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.
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
Contents

About This Book 5

Updated Information 7

1 Security for ESXi Systems 9
   ESXi Architecture and Security Features 9
   Security Resources and Information 16

2 Securing ESXi Configurations 17
   Securing the Network with Firewalls 17
   Securing Virtual Machines with VLANs 22
   Securing Standard Switch Ports 27
   Internet Protocol Security 28
   Securing iSCSI Storage 32
   Cipher Strength 34

3 Securing the Management Interface 37
   General Security Recommendations 37
   ESXi Firewall Configuration 38
   ESXi Firewall Commands 42

4 Authentication and User Management 43
   Securing ESXi Through Authentication and Permissions 43
   Managing vSphere Users 44
   Managing vSphere Groups 48
   Password Requirements 49
   Assigning Permissions 50
   Assigning Roles 60
   Using Active Directory to Manage Users and Groups 65
   Using vSphere Authentication Proxy 67

5 Encryption and Security Certificates for ESXi and vCenter Server 73
   Enable Certificate Checking and Verify Host Thumbprints 74
   Generate New Certificates for ESXi 74
   Replace a Default Host Certificate with a CA-Signed Certificate 75
   Replace a Default ESXi Certificate with a CA-Signed Certificate Using the vifs Command 76
   Replace a Default ESXi Certificate and Key Using HTTPS PUT 76
   Upload an SSH Key Using HTTPS PUT 77
   Upload an SSH Key Using a vifs Command 77
   Configure SSL Timeouts 78
   Modifying ESXi Web Proxy Settings 79
6 Lockdown Mode 83
   Lockdown Mode Behavior 84
   Lockdown Mode Configurations 84
   Enable Lockdown Mode Using the vSphere Client 85
   Enable Lockdown Mode from the Direct Console User Interface 85
   Using the ESXi Shell 85

7 Best Practices for Virtual Machine and Host Security 89
   Virtual Machine Recommendations 89
   Auto Deploy Security Considerations 94
   Host Password Strength and Complexity 94

Index 97
About This Book

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

To help you protect your ESXi™ installation, this documentation describes security features built in to ESXi and the measures that you can take to safeguard it from attack.

**Intended Audience**

This information is intended for anyone who wants to secure their ESXi configuration. The information is written for experienced Windows or Linux system administrators who are familiar with virtual machine technology and datacenter operations.
Updated Information

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

<table>
<thead>
<tr>
<th>Revision</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>000789-01</td>
<td>Added topic “Replace a Default ESXi Certificate with a CA-Signed Certificate Using the vifs Command,” on page 76.</td>
</tr>
<tr>
<td>000789-00</td>
<td>Initial release.</td>
</tr>
</tbody>
</table>
Security for ESXi Systems

ESXi is developed with a focus on strong security. VMware ensures security in the ESXi environment and addresses system architecture from a security standpoint.

This chapter includes the following topics:
- “ESXi Architecture and Security Features,” on page 9
- “Security Resources and Information,” on page 16

ESXi Architecture and Security Features

The components and the overall architecture of ESXi are designed to ensure security of the ESXi system as a whole.

From a security perspective, ESXi consists of three major components: the virtualization layer, the virtual machines, and the virtual networking layer.

Figure 1-1. ESXi Architecture
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.

**Trusted Platform Module (TPM)**  
Each time ESXi boots, it measures the VMkernel and a subset of the loaded modules (VIBs) and stores the measurements into Platform Configuration Register (PCR) 20 of the TPM. This behavior is enabled by default and cannot be disabled. Hardware support for this feature is fully tested and supported by VMware and its OEM partners.

**NOTE**  
Not all VIBs are measured as part of this process.

The VMware TPM/TXT feature that leverages the fully tested hardware support is suitable for a proof-of-concept that demonstrates monitoring of certain TPM PCR values, by alerting when any values change from one boot to the next. Third-party solutions could use this feature to detect changes to VIB measurements stored in these PCRs for the following cases:

- Corruption of the measured images
- Unexpected or unauthorized updates, or other types of changes to the measured images

Security and Virtual Machines

Virtual machines are the containers in which applications and guest operating systems run. By design, all VMware virtual machines are isolated from one another. This isolation enables multiple virtual machines to run securely while sharing hardware and ensures both their ability to access hardware and their uninterrupted performance.

Even a user with system administrator privileges on a virtual machine’s guest operating system cannot breach this layer of isolation to access another virtual machine without privileges explicitly granted by the ESXi system administrator. As a result of virtual machine isolation, if a guest operating system running in a virtual machine fails, other virtual machines on the same host continue to run. The guest operating system failure has no effect on:

- The ability of users to access the other virtual machines
- The ability of the operational virtual machines to access the resources they need
- The performance of the other virtual machines
Each virtual machine is isolated from other virtual machines running on the same hardware. Although virtual machines share physical resources such as CPU, memory, and I/O devices, a guest operating system on an individual virtual machine cannot detect any device other than the virtual devices made available to it.

**Figure 1-2. Virtual Machine Isolation**

![Virtual Machine Resources](image)

Because the VMkernel mediates the physical resources and all physical hardware access takes place through the VMkernel, virtual machines cannot circumvent this level of isolation.

Just as a physical machine communicates with other machines in a network through a network card, a virtual machine communicates with other virtual machines running in the same host through a virtual switch. Further, a virtual machine communicates with the physical network, including virtual machines on other ESXi hosts, through a physical network adapter.

**Figure 1-3. Virtual Networking Through Virtual Switches**

![Virtual Networking](image)

These characteristics apply to virtual machine isolation in a network context:

- If a virtual machine does not share a virtual switch with any other virtual machine, it is completely isolated from virtual networks within the host.
- If no physical network adapter is configured for a virtual machine, the virtual machine is completely isolated from any physical networks.
- If you use the same safeguards (firewalls, antivirus software, and so forth) to protect a virtual machine from the network as you would for a physical machine, the virtual machine is as secure as the physical machine.
You can further protect virtual machines by setting up resource reservations and limits on the host. For example, through the detailed resource controls available in ESXi, you can configure a virtual machine so that it always receives at least 10 percent of the host’s CPU resources, but never more than 20 percent.

Resource reservations and limits protect virtual machines from performance degradation that would result if another virtual machine consumed excessive shared hardware resources. For example, if one of the virtual machines on a host is incapacitated by a denial-of-service (DoS) attack, a resource limit on that machine prevents the attack from taking up so much of the hardware resources that the other virtual machines are also affected. Similarly, a resource reservation on each of the virtual machines ensures that, in the event of high resource demands by the virtual machine targeted by the DoS attack, all the other virtual machines still have enough resources to operate.

By default, ESXi imposes a form of resource reservation by applying a distribution algorithm that divides the available host resources equally among the virtual machines while keeping a certain percentage of resources for use by other system components. This default behavior provides a degree of natural protection from DoS and distributed denial-of-service (DDoS) attacks. You set specific resource reservations and limits on an individual basis to customize the default behavior so that the distribution is not equal across the virtual machine configuration.

**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.
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 1-4. 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 virtual adapters through standard switches. Both of these virtual machines are multi homed.
- Virtual Machine 2 runs a Web server, and Virtual Machine 3 runs as an application server. Both of these virtual machines are single-homed.

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 1-5. 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 through 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 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.

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>
<thead>
<tr>
<th>Topic</th>
<th>Resource</th>
</tr>
</thead>
<tbody>
<tr>
<td>VMware security policy, up-to-date security alerts, security downloads, and focus discussions of security topics</td>
<td><a href="http://www.vmware.com/security/">http://www.vmware.com/security/</a></td>
</tr>
</tbody>
</table>
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. |
| Third-party software support policy | [http://www.vmware.com/support/policies/](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/](http://www.vmware.com/vmtn/resources/) for ESXi compatibility guides.
The industry offers more products and configurations than VMware can test. If VMware does not list a product or configuration in a compatibility guide, Technical Support will attempt to help you with any problems, but cannot guarantee that the product or configuration can be used. Always evaluate security risks for unsupported products or configurations carefully. |
| Compliance and security standards, as well as partner solutions and in-depth content about virtualization and compliance | [http://www.vmware.com/go/compliance/](http://www.vmware.com/go/compliance/) |
| Information about VMsafe technology for protection of virtual machines, including a list of partner solutions | [http://www.vmware.com/go/vmsafe/](http://www.vmware.com/go/vmsafe/) |
You can take measures to promote a secure environment for your ESXi hosts, virtual machines, and iSCSI SANs. Consider network configuration planning from a security perspective and the steps that you can take to protect the components in your configuration from attack.

This chapter includes the following topics:

- “Securing the Network with Firewalls,” on page 17
- “Securing Virtual Machines with VLANs,” on page 22
- “Securing Standard Switch Ports,” on page 27
- “Internet Protocol Security,” on page 28
- “Securing iSCSI Storage,” on page 32
- “Cipher Strength,” on page 34

### 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 5.0 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 your layout for firewalls between components.

- Physical machines such as vCenter Server systems and ESXi hosts.
- 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.
- 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, vCenter Server and the clients can be behind the firewall, depending on your deployment. 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 for Management Access,” on page 21.

Networks configured with vCenter Server can receive communications through the vSphere 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 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 Client, between the vSphere Client and the ESXi host. This connection is in addition to the connection between the vSphere 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.
Firewalls for Configurations Without vCenter Server

If you connect clients directly to your ESXi network instead of using vCenter Server, your firewall configuration is somewhat simpler.

Networks configured without vCenter Server receive communications through the same types of clients as they do if vCenter Server were present: the vSphere Client or third-party network management clients. For the most part, the firewall needs are the same, but there are several key differences.

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

If you are using the vSphere Client and do not want to use port 443 as the port for vSphere Client-to-vCenter Server communication, you can switch to another port by changing the vCenter Server settings in the vSphere Client. To learn how to change these settings, see the vCenter Server and Host Management documentation.

Connecting to the Virtual Machine Console Through a Firewall

Whether you connect your client to ESXi hosts through vCenter Server or use a direct connection to the host, 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.

Port 902

This is the port that vCenter Server assumes is available for receiving data from ESXi. The vSphere Client uses this port to provide a connection for guest operating system mouse, keyboard, screen (MKS) activities on virtual machines. It is through this port that users interact with the virtual machine guest operating systems and applications. Port 902 is the port that the vSphere Client assumes is available when interacting with virtual machines.
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.

**Port 443**

The vSphere Client and SDK use this port to send data to vCenter Server managed hosts. Also, the vSphere Client and SDK, when connected directly to ESXi, use this port to support any management functions related to the server and its virtual machines. Port 443 is the port that clients assume is available when sending data to ESXi. VMware does not support configuring a different port for these connections.

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

**Port 903**

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. Port 903 is the port that the vSphere Client assumes is available when interacting with virtual machines. VMware does not support configuring a different port for this function.

Port 903 connects the vSphere Client to a specified virtual machine configured on ESXi.

The following figure shows the relationships between vSphere Client functions, ports, and processes.

**Figure 2-1. Port Use for vSphere Client Communications with ESXi**

If you have a firewall between your vCenter Server system and vCenter Server managed host, open ports 443 and 903 in the firewall to allow data transfer to ESXi hosts from vCenter Server and ESXi hosts directly from the vSphere Client.

For additional information on configuring the ports, see the firewall system administrator.
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 “TCP and UDP Ports for Management Access,” on page 21 for a list of ports. Refer to the firewall system administrator for additional information on configuring the ports.

TCP and UDP Ports for Management Access

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).

Table 2-1. TCP and UDP Ports

<table>
<thead>
<tr>
<th>Port</th>
<th>Purpose</th>
<th>Traffic Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>22 (Default)</td>
<td>SSH Server</td>
<td>Incoming TCP</td>
</tr>
<tr>
<td>53 (Default)</td>
<td>DNS Client</td>
<td>Incoming and outgoing UDP</td>
</tr>
<tr>
<td>68 (Default)</td>
<td>DHCP Client</td>
<td>Incoming and outgoing UDP</td>
</tr>
<tr>
<td>161 (Default)</td>
<td>SNMP Server</td>
<td>Incoming UDP</td>
</tr>
<tr>
<td>80 (Default)</td>
<td>vSphere Fault Tolerance (FT) (outgoing TCP, UDP) HTTP access</td>
<td>Incoming TCP</td>
</tr>
<tr>
<td></td>
<td>The default non-secure TCP Web port typically used in conjunction with port</td>
<td>Outgoing TCP, UDP</td>
</tr>
<tr>
<td></td>
<td>443 as a front end for access to ESXi networks from the Web. Port 80 redirects</td>
<td></td>
</tr>
<tr>
<td></td>
<td>traffic to an HTTPS landing page (port 443). WS-Management</td>
<td></td>
</tr>
<tr>
<td>123</td>
<td>NTP Client</td>
<td>Outgoing UDP</td>
</tr>
<tr>
<td>427 (Default)</td>
<td>The CIM client uses the Service Location Protocol, version 2 (SLPv2) to find</td>
<td>Incoming and outgoing UDP</td>
</tr>
<tr>
<td></td>
<td>CIM servers.</td>
<td></td>
</tr>
<tr>
<td>443 (Default)</td>
<td>HTTPS access</td>
<td>Incoming TCP</td>
</tr>
<tr>
<td></td>
<td>vCenter Server access to ESXi hosts</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Default SSL Web port</td>
<td></td>
</tr>
<tr>
<td></td>
<td>vSphere Client access to vCenter Server</td>
<td></td>
</tr>
<tr>
<td></td>
<td>vSphere Client access to ESXi hosts</td>
<td></td>
</tr>
<tr>
<td></td>
<td>WS-Management</td>
<td></td>
</tr>
<tr>
<td></td>
<td>vSphere Client access to vSphere Update Manager</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Third-party network management client connections to vCenter Server</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Third-party network management clients access to hosts</td>
<td></td>
</tr>
<tr>
<td>902 (Default)</td>
<td>Host access to other hosts for migration and provisioning</td>
<td>Incoming and outgoing TCP, outgoing UDP</td>
</tr>
<tr>
<td></td>
<td>Authentication traffic for ESXi and remote console traffic (xinetd/vmware-authd)</td>
<td></td>
</tr>
<tr>
<td></td>
<td>vSphere Client access to virtual machine consoles (UDP) Status update (heartbeat) connection from ESXi to vCenter Server</td>
<td></td>
</tr>
</tbody>
</table>
In addition to the TCP and UDP ports, you can configure other ports depending on your needs.

