Security Hardening

VMware® Infrastructure 3 (VMware ESX 3.5 and VMware VirtualCenter 2.5)

By introducing a layer of abstraction between the physical hardware and virtualized systems running IT services, virtualization technology provides a powerful means to deliver cost savings via server consolidation as well as increased operational efficiency and flexibility. However, the added functionality introduces a virtualization layer that itself becomes a potential avenue of attack for the virtual services being hosted. Because a single host system can house multiple virtual machines, the security of that host becomes even more important.

Because it is based on a light-weight kernel optimized for virtualization, VMware® ESX and VMware ESXi are less susceptible to viruses and other problems that affect general-purpose operating systems. However, ESX/ESXi is not impervious to attack, and you should take proper measures to harden it, as well as the VMware VirtualCenter management server, against malicious activity or unintended damage. This paper provides recommendations for steps you can take to ensure that your VMware Infrastructure 3 environment is properly secured. The paper also explains in detail the security-related configuration options of the components of VMware Infrastructure 3 and the consequences for security of enabling certain capabilities.

For additional up-to-date information on the security of VMware products, go to the VMware Security Center. See "References" on page 30 for a link. The VMware Security Center provides links to security advisories, alerts, and updates, as well as security utilities and other security-related papers.

The information in this paper applies to ESX 3.5/ESXi 3.5 and VirtualCenter 2.5. It is divided into sections based upon the components of VMware Infrastructure 3. The sections on virtual machines, VirtualCenter, and client components apply to both ESX 3.5 and ESXi 3.5. Host configuration issues are discussed in separate sections for ESX 3.5 and ESXi 3.5. Be sure to consult the sections that apply to the VMware Infrastructure software you are using.

The paper covers the following topics:

Virtual Machines

The recommendations in this section apply to the way you configure virtual machines and the ways you interact with virtual machines.

Secure Virtual Machines as You Would Secure Physical Machines

A key to understanding the security requirements of a virtualized environment is the recognition that a virtual machine is, in most respects, the equivalent of a physical server. Hence the guest operating system that runs in the virtual machine is subject to the same security risks as a physical system. Therefore, it is critical that you employ the same security measures in virtual machines that you would for physical servers.

Ensure that antivirus, antispyware, intrusion detection, and other protection are enabled for every virtual machine in your virtual infrastructure. Make sure to keep all security measures up-to-date, including applying appropriate patches. It is especially important to keep track of updates for dormant virtual machines that are powered off, because it could be easy to overlook them.

Disable Unnecessary or Superfluous Functions

By disabling unnecessary system components that are not needed to support the application or service running on the system, you reduce the number of parts that can be attacked. Some of these steps include:

- Disable unused services in the operating system. For example, if the system runs a file server, make sure to turn off any Web services.
- Disconnect unused physical devices, such as CD/DVD drives, floppy drives, and USB adapters. This is described in the section "Removing Unnecessary Hardware Devices" in the *ESX Server 3 Configuration Guide*.
- Turn off any screen savers. If using a Linux, BSD, or Solaris guest operating system, do not run the X Window system unless it is necessary.

Take Advantage of Templates

By capturing a hardened base operating system image (with no applications installed) in a template, you can ensure that all your virtual machines are created with a known baseline level of security. You can then use this template to create other, application-specific templates, or you can use the application template to deploy virtual machines. Make sure to keep patches and security measures up-to-date in templates. In VMware Infrastructure 3, you can convert a template to a virtual machine and back again quickly, which makes updating templates quite easy. VMware Update Manager also provides the ability to patch the operating system and certain applications in a template automatically, thus ensuring that they remain up to date.

Prevent Virtual Machines from Taking Over Resources

By using the resource management capabilities of ESX/ESXi, such as shares and limits, you can control the server resources that a virtual machine consumes. You can use this mechanism to prevent a denial of service that causes one virtual machine to consume so much of the host's resources that other virtual machines on the same host cannot perform their intended functions. By default, all virtual machines on an ESX/ESXi host share the resources equally. Bear in mind, however, that a virtual machine that exhibits unusual memory and storage access patterns might still have the potential to cause performance degradation on other virtual machines. It is recommended that you monitor all virtual machines for unusual or unexpected performance to be aware of such situations.

Isolate Virtual Machine Networks

Although the virtual hardware of one virtual machine is isolated from that of other virtual machines, virtual machines also are typically connected to shared networks. Any virtual machine or group of virtual machines connected to a common network can communicate across those network links and can, therefore, still be the target of network attacks from other virtual machines on the network. As a result, you should apply network best practices to harden the network interfaces of virtual machines Consider isolating sets of virtual machines on their own network segments to minimize the risks of data leakage from one virtual machine zone to the next across the network.

Network segmentation mitigates the risk of several types of network attacks, including Address Resolution Protocol (ARP) address spoofing, in which an attacker manipulates the ARP table to remap MAC and IP addresses to redirect network traffic to and from a given host to another unintended destination. Attackers use ARP spoofing to generate denials of service, hijack the target system, and otherwise disrupt the virtual network.

Segmentation has the added benefit of making compliance audits much easier, because it gives you a clear view of which virtual machines are linked by a network.

You can implement segmentation using either of two approaches, each of which has its own benefits:

- Use separate physical network adapters for virtual machine zones by creating separate virtual switches for each one. Maintaining separate physical network adapters for virtual machine zones is less prone to misconfiguration after you initially create segments.
- 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, while also allowing for redundancy options.

For more information on using VLANs with virtual machines, see the section “Securing Virtual Machines with VLANs” in the *ESX Server 3 Configuration Guide*.

Minimize Use of the VI Console

The VI Console allows you to connect to the console of a virtual machine, in effect seeing what a monitor on a physical server would show. However, the VI Console also provides power management and removable device connectivity controls, which could potentially allow a malicious user to bring down a virtual machine. In addition, it also has a performance impact on the service console, especially if many VI Console sessions are open simultaneously. Instead of VI Console, use native remote management services, such as terminal services and ssh, to interact with virtual machines.

Virtual Machine Files and Settings

Virtual machines are encapsulated in a small number of files. One of the important is the configuration file (`.vmx`), which governs the behavior of the virtual hardware and other settings. You can view and modify the configuration settings by viewing the `.vmx` file directly in a text editor or by checking the settings in the VI Client, using the following procedure:

1 Choose the virtual machine in the inventory panel.

2 Click **Edit settings**. Click **Options** > **Advanced/General**.

3 Click **Configuration Parameters** to open the Configuration Parameters dialog box.

Whether you change a virtual machine's settings in the VI Client or using a text editor, you must restart the virtual machine for most changes to take effect.

A virtual machine also includes one or more `.vmdk` files, which represent the virtual disks used by the guest operating system.

The following sections provide guidelines you should observe when dealing with these and other virtual machine files.

Disable Copy and Paste Operations Between the Guest Operating System and Remote Console

When VMware Tools runs in a virtual machine, by default you can copy and paste between the guest operating system and the computer where the remote console is running. As soon as the console window gains focus, nonprivileged 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. It is recommended that you disable copy and paste operations for the guest operating system by creating the parameters shown in Table 1.

Table 1. Configuration Settings to Disable Copy and Paste

Name	Value
`isolation.tools.copy.disable`	`true`
`isolation.tools.paste.disable`	`true`
`isolation.tools.setGUIOptions.enable`	`false`

Limit Data Flow from the Virtual Machine to the Datastore

Virtual machines can write troubleshooting information to a virtual machine log file (`vmware.log`) stored on the VMware VMFS volume used to store other files for the virtual machine. Virtual machine users and processes can be configured to abuse the logging function, either intentionally or inadvertently, so that large amounts of data flood the log file. Over time, the log file can consume so much of the ESX/ESXi host's file system space that it fills the hard disk, causing an effective denial of service as the datastore can no longer accept new writes.

To prevent this problem, consider modifying the logging settings for virtual machines. You can use these settings to limit the total size and number of log files. Normally a new log file is created only when a host is rebooted, so the file can grow to be quite large, but you can ensure new log files are created more frequently by limiting the maximum size of the log files. If you want to restrict the total size of logging data, VMware recommends saving 10 log files, each one limited to 100KB. These values are small enough that the log files should not consume an undue amount of disk space on the host, yet the amount of data stored should capture sufficient information to debug most problems.

Each time an entry is written to the log, the size of the log is checked, and if it is over the limit, the next entry is written to a new log. If the maximum number of log files already exists, when a new one is created, the oldest log file is deleted. A denial of service attack that avoids these limits could be attempted by writing an enormous log entry, but each log entry is limited to 4KB, so no log files are ever more than 4KB larger than the configured limit. Table 2 shows which parameters to set and their recommended values:

Table 2. Configuration Settings to Limit Log File Size and Number of Log Files

Name	Recommended Value
`log.rotateSize`	`100000`
`log.keepOld`	`10`

A second option is to disable logging for the virtual machine. Disabling logging for a virtual machine makes troubleshooting challenging and support difficult, so you should not consider disabling logging unless the log file rotation approach proves insufficient. To disable logging, set the parameter shown in Table 3.

Table 3. Configuration Setting to Disable Virtual Machine Logging

Name	Recommended Value
`Isolation.tools.log.disable`	`true`

Disabling logging in this manner does not completely disable all logging messages. The VMX process, which runs on the ESX host and is partly responsible for providing virtualization services for the virtual machine, continues to write logging messages to the virtual machine log file. However, the volume of messages from this source is very low and cannot be exploited from within the virtual machine, so it is not normally considered a potential source of data flooding.

If you nevertheless want to prevent all forms of logging, you can disable all messages by setting the parameter shown in Table 4. However this is not recommended in a normal production environment.

Table 4. Configuration Setting to Disable Virtualization Service Logging

Name	Recommended Value
`logging`	`false`

In addition to logging, guest operating system processes can send informational messages to the ESX/ESXi host through VMware Tools. These messages, known as setinfo messages, are written to the virtual machine's configuration file (`.vmx`). They typically contain name-value pairs that define virtual machine characteristics or identifiers that the host stores—for example, `ipaddress=10.17.87.224`. A setinfo message has no predefined format and can be any length. Therefore, the amount of data passed to the host in this way is unlimited. An unrestricted data flow provides an opportunity for an attacker to stage a DOS attack by writing software that mimics VMware Tools and flooding the host with packets, thus consuming resources needed by the virtual machines.

