the CENTER for
INTERNET SECURITY

VMware ESX Server 3.x Benchmark

Version 1.0

October 2007

http://cisecurity.org
cis-feedback@cisecurity.org

Editor: Joel Kirch
WBB Consulting

1 TERMS OF USE AGREEMENT

August 2006

TERMS OF USE AGREEMENT

Background.

The Center for Internet Security ("**CIS**") provides benchmarks, scoring tools, software, data, information, suggestions, ideas, and other services and materials from the CIS website or elsewhere ("**Products**") as a public service to Internet users worldwide. Recommendations contained in the Products ("**Recommendations**") result from a consensus-building process that involves many security experts and are generally generic in nature. The Recommendations are intended to provide helpful information to organizations attempting to evaluate or improve the security of their networks, systems, and devices. Proper use of the Recommendations requires careful analysis and adaptation to specific user requirements. The Recommendations are not in any way intended to be a "quick fix" for anyone's information security needs.

No Representations, Warranties, or Covenants.

CIS makes no representations, warranties, or covenants whatsoever as to (i) the positive or negative effect of the Products or the Recommendations on the operation or the security of any particular network, computer system, network device, software, hardware, or any component of any of the foregoing or (ii) the accuracy, reliability, timeliness, or completeness of the Products or the Recommendations. CIS is providing the Products and the Recommendations "as is" and "as available" without representations, warranties, or covenants of any kind.

User Agreements.

By using the Products and/or the Recommendations, I and/or my organization ("**We**") agree and acknowledge that:

1. No network, system, device, hardware, software, or component can be made fully secure;

2. We are using the Products and the Recommendations solely at our own risk;

3. We are not compensating CIS to assume any liabilities associated with our use of the Products or the Recommendations, even risks that result from CIS's negligence or failure to perform;

4. We have the sole responsibility to evaluate the risks and benefits of the Products and Recommendations to us and to adapt the Products and the Recommendations to our particular circumstances and requirements;

5. Neither CIS, nor any CIS Party (defined below) has any responsibility to make any corrections, updates, upgrades, or bug fixes; or to notify us of the need for any such corrections, updates, upgrades, or bug fixes; and

6. Neither CIS nor any CIS Party has or will have any liability to us whatsoever (whether based in contract, tort, strict liability or otherwise) for any direct, indirect, incidental, consequential, or special damages (including without limitation loss of profits, loss of sales, loss of or damage to reputation, loss of customers, loss of software, data, information or emails, loss of privacy, loss of use of any computer or other equipment, business interruption, wasted management or other staff resources or claims of any kind against us from third parties) arising out of or in any way connected with our use of or our inability to use any of the Products or Recommendations (even if CIS has been advised of the possibility of such damages), including without limitation any liability associated with infringement of intellectual property, defects, bugs, errors, omissions, viruses, worms, backdoors, Trojan horses or other harmful items.

Grant of Limited Rights.

CIS hereby grants each user the following rights, but only so long as the user complies with all of the terms of these Agreed Terms of Use:

1. Except to the extent that we may have received additional authorization pursuant to a written agreement with CIS, each user may download, install and use each of the Products on a single computer;

2. Each user may print one or more copies of any Product or any component of a Product that is in a .txt, .pdf, .doc, .mcw, or .rtf format, provided that all such copies are printed in full and are kept intact, including without limitation the text of this Agreed Terms of Use in its entirety.

Retention of Intellectual Property Rights; Limitations on Distribution.

The Products are protected by copyright and other intellectual property laws and by international treaties. We acknowledge and agree that we are not acquiring title to any intellectual property rights in the Products and that full title and all ownership rights to the Products will remain the exclusive property of CIS or CIS Parties. CIS reserves all rights not expressly granted to users in the preceding section entitled "Grant of limited rights."

Subject to the paragraph entitled "Special Rules" (which includes a waiver, granted to some classes of CIS Members, of certain limitations in this paragraph), and except as we may have otherwise agreed in a written agreement with CIS, we agree that we will not (i) decompile, disassemble, reverse engineer, or otherwise attempt to derive the source code for any software Product that is not already in the form of source code; (ii) distribute, redistribute, encumber, sell, rent, lease, lend, sublicense, or otherwise transfer or exploit rights to any Product or any component of a Product; (iii) post any Product or any component of a Product on any website, bulletin board, ftp server, newsgroup, or other similar mechanism or device, without regard to whether such mechanism or device is internal or external, (iv) remove or alter trademark, logo, copyright or other proprietary notices, legends, symbols or labels in any Product or any component of a Product; (v) remove these Agreed Terms of Use from, or alter these Agreed Terms of Use as they appear in, any Product or any component of a Product; (vi) use any Product or any component of a Product with any derivative works based directly on a Product or any component of a Product; (vii) use any Product or any component of a Product with other products or applications that are directly and specifically dependent on such Product or any component for any part of their functionality, or (viii) represent or claim a particular level of compliance with a CIS Benchmark, scoring tool or other Product. We will not facilitate or otherwise aid other individuals or entities in any of the activities listed in this paragraph.

We hereby agree to indemnify, defend, and hold CIS and all of its officers, directors, members, contributors, employees, authors, developers, agents, affiliates, licensors, information and service providers, software suppliers, hardware suppliers, and all other persons who aided CIS in the creation, development, or maintenance of the Products or Recommendations ("**CIS Parties**") harmless from and against any and all liability, losses, costs, and expenses (including attorneys' fees and court costs) incurred by CIS or any CIS Party in connection with any claim arising out of any violation by us of the preceding paragraph, including without limitation CIS's right, at our expense, to assume the exclusive defense and control of any matter subject to this indemnification, and in such case, we agree to cooperate with CIS in its defense of such claim. We further agree that all CIS Parties are third-party beneficiaries of our undertakings in these Agreed Terms of Use.

Special Rules.

The distribution of the NSA Security Recommendations is subject to the terms of the NSA Legal Notice and the terms contained in the NSA Security Recommendations themselves (http://nsa2.www.conxion.com/cisco/notice.htm).

CIS has created and will from time to time create, special rules for its members and for other persons and organizations with which CIS has a written contractual relationship. Those special rules will override and supersede these Agreed Terms of Use with respect to the users who are covered by the special rules.

CIS hereby grants each CIS Security Consulting or Software Vendor Member and each CIS Organizational User Member, but only so long as such Member remains in good standing with CIS and complies with all of the terms of these Agreed Terms of Use, the right to distribute the Products and Recommendations within such Member's own organization, whether by manual or electronic means. Each such Member acknowledges and agrees that the foregoing grant is subject to the terms of such Member's membership arrangement with CIS and may, therefore, be modified or terminated by CIS at any time.

Choice of Law; Jurisdiction; Venue

We acknowledge and agree that these Agreed Terms of Use will be governed by and construed in accordance with the laws of the State of Maryland, that any action at law or in equity arising out of or relating to these Agreed Terms of Use shall be filed only in the courts located in the State of Maryland, that we hereby consent and submit to the personal jurisdiction of such courts for the purposes of litigating any such action. If any of these Agreed Terms of Use shall be determined to be unlawful, void, or for any reason unenforceable, then such terms shall be deemed severable and shall not affect the validity and enforceability of any remaining provisions.

Terms of Use Agreement Version 2.1 – 02/20/04

Table of Contents

2 Introduction

This document addresses the security aspects of virtual machine technologies and VMware ESX Server 3.x implementations. While these topics cannot be completely separated from the standard security issues of operating a physical computer or basic issues of running the individual operating systems involved, this document's primary focus is on virtual machine security issues. For this reason, we do not cover all of the steps needed to harden the guest operating systems. The Center for Internet Security has multiple documents, which address guest operating system security recommendations. Recommendations are based on a variety of public sources and input from members of the Center for Internet Security (CIS).

2.1 CIS Virtual Machine Security Guidelines

General information about virtual machines and the security concerns associated with them can be found in the CIS Virtual Machine Security Guidelines. This whitepaper addresses security concerns that apply generally to VM technologies. The recommendations contained within it are vendor neutral and should apply to most virtualization deployments. Recommendations are based on a variety of public sources and input from members of the Center for Internet Security.

For further reading see:

http://www.cisecurity.com/bench_vm.html

2.2 Audience

This document is intended for system administrators, but should be read by anyone responsible for installing and/or configuring Virtual Machines. In the context of this document, a system administrator is defined as someone who can create and manage accounts and groups, understands how operating systems perform access control, understands how to set account policies and user rights, is familiar with auditing and read audit logs, and can configure other similar system-related functionality.

2.3 Service Console Operating System*

Whenever possible, the recommendations for hardening the Service Console (sometimes called the "COS" for Console OS) are noted with an asterisk (*) at the end of the title to make them appear distinct from those that pertain to hardening the hypervisor layer and ensuring VM isolation.

2.4 Data Isolation

One of the key issues that separates virtual computing from physical computing is the issue of data isolation. The ability of a virtual machine to isolate data from the other guests is a key factor in determining the deployment and implementation in an environment.

John Scott Robin and Cynthia E. Irvine wrote a white paper in 2000 titled, “Analysis of the Intel Pentium's Ability to Support a Secure Virtual Machine Monitor.” In this paper they concluded the following:

"After defining a strategy to “virtualize” the Pentium architecture, an analysis was conducted to determine whether a Pentium-based secure virtual machine monitor is able to securely isolate classified from unclassified virtual machines could be built. We conclude that current VMM products for the Intel architecture should not be used as a secure virtual machine monitor." - http://www.cs.nps.navy.mil/people/faculty/irvine/publications/2000/VMM-usenix00-0611.pdf

In contrast, recent papers reviewing more current hardware support the ability of modern processors to provide appropriate isolation. It is imperative that the underlying processor be known when making decisions about multi-classification VM guests created on a single host system. A security best practice is to take the position of treating the virtual machine platform with strongest security controls needed to protect the most sensitive data in the guest operating systems, regardless of the hardware architecture (Intel, AMD, Bochs, etc) or virtualization technology.

This document will address data isolation in terms of protecting data of the same classification on a particular host. Protecting dissimilar classifications on a single host may be done using appropriately certified hardware and operating systems, but is outside the scope of this benchmark document.

For further reading see:

- www.intel.com/technology/magazine/computing/intel-virtualization-0405.pdf
- http://www.amd.com/us-en/assets/content_type/white_papers_and_tech_docs/41632A_Virtualization_WP.pdf
- http://www.cs.nps.navy.mil/people/faculty/irvine/publications/2000/VMM-usenix00-0611.pdf
- http://web.mit.edu/Saltzer/www/publications/protection/
- http://research.microsoft.com/~yuqunc/papers/ngscb.pdf

2.5 VM Escape

Virtual Machines allow us to share the resources of the host computer and provide isolation between VMs and their host. In an ideal world, a program running inside a virtual machine would not be able to monitor, affect or communicate with another program on the host or another VM. Unfortunately, this can happen, due to architectural limitations, the VM vendor’s approach to isolation, or bugs in the VM technology.

In the worst case, a program running inside a virtual machine would be able to completely bypass the VM layer, getting full access to the host system. The term for this is "VM escape". Because of the host's privileged position in controlling the other VMs, this is a complete breakdown in the security model of the system. This problem may be compounded significantly by unfettered file sharing between host and guest operating systems.

There have been demonstrations of this technique shown for under-patched versions of VMware Workstation. While we are not aware of similar demonstrations for ESX Server at the time of this release, it is not inconceivable that an escape could be created. For this reason, when a virtual machine environment is established, one should consider setting up additional security layers to handle the possibility that a rogue application in a virtual machine could start execution on the host.

3 Preconditions

This section details the steps that should be taken before attempting to harden the ESX Server.

The commands provided in this document are bash shell commands. All should run without modification on a standard VMware VI3/ESX system. There are a few suggestions about their use.

If two or more lines to are shown in the action area to run, we encourage you to run them from a shell script file rather than pasting them directly in an ssh session or terminal to the shell. There can be line wrapping, line termination, and quoting issues with the latter. To make a shell script, do the following:

- Create a file with your favorite editor, such as:

  ```
  vi /root/myscript.sh
  ```

- Put this as the first line in the file:

  ```
  #!/bin/bash
  ```

- Paste the commands you wish to run from the benchmark into the file.

- If any of the lines end in a "\", make sure that's the last character on the line. The line feed must immediately follow it, with no trailing spaces or tabs.

- Once you've saved the script, make it executable with:

  ```
  chmod 700 /root/myscript.sh
  ```

Note:

If you're pasting from Windows or a Macintosh, make sure the final file has the Unix style of line break; a single LF (Line Feed, ascii 0x10). Files edited on Windows will commonly have a CR (Carriage Return, 0x13) followed by LF. This causes odd errors including shell scripts that can't be run; the typical "Command not found" error comes because it appears you've asked for a shell of "`/bin/bash^M`", not "`/bin/bash`".

If you suspect this is happening, edit the file with `vi`; lines that have the Windows CR/LF linefeeds will appear to have a Ctrl-M at the end:

```
#!/bin/bash^M
cd /etc^M
etc...
```

Remove the ^M's by deleting this last byte from each line. This will leave just the LF linefeed.

3.1 Validate the System Before Making Changes

Ensuring your system is functioning properly before you make a change is a prudent system administration best practice and will save hours of aggravation. Applying this Benchmark to a system that may have operational issues increases the complexity of troubleshooting and may lead to undesirable results when implementing this benchmark.

Examine the system and application logs `(/var/log`). Key words to look for include, but are not limited to: `error`, `warning`, `critical`, and `alert`.

Resolve all issues before continuing.

3.2 Backup Configuration Files

Before making any changes to a configuration file in this benchmark, you should backup and protect (`chmod 600 filename`) the file. When backing up files manually, we recommend adopting a naming convention such as, `filename.orig.` A backup script has also been provided in Appendix A.

WARNING:

It is strongly recommended that administrators make backup copies of critical configuration files that may be modified by various benchmark items before performing the steps of this benchmark.

If this step is not performed, then the system administrator may have no reasonable back-out strategy for reversing system modifications made as a result of this document. The script provided in Appendix B of this document will automatically back up all files that may be modified by the actions below. Assuming the administrator is in the directory where the script resides, the command to execute the backup script is:

```
./do-backup.sh
```

One of the byproducts of the do-backup.sh script is `/root/do-restore.sh`, which is dynamically generated based on the results of the `do-backup.sh` script. To roll back the changes performed by this benchmark, execute the `do-restore.sh` script, and all changes will be backed out. Since not all ESX Server installations will be identical, the `do-restore.sh` script is created based on the files that actually existed at the time do-backup.sh was run.

Note:

If you make any changes manually to any of the files that were preserved by do-`backup.sh`, those changes will be lost when `do-restore.sh` is executed. It may be prudent to delete the `do-restore.sh` script once you have validated the changes to prevent inadvertently undoing the changes.

3.3 Keep Systems Patched

It is critical that an organization develop a formal process for keeping up-to-date with applicable vendor patches. VMware uses three categories for patches: Security, Critical, and General. The patch # refers to KB (knowledge base) article number that goes into more detail. VMware will (usually) issue a KB article when they become aware of security vulnerabilities and other serious functionality issues before they issue a patch. However, it is up to the organization to actually download and install these patches. Patches should typically be evaluated in a test environment, before being implemented into a QA/Production environment.

Only VMware released patches and tools (such as `esxupdate`) should be implemented. Do not use RedHat or third party patches or tools such as `yum` or `rpm` to update the system because VMware has made modifications to the system and kernel.

VMware patches can be downloaded here:
http://www.vmware.com/download/vi/vi3_patches.html

See section "Security Patches and Security Vulnerability Scanning Software" at www.vmware.com/pdf/vi3_server_config.pdf

See "Patch Management for ESX Server 3" at http://www.vmware.com/pdf/esx3_esxupdate.pdf

See "VI 3 Upgrade & Patching" at http://www.vmware-tsx.com/download.php?asset_id=54

"A script to fully automate the ESX patching process" at
http://vmprofessional.com/index.php?content=esx-autopatch

3.4 Establish a BIOS Password

Before installing ESX Server, an organization may choose to establish a strong BIOS password. Establishing a strong BIOS password can reduce the exposure of a system compromise via physical access.

Be aware that establishing a BIOS password can have a potentially negative effect of limiting the ability to remotely reboot the server.

3.5 Configure BIOS Boot Devices

An additional countermeasure to mitigate the threat of a physical attack is configuring the BIOS boot sequence. This can be accomplished by disabling the server's ability to boot off all non-hard disk devices, including floppy, CD-ROM, and USB.

3.6 SSH

The settings in this section attempt to ensure safe defaults for both the client and the server. Specifically, both the ssh client and the sshd server are configured to use only SSHv2 protocol, as significant security vulnerabilities have been found with the SSHv1 protocol. Disabling support for SSHv1 may cause compatibility issues at sites still using the vulnerable SSHv1 protocol. These sites should endeavor to configure all systems to use only SSHv2 protocol.

Note:

A banner is added in the `sshd_config` file (this banner will be created later and is discussed in detail in section 12). If you choose not to implement a banner, you will have to remove the reference to `/etc/issue` from `sshd_config` manually. Please read the section on the legal use of banners before deciding to remove it.

Action:

Configure `ssh_config`

```
unalias cp rm mv
cd /etc/ssh
cp ssh_config ssh_config.tmp
awk '/^#? *Protocol/ { print "Protocol 2"; next };
    { print }' ssh_config.tmp > ssh_config
if [ "`egrep -l ^Protocol ssh_config`" == "" ]; then
    echo 'Protocol 2' >> ssh_config
fi
rm ssh_config.tmp
diff ssh_config-preCIS ssh_config
```

Configure `sshd_config`

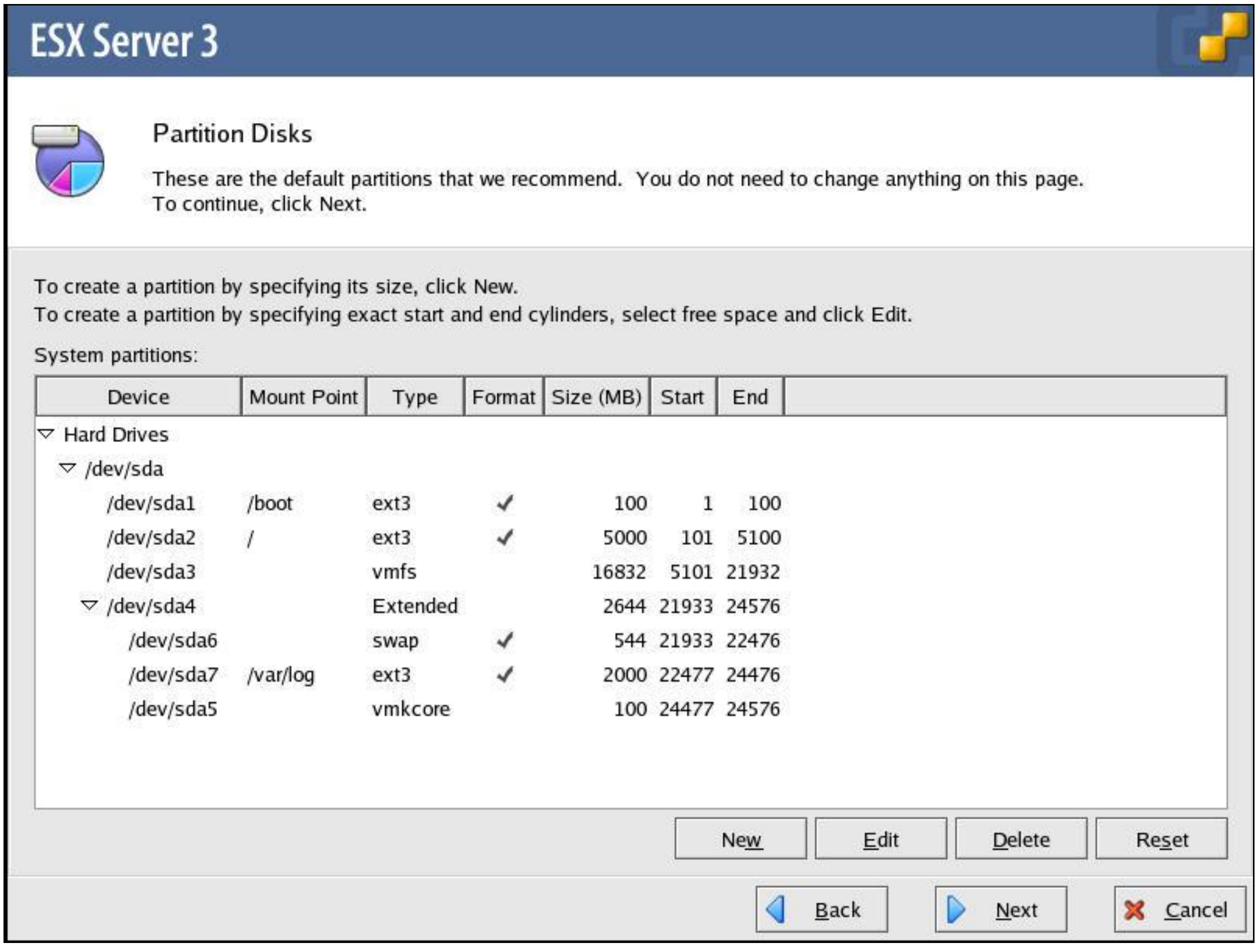
```
cp sshd_config sshd_config.tmp
awk '/^#? *Protocol/ { print "Protocol 2"; next };
    /^#? *X11Forwarding/ \
        { print "X11Forwarding yes"; next };
    /^#? *IgnoreRhosts/ \
        { print "IgnoreRhosts yes"; next };
    /^#? *RhostsAuthentication/ \
        { print " RhostsAuthentication no"; next };
    /^#? *RhostsRSAAuthentication/ \
        { print "RhostsRSAAuthentication no"; next };
    /^#? *HostbasedAuthentication/ \
        { print "HostbasedAuthentication no"; next };
    /^#? *PermitRootLogin/ \
        { print "PermitRootLogin no"; next };
    /^#? *PermitEmptyPasswords/ \
        { print "PermitEmptyPasswords no"; next };
    /^#? *Banner/ \
        { print "Banner /etc/issue.net"; next };
    {print}' sshd_config.tmp > sshd_config
rm sshd_config.tmp
diff sshd_config-preCIS sshd_config
```

4 Installation Considerations

This section addresses concerns that should be addressed prior to, or during installation.

4.1.1 Protect against the Root File System Filling Up

During installation, use the recommended disk partitioning scheme. If you need to manually partition the disk, create separate partitions for `/`, `/home`, `/tmp`, and `/var/log` (or `/var`). If these partitions fill up, they can cause a denial of service type scenario.



Partition Disks

These are the default partitions that we recommend. You do not need to change anything on this page. To continue, click Next.

To create a partition by specifying its size, click New.
To create a partition by specifying exact start and end cylinders, select free space and click Edit.

System partitions:

Device	Mount Point	Type	Format	Size (MB)	Start	End
▽ Hard Drives						
▽ /dev/sda						
/dev/sda1	/boot	ext3	✓	100	1	100
/dev/sda2	/	ext3	✓	5000	101	5100
/dev/sda3		vmfs		16832	5101	21932
▽ /dev/sda4		Extended		2644	21933	24576
/dev/sda6		swap	✓	544	21933	22476
/dev/sda7	/var/log	ext3	✓	2000	22477	24476
/dev/sda5		vmkcore		100	24477	24576

Figure 4-1 Disk Partitioning

Additional guidance can be found in Appendix B of the "Installation and Upgrade Guide." http://www.vmware.com/pdf/vi3_installation_guide.pdf

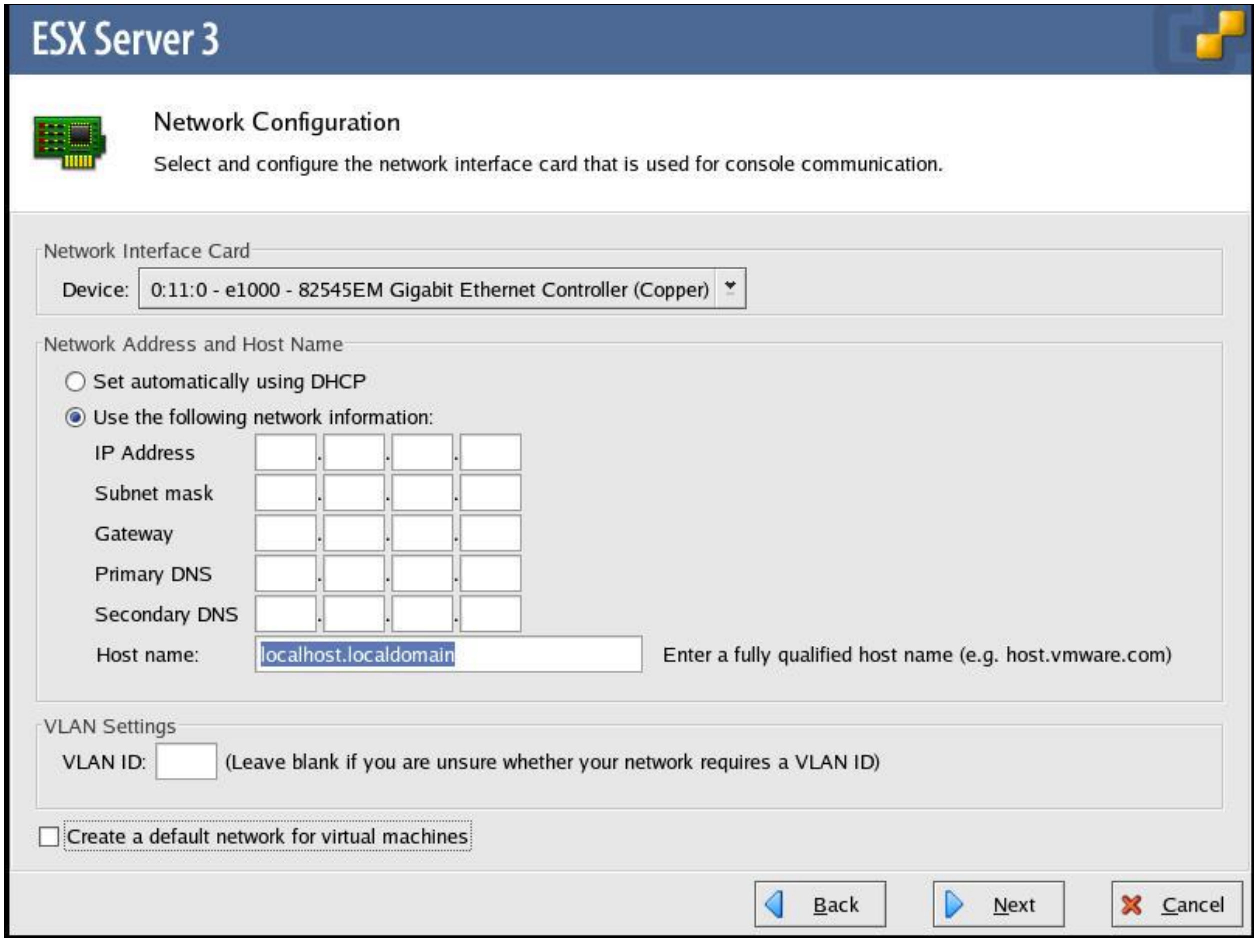
4.1.2 Do Not Create a Default Network for Virtual Machines During Installation

Action:

Ensure that when configuring the network elements during the installation of ESX that the checkbox titled "Create a default network for virtual machines" is not selected. It is selected by default.

Discussion:

During the installation of ESX, there is an option to create a default network for virtual machines. If this setting is left at its default setting, it could potentially allow network-based access to sensitive information because virtual machines will share the same network interface as the service console which is not a secure solution. Since the service console should always be isolated on a separate, private network, this option should not be used in production environments.



ESX Server 3

Network Configuration

Select and configure the network interface card that is used for console communication.

Network Interface Card

Device: 0:11:0 - e1000 - 82545EM Gigabit Ethernet Controller (Copper)

Network Address and Host Name

○ Set automatically using DHCP

● Use the following network information:

IP Address . . .

Subnet mask . . .

Gateway . . .

Primary DNS . . .

Secondary DNS . . .

Host name: localhost.localdomain   Enter a fully qualified host name (e.g. host.vmware.com)

VLAN Settings

VLAN ID: (Leave blank if you are unsure whether your network requires a VLAN ID)

□ Create a default network for virtual machines

Figure 4-2 Network Configuration

Review section 6.3 Configure a Dedicated Physical Network Interface or VLAN to Isolate the Management Network.

4.1.3 Configure the Service Console Firewall for High Security

Action:

Ensure that the service console firewall is properly configured to limit network access and protect the service console from unauthorized access.

Discussion:

ESX Server includes a built-in firewall feature that protects the service console that is enabled by default. Management of this firewall functionality is performed via the command line using the `esxcfg-firewall` command and on a limited basis via the VI GUI client.

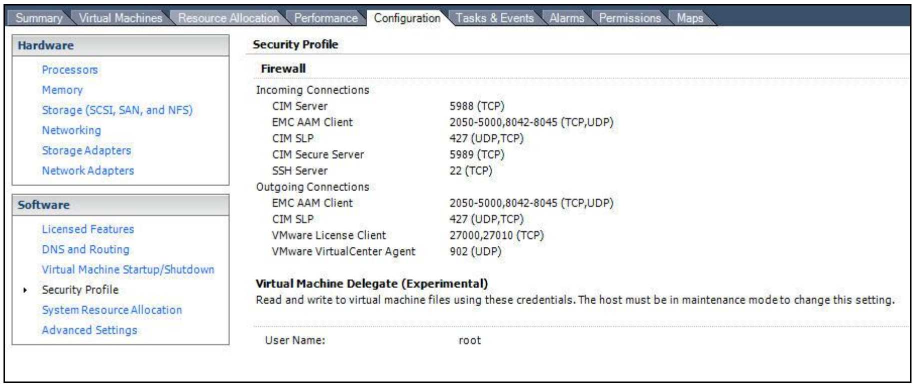
The service console firewall is configured by default to block all incoming and outgoing traffic except for those ports summarized in the table below.

Unless required, the default firewall settings should be utilized to restrict access to the service console. Please note, however, that the settings displayed using the VI client in the *Configuration* -> *Security Profile* (figure 4.3 below) as well as the *Configuration* -> *Security Profile* -> *Firewall* -> *Properties* section (figure 4.4 below) do not represent all of the ports open and available at the network layer via the service console connection or those ports in use and open by the Service Console OS that are available via localhost access only.

Please see section 7 for more information.

Because the ports open by default are limited, it is not uncommon to require communication via additional ports after installation for third party applications such as management, storage, authentication, NTP and backup tools, for example. Furthermore, you may be required to open additional ports in an external firewall in order to allow connectivity to the service console from clients and other management tools.

If you modify the service console firewall configuration, it is a recommended best practice to document any change, including the change agent, purpose of the change, and expected duration access is required. Including any change control tracking annotation is also suggested.



Security Profile

Firewall

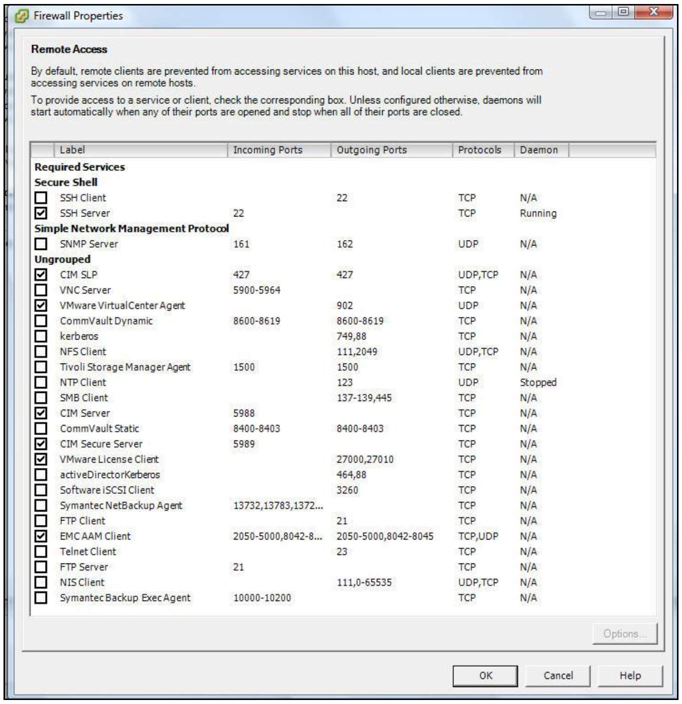
Incoming Connections	
CIM Server	5988 (TCP)
EMC AAM Client	2050-5000,8042-8045 (TCP,UDP)
CIM SLP	427 (UDP,TCP)
CIM Secure Server	5989 (TCP)
SSH Server	22 (TCP)
Outgoing Connections	
EMC AAM Client	2050-5000,8042-8045 (TCP,UDP)
CIM SLP	427 (UDP,TCP)
VMware License Client	27000,27010 (TCP)
VMware VirtualCenter Agent	902 (UDP)

Virtual Machine Delegate (Experimental)

Read and write to virtual machine files using these credentials. The host must be in maintenance mode to change this setting.

User Name: root

Figure 4-3 Security Profile for the Service Console Firewall



Remote Access

By default, remote clients are prevented from accessing services on this host, and local clients are prevented from accessing services on remote hosts.

To provide access to a service or client, check the corresponding box. Unless configured otherwise, daemons will start automatically when any of their ports are opened and stop when all of their ports are closed.

	Label	Incoming Ports	Outgoing Ports	Protocols	Daemon
Required Services					
Secure Shell					
□	SSH Client		22	TCP	N/A
☑	SSH Server	22		TCP	Running
Simple Network Management Protocol					
□	SNMP Server	161	162	UDP	N/A
Ungrouped					
☑	CIM SLP	427	427	UDP,TCP	N/A
□	VNC Server	5900-5964		TCP	N/A
☑	VMware VirtualCenter Agent		902	UDP	N/A
□	CommVault Dynamic	8600-8619	8600-8619	TCP	N/A
□	kerberos		749,88	TCP	N/A
□	NFS Client		111,2049	UDP,TCP	N/A
□	Tivoli Storage Manager Agent	1500	1500	TCP	N/A
□	NTP Client		123	UDP	Stopped
□	SMB Client		137-139,445	TCP	N/A
☑	CIM Server	5988		TCP	N/A
□	CommVault Static	8400-8403	8400-8403	TCP	N/A
☑	CIM Secure Server	5989		TCP	N/A
☑	VMware License Client		27000,27010	TCP	N/A
□	activeDirectorKerberos		464,88	TCP	N/A
□	Software iSCSI Client		3260	TCP	N/A
□	Symantec NetBackup Agent	13732,13783,1372...		TCP	N/A
□	FTP Client		21	TCP	N/A
☑	EMC AAM Client	2050-5000,8042-8...	2050-5000,8042-8045	TCP,UDP	N/A
□	Telnet Client		23	TCP	N/A
□	FTP Server	21		TCP	N/A
□	NIS Client		111,0-65535	UDP,TCP	N/A
□	Symantec Backup Exec Agent	10000-10200		TCP	N/A

Figure 4-4 Firewall Properties (remote access)

The following table lists the ICMP, TCP and UDP ports that are enabled by default in the service console firewall. If you need access any of these ports from outside a firewall, you will likely be required to reconfigure any external firewalls to allow access on the appropriate ports.

Note:

The ports listed in the table are connected through the service console interface unless otherwise indicated.

Protocol	Port #	Purpose	Traffic Type
IP	22	SSH for management	Incoming TCP
IP	53	DNS Lookups	Outbound UDP
IP	67-68	DHCP	Incoming & Outgoing UDP
IP	80	HTTP access. ESX Server redirects to port 443	Incoming TCP
IP	427	CIM SLP	Incoming TCP, UDP & Outgoing TCP, UDP
IP	443	HTTPS access	Incoming TCP
IP	902	Authentication traffic	Incoming TCP& Outgoing TCP &UDP
IP	2050 – 5000	VMware High Availability & EMC Autostart Manager traffic	Incoming TCP, UDP & Outgoing TCP, UDP
IP	5988	CIM Server	Incoming TCP
IP	5989	CIM Secure Server	Incoming TCP

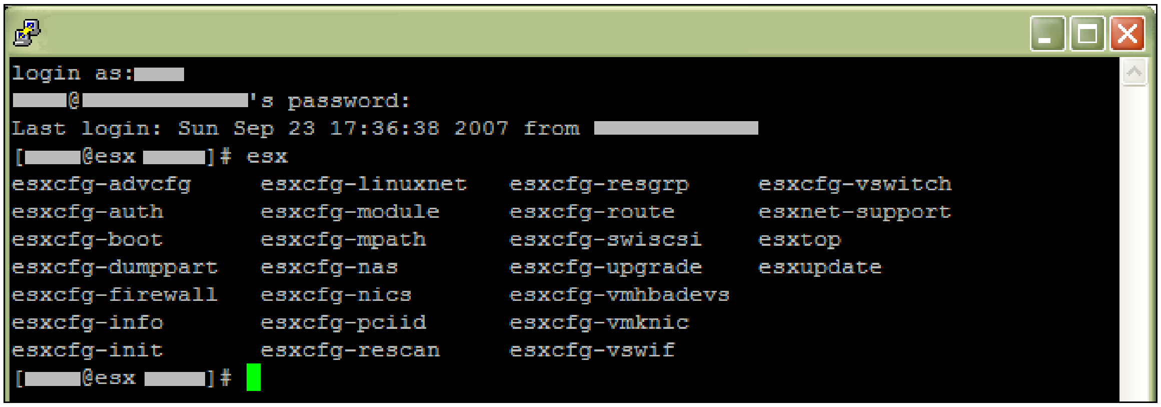
IP	8042 - 8045	VMware High Availability & EMC Autostart Manager traffic	Incoming TCP, UDP & Outgoing TCP, UDP
IP	27000	License transactions from ESX host to license server	Outgoing TCP
IP	27010	License transactions from the license server	Outgoing TCP, UDP
ICMP	Type 0,8	ICMP echo requests & replies	Incoming & Outgoing
ICMP	Type 3, Code 4	ICMP Destination Unreachable, Fragmentation required but DF bit set	Inbound

Additional guidance regarding Service Console firewall configuration can be found in the Chapter 12 of the "Server Configuration Guide."
http://www.vmware.com/pdf/vi3_301_201_server_config.pdf

4.2 Administering ESX Server

There are four ways to administer the ESX Server:

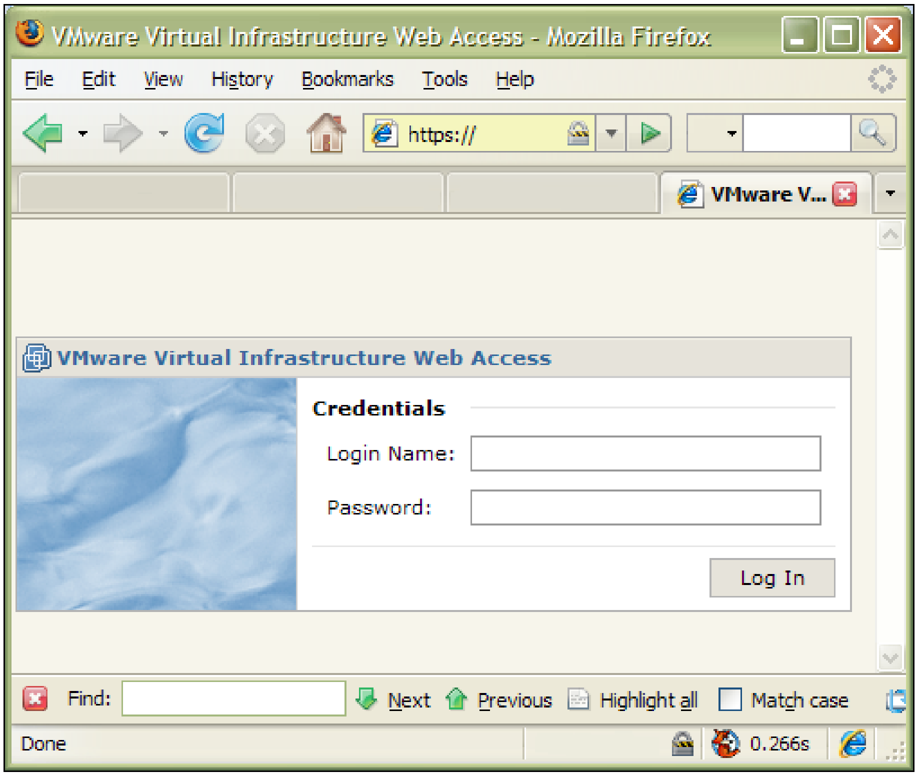
1. Console access to the Service Console (physical access to the machine)
2. SSH to the Service Console (remote access)



```
login as:[redacted]
[redacted]@[redacted]'s password:
Last login: Sun Sep 23 17:36:38 2007 from [redacted]
[[redacted]@esx [redacted]]# esx
esxcfg-advcfg      esxcfg-linuxnet    esxcfg-resgrp      esxcfg-vswitch
esxcfg-auth        esxcfg-module      esxcfg-route       esxnet-support
esxcfg-boot        esxcfg-mpath       esxcfg-swiscsi     esxtop
esxcfg-dumppart    esxcfg-nas         esxcfg-upgrade     esxupdate
esxcfg-firewall    esxcfg-nics        esxcfg-vmhbadevs
esxcfg-info        esxcfg-pciid       esxcfg-vmknic
esxcfg-init        esxcfg-rescan      esxcfg-vswif
[[redacted]@esx [redacted]]# 
```

Figure 4-5 SSH to the Service Console (remote access)

3. VMware Virtual Infrastructure (VI) Web Access



VMware Virtual Infrastructure Web Access - Mozilla Firefox

https://

VMware Virtual Infrastructure Web Access

Credentials

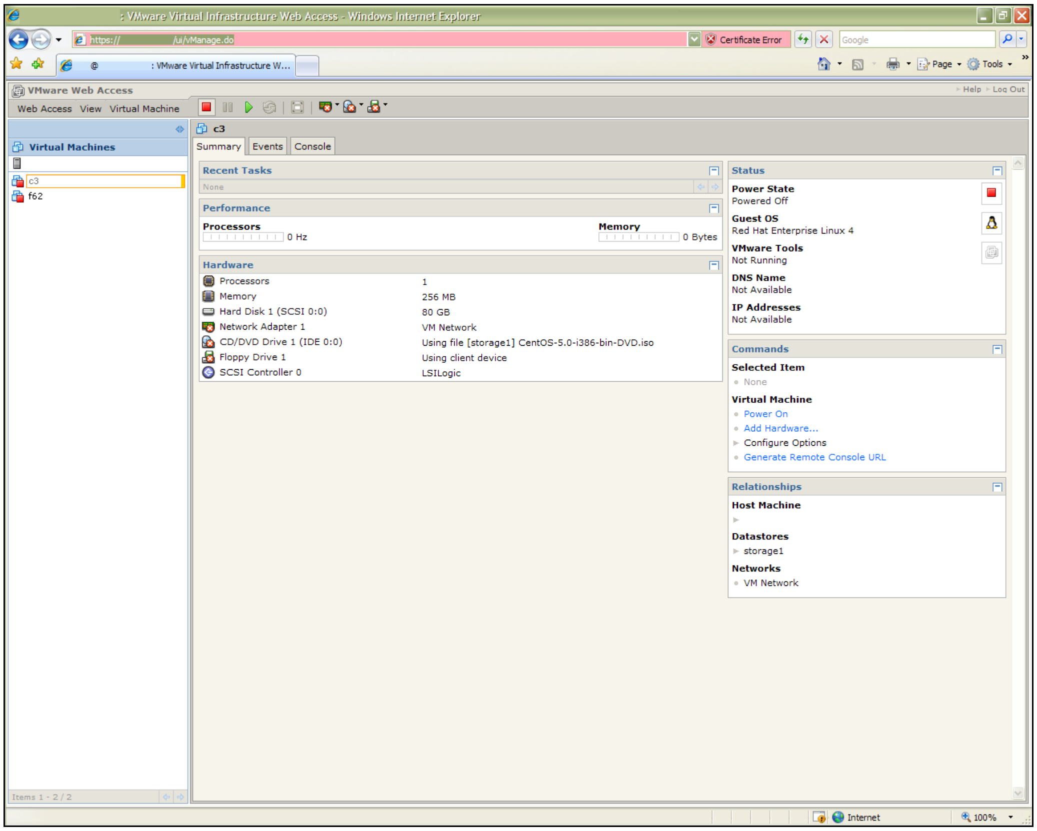
Login Name:

Password:

Done

0.266s

Figure 4-6 VMware Virtual Infrastructure Login (VI) Web Access



: VMware Virtual Infrastructure Web Access - Windows Internet Explorer

https:// /ui/vManage.do

@ : VMware Virtual Infrastructure W...