### 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. You can add security to your virtual machine network in several ways.

If your virtual machine network is connected to a physical network, it can be subject to breaches to the same degree that a network made up of physical machines is. 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 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.

You can add this level of security in different ways.

- Adding 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 serves as a protective buffer between the physical network adapter and the remaining virtual machines in the virtual network.

---

### Table 2-1. TCP and UDP Ports (Continued)

<table>
<thead>
<tr>
<th>Port</th>
<th>Purpose</th>
<th>Traffic Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>903</td>
<td>Remote console traffic generated by user access to virtual machines on a</td>
<td>Incoming TCP</td>
</tr>
<tr>
<td></td>
<td>specific host. vSphere Client access to virtual machine consoles</td>
<td></td>
</tr>
<tr>
<td></td>
<td>MKS transactions (xinetd/vmware-authd-mks)</td>
<td></td>
</tr>
<tr>
<td>1234,</td>
<td>vSphere Replication</td>
<td>Outgoing TCP</td>
</tr>
<tr>
<td>1235</td>
<td>(Default)</td>
<td></td>
</tr>
<tr>
<td>2049</td>
<td>Transactions from NFS storage devices</td>
<td>Incoming and outgoing TCP</td>
</tr>
<tr>
<td></td>
<td>This port is used on the VMkernel interface.</td>
<td></td>
</tr>
<tr>
<td>3260</td>
<td>Transactions to iSCSI storage devices</td>
<td>Outgoing TCP</td>
</tr>
<tr>
<td>5900-5964</td>
<td>RFB protocol, which is used by management tools such as VNC</td>
<td>Incoming and outgoing TCP</td>
</tr>
<tr>
<td>5988 (Default)</td>
<td>CIM transactions over HTTP</td>
<td>Incoming TCP</td>
</tr>
<tr>
<td>5989 (Default)</td>
<td>CIM XML transactions over HTTPS</td>
<td>Incoming and outgoing TCP</td>
</tr>
<tr>
<td>8000 (Default)</td>
<td>Requests from vMotion</td>
<td>Incoming and outgoing TCP</td>
</tr>
<tr>
<td>8100,</td>
<td>Traffic between hosts for vSphere Fault Tolerance (FT)</td>
<td>Incoming and outgoing TCP, UDP</td>
</tr>
<tr>
<td>8200 (Default)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>8182</td>
<td>Traffic between hosts for vSphere High Availability (HA)</td>
<td>Incoming and outgoing TCP, incoming and outgoing UDP</td>
</tr>
</tbody>
</table>

In addition to the TCP and UDP ports, you can configure other ports depending on your needs.
Installing a host-based firewall on virtual machines at the head of virtual networks is a good security practice. However, because host-based firewalls can slow performance, balance your security needs against performance before you decide to install host-based firewalls on virtual machines elsewhere in the virtual network.

- Keeping different virtual machine zones within a host on different network segments. If you isolate virtual machine zones on their own network segments, you minimize the risks 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 denials of service, 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 of which 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.

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.
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.
VLANs as Part of a Broader Security Implementation

VLANs are an effective means of controlling where and how widely data is transmitted within the network. If an attacker gains access to the network, the attack is likely to be limited to the VLAN that served as the entry point, lessening the risk to the network as a whole.

VLANs provide protection only in that they control how data is routed and contained after it passes through the switches and enters the network. You can use VLANs to help secure Layer 2 of your network architecture—the data link layer. However, configuring VLANs does not protect the physical layer of your network model or any of the other layers. Even if you create VLANs, provide additional protection by securing your hardware (routers, hubs, and so forth) and encrypting data transmissions.

VLANs are not a substitute for firewalls in your virtual machine configurations. Most network configurations that include VLANs also include firewalls. If you include VLANs in your virtual network, be sure that the firewalls that you install are VLAN-aware.

Properly Configure VLANs

Equipment misconfiguration and network hardware, firmware, or software defects can make a VLAN susceptible to VLAN-hopping attacks.

VLAN hopping occurs when an attacker with authorized access to one VLAN creates packets that trick physical switches into transmitting the packets to another VLAN that the attacker is not authorized to access. Vulnerability to this type of attack usually results from a switch being misconfigured for native VLAN operation, in which the switch can receive and transmit untagged packets.

To help prevent VLAN hopping, keep your equipment up to date by installing hardware and firmware updates as they become available. Also, follow your vendor’s best practice guidelines when you configure your equipment.

VMware standard switches do not support the concept of a native VLAN. All data passed on these switches is appropriately tagged. However, because other switches in the network might be configured for native VLAN operation, VLANs configured with standard switches can still be vulnerable to VLAN hopping.

If you plan to use VLANs to enforce network security, disable the native VLAN feature for all switches unless you have a compelling reason to operate some of your VLANs in native mode. If you must use native VLAN, see your switch vendor’s configuration guidelines for this feature.

Standard Switch Protection and VLANs

VMware standard switches provide safeguards against certain threats to VLAN security. Because of the way that standard switches are designed, they protect VLANs against a variety of attacks, many of which involve VLAN hopping.

Having this protection does not guarantee that your virtual machine configuration is invulnerable to other types of attacks. For example, standard switches do not protect the physical network against these attacks; they protect only the virtual network.
Standard switches and VLANs can protect against the following types of attacks.

<table>
<thead>
<tr>
<th>Type of Attack</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>MAC flooding</strong></td>
<td>Floods a switch with packets that contain MAC addresses tagged as having come from different sources. Many switches use a content-addressable memory table to learn and store the source address for each packet. When the table is full, the switch can enter a fully open state in which every incoming packet is broadcast on all ports, letting the attacker see all of the switch’s traffic. This state might result in packet leakage across VLANs. Although VMware standard switches store a MAC address table, they do not get the MAC addresses from observable traffic and are not vulnerable to this type of attack.</td>
</tr>
<tr>
<td><strong>802.1q and ISL tagging attacks</strong></td>
<td>Force a switch to redirect frames from one VLAN to another by tricking the switch into acting as a trunk and broadcasting the traffic to other VLANs. VMware standard switches do not perform the dynamic trunking required for this type of attack and, therefore, are not vulnerable.</td>
</tr>
<tr>
<td><strong>Double-encapsulation attacks</strong></td>
<td>Occur when an attacker creates a double-encapsulated packet in which the VLAN identifier in the inner tag is different from the VLAN identifier in the outer tag. For backward compatibility, native VLANs strip the outer tag from transmitted packets unless configured to do otherwise. When a native VLAN switch strips the outer tag, only the inner tag is left, and that inner tag routes the packet to a different VLAN than the one identified in the now-missing outer tag. VMware standard switches drop any double-encapsulated frames that a virtual machine attempts to send on a port configured for a specific VLAN. Therefore, they are not vulnerable to this type of attack.</td>
</tr>
<tr>
<td><strong>Multicast brute-force attacks</strong></td>
<td>Involve sending large numbers of multicast frames to a known VLAN almost simultaneously to overload the switch so that it mistakenly allows some of the frames to broadcast to other VLANs. VMware standard switches do not allow frames to leave their correct broadcast domain (VLAN) and are not vulnerable to this type of attack.</td>
</tr>
<tr>
<td><strong>Spanning-tree attacks</strong></td>
<td>Target Spanning-Tree Protocol (STP), which is used to control bridging between parts of the LAN. The attacker sends Bridge Protocol Data Unit (BPDU) packets that attempt to change the network topology, establishing themselves as the root bridge. As the root bridge, the attacker can sniff the contents of transmitted frames. VMware standard switches do not support STP and are not vulnerable to this type of attack.</td>
</tr>
<tr>
<td><strong>Random frame attacks</strong></td>
<td>Involve sending large numbers of packets in which the source and destination addresses stay the same, but in which fields are randomly changed in length, type, or content. The goal of this attack is to force packets to be mistakenly rerouted to a different VLAN. VMware standard switches are not vulnerable to this type of attack.</td>
</tr>
</tbody>
</table>

Because new security threats develop over time, do not consider this an exhaustive list of attacks. Regularly check VMware security resources on the Web to learn about security, recent security alerts, and VMware security tactics.
Securing Standard Switch Ports

As with physical network adapters, a virtual network adapter can send frames that appear to be from a different machine or impersonate another machine so that it can receive network frames intended for that machine. Also, like physical network adapters, a virtual network adapter can be configured so that it receives frames targeted for other machines.

When you create a standard switch for your network, you add port groups to impose a policy configuration for the virtual machines and storage systems attached to the switch. You create virtual ports through the vSphere Client.

As part of adding a port or standard port group to a standard switch, the vSphere Client configures a security profile for the port. You can use this security profile to ensure that the host prevents the guest operating systems for 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 profile 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 the basics of how virtual network adapters control transmissions and how attacks are staged at this level.

Each virtual network adapter has its own MAC address assigned when the adapter is created. This address is called the initial MAC address. Although the initial MAC address can be reconfigured from outside the guest operating system, it cannot be changed by the guest operating system. In addition, each adapter has an effective MAC address that filters out incoming network traffic with a destination MAC address 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.

When sending packets, an operating system typically places its own network adapter’s effective MAC address in the source MAC address field of the Ethernet frame. It also places the MAC address for the receiving network adapter in the destination MAC address field. The receiving adapter accepts packets only when the destination MAC address in the packet matches its own effective MAC address.

Upon creation, a network adapter’s effective MAC address and initial MAC address are the same. The virtual machine’s 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 destined for the new MAC address. The operating system can send frames with an impersonated source MAC address at any time. 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 use standard switch security profiles on hosts to protect against this type of attack by setting three options. If you change any default settings for a port, you must modify the security profile by editing standard switch settings in the vSphere Client.

**MAC Address Changes**

The setting for the MAC Address Changes option affects traffic that a virtual machine receives.

When the option is set to **Accept**, ESXi accepts requests to change the effective MAC address to other than the initial MAC address.

When the option is set to **Reject**, ESXi does not honor requests to change the effective MAC address to anything other than the initial MAC address, which protects the host against MAC impersonation. The port that the virtual adapter used to send the request is disabled and the virtual adapter does not receive any more frames until it changes the effective MAC address to match the initial MAC address. The guest operating system does not detect that the MAC address change 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 and have 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.

MAC address changes settings affect traffic leaving a virtual machine. MAC address changes will occur if the sender is permitted to make them, even if standard switches or a receiving virtual machine does not permit MAC address changes.

Forged Transmissions

The setting for the Forged Transmits option affects traffic that is transmitted from a virtual machine.

When the option is set to Accept, ESXi does not compare source and effective MAC addresses.

To protect against MAC impersonation, you can set this option to Reject. If you do, the host compares the source MAC address being transmitted by the operating system with the effective MAC address for its adapter to see if they match. If the addresses do not match, ESXi drops the packet.

The guest operating system does not detect that its virtual network 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 network adapter would perform so that the guest operating system receives all traffic observed on the wire. By default, the virtual network 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 regardless of whether 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 switch to operate in promiscuous mode (for example, if you are running network intrusion detection software or a packet sniffer).

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 is 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, 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.

Add a Security Association

Add a security association to specify encryption parameters for associated IP traffic.

You can add a security association using the vicfg-ipv6 vSphere CLI command.
In the procedure, `--server=server_name` specifies the target server. The specified target server prompts you for a user name and password. Other connection options, such as a configuration file or session file, are supported. For a list of connection options, see *Getting Started with vSphere Command-Line Interfaces*.

**Prerequisites**

Install vCLI or deploy the vSphere Management Assistant (vMA) virtual machine. See *Getting Started with vSphere Command-Line Interfaces*. For troubleshooting, run `esxcli` commands in the ESXi Shell.