To prevent this problem, the configuration file containing these name-value pairs is limited to a size of 1MB. This 1MB capacity should be sufficient for most cases, but you can change this value, if necessary. You might increase this value if large amounts of custom information are being stored in the configuration file.

To modify the `GuestInfo` file memory limit, set the `tools.setInfo.sizeLimit` parameter in the `.vmx` file. The default limit is 1MB, and this limit is applied even when the `sizeLimit` parameter is not listed in the `.vmx` file. The example in Table 5 sets the size limit to 1MB.

Table 5. Configuration Setting to Limit Size of GuestInfo File

Name	Recommended Value
`tools.setInfo.sizeLimit`	`1048576`

You may also entirely prevent guest operating systems from writing any name-value pairs to the configuration file, using the setting in Table 6. This is appropriate when guest operating systems must be prevented from modifying configuration settings.

Table 6. Configuration Setting to Prevent Writing SetInfo Data to Configuration File

Name	Value
`isolation.tools.setinfo.disable`	`true`

Do Not Use Nonpersistent Disks

The security issue with nonpersistent disk mode is that attackers may undo or remove any traces that they were ever on the machine with a simple shutdown or reboot. Once the virtual machine has been shut down, the vulnerability used to access the virtual machine will still be present, and the attackers may access the virtual machine in the future at a time of their choice. The danger is that administrators may never know if they have been attacked or hacked. To safeguard against this risk, you should use nonpersistent disk mode only for test and development virtual machines. You should set production virtual machines to use persistent disk mode only. To verify, make sure that the parameter `scsiX:Y.mode` is not present, where `X` and `Y` are single digits, or that if it is present, the value is not `independent-nonpersistent`. You can configure this option in the VI Client for each individual disk on a virtual machine. You can make changes only when the virtual machine is not powered on. To review and modify these settings:

1 Log in to the VI Client and choose the server from the inventory panel.

  The hardware configuration page for the server appears.

2 Expand the inventory as needed and choose the virtual machine you want to check.

3 Click the **Edit Settings** link in the Commands panel to display the Virtual Machine Properties dialog box.

4 Click the **Hardware** tab.

5 Click the appropriate hard disk in Hardware list.

Ensure Unauthorized Devices are Not Connected

Besides disabling unnecessary virtual devices from within the virtual machine, you should ensure that no device is connected to a virtual machine if it does not need to be there. For example, serial and parallel ports are rarely used for virtual machines in a datacenter environment, and CD/DVD drives are usually connected only temporarily during software installation.

For less commonly-used devices, Table 7 shows the `.vmx` parameters that specify whether the device is available for a virtual machine to use. If the device is not needed, either the parameter should not be present or its value must be `FALSE`. The parameters listed in Table 7 are not sufficient to ensure that a device is usable, because other parameters are needed to indicate specifically how each device is instantiated.

Table 7. Configuration Parameters that Specify Certain Devices

Device	Configuration file parameter (where <x> is an integer 0 or greater)
Floppy drive	`floppy<X>.present`
Serial port	`serial<X>.present`
Parallel port	`parallel<X>.present`

Prevent Unauthorized Removal or Connection of Devices

Normal users and processes—that is users and processes without root or administrator privileges—within virtual machines have the capability to connect or disconnect devices, such as network adapters and CD-ROM drives.

For example, by default, a rogue user within a virtual machine can:

- Connect a disconnected CD-ROM drive and access sensitive information on the media left in the drive
- Disconnect a network adapter to isolate the virtual machine from its network, which is a denial of service

In general, you should use the virtual machine settings editor or Configuration Editor to remove any unneeded or unused hardware devices. However, you may want to use the device again, so removing it is not always a good solution. In that case, you can prevent a user or running process in the virtual machine from connecting or disconnecting a device from within the guest operating system by adding the parameter shown in Table 8.

Table 8. Configuration Setting to Prevent Device Removal or Connection

Name	Value
`Isolation.tools.connectable.disable`	`true`

Avoid Denial of Service Caused by Virtual Disk Modification Operations

Shrinking a virtual disk reclaims unused space in the virtual disk. If there is empty space in the disk, this process reduces the amount of space the virtual disk occupies on the host drive. Normal users and processes—that is users and processes without root or administrator privileges—within virtual machines have the capability to invoke this procedure. However, if this is done repeatedly, the virtual disk can become unavailable, effectively causing a denial of service. In most datacenter environments, disk shrinking is not done, so you should disable this feature by setting the parameters listed in Table 9.

Table 9. Configuration Settings to Prevent Virtual Disk Shrinking

Name	Value
`isolation.tools.diskWiper.disable`	`True`
`isolation.tools.diskShrink.disable`	`True`

Specify the Guest Operating System Correctly

Choosing the correct guest operating system in the configuration for each virtual machine is important. ESX optimizes certain internal configurations on the basis of this choice. The correct guest operating setting can aid the chosen operating system greatly and may cause significant performance degradation if there is a mismatch between the setting and the operating system actually running in the virtual machine. The performance degradation may be similar to running an unsupported operating system on ESX. Choosing the wrong guest operating system is not likely to cause a virtual machine to run incorrectly, but it could degrade the virtual machine's performance.

The parameter that specifies the guest operating system is `guestOS`. Verify that the specified operating system and matches the operating system actually running in the virtual machine, which you can determine by checking the virtual machine directly.

Verify Proper File Permissions for Virtual Machine Files

Be sure permissions for the virtual machine's files are set according to the guidelines in this section. Permissions for the configuration file (`.vmx`), should be read, write, execute (`rwx`) for owner, and read and execute (`r-x`) for group (755). Permissions for the virtual machine's virtual disk (`.vmdk`) should be read and write (`rw-`) for owner (600). For all of these files, both the user and group should be root.

Configuring the Service Console in ESX 3.5

Whether you use a management client or the command line, all configuration tasks for ESX 3.5 are performed through the service console, including configuring storage, controlling aspects of virtual machine behavior, and setting up virtual switches or virtual networks. As with an intelligent platform management interface (IPMI) or service processor on a physical server, someone logged in to the service console with privileged permissions has the ability to modify, shut down, or even destroy virtual machines on that host. The difference is that, instead of a single physical server, this can affect many virtual machines. Although ESX 3.5

management clients use authentication and encryption to prevent unauthorized access to the service console, other services might not offer the same protection. If attackers gain access to the service console, they are free to reconfigure many attributes of the ESX host. For example, they could change the entire virtual switch configuration or change authorization methods. Because the service console is the point of control for ESX, safeguarding it from misuse is crucial.

Configure the Firewall for Maximum Security

ESX 3.5 includes a firewall between the service console and the network. By default, the service console firewall is configured at a high security setting, with both incoming and outgoing traffic blocked by default except for a limited set of ports used by services that are enabled. The firewall contains a list of known services for which the appropriate incoming and outgoing ports are known, and it automatically opens ports for enabled services and closes them when a service is disabled. This section lists the services that are enabled by default when you install ESX 3.5. You can see the list of currently enabled services on an ESX host and the associated ports in the VI Client:

1 Choose the host.

2 Click the **Configuration** tab, then choose the **Security Profile** item under the Software heading.

3 Click **Firewall Properties**.

It is best to leave the default security firewall settings, which block all incoming and outgoing traffic that is not associated with an enabled services, then use the firewall's built-in service registry to enable and disable services. If you have a particular service or agent that is not part of the built-in list, you can open individual ports using the service console command `esxcfg-firewall`. If you do open ports, make sure to document the changes, including the purpose for opening each port. For more information on how to use the `esxcfg-firewall` command, see the section "Changing the Service Console Security Level" in the *ESX Server 3 Configuration Guide* or type `man esxcfg-firewall` on the command line.

Limit the Software and Services Running in the Service Console

Although the service console is based on Linux and is capable of running most Linux-based software, you should avoid running any additional software or services inside it wherever possible. Each additional component that is running represents an additional attack vector and also increases the potential for misconfiguration. For any service that you run in the service console, consider whether it is really needed and whether the equivalent functionality can be provided by an external agent that communicates with the ESX host using the standard built-in APIs.

The services that are on by default in the ESX 3.5 service console and the ports they use are described in Table 10. The second column of the table shows the string used to identify the service when using the `esxcfg-firewall` command—for example when running `esxcfg-firewall --query` to show the current status. The table also indicates when it is appropriate to disable a service. For example, if you are not using NFS to mount network shares in the service console, you should disable this service. "Configure the Firewall for Maximum Security" on page 8 describes how to use the VI Client to view which services are enabled. You can use the same properties dialog box to disable services as well as view them.

Table 10. Default Services in the ESX 3.5 Service Console

Service	Identification in esxcfg-firewall command	Port	Traffic Type	When to disable
CIM Service Location Protocol	CIMSLP	427	Incoming and outgoing UDP and TCP	If not using CIM-based software for monitoring or management
NFS client	nfsClient	111, 2049	Outgoing TCP and UDP	If not mounting NFS-based storage in the service console
VMware Consolidated Backup	VCB	443, 902	Outgoing TCP	If not using VCB for backup

Table 10. Default Services in the ESX 3.5 Service Console

Service	Identification in esxcfg-firewall command	Port	Traffic Type	When to disable
CIM over HTTP	CIMHttpServer	5988	Incoming TCP	If not using CIM-based software for monitoring or management
CIM over HTTPS	CIMHttpsServer	5989	Incoming TCP	If not using CIM-based software for monitoring or management
Licensing	LicenseClient	27000, 27010	Outgoing TCP	If using only host-based licensing
SSH Server	sshServer	22	Incoming TCP	If all management is done via VirtualCenter, VI Client, or other remote means
VirtualCenter Agent	vpxHeartbeats	902	Outgoing UDP	If not managed by VirtualCenter
VI API	n/a	443	Incoming and outgoing TCP	Must always be available
Secure access redirect	n/a	80	Incoming TCP	Must always be available

Additional software that might run in the service console includes management agents and backup agents. Although this software might have a legitimate purpose, the more components you have running in the service console, the more potential objects are susceptible to security vulnerabilities. In addition, these components often require specific network ports to be open in order to function, thus further increasing the avenues of attack.