VMware Web Access

Virtual Machines

c3

f62

c3

Recent Tasks

None

Performance

Processors 0 Hz

Memory 0 Bytes

Hardware

Processors	1
Memory	256 MB
Hard Disk 1 (SCSI 0:0)	80 GB
Network Adapter 1	VM Network
CD/DVD Drive 1 (IDE 0:0)	Using file [storage1] CentOS-5.0-i386-bin-DVD.iso
Floppy Drive 1	Using client device
SCSI Controller 0	LSILogic

Status

Power State
Powered Off

Guest OS
Red Hat Enterprise Linux 4

VMware Tools
Not Running

DNS Name
Not Available

IP Addresses
Not Available

Commands

Selected Item
- None

Virtual Machine
- Power On
- Add Hardware...
- Configure Options
- Generate Remote Console URL

Relationships

Host Machine

Datastores
- storage1

Networks
- VM Network

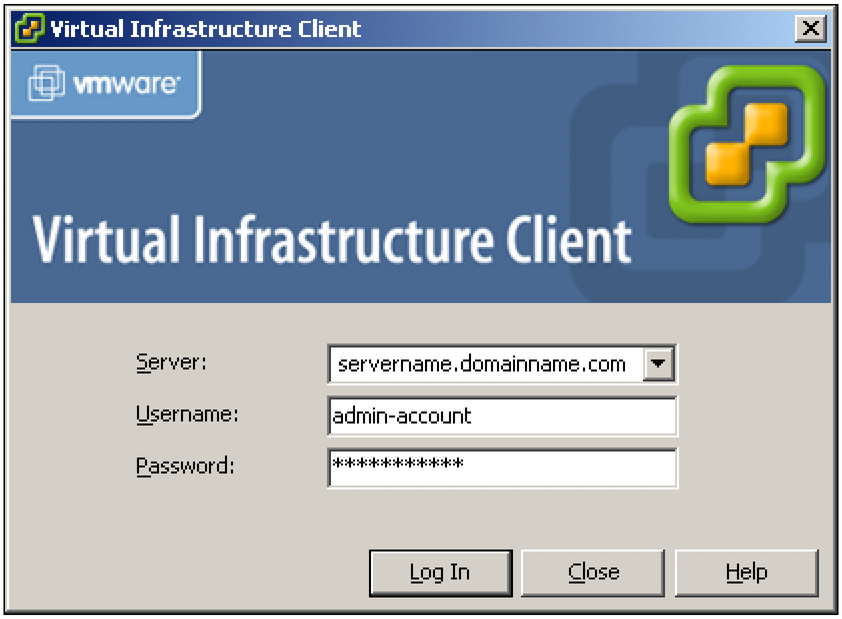
Items 1 - 2 / 2

Internet

100%

Figure 4-7 VMware Virtual Infrastructure (VI) Web Access

4. VMware Virtual Infrastructure Client (VI Client)

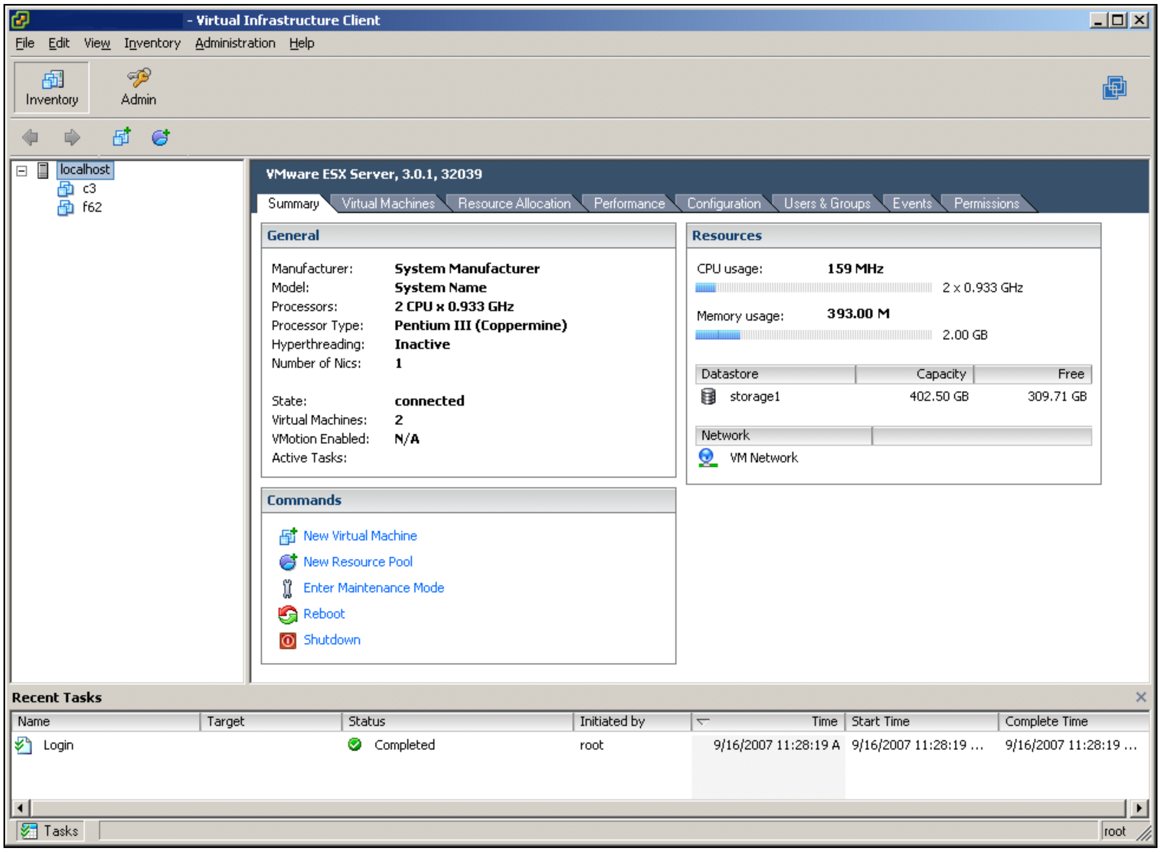


Server: servername.domainname.com

Username: admin-account

Password: ***********

Figure 4-8 VMware Virtual Infrastructure Client Login (VI Client)



VMware ESX Server, 3.0.1, 32039

General

Manufacturer: System Manufacturer
Model: System Name
Processors: 2 CPU x 0.933 GHz
Processor Type: Pentium III (Coppermine)
Hyperthreading: Inactive
Number of Nics: 1

State: connected
Virtual Machines: 2
VMotion Enabled: N/A
Active Tasks:

Resources

CPU usage: 159 MHz — 2 x 0.933 GHz
Memory usage: 393.00 M — 2.00 GB

Datastore	Capacity	Free
storage1	402.50 GB	309.71 GB

Network
VM Network

Recent Tasks

Name	Target	Status	Initiated by	Time	Start Time	Complete Time
Login		Completed	root	9/16/2007 11:28:19 A	9/16/2007 11:28:19 ...	9/16/2007 11:28:19 ...

Figure 4-9 VMware Virtual Infrastructure Client (VI Client)

4.3 Debugging and Troubleshooting Information

The command to produce debugging, troubleshooting and tech support information is listed below:

```
esxcfg-info
```

`esxcfg-info` provides a view of the internal state of the VMkernel and Service Console components. This tool is designed to provide information used in debugging and troubleshooting VMware ESX Servers. More information can be found using the man page (`man esxcfg-info`).

5 ESX Server Guidance

This section addresses specific issues that affect the ESX Sever (host). These are items that you should implement, but require additional reading outside of the scope of this benchmark.

5.1 Configuring NTP on VMware ESX Server

Question:

Do you run NTP servers inside your organization or has your ISP has made a few available?

Action:

If yes, then follow these steps:

- Edit `/etc/ntp.conf` file and the IP addresses as shown below (using the information supplied from your ISP or organization):

```
server 1.2.3.4
server 2.3.4.5
server 3.4.5.6
```

- Then update the `/etc/ntp.conf` file as shown below:

```
server  127.127.1.0 # local clock
fudge   127.127.1.0 stratum 10
```

The order and placement of the lines doesn't matter.

If no, then follow these steps:

If you do not have access to NTP time servers, use those provided by the pool.ntp.org project. This service provides public NTP servers by country, or where there aren't enough servers in a country, by continent.

1. For example, if you are in the United States, you would add the following lines to `/etc/ntp.conf` verbatim:

```
server 0.us.pool.ntp.org
server 1.us.pool.ntp.org
server 2.us.pool.ntp.org
```

The NTP daemon will pick three random servers out of the US pool for synchronization. If you're in another country, see http://www.pool.ntp.org/use.html for more details on how to pick servers.

2. Add these same hostnames (without the word "server" in front) to `/etc/ntp/step-tickers` as well:

```
0.us.pool.ntp.org
1.us.pool.ntp.org
2.us.pool.ntp.org
```

It's a good practice to use at least three servers for synchronization. In the unlikely, but technically possible, case where an NTP server is deliberately or accidentally feeding you incorrect time information, your NTP server could sense this and ignore the bogus data as long as it is in contact with at least two other NTP servers.

Additional steps:

1. Add this line to `/etc/ntp.conf`:

```
restrict default kod nomodify notrap
```

This limits the access for non-loopback machines.

2. On VMware ESX 3 and higher, you'll need to open up the firewall to allow the NTP daemon to talk to external servers with the following command, run as root:

```
esxcfg-firewall --enableService ntpClient
```

3. Now, restart the NTP daemon with:

```
service ntpd restart
```

4. Instruct the ESX host to start the NTP daemon by default after a reboot:

```
chkconfig --level 345 ntpd on
```

5. Finally, instruct the kernel to occasionally synchronize the system time (now accurate because of NTP) back to the hardware clock with the following command:

```
hwclock --systohc
```

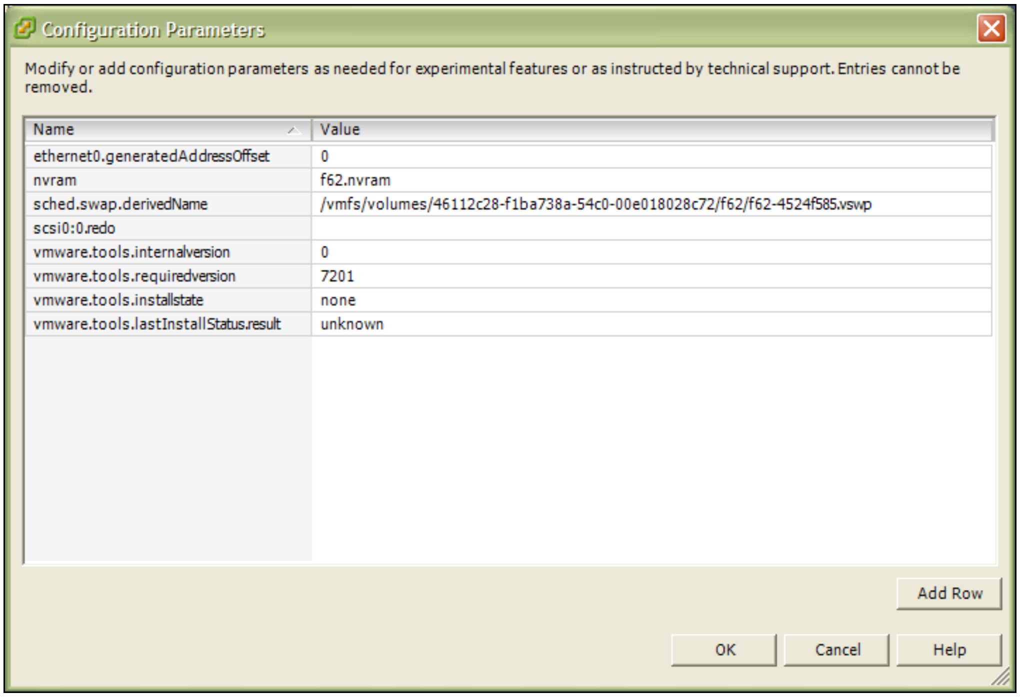
Discussion:

For a more detailed discussion of the configuration choices, see the VMware Knowledgebase article at http://kb.vmware.com/kb/1339. This article suggests using {0,1,2}.vmware.pool.ntp.org as nameservers, however these servers are picked from a random pool of machines around the world, and the servers chosen may be further away geographically than those from {0,1,2}.your_country_code.pool.ntp.org.

5.2 Disable Copy & Paste Operations Between the Guest OS and Remote Console

Action:

1) Login to the VI Client and select each virtual machine.
2) From Summary tab, select *Edit Settings.*
3) Select *Options* > *Advanced* > *Configuration Parameters* to open the Configuration Parameters.
4) Click the *Add Row* button.
5) Add the following three rows (see below):

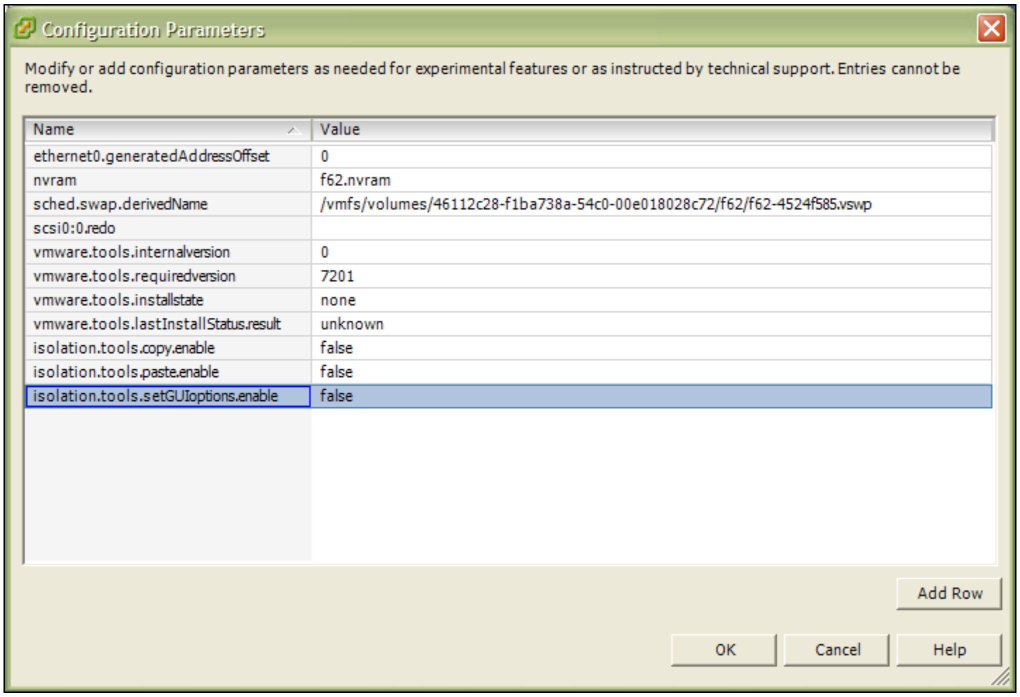


Modify or add configuration parameters as needed for experimental features or as instructed by technical support. Entries cannot be removed.

Name	Value
ethernet0.generatedAddressOffset	0
nvram	f62.nvram
sched.swap.derivedName	/vmfs/volumes/46112c28-f1ba738a-54c0-00e018028c72/f62/f62-4524f585.vswp
scsi0:0.redo	
vmware.tools.internalversion	0
vmware.tools.requiredversion	7201
vmware.tools.installstate	none
vmware.tools.lastInstallStatus.result	unknown

Figure 5-1 Configuration Parameters - Before

Name Field	**Value Field**
`isolation.tools.copy.enable`	`false`
`isolation.tools.paste.enable`	`false`
`isolation.tools.setGUIOptions.enable`	`false`



Modify or add configuration parameters as needed for experimental features or as instructed by technical support. Entries cannot be removed.

Name	Value
ethernet0.generatedAddressOffset	0
nvram	f62.nvram
sched.swap.derivedName	/vmfs/volumes/46112c28-f1ba738a-54c0-00e018028c72/f62/f62-4524f585.vswp
scsi0:0.redo	
vmware.tools.internalversion	0
vmware.tools.requiredversion	7201
vmware.tools.installstate	none
vmware.tools.lastInstallStatus.result	unknown
isolation.tools.copy.enable	false
isolation.tools.paste.enable	false
isolation.tools.setGUIoptions.enable	false

Figure 5-2 Configuration Parameters - After

6) Click OK, to close the Configuration Parameters dialog, and then click OK to close the Virtual Machine Properties dialog.

5.3 Remove Unnecessary Hardware Devices

Action:

1) Login to the VI Client and select each virtual machine.
2) From Summary tab, select *Edit Settings*.
3) Select *Options* > *General*. Record the path displayed in the Virtual Machine Configuration File field.
4) Do not close the dialog.
5) Log into the service console as root.
6) Change to the directory recorded in step 3 (above).
7) Add the following line to the .vmx file:

```
<device_name>.allowGuestConnectionControl = “false”
```

For example:

```
ethernet1.allowGuestConnectionControl = “false”
```

8) Save and close the file.
9) From the VI Client: power off and then power on the virtual machine.
10) Close VI Client and logoff service console.