**Procedure**

- At the command prompt, enter the command `vicfg-ipsec --server=server_name --add-sa` with one or more of the following options.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>--sa-src source address</code></td>
<td>Specify the source address.</td>
</tr>
<tr>
<td><code>--sa-dst destination address</code></td>
<td>Specify the destination address.</td>
</tr>
<tr>
<td><code>--sa-mode mode</code></td>
<td>Specify the mode, either transport or tunnel.</td>
</tr>
<tr>
<td><code>--spi security parameter index</code></td>
<td>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.</td>
</tr>
<tr>
<td><code>--ealgo encryption algorithm</code></td>
<td>Specify the encryption algorithm using one of the following parameters.</td>
</tr>
<tr>
<td></td>
<td>- 3des-cbc</td>
</tr>
<tr>
<td></td>
<td>- aes128-cbc</td>
</tr>
<tr>
<td></td>
<td>- null</td>
</tr>
<tr>
<td></td>
<td>null provides no encryption.</td>
</tr>
<tr>
<td><code>--ekey encryption key</code></td>
<td>Specify the encryption key. You can enter keys as ASCII text or as a hexadecimal with a 0x prefix.</td>
</tr>
<tr>
<td><code>--ialgo authentication algorithm</code></td>
<td>Specify the authentication algorithm, either hmac-sha1 or hmac-sha2-256.</td>
</tr>
<tr>
<td><code>--ikey authentication key</code></td>
<td>Specify the authentication key. You can enter keys as ASCII text or as a hexadecimal with a 0x prefix.</td>
</tr>
<tr>
<td><code>name</code></td>
<td>Provide a name for the security association.</td>
</tr>
</tbody>
</table>

**Example: New Security Association Command**

The following example contains extra line breaks for readability.

```
vicfg-ipsec --server=server_name --add-sa
  --sa-src 3ffe:501:ffff:0::a
  --sa-mode transport
  --spi 0x1000
  --ealgo 3des-cbc
  --ekey 0x6970763672656164796c6f676f3364657362636f757432
  --ialgo hmac-sha1
  --ikey 0x6970763672656164796c6f67736861316f757432
  sa1
```

**Remove a Security Association**

You can remove a security association from the host.

You can remove a security association using the `vicfg-ipsec` command.
In the procedure, `--server=server_name` specifies the target server. The specified target server prompts you for a user name and password. Other connection options, such as a configuration file or session file, are supported. For a list of connection options, see *Getting Started with vSphere Command-Line Interfaces*.

### 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.

Install vCLI or deploy the vSphere Management Assistant (vMA) virtual machine. See *Getting Started with vSphere Command-Line Interfaces*. For troubleshooting, run `esxcli` commands in the ESXi Shell.

### Procedure

- At the command prompt, enter the command
  
  \[
  \text{vicfg-ipsec --server=server_name --remove-sa security_association_name}.
  \]

### 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 `vicfg-ipsec` command.

In the procedure, `--server=server_name` specifies the target server. The specified target server prompts you for a user name and password. Other connection options, such as a configuration file or session file, are supported. For a list of connection options, see *Getting Started with vSphere Command-Line Interfaces*.

### Prerequisites

Install vCLI or deploy the vSphere Management Assistant (vMA) virtual machine. See *Getting Started with vSphere Command-Line Interfaces*. For troubleshooting, run `esxcli` commands in the ESXi Shell.

### Procedure

- At the command prompt, enter the command
  
  \[
  \text{vicfg-ipsec --server=server_name -l}.
  \]

ESXi displays a list of all available security associations.

### 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 `vicfg-ipsec` vSphere CLI command.

In the procedure, `--server=server_name` specifies the target server. The specified target server prompts you for a user name and password. Other connection options, such as a configuration file or session file, are supported. For a list of connection options, see *Getting Started with vSphere Command-Line Interfaces*.

### 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 28.

Install vCLI or deploy the vSphere Management Assistant (vMA) virtual machine. See *Getting Started with vSphere Command-Line Interfaces*. For troubleshooting, run `esxcli` commands in the ESXi Shell.
Procedure

- At the command prompt, enter the command `vicfg-ipsec --server=server_name --add-sp` with one or more of the following options.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>--sp-src source address</code></td>
<td>Specify the source IP address and prefix length.</td>
</tr>
<tr>
<td><code>--sp-dst destination address</code></td>
<td>Specify the destination address and prefix length.</td>
</tr>
<tr>
<td><code>--src-port port</code></td>
<td>Specify the source port. The source port must be a number between 0 and 65535.</td>
</tr>
<tr>
<td><code>--dst-port port</code></td>
<td>Specify the destination port. The source port must be a number between 0 and 65535.</td>
</tr>
<tr>
<td><code>--ulproto protocol</code></td>
<td>Specify the upper layer protocol using one of the following parameters.</td>
</tr>
<tr>
<td></td>
<td>tcp</td>
</tr>
<tr>
<td></td>
<td>udp</td>
</tr>
<tr>
<td></td>
<td>icmp6</td>
</tr>
<tr>
<td></td>
<td>any</td>
</tr>
<tr>
<td><code>--dir direction</code></td>
<td>Specify the direction in which you want to monitor traffic using either in or out.</td>
</tr>
<tr>
<td><code>--action action</code></td>
<td>Specify the action to take when traffic with the specified parameters is encountered using one of the following parameters.</td>
</tr>
<tr>
<td></td>
<td>none: Take no action</td>
</tr>
<tr>
<td></td>
<td>discard: Do not allow data in or out.</td>
</tr>
<tr>
<td></td>
<td>ipsec: Use the authentication and encryption information supplied in the security association to determine whether the data comes from a trusted source.</td>
</tr>
<tr>
<td><code>--sp-mode mode</code></td>
<td>Specify the mode, either tunnel or transport.</td>
</tr>
<tr>
<td><code>--sa-name security association name</code></td>
<td>Provide the name of the security association for the security policy to use.</td>
</tr>
<tr>
<td><code>name</code></td>
<td>Provide a name for the security policy.</td>
</tr>
</tbody>
</table>

Example: New Security Policy Command

The following example includes extra line breaks for readability.

```
vicfg-ipsec --server=server_name --add-sp
--sp-src 2001:db8:1::/64
--sp-dst 2002:db8:1::/64
--src-port 23
--dst-port 25
--ulproto tcp
--dir out
--action ipsec
--sp-mode transport
--sa-name sa1
sp1
```

Remove a Security Policy

You can remove a security policy from the ESXi host.

You can remove a security policy using the `vicfg-ipsec` command.

In the procedure, `--server=server_name` specifies the target server. The specified target server prompts you for a user name and password. Other connection options, such as a configuration file or session file, are supported. For a list of connection options, see *Getting Started with vSphere Command-Line Interfaces*. 
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.

Install vCLI or deploy the vSphere Management Assistant (vMA) virtual machine. See Getting Started with vSphere Command-Line Interfaces. For troubleshooting, run esxcli commands in the ESXi Shell.

Procedure

- At the command prompt, enter the command
  
  \texttt{vicfg-ipsec server=server\_name --remove-sp security\_policy\_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 \texttt{vicfg-ipsec} command.

In the procedure, \texttt{--server=server\_name} specifies the target server. The specified target server prompts you for a user name and password. Other connection options, such as a configuration file or session file, are supported. For a list of connection options, see Getting Started with vSphere Command-Line Interfaces.

Prerequisites

Install vCLI or deploy the vSphere Management Assistant (vMA) virtual machine. See Getting Started with vSphere Command-Line Interfaces. For troubleshooting, run esxcli commands in the ESXi Shell.

Procedure

- At the command prompt, enter the command \texttt{vicfg-ipsec --server=server\_name -L}.

  The host displays a list of all available security policies.

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.

\textbf{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 Client to determine whether authentication is being performed and to configure the authentication method.

**Enabling Challenge Handshake Authentication Protocol (CHAP) for iSCSI SANs**

You can configure the iSCSI SAN to use CHAP authentication.

In CHAP authentication, when the initiator contacts an iSCSI target, the target sends a predefined ID value and a random value, or key, to the initiator. The initiator creates a one-way hash value that it sends to the target. The hash contains three elements: a predefined ID value, the random value that the target sends, and a private value, or CHAP secret, that the initiator and target share. When the target receives the hash from the initiator, it creates its own hash value by using the same elements and compares it to the initiator’s hash. If the results match, the target authenticates the initiator.

ESXi supports unidirectional and bidirectional CHAP authentication for iSCSI. In unidirectional CHAP authentication, the target authenticates the initiator, but the initiator does not authenticate the target. In bidirectional CHAP authentication, an additional level of security enables the initiator to authenticate the target.

ESXi supports CHAP authentication at the adapter level, when only one set of authentication credentials can be sent from the host to all targets. It also supports per-target CHAP authentication, which enables you to configure different credentials for each target to achieve greater target refinement.

See the *vSphere Storage* documentation for information about how to work with CHAP.

**Disabling iSCSI SAN Authentication**

You can configure the iSCSI SAN to use no authentication. Communications between the initiator and target are still authenticated in a rudimentary way because the iSCSI target devices are typically set up to communicate with specific initiators only.

Choosing not to enforce more stringent authentication can make sense if your iSCSI storage is housed in one location and you create a dedicated network or VLAN to service all your iSCSI devices. The iSCSI configuration is secure because it is isolated from any unwanted access, much as a Fibre Channel SAN is.

As a basic rule, disable authentication only if you are willing to risk an attack to the iSCSI SAN or cope with problems that result from human error.

See the *vSphere Storage* documentation for information about how to work with CHAP.

**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.

**Cipher Strength**

Transmitting data over insecure connections presents a security risk because malicious users might be able to scan data as it travels through the network. As a safeguard, network components commonly encrypt the data so that it cannot be easily read.

To encrypt data, the sending component, such as a gateway or redirector, applies 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.

To ensure the protection of the data transmitted to and from external network connections, ESXi uses one of the strongest block ciphers available—256-bit AES block encryption. ESXi also uses 1024-bit RSA for key exchange. These encryption algorithms are the default for the following connections:

- vSphere Client connections to vCenter Server and to ESXi through the management interface.
- SDK connections to vCenter Server and to ESXi.
- Management interface connections to virtual machines through the VMkernel.
- SSH connections to ESXi through the management interface.
**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. If this configuration is too restricted for your needs, you can lower security parameters.
Securing the Management Interface

Security of the ESXi management interface is critical to protect against unauthorized intrusion and misuse. If a host is compromised in certain ways, the virtual machines it interacts with might also be compromised. To minimize the risk of an attack through the management interface, ESXi is protected with a firewall.

This chapter includes the following topics:

- “General Security Recommendations,” on page 37
- “ESXi Firewall Configuration,” on page 38
- “ESXi Firewall Commands,” on page 42

General 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, but if you do so, make sure that you are working in a trusted environment and 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 management interface and enforce access security policies like setting up password restrictions.

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

  Also, strive to run only the essential processes, services, and agents such as virus checkers, and virtual machine backups.

- **Use the vSphere Client to administer your 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 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 SHA-1 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, if needed, issues a security patch.
- 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. If you must use insecure services and have implemented sufficient protection for the host, you must explicitly open ports to support them.

**NOTE** Follow only VMware security advisories, found at [http://www.vmware.com/security/](http://www.vmware.com/security/).

### 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 for Management Access,”* on page 21.

**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 40 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 only.

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.

An indication of 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**

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 can enable or disable these services and agents using the vSphere 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. Log in to a vCenter Server system using the vSphere Client.
2. Select the host in the inventory panel.
3. Click the **Configuration** tab and click **Security Profile**.

   The vSphere Client displays a list of active incoming and outgoing connections with the corresponding firewall ports.

4. In the Firewall section, click **Properties**.

   The Firewall Properties dialog box lists all the rule sets that you can configure for the host.
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 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

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

You can use the vSphere Client or the command line to update the Allowed IP list for a service. By default,
all IP addresses are allowed.

Procedure

1 Log in to a vCenter Server system using the vSphere Client.
2 Select the host in the inventory panel.
3 Click the Configuration tab and click Security Profile.
4 In the Firewall section, click Properties.
5 Select a service in the list and click Firewall.
6 Select Only allow connections from the following networks and enter the IP addresses of networks
that are allowed to connect to the host.

You can enter IP addresses in the following formats: 192.168.0.0/24, 192.168.1.2, 2001::1/64, or fd3e:
29a6:0a81:e478::/64.

7 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 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.

**Set Service or Client Startup Options**

By default, daemon processes start when any of their ports are opened and stop when all of their ports are closed. You can change this startup policy for the selected service or client.

**Procedure**

1. Log in to a vCenter Server system using the vSphere Client.
2. Select the host in the inventory panel.
3. Click the Configuration tab and click Security Profile.
4. In the Firewall section, click Properties.

   The Firewall Properties dialog box lists all the services and management agents you can configure for the host.
Select the service or management agent to configure and click Options.

The Startup Policy dialog box determines when the service starts. This dialog box also provides information about the current state of the service and provides an interface for manually starting, stopping, or restarting the service.

Select a policy from the Startup Policy list. Click OK.

**ESXi Firewall Commands**

You can configure the ESXi firewall at the command line.

**Firewall Configuration Using the ESXi Shell**

The vSphere Client graphical user interface provides the preferred means of performing many configuration tasks. However, you can use the ESXi Shell to configure ESXi at the command line if necessary.

**Table 3-1. Firewall Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>esxcli network firewall get</td>
<td>Returns the enabled or disabled status of the firewall and lists default actions.</td>
</tr>
<tr>
<td>esxcli network firewall set --defaultaction</td>
<td>Update default actions.</td>
</tr>
<tr>
<td>esxcli network firewall set --enabled</td>
<td>Enable or disable the ESXi firewall.</td>
</tr>
<tr>
<td>esxcli network firewall load</td>
<td>Load the firewall module and rule set configuration files.</td>
</tr>
<tr>
<td>esxcli network firewall refresh</td>
<td>Refresh the firewall configuration by reading the rule set files if the firewall module is loaded.</td>
</tr>
<tr>
<td>esxcli network firewall unload</td>
<td>Destroy filters and unload the firewall module.</td>
</tr>
<tr>
<td>esxcli network firewall ruleset list</td>
<td>List rule sets information.</td>
</tr>
<tr>
<td>esxcli network firewall ruleset set --allowedall</td>
<td>Set the allowedall flag.</td>
</tr>
<tr>
<td>esxcli network firewall ruleset set --enabled</td>
<td>Enable or disable the specified rule set.</td>
</tr>
<tr>
<td>esxcli network firewall ruleset allowedip list</td>
<td>List the allowed IP addresses of the specified rule set.</td>
</tr>
<tr>
<td>esxcli network firewall ruleset allowedip add</td>
<td>Allow access to the rule set from the specified IP address or range of IP addresses.</td>
</tr>
<tr>
<td>esxcli network firewall ruleset allowedip remove</td>
<td>Remove access to the rule set from the specified IP address or range of IP addresses.</td>
</tr>
</tbody>
</table>
ESXi handles user authentication and supports user and group permissions. In addition, you can encrypt connections to the vSphere Client and SDK.

