the CENTER for
INTERNET SECURITY

Security Configuration Benchmark For

VMware ESX 4

Version 1.0.0
December 30th, 2010

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

TERMS OF USE

Background.

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 and 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 any Product or Recommendation. 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:

No network, system, device, hardware, software or component can be made fully secure;
We are using the Products and the Recommendations solely at our own risk;

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;

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;

Neither CIS, nor any CIS Party (defined below) has any responsibility to make any corrections, updates, upgrades or bug fixes or to notify us if it chooses at it sole option to do so; and

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:

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;

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.

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. We acknowledge and agree that we have read these Agreed Terms of Use in their entirety, understand them and agree to be bound by them in all respects.

Table of Contents

Overview

This document, *Security Configuration Benchmark for VMware vSphere (ESX 4)*, provides prescriptive guidance for establishing a secure configuration posture for *VMware vSphere (ESX 4)* running on hardware compliant with the vendor compatibility guide *http://www.vmware.com/resources/compatibility/search.php?action=base&deviceCategory=server*. This guide was tested against *VMware vSphere (ESX 4.1.0)* as installed using a vendor evaluation ISO, build number 260247 downloaded from http://www.vmware.com. To obtain the latest version of this guide, please visit http://cisecurity.org.

This guide is not intended to be a benchmark for VMware vCenter management server or VMware's ESXi (embedded) host. Any reference to those two products is ancillary and only used when it is informative.

If you have questions, comments, or have identified ways to improve this guide, please write to us at feedback@cisecurity.org.

1.1 Consensus Guidance

This guide was created using a consensus review process comprised of volunteer and contract subject matter experts. Consensus participants provide perspective from a diverse set of backgrounds including consulting, software development, audit and compliance, security research, operations, government, and legal.

Each CIS benchmark undergoes two phases of consensus review. The first phase occurs during initial benchmark development. During this phase, subject matter experts convene to discuss, create, and test working drafts of the benchmark. This discussion occurs until consensus has been reached on benchmark recommendations. The second phase begins after the benchmark has been released to the public Internet. During this phase, all feedback provided by the Internet community is reviewed by the consensus team for incorporation in the CIS benchmark. If you are interested in participating in the consensus review process, please send us a note to feedback@cisecurity.org.

1.2 Intended Audience

This document is intended for system and application administrators, security specialists, auditors, help desk, and platform deployment personnel, who plan to develop, deploy, assess, or secure solutions that incorporate *VMware vSphere (ESX 4)* on hardware compliant with the vendor compatibility guide.

1.3 Acknowledgements

This benchmark exemplifies the great things a community of users, vendors, and subject matter experts can accomplish through consensus collaboration. The CIS community thanks the entire consensus team with special recognition to the following individuals who contributed greatly to the creation of this guide:

Authors
Michael Hoesing, *University of Nebraska at Omaha*

Maintainers
Edward L. Haletky, *AstroArch Consulting, Inc.*
Michael Hoesing, *University of Nebraska at Omaha*
Iben Rodriguez
Lance Seelbach, *CSC*

Contributors and Reviewers
Blake Frantz, *Center for Internet Security*
Edward L. Haletky, *AstroArch Consulting, Inc.*
Joel Kirch
Steven Piliero, *Center for Internet Security*
John Reeman, *VM Informer*
Iben Rodriguez
Lance Seelbach, *CSC*

The CIS community also extends special thanks to the contributors of the CIS VMware ESX 3.5 Benchmark, on which this benchmark builds upon.

Michael Hoesing of *University of Nebraska at Omaha,* Iben Rodriguez, Edward L. Haletky of *AstroArch Consulting, Inc.,* Lance Seelbach of *CSC,* Chyna Trople of *TripWire,* JP Schaaphok of *4Base Technology, Inc.,* Jason Young of *HyTrust, Inc.*, Michael Berman of *Catbird,* Cody Bunch of *Rackspace,* Banjot Chanana of *VMware,* Charu Chaubal of *VMware,* Blake Frantz of *Center for Internet Security,* Moses Hernandez, Wade Holmes of *Siwel Consulting,* Joel Kirch, Steven Piliero of *Center for Internet Security,* Hemma Prafullchandra of *HyTrust, Inc.,* Rob Randell of *VMware,* John Reeman of *VM Informer,* William Stearns, Rob VandenBrink, and Joe Wulf of *ProSync Technologies Group, Inc.*

1.4 Typographic Conventions

The following typographical conventions are used throughout this guide:

Convention	Meaning
`Stylized Monospace font`	Used for blocks of code, command, and script examples. Text should be interpreted exactly as presented.
`Monospace font`	Used for inline code, commands, or examples. Text should be interpreted exactly as presented.
<italic font in brackets>	Italic texts set in angle brackets denote a variable requiring substitution for a real value.
Italic font	Used to denote the title of a book, article, or other publication.
Note	Additional information or caveats

1.5 Configuration Levels

This section defines the configuration levels that are associated with each benchmark recommendation. Configuration levels represent increasing levels of security assurance.