5.4 Prevent the Guest OS Processes from Flooding the ESX Server Host

Action:

1) Login to the VI Client and select each virtual machine.
2) From Summary tab, select *Edit Settings.*
3) Select *Options* > *Advanced* > *Configuration Parameters* to open the Configuration Parameters.
4) Click the *Add Row* button.
5) Add the following three rows (see below):

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

6) Click OK, to close the Configuration Parameters dialog, and then click OK to close the Virtual Machine Properties dialog.

5.5 Use sudo*

Action:

Configure `sudo` using the command `visudo`. `visudo` is a wrapper for a standard text editor that includes error checking to ensure that the `/etc/sudoers` file doesn't contain incorrect syntax. It is important to use this command and not edit the `/etc/sudoers` file directly. By default, `visudo` will use the `vi` editor, however, you can use another text editor by setting the environment variable for EDITOR to another value. For example:

```
export EDITOR=/usr/bin/nano
```

To customize sudo for your particular situation you can create a setup based on the example below:

```
User_Alias  VI_ADMINS    = user1, user2, user3
User_Alias  VI_JR_ADMINS = user4, user5


Cmnd_Alias  STOP   =    /usr/sbin/shutdown, /usr/sbin/halt,
                        /usr/sbin/poweroff
Cmnd_Alias  REBOOT =    /usr/sbin/reboot
Cmnd_Alias  KILL   =    /usr/bin/kill
Cmnd_Alias  MOUNT  =    /bin/mount /media/*, /bin/umount /media/
Cmnd_Alias  NTP    =    /usr/sbin/ntpdate, /sbin/hwclock
Cmnd_Alias  MISC   =    /bin/ls, /bin/cat, /bin/less, /bin/rm

VI_ADMINS       ALL = STOP, REBOOT, KILL, NTP, MISC
VI_JR_ADMINS    ALL = KILL, MOUNT
```

In this example, VI_JR_ADMINS can run the all of the commands listed in the KILL, and MOUNT aliases, but not the commands listed in the STOP, REBOOT, KILL, NTP or MISC aliases. This schema also makes it easy to create groups of users that can perform actions that (without sudo) would have required access to the root password.

Discussion:

`sudo` is a package that allows the System Administrator to delegate activities to groups of users. These activities are normally beyond the administrative capability of that user (i.e. restarting the web server). If frequent web server configuration changes are taking place (or you have a bug and the web server keeps crashing), it becomes very cumbersome to continually engage the SysAdmin just to restart the web server. `sudo` allows the Administrator to delegate just that one task using root authority without allowing that group of users any other root capability.

Enforce the principle of least privilege. Only allow the minimum commands necessary for each user and alias. Permit limited users to run the `su` command, because `su` opens a root shell that is difficult to audit for multiple users.

For those new to `sudo`, a configurable period of time (5 mins by default) can pass before the user will be required to reenter their password. This can be adjusted in the `/etc/sudoers` file my modifying the `timestamp_timeout` setting.

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

5.6 iSCSI

ESX Server only supports one-way CHAP authentication for iSCSI. It does not support Kerberos, Secure Remote Protocol (SRP), IPsec, or public key authentication methods for iSCSI authentication. Communication to iSCSI devices is unencrypted. Measures should be taken to minimize this risk.

Review “Protecting an iSCSI SAN” beginning on page 208 of the “Server Configuration Guide” from VMware.

5.6.1 Use CHAP to connect to iSCSI devices

Challenge Handshake Authentication Protocol (CHAP)

Review sections “Setting up CHAP Parameters for Hardware Initiators” and “Securing iSCSI Devices Through Authentication” which can be found on pages 118 and 204 of the “Server Configuration Guide” from VMware.

5.6.2 iSCSI Naming Requirements

ESX Sever supports two conventions, IQN and EUI for iSCSI devices.

1. IQN (iSCSI qualified name) – Can be up to 255 characters long and has the following format:

Syntax：

```
iqn.<year-mo>.<reversed_domain_name>:<unique_name>
```

Example:

```
iqn.2005-03.org.cisecurity:azul-03
```

`<year-mo>` should be the year and month the domain name was registered
`<reversed_domain_name>` is the domain name with suffix placed first
`<unique_name>` is any name you want to use.

2. EUI (extended unique identifier) – IEEE standard that requires 24 bits for company name (pre-assigned by IEEE) and a 40 bit unique ID.

Syntax:

```
eui.<24-bit-IEEE-assigned-company-name+40-bit-uniqueID>
```

Example:

```
eui.02004567A425678DService Console
```

6 Network Security Settings

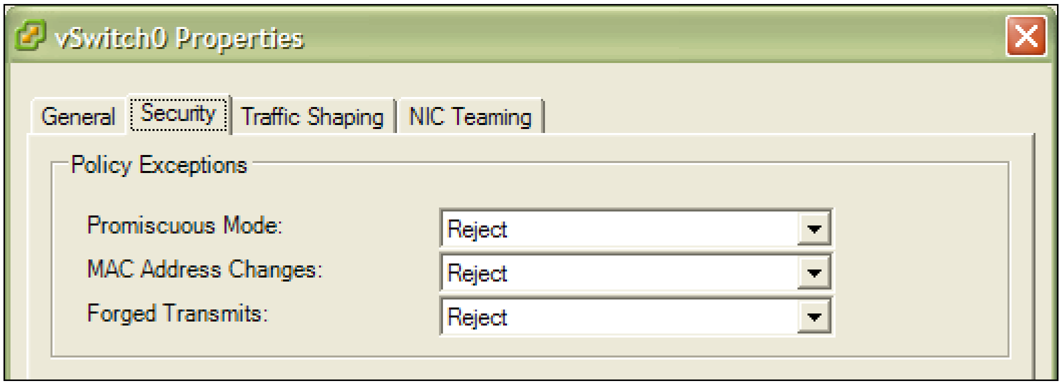
This section addresses network security settings, which will provide a more secure operating environment for both the ESX Server Host as well as the virtual machines that run on it.

6.1 Protect against MAC Address Spoofing & Forged Transmits

Action:

Use the VI client to navigate: *Configuration* -> *Networking* -> *Properties* of the vSwitch you wish to configure and choose the appropriate connection/port to be edited. Click on the Security tab and change the following settings accordingly:

• MAC Address Changes - Set this option to Reject.
• Forged Transmits - Set this option to Reject.



Promiscuous Mode: Reject
MAC Address Changes: Reject
Forged Transmits: Reject

Figure 6-1 VI Console Network Configuration

Discussion:

ESX virtual switches have layer 2 network security features available to protect virtual machines and the virtual host that house them. Each virtual machine is configured with an initial MAC address when the virtual network adapter is created as well as an effective MAC address that may be implemented for network security filtering purposes. When the virtual network adapter is first created the initial and effective MAC addresses are the same.

ESX features the ability to filter incoming network traffic when a destination MAC address is detected that is different than that of the virtual network adapter’s effective MAC address.

Since the guest operating system in a virtual machine has the ability to reconfigure the effective MAC address of its virtual network adapter, there is the potential to spoof or impersonate the source MAC address of another network adapter as well as intercept / redirect traffic destined for another MAC address.

ESX can be configured to protect against both inadvertent and malicious activity by preventing MAC address changes and detecting and preventing forged/spoofed transmissions based upon MAC address manipulation.

By default, each of these settings is set to “Accept,” and should be set to “Reject” to prevent both MAC address changes and forged transmissions. When set to “Reject,” ESX will not honor changes to the effective MAC address except one that is identical to the initial MAC address. It does so by comparing the source MAC address of the transmission against the effective MAC expecting that they match. If they do not match, ESX will drop the packet.

6.2 Promiscuous Mode

Action:

Use the VI client to navigate: *Configuration* -> *Networking* -> *Properties* of the vSwitch you wish to configure and choose the appropriate connection/port to be edited. Click on the Security tab and validate that Promiscuous Mode is set to ‘Reject’ (as seen is Figure 6-1 VI Console Network Configuration above).

Discussion:

Promiscuous mode is a useful network troubleshooting and monitoring tool that allows a network adapter (physical or virtual) to capture all network traffic it has access to, regardless of source or destination. Promiscuous mode may be enabled for virtual switches which are either bound (called a vmnic) or unbound to a to a physical adapter (called a vmnet.)

When promiscuous mode is enabled for a vmnic virtual switch, any connected virtual machines within the virtual host has the capability to intercept any packet sent across the virtual switch fabric or to/from any other virtual machine or network device connected to the same physical network. Likewise, when promiscuous mode is enabled for vmnet virtual switches, any traffic to/from virtual machines connected to the same virtual switch may be intercepted.

By default, promiscuous mode is set to “Reject” and should be left at this setting unless required for troubleshooting or by tools such as IDS/IPS systems that specifically call for its reconfiguration.

6.3 Configure a Dedicated Physical Network Interface or VLAN to Isolate the Management Network

Action:

There are several possible actions that can be taken depending on the particular implementation in your organization. However, some more common approaches are listed below:

- Utilize a private administrative management VLAN

- Utilize a private administrative management VLAN in conjunction with an isolated virtual switch and one or more uplink ports

- Utilize a private administrative management VLAN in conjunction with an isolated virtual switch and a dedicated physical NIC connected to a secure management LAN

Discussion:

In order to protect the service console from attack or misuse, it is recommended that the management network be isolated from any network path used by virtual machines. This is a best practice for securing any management network.

Either of these methods will aid in protecting the service console against illegitimate network access and/or manipulation of network traffic.

For more information, please review the following:

http://www.vmware.com/pdf/vi3_security_hardening_wp.pdf - "Isolate the Management Network", page 5.
http://www.vmware.com/pdf/esx3_best_practices.pdf - "Plan Your Network Structure", page 7.
http://download3.vmware.com/vmworld/2006/TAC9689-A.pdf

7 Minimize boot services

This section addresses minimizing services running in an effort to reduce the threat surface area of the ESX Server. To view the default services execute the following command as root:

```
    ls -A1 /etc/rc3.d/S*
```

The following is a list of the recommended minimum services for ESX.:

```
/etc/rc3.d/S00microcode_ctl
/etc/rc3.d/S00vmkstart
/etc/rc3.d/S01vmware
/etc/rc3.d/S02mptctlnode
/etc/rc3.d/S08iptables
/etc/rc3.d/S09firewall
/etc/rc3.d/S10network
/etc/rc3.d/S12syslog
/etc/rc3.d/S13irqbalance
/etc/rc3.d/S20random
/etc/rc3.d/S55sshd
/etc/rc3.d/S55vmware-late
/etc/rc3.d/S56rawdevices
/etc/rc3.d/S56xinetd
/etc/rc3.d/S58ntpd
/etc/rc3.d/S85gpm
/etc/rc3.d/S85vmware-webAccess
/etc/rc3.d/S90crond
/etc/rc3.d/S91httpd.vmware
/etc/rc3.d/S97vmware-vmkauthd
/etc/rc3.d/S98mgmt-vmware
/etc/rc3.d/S99local
/etc/rc3.d/S99pegasus
/etc/rc3.d/S99vmware-autostart
```

To view the current listening ports execute the following command as root:

```
     netstat -an | egrep '0\.0\.0\.0:\*'
```

Of these, only the following have network ports open (by default):

S55sshd	sshd, tcp port 22
S56xinetd	xinetd, tcp port 902 (vmware-authd)
S58ntpd	ntpd, udp port 123
S85vmware-webAccess	webAccess, tcp ports 8005*, 8009, 8080

S98mgmt-vmware	vmware-hostd, tcp ports 80, 8085*, 8087*, 9080*, 443
S99pegasus	cimserver, tcp ports 32770*, 5988, 5989, and udp port 427

`* accessible to localhost only`

7.1 Set Daemon umask*

Action:

```
cd /etc/init.d
awk '($1=="umask") { if ($2 < "027") { $2="027";}  }; \
    { print }' functions-preCIS > functions
if [ `grep -c umask functions` -eq 0 ]; then
    echo "umask 027" >> functions
fi
chown root:root /etc/init.d/functions
chmod 0755 /etc/init.d/functions
diff  functions-preCIS  functions
```

Discussion:

The system default umask should be set to at least 027 in order to prevent daemon processes (such as the syslog daemon) from creating world-writable files by default. If a particular daemon needs a less restrictive umask, consider editing the daemon startup script to grant that daemon the required umask while maintaining the increased server security posture.

ESX Server is 022 by default. A umask of 027 would make files and directories readable by users in the same Unix group, while a umask of 022 would make files readable by every user on the system.

With a default umask setting of 077 – a setting agreed to as part of the consensus process with DISA and NSA – files and directories created by users will not be readable by any other user on the system. The user creating the file has the discretion of making their files and directories readable by others via the `chmod` command. Users who wish to allow their files and directories to be readable by others by default may choose a different default umask by inserting the umask command into the standard shell configuration files (.profile, .cshrc, etc.) in their home directories. A umask of 027 would make files and directories readable by users in the same Unix group, while a umask of 022 would make files readable by every user on the system.

Adjust root's umask setting separately, as root shells don't necessarily read the system-wide configuration files. For example, root sessions using bash do not get umask settings from `/etc/profile`.

Note:

This is been shown to cause problems with the installation of software packages where the installation script uses the default umask – the directories are owned by root with 700 permissions, and then the application and/or daemon cannot read its files. A simple fix to this problem is to manually issue a less restrictive umask (such as umask 022) for the shell session doing the installation, or place such a umask command in the beginning to a less restrictive value before the installation, or in the beginning of the installation script.

7.2 SNMP

In the files located at `/etc/snmp` (`snmp.conf` and `snmp.conf.preesx`) do the following to secure SNMP:

1. `chmod 700 snmp.conf`
2. `chmod 700 snmp.conf.preesx`

The files should also maintain root as owner and group.

```
-rwxr--r--    1 root     root          159 Jun 13 13:42 snmpd.conf
-rwxr--r--    1 root     root        14895 Jun  5  2002 snmpd.conf.preesx
```

3. The default SNMP read and write community strings should be changed to passphrases that utilize strong passphrase standards
4. SNMP access should be restricted to authorized IP address on separate administrative network
5. Use read-only mode if possible.

Use the command, `man snmpd.conf` for additional information about configuring SNMP.

8 Kernel Tuning

This sections addresses techniques to modify the kernel for some additional network security robustness.

8.1.1 Network Parameter Modifications*

Action:

```
cat <<END_SCRIPT >> /etc/sysctl.conf
# Following 11 lines added - CISecurity Benchmark sec 8.1.1
net.ipv4.tcp_max_syn_backlog = 4096
net.ipv4.tcp_syncookies = 1
net.ipv4.conf.all.rp_filter = 1
net.ipv4.conf.all.accept_source_route = 0
net.ipv4.conf.all.accept_redirects = 0
net.ipv4.conf.all.secure_redirects = 0
net.ipv4.conf.default.rp_filter = 1
net.ipv4.conf.default.accept_source_route = 0
net.ipv4.conf.default.accept_redirects = 0
net.ipv4.conf.default.secure_redirects = 0
net.ipv4.icmp_echo_ignore_broadcasts = 1
END_SCRIPT

chown root:root /etc/sysctl.conf
chmod 0600 /etc/sysctl.conf
diff /etc/sysctl.conf-preCIS /etc/sysctl.conf
```

Discussion:

For additional explanation of these parameters, see `/Documentation/networking/ip-sysctl.txt` in your local copy of the kernel source or read the latest from the cross-referencing Linux site: http://lxr.linux.no/source/Documentation/networking/ip-sysctl.txt .

```
     net.ipv4.tcp_max_syn_backlog = 4096
```

The `tcp_max_syn_backlog` specifies the maximum number of incomplete tcp connection requests that will be remembered. When this system is under a syn flood, a larger number will increase its chance of being able to handle legitimate requests.

```
     net.ipv4.tcp_syncookies=1
```

With `syncookies` enabled, if we reach a point where there are more than 4096 incomplete connections (highly unlikely under most normal loads), this system will change how it responds to new connection requests. Instead of remembering all new connections, it sends out a coded response (the "syncookie") and completely forgets that the connection request came in at all. If the client actually completes the connection request with the third ACK packet, the server can see the cookie coming back and can then rebuild the connection in memory. The remaining connection requests (the SYN flood packets) will never send this third ACK packet, so the server now has a way to hold legitimate conversations without tying up large amounts of memory and processor time handling the flood. When `syncookies` are turned on and there is an overflow in the backlog, the excess connections are completed, but we lose the ability to use TCP extensions for those connections. This may result in some performance degradation for those connections, but the impact is far less than the damage from the SYN flood itself.

```
net.ipv4.conf.all.rp_filter = 1
```

Arriving packets get a simple check - is the packet arriving on the correct interface for its source address? In other words, would a response to this packet go back out the same interface? This simple routing table check can quickly handle some attempts at spoofing source addresses.