This chapter includes the following topics:

- “Securing ESXi Through Authentication and Permissions,” on page 43
- “Managing vSphere Users,” on page 44
- “Managing vSphere Groups,” on page 48
- “Password Requirements,” on page 49
- “Assigning Permissions,” on page 50
- “Assigning Roles,” on page 60
- “Using Active Directory to Manage Users and Groups,” on page 65
- “Using vSphere Authentication Proxy,” on page 67

**Securing ESXi Through Authentication and Permissions**

When a vSphere Client or vCenter Server user connects to ESXi, a connection is established with the VMware Host Agent process. The process uses the user names and passwords for authentication.

ESXi authenticates users accessing hosts using the vSphere Client or SDK. The default installation of ESXi uses a local password database for authentication.

ESXi uses the Pluggable Authentication Modules (PAM) structure for authentication when users access the ESXi host using the vSphere Client. The PAM configuration for VMware services is located in `/etc/pam.d/system-auth-generic`, which stores paths to authentication modules. Changes to this configuration affect all host services.

The reverse proxy in the VMware Host Agent process listens on ports 80 and 443. vSphere Client or vCenter Server users connect to the host agent through these ports. The host process receives the user name and password from the client and forwards them to the PAM module to perform the authentication.

The following figure shows a basic example of how the host authenticates transactions from the vSphere Client.

>Note: CIM transactions also use ticket-based authentication in connecting with the host process.
To make sure that authentication works efficiently for your site, perform basic tasks such as setting up users, groups, permissions, and roles, configuring user attributes, adding your own certificates, and determining whether you want to use SSL.

Managing vSphere Users

A user is an individual authorized to log in to either ESXi or vCenter Server.

ESXi users fall into two categories: those who can access the host through vCenter Server and those who can access by directly logging in to the host from the vSphere Client, a third-party client, or a command shell.

**Authorized vCenter Server users**

Authorized users for vCenter Server are those included in the Windows domain list that vCenter Server references or are local Windows users on the vCenter Server host.

You cannot use vCenter Server to manually create, remove, or otherwise change users. You must use the tools for managing your Windows domain. Any changes you make are reflected in vCenter Server. However, the user interface does not provide a user list for you to review.

**Direct-access users**

Users authorized to work directly on the host are those added to the internal user list by a system administrator.

An administrator can perform a variety of management activities for these users, such as changing passwords, group memberships, and permissions as well as adding and removing users.

The user list that ESXi maintains locally is separate from the users known to vCenter Server, which are either local Windows users or users that are part of the Windows domain. If Active Directory authentication has been configured on the host, then the same Windows domain users known to vCenter Server will be available on the ESXi host.

Best Practices for vSphere Users

Use best practices for creating and managing users to increase the security and manageability of your vSphere environment.

VMware recommends several best practices for creating users in your vSphere environment:

- Do not create a user named **ALL**. Privileges associated with the name **ALL** might not be available to all users in some situations. For example, if a user named **ALL** has Administrator privileges, a user with **ReadOnly** privileges might be able to log in to the host remotely. This is not the intended behavior.
- Use a directory service or vCenter Server to centralize access control, rather than defining users on individual hosts.
- Choose a local Windows user or group to have the Administrator role in vCenter Server.
- Because of the confusion that duplicate naming can cause, check the vCenter Server user list before you create ESXi host users to avoid duplicating names. To check for vCenter Server users, review the Windows domain list.

**IMPORTANT** By default, some versions of the Windows operating system include the NT AUTHORITY\INTERACTIVE user in the Administrators group. When the NT AUTHORITY\INTERACTIVE user is in the Administrators group, all users you create on the vCenter Server system have the Administrator privilege. To avoid this, remove the NT AUTHORITY\INTERACTIVE user from the Administrators group on the Windows system where you run vCenter Server.

**Add a Local User**

Adding a user to the users table updates the internal user list that the host maintains.

**Prerequisites**

Review the password requirements described in “Password Requirements,” on page 49.

**Procedure**

1. Log in to ESXi using the vSphere Client.
2. Click the Local Users & Groups tab and click Users.
3. Right-click anywhere in the Users table and click Add to open the Add New User dialog box.
4. Enter a login, a user name, a numeric user ID (UID), and a password.

   **NOTE** Do not create a user named ALL. Privileges associated with the name ALL might not be available to all users in some situations. For example, if a user named ALL has Administrator privileges, a user with ReadOnly privileges might be able to log in to the host remotely. This is not the intended behavior.

   - Specifying the user name and UID are optional. If you do not specify the UID, the vSphere Client assigns the next available UID.
   - Create a password that meets the length and complexity requirements. The host checks for password compliance using the default authentication plug-in, pam_passwdqc.so. If the password is not compliant, the following error appears: A general system error occurred: passwd: Authentication token manipulation error.
5. To change the user’s ability to access ESXi through a command shell, select or deselect Grant shell access to this user.

   **NOTE** To be granted shell access, users must also have an Administrator role for an inventory object on the host.

   In general, do not grant shell access unless the user has a justifiable need. Users that access the host only through the vSphere Client do not need shell access.

6. To add the user to a group, select the group name from the Group drop-down menu and click Add.
7. Click OK.
Modify the Settings for a User on the Host

You can change the user ID, user name, password, and group settings for a user. You can also grant a user shell access.

**Prerequisites**

Review the password requirements as described in “Password Requirements,” on page 49.

**Procedure**

1. Log in to ESXi using the vSphere Client.
2. Click the **Local Users & Groups** tab and click **Users**.
3. Right-click the user and click **Edit** to open the Edit User dialog box.
4. To change the user ID, enter a numeric user UID in the **UID** text box.
   The vSphere Client assigns the UID when you first create the user. In most cases, you do not have to change this assignment.
5. Enter a new user name.
6. To change the user’s password, select **Change Password** and enter the new password.
   Create a password that meets the length and complexity requirements. The host checks for password compliance using the default authentication plug-in, `pam_passwdqc.so`. If the password is not compliant, the following error appears: A general system error occurred: passwd: Authentication token manipulation error.
7. To change the user’s ability to access ESXi through a command shell, select or deselect **Grant shell access to this user**.
   **NOTE** To be granted shell access, users must also have an Administrator role for an inventory object on the host.
   In general, do not grant shell access unless the user has a justifiable need. Users that access the host only through the vSphere Client do not need shell access.
8. To add the user to a group, select the group name from the **Group** drop-down menu and click **Add**.
9. To remove the user from a group, select the group name from the **Group membership** box and click **Remove**.
10. Click **OK**.

Remove a User from a Host

You can remove a user from the host.

**CAUTION** Do not remove the root user.

If you remove a user from the host, they lose permissions to all objects on the host and cannot log in again.

**NOTE** Users who are logged in and are removed from the domain keep their host permissions until you restart the host.

**Procedure**

1. Log in to ESXi using the vSphere Client.
2 Click the Local Users & Groups tab and click Users.
3 Right-click the user to remove and select Remove.

Do not remove the root user for any reason.

Removing or Modifying vCenter Server Users

When you remove users from vCenter Server, you also remove permissions granted to those users. Modifying a user or group name causes the original name to become invalid.

To remove users from vCenter Server, you must remove them from the domain or Active Directory users list.

If you remove users from the vCenter Server domain, they lose permissions to all objects in the vSphere environment and cannot log in again.

**Note** Users who are logged in and are removed from the domain keep their vSphere permissions until the next validation period. The default is every 24 hours.

Removing a group does not affect the permissions granted individually to the users in that group or permissions granted as part of inclusion in another group.

If you change a user’s name in the domain, the original user name becomes invalid in the vCenter Server system. If you change the name of a group, the original group becomes invalid after you restart the vCenter Server system.

Sort, Export, and View Users and Groups

You can view, sort, and export lists of a host's local users and groups to a file that is in HTML, XML, Microsoft Excel, or CSV format.

**Procedure**

1 Log in to ESXi using the vSphere Client.
2 Click the Local Users & Groups tab and click Users or Groups.
3 Determine how to sort the table, and hide or show columns according to the information you want to see in the exported file.

- To sort the table by any of the columns, click the column heading.
- To show or hide columns, right-click any of the column headings and select or deselect the name of the column to hide.
- To show or hide columns, right-click any of the column headings and select or deselect the name of the column to hide.
4 Right-click anywhere in the table and click Export List to open the Save As dialog box.
5 Select a path and enter a filename.
6 Select the file type and click OK.
Managing vSphere Groups

A group is a set of users that share a common set of rules and permissions. When you assign permissions to a group, all users in the group inherit them, and you do not have to work with the user profiles individually.

The group lists in vCenter Server and the ESXi host are drawn from the same sources as their respective user lists. The group lists in vCenter Server are drawn from the local users or any trusted domain, and the group lists for the host are drawn from the local user list or from any trusted Windows domain.

As an administrator, decide how to structure groups to achieve your security and usage goals. For example, three part-time sales team members work different days, and you want them to share a single virtual machine but not use the virtual machines belonging to sales managers. In this case, you might create a group called SalesShare that includes the three sales people and give the group permission to interact with only one object, the shared virtual machine. They cannot perform any actions on the sales managers’ virtual machines.

Best Practices for vSphere Groups

Use best practices for managing groups to increase the security and manageability of your vSphere environment.

VMware recommends several best practices for creating groups in your vSphere environment:

- Use a directory service or vCenter Server to centralize access control, rather than defining groups on individual hosts.
- Choose a local Windows user or group to have the Administrator role in vCenter Server.
- Create new groups for vCenter Server users. Avoid using Windows built-in groups or other existing groups.
- If you use Active Directory groups, make sure that they are security groups and not distribution groups. Permissions assigned to distribution groups are not enforced by vCenter Server. For more information about security groups and distribution groups, see the Microsoft Active Directory documentation.

**IMPORTANT** By default, some versions of the Windows operating system include the NT AUTHORITY\INTERACTIVE user in the Administrators group. When the NT AUTHORITY\INTERACTIVE user is in the Administrators group, all users you create on the vCenter Server system have the Administrator privilege. To avoid this, remove the NT AUTHORITY\INTERACTIVE user from the Administrators group on the Windows system where you run vCenter Server.

Add a Group

Adding a group to the groups table updates the internal group list maintained by the host.

Procedure

1. Log in to ESXi using the vSphere Client.
2. Click the Local Users & Groups tab and click Groups.
3. Right-click anywhere in the Groups table and click Add to open the Create New Group dialog box.
4. Enter a group name and numeric group ID (GID).
   
   Specifying the ID is optional. If you do not specify an ID, the vSphere Client assigns the next available group ID.
5 From the User list, select user to add and click Add.

6 Click OK.

**Remove a Group from a Host**

You can remove a group from the host.

Removing a group does not affect the permissions granted individually to the users in that group or permissions granted as part of inclusion in another group.

**Procedure**

1 Log in to ESXi using the vSphere Client.
2 Click the Local Users & Groups tab and click Groups.
3 Right-click the group to remove and select Remove.

**Add or Remove Users from a Group**

You can add or remove a user from a group in the groups table.

**Procedure**

1 Log in to ESXi using the vSphere Client.
2 Click the Local Users & Groups tab and click Groups.
3 Right-click the group to modify and select Properties to open the Edit Group dialog box.
4 To add the user to a group, select the user name from the User drop-down menu and click Add.
5 To remove the user from a group, select the user name from the Users in this Group box and click Remove.
6 Click OK.

**Password Requirements**

By default, ESXi enforces requirements for user passwords.

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.

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.

**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 Passwords**

The following password candidates meet the requirements of ESXi.

- xQaTEhbU: Contains eight characters from two character classes.
Assigning Permissions

For ESXi and vCenter Server, 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.

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

By default, all users who are members of the Windows Administrators group on the vCenter Server system have the same access rights as a user assigned to the Administrator role on all objects. When connecting directly to the host, the root and vpxuser user accounts have the same access rights as any user assigned the Administrator role on all objects.

All other users 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.

Many tasks require permissions on more than one object. 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.

The list of privileges is the same for both ESXi and vCenter Server, and you use the same method to configure permissions.

You can create roles and set permissions through a direct connection to the ESXi host.

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 4-2. vSphere Inventory Hierarchy

Most inventory objects inherit permissions from a single parent object in the hierarchy. For example, a datastore inherits permissions from either its parent datastore folder or parent 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

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

Example 2: Child Permissions Overriding Parent Permissions

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

In this example, permissions are 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 4-4. 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 4-5. Example 3: User Permissions Overriding Group Permissions](image)

**root User Permissions**

Root users can only perform activities on the specific host that they are logged in to.

For security reasons, you might not want to use the root user in the Administrator role. In this case, you can change permissions after installation so that the root user no longer has administrative privileges. Alternatively, you can remove the access permissions for the root user. (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.