1.5.1 Level-I Benchmark settings/actions

Level-I Benchmark recommendations are intended to:

- be practical and prudent;
- provide a clear security benefit; and
- do not negatively impact the utility of the technology beyond acceptable means

1.5.2 Level-II Benchmark settings/actions

Level-II Benchmark recommendations exhibit one or more of the following characteristics:

- are intended for environments or use cases where security is paramount
- acts as defense in depth measure
- may negatively impact the utility or performance of the technology

1.6 Scoring Status

This section defines the scoring statuses used within this document. The scoring status indicates whether compliance with the given recommendation is discernable in an automated manner.

1.6.1 Scorable

The platform's compliance with the given recommendation can be determined via automated means.

1.6.2 Not Scorable

The platform's compliance with the given recommendation cannot be determined via automated means.

Recommendations

1.7 Service Console/Hypervisor - Preparation for Installation

1.7.1 Validate the System before Making Changes (Level 1, Not Scorable)

Description:
Equipment where the ESX Host is to be installed should have devices installed, burn in, or other steps completed according to specifications of the hardware manufacturer. Media containing the vSphere Server should be verified as unaltered before use in installation.

Rationale:
Hardware or installation software that is altered or damaged in transit from the vendor can provide an unstable foundation for a vSphere environment, possibly causing security, performance, or continuity issues post-installation.

Remediation:
Develop documented procedures to follow manufacturer's recommendations for pre-installation processes. Verify vendors hash totals of software before installation.

Audit:
Review change control documentation for host builds and match steps taken to the steps planned regarding hardware and software testing.

1.7.2 Configure the Firmware (BIOS) (Level 1, Not Scorable)

Description:
Disable the server's ability to boot off all non-hard disk devices, including floppy, CD-ROM, and USB. Configure any required BIOS passwords in conformance with the organization's policy.

Rationale:
Providing access control (see sections 1.4.5 through 1.4.8 for password guidance) to the BIOS and limiting boot sources can reduce the risk that the host's BIOS can be insecurely configured or that an organization's storage or network resources may be accessed by a non-conforming operating system booted from unauthorized media.

Remediation:
While the system is booting press the appropriate key to enter the BIOS configuration, enter a password if required, and navigate to the menu item that controls the boot sequence and set the boot capability and boot order to not boot off of removable media. Also, on the BIOS configuration screens set the BIOS password to the organization's required level.

Audit:
While the system is booting, observe the administrator accessing the BIOS menu using organization approved credentials and review the displayed boot settings for the absence of unauthorized removable media choices.

1.7.3 Change the Default Credentials for Remote Host Access (Level 1, Not Scorable)

Description:

Host hardware with remote access capabilities built into the motherboard (i.e. DRAC, iLO) should have the default credentials changed.

Rationale:
These remote tools allow the ability to boot the host from a CD/DVD device attached to a remote client to facilitate installation when the host is new, but also could be used to install unauthorized operating systems.

Remediation:
At host boot, enter the appropriate keys (i.e. ctrl + D) to enter the remote access configuration screen and change the password to one compliant with your organization's standards (see sections 1.4.5 through 1.4.8 for password guidance). Also, the network to which this remote capability is connected should be a management segment limited to authorized employees.

Audit:
Observe the system administrator attempt to access the host using the vendor default credentials and note the rejected access.

1.8 Service Console/Hypervisor - Installation

1.8.1 Segregate Networks (Level 1, Not Scorable)

Description:
The default installation of vSphere places Virtual Machines (VM's) in a PortGroup (VM Network) on the same virtual switch as the management PortGroup (Service Console). Furthermore, unencrypted data traffic using iSCSI protocols and some vSphere functions (VMotion and others), are normally in the clear and should also be segregated.

Rationale:
The default installation option will combine the Virtual Machine network with the virtual infrastructure Service Console management network. These two groups have different audiences, system administrators and end users, and should be segregated. Failing to segregate this traffic could potentially allow network access to the Service Console to a wider population of users than just system administrators, possibly allowing access to sensitive configuration traffic are unencrypted data traffic.

Remediation:
During the installation of ESX, unselect the default option to create a default network for virtual machines. If subsequent to installation it is determined the management network segment is not to be on the same segment as the guest VMs or data (i.e. iSCSI) traffic, additional networking will need to be enabled. Assuming the requisite amount of physical network interface cards (NICs) are present in the host (depending if IP data network is involved and to provide for redundancy) and cabled to the correct external network routing, switching, DNS and other components or services, configure the additional NICs using:

1. Select the <*host*> in the navigation panel.
2. Select the `Configuration` tab.
3. Click the `Network Adapters` link.

4. Verify all physical network adapters, each sequentially named <*vmnic**>, for the host are listed.

   Note: The <*vmnic**> number assigned to the desired NIC and the vSwitch assigned should be `none` for newly added NICs.

5. Select the `Networking` link on the left `Hardware` panel.

6. Select `Add Networking` link in the upper right hand corner.

7. Select the `Virtual Machine` radio button for a connection type, then `Next`.

8. In the succeeding panel, verify the radio button for `Create a virtual switch` is selected.

9. Click the check box for the appropriate unused <*vmnic**> connected to the desired segment of your external network that was just added, and then select `Next`.

10. Enter a <*network label name*> (which is the new PortGroup name), then select `Next`.

11. Verify the network label and NIC association is correct.

12. Select `Finish`.

13. Configure security settings for both the new vSwitch and the PortGroup (see section 1.6.1 thru 1.6.3 [MAC Spoofing, