user—you can track the actions of each administrator.

vpxuser Permissions

The vpxuser permission is used for vCenter Server when managing activities for the host. The vpxuser is created when a host is attached to vCenter Server.

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 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 Permissions

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.

Configure a Host to Use Active Directory in the vSphere Web Client

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 all user and group accounts are assigned full administrative access to the host if the group ESX Admins exists. If you do not want to make full administrative access available, see VMware Knowledge Base article 1025569 for a workaround.

NOTE When you define user account settings in Active Directory, you can limit the computers that a use 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 GUID-B77341E3-9D7D-48B6-A221-B782C21AF98E#GUID-B77341E3-9D7D-48B6-A221-B782C21AF98E or the VMware Knowledge Base for information about how to synchronize ESXi time with a Microsoft Domain Controller.

2 Ensure that the DNS servers 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.

Add a Host to a Directory Service Domain in the vSphere Web Client

To 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 "Use vSphere Authentication Proxy to Add a Host to a Domain in the vSphere Web Client," on page 106.

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 Click **OK** to close the Directory Services Configuration dialog box.

View Directory Service Settings in the vSphere Web Client

You can view the type of directory server, if any, 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.

Replacing ESXi SSL Certificates and Keys

Your company's security policy might require that you replace the default ESXi SSL certificate with trusted a certificate on each host. You can also regenerate a self-signed certificate and key if the default certificate and key were accidentally deleted.

SSL certificates are used to vouch for the identity of the components involved in the communication and to secure communication between vSphere components.

By default, vSphere components use the self-signed certificate and key that are created during installation. Self-signed certificates are as secure as certificates that are issued by an external Certificate Authority as long as the user validates the certificate and its thumbprint when the warning dialog appears.

Replace self-signed certificates with certificates from a trusted CA, either a commercial CA or an organizational CA, if company policy requires it. Consider also replacing certificates to avoid having users get used to clicking through browser warnings. The warning might be an indication of a man-in-the-middle attack, and only inspection of the certificate and thumbprint can guard against such attacks.

You can replace the default certificates with trusted certificates in a number of ways.

- "Replace a Default ESXi Certificate and Key from the ESXi Shell," on page 92
- "Replace a Default ESXi Certificate and Key by Using the vifs Command," on page 93
- "Replace a Default ESXi Certificate and Key Using HTTPS PUT," on page 94

If you accidentally deleted the default self-signed certificate and key or you changed the host name, you can generate a new self-signed certificate and key from the ESXi Shell. See "Generate New Self-Signed Certificates for ESXi," on page 92.

Preparing Your Environment for ESXi Certificate Replacement

If you plan to replace the default certificate and key with a certificate and key from a certificate authority, ensure that your environment has the required software installed.

Your environment does not have to meet these requirements if you use self-signed certificates.

- Microsoft CA (2000 or higher), with Web Server template
- Microsoft Visual C++ 2008 Redistributable Package (x86) installed on the system where you will generate the certificate-signing request
- OpenSSL 0.98r or higher installed on the system where you will generate the certificate-signing request
- Putty or other SSH client (recommended)
- WinSCP or other SFTP/SCP client
- vCenter Server

- ESXi 5.1 or later

Generate New Self-Signed Certificates for ESXi

You typically generate new certificates only if you change the host name or accidentally delete the certificate. Under certain circumstances, you must force the host to generate new certificates.

NOTE To receive the full benefit of certificate checking, particularly if you intend to use encrypted remote connections externally, do not use a self signed certificate. Instead, install new certificates that are signed by a valid internal certificate authority or purchase a certificate from a trusted security authority.

Procedure

1. Log in to the ESXi Shell as a user with administrator privileges.
2. In the directory `/etc/vmware/ssl`, back up any existing certificates by renaming them using the following commands.

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

   NOTE If you are regenerating certificates because you have deleted them, this step is unnecessary.
3. Run the command `/sbin/generate-certificates` to generate new certificates.
4. Restart the host.

   Generating the certificates places them in the correct location. You can alternatively put the host into maintenance mode, install the new certificate, and then use the Direct Console User Interface (DCUI) to restart the management agents.
5. Confirm that the host successfully generated new certificates by using the following command and comparing the time stamps of the new certificate files with `orig.rui.crt` and `orig.rui.key`.

   ```
   ls -la
   ```

What to do next

Consider replacing the self-signed certificate and key with a trusted certificate and key.

Replace a Default ESXi Certificate and Key from the ESXi Shell

ESXi uses automatically generated certificates that are created as part of the installation process. These certificates are unique and make it possible to begin using the server, but they are not verifiable and they are not signed by a trusted certificate authority (CA). This topic explains how to replace the default certificates with self-signed or CA-signed certificates.

Using default certificates might not comply with the security policy of your organization. If you require a certificate from a trusted certificate authority, you can replace the default certificate.

NOTE If the host has Verify Certificates enabled, replacing the default certificate might cause vCenter Server to stop managing the host. Disconnect and reconnect the host if vCenter Server cannot verify the new certificate.

ESXi supports only X.509 certificates to encrypt session information sent over SSL connections between server and client components.

Prerequisites

- If you want to use CA-signed certificates, generate the certificate request, send it to the certificate authority, and store the certificates you receive in a location that the host can access.

- 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 96.
- 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 ESXi privileges, see the *vSphere Single Host Management* publication.

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 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.

Replace a Default ESXi Certificate and Key by Using the vifs Command

ESXi uses automatically generated certificates that are created as part of the installation process. These certificates are unique and make it possible to begin using the server, but they are not verifiable and they are not signed by a trusted certificate authority (CA).

Using default certificates might not comply with the security policy of your organization. If you require a certificate from a trusted certificate authority, you can replace the default certificate.

NOTE If the host has Verify Certificates enabled, replacing the default certificate might cause vCenter Server to stop managing the host. Disconnect and reconnect the host if vCenter Server cannot verify the new certificate.

ESXi supports only X.509 certificates to encrypt session information sent over SSL connections between server and client components.

Prerequisites

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 ESXi privileges, see the *vSphere Single Host Management* publication.

Procedure

1. Back up the existing certificates.
2. Generate a certificate request following the instructions from the certificate authority.
3. At the command line, use the `vifs` command to upload the certificate to the appropriate location on the host.

   ```
   vifs --server hostname --username username --put rui.crt /etc/vmware/ssl
   ```

   ```
   vifs --server hostname --username username --put rui.key /etc/vmware/ssl
   ```

4 Restart the host.

Alternatively, you can put the host into maintenance mode, install the new certificate, and then use the Direct Console User Interface (DCUI) to restart the management agents.

Replace a Default ESXi Certificate and Key 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.

Procedure

1 In your upload application, open the file.

2 Publish the file to one of these locations.

Option	Description
Certificates	`https://hostname/host/ssl_crt`
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 In the Direct Console User Interface (DCUI), use the Restart Management Agents operation to initiate the settings.

Uploading an SSH Key to Your ESXi Host

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 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 79.

NOTE A user with an SSH key can access the host even when the host is in lockdown mode.

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 one of these 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/host/ssh_host_dsa_key_pub`
RSA keys	`https://hostname or ip/host/ssh_host_rsa_key`
RSA public keys	`https://hostname or ip/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.

ESXi Shell	Enable this service to access the ESXi Shell locally.
SSH	Enable this service to access the ESXi Shell remotely using SSH.
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 it is required.

- Use the vSphere Web Client to Enable Access to the ESXi Shell on page 96

  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 98

  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 99

  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.

- SSH Security on page 100

  You can use SSH to remotely log in to the ESXi Shell and perform troubleshooting tasks for the host.

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 "Uploading an SSH Key to Your ESXi Host," on page 94.

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 97 and "Create a Timeout for Idle ESXi Shell Sessions in the vSphere Web Client," on page 97

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 users 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 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.

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 98 and "Create a Timeout for Idle ESXi Shell Sessions," on page 99.

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.

Procedure

1 From the Troubleshooting Mode Options menu, select **Modify ESXi Shell and SSH timeouts** and press Enter.

2 Enter the idle timeout, in minutes.

   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 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.

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.

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.

Lockdown Mode

To increase the security of your ESXi hosts, you can put them in lockdown mode. In lockdown mode, all operations must be performed through vCenter Server. Only the vpxuser user has authentication permissions, no other users can perform operations against the host directly.

When a host is in lockdown mode, you cannot run vSphere CLI commands from an administration server, from a script, or from vMA against the host. External software or management tools might not be able to retrieve or modify information from the ESXi host.