A reason why this might need to be left off is the network using asymmetric routing. One example might be a satellite link where incoming packets arrive on an Ethernet interface, but outgoing packets go out through a modem.

```
net.ipv4.conf.all.accept_source_route = 0
```

This IP option specifies how incoming and outgoing packets get routed. While originally intended as a troubleshooting technique, it is used almost exclusively to exploit IP trust relationships with spoofed source packets, and should be disabled.

```
net.ipv4.conf.all.accept_redirects = 0
```

When this is disabled, the system will no longer be able to accept ICMP Redirect messages. While these can be occasionally be legitimately used to temporarily patch an incorrect routing table on a host machine, malicious hosts can use these to force packets through a sniffer or invalid gateway.

For hosts with correct routing tables, this type of packet only has malicious uses. For hosts with incorrect routing tables, ignoring these packets will only slightly impact network performance.

```
net.ipv4.conf.all.secure_redirects = 0
```

When enabled, this would allow redirects from local routers. It's disabled for the same reasons as the above; malicious hosts could lie about the source address for the redirect.

```
net.ipv4.conf.default.rp_filter = 1
net.ipv4.conf.default.accept_source_route = 0
net.ipv4.conf.default.accept_redirects = 0
net.ipv4.conf.default.secure_redirects = 0
```

The previous settings (the "`net.ipv4.conf.all.*`" settings) affect all interfaces that exist when the change is implemented at boot time. These "`net.ipv4.conf.default.*`" make the same changes for any additional interfaces that are created later, such as hotplug USB or PCMCIA network cards.

```
     net.ipv4.icmp_echo_ignore_broadcasts = 1
```

When set to ignore, this system will not respond to broadcast pings such as those used in Smurf attacks. The system will continue to respond to normal ping packets, just not participate in creating floods of echo replies.

9 Logging

This section addresses the configuration, maintenance, and administration of logs on the ESX Server. While these guidelines assist administrators with the configuration and retention of system logging, they are not intended to meet all possible regulatory requirements. Logs are a critical component to proper auditing, maintenance, and incident response. Administrators should adjust settings as appropriate dependant on the size, complexity, and regulatory requirements applicable to the system.

9.1.1 Rotate Log Files from Virtual Machines to the ESX Server Host

You can enable and configure size-based log file rotation by performing the following steps:

1. Log on to the Virtual Infrastructure Client
2. Select the virtual machine from the inventory panel. The configuration page for this virtual machine appears with the Summary tab displayed.
3. Click *Edit Settings*.
4. Click *Options* > *Advanced* > *Configuration Parameters* to open the Configuration Parameters dialog box.
5. Click the *Add Row* button and type the following:
   Name field: log.rotateSize
   Value field: <maximum size in bytes of log file>
   This enables log file rotation based on maximum size specified above.
6. Click the *Add Row* button and type the following:
   Name field: log.keepOld
   Value field: <number of log files to keep>

9.1.2 Maintain Proper Logging

Action:

Make the following changes to the `/etc/logrotate.d/vmkernel` and `/etc/logrotate.d/vmksummary` files:

- Change "`nocompress`" to "`compress`"
- Change "`size 200k`" to "`size 2096K`"

Make the following changes to the `/etc/logrotate.d/vmkwarning` file:

- Add "`compress`"
- Add "`size 2096k`"

Discussion:

The settings for logging are located in the `/etc/logrotate.conf` and `/etc/logrotate.d`. Use "`man logrotate`" for more information.

1. Enable log compression by uncommenting the compress setting in the `/etc/logroatate.conf` file. Uncommenting is performed by removing the "#" at the beginning of the line.

2. Enable log compression and increase the maximum log file size by modifying the configuration files located in the `/etc/logrotate.d` directory.

9.1.3 Confirm Permissions On System Log Files*

Action:

```
cd /var/log

chmod go-rwx boot.log* cron* maillog* messages* secure* spooler*
storageMonitor* sudolog* vmkernel* vmkproxy* vmksummary*
vmkwarning*

chmod -R go-rwx initrdlogs/ oldconf/ vmfsupgrade/ vmksummary.d/
vmkusage/ vmware/ vmware-mui/

chmod g-w,o-rwx dmesg ksyms* rpmpkgs* samba/*

chmod o-rwx wtmp

chmod go-rwx samba/

chown -R root:root .

chgrp utmp wtmp
```

Discussion:

It is critical to protect system log files from being modified or accessed by unauthorized individuals. Some logs may contain sensitive data that should only be available to the system administrator.

If you should add any of the services that affect the above logs, please revisit this section to ensure the logs have the correct/secure permissions.

Note:

You may get some errors from `chmod` if one or more of the files do not exist.

9.1.4 Review Logs

VMkernel:

```
      /var/log/vmkernel
```

VMkernel warnings:

```
      /var/log/vmkwarning
```

VMkernel summary:

`/var/log/vmksummary.html` (`lynx vmksummary.html` to view in console)

ESX Server host agent log:

```
      /var/log/vmware/hostd.log
```

Web access:

```
      /var/log/vmware/webAccess
```

Service console:

```
      /var/log/messages
```

Authentication log:

```
      /var/log/secure
```

Individual virtual machine logs:

```
      <path to virtual machine on ESX Server>/vmware.log
```

vmware-specific logs:

```
      storageMonitor
      sudolog
      vmkproxy
```

vmware-specific directories:

```
      initrdlogs/
      oldconf/
      vmfsupgrade/
      vmksummary.d/
      vmkusage/
      vmware/
      vmware-mui/
```

9.1.5 Configure syslogd to Send Logs to a Remote LogHost

Action:

In the script below, replace `logip` with the IP address (not hostname) of your loghost. It is important to note that using an IP address, instead of the syslog server hostname can help to prevent the spoofing associated with domain name to IP address resolution.

```
echo "### Following lines added by CIS-ESX BM" >> /etc/syslog.conf
echo "### ESX Server 3.x Benchmark Section 9.1.5" >> /etc/syslog.conf
echo -e "local2.*\t/var/log/sudolog" >> /etc/syslog.conf
echo -e "kern.warning;*.err;authpriv.none\t@logip" >> /etc/syslog.conf
echo -e "*.info;mail.none;*.emerg;cron.none;local7.*\t@logip" >>
/etc/syslog.conf
echo -e "local2.*\t@logip" >> /etc/syslog.conf
```

```
diff /etc/syslog.conf-preCIS /etc/syslog.conf
```

Test:

On the loghost machine verify the logs are sent. In a separate terminal, running as root, execute the following command to watch the log file:

```
     # tail –f /var/log/messages
```

From the ESX Server host run the following from the command line (as root):

```
logger -ip kern.warning -t kern.warning-TEST "SYSLOG TEST #1"
logger -ip user.err -t *.err-TEST "SYSLOG TEST #2"
logger -ip authpriv.none -t authpriv.none-TEST "SYSLOG TEST #3"
logger -ip user.info -t *.info-TEST "SYSLOG TEST #4"
logger -ip mail.none -t mail.none-TEST "SYSLOG TEST #5"
logger -ip cron.none -t cron.none-TEST "SYSLOG TEST #6"
logger -ip user.emerg -t *.emerg-TEST "SYSLOG TEST #7"
logger -ip local7.warning -t local7.warning-TEST "SYSLOG TEST #8"
logger -ip local2.warning -t local2.warning-TEST "SYSLOG TEST #9"
```

Discussion:

Remote logging is essential in detecting intrusion and monitoring multiple servers simultaneously. If an intruder is able to obtain root on a host, they may be able to edit the system logs to remove all traces of the attack. If the logs are stored off the machine, those logs can be analyzed for anomalies and used for prosecuting the attacker. Centralized log monitoring and storage is a critical component of incident response and assuring the integrity of system logs.

10 File / Directory Permissions / Access

This section addresses file, directory permissions and access control for the ESX Server.

10.1.1 Add 'nodev' Option To Appropriate Partitions In /etc/fstab*

Action:

```
cp -p /etc/fstab /etc/fstab.tmp
awk '($3 ~ /^ext[23]$/ && $2 != "/") \
    { $4 = $4 ",nodev" }; \
    { print }' /etc/fstab.tmp > /etc/fstab
chown root:root /etc/fstab
chmod 0644 /etc/fstab
rm -f /etc/fstab.tmp
diff /etc/fstab-preCIS /etc/fstab
```

Discussion:

Placing "nodev" on these partitions prevents users from mounting unauthorized devices on any partitions that we know should not contain devices. It is not normally necessary to mount devices on any partitions other than /dev.

One notable exception, is the case where system programs are being placed into "chroot jails"- these often require that several devices be created in the chroot directory. If you are using chroot jails on your machines, you should be careful with the nodev option.

10.1.2 Add 'nosuid' and 'nodev' Option for Removable Media In /etc/fstab*

Action:

```
cp -p /etc/fstab /etc/fstab.tmp
awk '($2 ~ /^\/m.*\/(floppy|cdrom)$/) && \
($4 !~ /,nodev,nosuid/) \
    { $4 = $4 "nodev,nosuid" }; \
    { print }' /etc/fstab.tmp > /etc/fstab
chown root:root /etc/fstab
chmod 0644 /etc/fstab
rm -f /etc/fstab.tmp
diff /etc/fstab-preCIS /etc/fstab
```

Additional Action:

```
chattr +i /etc/fstab
```

Discussion:

Removable media is one vector by which malicious software can be introduced onto the system. By forcing these file systems to be mounted with the `nosuid` option, the administrator prevents users from bringing set-UID programs onto the system via CDROMs and floppy disks. This will also force these filesystems to mount with the `nodev` option, as explained above.

If this machine has multiple CD-ROM or floppy drives, additional action must be taken. Simply add `nosuid` to the fourth field for the `/etc/fstab` lines that reference those drives.

The additional action is required because ESX Server uses the Hardware Abstraction Layer (HAL) Daemon software to update the filesystem description table (`/etc/fstab`) based on a series of SGML policies located in `/usr/share/hal/fdi/` using the program `fstab-sync`. Experience has shown HAL is still maturing and there is a lack of tools available to configure the SGML configuration files. Editing these SHML files manually is beyond the scope of this Benchmark. Therefore, once the desired changes are made to `/etc/fstab`, set it to be immutable (as discussed in the `fstab-sync` man page).

10.1.3 Disable User-Mounted Removable File Systems*

Question:

Are there business justification / mission critical reasons to allow unprivileged users to mount CD-ROMs and floppy disk file systems on this system?

If the answer to this question is no, then perform the action below.

Action:

```
cd /etc/security

CONS_PERM_FILE="console.perms"

DEF_FILE="console.perms.d/50-default.perms"

test -f $DEF_FILE && CONS_PERM_FILE="$DEF_FILE"
awk '($1 == "<console>") && ($3 !~ \
    /sound|fb|kbd|joystick|v4l|mainboard|gpm|scanner/) \
    { $1 = "#<console>" }; \
    { print }' ${CONS_PERM_FILE}-preCIS > $CONS_PERM_FILE
chown root:root $CONS_PERM_FILE
chmod 0600 $CONS_PERM_FILE
diff ${CONS_PERM_FILE}-preCIS $CONS_PERM_FILE
```

Discussion:

In Red Hat Linux, the `pam_console` PAM module gives the user at console (the machine's true physical keyboard) temporarily enhanced privileges. This is configured through the `/etc/security/console.perms` file or `console.perms.d/50-default.perms`. Under the VMware ESX Server 3.x default settings, the console user is given ownership of the floppy and CD-ROM drive, along with a host of other devices. Many of these devices correspond to removable media and thus represent a security risk. This item disables the enhanced privileges on these devices. Be aware that allowing users to mount and access data from removable media drives makes it easier for malicious programs and data to be imported onto the network or data to be removed from the server.

10.2 Establish and Maintain File System Integrity*

The ESX Server has several configuration files in locations listed below:

/etc/profile	644
/etc/ssh/sshd_config	600
/etc/pam.d/system_auth	644
/etc/ntp	755
/etc/ntp.conf	644
/etc/passwd	644
/etc/group	644
/etc/sudoers	440
/etc/shadow	400
/etc/vmware	755

Ensure these files have the correct permissions and are not modified. Use `md5sum` or `sha1sum` to create signatures of these files and store them offline.

10.2.1 Verify passwd, shadow, and group File Permissions*

Action:

```
cd /etc
chown root:root passwd shadow group
chmod 644 passwd group
chmod 400 shadow gshadow
```

Discussion:

These are the default owners and access permissions for these files. It is worthwhile to periodically check these file permissions as there have been package defects that changed `/etc/shadow permissions` to `644`. Tripwire (http://www.tripwire.org/downloads/index.php) and AIDE (http://sourceforge.net/projects/aide) – the successor to Tripwire – are examples of products for alerting you to changes in these files.

Whereas AIDE is an improvement to Tripwire, it is still listed as Beta software, and may not be suitable for Enterprise Production systems.

10.2.2 World-Writable Directories Should Have Their Sticky Bit Set*

Action:

Administrators who wish to obtain a list of these directories may execute the following commands:

```
for PART in `awk '($3 == "ext2" || $3 == "ext3") \
    { print $2 }' /etc/fstab`; do
    find $PART -xdev -type d \
    \( -perm -0002 -a ! -perm -1000 \) -print
done
```

There should be no entries returned. If any are returned, run the following command for each directory:

```
chmod +t /full/directory/path/
```

Discussion:

When the so-called "sticky bit" is set on a directory, then only the owner of a file may remove that file from the directory (as opposed to the usual behavior where anybody with write access to that directory may remove the file). Setting the sticky bit prevents users from overwriting each other's files, whether accidentally or maliciously, and is generally appropriate for most world-writable directories. However, consult appropriate vendor documentation before applying the sticky bit to any world writable directories found in order to avoid breaking any application dependencies on a given directory.

10.2.3 Find Unauthorized World-Writable Files*

Action:

Administrators who wish to obtain a list of the world-writable files currently installed on the system may run the following commands:

```
for PART in $(grep -v '^#' /etc/fstab |

awk '($6 != "0") { print $2 }' ); do

    find $PART -xdev -type f \
    \( -perm -0002 -a ! -perm -1000 \) -print
done
```

There should be no entries returned. If `grub.conf` shows up, its permissions will be adjusted in step 10.4.1.

Discussion:

Data in world-writable files can be modified and compromised by any user on the system. World-writable files may also indicate an incorrectly written script or program that could potentially cause a compromise to the system's integrity. Generally removing write access for the "other" category (`chmod o-w <filename>`) is advisable, but always consult relevant vendor documentation in order to avoid breaking any application dependencies on a given file.