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 or user group—you can track the actions of each administrator or administrative group.

After you create an alternative Administrator user, you can assign a different role to the root user. To manage the host using vCenter Server, the new user you created must have full Administrator privileges on the host.

**NOTE** vicfg commands do not perform an access check. Therefore, even if you limit the root user’s privileges, it does not affect what that user can do using the command-line interface commands.

**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 must not be modified or used by interactive users.

**CAUTION** Do not change the dcui user in any way and do not change its permissions. If you do so, you might experience problems in working with the host through the local user interface.

---

**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.

**Assign Permissions**

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.

**Prerequisites**

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

**Procedure**

1. Select an object and click the **Permissions** tab.
2. Right-click the **Permissions** tab and select **Add Permission**.
3. 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.
4. (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.
5. Click **Add** to open the Select Users or Groups dialog box.
6 Identify the user or group to assign to this role.
   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 Name list.
   c Click Add.
      The name is added to either the Users or Groups list.
   d Repeat Step 6a through Step 6c to add additional users or groups.
   e Click OK when finished.

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

8 Click OK to finish.
   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.

Adjust the Search List in Large Domains
If you have domains with thousands of users or groups, or if searches take a long time to complete, adjust
the search settings in the Select Users or Groups dialog box.

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

**Prerequisites**
To configure Active Directory settings, the vSphere Client must be connected to the vCenter Server system.

**Procedure**
1 From the vSphere Client connected to a vCenter Server system, select Administration > vCenter Server
   Settings.
2 In the navigation pane, select Active Directory.
3 Change the values as needed.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Active Directory Timeout</strong></td>
<td>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.</td>
</tr>
<tr>
<td><strong>Enable Query Limit</strong></td>
<td>Select the check box to limit the number of users and groups that vCenter Server displays in the Add Permissions dialog box for the selected domain.</td>
</tr>
<tr>
<td><strong>Users &amp; Groups value</strong></td>
<td>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.</td>
</tr>
</tbody>
</table>

4 Click OK.
Change Permission Validation Settings

vCenter Server periodically validates its user and group lists against the users and groups in the Windows Active Directory domain. It then removes users or groups that no longer exist in the domain. You can change the interval between validations.

Procedure

1. From the vSphere Client connected to a vCenter Server system, select Administration > vCenter Server Settings.
2. In the navigation pane, select Active Directory.
3. (Optional) Deselect the Enable 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.
4. If validation is enabled, enter a value in the Validation Period text box to specify a time, in minutes, between validations.

Change Permissions

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

Procedure

1. From the vSphere Client, select an object in the inventory.
2. Click the Permissions tab.
3. Click the line item to select the user or group and role pair.
4. Select Inventory > Permissions > Properties.
5. Select a role for the user or group from the 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

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. From the vSphere Client, click the Inventory button.
2. Expand the inventory as needed and click the appropriate object.
3. Click the Permissions tab.
4. Click the appropriate line item to select the user or group and role pair.
5. Select Inventory > Permissions > Delete.

vCenter Server removes the permission setting.
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 into the inventory hierarchy, they inherit permissions and are accessible to users.
- Use the No Access role to mask 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>
<thead>
<tr>
<th>Task</th>
<th>Required Privileges</th>
<th>Applicable Role</th>
</tr>
</thead>
</table>
| Create a virtual machine | On the destination folder or datacenter:  
  - Virtual Machine.Inventory.Raw Create  
  - 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 a RDM or SCSI pass-through device)  
  - Virtual Machine.Inventory.Raw Create | Virtual Machine Administrator |
<p>| On the destination datastore or folder containing a datastore: | | |
| Datastore.Allocate Space | | Datastore Consumer or Virtual Machine Administrator |</p>
<table>
<thead>
<tr>
<th>Task</th>
<th>Required Privileges</th>
<th>Applicable Role</th>
</tr>
</thead>
</table>
| Deploy a virtual machine from a template | On the destination folder or datacenter:  
- Virtual Machine.Inventory.Raw Create  
| | On a template or folder of templates:  
Virtual Machine.Provisioning.Deploy Template | Virtual Machine Administrator |
| | On the destination host, cluster or resource pool:  
| | On the destination datastore or folder of datastores:  
Datastore.Allocate Space | Datastore Consumer or Virtual Machine Administrator |
| | On the network that the virtual machine will be assigned to:  
Network.Assign Network | Network Consumer or Virtual Machine Administrator |
| Take a virtual machine snapshot | On the virtual machine or a folder of virtual machines:  
Virtual Machine.State.Create Snapshots | Virtual Machine Power User or Virtual Machine Administrator |
| | On the destination datastore or folder of datastores:  
Datastore.Allocate Space | Datastore Consumer or Virtual Machine Administrator |
| Move a virtual machine into a resource pool | On the virtual machine or folder of virtual machines:  
- Virtual Machine.Inventory.Move | Virtual Machine Administrator |
| | On the destination resource pool:  
| 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 Offs  
- 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)  
| | On a datastore containing the installation media ISO image:  
Datastore.Browse Datastore (if installing from an ISO image on a datastore) | Virtual Machine Power User or Virtual Machine Administrator |
| Migrate a virtual machine with vMotion | On the virtual machine or folder of virtual machines:  
- Resource.Migrate  
- Resource.Assign Virtual Machine to Resource Pool (if destination is a different resource pool from the source) | Datacenter Administrator or Resource Pool Administrator or Virtual Machine Administrator |
### Table 4-1. Required Privileges for Common Tasks (Continued)

<table>
<thead>
<tr>
<th>Task</th>
<th>Required Privileges</th>
<th>Applicable Role</th>
</tr>
</thead>
<tbody>
<tr>
<td>On the destination host, cluster, or resource pool (if different from the source):</td>
<td><strong>Resource.Assign Virtual Machine to Resource Pool</strong></td>
<td>Datacenter Administrator or Resource Pool Administrator or Virtual Machine Administrator</td>
</tr>
<tr>
<td>Cold migrate (relocate) a virtual machine</td>
<td>On the virtual machine or folder of virtual machines:</td>
<td>Datacenter Administrator or Resource Pool Administrator or Virtual Machine Administrator</td>
</tr>
<tr>
<td>■ <strong>Resource.Relocate</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>■ <strong>Resource.Assign Virtual Machine to Resource Pool</strong></td>
<td>(if destination is a different resource pool from the source)</td>
<td></td>
</tr>
<tr>
<td>On the destination host, cluster, or resource pool (if different from the source):</td>
<td><strong>Resource.Assign Virtual Machine to Resource Pool</strong></td>
<td>Datacenter Administrator or Resource Pool Administrator or Virtual Machine Administrator</td>
</tr>
<tr>
<td>On the destination datastore (if different from the source):</td>
<td><strong>Datastore.Allocate Space</strong></td>
<td>Datastore Consumer or Virtual Machine Administrator</td>
</tr>
<tr>
<td>Migrate a Virtual Machine with Storage vMotion</td>
<td>On the virtual machine or folder of virtual machines:</td>
<td>Datacenter Administrator or Resource Pool Administrator or Virtual Machine Administrator</td>
</tr>
<tr>
<td>■ <strong>Resource.Migrate</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>On the destination datastore:</td>
<td><strong>Datastore.Allocate Space</strong></td>
<td>Datastore Consumer or Virtual Machine Administrator</td>
</tr>
<tr>
<td>Move a host into a cluster</td>
<td>On the host:</td>
<td>Datacenter Administrator or Virtual Machine Administrator</td>
</tr>
<tr>
<td>■ <strong>Host.Inventory.Add Host to Cluster</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>On the destination cluster:</td>
<td><strong>Host.Inventory.Add Host to Cluster</strong></td>
<td>Datacenter Administrator or Virtual Machine Administrator</td>
</tr>
</tbody>
</table>

### Assigning Roles

vCenter Server and ESXi grant access to objects only to users who are assigned permissions for the object. When you assign a user or group permissions for the object, you do so by pairing the user or group with a role. A role is a predefined set of privileges.

ESXi hosts provide three default roles, and you cannot change the privileges associated with these roles. Each subsequent default role includes the privileges of the previous role. For example, the Administrator role inherits the privileges of the Read Only role. Roles you create yourself do not inherit privileges from any of the default roles.

You can create custom roles by using the role-editing facilities in the vSphere Client to create privilege sets that match your user needs. If you use the vSphere Client connected to vCenter Server to manage ESXi hosts, you have additional roles to choose from in vCenter Server. Also, the roles you create directly on a host are not accessible within vCenter Server. You can work with these roles only if you log in to the host directly from the vSphere Client.

**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.
If you manage ESXi hosts through vCenter Server, maintaining custom roles in the host and vCenter Server can result in confusion and misuse. In this type of configuration, maintain custom roles only in vCenter Server.

You can create roles and set permissions through a direct connection to the ESXi host.

### 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 a user or group permissions, 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 would allow that user to turn on virtual machines in Pool A, but not those in Pool B. The user would still be able to view the status of the 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 created through vCenter Server are available. If you connect directly to the host using the vSphere Client, the roles created directly on the host are available.

vCenter Server and ESXi hosts provide default 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.

You can also create 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.

### Default Roles for ESXi and vCenter Server

vCenter Server and ESXi provide default roles. These roles group privileges for common areas of responsibility in a vSphere environment.

You can use the default roles to assign permissions in your environment, or use them as a model to develop your own roles.

<table>
<thead>
<tr>
<th>Table 4-2. Default Roles</th>
</tr>
</thead>
<tbody>
<tr>
<td>Role</td>
</tr>
<tr>
<td>------</td>
</tr>
<tr>
<td>No Access</td>
</tr>
<tr>
<td>Read Only</td>
</tr>
<tr>
<td>Role</td>
</tr>
<tr>
<td>----------------------</td>
</tr>
<tr>
<td>Administrator</td>
</tr>
</tbody>
</table>
| Virtual Machine Power User | sample | A set of privileges to allow the user to interact with and make hardware changes to virtual machines, as well as perform snapshot operations. Privileges granted include:  
- All privileges for the scheduled task privileges group.  
- Selected privileges for global items, datastore, and virtual machine privileges groups.  
- No privileges for folder, datacenter, network, host, resource, alarms, sessions, performance, and permissions privileges groups. Usually granted on a folder that contains virtual machines or on individual virtual machines. Available on vCenter Server. |
| Virtual Machine User  | sample    | A set of privileges to allow the user to interact with a virtual machine’s console, insert media, and perform power operations. Does not grant privileges to make virtual hardware changes to the virtual machine. Privileges granted include:  
- All privileges for the scheduled tasks privileges group.  
- Selected privileges for the global items and virtual machine privileges groups.  
- No privileges for the folder, datacenter, datastore, network, host, resource, alarms, sessions, performance, and permissions privileges groups. Usually granted on a folder that contains virtual machines or on individual virtual machines. Available on vCenter Server. |
| Resource Pool Administrator | sample | A set of privileges to allow the user to create child resource pools and modify the configuration of the children, but not to modify the resource configuration of the pool or cluster on which the role was granted. Also allows the user to grant permissions to child resource pools, and assign virtual machines to the parent or child resource pools. Privileges granted include:  
- All privileges for folder, virtual machine, alarms, and scheduled task privileges groups.  
- Selected privileges for resource and permissions privileges groups.  
- No privileges for datacenter, network, host, sessions, or performance privileges groups. Additional privileges must be granted on virtual machines and datastores to allow provisioning of new virtual machines. Usually granted on a cluster or resource pool. Available on vCenter Server. |
### Table 4-2. Default Roles (Continued)

<table>
<thead>
<tr>
<th>Role</th>
<th>Role Type</th>
<th>Description of User Capabilities</th>
</tr>
</thead>
<tbody>
<tr>
<td>Datastore Consumer</td>
<td>sample</td>
<td>A set of privileges to allow the user to consume space on the datastores on which this role is granted. To perform a space-consuming operation, such as creating a virtual disk or taking a snapshot, the user must also have the appropriate virtual machine privileges granted for these operations. Usually granted on a datastore or a folder of datastores. This role is available on vCenter Server.</td>
</tr>
<tr>
<td>Network Consumer</td>
<td>sample</td>
<td>A set of privileges to allow the user to assign virtual machines or hosts to networks, if the appropriate permissions for the assignment are also granted on the virtual machines or hosts. Usually granted on a network or folder of networks. Available on vCenter Server.</td>
</tr>
</tbody>
</table>

### Create a Role

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 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. On the vSphere Client Home page, click Roles.
2. Right-click the Roles tab information panel and click Add.
3. Type a name for the new role.
4. Select privileges for the role and click OK.

### Clone a Role

You can make a copy of an existing role, rename it, and later 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 modify 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. On the vSphere Client Home page, click Roles.
2. To select the role to duplicate, click the object in the list of Roles.
3. To clone the selected role, select Administration > Role > Clone.

A duplicate of the role is added to the list of roles. The name is Copy of rolename.
Edit a Role

When you edit a role, you can change the privileges selected for that role. When completed, these privileges are applied to any user or group 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. However, 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. On the vSphere Client Home page, click Roles.
2. Right-click the role to edit and select Edit Role.
3. Select privileges for the role and click OK.

Remove a Role

When you remove a role that is not assigned to any users or groups, the definition is removed from the list of roles. When you remove a role that is assigned to a user or group, you can remove assignments or replace them with an assignment to another role.

CAUTION You must understand how users will be affected before removing all assignments or replacing them. Users who have no permissions granted to them cannot log in to vCenter Server.