Note Users can be assigned DCUI access privileges explicitly via the DCUI Access advanced configuration option. The option has DCUI.Access as the key, and a comma-separated list of ESXi users as the value. Users in the list which can access the DCUI at any time, even if these users are not administrators (Admin role), and even when the host is in lockdown mode.

Enabling or disabling lockdown mode affects which types of users are authorized to access host services, but it does not affect the availability of those services. In other words, if the ESXi Shell, SSH, or Direct Console User Interface (DCUI) services are enabled, they will continue to run whether or not the host is in lockdown mode.

You can enable lockdown mode using the Add Host wizard to add a host to vCenter Server, using the vSphere Web Client to manage a host, or using the Direct Console User Interface (DCUI).

Note If you enable or disable lockdown mode using the Direct Console User Interface (DCUI), permissions for users and groups on the host are discarded. To preserve these permissions, you must enable and disable lockdown mode using the vSphere Web Client connected to vCenter Server.

Lockdown mode is available only on ESXi hosts that have been added to vCenter Server.

Lockdown Mode Behavior

Enabling lockdown mode affects which users are authorized to access host services.

Users Logged in When Lockdown Mode Is Enabled

Users who were logged in to the ESXi Shell before lockdown mode was enabled remain logged in and can run commands. However, these users cannot disable lockdown mode. No other users, including the root user and users with the Administrator role on the host, can use the ESXi Shell to log in to a host that is in lockdown mode.

Access Through vCenter Server

Users with administrator privileges on the vCenter Server system can use the vSphere Web Client to disable lockdown mode for hosts that are managed by the vCenter Server system.

Access From the DCUI

Users granted the DCUI Access privilege can always log directly in to the host using the Direct Console User Interface (DCUI) to disable lockdown mode, even if the user does not have the Administrator role on the host. You must use Advanced Settings to grant the DCUI Access privilege.

NOTE When you disable lockdown mode using the DCUI, all users with the DCUI Access privilege are granted the Administrator role on the host.

Root users or users with the Administrator role on the host cannot log directly in to the host with the DCUI if they have not been granted the DCUI Access privilege. If the host is not managed by vCenter Server or if the host is unreachable, only DCUI Access users can log into the DCUI and disable lockdown mode. If the DCUI service is stopped, you must reinstall ESXi.

Lockdown Mode Services for Different Users

The following table shows the services that are are available to different types of users when the host is running in lockdown mode and in normal mode. As a rule, changes can be made only through vCenter Server. The root user can make changes from the Direct Console Interface, but not from the ESXi Shell or through an SSH session.

Table 7-2. Lockdown Mode Behavior

Service	Normal Mode	Lockdown Mode
vSphere WebServices API	All users, based on ESXi permissions	vCenter only (vpxuser)
CIM Providers	Root users and users with Admin role on the host	vCenter only (ticket)
Direct Console UI (DCUI)	Root users and users with Admin role on the host	Root users
ESXi Shell	Root users and users with Admin role on the host	No users
SSH	Root users and users with Admin role on the host	No users

Lockdown Mode Configurations

You can enable or disable remote and local access to the ESXi Shell to create different lockdown mode configurations.

The following table lists which services are enabled for three typical configurations.

CAUTION If you lose access to vCenter Server while running in Total Lockdown Mode, you must reinstall ESXi to gain access to the host.

Table 7-3. Lockdown Mode Configurations

Service	Default Configuration	Recommended Configuration	Total Lockdown Configuration
Lockdown	Off	On	On
ESXi Shell	Off	Off	Off

Table 7-3. Lockdown Mode Configurations (Continued)

Service	Default Configuration	Recommended Configuration	Total Lockdown Configuration
SSH	Off	Off	Off
Direct Console UI (DCUI)	On	On	Off

Enable Lockdown Mode Using the vSphere Web Client

Enable lockdown mode to require that all configuration changes go through vCenter Server. You can also enable or disable lockdown mode through the Direct Console User Interface (DCUI).

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 Select **Enable Lockdown Mode**.

6 Click **OK**.

Enable Lockdown Mode from the Direct Console User Interface

You can enable lockdown mode from the Direct Console User Interface (DCUI).

NOTE If you enable or disable lockdown mode using the Direct Console User Interface, permissions for users on the host are discarded. To preserve these permissions, you must enable and disable lockdown mode using a vSphere Web Client connected to vCenter Server.

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.

3 Press Esc until you return to the main menu of the Direct Console User Interface.

Specify Users with DCUI Access in Lockdown Mode

You can specify which users can log into a host that is lockdown mode. DCUI Access users do not need to have full administrative privileges on the host. You grant the DCUI Access privilege in Advanced Settings in the vSphere Web Client.

In versions of vSphere earlier than vSphere 5.1, the root user can log into the DCUI on a host that is in lockdown mode. In vSphere 5.1, you can specify which local ESXi users are allowed to log in to the DCUI when the host is in lockdown mode. These special users do not need to have full administrative privileges on the host. Specifying users other than the anonymous root user allows you to log which users have performed operations on the host while it is in lockdown mode.

IMPORTANT When you disable lockdown mode using the DCUI, all users with the DCUI Access privilege are granted the Administrator role on the host.

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 the setting **DCUI.Access**.

4 Click **Edit** and enter the user names, separated by commas.

By default, the root user is specified. You can remove root from the list of DCUI access users, as long as you specified at least one other user.

5 Click **OK**.

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.

Install the vSphere Authentication Proxy Service

To use the vSphere Authentication Proxy service for authentication, you must install the service on a host machine.

You can install the vSphere Authentication Proxy on the same machine as the associated vCenter Server, or on a different machine that has a network connection to the vCenter Server. The vSphere Authentication Proxy is not supported with vCenter Server versions earlier than version 5.0.

The vSphere Authentication Proxy service binds to an IPv4 address for communication with vCenter Server, and does not support IPv6. vCenter Server can be on an IPv4-only, IPv4/IPv6 mixed-mode, or IPv6-only host machine, but the machine that connects to vCenter Server through the vSphere Client must have an IPv4 address for the vSphere Authentication Proxy service to work.

Prerequisites

- Verify that you have administrator privileges on the host machine where you install the vSphere Authentication Proxy service.
- Verify that the host machine has Windows Installer 3.0 or later.
- Verify that the host machine has a supported processor and operating system. The vSphere Authentication Proxy supports the same processors and operating systems as vCenter Server.
- Verify that the host machine has a valid IPv4 address. You can install vSphere Authentication Proxy on an IPv4-only or IPv4/IPv6 mixed-mode host machine, but you cannot install vSphere Authentication Proxy on an IPv6-only host machine.
- 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 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.`

Gather the following information to complete the installation:

- The location where you will install the vSphere Authentication Proxy, if you are not using the default location.
- The IP address or host name, HTTP port, and credentials for the vCenter Server system that the vSphere Authentication Proxy will connect to.
- The host name or IP address to identify the vSphere Authentication Proxy host machine on the network.

Procedure

1 On the host machine where you will install the vSphere Authentication Proxy service, install the .NET Framework 3.5.

2 Install vSphere Auto Deploy.

You do not have to install Auto Deploy on the same host machine as the vSphere Authentication Proxy service.

3 Add the host machine where you will install the authentication proxy service to the domain.

4 Use the Domain Administrator account to log in to the host machine.

5 In the software installer directory, double-click the `autorun.exe` file to start the installer.

6 Select **VMware vSphere Authentication Proxy** and click **Install**.

7 Follow the wizard prompts to complete the installation.

During installation, the authentication service registers with the vCenter Server instance where Auto Deploy is registered.

The authentication proxy service is installed on the host machine.

NOTE 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.

What to do next

Configure the host to use the authentication proxy service to join the domain.

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 as described in "Install the vSphere Authentication Proxy Service," on page 103.

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
Self-signed certificate	If you replace the default certificate with a self-signed certificate, add the host to vCenter Server so that the authentication proxy server will trust the host.
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 Adapter 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`.

Authenticating vSphere Authentication Proxy to ESXi

Before you use the vSphere Authentication Proxy to connect ESXi to a domain, you must authenticate the vSphere Authentication Proxy server to ESXi. If you use Host Profiles to connect a domain with the vSphere Authentication Proxy server, you do not need to authenticate the server. The host profile authenticates the proxy server to ESXi.

To authenticate ESXi to use the vSphere Authentication Proxy, export the server certificate from the vSphere Authentication Proxy system and import it to ESXi. You need only authenticate the server once.