For more information and recommendations on running third-party software in the service console, see http://www.vmware.com/vmtn/resources/516.

Use VI Client and VirtualCenter to Administer the Hosts Instead of Service Console

The best measure to prevent security incidents in the service console is to avoid accessing it if at all possible. You can perform many of the tasks necessary to configure and maintain the ESX host using the VI Client, either connected directly to the host or, better yet, going through VirtualCenter. The VI Client communicates using a well-defined API, which limits what can be done. This is safer than direct execution of arbitrary commands. Going through VirtualCenter has the added benefit that authorization and authentication are performed via your standard central Active Directory service, instead of using special local accounts in the service console. In addition, roles and users are stored in a database, providing an easy way to view the current permissions as well as take a snapshot of them. VirtualCenter also keeps track of every task invoked through it, providing an automatic audit trail.

Another alternative is to use a remote scripting interface, such as the VI Perl Toolkit or the remote command line interface (Remote CLI). These interfaces are built on the same API that VI Client and VirtualCenter use, so any script using them automatically enjoys the same benefits of authentication, authorization, and auditing.

In ESX 3.5, some advanced tasks, such as initial configuration for password policies, cannot be performed via the VI Client. For these tasks, you must log in to the service console. Also, if you lose your connection to the host, executing certain of these commands through the command line interface may be your only recourse—for example, if the network connection fails and you are therefore unable to connect using VI Client. These tasks are described in Appendix A of the *ESX Server 3 Configuration Guide*.

Use a Directory Service for Authentication

Advanced configuration and troubleshooting of an ESX host may require local privileged access to the service console. For these tasks, you should set up individual host-localized user accounts and groups for the few administrators with overall responsibility for your virtual infrastructure. Ideally, these accounts should correspond to real individuals and not be accounts shared by multiple people. Although you can create on the

service console of each host local accounts that correspond to each global account, this presents the problem of having to manage user names and passwords in multiple places. It is much better to use a directory service, such as NIS or LDAP, to define and authenticate users on the service console, so you do not have to create local user accounts.

In the default installation, ESX 3.5 cannot use Active Directory to define user accounts. However, it can use Active Directory to authenticate users. In other words, you can define individual user accounts on the host, then use the local Active Directory domain to manage the passwords and account status. You must create a local account for each user that requires local access on the service console. This should not be seen as a burden; in general, only relatively few people should have access to the service console, so it is better that the default is for no one to have access unless you have created an account explicitly for that user.

Authentication on the service console is controlled by the command `esxcfg-auth`. You can find information on this command in its man page. Type `man esxcfg-auth` at the command line when logged in to the service console. For information on authentication with Active Directory, see the technical note at http://www.vmware.com/vmtn/resources/582.

It is also possible to use third-party packages, such as Winbind or Centrify, to provide tighter integration with Active Directory. Consult the documentation for those solutions for guidance on how to deploy them securely.

Strictly Control Root Privileges

Because the root user of the service console has almost unlimited capabilities, securing this account is the most important step you can take to secure the ESX host. By default, all insecure protocols, such as FTP, Telnet, and HTTP, are disabled. Remote access via SSH is enabled, but not for the root account. You can copy files remotely to and from the service console using an scp (secure cp) client, such as WinSCP.

Enabling remote root access over SSH or any other protocol is not recommended, because it opens the system to network-based attack should someone obtain the root password. A better approach is to log in remotely using a regular user account, then use `sudo` to perform privileged commands. The `sudo` command enhances security because it grants root privileges only for select activities, in contrast with the `su` command, which grants root privileges for all activities. Using `sudo` also provides superior accountability because all `sudo` activities are logged, whereas if you use `su`, ESX logs only the fact that the user switched to root by way of `su`. The `sudo` command also provides a way for you to grant or revoke execution rights to commands on an as-needed basis.

You can go a step further and disallow root access even on the console of the ESX host—that is, when you log in using a screen and keyboard attached to the server itself, or to a remote session attached to the server's console. This approach forces anyone who wants to access the system to first log in using a regular user account, then use `sudo` or `su` to perform tasks. Ideally, only a limited set of individuals need permission to run `su` in order to perform arbitrary administrative tasks. If you decide to disallow root login on the console, you should first create a nonprivileged account on the host to enable logins, otherwise you could find yourself locked out of the host. This nonprivileged account should be a local account—that is, one that does not require remote authentication—so that if the network connection to the directory service is lost, access to the host is still possible. You can assure this access by defining a local password for this account, using the `passwd` command. The local password overrides authentication via directory services (as discussed in the previous section). The net effect is that administrators can continue to access the system, but they never have to log in as root. Instead, they use `sudo` to perform particular tasks or `su` to perform arbitrary commands.

To prevent direct root login on the console, modify the file `/etc/securetty` to be empty. While logged in as root, enter the following command:

```
cat /dev/null > /etc/securetty
```

After you do this, only nonprivileged accounts are allowed to log in at the console. Note that this also can disable remote console capabilities, such as iLO and DRAC.

Control Access to Privileged Capabilities

Because `su` is such a powerful command, you should limit access to it. By default, only users that are members of the wheel group in the service console have permission to run `su`. If a user attempts to run `su -` to gain root privileges and that user is not a member of the wheel group, the `su -` attempt fails and the event is logged.

Besides controlling who has access to the `su` command, through the pluggable authentication module (PAM) infrastructure, you can specify what type of authentication is required to successfully execute the command. In the case of the `su` command, the relevant PAM configuration file is `/etc/pam.d/su`. To allow only members of the wheel group to execute the `su` command, and then only after authenticating with a password, find the line beginning with `auth required` and remove the leading pound sign (#) so it reads:

```
auth required /lib/security/$ISA/pam_wheel.so use_uid
```

The `sudo` utility should be used to control what privileged commands users can run while logged in to the service console. Among the commands you should regulate are all of the `esxcfg-*` commands as well as those that configure networking and other hardware on the ESX host. You should decide what set of commands should be available to more junior administrators and what commands you should allow only senior administrators to execute. You can also use `sudo` to restrict access to the `su` command.

Use the following tips to help you configure `sudo`:

- Configure local and remote `sudo` logging (see "Maintain Proper Logging" on page 12).
- Create a special group, such as vi_admins, and allow only members of that group to use `sudo`.
- Use `sudo` aliases to determine the authorization scheme, then add and remove users in the alias definitions instead of in the commands specification.
- Be careful to permit only the minimum necessary operations to each user and alias. Permit very few users to run the `su` command, because `su` opens a shell that has full root privileges but is not auditable.
- If you have configured authentication using a directory service, `sudo` uses it by default for its own authentication. This behavior is controlled by the `/etc/pam.d/sudo` file, on the line for `auth`. The default setting—`service=system-auth`—tells `sudo` to use whatever authentication scheme has been set globally using the `esxcfg-auth` command.
- Require users to enter their own passwords when performing operations. This is the default setting. Do not require the root password, because this presents a security risk, and do not disable password checking. In `sudo` the authentication persists for a brief period of time before `sudo` asks for a password again.

For further information and guidelines for using `sudo`, see http://www.gratisoft.us/sudo/.

Establish a Password Policy for Local User Accounts

For any local user accounts, the service console provides password controls on two levels to help you enforce password policies to limit the risk of password cracking:

- **Password aging**—These controls govern how long a user password can be active before the user is required to change it. They help ensure that passwords change often enough that if an attacker obtains a password through sniffing or social engineering, the attacker cannot continue to access the ESX host indefinitely.
- **Password complexity**—These controls ensure that users create passwords that are hard for password generators to determine. Instead of using words, a common technique for ensuring password complexity is to use a memorable phrase, then derive a password from it—for example, by using the first letter of each word.

Both of these policies are described in the section "Password Restrictions" in the *ESX Server 3 Configuration Guide*.

The default `pam_cracklib.so` plug-in provides sufficient password strength enforcement for most environments. However, if the `pam_cracklib.so` plug-in is not stringent enough for your needs, you can use the `pam_passwdqc.so` plug-in instead. You change the plug-in using the `esxcfg-auth` command.

For further protection, you can enforce account lockout after too many unsuccessful login attempts. To configure the ESX service console to disable the account after three unsuccessful login attempts, add the following lines to `/etc/pam.d/system-auth`:

```
auth required /lib/security/pam_tally.so no_magic_root
account required /lib/security/pam_tally.so deny=3
no_magic_root
```

To create the file for logging failed login attempts, execute the following commands:

```
touch /var/log/faillog
chown root:root /var/log/faillog
chmod 600 /var/log/faillog
```

Do Not Manage the Service Console as a Linux Host

The service console is generated from a Red Hat Linux distribution that has been modified to provide exactly the functionality necessary to communicate with and allow management of the VMkernel. Any additional software installed should not make assumptions about what RPM packages are present, nor that the software can modify them. In several cases, the packages that do exist have been modified especially for ESX.

It is particularly important that you not treat the service console like a Linux host when it comes to patching. Never apply patches issued by Red Hat or any other third-party vendor. Apply only patches that are published by VMware specifically for the versions of ESX that you have in use. These are published for download periodically, as well as on an as-needed basis for security fixes. You can receive notifications for security-related patches by signing up for email notifications at http://www.vmware.com/security.

Similarly, you should never use a scanner to analyze the security of the service console unless the scanner is specifically designed to work with your version of ESX. In particular, scanners that assume the service console is a standard Red Hat Linux distribution routinely yield false positives. These scanners typically look only for strings in the names of software, and therefore do not account for the fact that VMware releases custom versions of packages with special names when providing security fixes. Because these special names are unknown to the scanners, they flag them as vulnerabilities when in reality they are not. You should use only scanners that specifically treat the ESX service console as a unique target. For more information, see the section "Security Patches and Security Vulnerability Scanning Software" in the chapter "Service Console Security" of the *ESX Server 3 Configuration Guide*.