10.2.4 Find Unauthorized `SUID` / `SGID` System Executables*

SUID

Action:
Administrators who wish to obtain a list of the set-UID and set-GID programs currently installed on the system may run the following commands:

```
for PART in $(grep -v '^#' /etc/fstab | awk '($6 != "0") { print
$2 }' ); do
    find $PART -xdev \( -perm -04000 -o -perm -02000 \) \
    -type f -print
done
```

Discussion:

The administrator should take care to ensure that no rogue set-UID programs have been introduced into the system. In addition, if possible, the administrator should attempt a set-UID audit and reduction.

Required:

- `pam_timestamp_check`
- `passwd`
- `pwdb_chkpwd`
- `su`
- `unix_chkpwd`
- `vmkload_app` (two locations)
- `vmware-authd`
- `vmware-vmx` (two locations)

Optional:

- `crontab`
- `ping`
- `sudo`
- `vmkping`

Special Cases:

- `ssh-keysign`

To disable an optional `setuid` application:

1. Log on to the service console and acquire root privileges.
2. Execute this command:

```
    chmod a-s <path_to_executable>
```

SGID

Optional:

- `wall`

Special Cases:

- `lockfile` – only required if the Dell OM management agent is used, otherwise it is optional

To disable an optional `setgid` application:

1. Log on to the service console and acquire root privileges.
2. Execute this command:

```
     chmod a-g <path_to_executable>
```

10.2.5 Find All Unowned Files*

Action:

```
for PART in $(grep -v '^#' /etc/fstab | awk '($6 != "0") { print
$2 }'); do
    find $PART -xdev -nouser -o -nogroup -print
done
```

There should be no entries returned.

Discussion:

Do not allow any unowned files on your system. Unowned files may be an indication of unauthorized system access or improper package maintenance/installation. Sometimes a package removal results in unowned files or directories related to this software as the user/group associated with that package is removed, but that user's files (i.e., files changed after the package was installed) are left behind. Another common cause is the installation of software that does not properly set file ownerships.

Files in any NFS mounts may be ignored as the user ID mapping between systems may be out of sync. If your Enterprise uses a central user management system (NIS or LDAP), the presence of unowned files may indicate another problem and should be investigated.

10.3 System Access, Authentication, and Authorization

This section addresses system administration, system access, authentication, and authorization of the ESX Server.

10.3.1 Restrict at /cron To Authorized Users*

Action:

```
cd /etc/
rm -f cron.deny at.deny
echo root > cron.allow
[ -e cron.allow-preCIS ] && \
    diff cron.allow-preCIS cron.allow
echo root > at.allow
[ -e at.allow-preCIS ] && \
    diff at.allow-preCIS at.allow
chown root:root cron.allow at.allow
chmod 400 cron.allow at.allow
```

Discussion:

The cron.allow and at.allow files are a list of users who are allowed to run the crontab and at commands to submit jobs to be run at scheduled intervals. On many systems, only the system administrator needs the ability to schedule jobs. Note that even though a given user is not listed in cron.allow, cron jobs can still be run as that user. cron.allow only controls administrative access to the crontab command for scheduling and modifying cron jobs.

10.3.2 Restrict Permissions On crontab Files*

Action:

```
chown root:root /etc/crontab
chmod 400 /etc/crontab
chown -R root:root /var/spool/cron
chmod -R go-rwx /var/spool/cron
cd /etc
ls | grep cron | grep -v preCIS | xargs chown -R root:root
ls | grep cron | grep -v preCIS | xargs chmod -R go-rwx
```

Discussion:

The system crontab files are accessed only by the cron daemon (which runs with superuser privileges) and the crontab command (which is set-UID to root). Allowing unprivileged users to read or modify system crontab files can create the potential for a local user on the system to gain elevated privileges.

10.3.3 Configure xinetd Access Control*

Action:

Insert the following line into the "defaults" block in /etc/xinetd.conf:

```
only_from	= <net>/<num_bits> <net>/<num_bits>
```

where each <net>/<num_bits> combination represents one network block in use by your organization. For example:

```
only_from	= 192.168.1.0/24
```

would restrict connections to only the 192.168.1.0/24 network, with the netmask 255.255.255.0.

Note: There are two <TAB>'s between the only_from and the = in the above lines.

Discussion:

This item configures xinetd to use simple IP-based access control and log connections. Just as xinetd's access control mechanisms are used to monitor illicit connection attempts, other tools, such as PortSentry, available from http://www.psionic.com/products/portsentry.html, can be used to monitor access attempts on unused ports.

Note:

Running PortSentry may result in the CIS testing tools reporting "false positives" for "active" ports that are actually being held by the PortSentry daemon. Consider replacing the PortSentry daemon with PSAD, short for Port Scan Attack Detector, available from http://www.cipherdyne.com/psad/. Unlike PortSentry, PSAD doesn't have to hold open ports, instead, it communicates directly with the kernel.

10.3.4 Restrict root Logins To System Console*

Action:

```
rm -f /etc/securetty

echo console >> /etc/securetty

for i in `seq 1 11`; do
    echo vc/$i >> /etc/securetty
done
```

```
for i in `seq 1 6`; do
    echo tty$i >> /etc/securetty
done


chown root:root /etc/securetty
chmod 400 /etc/securetty
diff /etc/securetty-preCIS /etc/securetty
```

Discussion:

Anonymous `root` logins should not normally be allowed. At all other times, the administrator should access the system via an unprivileged account and use some authorized mechanism (such as the `su` command, or the freely-available `sudo` package) to gain additional privileges. These mechanisms provide at least some audit trail in the event of problems.

Many Enterprises – who use serial port concentrators to connect to a server in a data center without physically having to use the keyboard – consider the serial port a console. This is in keeping with the Unix server tradition of controlling headless Unix machines using a serial port console. Just like the virtual consoles, this requires protection as well. If this applies to your organization, you may execute these lines:

```
echo ttyS0 >> /etc/securetty
echo ttyS1 >> /etc/securetty
```

10.4 Limiting Access to su*

Action:

WARNING:

If you do not have immediate physical access to the server, ensure you have a user in the `wheel` group before running the below script. Failure to do so will prevent you from using `su` to become `root`.

```
cd /etc/pam.d/
awk '($1=="#auth" && $2=="required" && \
    $3~"pam_wheel.so")  \
    { print "auth\t\trequired\t”,$3,”\tuse_uid"; next };
    { print }' /etc/pam.d-preCIS/su > su
diff /etc/pam.d-preCIS/su su
```

Discussion:

The `su` command allows you to become other users on the system. This is commonly used to become “root” and execute commands as the super-user. If you do not want certain users to `su` to `root` then uncomment the following line in `/etc/pam.d/su`:

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

Uncommenting this line allows only the users in the `wheel` group to become `root` by using the `su` command and entering the root password. All other users will receive a message stating the password is incorrect.

By limiting access to the root account, even if a user knows the root password, they will not be able to become root unless that user has physical access to the server's console, or they are added to the `wheel` group. This adds another layer of security to the system and prevents unauthorized system access.

10.4.1 Set GRUB Password

Action:

1. Add this line to /boot/grub/grub.conf before the first uncommented line:

```
     password <password>
```

Replace `<password>` with an appropriate password for your organization.

2. Execute the following commands as root:

```
     chown root:root /boot/grub/grub.conf
     chmod 600 /boot/grub/grub.conf
```

Discussion:

By default on most Linux systems, the boot loader prompt allows an attacker to subvert the normal boot process very easily. The action above will allow the system to boot normally, only requiring a password when the user attempts to modify the boot process by passing commands to `GRUB`. Make sure to replace `<password>` in the actions above with a good password.

10.4.2 Require Authentication for Single-User Mode

Action:

Examine the `/etc/inittab` file. If there's no line with "`sulogin`", add the following line after the "`initdefault`" line:

```
     ~~:S:wait:/sbin/sulogin
```

Then protect the file:

```
chown root:root inittab
chmod 644 inittab
```

Discussion:

By default on ESX Server, you can enter single user mode simply by typing "`linux single`" in the GRUB boot-editing menu. Some believe that this is left in to ease support of users with lost root passwords. In any case, it represents a clear security risk – authentication should always be required for root-level access. It should be noted that it is extremely difficult to prevent compromise by any attacker who has knowledge, tools, and full physical access to a system. This kind of measure simply increases the difficulty of compromise by requiring more of each of these factors.

These last two items have attempted to address concerns of physical/boot security. To make these preparations more complete, one should consider setting the BIOS to boot only from the main hard disk and locking this setting with a BIOS password (see section 1.5) . For more information on reducing the threat posed by an attacker with physical / boot access, consider the article "Anyone with a Screwdriver Can Break In," available at http://www.bastille-unix.org/jay/anyone-with-a-screwdriver.html.

11 User Accounts and Environment

This section addresses user accounts and environment settings for ESX Server. The following useful commands will provide information about the ESX Server environment:

`esxcfg-auth`	**configure network authentication and password complexity**
`esxcfg-firewall`	display and configure iptables
`esxcfg-info`	display debugging and troubleshooting information
`esxcfg-module`	displays driver modules loaded on startup
`esxcfg-mpath`	display settings for Fibre channel or iSCSI LUNs
`esxcfg-nics`	display and configure information about the physical NICs
`esxcfg-vmknic`	display and configure VMkernel NIC
`esxcfg-vswif`	display and configure Service Console NIC
`esxcfg-vswitch`	display and configure virtual switches

11.1 Passwords

The following command will display the current password settings on ESX Server:

```
esxcfg-auth --probe
```

11.1.1 Password Complexity

Action:

As root from the service console:

```
esxcfg-auth --usepamqc=disabled disabled -1 12 8
```

Using this example, a user would not be allowed to set passwords that contain only one or two character classes. Also, they would not be able to create passphrases.

The user would need to create a password that consisted of either 12 characters for a three-character class, or 8 characters for four-character class. These are recommended starting values. Some regulated industries require more restrictive values – ensure they comply with your Enterprise security policy.

Discussion:

ESX Server uses the `pam_cracklib.so` plugin by default. This plugin does not check the root account for complexity. You should use the `pam_passwdqc.so` library to handle password complexity for all accounts (including the root account).

```
esxcfg-auth --usepamqc=<N0> <N1> <N2> <N3> <N4> <match>
```

Classes consist of upper case, lower case, numbers, and special characters.

N0 = # of chars required for using one class only
N1 = # of chars required for using two classes
N2 = passphrases
N3 = # of chars required for using three classes
N4 = # of chars required for using all four classes
match = # of chars allowed to be reused from the old password

11.1.2 Minimum Days Before Password Change

Action:

```
esxcfg-auth --passmindays=7
```

This will prevent password changes for seven days.

Discussion:

```
esxcfg-auth --passmindays=<number_of_days>
```

The `<number_of_days>` is the minimum number of days allowed before a password can be changed.

12 Warning Banners

This section addresses the implementation of warning banners on the ESX Server.

Presenting some sort of statutory warning message prior to the normal user logon may assist the prosecution of trespassers on the computer system. Changing some of these login banners also has the side effect of hiding OS version information and other detailed system information from attackers attempting to target specific attacks at a system (though there are other mechanisms available for acquiring this information). Guidelines published by the US Department of Defense require that warning messages include at least the name of the organization that owns the system, the fact that the system is subject to monitoring and that such monitoring is in compliance with local statutes, and that use of the system implies consent to such monitoring. The organization's local legal counsel and/or site security administrator should review the content of all messages before any system modifications are made, as these warning messages are inherently site-specific.

More information (including citations of relevant case law) can be found at http://www.usdoj.gov/criminal/cybercrime/s&sappendix2002.htm.

12.1 Create Warnings for Network and Physical Access Services

Action:
If you have already customized your `/etc/motd, /etc/issue`, or `/etc/issue.net` files, skip step 1. Otherwise, edit the files manually and replace their contents with a single line for your organization, as shown below before proceeding to step 2.

1. Edit the banner currently in the `/etc/issue, /etc/issue.net,` and `/etc/motd` files and add the name of your organization on a separate line at the end.

   Before –

   ```
   VMware ESX Server 3 (Dali)
   Kernel \r on an \m
   ```

   After –

   ```
   Your Organization’s Name
   ```

2. Create banners for console access:

   ```
   unalias cp mv
   cd /etc
   # Remove OS indicators from banners
   for FILE in issue motd; do
       cp -f ${FILE} ${FILE}.tmp
   ```

```
        egrep -vi "red hat|kernel|fedora|vmware esx" ${FILE}.tmp > ${FILE}
        rm -f ${FILE}.tmp
    done
    diff issue-preCIS issue

    if [ "`grep -i authorized /etc/issue`" == "" ]; then
        echo "Authorized uses only. All activity may be \
    monitored and reported." >> /etc/issue
    fi
    if [ "`grep -i authorized /etc/motd`" == "" ]; then
        echo "Authorized uses only. All activity may be \
    monitored and reported." >> /etc/motd
    fi
```

3. Create banners for network access:

```
    cp -fp /etc/issue /etc/issue.net
    if [ "`grep -i authorized /etc/issue.net`" == "" ]; then
        echo "Authorized uses only. All activity may be \
    monitored and reported." >> /etc/issue.net
    fi
    diff issue.net-preCIS issue.net
```

4. Protect banner:

```
    chown root:root /etc/motd /etc/issue /etc/issue.net
    chmod 644 /etc/motd /etc/issue /etc/issue.net
```

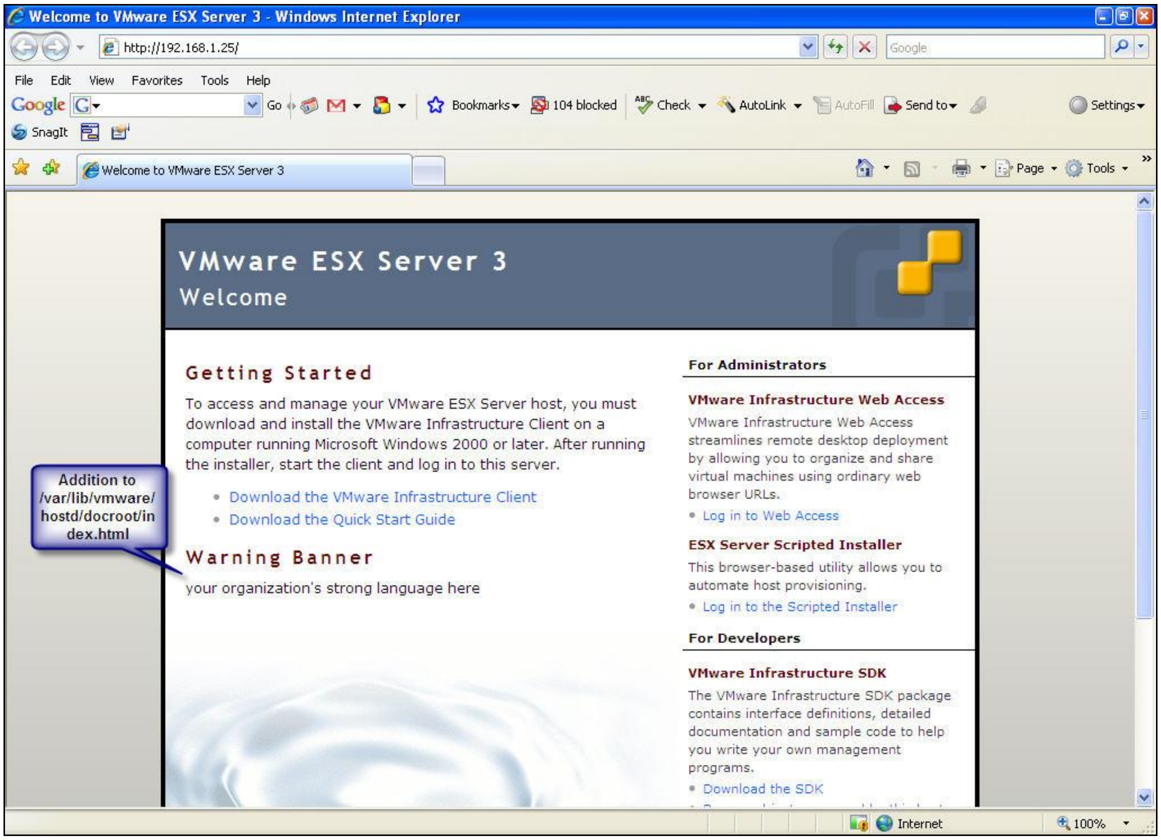
Discussion:

The contents of the `/etc/issue` file are displayed prior to the login prompt on the system's console and serial devices. `/etc/motd` is generally displayed after all successful logins, no matter where the user is logging in from, but is thought to be less useful because it only provides notification to the user after the machine has been accessed.