NOTE By default, ESXi must authenticate the vSphere Authentication Proxy server when using it to join a domain. 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 on a host as described in "Install the vSphere Authentication Proxy Service," on page 103.

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 in the vSphere Web Client

To authenticate the vSphere Authentication Proxy server to ESXi, upload the proxy server certificate to ESXi.

You use the vSphere Web Clientuser interface to upload the vSphere Authentication Proxy server certificate to ESXi.

Prerequisites

Install the vSphere Authentication Proxy service on a host as described in "Install the vSphere Authentication Proxy Service," on page 103.

Export the vSphere Authentication Proxy server certificate as described in "Export vSphere Authentication Proxy Certificate," on page 105.

Procedure

1. Upload the certificate for the authentication proxy server to a temporary location accessible to the host.
   a. In the vSphere Web Client, browse to a datastore accessible to the host and click the **Manage** tab.
   b. Click **Files** and click **Upload File**.
2. Browse to the certificate and select **Open**.

   To upload or download files from a datastore, you must have the Client Integration Plug-in installed on the system where you use the vSphere Web Client.
3. Browse to the host and click the **Manage** tab.
4. Select the **Configuration** tab and click **Authentication Services**.
5. Click **Import Certificate**.
6. 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.
7. Click **Import**.

What to do next

Set up the host to use vSphere Authentication Proxy server to authenticate users.

Use vSphere Authentication Proxy to Add a Host to a Domain in the vSphere Web Client

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 self-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 104.
- 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.

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 using a password or pass phrases. ESXi does not support passwords or pass phrases, also known as encrypted keys. If you set up a pass word or pass phrase, ESXi processes cannot start correctly.

- You can configure the Web proxy so that it searches for certificates in a location other than the default location. This capability proves useful for companies that prefer to centralize their certificates on a single machine so that multiple hosts can use the certificates.

CAUTION If certificates are not stored locally on the host—for example, if they are stored on an NFS share—the host cannot access those certificates if ESXi loses network connectivity. As a result, a client connecting to the host cannot successfully participate in a secure SSL handshake with the host.

- 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 the 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 vCenter Server, the certificate remains in place.

Configure the Web Proxy to Search for Certificates in Nondefault Locations

You can configure the Web proxy so that it searches for certificates in a location other than the default location. This is useful for companies that centralize their certificates on a single machine so that multiple hosts can use the certificates.

Procedure

1. Log in to the ESXi Shell as a user with administrator privileges.
2. Change to the `/etc/vmware/rhttpproxy/` directory.
3. Use a text editor to open the `config.xml` file and find the following XML segment.

   ```
   <ssl>
   <!-- The server private key file -->
   <privateKey>/etc/vmware/ssl/rui.key</privateKey>
   <!-- The server side certificate file -->
   <certificate>/etc/vmware/ssl/rui.crt</certificate>
   </ssl>
   ```

4. Replace `/etc/vmware/ssl/rui.key` with the absolute path to the private key file that you received from your trusted certificate authority.

   This path can be on the host or on a centralized machine on which you store certificates and keys for your company.

   NOTE Leave the `<privateKey>` and `</privateKey>` XML tags in place.

5 Replace `/etc/vmware/ssl/rui.crt` with the absolute path to the certificate file that you received from your trusted certificate authority.

CAUTION Do not delete the original `rui.key` and `rui.crt` files. The host uses these files.

6 Save your changes and close the file.

7 Restart the rhttpproxy process:

```
/etc/init.d/rhttpproxy restart
```

Change Security Settings for a Web Proxy Service

You can change the security configuration so that individual services are directly accessible through HTTP connections.

To configure security settings for vSphere 5.0 and earlier, see "Change Security Settings for a Web Proxy Service 5.0 and earlier," on page 110.

Procedure

1 Log in to the ESXi Shell as a user with administrator privileges.

2 Change to the `/etc/vmware/rhttpproxy/endpoints/conf` directory.

3 Use a text editor to open the `endpoints.conf` file.

4 Change the security settings as required.

For example, you might want to modify entries for services that use HTTPS to add the option of HTTP access.

Option	Description
connection-type	Acceptable values include: ■ local ■ remote ■ namedpipe ■ localtunnel ■ remotetunnel ■ namedpipetunnel
endpoint-address	■ For *local* and *localtunnel*, supply the port number. ■ For *remote* and *remotetunnel*, supply the *HostName/IP_address:Port*. ■ For *namedpipe* and *namedpipetunnel*, supply the location of the name pipe in the file system.
HTTP Access mode	Forms of communication the service permits. Acceptable values include: ■ allow - Allow HTTP access. ■ redirect – If the Endpoint address is a local port, then the client is redirected to 443. If the Endpoint address is a remote host, then the client is redirected to that host. ■ reject - No HTTP access.
HTTPS Access mode	Acceptable values include: ■ allow - Allow HTTPS access. ■ reject - Do not allow HTTPS access.

5 Save your changes and close the file.

The following example shows a completed endpoints.conf file.

```
# Endpoint Connection-type Endpoint-address HTTP-access-Mode HTTPS-access-mode
/ local 8309 redirect allow
/sdk local 8307 redirect allow
/client/clients.xml local 8309 allow allow
/ui local 8308 redirect allow
/vpxa local 8089 reject allow
/mob namedpipe /var/run/vmware/proxy-mob redirect allow
/wsman local 8889 redirect allow
/sdkTunnel namedpipetunnel /var/run/vmware/proxy-sdk-tunnel allow reject
/ha-nfc local 12001 allow allow
/nfc local 12000 allow allow
```

What to do next

After you make the changes to the `endpoints.conf` file, make the reverse proxy reload the new endpoints by using the command `kill -HUP <pid_of_rhttpproxy>`

Change Security Settings for a Web Proxy Service 5.0 and earlier

You can change the security configuration so that individual services are directly accessible through HTTP connections.

These steps are for version 5.0 and earlier. Beginning with 5.1, the file that needs to be modified is completely different. For instructions to modify the new file, see "Change Security Settings for a Web Proxy Service," on page 109.

Procedure

1 Log in to the ESXi Shell as a user with administrator privileges.

2 Change to the `/etc/vmware/hostd/directory`directory.

3 Use a text editor to open the `proxy.xml` file.

The contents of the file typically appears as follows.

```
<ConfigRoot>
<EndpointList>
<_length>10</_length>
<_type>vim.ProxyService.EndpointSpec[]</_type>
<e id="0">
<_type>vim.ProxyService.LocalServiceSpec</_type>
<accessMode>httpsWithRedirect</accessMode>
<port>8309</port>
<serverNamespace>/</serverNamespace>
</e>
<e id="1">
<_type>vim.ProxyService.LocalServiceSpec</_type>
<accessMode>httpAndHttps</accessMode>
<port>8309</port>
<serverNamespace>/client/clients.xml</serverNamespace>
</e>
<e id="2">
<_type>vim.ProxyService.LocalServiceSpec</_type>
<accessMode>httpAndHttps</accessMode>
<port>12001</port>
<serverNamespace>/ha-nfc</serverNamespace>
</e>
```

```
<e id="3">
<_type>vim.ProxyService.NamedPipeServiceSpec</_type>
<accessMode>httpsWithRedirect</accessMode>
<pipeName>/var/run/vmware/proxy-mob</pipeName>
<serverNamespace>/mob</serverNamespace>
</e>
<e id="4">
<_type>vim.ProxyService.LocalServiceSpec</_type>
<accessMode>httpAndHttps</accessMode>
<port>12000</port>
<serverNamespace>/nfc</serverNamespace>
</e>
<e id="5">
<_type>vim.ProxyService.LocalServiceSpec</_type>
<accessMode>httpsWithRedirect</accessMode>
<port>8307</port>
<serverNamespace>/sdk</serverNamespace>
</e>
<e id="6">
<_type>vim.ProxyService.NamedPipeTunnelSpec</_type>
<accessMode>httpOnly</accessMode>
<pipeName>/var/run/vmware/proxy-sdk-tunnel</pipeName>
<serverNamespace>/sdkTunnel</serverNamespace>
</e>
<e id="7">
<_type>vim.ProxyService.LocalServiceSpec</_type>
<accessMode>httpsWithRedirect</accessMode>
<port>8308</port>
<serverNamespace>/ui</serverNamespace>
</e>
<e id="8">
<_type>vim.ProxyService.LocalServiceSpec</_type>
<accessMode>httpsOnly</accessMode>
<port>8089</port>
<serverNamespace>/vpxa</serverNamespace>
</e>
<e id="9">
<_type>vim.ProxyService.LocalServiceSpec</_type>
<accessMode>httpsWithRedirect</accessMode>
<port>8889</port>
<serverNamespace>/wsman</serverNamespace>
</e>
</EndpointList>
</ConfigRoot>
```

4 Change the security settings as required.

For example, you might want to modify entries for services that use HTTPS to add the option of HTTP access.