In addition, you should not manage the service console as if it were a traditional Linux host. The usual `redhat-config-*` commands are not present, nor are other components such as the X server. Instead, you manage the ESX host using a series of purpose-built commands, such as `vmkfstools` and the `esxcfg-*` commands. Many of these commands should be used only upon instruction from VMware Technical Support, or not invoked manually at all, but a few provide functionality that is not available via the VI Client, such as authentication management and advanced storage configuration.

If you follow the best practice of isolating the network for the service console, there is no reason to run any antivirus or other such security agents, and their use is not necessarily recommended. However, if your environment requires that such agents be used, use a version designed to run on Red Hat Enterprise Linux 3, Update 6.

For more information on the special administrative commands in the service console, see "ESX Technical Support Commands" and "Using vmkfstools" in the appendices of the *ESX Server 3 Configuration Guide*.

Maintain Proper Logging

Proper and thorough logging allows you to keep track of any unusual activity that might be a precursor to an attack and also allows you to do a postmortem on any compromised systems and learn how to prevent attacks from happening in the future.

The syslog daemon performs the system logging in ESX. You can access the log files in the service console by going to the /var/log/ directory. Several types of log files generated by ESX are shown in Table 11.

Table 11. Key Log Files Generated by ESX

Component	Location	Purpose
Vmkernel	/var/log/vmkernel	Records activities related to the virtual machines and ESX
VMkernel warnings	/var/log/vmkwarning	Records activities with the virtual machines
VMkernel summary	/var/log/vmksummary	Used to determine uptime and availability statistics for ESX; human-readable summary found in /var/log/vmksummary.txt
ESX host agent log	/var/log/vmware/hostd.log	Contains information on the agent that manages and configures the ESX host and its virtual machines
Virtual machines	The same directory as the affected virtual machine's configuration files; named vmware.log and vmware–*.log	Contain information when a virtual machine crashes or ends abnormally
VirtualCenter agent	/var/log/vmware/vpx	Contains information on the agent that communicates with VirtualCenter
Web access	Files in /var/log/vmware/webAccess	Records information on Web-based access to ESX
Service console	/var/log/messages	Contain all general log messages used to troubleshoot virtual machines or ESX
Authentication log	/var/log/secure	Contains records of connections that require authentication, such as VMware daemons and actions initiated by the xinetd daemon.

The log files provide an important tool for diagnosing security breaches as well as other system issues. They also provide key sources of audit information. In addition to storing log information in files on the local file system, you can send this log information to a remote system. The syslog program is typically used for computer system management and security auditing, and it can serve these purposes well for ESX hosts. You can select individual service console components for which you want the logs sent to a remote system.

The following tips provide best practices for logging:

- Ensure accurate time-keeping.

  By ensuring that all systems use the same relative time source (including the relevant localization offset), and that the relative time source can be correlated to an agreed-upon time standard (such as Coordinated Universal Time—UTC), you can make it simpler to track and correlate an intruder's actions when reviewing the relevant log files. In the service console, you set the time source using the NTP (Network Time Protocol) system. For instructions on how to configure NTP, see VMware knowledge base article 1339 (http://kb.vmware.com/kb/1339).

- Control growth of log files.

  In order to prevent the log file from filling up the disk partition on which it resides, configure log file rotation. This automatically creates a backup of the log file after it reaches a certain specified size and keeps only a specified number of older backup files before automatically deleting them, thus limiting the total disk usage for logging. The log rotation behavior is specified for each component in configuration files located in the directory /etc/logrotate.d as well as in the file /etc/logrotate.conf.

  For the three files in /etc/logrotate.d—vmkernel, vmksummary, and vmkwarning—it is recommend that the configuration be modified to:

  - Increase the size of the log file to 4096k.
  - Enable compression by setting the line compress instead of nocompress.

This allows greater logging in the same file system space. For more information on configuring log file rotation, see `man logrotate`.

- Use remote syslog logging.

  Remote logging to a central host provides a way to greatly increase administration capabilities. By gathering log files onto a central host, you can easily monitor all hosts with a single tool as well as do aggregate analysis and searching to look for such things as coordinated attacks on multiple hosts.

  An important point to consider is that the log messages are not encrypted when sent to the remote host, so it is important that the network for the service console be strictly isolated from other networks.

  Syslog behavior is controlled by the configuration file `/etc/syslog.conf`. For logs you want to send to a remote log host, add a line with `@<loghost.company.com>` after the message type, where `<loghost.company.com>` is the name of a host configured to record remote log files. Make sure that this host name can be properly resolved, putting an entry in the name service maps if needed.

  Example:

  ```
  local6.warning @<loghost.company.com>
  ```

  After modifying the file, tell the syslog daemon to reread it by issuing the following command:

  ```
  kill –SIGHUP `cat /var/run/syslogd.pid`
  ```

- Display different log level messages on different screens.

  An option for syslog is to log to an alternate console, which can be displayed from the terminal of the ESX host. ESX has the capability at the console to display a number of virtual terminals. This gives you the capability to have critical, error, and warning messages displayed on different screens, enabling you to quickly differentiate types of errors.

  To enable this separation of log message display, add the following lines to the `/etc/syslog.conf` file:

  ```
  *.crit /dev/tty2
  ```

  All log items at the critical level or higher are logged to the virtual terminal at tty2. Press Alt-F2 at the ESX console to view these logs.

  ```
  *.err /dev/tty3
  ```

  All log items at the error level or higher are logged to the virtual terminal at tty3. Press Alt-F3 at the ESX console to view these logs

  ```
  *.warning /dev/tty4
  ```

  All log items at the warning level or higher are logged to the virtual terminal at tty4. Press Alt-F4 at the ESX Server console to view these logs.

  When you are finished, issue the command for rereading the configuration file:

  ```
  kill –SIGHUP `cat /var/run/syslogd.pid`
  ```

- Use local and remote `sudo` logging.

  If you have configured `sudo` to enable controlled execution of privileged commands, you can benefit from using syslog to audit use of these commands. By default, all invocations of `sudo` are logged to `/var/log/secure`. By modifying the line containing this filename in the syslog configuration file as described above, you can have all these log messages also sent to a remote syslog server.

Establish and Maintain File System Integrity

The service console has a number of files that specify its configurations:

- `/etc/profile`
- `/etc/ssh/sshd_config`
- `/etc/pam.d/system–auth`

- /etc/grub.conf
- /etc/krb.conf
- /etc/krb5.conf
- /etc/krb.realms
- /etc/login.defs
- /etc/openldap/ldap.conf
- /etc/nscd.conf
- /etc/ntp
- /etc/ntp.conf
- /etc/passwd
- /etc/group
- /etc/nsswitch.conf
- /etc/resolv.conf
- /etc/sudoers
- /etc/shadow

In addition, ESX configuration files located in the /etc/vmware directory store all the VMkernel information.

All of these files should be monitored for integrity and unauthorized tampering, using a commercial tool such as Tripwire or Configuresoft, or by using a checksum tool such as sha1sum, which is included in the service console. These files should also be backed up regularly, either using backup agents or by doing backups based on file copying. Not all of these files are actually used by your particular ESX deployment, but all the files are listed for completeness.

Another check to perform is to make sure that the file permissions of important files and utility commands have not been changed from the default. Some files in particular to check include:

- The /usr/sbin/esxcfg-* commands, which are all installed by default with permissions 500, except for esxcfg-auth which has permissions 544.
- The log files discussed in the previous section, which all have permissions 600, except for the directory /var/log/vmware/webAccess, which has permissions 755, and the virtual machine log files, which have permissions 644.
- Certain system commands that have the SUID bit. These commands are listed in Table 12-3 of the *ESX Server 3 Configuration Guide*.

For all of these files, the user and group owner should be root.

Secure the SNMP Configuration

ESX 3.5 provides an SNMP agent to monitor faults and system status. It supports SNMP versions 1, 2c, and 3. When an SNMP agent is enabled in ESX, network management tools can listen for notifications or poll for status information about the configuration of virtual machines and the state of the network, CPU, disk, and installed software.

It is recommended that you configure ESX 3.5 to use SNMP version 3, which provides for authentication and privacy of messages between the agent and management station. Consult the snmpd.conf man page for more information on configuring SNMP.

Protect against the Root File System Filling Up

When you install ESX 3.5, you should accept the recommended disk partitioning for the most effective installation. If you choose to partition the disk manually, you should ensure that you have created separate partitions for the directories `/home`, `/tmp`, and `/var/log`. These are all directories that have the potential to fill up, and if they are not isolated from the root partition, you could experience a denial of service if the root partition is full and unable to accept any more writes. "Datastore Partitioning," an appendix of the *Installation and Upgrade Guide*, covers disk partitions in more detail.

Disable Automatic Mounting of USB Devices

External USB drives can be connected to the ESX host and be loaded automatically on the service console. The USB drive must be mounted before you can use it, but drivers are loaded to recognize the device. Malicious users may be able to run malicious code on the ESX host and go undetected because the USB drive is external. By default, automatic USB drive mounting is enabled, but it is recommended that you disable this feature by editing the service console file `/etc/modules.conf` and commenting out the line containing `alias usb-controller` by placing a pound sign (`#`) at the beginning.

Configuring Host-level Management in ESXi 3.5

Even though ESXi 3.5 does not ship with a service console, there are some aspects of host-level management that you can configure and monitor. Some of these options are new to the ESXi architecture, and some are analogous to options available in ESX 3.5.

Strictly Control Root Privileges

You might want to avoid managing ESXi hosts directly, but instead prefer to require that all management be done through VirtualCenter. This enforces the use of a central authentication model (typically Active Directory) and allows permissions to be set globally. It also allows all tasks to be logged in one place, the VirtualCenter database, which makes auditing easier.

Lockdown mode is available on any ESXi 3.5 host that you have added to a VirtualCenter Server. Enabling lockdown mode disables all remote root access to ESXi 3.5 machines. Any subsequent local changes to the host must be made:

- In a VI Client session or using Remote CLI commands to VirtualCenter.
- In a VI Client session or using Remote CLI commands direct to the ESXi 3.5 system using a local user account defined on the host. By default, no local user accounts exist on the ESXi system. You must create those accounts before enabling lockdown mode and must create them in a VI Client session connected directly to the ESXi system. Changes to a host are limited to those that can be made with the privileges granted to a particular user locally on that host.