A copy of a DoD warning banner can be found here:
www.dss.mil/isp/odaa/documents/dod_warning_banner.pdf

12.2 Create Warnings For GUI-Based Logins

The configuration file for web access to the host `/var/lib/vmware/hostd/docroot/index.html` should be modified to add the organization's warning banner in the panel area following the "Getting Started" text as seen below:


Welcome to VMware ESX Server 3 - Windows Internet Explorer
http://192.168.1.25/
File Edit View Favorites Tools Help
Google
Go
Bookmarks
104 blocked
Check
AutoLink
AutoFill
Send to
Settings
SnagIt
Welcome to VMware ESX Server 3
Page
Tools
Internet
100%

VMware ESX Server 3

Welcome

Getting Started

To access and manage your VMware ESX Server host, you must download and install the VMware Infrastructure Client on a computer running Microsoft Windows 2000 or later. After running the installer, start the client and log in to this server.

- Download the VMware Infrastructure Client
- Download the Quick Start Guide

Warning Banner

your organization's strong language here

For Administrators

VMware Infrastructure Web Access

VMware Infrastructure Web Access streamlines remote desktop deployment by allowing you to organize and share virtual machines using ordinary web browser URLs.

- Log in to Web Access

ESX Server Scripted Installer

This browser-based utility allows you to automate host provisioning.

- Log in to the Scripted Installer

For Developers

VMware Infrastructure SDK

The VMware Infrastructure SDK package contains interface definitions, detailed documentation and sample code to help you write your own management programs.

- Download the SDK

Addition to /var/lib/vmware/hostd/docroot/index.html

12.3 Reboot

Action:

```
init 6
```

Discussion:

Whenever you make substantial changes to a system, Administrators should ensure the system is rebooted. Some System Administrators believe any change to the init scripts warrant a reboot to ensure the system comes up as expected. Hours of lost productivity with extensive troubleshooting (not to mention lost revenue) have occurred because a system did not start up as expected. The root cause was an `init` problem that would have been detected had the reboot taken place.

13 Virtual Machines (Guests)

Each of the guest operating systems or applications should have the appropriate security configurations applied before connecting to untrusted networks (i.e. the Internet) or placed into production. The Center for Internet Security, vendors, NIST, DISA, NSA and others provide security hardening guides.

14 References

1. http://www.vmware.com/pdf/vi3_admin_guide.pdf - “Basic System Administration”

2. www.vmware.com/vmtn/resources/582 - “Enabling Active Directory Authentication with ESX Server”

3. http://marketopsrepo.vmware.com/usergroup/preso/Omaha_VMUG_05_29_2007_V4.ppt - “ESX Security Omaha VMUG May 29, 2007”, Michael T. Hoesing

4. “Red Hat Enterprise Linux Benchmark v1.0.54”, Center for Internet Security

5. http://www.vmware.com/vmtn/resources/726 - “VMware Infrastructure 3 Security Hardening”

6. www.gnu.org/software/grub/manual/html_node/index.html

7. www.vmware-tsx.com/download.php?asset_id=37 – “ESX Console Security A Practical guide.”, Yvo Wiskerke

8. http://download3.vmware.com/vmworld/2006/labs2006/vmworld.06.lab05-SECURITY-MANUAL-APPENDIX.pdf - “VI3 Securing and Monitoring”

9. http://www.xtravirt.com/index.php?option=com_remository&Itemid=75&func=fileinfo&id=15 - VI3 Security Risk Assessment Template, Gavin Jolliffe (xtravirt), Jul 08, 2007
10. http://www.cisecurity.com/bench_vm.html - CIS Virtual Machine Security Guidelines

11. http://www.cs.nps.navy.mil/people/faculty/irvine/publications/2000/VMM-usenix00-0611.pdf - “Analysis of the Intel Pentium’s Ability to Support a Secure Virtual Machine Monitor”, Robin and Irvine, 2000

12. www.intel.com/technology/magazine/computing/intel-virtualization-0405.pdf - “Enhanced Virtualization on Intel Architecture-based Servers”, Shiveley, 2005

13. http://www.amd.com/us-en/assets/content_type/white_papers_and_tech_docs/41632A_Virtualization_WP.pdf - “It Takes Virtualization to Make an Agile Infrastructure”, 2006

14. http://web.mit.edu/Saltzer/www/publications/protection/ - “The Protection of Information in Computer Systems”, Saltzer and Schroeder

15. http://research.microsoft.com/~yuqunc/papers/ngscb.pdf - “NGSCB: A Trusted Open System”, Peinado, Chen, England, and Manferdelli

16. http://www.vmware.com/download/vi/vi3_patches.html - VMware patches can be downloaded here

17. www.vmware.com/pdf/vi3_server_config.pdf - “Server Configuration Guide Server Configuration Guide, ESX Server 3.0.1 and VirtualCenter 2.0.1”

18. http://www.vmware.com/pdf/esx3_esxupdate.pdf - “Patch Management for ESX Server 3”

19. http://www.vmware-tsx.com/download.php?asset_id=54 - “VI 3 Upgrade & Patching”

20. http://vmprofessional.com/material/esx-autopatch.html - “A script to fully automate the ESX patching process”

21. http://www.vmware.com/pdf/vi3_installation_guide.pdf - “Installation and Upgrade Guide.”

22. http://www.vmware.com/pdf/vi3_301_201_server_config.pdf - "Server Configuration Guide, Server Configuration Guide, ESX Server 3.0.1 and VirtualCenter 2.0.1."

23. http://www.pool.ntp.org/use.html - NTP

24. http://kb.vmware.com/kb/1339 - “Installing and Configuring NTP on VMware ESX Server”

25. www.gratisoft.us/sudo/ - sudo

26. http://www.vmware.com/pdf/vi3_security_hardening_wp.pdf - “Isolate the Management Network”

27. http://www.vmware.com/pdf/esx3_best_practices.pdf - “Plan Your Network Structure”

28. http://download3.vmware.com/vmworld/2006/TAC9689-A.pdf -

29. http://lxr.linux.no/source/Documentation/networking/ip-sysctl.txt - ip-sysctl variables

30. http://www.psionic.com/products/portsentry.html - Portsentry

31. http://www.cipherdyne.com/psad/ - Port Scan Attack Detector

32. http://www.bastille-unix.org/jay/anyone-with-a-screwdriver.html - "Anyone with a Screwdriver Can Break In"

33. http://www.usdoj.gov/criminal/cybercrime/s&sappendix2002.htm. - “APPENDIX A: Sample Network Banner Language”

34. www.dss.mil/isp/odaa/documents/dod_warning_banner.pdf - DoD Warning Banner

35. http://kb.vmware.com/kb/4646606 – “Enabling Server-Certificate Verification for Virtual Infrastructure Clients”

36. www.vmware.com/vmtn/resources/658 - “Replacing VirtualCenter Server Certificates”

Credits

Dave Shackleford, CIS – Project Lead

Joel Kirch, WBB Consulting – Editor

Bill Stearns, Intelguardians – Co-editor

Special thanks to all of the active CIS Virtual Machine Mailing list participants:

Charu Chaubal

Michael Davis

Chris Farrow

Michael Hoesing

Christofer Hoff

Kirk Larsen

Eric Martin

Tom McAndrew

Taylor Merry

Steve Nelson

Jared Skinner

Ed Skoudis

Doug Staz

Iben Rodriguez

Greg Shipley

Brian Waite

Don C. Weber

Joe Wulf

and many more.

"This work was supported in part by the Department of Homeland Security (DHS) Science and Technology (S&T) Directorate and the Air Force Research Laboratory (AFRL) under contract FA8750-05-C. Points of view expressed in this document are those of the authors, and do not represent the official position of the DHS S&T Directorate or the Air Force Research Laboratory."

Appendix A – Backup Script

Both the backup script and the file list are available on the CIS website for you to download.

```
#!/bin/bash

#Backup files and dirs
/bin/tar -cvf /root/backup.`/bin/date +%Y%m%d%H%M`.tar `/bin/cat \
/tmp/filelist`
#Create restore script
if [ -e /root/do-restore.sh ]; then
  echo "/root/do-restore.sh exists, exiting"
  exit 1
else
  echo '#!/bin/bash' >>/root/do-restore.sh
  /bin/chmod 700 /root/do-restore.sh
  echo 'cd /' >>/root/do-restore.sh
  echo '/bin/tar -Uxvf `/bin/ls -A1rt /root/backup.*.tar | tail -1`' \
  >>/root/do-restore.sh
  /usr/bin/find /var/log -printf "chmod %m %h/%f\n" \
  >>/root/do-restore.sh
fi
echo “Backup complete.”
```

You will also need a list of files called `/tmp/filelist` with the following files listed in it:

```
/etc/.login
/etc/at.allow
/etc/at.deny
/etc/bashrc
/etc/cron.*
/etc/cron.allow
/etc/cron.d/at.allow
/etc/cron.d/at.deny
/etc/cron.d/cron.allow
/etc/cron.d/cron.deny
/etc/cron.deny
/etc/crontab
/etc/csh.cshrc
/etc/csh.login
/etc/cups/cupsd.conf
/etc/default/cron
/etc/default/inetinit
/etc/default/init
/etc/default/keyserv
/etc/default/login
/etc/default/passwd
/etc/default/syslogd
/etc/dt/config/*/sys.resources
/etc/dt/config/*/xresources
```

```
/etc/dt/config/xconfig
/etc/dt/config/xservers
/etc/exports
/etc/fstab
/etc/ftpaccess
/etc/ftpd/banner.msg
/etc/ftpd/ftpaccess
/etc/ftpd/ftpusers
/etc/ftpusers
/etc/group
/etc/grub.conf
/etc/gshadow
/etc/hosts.allow
/etc/hosts.deny
/etc/hosts.equiv
/etc/inetd.conf
/etc/init.d/functions
/etc/init.d/netconfig
/etc/init.d/syslog
/etc/inittab
/etc/issue
/etc/issue.net
/etc/lilo.conf
/etc/limits.conf
/etc/login.defs
/etc/mail/sendmail.cf
/etc/motd
/etc/ntp.conf
/etc/ntp/
/etc/pam.conf
/etc/pam.d/
/etc/passwd
/etc/profile
/etc/proftpd.conf
/etc/rc.d/
/etc/rmmount.conf
/etc/securetty
/etc/security/audit_class
/etc/security/audit_control
/etc/security/audit_event
/etc/security/audit_startup
/etc/security/audit_user
/etc/security/console.perms
/etc/security/limits.conf
/etc/security/policy.conf
/etc/shadow
/etc/skel/
```

```
/etc/ssh/ssh_config
/etc/ssh/sshd_config
/etc/suauth
/etc/sudoers
/etc/sysconfig/sendmail
/etc/sysctl.conf
/etc/syslog.conf
/etc/system
/etc/vsftpd.conf
/etc/vsftpd.ftpusers
/etc/vsftpd/vsftpd.conf
/etc/x11/gdm/gdm.conf
/etc/x11/xdm/kdmrc
/etc/x11/xdm/xresources
/etc/x11/xdm/xservers
/etc/x11/xinit/xserverrc
/etc/xinetd.conf
/etc/xinetd.d/
/opt/kde/share/config/kdm/kdmrc
/root/.bash_profile
/root/.bashrc
/root/.cshrc
/root/.tcshrc
/usr/openwin/lib/app-defaults/xscreensaver
/var/lib/vmware/hostd/docroot/index.html
/var/spool/cron/
/var/spool/cron/crontabs/
```

Appendix B – Kickstart File

```
# START OF KICKSTART FILE FOR ESX SERVER

install
text
reboot

lang en_US.UTF-8
langsupport --default en_US.UTF-8
keyboard us
mouse generic3ps/2 --device psaux
skipx
network --device eth0
--bootproto static
--ip 10.1.1.15
--netmask 255.255.255.0
--gateway 10.1.1.254
--nameserver 1.1.1.1,1.1.2.1
--hostname esx-hostname.domain.com
--addvmportgroup=1
--vlanid=0 rootpw
--iscrypted encrypted-root-password.

#authconfig --enableshadow --enablemd5 --enablekrb5
--krb5realm=hq.domain.com --krb5kdc=active-directory-domain-controller-name
authconfig --enableshadow --enablemd5
timezone --utc America/Los_Angeles
nfs --server=10.1.1.249 --dir=/usr/pkg/ossrc/VMware-ESX
bootloader --driveorder=cciss/c0d0 --location=mbr
# The following is the partition information you requested
# Note that any partitions you deleted are not expressed
# here so unless you clear all partitions first, this is
# not guaranteed to work. These are from HP Blade Center
clearpart --all --drives=cciss/c0d0 --initlabel
part /boot --fstype ext3 --size=200 --ondisk=cciss/c0d0
part / --fstype ext3 --size=2048 --ondisk=cciss/c0d0
part swap --size=2048 --ondisk=cciss/c0d0
part /var/log --fstype ext3 --size=500 --grow --maxsize=2000
--ondisk=cciss/c0d0
# this command skips the EULA screen that comes up during ESX Server
# kickstart...
vmaccepteula

%packages
grub

%post --interpreter=/bin/sh
mkdir -p /mnt/local-root
mount -v 10.1.1.249:/usr/pkg/ossrc/Linux-2.6-i686/local-root
/mnt/local-root
date >> /root/finish-install.log
/mnt/local-root/etc/netinstall/bin/esx-finish-install.ksh >>
/root/finish-install.log 2>&1
echo finish >> /root/finish-install.log
date >> /root/finish-install.log
```

```
umount -v /mnt/local-root >> /root/finish-install.log 2>&1

# END OF KICKSTART FILE
```

Appendix C - Additional Security Notes

The items in this section are security configuration settings that have been suggested by several other resources and system hardening tools. However, given the other settings in the benchmark document, the settings presented here provide relatively little incremental security benefit. Nevertheless, none of these settings should have a significant impact on the functionality of the system, and some sites may feel that the slight security enhancement of these settings outweighs the (sometimes minimal) administrative cost of performing them. They are purely optional and may be applied or not at the discretion of local site administrators.

SN 1 - Enabling Server-Certificate Verification for Virtual Infrastructure Clients

Review “Enabling Server-Certificate Verification for Virtual Infrastructure Clients” which can be found by entering the following into a web browser:

http://kb.vmware.com/kb/4646606

SN 2 - Enable Full and Secure Use of Certificate-based Encryption

Review “Enable Full and Secure Use of Certificate-based Encryption” which can be found at the URL:

www.vmware.com/vmtn/resources/658