Option	Description
e id	ID number for the server ID XML tag. ID numbers must be unique within the HTTP area.
_type	Name of the service you are moving.

Option	Description
accessmode	Forms of communication the service permits. Acceptable values include: ■ httpOnly – The service is accessible only over plain-text HTTP connections. ■ httpsOnly – The service is accessible only over HTTPS connections. ■ httpsWithRedirect – The service is accessible only over HTTPS connections. Requests over HTTP are redirected to the appropriate HTTPS URL. ■ httpAndHttps – The service is accessible both over HTTP and HTTPS connections.
port	Port number assigned to the service. You can assign a different port number to the service.
serverNamespace	Namespace for the server that provides this service, for example `/sdk` or `/mob`.

5 Save your changes and close the file.

6 Restart the `hostd` process:

```
/etc/init.d/hostd restart
```

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.

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`.

Option	Description
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://hostName1:514`. 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.

8 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:

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.

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 antivirus, 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.

Installing Anti-Virus Software

Because each virtual machine hosts a standard operating system, you must protect it from viruses by installing antivirus 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.

Configure Logging Levels for the Guest Operating System

Virtual machines can write troubleshooting information into a virtual machine log file stored on the VMFS volume. Virtual machine users and processes can abuse logging either on purpose or inadvertently so that large amounts of data flood the log file. Over time, the log file can consume enough file system space to cause a denial of service.

To prevent this problem, consider modifying logging settings for virtual machine guest operating systems. These settings can limit the total size and number of log files. Normally, a new log file is created each time you reboot a host, so the file can grow to be quite large. You can ensure new log file creation happens more frequently by limiting the maximum size of the log files. VMware recommends saving 10 log files, each one limited to 100KB. These values are large enough to capture sufficient information to debug most problems that might occur.

Each time an entry is written to the log, the size of the log is checked. If it is over the limit, the next entry is written to a new log. If the maximum number of log files exists, the oldest log file is deleted. A Denial of Service attack that avoids these limits could be attempted by writing an enormous log entry, but each log entry is limited in size to 4KB, so no log files are ever more than 4KB larger than the configured limit.

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.

  See “Removing Unnecessary Hardware Devices,” on page 118.

- Turn off screen savers.

- Do not run the X Window system on Linux, BSD, or Solaris guest operating systems unless it is necessary.

Removing 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.

Use the following guidelines to increase virtual machine security.

- Ensure that unauthorized devices are not connected and remove any unneeded or unused hardware devices.

- Disable unnecessary virtual devices from within a virtual machine. An attacker with access to a virtual machine can connect a disconnected CD-ROM drive 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 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 datacenter environment, and CD/DVD drives are usually connected only temporarily during software installation.
- For less commonly used devices that are not required, either the parameter should not be present or its value must be false. Ensure that the following parameters are either not present or set to false unless the device is required.

Parameter	Value	Device
floppyX.present	false	floppy drives
serialX.present	false	serial ports
parallelX.present	false	parallel ports
usb.present	false	USB controller
ideX:Y.present	false	CD-ROM

Disable Unexposed Features

VMware virtual machines are designed to work on both vSphere systems and hosted virtualization platforms such as Workstation and Fusion. Certain VMX 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 To find a virtual machine, select a datacenter, 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.unity.push.update.disable	TRUE
isolation.tools.ghi.launchmenu.change	TRUE
isolation.tools.memSchedFakeSampleStats.disable	TRUE
isolation.tools.getCreds.disable	TRUE
isolation.tools.ghi.autologon.disable	TRUE
isolation.bios.bbs.disable	TRUE
isolation.tools.hgfsServerSet.disable	TRUE

6 Click **OK**.

Setting `isolation.tools.hgfsServerSet.disable` to true disables registration of the guest's HGFS server with the host. 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, will not function.

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, the vCenter Server Administrator role lets users 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 datacenter as you are to the physical datacenter. To avoid giving users full administrator access, apply the nonguest access 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, you want to 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 **Access > Roles**.

3 Click the **Create role** 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

Assign users who require **Administrator** privileges without guest access privileges to the newly created role, ensuring that these users are removed from the default Administrator role.

Prevent a Virtual Machine User or Process from Disconnecting Devices in the vSphere Web Client

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, as well as 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 To find a virtual machine, select a datacenter, 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 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.

5 Click **OK** to close the Configuration Parameters dialog box, and click **OK** again to close the Virtual Machine Properties dialog box.

Limiting Guest Operating System Writes to Host Memory

The guest operating system processes send informational messages to the host through VMware Tools. If the amount of data the host stored as a result of these messages was unlimited, an unrestricted data flow would provide an opportunity for an attacker to stage a denial-of-service (DoS) attack.

The informational messages sent by guest operating processes are known as `setinfo` messages and typically contain name-value pairs that define virtual machine characteristics or identifiers that the host stores (for example, `ipaddress=10.17.87.224`). The configuration file containing these name-value pairs is limited to a size of 1MB, which prevents attackers from staging a DoS attack by writing software that mimics VMware Tools and filling the host's memory with arbitrary configuration data, which consumes space needed by the virtual machines.

If you require more than 1MB of storage for name-value pairs, you can change the value as required. You can also prevent the guest operating system processes from writing any name-value pairs to the configuration file.

Modify Guest Operating System Variable Memory Limit in the vSphere Web Client

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 To find a virtual machine, select a datacenter, 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 the 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 Log in to a vCenter Server system using the vSphere Client.

2 Select the virtual machine in the inventory panel.

3 On the **Summary** tab, click **Edit Settings**.

4 Select **Options > Advanced > General** and click **Configuration Parameters**.

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 to close the Virtual Machine Properties dialog box.

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

You can convert a template to a virtual machine and back to a template in the vSphere Web Client, which makes updating templates easy. For more information about templates, see the *vSphere Virtual Machine Administration* documentation.

You can use vSphere Update Manager to automatically patch the operating system and certain applications in the template. See the *vSphere Update Manager* documentation.

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 limits to control the server resources that a virtual machine consumes.

By default, all virtual machines on a host share resources equally.

Procedure

- Use shares or reservations to guarantee resources to critical virtual machines.

  Limits constrain resource consumption by virtual machines that have a greater risk of being exploited or attacked, or that run applications that are known to have the potential to greatly consume resources.

What to do next

See the *vSphere Resource Management* documentation for information about shares and limits.

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 sizeLimit parameter is not listed in the VMX file.

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 on which the virtual machine files reside. For example, `/vmfs/volumes/vol1/vm-finance/`.

2 Use a text editor to add or edit the following line in the VMX file:

```
tools.setInfo.sizeLimit=104857
```

3 Save and close the file.

Prevent Virtual Disk Shrinking in the vSphere Web Client

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.

Procedure

1 Find the virtual machine in the vSphere Web Client inventory.

a To find a virtual machine, select a datacenter, 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.

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

- 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.

Configuring Logging Levels for the Guest Operating System

Virtual machines can write troubleshooting information into a virtual machine log file stored on the VMFS volume. Virtual machine users and processes can abuse logging either on purpose or inadvertently so that large amounts of data flood the log file. Over time, the log file can consume enough file system space to cause a denial of service.

To prevent this problem, consider modifying logging settings for virtual machine guest operating systems. These settings can limit the total size and number of log files. Normally, a new log file is created each time you reboot a host, so the file can grow to be quite large. You can ensure new log file creation happens more frequently by limiting the maximum size of the log files. VMware recommends saving 10 log files, each one limited to 100KB. These values are large enough to capture sufficient information to debug most problems that might occur.

Each time an entry is written to the log, the size of the log is checked. If it is over the limit, the next entry is written to a new log. If the maximum number of log files exists, the oldest log file is deleted. A DoS attack that avoids these limits could be attempted by writing an enormous log entry, but each log entry is limited in size to 4KB, so no log files are ever more than 4KB larger than the configured limit.

Limit Log File Numbers in the vSphere Web Client

To prevent virtual machine users and processes from creating large numbers of log files, which can lead to denial of service, you can limit the number of the log files for a virtual machine. You cannot limit the log file size for individual virtual machines.