Prerequisites

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

If you remove a role from a vCenter Server system that is part of a connected group in Linked Mode, check the use of that role on the other vCenter Server systems in the group. Removing a role from one vCenter Server system removes the role from all other vCenter Server systems in the group, even if you reassign permissions to another role on the current vCenter Server system.

Procedure

1. On the vSphere Client Home page, click Roles.
2. Click the object you want to remove in the list of roles.
3. Select Administration > Role > Remove.
4. Click OK.

The role is removed from the list.

If the role is assigned to a user or group, a warning message appears.

5. Select a reassignment option and click OK.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Remove Role Assignments</td>
<td>Removes configured user or group and role pairings on the server. If a user or group does not have other permissions assigned, they lose all privileges.</td>
</tr>
<tr>
<td>Reassign affected users to</td>
<td>Reassigns any configured user or group and role pairings to the selected new role.</td>
</tr>
</tbody>
</table>
Rename a Role

When you rename a role, no changes occur to that role’s assignments.

If you create or modify a role on a vCenter Server system that is part of a connected group in Linked Mode, the changes you make are propagated to 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. On the vSphere Client Home page, click Roles.
2. Click the object in the list of roles that you want to rename.
3. Select Administration > Role > Rename.
4. Type the new name.

Direct Console User Interface Access

Only users that are assigned the Administrator role can log in to the Direct Console User Interface (DCUI). To allow access to the direct console, add the user to the local administrators group.

Procedure

1. Log in to ESXi using the vSphere Client.
2. Click the Local Users & Groups tab and click Users.
3. Right-click the user and click Edit to open the Edit User dialog box.
4. From the Group drop-down menu, select localadmin and click Add.
5. Click OK.

Using Active Directory to Manage Users and Groups

You can configure ESXi to use a directory service such as Active Directory to manage users and groups.

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

You can configure the ESXi host to use a directory service such as Active Directory to manage users and groups.

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.
   
   ESXi supports synchronizing time with an external NTPv3 or NTPv4 server that is compliant with RFC 5905 and RFC 1305. The Microsoft Windows W32Time service does not meet these requirements when running with default settings. See 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.
   
   - In the vSphere Client, select the host in the inventory.
   - Click the **Configuration** tab and click **DNS and Routing**.
   - Click the **Properties** link at the top right of the panel.
   - In the DNS and Routing Configuration dialog box, verify that the host name and DNS server information for the host are correct.

**What to do next**

Use the vSphere Client to join a directory service domain.

**Add a Host to a Directory Service Domain**

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 (CAM service), see “Use vSphere Authentication Proxy to Add a Host to a Domain,” on page 71.

**Prerequisites**

Verify that the vSphere Client is connected to a vCenter Server system or to the host.

**Procedure**

1. Select a host in the vSphere Client inventory, and click the **Configuration** tab.

2. Click **Properties**.

3. In the Directory Services Configuration dialog box, select the directory service from the drop-down menu.

4. Enter a domain.
   
   Use the form **name.tld** or **name.tld/container/path**.

5. Click **Join Domain**.

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

You can view the type of directory server, if any, the host uses to authenticate users and the directory server settings.

Procedure

1. Select a host in the vSphere Client inventory, and click the Configuration tab.

The Authentication Services Settings page displays the directory service and domain settings.

Using vSphere Authentication Proxy

When you use the vSphere Authentication Proxy, you do not need to transmit Active Directory credentials to the host. Users supply the domain name of the Active Directory server and the IP address of the authentication proxy server when they add a host to a domain.

Install the vSphere Authentication Proxy Service

To use the vSphere Authentication Proxy service (CAM 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 67.
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.

<table>
<thead>
<tr>
<th>Option</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>For IIS 6</td>
<td>a Browse to Computer Account Management Web Site.</td>
</tr>
<tr>
<td></td>
<td>b Right-click the virtual directory CAM ISAPI.</td>
</tr>
<tr>
<td></td>
<td>c Select Properties &gt; Directory Security &gt; Edit IP Address and Domain Name Restrictions &gt; Add Group of Computers.</td>
</tr>
<tr>
<td>For IIS 7</td>
<td>a Browse to Computer Account Management Web Site.</td>
</tr>
<tr>
<td></td>
<td>b Click the CAM ISAPI virtual directory in the left pane and open IPv4 Address and Domain Restrictions.</td>
</tr>
<tr>
<td></td>
<td>c Select Add Allow Entry &gt; IPv4 Address Range.</td>
</tr>
</tbody>
</table>

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).

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Self-signed certificate</td>
<td>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.</td>
</tr>
<tr>
<td>CA-signed certificate</td>
<td>Add the CA-signed certificate (Windows format only) to the local trust certificate store on the system where the authentication proxy service is installed and restart the vSphere Authentication Proxy Adapter service.</td>
</tr>
<tr>
<td></td>
<td>- For Windows 2003, copy the certificate file to C:\Documents and Settings\All Users\Application Data\VMware\vSphere Authentication Proxy\trust.</td>
</tr>
<tr>
<td></td>
<td>- For Windows 2008, copy the certificate file to C:\Program Data\VMware\vSphere Authentication Proxy\trust.</td>
</tr>
</tbody>
</table>

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.ActiveDirectoryVerifyCAMCertificate attribute to 0.

Export vSphere Authentication Proxy Certificate

To authenticate the vSphere Authentication Proxy to ESXi, you must provide ESXi with the proxy server certificate.

**Prerequisites**

Install the vSphere Authentication Proxy service (CAM service) on a host as described in “Install the vSphere Authentication Proxy Service,” on page 67.
Procedure

1. On the authentication proxy server system, use the IIS Manager to export the certificate.

<table>
<thead>
<tr>
<th>Option</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>For IIS 6</td>
<td>a. Right-click Computer Account Management Web Site.</td>
</tr>
<tr>
<td>For IIS 7</td>
<td>a. Click Computer Account Management Web Site in the left pane.</td>
</tr>
<tr>
<td></td>
<td>b. Select Bindings to open the Site Bindings dialog box.</td>
</tr>
<tr>
<td></td>
<td>c. Select https binding.</td>
</tr>
<tr>
<td></td>
<td>d. Select Edit &gt; View SSL Certificate.</td>
</tr>
</tbody>
</table>

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 vSphere Authentication Proxy Server Certificate to ESXi

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

You use the vSphere Client user interface to upload the vSphere Authentication Proxy server certificate to ESXi.

Prerequisites

Install the vSphere Authentication Proxy service (CAM service) on a host as described in “Install the vSphere Authentication Proxy Service,” on page 67.

Export the vSphere Authentication Proxy server certificate as described in “Export vSphere Authentication Proxy Certificate,” on page 69.

Procedure

1. Select a host in the vSphere Client inventory and click the Summary tab.
2. Upload the certificate for the authentication proxy server to a temporary location on ESXi.
   a. Under Resources, right-click a datastore and select Browse Datastore.
   b. Select a location for the certificate and select the Upload File button.
   c. Browse to the certificate and select Open.
3. Select the Configuration tab and click Authentication Services.
4. Click Import Certificate.
5. 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.
6. 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

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**

- Verify that the vSphere Client is connected to a vCenter Server system or to the host.
- If ESXi is configured with a DHCP address, set up the DHCP range as described in “Configure a Host to Use the vSphere Authentication Proxy for Authentication,” on page 68.
- 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 68.
- Authenticate the vSphere Authentication Proxy server to the host as described in “Authenticating vSphere Authentication Proxy to ESXi,” on page 69.

**Procedure**

1. In the vSphere Client inventory, select the host.
2. Select the **Configuration** tab and click **Authentication Services**.
3. Click **Properties**.
4. In the Directory Services Configuration dialog box, select the directory server from the drop-down menu.
5. Enter a domain.
   - Use the form **name.tld** or **name.tld/container/path**.
6. Select the **Use vSphere Authentication Proxy** check box.
7. Enter the IP address of the authentication proxy server.
8. Click **Join Domain**.
9. Click **OK**.

**View vSphere Authentication Proxy Settings**

You can verify the IP address and the port where the proxy server listens.

After you set up a vSphere Authentication Proxy service on a host machine, you can view the host machine address and port information in the vSphere Client.
Procedure

* In the vSphere Client, select **Inventory > Administration > vSphere Authentication Proxy**.

  The VMware vSphere Authentication Proxy page is displayed.
ESXi and vCenter Server support standard X.509 version 3 (X.509v3) certificates to encrypt session information sent over Secure Socket Layer (SSL) protocol connections between components. If SSL is enabled, data is private, protected, and cannot be modified in transit without detection.

All network traffic is encrypted as long as the following conditions are true:

- You did not change the Web proxy service to allow unencrypted traffic for the port.
- Your firewall is configured for medium or high security.

Certificate checking is enabled by default and SSL certificates are used to encrypt network traffic. However, ESXi and vCenter Server use automatically generated certificates that are created as part of the installation process and stored on the server system. These certificates are unique and make it possible to begin using the server, but they are not verifiable and are not signed by a trusted-well-known certificate authority (CA). These default certificates are vulnerable to possible man-in-the-middle attacks.

To receive the full benefit of certificate checking, particularly if you intend to use encrypted remote connections externally, install new certificates that are signed by a valid internal certificate authority or purchase a certificate from a trusted security authority. Replacing vCenter Server certificates is described in the vSphere Examples and Scenarios documentation.

**NOTE** If the self-signed certificate is used, clients receive a warning about the certificate. To address this issue, install a certificate that is signed by a recognized certificate authority. If CA-signed certificates are not installed, all communication between vCenter Server and vSphere Clients is encrypted using a self-signed certificate. These certificates do not provide the authentication security you might need in a production environment.

The certificate consists of two files: the certificate itself (rui.crt) and the private-key file (rui.key).

**Table 5-1. Default Location of ESXi and vCenter Server Certificate Files**

<table>
<thead>
<tr>
<th>Server</th>
<th>Location</th>
</tr>
</thead>
<tbody>
<tr>
<td>ESXi 5.0</td>
<td>/etc/vmware/ssl/</td>
</tr>
<tr>
<td>vCenter Server (Windows 2008)</td>
<td>C:\Program Data\VMware\VMware VirtualCenter\SSL</td>
</tr>
<tr>
<td>vCenter Server (Windows 2003)</td>
<td>C:\Documents and Settings\All Users\Application Data\VMware\VMware VirtualCenter\SSL</td>
</tr>
</tbody>
</table>

This chapter includes the following topics:

- “Enable Certificate Checking and Verify Host Thumbprints,” on page 74
- “Generate New Certificates for ESXi,” on page 74
- “Replace a Default Host Certificate with a CA-Signed Certificate,” on page 75
Enable Certificate Checking and Verify Host Thumbprints

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 Client.

NOTE vCenter Server certificates are preserved across upgrades.

Procedure

1. Log in to the vCenter Server system using the vSphere Client.
2. Select Administration > vCenter Server Settings.
3. Click SSL Settings in the left pane and verify that Check host certificates is selected.
4. 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.
5. 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.
6. Click OK.

Generate New Certificates for ESXi

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

Procedure

1. Log in to the ESXi Shell and acquire root 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 after you install the new certificate. 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.