It is recommended that you enable lockdown mode for your ESXi 3.5 hosts. You can enable and disable lockdown mode either using a VI Client logged into VirtualCenter or using the direct console user interface (DCUI). For details on how to do this, see the chapter "Security Deployments and Recommendations" in the *ESX Server 3i Configuration Guide.*

Control Access to Privileged Capabilities

Ideally, you manage users who access the ESXi 3.5 system with the user management features of VirtualCenter. In certain cases, however, you need to manage a host directly—for example:

- You have not purchased VirtualCenter—perhaps because you are just starting out with ESXi or because you have a very small deployment
- You want to provide for administrative access to the system in case VirtualCenter is down or otherwise unavailable, or if the VirtualCenter agent on the host is not working properly
- You need to use Remote CLI commands, such as those for backing up and restoring the configuration of the system, that must be run directly on the host, not through VirtualCenter

Security best practices dictate that the root password should be known to as few individuals as possible, and the root account should not be used if any alternative is possible, because it is an anonymous account and activity by the root user cannot be definitively associated with a specific individual. The root password is initially blank, so one of your first steps in configuring the server should be to create a strong password for the root account.

ESXi 3.5 allows you to create local users and groups on the system. Definitions for these users and groups are stored locally on each individual ESXi host, and the definitions for each host are totally independent of other hosts. You cannot use Active Directory or any other directory service to identify or authenticate the local users. Furthermore, the user and group lists maintained by VirtualCenter are completely separate from the lists maintained by ESXi hosts. Even if the lists maintained by a host and VirtualCenter appear to have common users (for instance, a user called devuser), you must treat these users as separate users who happen to have the same name. The attributes of devuser in VirtualCenter, including permissions and passwords, are separate from the attributes of devuser on the ESXi host. If you log on to VirtualCenter as devuser, you might have permission to view and delete files from a datastore, whereas if you log on to an ESXi host as devuser, you might not.

Because of the confusion that duplicate naming can cause, VMware recommends that you check the VirtualCenter user list before you create ESXi host users so you can avoid creating host users that have the same names as VirtualCenter users. To check for VirtualCenter users, review the Windows domain list.

You can grant various levels of permissions to local users. The privilege model for an ESXi host mirrors that of VirtualCenter, except it lacks objects such as datacenters and clusters, which have no meaning for an individual host. You can create custom roles that grant specific privileges, then assign them to certain users. These privileges affect what a particular user can do, both in a VI Client and using the Remote CLI. You should create a different local user account for any person who might need direct access to the host and grant that user particular privileges to limit the user's capabilities. You can use local group definitions to simplify this assignment.

One particular built-in local group has special meaning. If you give a user membership in the localadmin group, that user has the ability to log in to the DCUI, which is the interface available at the console of an ESXi host that allows for basic host configuration—modifying networking settings and the root password, for example. Assignment to this group enables an administrative user to perform tasks on the DCUI without logging in as root. However, this is a very powerful privilege, because access to the DCUI allows someone to change the root password or even power off the host. Therefore, only the most trusted administrators should be granted membership to the localadmin group.

For more information on local users and privileges in ESXi, see the chapter "Authentication and User Management" in the *Server 3i Configuration Guide*.

Maintain Proper Logging

ESXi 3.5 maintains a log of activity in log files. It uses a syslog facility, just as ESX 3.5 does. However, ESXi maintains a smaller number of log files. The following logs are available:

- `hostd.log`
- `messages`
- `vpxa.log` (only if the host has beed joined to a VirtualCenter instance)

There are several ways to view the contents of these log files.

To view the logs in a VI Client, take the following steps:

1 Log in directly to the ESXi host using VI Client and make sure the host is selected in the Inventory.

2 Click **Administration**, then click the **System Logs** tab.

3 Choose the log file you want to view in the drop-down menu in the upper left.

To view the logs in a Web browser, enter the URL `https://<hostname>/host`, where `<hostname>` is the host name or IP address of the management interface of the ESXi host, then choose from the list of files presented.

You can use the Remote CLI command `vifs` to download the log files to your local system.

You can also configure syslog to send log messages to a remote system.

As with ESX 3.5, you should configure NTP on the host to ensure accurate time-keeping.

You can find more information on configuring syslog and NTP for ESXi hosts in the following documents:

- The "System Log Files" and "Host Configuration for ESX Server and VirtualCenter" sections of the "System Configuration" chapter in the *Basic System Administration Guide*.
- The appendix "Remote Command Line Interface Reference" in the *ESX Server 3i Configuration Guide*.

Establish and Maintain Configuration File Integrity

As with ESX, ESXi maintains its configuration state in a set of configuration files. However, on ESXi these files can be accessed only using the remote file access API, and there are far fewer files involved. These files normally are not modified directly. Instead, their contents normally change indirectly because of some action invoked on the host. However, the file access API does allow for direct modification of these files, and some modifications might be warranted in special circumstances. Therefore, you should monitor all of these files for integrity and unauthorized tampering, either by periodically downloading them and tracking their contents or by using a commercial tool designed to do this. The accessible and relevant configuration files in ESXi 3.5 are:

- `esx.conf`
- `hostAgentConfig.xml`
- `hosts`
- `license.cfg`
- `motd`
- `openwsman.conf`
- `proxy.xml`
- `snmp.xml`
- `ssl_cert`
- `ssl_key`
- `syslog.conf`
- `vmware_config`
- `vmware_configrules`
- `vmware.lic`
- `vpxa.cfg`

To view the configuration files in a Web browser, enter the URL `https://<hostname>/host` where `<hostname>` is the host name or IP address of the management interface of the ESXi host, then choose from the list of files presented.

You can use the Remote CLI command `vifs` to download the configuration files to your local system, as well as to upload new versions of these files. Although in some cases the new settings take effect immediately, you should always restart the ESX host after making changes directly to the configuration files (as opposed to making configuration changes via the VI Client, VirtualCenter, or the Remote CLI).

Secure the SNMP Configuration

ESXi 3.5 contains a different SNMP agent from that in ESX 3.5, and it supports only versions 1 and 2c. It provides the same notifications as ESX 3.5 and adds notifications for hardware-related sensors. Unlike ESX 3.5, it supports only the SNMPv2-MIB and supports it only for discovery, inventory, and diagnostics of the SNMP agent.

SNMP messages contain a field called the community string, which conveys context and usually identifies the sending system for notifications. This field also provides context for the instance of a MIB module on which the host should return information. ESX/ESXi SNMP agents allow multiple community strings per notification target as well as for polling. Keep in mind that community strings are not meant to function as passwords, but only as a method for logical separation.

SNMP v1 and v2c traffic is not encrypted, which means that messages can be snooped, and they could be modified in-flight without the receiver knowing about it. Ways to mitigate this risk include:

- Run SNMP on trusted networks, use routing and layer 2 filtering to lock down MAC addresses to layer 2 ports, and route SNMP traffic to trusted servers.
- Run SNMP in a VPN/IPsec tunnel on your edge routers for SNMP traffic.

Ensure Secure Access to CIM

The Common Information Model (CIM) system provides an interface that enables hardware-level management from remote applications via a set of standard APIs. To ensure that the CIM interface is secure, follow these recommendations:

- Do not provide root credentials to remote applications to access the CIM interface. Instead, create a service account specific to these applications. Read-only access to CIM information is granted to any local account defined on the ESXi system.
- If the application requires write access to the CIM interface, only two local privileges are required. It is recommended that you create a local role to apply to the service account with only these privileges:
  - **Host > Config > SystemManagement**
  - **Host > CIM > CIMInteraction**

Audit or Disable Technical Support Mode

ESXi has a special technical support mode, which is an interactive command line available only on the console of the server. Technical support mode is unsupported unless used in consultation with VMware Technical Support and must be activated before it can be used. Access to this mode requires the root password of the server in addition to access to the console of the server, either physically or through a remote KVM or iLO interface.

Technical support mode is designed to be used only in cases of emergency, when management agents that provide the remote interfaces are inoperable and they cannot be restarted through the DCUI. There is no reason to use technical support mode for any other purpose apart from technical support. Technical support mode is on by default, but you can disable it entirely.

Technical support mode is secured in the following ways:

- It is accessible only on the local console; unlike SSH or Telnet, it cannot be accessed remotely. Thus, physical access to the host—or something equivalent to physical access, such as HP ILO, Dell DRAC, IBM RSA, or a similar remote console tool—is absolutely required for access to technical support mode. Most organizations have sufficient forms of protection on physical (or physical equivalent) access to the host (for example, door locks, key cards, and authentication for the remote console).
- It requires the root password before access is granted. Any individuals who have both physical (or console) access and the root password are already fully privileged and can do anything they want on the system. The presence of technical support mode does not augment or reduce this risk.

You can audit technical support mode using the following information:

- Whenever someone activates technical support mode, the time and date of activation are sent to the system log messages file.
- All unsuccessful attempts to access technical support mode (that is, someone enters the incorrect root password) are recorded in the system log.
- The time and date of all successful accesses to technical support mode are sent to the system log

To ensure accurate and reliable system logs, you should configure remote syslog on the server, so log messages are kept on an outside system and cannot be altered from the server. Actions performed while in technical support mode are not logged. Any access to technical support mode should be correlated with a specific call to VMware Technical Support. If there is no corresponding support session, you should immediately suspect malicious activity and inspect the system for tampering.

If you are unable to audit technical support mode to a degree that matches your security risk posture, you should disable it for all of your ESXi hosts. For details on disabling technical support mode, see VMware knowledge base article 1003677 (http://kb.vmware.com/kb/1003677).

Configuring the ESX/ESXi Host

The following recommendations apply to the way the ESX/ESXi host itself is configured. Many of the recommendations apply to the configuration of the networks to which virtual machines are attached, because most security attacks occur through network connections. Others pertain to the operation of the ESX/ESXi software itself.

Isolate the Infrastructure-related Networks

Several capabilities of VMware Infrastructure involve communication among components over a network.