You can make changes to logging for all virtual machines for a host by editing the `vms.log.xxx` parameter in the `/etc/config/vmware` file.

Prerequisites

Turn off the virtual machine.

Procedure

1 Find the virtual machine in the vSphere Web Client inventory.

  a To find a virtual machine, select a datacenter, 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 log.keepOld parameter to the number of files to keep. For example, to keep 10 log files and begin deleting the oldest files as new ones are created, enter **10**.

6 Click **OK**.

Disable Logging for the Guest Operating System in the vSphere Web Client

If you choose not to write troubleshooting information into a virtual machine log file stored on the VMFS volume, you can stop logging altogether.

If you disable logging for the guest operating system, be aware that you might not be able to gather adequate logs to allow troubleshooting. Further, VMware does not offer technical support for virtual machine problems if logging has been disabled.

Procedure

1 Find the virtual machine in the vSphere Web Client inventory.

   a To find a virtual machine, select a datacenter, 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**.

4 In Settings, deselect **Enable logging**.

5 Click **OK**.

9 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

Network security in the vSphere environment shares many characteristics of securing a physical network environment, but also includes some characteristics that apply only with 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 128.

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 137.

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 "TCP and UDP Ports," on page 132.

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

The port that vCenter Server uses to listen for data transfer from its clients is 443. 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.

To enable vCenter Server to receive data from the vSphere Web Client, open port 443 in the firewall to allow data transfer from the vSphere Web Client to vCenter Server. Contact the firewall system administrator for additional information on configuring ports in a firewall.

If you are using the vSphere Web Client and 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 in the vSphere Web Client. To learn how to change these settings, see the *vCenter Server and Host Management* 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. The firewall ports you use are the same as those you use if vCenter Server is in place.
- 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.

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 82 for a discussion of configuration files, vSphere Web Client access, and firewall commands. See "TCP and UDP Ports," on page 132 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 are required 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 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.

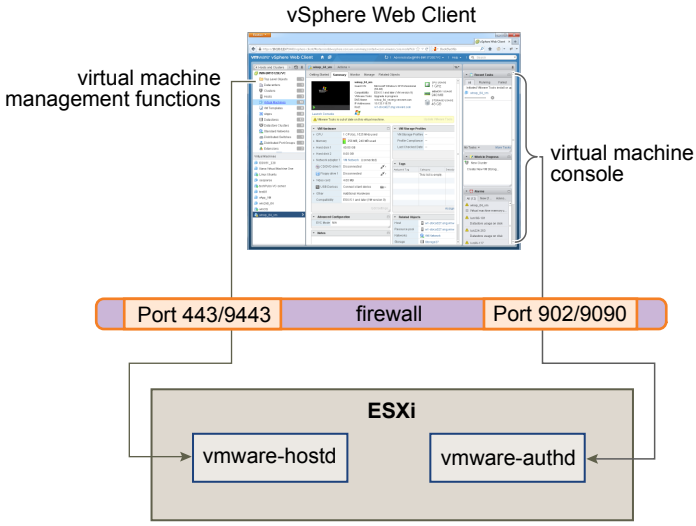
The following ports are involved.

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 accessvCenter 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 9-1. 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 Through vCenter Server with the vSphere Client

When you are connecting with the vSphere Client, the required ports depend on whether you connect directly to the ESXi host or you connect to a vCenter Server system.

Port 443 Port 443 connects clients such as the vSphere Web Services SDK to ESXi through the Tomcat Web service or the SDK. The host process multiplexes port 443 data to the appropriate recipient for processing.

When the vSphere SDK is connected directly to ESXi, it can use this port to support any management functions related to the host and its virtual machines. Port 443 is the port that clients such as the vSphere SDK assume is available when sending data to ESXi. VMware does not support configuring a different port for these connections.

Port 902 This is the port that vCenter Server assumes is available for receiving data from ESXi.

Port 902 connects vCenter Server to the host through the VMware Authorization Daemon (`vmware-authd`). This daemon multiplexes port 902 data to the appropriate recipient for processing. VMware does not support configuring a different port for this connection.

Connecting Directly with the vSphere Client

With the vSphere Client, you can connect directly to an ESXi host.

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.

TCP and UDP Ports

vCenter Server, ESXi hosts, and other network components are accessed using 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 http://kb.vmware.com/kb/1012382.

Table 9-1. TCP and UDP Ports

Port	Purpose	Traffic Type
22	SSH Server (vSphere Client)	Incoming TCP
53 (Default)	DNS Client	Incoming and outgoing UDP
68 (Default)	DHCP Client	Incoming and outgoing UDP
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)	Incoming TCP Outgoing TCP, UDP
88, 2013	Control interface RPC for Kerberos, used by vCenter Single Sign-On	
111 (Default)	RPC service that is used for the NIS register by the vCenter Server Appliance	Incoming and outgoing TCP
123	NTP Client	Outgoing UDP
135 (Default)	Used to join vCenter Server Appliance to an Active Directory domain.	Incoming and outgoing TCP
161 (Default)	SNMP Server	Incoming UDP
443 (Default)	The default port that the vCenter Server system uses to listen for connections from the vSphere Client. To enable the vCenter Server system to receive data from the vSphere Client, open port 443 in the firewall. The vCenter Server system also uses 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) ■ vSphere Client access to vSphere Update Manager ■ Third-party network management client connections to vCenter Server ■ Third-party network management clients access to hosts	Incoming TCP
427 (Default)	The CIM client uses the Service Location Protocol, version 2 (SLPv2) to find CIM servers.	Incoming and outgoing UDP
513 (Default)	vCenter Server Appliance used for logging activity	Incoming UDP

Table 9-1. TCP and UDP Ports (Continued)

Port	Purpose	Traffic Type
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. Port 902 must not be blocked between the vSphere Client and the hosts. The vSphere Client uses this port to display virtual machine consoles.	Incoming and outgoing TCP, outgoing UDP
903	Access a virtual machine console from the vSphere Client when the vSphere Client is connected directly to the ESXi host (no vCenter Server). MKS transactions (xinetd/vmware-authd-mks)	Incoming TCP
1234, 1235 (Default)	vSphere Replication	Outgoing TCP
2012	Control interface RPC for vCenter Single Sign-On vmdir.	
2014	RPC port for all VMCA (VMware Certificate Authority) APIs	
2049	Transactions from NFS storage devices This port is used on the VMkernel interface.	Incoming and outgoing TCP
3260	Transactions to iSCSI storage devices	Outgoing TCP
5900-5964	RFB protocol, which is used by management tools such as VNC	Incoming and outgoing TCP
5988 (Default)	CIM transactions over HTTP	Incoming TCP
5989 (Default)	CIM XML transactions over HTTPS	Incoming and outgoing TCP
7444	vCenter Single Sign-On HTTPS	
8000 (Default)	Requests from vMotion	Incoming and outgoing TCP
8009	AJP connector port for vCenter Server Appliance communication with Tomcat	Outgoing TCP
8100, 8200 (Default)	Traffic between hosts for vSphere Fault Tolerance (FT)	Incoming and outgoing TCP, UDP
8182	Traffic between hosts for vSphere High Availability (HA)	Incoming and outgoing TCP, incoming and outgoing UDP
9009	Used to allow a vCenter Server Appliance to communicate with the vSphere Web Client	Incoming and outgoing TCP
9090	Remote console traffic generated by user access to virtual machines on a specific host. vSphere Web Client HTTPS access to virtual machine consoles	Incoming TCP
9443	vSphere Web Client HTTP access to ESXi hosts	Incoming TCP
11711	vCenter Single Sign-On LDAP	
11712	vCenter Single Sign-On LDAPS	
12721	VMware Identity Management service	

In addition to the TCP and UDP ports, you can configure other ports depending on your needs.

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 Standard Switch MAC Addresses

You can secure standard switch traffic against Layer 2 attacks by restricting some of the MAC address modes.

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.

You can secure the traffic through the standard switches against this type of Layer 2 attacks by restricting the following modes:

- Promiscuous mode
- MAC address changes
- Forged transmission

To change any default settings for a port, you modify the security policy of the standard switch or of the port group from the vSphere Web Client.

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 Transmissions

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

Administrators have several options for securing a vSphere Distributed Switches in their vSphere environment.

Procedure

1 Verify that the Auto Expand feature for the distributed port groups with static binding 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 API/SDK Documentation*.