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
```

### Replace a Default Host Certificate with a CA-Signed Certificate

The ESXi host 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, well-known 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. If the new certificate is not verifiable by vCenter Server, you must reconnect the host using the vSphere Client.

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

**Note** For information about replacing default certificates on a vCenter Server system, see the vSphere Examples and Scenarios documentation.

### Prerequisites

All file transfers and other communications occur over a secure HTTPS session. The user used to authenticate the session must have the privilege `Host.Config.AdvancedConfig` on the host. For more information on ESXi privileges, see Chapter 4, “Authentication and User Management,” on page 43.

### Procedure

1 Log in to the ESXi Shell and acquire root 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 new certificate and key 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, and then use the Direct Console User Interface (DCUI) to restart the management agents.
Replace a Default ESXi Certificate with a CA-Signed Certificate Using the vifs Command

The ESXi host 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, well-known 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. If the new certificate is not verifiable by vCenter Server, you must reconnect the host using the vSphere Client.

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

**NOTE** For information about replacing default certificates on a vCenter Server system, see the *vSphere Examples and Scenarios* documentation.

**Prerequisites**

All file transfers and other communications occur over a secure HTTPS session. The user used to authenticate the session must have the privilege `Host.Config.AdvancedConfig` on the host. For more information on ESXi privileges, see Chapter 4, “Authentication and User Management,” on page 43.

**Procedure**

1. Back up the existing certificates.
2. 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 /host/ssl_cert`
   - `vifs --server hostname --username username --put rui.key /host/ssl_key`
3. 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.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Certificates</td>
<td><a href="https://hostname/host/ssl_cert">https://hostname/host/ssl_cert</a></td>
</tr>
<tr>
<td>Keys</td>
<td><a href="https://hostname/host/ssl_key">https://hostname/host/ssl_key</a></td>
</tr>
</tbody>
</table>

   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.

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.

**NOTE**  Lockdown mode does not apply to root users who log in using authorized keys. When you use an authorized key file for root user authentication, root users are not prevented from accessing a host with SSH when the host is in lockdown mode.

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.

<table>
<thead>
<tr>
<th>Type of key</th>
<th>Location</th>
</tr>
</thead>
<tbody>
<tr>
<td>Authorized key files for the root user</td>
<td><code>https://hostname or IP address/host/ssh_root_authorized_keys</code></td>
</tr>
<tr>
<td></td>
<td>You must have root user privileges to upload this file.</td>
</tr>
<tr>
<td>DSA keys</td>
<td><code>https://hostname or IP address/host/ssh_host_dsa_key</code></td>
</tr>
<tr>
<td>DSA public keys</td>
<td><code>https://hostname or IP address/host/ssh_host_dsa_key_pub</code></td>
</tr>
<tr>
<td>RSA keys</td>
<td><code>https://hostname or ip/host/ssh_host_rsa_key</code></td>
</tr>
<tr>
<td>RSA public keys</td>
<td><code>https://hostname or ip/host/ssh_host_rsa_key_pub</code></td>
</tr>
</tbody>
</table>

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.

**NOTE**  Lockdown mode does not apply to root users who log in using authorized keys. When you use an authorized key file for root user authentication, root users are not prevented from accessing a host with SSH when the host is in lockdown mode.

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`

<table>
<thead>
<tr>
<th>Type of key</th>
<th>Location</th>
</tr>
</thead>
<tbody>
<tr>
<td>Authorized key files for the root user</td>
<td>/host/ssh_root_authorized_keys You must have root user privileges to upload this file.</td>
</tr>
<tr>
<td>DSA keys</td>
<td>/host/ssh_host_dsa_key</td>
</tr>
<tr>
<td>DSA public keys</td>
<td>/host/ssh_host_dsa_key_pub</td>
</tr>
<tr>
<td>RSA keys</td>
<td>/host/ssh_host_rsa_key</td>
</tr>
<tr>
<td>RSA public keys</td>
<td>/host/ssh_host_rsa_key_pub</td>
</tr>
</tbody>
</table>

**Configure SSL Timeouts**

You can configure SSL timeouts for ESXi.

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 and acquire root privileges.
2. Change to the directory `/etc/vmware/hostd/`.
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, enter the following command.
   
   `<readTimeoutMs>20000</readTimeoutMs>`
5. Enter the `<handshakeTimeoutMs>` value in milliseconds.
   
   For example, to set the Handshake Timeout to 20 seconds, enter the following command.
   
   `<handshakeTimeoutMs>20000</handshakeTimeoutMs>`
6  Save your changes and close the file.
7  Restart the hostd process:

    /etc/init.d/hostd restart

Example: Configuration File

The following section from the file /etc/vmware/hostd/config.xml shows where to enter the SSL timeout settings.

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

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 pass phrases. ESXi does not support pass phrases, also known as encrypted keys. If you set up a 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 and acquire root privileges.
2. Change to the `/etc/vmware/hostd/` directory.
3. Use a text editor to open the `config.xml` file and find the following XML segment.
   ```xml
   <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 host process:
   ```
   /etc/init.d/hostd 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.

**Procedure**

1. Log in to the ESXi Shell and acquire root privileges.
2. Change to the `/etc/vmware/hostd/` directory.
3. Use a text editor to open the `proxy.xml` file.

   The contents of the file typically appears as follows.
   ```xml
   <ConfigRoot>
   <EndpointList>
   <_length>10</_length>
   <_type>vim.ProxyService.EndpointSpec[]</_type>
   ```
Chapter 5 Encryption and Security Certificates for ESXi and vCenter Server

<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>8089</port>
  <serverNamespace>/vpxa</serverNamespace>
</e>
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.

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

5 Save your changes and close the file.

6 Restart the hostd process:

/etc/init.d/hostd restart
Lockdown Mode

To increase the security of your ESXi hosts, you can put them in lockdown mode.

When you enable lockdown mode, no users other than vpxuser have authentication permissions, nor can they perform operations against the host directly. Lockdown mode forces all operations to be performed through vCenter Server.

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** The root user is still authorized to log in to the direct console user interface when lockdown mode is enabled.

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 Client to manage a host, or using the direct console user interface.

**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 Client connected to vCenter Server.

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

This chapter includes the following topics:

- “Lockdown Mode Behavior,” on page 84
- “Lockdown Mode Configurations,” on page 84
- “Enable Lockdown Mode Using the vSphere Client,” on page 85
- “Enable Lockdown Mode from the Direct Console User Interface,” on page 85
- “Using the ESXi Shell,” on page 85
**Lockdown Mode Behavior**

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

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.

Users with administrator privileges on the vCenter Server system can use the vSphere Client to disable lockdown mode for hosts that are managed by the vCenter Server system. Root users and users with the Administrator role on the host can always log directly in to the host using the Direct Console User Interface (DCUI) to disable lockdown mode. If the host is not managed by vCenter Server or if the host is unreachable, you must reinstall ESXi.

**Note** Lockdown mode does not apply to root users who log in using authorized keys. When you use an authorized key file for root user authentication, root users are not prevented from accessing a host with SSH when the host is in lockdown mode.

Different services are available to different types of users when the host is running in lockdown mode, compared to when the host is running in normal mode. Non-root users cannot run system commands in the ESXi Shell.

**Table 6-1. Lockdown Mode Behavior**

<table>
<thead>
<tr>
<th>Service</th>
<th>Normal Mode</th>
<th>Lockdown Mode</th>
</tr>
</thead>
<tbody>
<tr>
<td>vSphere WebServices API</td>
<td>All users, based on ESXi permissions</td>
<td>vCenter only (vpuser)</td>
</tr>
<tr>
<td>CIM Providers</td>
<td>Root users and users with Admin role on the host</td>
<td>vCenter only (ticket)</td>
</tr>
<tr>
<td>Direct Console UI (DCUI)</td>
<td>Root users and users with Admin role on the host</td>
<td>Root users</td>
</tr>
<tr>
<td>ESXi Shell</td>
<td>Root users and users with Admin role on the host</td>
<td>No users</td>
</tr>
<tr>
<td>SSH</td>
<td>Root users and users with Admin role on the host</td>
<td>No users</td>
</tr>
</tbody>
</table>

**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 6-2. Lockdown Mode Configurations**

<table>
<thead>
<tr>
<th>Service</th>
<th>Default Configuration</th>
<th>Recommended Configuration</th>
<th>Total Lockdown Configuration</th>
</tr>
</thead>
<tbody>
<tr>
<td>Lockdown</td>
<td>Off</td>
<td>On</td>
<td>On</td>
</tr>
<tr>
<td>ESXi Shell</td>
<td>Off</td>
<td>Off</td>
<td>Off</td>
</tr>
<tr>
<td>SSH</td>
<td>Off</td>
<td>Off</td>
<td>Off</td>
</tr>
<tr>
<td>Direct Console UI (DCUI)</td>
<td>On</td>
<td>On</td>
<td>Off</td>
</tr>
</tbody>
</table>
Enable Lockdown Mode Using the vSphere 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. Log in to a vCenter Server system using the vSphere Client.
2. Select the host in the inventory panel.
3. Click the Configuration tab and click Security Profile.
4. Click the Edit link next to lockdown mode.
   The Lockdown Mode dialog box appears.
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 and groups on the host are discarded. To preserve these permissions, you must enable and disable lockdown mode using the vSphere 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.

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.
Log in to the ESXi Shell for Troubleshooting

You should perform ESXi configuration tasks through the vSphere Client or using the vSphere CLI. 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+F2 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.

Use the vSphere Client to Enable Access to the ESXi Shell

Use the vSphere Client to enable local and remote access to the ESXi Shell.

Procedure
1. Log in to a vCenter Server system using the vSphere Client.
2. Select the host in the inventory panel.
3. Click the Configuration tab and click Security Profile.
4. In the Services section, click Properties.
5. Select a service from the list.
   - ESXi Shell
   - SSH
   - Direct Console UI
6. Click Options and select 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.
9. (Optional) Set the timeout for the ESXi Shell.
   By default, the timeout for the ESXi Shell is 0 (disabled).
   The timeout setting is the number of minutes that can elapse before you must log in after the ESXi Shell is enabled. After the timeout period, if you have not logged in, the shell is disabled.

Note: If you are logged in when the timeout period elapses, your session will persist. However, the ESXi Shell will be disabled, preventing other users from logging in.

a. Select the host in the inventory and click the Configuration tab.
c. In the left panel, select UserVars.
d. In the UserVars.ESXiShellTimeOut field, enter the timeout setting.
e. Click OK.
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. 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 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. (Optional) Set the timeout for the ESXi Shell.
   - By default, the timeout for the ESXi Shell is 0 (disabled).
   - The timeout setting is the number of minutes that can elapse before you must log in after the ESXi Shell is enabled. After the timeout period, if you have not logged in, the shell is disabled.

   **NOTE** If you are logged in when the timeout period elapses, your session will persist. However, the ESXi Shell will be disabled, preventing other users from logging in.

   a. From the Troubleshooting Mode Options menu, select **Modify ESXi Shell timeout** and press Enter.
   b. Enter the timeout in minutes.
   c. Press Enter.
6. Press Esc until you return to the main menu of the Direct Console User Interface.
Best Practices for Virtual Machine and Host Security

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

This chapter includes the following topics:
- “Virtual Machine Recommendations,” on page 89
- “Auto Deploy Security Considerations,” on page 94
- “Host Password Strength and Complexity,” on page 94

Virtual Machine Recommendations

There are several safety precautions to consider when evaluating virtual machine security and administering virtual machines.

Installing Antivirus Software

Because each virtual machine hosts a standard operating system, consider protecting 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 will degrade 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.

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.
Enable Copy and Paste Operations Between the Guest Operating System and Remote Console

To copy and paste between the guest operating system and remote console, you must enable copy and paste operations using the vSphere Client.

Procedure

1. Log into a vCenter Server system using the vSphere Client and select the virtual machine.
2. On the Summary tab, click Edit Settings.
3. Select Options > Advanced > General and click Configuration Parameters.
4. Click Add Row and type the following values in the Name and Value columns:

<table>
<thead>
<tr>
<th>Name</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>isolation.tools.copy.disable</td>
<td>false</td>
</tr>
<tr>
<td>isolation.tools.paste.disable</td>
<td>false</td>
</tr>
</tbody>
</table>

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.
6. Restart the virtual machine.

Removing Unnecessary Hardware Devices

Users and processes without privileges on a virtual machine can connect or disconnect hardware devices, such as network adapters and CD-ROM drives. Therefore, removing unnecessary hardware devices can help prevent attacks.

Attackers can use this capability to breach virtual machine security in several ways. For example, 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.

As a general security precaution, use commands on the vSphere Client Configuration tab to remove any unneeded or unused hardware devices. Although this measure tightens virtual machine security, it is not a good solution in situations where you might bring an unused device back into service at a later time.

Prevent a Virtual Machine User or Process from Disconnecting 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.

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 > General Options and make a record of the path displayed in the Virtual Machine Configuration File text box.
5. Log in to the ESXi Shell and acquire root privileges.
6 Change directories to access the virtual machine configuration file whose path you recorded in Step 4. 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, if the virtual machine configuration file you obtained from the Virtual Machine Properties dialog box is [vol1]vm-finance/vm-finance.vmx, you would change to the following directory.

/vmfs/volumes/vol1/vm-finance/

7 Use a text editor to add the following line to the .vmx file, where device_name is the name of the device you want to protect (for example, ethernet1).

device_name.allowGuestConnectionControl = "false"

**NOTE** By default, Ethernet 0 is configured to disallow device disconnection. The only reason you might change this is if a prior administrator set device_name.allowGuestConnectionControl to true.

8 Save your changes and close the file.

9 In the vSphere Client, right-click the virtual machine and select **Power Off**.

10 Right-click the virtual machine and select **Power On**.

### 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

You can increase the guest operating system variable memory limit if large amounts of custom information are being stored in the configuration file.

**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 If the size limit attribute is not present, you must add it.

   a Click **Add Row**.

   b In the Name column, type **tools.setInfo.sizeLimit**.

   c In the Value column, type **Number of Bytes**.

   If the size limit attribute exists, modify it to reflect the appropriate limits.
6 Click OK to close the Configuration Parameters dialog box, and click OK again to close the Virtual Machine Properties dialog box.

**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.

**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.

**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 and Sizes**

To prevent virtual machine users and processes from flooding the log file, which can lead to denial of service, you can limit the number and size of the log files ESXi generates.

**Procedure**

1. Log in to a vCenter Server system using the vSphere Client.
2. On the Summary tab, click Edit Settings.
3. Select Options > General Options and make a record of the path displayed in the Virtual Machine Configuration File text box.
4. Log into the ESXi Shell and acquire root privileges.
5 Change directories to access the virtual machine configuration file whose path you recorded in Step 3. 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, if the virtual machine configuration file you obtained from the Virtual Machine Properties dialog box is `/vmfs/volumes/vol1/vm-finance/vm-finance.vmx`, you would change to the following directory.

```
/vmfs/volumes/vol1/vm-finance/
```

6 To limit the log size, use a text editor to add or edit the following line to the `.vmx` file, where `maximum_size` is the maximum file size in bytes.

```
log.rotateSize=maximum_size
```

For example, to limit the size to around 100KB, enter `100000`.

7 To keep a limited number of log files, use a text editor to add or edit the following line to the `.vmx` file, where `number_of_files_to_keep` is the number of files the server keeps.