- Management. This includes the following types of communication:
  - Between ESX/ESXi and VirtualCenter
  - Amongst ESX/ESXi hosts—for example, for VMware High Availability coordination
  - Between ESX/ESXi or VirtualCenter and systems running client software such as the VI Client or a VI SDK application
  - Between ESX/ESXi and ancillary management services, such as DNS, NTP, syslog, and the user authentication service
  - Between ESX/ESXi and third-party management tools, such as hardware monitoring, systems management, and backup tools
  - Between VirtualCenter and supporting services, such as the VirtualCenter database and the user authentication service
  - Between VirtualCenter and optional add-on components such as VMware Update Manager and VMware Converter Enterprise, if they are installed on separate servers
- VMotion. This involves transferring the live running state of a virtual machine from one ESX/ESXi host to another.
- Storage. This includes any network-based storage, such as iSCSI and NFS.

All of the networks used for these communications provide direct access to core functionality of VMware Infrastructure, The management network provides access to the VMware Infrastructure management interface on each component, and any remote attack would most likely begin with gaining entry to this network. VMotion traffic is not encrypted, so the entire state of a virtual machine could potentially be snooped from this network. Finally, access to the storage network potentially allows someone to read the contents of

virtual disks residing on shared storage. Therefore, all of these networks should be isolated and strongly secured from all other traffic, especially any traffic going to and from virtual machines. The exception is if one of the components listed above actually runs in a virtual machine. In that case, this virtual machine naturally has an interface on the management network and thus should not have an interface on any other network.

VMware recommends that you isolate networks using one of these methods:

- Create a separate VLAN for each network.
- Configure network access for each network through its own virtual switch and one or more uplink ports.

In either case, you should consider using NIC teaming for the virtual switches to provide redundancy.

If you use VLANs, you need fewer physical NICs to provide the isolation, a factor that is especially important in environments with constrained hardware such as blades. VMware virtual switches are by design immune to certain types of attacks that have traditionally targeted VLAN functionality. For details, see the chapter "Securing an ESX Server 3 Configuration" in the *ESX Server 3 Configuration Guide*. In general, VMware believes that VLAN technology is mature enough that it can be considered a viable option for providing network isolation.

ESX/ESXi does not support virtual switch port groups configured to VLAN 1. If the physical switch port to which the ESX/ESXi host is connected is configured with VLAN 1, ESX/ESXi drops all packets. You can configure the ESX/ESXi virtual switch port groups with any value between 2 and 4094. Utilizing VLAN 1 causes a denial of service because ESX/ESXi drops this traffic. It is recommended that you check the physical network hardware configuration to verify the ports to which the ESX/ESXi host connects are not configured to VLAN 1. In addition, VLAN ID 4095 specifies that the port group should use trunk mode or VGT mode, which allows the guest operating system to manage its own VLAN tags. Guest operating systems typically do not manage their VLAN membership on networks, so if this value is set, ensure that there is a legitimate reason for doing so.

If you do not use VLANs, either because you have no VLAN support in your environment or because you do not consider VLANs strong enough for isolation, you can combine the three types of infrastructure-related networks onto two or fewer virtual switches. However, you should still keep the virtual machine networks separate from the infrastructure networks by using separate virtual switches with separate uplinks.

Configure Encryption for Communication between Clients and ESX/ESXi

Client sessions with the ESX/ESXi host may be initiated from any VI API client, such as VI Client, VirtualCenter, and the Remote Command Line Interface. SSL encryption protects the connection between the VI Client and ESX/ESXi, but the default certificates used to secure your VirtualCenter and VI Web Access sessions are not signed by a trusted certificate authority and, therefore, do not provide the authentication security you might need in a production environment. These self-signed certificates are vulnerable to man-in-the-middle attacks, and clients receive a warning about them. If you intend to use encrypted remote connections externally, consider purchasing a certificate from a trusted certificate authority or use your own security certificate for your SSL connections. Enabling certificate checking and installation of new certificates are described in the chapter "Authentication and User Management" in the *ESX Server 3 Configuration Guide*.

Label Virtual Networks Clearly

Label all your virtual networks appropriately to prevent confusion or security compromises. This labeling prevents operator error caused by attaching a virtual machine to a network it is not authorized for or to a network that could allow the leakage of sensitive information.

Do Not Create a Default Port Group

During ESX/ESXi installation, you have the option of creating a default virtual machine port. However, this option creates a virtual machine port group on the same network interface as the service console. If this setting is left unchanged, it could allow virtual machines to detect sensitive and often unencrypted information. Because the service console should always be on a separate, private network, this option should never be used except in a test environment.

Do Not Use Promiscuous Mode on Network Interfaces

ESX/ESXi can run virtual network adapters in promiscuous mode. You can enable promiscuous mode on virtual switches that are bound to a physical network adapter (vmnic) and virtual switches that do not bind to a physical network adapter (vmnet). When promiscuous mode is enabled for a vmnic switch, all virtual machines connected to the virtual switch have the potential of reading all packets sent across that network, from other virtual machines as well as any physical machines or other network devices. When promiscuous mode is enabled for a vmnet switch, all virtual machines connected to the vmnet switch have the potential of reading all packets across that network—that is, traffic among the virtual machines connected to that vmnet switch.

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 packets regardless of whether some of the packets should be 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 operating systems. You should use promiscuous mode only for security monitoring— for example, for an IDS system, debugging, or troubleshooting.

By default, promiscuous mode is set to Reject. You can change this option by modifying the security policy on an individual port group or on the entire virtual switch, as described in the section "Layer 2 Security Policy" in the *ESX Server 3 Configuration Guide*. Setting this policy per port group allows you to have one or more privileged virtual machines on a port group that allows promiscuous mode, while other port groups on the same switch do not grant this privilege.

Protect against MAC Address Spoofing

Each virtual network adapter in a virtual machine has its own initial MAC address assigned when the adapter is created. 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.

When it is created, a network adapter's effective MAC address and initial MAC address are the same. However, 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 then receives network traffic destined for the new MAC address. The operating system can send frames with an impersonated source MAC address at any time. Thus, an operating system can stage malicious attacks on the devices in a network by impersonating a network adapter authorized by the receiving network. You can use virtual switch security profiles on ESX/ESXi hosts to protect against this type of attack by setting two options, which you should set for each virtual switch:

- **MAC address changes**—By default, this option is set to Accept, meaning that ESX/ESXi accepts requests to change the effective MAC address to a value other than the initial MAC address. The MAC Address Changes option setting affects traffic received by a virtual machine.

  To protect against MAC impersonation, you can set this option to Reject. If you do, ESX/ESXi does not honor requests to change the effective MAC address to anything other than the initial MAC address. Instead, the port that the virtual adapter used to send the request is disabled. As a result, 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 has not been honored.

- **Forged transmissions**—By default, this option is set to Accept, meaning ESX/ESXi does not compare source and effective MAC addresses. The Forged Transmits option setting affects traffic transmitted from a virtual machine.

  If you set this option to Reject, ESX/ESXi 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, ESX/ESXi drops the packet. The guest operating system does not detect that its virtual network adapter cannot send packets using the impersonated MAC address. ESX/ESXi intercepts any packets with impersonated addresses before they are delivered, and the guest operating system might assume that the packets have been dropped.

It is recommended that you set both of these options to Reject for maximal security.

You can also set these security policies on a per-port group basis, which lets you override the virtual switch setting for that particular port group. If you need to configure a different policy for a particular virtual machine—for example, if you have an intrusion detection virtual appliance that needs to monitor all traffic on a virtual switch—you can create a special port group for this (and only this) virtual appliance with the modified settings.

To learn how these options are configured, see the section "Layer 2 Security Policy" in the *ESX Server 3 Configuration Guide*.

Secure the ESX/ESXi Host Console

Even if you have locked down ESX/ESXi to protect it from attacks that arrive over the network, anyone with access to the console of the host might still cause problems. Although physical harm to the host cannot be prevented, it still might be possible, for example, to influence the host so that it behaves improperly, perhaps in a manner that is hard to detect.

For ESX 3.5, which runs a service console, one way to guard against this is to use grub passwords to prevent users from booting into single user mode or passing options to the kernel during boot. Unless the password is entered, the server boots only the kernel with the default options. For more information on grub passwords, see the *GNU Grub Manual* at http://www.gnu.org/software/grub/manual/html_node/index.html. This technique does not apply to ESXi 3.5, because there is no service console available at the console of the host.

Mask and Zone SAN Resources Appropriately

Zoning provides access control in a SAN topology. It defines which host bus adapters (HBAs) can connect to which SAN device service processors. When a SAN is configured using zoning, the devices outside a zone are not visible to the devices inside the zone. In addition, SAN traffic within each zone is isolated from the other zones. Within a complex SAN environment, SAN switches provide zoning, which defines and configures the necessary security and access rights for the entire SAN.

LUN masking is commonly used for permission management. LUN masking is also referred to as selective storage presentation, access control, and partitioning, depending on the vendor. LUN masking is performed at the storage processor or server level. It makes a LUN invisible when a target is scanned. The administrator configures the disk array so each server or group of servers can see only certain LUNs. Masking capabilities for each disk array are vendor specific, as are the tools for managing LUN masking.

You should use zoning and LUN masking to segregate SAN activity. For example, you manage zones defined for testing independently within the SAN so they do not interfere with activity in the production zones. Similarly, you could set up different zones for different departments. Zoning must take into account any host groups that have been set up on the SAN device.

Secure iSCSI Devices through Authentication

One means of securing iSCSI devices from unwanted intrusion is to require that the ESX/ESXi 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.

You have two choices when you set up authentication for iSCSI SANs on the ESX/ESXi host:

- **Challenge Handshake Authentication Protocol (CHAP)**—You can configure the iSCSI SAN to use CHAP authentication. ESX/ESXi supports one-way CHAP authentication for iSCSI. It does not support bidirectional CHAP. In one-way CHAP authentication, the target authenticates the initiator, but the initiator does not authenticate the target. The initiator has only one set of credentials, and all of the iSCSI targets use them. ESX/ESXi supports CHAP authentication at the HBA level only. It does not support per-target CHAP authentication, which enables you to configure different credentials for each target to achieve greater target refinement.

- **Disabled**—You can configure the iSCSI SAN to use no authentication. Communications between the initiator and target are 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 you create a dedicated network or VLAN to service all your iSCSI devices. Because the iSCSI facility is isolated from general network traffic, it is less vulnerable to exploit.