2 Ensure that all private VLAN IDs of any vSphere Distributed Switch are fully documented.

3 Ensure that no unused ports exist on a virtual port group associated with a vSphere Distributed Switch.

4 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 136)
   - MAC address changes (see"MAC Address Changes," on page 135)

- Forged transmits (see "Forged Transmissions," on page 136)

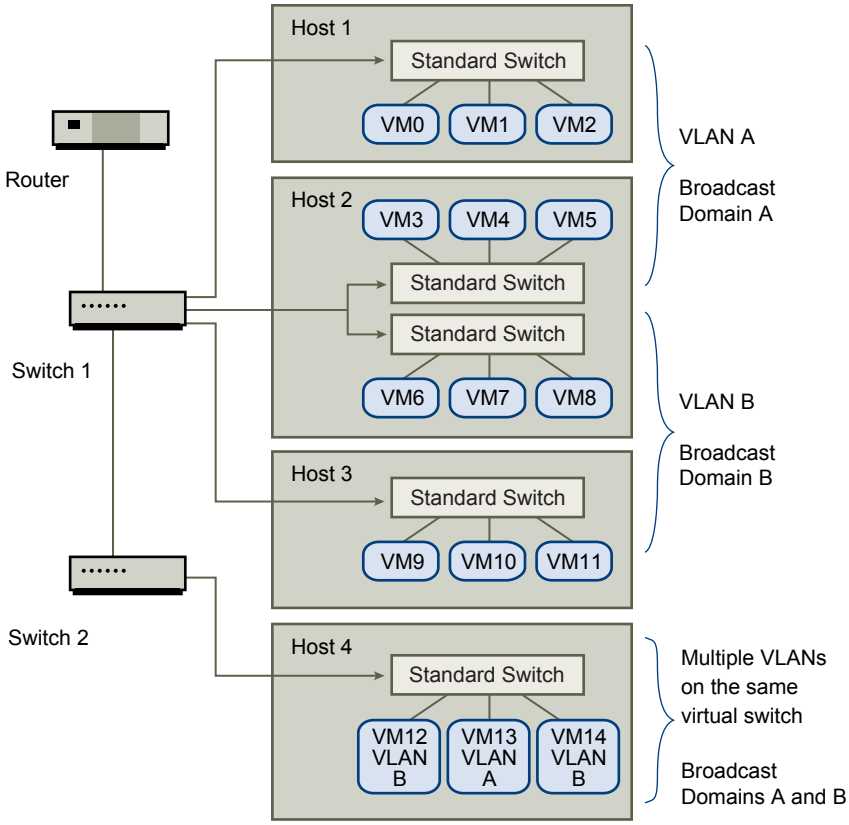
Securing Virtual Machines with VLANs

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 9-2. 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.

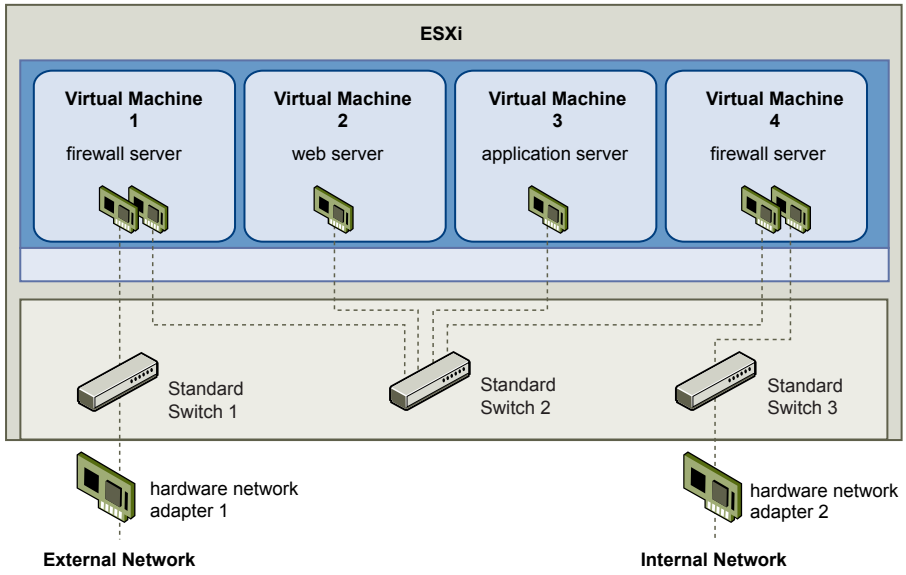
   On a standard switch you can configure VLAN networking mode at switch or port group level, and on a distributed switch at distributed port group or port level.

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 9-3. 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.

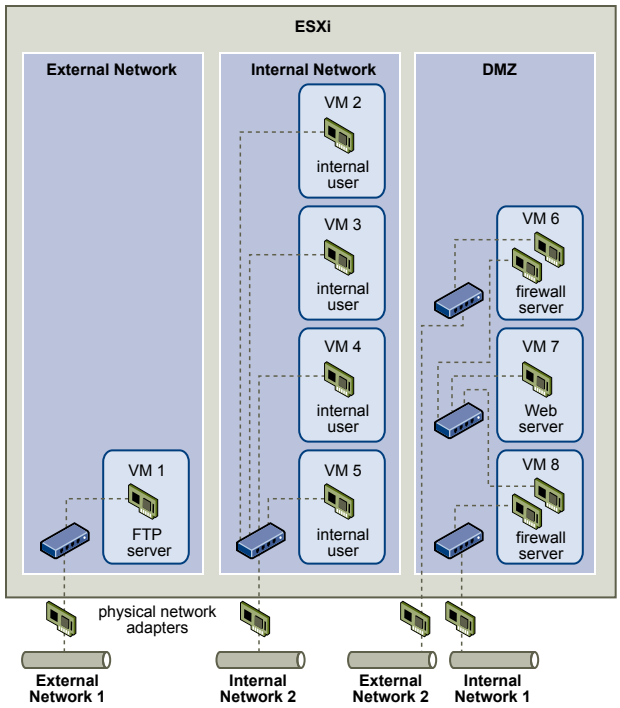
Standard Switch 2 is also connected to Virtual Machine 4. This virtual machine provides a firewall between the DMZ and the internal corporate network. This firewall filters packets from the Web server and application server. If a packet is verified, it is routed to Hardware Network Adapter 2 through 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 9-4. 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 a 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.