```
log.keepOld=number_of_files_to_keep
```

For example, to keep 10 log files and begin deleting the oldest ones as new ones are created, enter `10`.

8 Save your changes and close the file.

**Disable Logging for the Guest Operating System**

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. Log in to a vCenter Server system using the vSphere Client and select the virtual machine in the inventory.
2. On the **Summary** tab, click **Edit Settings**.
3. Click the **Options** tab and in the options list under **Advanced**, select **General**.
4. In Settings, deselect **Enable logging**.
5. Click **OK** to close the Virtual Machine Properties dialog box.

**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.
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.

In most cases, administrators set up Auto Deploy to provision target hosts not only with an image, but also with a host profile. The host profile includes configuration information such as authentication or network settings. Host profiles can be set up to prompt the user for input on first boot. The user input is stored in an answer file. The host profile and answer file (if applicable) are included in the boot image that Auto Deploy downloads to a machine.

- The administrator (root) password and user passwords that are included with the host profile and answer file are MD5-encrypted. Any other passwords associated with host profiles are in the clear.
- Use the vSphere Authentication Service to set up Active Directory to avoid exposing the Active Directory password. If you set up Active Directory using host profiles, the passwords are not protected.
- The files that contain the host profile and answer file information are stored on disk in an obfuscated form. The files can be retrieved only as part of the waiter.tgz file that is generated for each host. The raw files are not accessible through the web server. However, it is possible for malicious code to pretend to be a host and download the host's waiter.tgz file, which contains information that can be used to compromise the host.

To greatly reduce Auto Deploy security risks, completely isolate the network where Auto Deploy is used.

For more information about Auto Deploy, see the Auto Deploy information that is part of the vSphere Installation and Setup documentation. For more information about host profiles and answer files, see the vSphere Host Profiles documentation.

Host Password Strength and Complexity

By default, ESXi uses the pam_passwdqc.so plug-in to set the rules that users must observe when creating passwords and to check password strength.

The pam_passwdqc.so plug-in lets you determine the basic standards that all passwords must meet. By default, ESXi imposes no restrictions on the root password. However, when nonroot users attempt to change their passwords, the passwords they choose must meet the basic standards that pam_passwdqc.so sets.

A valid password should contain a combination of as many character classes as possible. Character classes include lowercase letters, uppercase letters, numbers, and special characters such as an underscore or dash.

**Note** When the number of character classes is counted, the plug-in does not count uppercase letters used as the first character in the password and numbers used as the last character of a password.

To configure password complexity, you can change the default value of the following parameters.

- retry is the number of times a user is prompted for a new password if the password candidate is not sufficiently strong.
- N0 is the number of characters required for a password that uses characters from only one character class. For example, the password contains only lowercase letters.
- N1 is the number of characters required for a password that uses characters from two character classes.
- N2 is used for passphrases. ESXi requires three words for a passphrase. Each word in the passphrase must be 8-40 characters long.
- N3 is the number of characters required for a password that uses characters from three character classes.
- $N4$ is the number of characters required for a password that uses characters from all four character classes.
- *match* is the number of characters allowed in a string that is reused from the old password. If the `pam_passwdqc.so` plug-in finds a reused string of this length or longer, it disqualifies the string from the strength test and uses only the remaining characters.

Setting any of these options to −1 directs the `pam_passwdqc.so` plug-in to ignore the requirement.

Setting any of these options to disabled directs the `pam_passwdqc.so` plug-in to disqualify passwords with the associated characteristic. The values used must be in descending order except for −1 and disabled.

**Note** The `pam_passwdqc.so` plug-in used in Linux provides more parameters than the parameters supported for ESXi.

For more information on the `pam_passwdqc.so` plug-in, see your Linux documentation.

### Change Default Password Complexity for the `pam_passwdqc.so` Plug-In

Configure the `pam_passwdqc.so` plug-in to determine the basic standards all passwords must meet.

**Procedure**

1. Log in to the ESXi Shell and acquire root privileges.
2. Open the `passwd` file with a text editor.
   - For example, `vi /etc/pam.d/passwd`
3. Edit the following line.
   ```
   password requisite /lib/security/$ISA/pam_passwdqc.so retry= N min=N0,N1,N2,N3,N4
   ```
4. Save the file.

**Example: Editing `/etc/pam.d/passwd**

password requisite /lib/security/$ISA/pam_passwdqc.so retry=3 min=12,9,8,7,6

With this setting in effect, the password requirements are:

- **retry=3**: A user is allowed 3 attempts to enter a sufficient password.
- **$N0$=12**: Passwords containing characters from one character class must be at least 12 characters long.
- **$N1$=9**: Passwords containing characters from two character classes must be at least nine characters long.
- **$N2$=8**: Passphrases must contain words that are each at least eight characters long.
- **$N3$=7**: Passwords containing characters from three character classes must be at least seven characters long.
- **$N4$=6**: Passwords containing characters from all four character classes must be at least six characters long.
Index

Numerics
802.1Q and ISL tagging attacks 25
disabling SSL for vSphere SDK 79
generating new 74
key file 73
location 73
SSL 73
uploading 76
vCenter Server 73
changing host proxy services 80
CHAP authentication 33
certificate file 73
checking 74
configuring host searches 80
default 73
double-encapsulated attacks 25
cipher strength, connections 34
client startup options, setting 41
copy and paste
  enabling for guest operating systems 90
guest operating systems 89
virtual machines 89

A
access, permissions 47
Active Directory 65, 66, 68, 71
Active Directory Timeout 56
adding users to groups 49
Administrator role 60
allowed IP addresses, firewall 40
antivirus software, installing 89
attacks
  802.1Q and ISL tagging 25
double-encapsulated 25
MAC flooding 25
multicast brute-force 25
random frame 25
spanning tree 25
authenticating, vSphere Authentication Proxy 69
authentication
groups 48
iSCSI storage 32
users 43, 44
vSphere Client to ESXi 43
authentication daemon 43
authentication proxy 65, 67, 68, 71
authentication proxy server 69, 70
Auto Deploy, security 94

device disconnection, preventing 90
direct access 44
direct console, accessing 65
directory server, viewing 67
directory services 65
disabling
  iSCSI SAN authentication 33
  logging for guest operating systems 92, 93
  SSL for vSphere SDK 79
  variable information size 91
distributed switches, permission 50
DMZ 14
double-encapsulated attacks 25

B
best practices
groups 48
permissions 58
roles 58
security 89
users 44

cryption
certificates 73
for user name, passwords, packets 73
ESXi Shell
  configuring 85
direct connections 86

C
CA-signed certificates 75, 76
CAM server 69–71
CAM service, installing 67
certificates
certificate file 73
checking 74
configuring host searches 80
default 73
VMware, Inc.  97
enabling 85–87
enabling with vSphere Client 86
logging in 86
remote connections 86
setting timeout 86, 87
SSH connections 35
exporting
  host groups 47
  host users 47

F
Fault Tolerance (FT)
  logging 93
  security 93
firewall
  commands 42
  configuration file 38
  configuring 42
host 38
NFS client 40
firewall ports
  automating service behavior 41
  configuring with vCenter Server 18
  configuring without vCenter Server 19
  connecting to vCenter Server 19
  connecting virtual machine console 19
encryption 73
host to host 21
overview 17
SDK and virtual machine console 19
vSphere Client and vCenter Server 18
vSphere Client and virtual machine console 19
vSphere Client direct connection 19
firewall settings 40
firewalls
  access for management agents 39
  access for services 39
forged transmissions 27, 28

G
generating certificates 74
  groups
    adding to hosts 48
    adding users 49
    authentication 48
    best practices 48
    exporting a group list 47
    modifying 47
    modifying on hosts 49
    removing 47
    removing from hosts 49
searching 56
viewing group lists 47
guest operating systems
  copy and paste 89
disabling logging 92, 93
enabling copy and paste 90
limiting variable information size 91
logging levels 92
security recommendations 89

H
hardware devices, removing 90
host certificate searches 80
host name, configuring 65
host-to-host firewall ports 21
hosts
  adding groups 48
  adding users 45
  memory 91
  thumbprints 74
HTTPS PUT, uploading certificates and keys 76, 77

I
Internet Protocol Security (IPsec) 28
IP addresses, adding allowed 40
IPsec, See Internet Protocol Security (IPsec)
iSCSI
  authentication 32
  protecting transmitted data 33
  QLogic iSCSI adapters 32
  securing ports 33
  security 32
iSCSI SAN authentication, disabling 33
isolation
  standard switches 12
  virtual machines 10
  virtual networking layer 12
  VLANs 12

J
join domain 68

K
keys
  authorized 77
  SSH 77
  uploading 76, 77

L
localadmin 65
lockdown mode
  behavior 84
  configurations 84

vSphere Security
98  VMware, Inc.
direct console user interface 85
  enabling 85
  vSphere Client 85
log files
  limiting number 92
  limiting size 92
  logging, disabling for guest operating systems 92, 93
  logging levels, guest operating systems 92
M
  MAC address changes 27
  MAC flooding 25
  managed entities, permissions 50
  management access
    firewalls 39
    TCP and UDP ports 21
  management interface
    securing 37
    securing with VLANs and virtual switches 24
  modifying groups on hosts 49
  multicast brute-force attacks 25
N
  networks, security 22
  NFS Client, firewall rule set 40
  No Access role 60
  NTP 41, 65
P
  pam_passwdqc.so plug-in 94
  passphrase 49
  passwords
    character classes 49
    complexity 94, 95
    criteria 94
    host 94, 95
    length 94
  pam_passwdqc.so plug-in 94
  plug-ins 94
  requirements 49
  restrictions 94
  permissions
    access 47
    administrator 50
    and privileges 50
    assigning 55, 61
    best practices 58
    changing 57
    distributed switches 50
    inheritance 50, 53, 54
    overriding 53, 54
    overview 50
    removing 57
  root user 50
  settings 52
  user 54, 55
  validating 55, 57
  vpxuser 50
  plug-ins, pam_passwdqc.so 94
  policies, security 30
  privileges
    assigning 61
    required for common tasks 58
  privileges and permissions 50
  promiscuous mode 27, 28
  proxy services
    changing 80
    encryption 73
R
  random frame attacks 25
  Read Only role 60
  removing users from groups 49
  replacing, default certificates 75, 76
  required privileges, for common tasks 58
  resource limits and guarantees, security 10
  roles
    Administrator 60
    and permissions 60
    best practices 58
    cloning 63
    copy 63
    creating 63
    default 60, 61
    editing 64
    No Access 60
    Read Only 60
    removing 57, 64
    renaming 65
    security 60
    root login, permissions 50, 54
S
  SDK, firewall ports and virtual machine console 19
  search lists, adjusting for large domains 56
  security
    architecture 9
    best practices 89
    certification 16
    cipher strength 34
    DMZ in single host 13, 14
    features 9
    host 37
    hosts 17
    iSCSI storage 32
    overview 9
PAM authentication 43
permissions 50
recommendations for virtual machines 89
resource guarantees and limits 10
standard switch ports 27
virtual machines 10
virtual machines with VLANs 22
virtual networking layer 12
virtualization layer 10
VLAN hopping 24
VMkernel 10
VMware policy 16
vmware-authd 43
security associations
adding 28
available 30
listing 30
removing 29
security policies
available 32
creating 30
listing 32
removing 31
security recommendations 83
service startup
changing policy 41
setting options 41
service startup options, setting 41
services, automating 41
setinfo 91
spanning tree attacks 25
SSH
ESXi Shell 35
security settings 35
SSL
enabling and disabling 73
encryption and certificates 73
timeouts 78
standard switch ports, security 27
standard switch security 24
standard switches
802.1Q and ISL tagging attacks 25
and iSCSI 33
double-encapsulated attacks 25
forged transmissions 27
MAC address changes 27
MAC flooding 25
multicast brute-force attacks 25
promiscuous mode 27
random frame attacks 25
security 25
spanning tree attacks 25
storage, securing with VLANs and virtual switches 24
T
TCP ports 21
third-party software support policy 16
thumbprints, hosts 74
timeouts, SSL 78
Trusted Platform Module (TPM) 10
U
UDP ports 21
updated information 7
user management 43
user permissions
dcui 55
vpxuser 54
users
adding to groups 49
adding to hosts 45
authentication 44
best practices 44
direct access 44
exporting a user list 47
from Windows domain 44
modifying on hosts 46
removing 55
removing from groups 49
removing from hosts 46
searching 56
security 44
vCenter Server 44
viewing user list 47
V
variable information size for guest operating systems
enabling and disabling 73
encryption and certificates 73
timeouts 78
standard switch ports, security 27
standard switch security 24
standard switches
802.1Q and ISL tagging attacks 25
and iSCSI 33
double-encapsulated attacks 25
forged transmissions 27
MAC address changes 27
MAC flooding 25
multicast brute-force attacks 25
promiscuous mode 27
random frame attacks 25
security 25
spanning tree attacks 25
vCenter Server
connecting through firewall 19
firewall ports 18
vCenter Server users 44
vifs, uploading certificates and keys 77
virtual machines
copy and paste 89
disabling logging 92, 93
enabling copy and paste 90
isolation 13, 14
limiting variable information size 91
preventing device disconnection 90
resource reservations and limits 10
security  10
security recommendations  89
virtual network, security  22
virtual networking layer and security  12
virtualization layer, security  10
VLAN security  24
VLANs
  and iSCSI  33
  Layer 2 security  24
  security  22, 25
  VLAN hopping  24
VLANS, configuring for security  25
VMkernel, security  10
vMotion, securing with VLANs and virtual
  switches  24
vpuser  54
vSphere Authentication Proxy
  authenticating  69
  viewing  71
vSphere Authentication Proxy Server  69, 70
vSphere Client
  firewall ports connecting to virtual machine
    console  19
  firewall ports for direct connection  19
  firewall ports with vCenter Server  18