ESX/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.

For information on how to determine whether authentication is currently being performed and to configure the authentication method, see the chapter "Securing an ESX Server 3 Configuration" in the *ESX Server 3 Configuration Guide*.

VirtualCenter

VirtualCenter provides a powerful way to manage and control your VMware Infrastructure environment from a central point and enables more sophisticated operations through tools that work through its SDK. It is extremely powerful and therefore should be subject to the strictest security standards.

Set Up the Windows Host for VirtualCenter with Proper Security

Because VirtualCenter runs on a Windows host, it is especially critical to protect this host against vulnerabilities and attacks. The standard set of recommendations applies, as it would for any host: install antivirus agents, spyware filters, intrusion detection systems, and any other security measures. Make sure to keep all security measures up-to-date, including application of patches.

The password that VirtualCenter uses to access its database is stored in the Windows registry in an encoded format. Although the password cannot be read directly, it is not protected by encryption, so you should protect the registry on the VirtualCenter host to prevent unauthorized access to the VirtualCenter database.

In general, you should harden and lock down the VirtualCenter host according to industry standard configuration guides, such as the DISA STIG or CIS Benchmark.

Limit Administrative Access

VirtualCenter runs as a user that requires local administrator privileges and must be installed by a local administrative user. To limit the scope of administrative access, avoid using the Windows Administrator user to run VirtualCenter after you install it. Instead, use a dedicated VirtualCenter administrator account. To set up the administrative account, take the following steps:

1. Create a local account for an ordinary user on the Windows host. This is the account the VirtualCenter administrator should use to manage VirtualCenter.
2. In VirtualCenter, log on as the Windows Administrator, then grant VirtualCenter root administrator access to the newly created account
3. Log out of VirtualCenter, then make sure you can log in to VirtualCenter as the new user and that this user is able to perform all tasks available to a VirtualCenter administrator
4. Remove the permissions in VirtualCenter for the local Administrators group.

By configuring accounts in this way, you avoid automatically giving administrative access to domain administrators, who typically belong to the local Administrators group. This also provides a way of logging in to VirtualCenter when the domain controller is down, because the local VirtualCenter administrator account does not require remote authentication.

Limit Network Connectivity to VirtualCenter

The only network connection VirtualCenter requires is to the management network described in "Isolate Virtual Machine Networks" on page 3. You should avoid putting the VirtualCenter server on any other network, such as your production or storage network. Specifically, VirtualCenter does not need access to the network on which VMotion takes place. By limiting the network connectivity, you cut down on the possible avenues of attack.

Use the following guidelines to limit network connectivity:

- Firewalls

  You should protect the VirtualCenter server using a firewall. This firewall may sit between the clients and the VirtualCenter server, or both the VirtualCenter Server and the clients may sit behind the firewall, depending on your deployment. The main consideration is ensuring that a firewall is present at what you consider to be an entry point for the system as a whole.

  Use firewalls to restrict which systems can access VirtualCenter by IP address.

  For more information on the possible locations for firewalls used with VirtualCenter, see the section "Firewalls for Configurations with a VirtualCenter Server" in the *ESX Server 3 Configuration Guide*.

- TCP and UDP ports for management access

  Networks configured with a VirtualCenter server can receive communications from several types of clients: the VI Client, VI Web Access, a system with the Remote CLI or one of the VI Toolkits for scripting installed, or third-party network management clients that use the SDK to interact with the host. During normal operation, VirtualCenter listens on designated ports for data from the hosts it is managing and from clients. VirtualCenter also assumes that the hosts it is managing listen for data from VirtualCenter on designated ports. If a firewall is present between any of these components, you must ensure that the appropriate ports are open to support data transfer through the firewall.

  The section "TCP and UDP Ports for Management Access" in the *ESX Server 3 Configuration Guide* lists all the predetermined TCP and UDP ports used for management access to your VirtualCenter server, ESX hosts, and other network components. Study this section carefully to determine how to configure your firewalls to maintain maximum security while still allowing required management operations.

  NOTE You might not be able to open a VI Client remote console when your network is configured such that a firewall using NAT stands between the ESX host and the computer running VI Client. See VMware knowledge base article 749640 (http://kb.vmware.com/kb/749640) for a workaround for this issue.

Use Proper Security Measures when Configuring the Database for VirtualCenter

You should install the VirtualCenter database on a separate server or virtual machine and subject it to the same security measures as any production database. You should also carefully configure the permissions used for access to the database to the minimum necessary. Use the guidelines appropriate to your database.

- Microsoft SQL Server

  During installation and upgrade, the VirtualCenter account must have the DB Owner role. During normal operations, you may further restrict permissions to the following:

  - Invoke/execute stored procedures
  - Select, update, insert
  - Delete

- Oracle

  The privileges required for the VirtualCenter account are listed in the section "Preparing the VirtualCenter Server Database" of the chapter "Installing VMware Infrastructure Management" in the *ESX Server 3 Installation Guide*.

Enable Full and Secure Use of Certificate-based Encryption

For environments that require strong security, VMware recommends that administrators replace all default self-signed certificates generated at installation time with legitimate certificates signed by their local root certificate authority or public, third-party certificates available from multiple public certificate authorities. You should also enable server-certificate verification on all VI Client installations and the VirtualCenter host. This involves a modification to the Windows registry on all client hosts.

NOTE You need to replace the default VirtualCenter Server certificate before enabling server-certificate verification.

For background and information on replacing VirtualCenter Server certificates, see the technical note "Replacing VirtualCenter Server Certificates" (http://www.vmware.com/vmtn/resources/658). For information on enabling server-certificate verification for VI Client installations, including how to pre-trust certificates and how to modify the Windows registry for client hosts, see VMware knowledge base article 4646606 (http://kb.vmware.com/kb/4646606).

Use VirtualCenter Custom Roles

Beginning with version 2.0, VirtualCenter provides a sophisticated system of roles and permissions. These roles and permissions allow fine-grained determination of authorization for administrative and user tasks, based on user or group and inventory item, such as clusters, resource pools, and hosts. You should take advantage of this system to assure that only the minimum necessary privileges are assigned to people in order to prevent unauthorized access or modification. Some recommendations are:

- Create roles that enable only the necessary tasks. For example, a user who is only going to make use of an assigned virtual machine might need permission only to power the machine on or off, and not necessarily to attach a CD or floppy device.
- Assign roles to as limited a scope as necessary. For example, you can give a user certain permissions on a resource pool instead of a discrete host, and you can use folders to contain the scope of a privilege.

For more information on VirtualCenter roles, see the paper "Managing VirtualCenter Roles and Permissions" (http://www.vmware.com/resources/techresources/826).

Document and Monitor Changes to the Configuration

Although most of a VMware Infrastructure environment is defined by information contained in the VirtualCenter database, certain important configuration information resides only on the VirtualCenter Server host's local file system. This includes the main configuration file `vpxd.cfg`, various log files, and, implicitly, the Windows registry settings that pertain to VirtualCenter.

For compliance and auditing, it is important that you have a record of these configurations over time. One convenient way to capture everything in one place is to use the Generate VirtualCenter Server log bundle command, in the VMware program file menu on the VirtualCenter host. This tool is designed to capture information to be used for troubleshooting and debugging, but the resulting archive file serves as a convenient way to maintain a historical record.

The resulting ZIP archive includes files that contain the values of relevant Windows registry entries, configuration files for VirtualCenter and any add-on components, and log files for VirtualCenter, the license server, and any add-on components. By performing this task on a regular basis, you can keep track of all changes that affect your VirtualCenter installation.

If you want to monitor the log files directly, use Table 12 to determine which files to watch:

Table 12. Paths to Key VirtualCenter Log Files

Component	Default path to file
VirtualCenter	`C:\Documents and Settings\All Users\Application Data\VMware\VMware VirtualCenter\Logs\*`
Web server component of VirtualCenter	`C:\Program Files\VMware\Infrastructure\VirtualCenter Server\tomcat\logs\*`
License manager	`C:\WINDOWS\Temp\lmgrd.log`

VirtualCenter Add-on Components

Beginning with version 2.5, VirtualCenter includes a framework that enables you to add components to VirtualCenter to extend its functionality. These components typically run as separate services, which are installed on the VirtualCenter server or in some cases a on separate host or in a virtual machine. Three of these components are bundled with VirtualCenter:

- VMware Update Manager: manages and automates patch management and tracking of ESX hosts and virtual machines, including turned-off virtual machines and virtual machine templates
- VMware Converter Enterprise for VirtualCenter: provides an integrated solution for migrating both physical and virtual machines to VMware Infrastructure.
- VMware Guided Consolidation: automatically discovers physical servers, helps analyze their performance, and triggers the conversion of physical to virtual machines placed intelligently on a suitable host.

VMware Update Manager

You should consider VMware Update Manager an essential component of any VMware Infrastructure deployment. The ability to make sure that critical operating system patches are applied to all virtual machines, especially offline virtual machines and templates, addresses one of the most important aspects of security in a virtualized environment. Furthermore, the ability to automate the patching of ESX hosts greatly increases the likelihood that you are protected against any vulnerabilities that may be discovered for this platform.

In order to maintain isolation of the VirtualCenter host, it is recommended that you install VMware Update Manager on a separate host or in a virtual machine. This host needs to have access to the VirtualCenter using the VI API interface (available by default on TCP port 443). In the default installation, the host where you install VMware Update Manager also needs access to the Internet in order to download patches and patch information. You can configure it to use a Web proxy, a step you should take if a Web proxy is available. For highest security, you can install the Update Manager Download Service on a separate server, and the patches and information that it downloads can be transferred manually to the Update Manager host—for example, using a USB key or scheduled, secure file transfer. This avoids having the Update Manager host itself connected to an external network. For more information on installing Update Manager and the Update Manager Download Service, see the chapter "Working with Update Manager" in the *Update Manager Administration Guide*.

VMware Converter Enterprise

As with Update Manager, you should install Converter on a separate system in order to maintain isolation of the VirtualCenter host. Converter and the source system need access to VirtualCenter using the VI API interface (TCP port 443 by default) and the VI API interface of any destination ESX host. However, the information from the hard disk of the source system is transferred to the destination ESX host over port 902. In addition, the Converter server needs access to port 139 on the source system.