Option	Description
--encryption-algorithm= ***encryption algorithm***	Required. Specify the encryption algorithm using one of the following parameters. ■ `3des-cbc` ■ `aes128-cbc` ■ `null` `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 6c6f676f3364657363726f757432
--integrity-algorithm hmac-sha1
--integrity-key 0x69707636726561647 96c6f67736861316f757432
--sa-name sa1
```

Remove a Security Association

You can remove a security association from the host.

You can remove a security association using the `esxcli` vSphere CLI command.

Prerequisites

Be sure 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 Security Policies

ESXi can provide a list of all security policies on the host.

You can get a list of 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 a 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 a Security Association," on page 142.

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 a Security Policy

You can remove a security policy from the ESXi host.

You can remove a security policy using the `esxcli` vSphere CLI command.

Prerequisites

Be sure 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 not 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 on the vSphere Network Appliance 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. Scroll until you find the parameter.

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.

Best Practices for Virtual Machine and Host Security 10

Consider basic security recommendations when creating and configuring hosts and virtual machines.

This chapter includes the following topics:

Synchronizing Clocks on the vSphere Network

Before you install vCenter Single Sign-On, install the vSphere Web Client, or deploy the vCenter Server Appliance, make sure that all machines on the vSphere network have their clocks synchronized.

If the clocks on vCenter Server network machines 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 vSphere Web Client installation to fail or prevent the vCenter Server Appliance vpxd service from starting.

Make sure that any Windows host 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 ESX and ESXi Clocks with a Network Time Server

Before you install vCenter Single Sign-On, the vSphere Web Client, or the vCenter Server appliance, make sure all machines on the vSphere network have their clocks synchronized.

Procedure

1 From the vSphere Web Client, connect to the vCenter Server.

2 Select the host in the inventory.

3 Select the **Manage** tab.

4 Select **Settings**.

5 In the System section, select **Time Configuration**.

6 Click **Edit** and set up the NTP server.

   a Select **Use Network Time Protocol (Enable NTP client)**.

   b Set the NTP Service Startup Policy.

   c Enter the IP addresses of the NTP servers to synchronize with.

   d Click **Start** or **Restart** in the NTP Service Status section.

7 Click **OK**.

   The host synchronizes with the NTP server.

Synchronize the vCenter Server Appliance Clock with an NTP Server

Before you deploy thevCenter Server Appliance, make sure all machines on the network have their clocks synchronized. Unsynchronized clocks can cause installation and authentication errors.

On systems that are joined to a Windows domain, the vCenter Server Appliance clock is synchronized automatically with the domain controller. On other systems, you can enable synchronizing the clock through VMware Tools. As an alternative, you can use this procedure.

Procedure

1 Open a Web browser and navigate to thevCenter Server Appliance Management Interface (https://*vCenter-Appliance-Address*:5480/).

2 Log in as root.

3 From the vCenter Server tab, select the Time subtab.

4 Select one or more of the available options.

Option	Description
No synchronization	Does not perform synchronization.
NTP synchronization	Select this option and specify one or more NTP servers to configure the appliance to synchronize with an NTP server directly.
VMware Tools synchronization	Select this option to synchronize all virtual machines.
Active Directory synchronization	This option becomes available only if you add the appliance to an Active Directory domain. If you select this option, none of the other options is available.

5 Click **Save Settings**.

The vCenter Server Appliance clock is synchronized with the NTP server.

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 Through Authentication

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 Kerberos, Secure Remote Protocol (SRP), or public-key authentication methods for iSCSI. Additionally, it does not support IPsec authentication and encryption.

Use the vSphere Web Client to determine whether authentication is being performed and to configure the authentication method.

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.

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.

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.

11 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

Alarms privileges control the ability to set and respond to alarms on inventory objects.

The table describes privileges needed to create, modify, and respond to alarms.

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 11-1. 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
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

Datacenter

Datacenter privileges control the ability to create and edit datacenters in the vSphere Web Client inventory.

The table describes the privileges required to create and edit datacenters. All datacenter privileges are used in vCenter Server only. The **Create datacenter** privilege is defined on datacenter folders or the root object. All other datacenter privileges are pair with datacenters, datacenter folders, or the root object.

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 11-2. Datacenter Privileges

Privilege Name	Description	Required On
Datacenter.Create datacenter	Allows creation of new datacenter.	Datacenter folder or root object
Datacenter.Move datacenter	Allows moving a datacenter. Privilege must be present at both the source and destination.	Datacenter, source and destination
Datacenter.Network profile configuration	Allows configuration of the network profile for a datacenter.	Datacenter
Datacenter.Query IP pool allocation	Allows configuration of a pool of IP addresses.	Datacenter
Datacenter.Reconfigure datacenter	Allows reconfiguration of a datacenter.	Datacenter
Datacenter.Release IP allocation	Allows releasing the assigned IP allocation for a datacenter.	Datacenter
Datacenter.Remove datacenter	Allows removal of a datacenter. In order to have permission to perform this operation, you must have this privilege assigned to both the object and its parent object.	Datacenter plus parent object
Datacenter.Rename datacenter	Allows changing the name of a datacenter.	Datacenter

Datastore

Datastore privileges control the ability to browse, manage, and allocate space on datastores.

The table describes the privileges required to work with 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 11-3. 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.	Datastores
Datastore.Browse datastore	Allows browsing files on a datastore.	Datastores
Datastore.Configure datastore	Allows configuration of a datastore.	Datastores
Datastore.Low level file operations	Allows performing read, write, delete, and rename operations in the datastore browser.	Datastores

Table 11-3. Datastore Privileges (Continued)

Privilege Name	Description	Required On
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, you must have this privilege assigned to both the object and its parent object.	Datastores
Datastore.Remove file	Allows deletion of files in the datastore. This privilege is deprecated. Assign the **Low level file operations** privilege.	Datastores
Datastore.Rename datastore	Allows renaming a datastore.	Datastores
Datastore.Update virtual machine files	Allows updating file paths to virtual machine files on a datastore after the datastore has been resignatured.	Datastores

Datastore Cluster

Datastore cluster privileges control the configuration of datastore clusters for Storage DRS.

The table describes privileges used for configuring datastore clusters.

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 11-4. 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

vSphere Distributed Switch

vSphere Distributed Switch privileges control the ability to perform tasks related to the management of vSphere Distributed Switches.

The table describes the privileges required to create and configure vSphere Distributed Switches.

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 11-5. vSphere Distributed Switch Privileges

Privilege Name	Description	Required On
vSphere Distributed Switch.Create	Allows creation of a vSphere Distributed Switch.	Datacenters, Network folders
vSphere Distributed Switch.Delete	Allows removal of a vSphere Distributed Switch. To have permission to perform this operation, you must have this privilege assigned to both the object and its parent object.	vSphere Distributed Switches
vSphere Distributed Switch.Host operation	Allows changing the host members of a vSphere Distributed Switch.	vSphere Distributed Switches
vSphere Distributed Switch.Modify	Allows changing the configuration of a vSphere Distributed Switch.	vSphere Distributed Switches

Table 11-5. vSphere Distributed Switch Privileges (Continued)

Privilege Name	Description	Required On
vSphere Distributed Switch.Move	Allows moving a vSphere Distributed Switch to another folder.	vSphere Distributed Switches
vSphere Distributed Switch.Network I/O control operation	Allow changing the resource settings for a vSphere Distributed Switch.	vSphere Distributed Switches
vSphere Distributed Switch.Policy operation	Allows changing the policy of a vSphere Distributed Switch.	vSphere Distributed Switches
vSphere Distributed Switch .Port configuration operation	Allow changing the configuration of a port in a vSphere Distributed Switch.	vSphere Distributed Switches
vSphere Distributed Switch.Port setting operation	Allows changing the setting of a port in a vSphere Distributed Switch.	vSphere Distributed Switches
vSphere Distributed Switch.VSPAN operation	Allows changing the VSPAN configuration of a vSphere Distributed Switch.	vSphere Distributed Switches

ESX Agent Manager

ESX Agent Manager privileges control operations related to ESX Agent Manager and agent virtual machines.

The table describes privileges related to ESX Agent Manager and agent 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 11-6. 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

Extension privileges control the ability to install and manage extensions.

The table describes privileges required to install and manage plug-ins.

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 11-7. 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

Folder privileges control the ability to create and manage folders.

The table describes privileges required 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 11-8. 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, you must have this privilege assigned to 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

Global privileges control global tasks related to tasks, scripts, and extensions.

The table describes privileges required for global tasks in the vSphere Web Client.

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 11-9. 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 forvCenter Server extensions to disable certain operations on objects managed by vCenter Server.	Root vCenter Server

Table 11-9. Global Privileges (Continued)

Privilege Name	Description	Required On
Global.Enable methods	Allows servers for vCenter Server extensions to enable certain operations on objects managed byvCenter Serverr.	Root vCenter Server
Global.Global tag	Allows adding or removing global tags.	Root host or vCenter Server
Global.Health	Allows viewing the health ofvCenter 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

Host CIM privileges control the use of CIM for host health monitoring.

The table describes privileges used for CIM 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 11-10. 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

Host configuration privileges control the ability to configure hosts.

The table describes the privileges required to configure host 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 11-11. Host Configuration Privileges

Privilege Name	Description	Required On
Host.Configuration.Advanced Settings	Allows setting advanced options in host configuration.	Hosts
Host.Configuration.Authentication Store	Allows configuring Active Directory authentication stores.	Hosts
Host.Configuration.Change date and time settings	Allows changes to date and time settings on the host.	Hosts
Host.Configuration.Change PciPassthru settings	Allows changes to PciPassthru settings for a host.	Hosts
Host.Configuration.Change settings	Allows setting of lockdown mode on ESXi hosts. Lockdown mode is not supported on ESX hosts.	Hosts
Host.Configuration.Change SNMP settings	Allows configuring, restarting, and stopping the SNMP agent.	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
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 11-12. 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, you must have this privilege assigned to 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, you must have this privilege assigned to both the object and its parent object.	Hosts plus parent object
Host.Inventory.Rename cluster	Allows renaming a a cluster.	Clusters

Host Local Operations

Host local operations privileges control actions performed when the vSphere Client is connected directly to a host.

The table describes the privileges required for actions performed when the vSphere Client is connected directly to a single 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 11-13. 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.	

Table 11-13. Host Local Operations Privileges (Continued)

Privilege Name	Description	Required On
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

Host vSphere replication privileges control the use of replication for a host's virtual machines.

The table describes privileges used for virtual machine replication by VMware vCenter Site Recovery Manager™.

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 11-14. Host vSphere Replication Privileges

Privilege Name	Description	Required On
Host.vSphere Replication.Manage Replication	Allows managment of virtual machine replication on this host.	Hosts

Host Profile

Host Profile privileges control operations related to creating and modifying host profiles.

The table describes privileges required for 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 11-15. 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
Host profile.Export	Allows exporting a host profile	Root vCenter Server
Host profile.View	Allows viewing a host profile.	Root vCenter Server

Network

Network privileges control tasks related to network management.

The table describes privileges required for 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 11-16. 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, you must have this privilege assigned to both the object and its parent object.	Networks

Performance

Performance privileges control modifying performance statistics settings.

The table describes privileges required to modify 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 11-17. Performance Privileges

Privilege Name	Description	Required On
Performance.Modify intervals	Allows creating, removing, and updating performance data collection intervals.	Root vCenter Server

Permissions

Permissions privileges control the assigning of roles and permissions.

The table describes permissions required for assigning 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 11-18. 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, you must have this privilege assigned to both the object and its parent object.	Any object plus parent object
Permissions.Modify role	Allows updating a role's name and its privileges.	Any object
Permissions.Reassign role permissions	Allows reassigning all permissions of a role to another role.	Any object

Profile-driven Storage

Profile-driven storage privileges control operations related to storage profiles.

The table describes privileges required for viewing and updating 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 11-19. 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 sstorage capabilities and storage profiles.	Root vCenter Server

Resource

Resource privileges control the creation and management of resource pools, as well as the migration of virtual machines.

The table describes privileges that control resource management and virtual machine migration.

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 11-20. 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 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
Resource.Query vMotion	Allows querying the general vMotion compatibility of a virtual machine with a set of hosts.	Root vCenter Server
Resource.Relocate	Allows cold migration of a virtual machine's execution to a specific resource pool or host.	Virtual machines

Table 11-20. Resource Privileges (Continued)

Privilege Name	Description	Required On
Resource.Remove resource pool	Allows deletion of a resource pool. To have permission to perform this operation, you must have this privilege assigned to both the object and its parent object.	Resource pools
Resource.Rename resource pool	Allows renaming of a resource pool.	Resource pools

Scheduled Task

Scheduled task privileges control creation, editing, and removal of scheduled tasks.

The table describes privileges required for creating and modifying 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 11-21. 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

Sessions privileges control the ability of extensions to open sessions on the vCenter Server.

The table describes the privileges associated with sessions on 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 11-22. 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

Storage Views privileges control the ability to configure and use storage views on vCenter Server.

The table describes privileges required to configure and use storage views.

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 11-23. Storage Views Privileges

Privilege Name	Description	Required On
Storage views.Configure service	Allows changing options such as the reports update interval and database connectivity information.	Root vCenter Server
Storage views.View	Allows viewing of the Storage Views tab.	Root vCenter Server

Tasks

Tasks privileges control the ability of extensions to create and update tasks on the vCenter Server.

The table describes privileges related to 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 11-24. Tasks Privileges

Privilege Name	Description	Required On
Tasks.Create task	Allows an extension to create a user-defined task.	Root vCenter Server
Tasks.Update task	Allows an extension to updates a user-defined task.	Root vCenter Server

vApp

vApp privileges control operations related to deploying and configuring a vApp.

The table describes privileges related to 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 11-25. 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, you must have this privilege assigned to 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

Table 11-25. vApp Privileges (Continued)

Privilege Name	Description	Required On
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, you must have this privilege assigned to 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, you must have this privilege assigned to both the object and its parent object.	vApps

vCenter Inventory Service Tagging

vCenter Inventory Service Tagging privileges control the ability to create and delete tags and tag categories, and assign and remove tags on vSphere inventory objects.

The table describes privileges related to tagging.

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 11-26. vCenter Inventory Service Privileges

Privilege Name	Description	Required On
vCenter Inventory Service.vCenter Inventory Service Tagging.Assign or Unassign Inventory Service Tag	Allows assignment or unassignment of a tag for an object in the vCenter Server inventory.	Any object
vCenter Inventory Service.vCenter Inventory Service Tagging.Create Inventory Service Tag Category	Allows creation of a tag category.	Any object
vCenter Inventory Service.vCenter Inventory Service Tagging.Create Inventory Service Tag	Allows creation of a tag.	Any object
vCenter Inventory Service.vCenter Inventory Service Tagging.Delete Inventory Service Tag Category	Allows deletion of a tag category.	Any object

Table 11-26. vCenter Inventory Service Privileges (Continued)

Privilege Name	Description	Required On
vCenter Inventory Service.vCenter Inventory Service Tagging.Delete Inventory Service Tag	Allows deletion of a tag.	Any object
vCenter Inventory Service.vCenter Inventory Service Tagging.Edit Inventory Service Tag Category	Allows editing of a tag caategory.	Any object
vCenter Inventory Service.vCenter Inventory Service Tagging.Edit Inventory Service Tag	Allows editing of a tag.	Any object

Virtual Machine Configuration

Virtual Machine Configuration privileges control the ability to configure virtual machine options and devices.

The table describes privileges required for configuring 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 11-27. 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.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

Table 11-27. Virtual Machine Configuration Privileges (Continued)

Privilege Name	Description	Required On
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
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

Virtual Machine Guest operations privileges control the ability to interact with files and programs inside a virtual machine's guest operating system.

The table describes privileges required for virtual machine guest operations accessed through the VMware vSphere 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 11-28. Virtual Machine Guest Operations

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

Virtual Machine Interaction privileges control the ability to interact with a virtual machine console, configure media, perform power operations, and install VMware Tools.

The table describes privileges required for virtual machine interaction.

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 11-29. 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

Table 11-29. Virtual Machine Interaction (Continued)

Privilege Name	Description	Required On
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
Virtual machine.Interaction.Disable Fault Tolerance	Allows disabling the Secondary virtual machine for a virtual machine using Fault Tolerance.	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.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

Table 11-29. Virtual Machine Interaction (Continued)

Privilege Name	Description	Required On
Virtual machine.Interaction.Turn Off Fault Tolerance	Allows turning off Fault Tolerance for a virtual machine.	Virtual machines
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

Virtual Machine Inventory privileges control adding, moving, and removing virtual machines.

The table describes privileges required to add, move, and remove virtual machines 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 11-30. 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	Allow 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, you must have this privilege assigned to 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, you must have this privilege assigned to both the object and its parent object.	Virtual machines

Virtual Machine Provisioning

Virtual Machine Provisioning privileges control activities related to deploying and customizing virtual machines.

The table describes privileges required for virtual machine provisioning.

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 11-31. 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 Snapshot Management Privileges

Virtual machine snapshot management privileges control the ability to take, delete, rename, and restore snapshots.

The table describes privileges required to work with virtual machine 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 11-32. 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
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

Virtual Machine vSphere replication privileges control the use of replication for virtual machines.

The table describes privileges used for virtual machine replication by VMware vCenter Site Recovery Manager™.

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 11-33. Virtual Machine vSphere Replication

Privilege Name	Description	Required On
Virtual machine.vSphere Replication.Configure vSphere Replication	Allows configuration of replication for the virtual machine.	Virtual machines
Virtual machine.vSphere Replication.Manage vSphere Replication	Allows triggering of full sync, online sync or offline sync on a replication.	Virtual machines
Virtual machine.vSphere Replication.Monitor vSphere Replication	Allows monitoring of replication.	Virtual machines

dvPort Group

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 11-34. Distributed Virtual Port Group Privileges

Privilege Name	Description	Required On
Distributed switch.Create	Allows creation of a distributed virtual port group.	Virtual port groups
Distributed switch.Delete	Allows deletion of distributed virtual port group. To have permission to perform this operation, you must have this privilege assigned to both the object and its parent object.	Virtual port groups
Distributed switch.Modify	Allows modification of a distributed virtual port group configuration.	Virtual port groups
Distributed switch.Policy operation	Allows setting the policy of a distributed virtual port group.	Virtual port groups
Distributed switch.Port configuration operation	Allows setting the scope of a distributed virtual port group.	Virtual port groups

vServices

vServices privileges control the ability to create, configure, and update vService dependencies for virtual machines and vApps.

The table describes privileges related to vService dependencies.

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 11-35. 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

VRM Policy

VRM policy privileges control the ability to query and update virtual rights management policies.

The table describes privileges related to virtual rights 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 11-36. VRM Policy Privileges

Privilege Name	Description	Required On
VRMPolicy.Query VRMPolicy	Allows querying virtual rights management policy.	Virtual machines
VRMPolicy.Update VRMPolicy	Allows update of virtual rights management policy.	Virtual machines

Index

T

U