The use of Converter has the potential for introducing some security risks. When migrating physical or virtual machines to VMware Infrastructure, you run the risk of importing a compromised or infected server. Because the import occurs with little modification to the source, you could be introducing a vulnerability directly into your environment. You might want to consider using Converter only in test or staging environments.

VMware Guided Consolidation

Guided Consolidation automates the process of discovering and analyzing existing servers (virtual or physical) for suitability of conversion to virtual machines, and choosing the destination ESX host onto which to migrate them. It then automatically invokes Converter to perform the actual migration process.

Guided Consolidation is not an optional component, and you cannot install it on a separate host. It is always running as a service on the VirtualCenter Server host. Guided Consolidation requires access to the ports for WMI, Perfmon, and Remote Registry—ports 135, 137, 138, 139, and 445. These ports must be open on both the VirtualCenter host and the target server. The Guided Consolidation service must be run as a user with VirtualCenter Administrator privileges, as well as with the necessary Windows privileges to query Active Directory for servers in the environment. In addition, administrator credentials are required for each target system to be analyzed, so that performance data can be collected from them. You can enter a default set of target system credentials and override this default for individual target systems that might deviate from the default.

The Guided Consolidation service relies on Converter to import target server, so all recommendations for Converter apply to Guided Consolidation, as well. It is recommended that you not use Guided Consolidation in higher-security environments.

General Considerations

With any add-on component, observe the following:

- Harden and lock down the server on which the component is installed according to the industry best practices for the host's operating system.
- These components often require you to provide credentials of a user account with full VMware Infrastructure administrator privileges. To reduce exposure and have a way of restricting access in case a problem is found, create a unique account for each component. Then, if a vulnerability or other problem is discovered, you can reduce or eliminate privileges on that account until the situation is resolved. Do not provide the credentials of the VirtualCenter host's Administrator account or of an actual user.
- These components usually have their own log files. Table 13 shows the log files for the components that are bundled with VirtualCenter:

Table 13. Paths to Log Files for Bundled VirtualCenter Components

Component	Default path to file
VMware Update Manager	`C:\Documents and Settings\All Users\Application Data\VMware\VMware Update Manager\Logs\*`
VMware Enterprise Converter	`C:\Documents and Settings\All Users\Application Data\VMware\VMware Converter Enterprise\Logs\*`
VMware Guided Consolidation	`C:\Documents and Settings\All Users\Application Data\VMware\VMware Capacity Planner\Logs\*`

Client Components

The recommendations in this section apply to clients that connect to VirtualCenter or ESX.

Restrict the use of Linux-based Clients

Although SSL-based encryption is used to protected communication between client components and VirtualCenter or ESX, the Linux versions of these components do not perform certificate validation. Therefore, even if you have replaced the self-signed certificates on VirtualCenter and ESX with legitimate certificates signed by your local root certificate authority or a third party, communications with Linux clients are still vulnerable to man-in-the-middle attacks. The components that are vulnerable when running on Linux include:

- Any Remote CLI command
- Any VI Perl Toolkit script

- Virtual machine console access initiated from a Linux-based Web Access browser session
- Any program written using the VI SDK

The management interfaces of VirtualCenter and ESX should be available only on trusted networks, but providing encryption and certificate validation add extra layers of defense against an attack. If you are able to mitigate against systems on the management network interposing themselves on network traffic, or can trust that such systems will not appear on the network, the use of Linux-based clients would not increase the security risk.

Verify the Integrity of VI Client

Beginning with version 2.5, VirtualCenter includes a VI Client extensibility framework, which provides the ability to extend the VMware Infrastructure Client (VI Client) with menu selections or toolbar icons that provide access to VirtualCenter add-on components or external, Web-based functionality. With the flexibility, customization, and innovation that this entails, there is also the risk of introducing VI Client capabilities that were not intended. For example, a plug-in could be surreptitiously installed on an administrator's VI Client instance, then execute arbitrary commands with the privilege level of that administrator. If a user with low or no privileges were to use such a client, there would be no added risk, because the plug-in can interact with VirtualCenter or ESX only with the permissions of the user running the client.

The integrity of client software is a common concern across all client-server platforms in which the client could be running on an insecure host, but the VI Client extensibility framework reduces the effort needed to compromise the client software. To protect against such compromises, users of VI Client, especially those with powerful privileges, should not install any plug-ins that do not come from a trusted source. You can check to see which plug-ins are actually installed for a given VI Client by going to the menu item **Plugins** > **Manage Plugins** and clicking the **Installed Plugins** tab.

Monitor the Usage of VI Client Instances

Although actions performed within VI Client are logged in the VirtualCenter Events table, in some cases you might be interested in knowing what occurred on the client side. For example, you might want to know the server to which the client had recently connected and which user account was used. VI Client maintains log files of its activities on the client system, and you can retrieve and inspect or even monitor them regularly for specific events. The log files are located in various directories found under the folder `C:\Documents and Settings\<username>\Local Settings\Application Data\VMware`. Because the VI Client plug-in framework allows for communication with various components, each could potentially have its own set of logs. For example, the directory `vpx` contains logs for interaction with VirtualCenter, and the directory `VMware Converter Enterprise\Logs` contains logs for interaction with the Converter Enterprise server.

Avoid the Use of Plain-Text Passwords

A number of scripting frameworks can be used to configure and monitor your VMware Infrastructure 3 deployment. In particular, the VI Perl Toolkit and the Remote CLI let you run commands and scripts from a remote system to modify VMware Infrastructure 3 configurations, perform actions such as taking snapshots of virtual machines or rebooting an ESX host, and monitor performance and other data.

The Remote CLI is implemented as a series of commands written using the VI Perl Toolkit. Both Remote CLI commands and VI Perl Toolkit scripts need valid credentials in the form of user name and password to work successfully. These credentials must be accepted on either the VirtualCenter host or the ESX host, depending on where the command is directed. Not only does the user need to be authenticated, but the user must also have sufficient privileges to execute the specific command or task.

Both of these frameworks allow you to specify passwords in plain text—as command-line options, in a configuration file, or as environment variables. However, use of plain-text passwords presents a security risk, because someone could read passwords in the configuration file itself, in shell history files, in backup files, or in other ways. When running commands and scripts interactively, it is recommended that you avoid specifying the password ahead of time. The commands typically prompt you for the password, which is then not echoed to the screen when you type it. If you use this approach, you avoid having the password exist on the file system in plain text.

If you need to run commands noninteractively—for example, in scripts—you should use session files. This mechanism allows you to provide your credentials once interactively. The system then generates a file that contains an authentication token. This token does not contain any password information, and it remains valid for up to 30 minutes. The session file may be used in lieu of credentials to authenticate commands. A script that references the session file can then run noninteractively.

Because the session file authenticates any command that references it, it is important that this file itself be closely guarded during its lifetime. It should be generated only as needed, then deleted as soon as it is no longer needed. Make sure not to inadvertently allow access to this file by other users.

For more information on the use of session files, see the section "Using Remote Command Line Interfaces" in the appendix of the *ESX Server 3i Configuration Guide*.

References

- "Accessing VMware ESX Server 3 securely using SSH and SUDO"
  http://www.xtravirt.com/index.php?option=com_remository&Itemid=75&func=startdown&id=10
- *Basic System Administration*
  http://www.vmware.com/pdf/vi3_35/esx_3/r35/vi3_35_25_admin_guide.pdf
- "Enabling Active Directory Authentication with ESX Server"
  http://www.vmware.com/vmtn/resources/582
- "Enabling Server-Certificate Verification for Virtual Infrastructure Clients"
  http://kb.vmware.com/kb/4646606
- *ESX Server 3 Configuration Guide*
  http://www.vmware.com/pdf/vi3_35/esx_3/r35/vi3_35_25_3_server_config.pdf
- *ESX Server 3i Configuration Guide*
  http://www.vmware.com/pdf/vi3_35/esx_3i_e/r35/vi3_35_25_3i_server_config.pdf
- *ESX Server 3 Installation Guide*
  http://www.vmware.com/pdf/vi3_35/esx_3/r35/vi3_35_25_installation_guide.pdf
- *ESX Server 3i Embedded Setup Guide*
  http://www.vmware.com/pdf/vi3_35/esx_3i_e/r35/vi3_35_25_3i_setup.pdf
- *ESX Server 3i Installable Setup Guide*
  http://www.vmware.com/pdf/vi3_35/esx_3i_i/r35/vi3_35_25_3i_i_setup.pdf
- *GNU Grub Manual*
  http://www.gnu.org/software/grub/manual/html_node/index.html
- "Installing and Configuring NTP on VMware ESX Server"
  http://kb.vmware.com/kb/1339
- "Red Hat Linux Security Guide, Chapter 4. Workstation Security"
  http://www.redhat.com/docs/manuals/linux/RHL-9-Manual/security-guide/ch-wstation.html
- "Replacing VirtualCenter Certificates"
  http://www.vmware.com/vmtn/resources/658
- Sudo Main Page
  http://www.gratisoft.us/sudo
- "Virtual Infrastructure client cannot open Remote Console session"
  http://kb.vmware.com/kb/749640
- "VMware ESX Server: Third-Party Software in the Service Console"
  http://www.vmware.com/vmtn/resources/516
- VMware Security Center
  http://www.vmware.com/security

About the Author

Charu Chaubal is a senior architect in the technical marketing department at VMware. His areas of expertise include virtualization security and virtual infrastructure management. Chaubal received a Bachelor of Science in Engineering from the University of Pennsylvania and a Ph.D. from the University of California at Santa Barbara, where he studied the numerical modeling of complex fluids. Previously, he worked at Sun Microsystems, where he had more than seven years experience with designing and developing distributed resource management and grid infrastructure software solutions. He is the author of numerous publications and several patents in the fields of datacenter automation and numerical price optimization.

Acknowledgements

The author would like to thank Brad Harris, Kirk Larsen, Rob Randell, Brian Cosker-Swerkske, and Petr Vandrovec for their valuable contributions.

If you have comments about this documentation, submit your feedback to: docfeedback@vmware.com

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

Revision 20080708 Item: BP-012-PRD-02-01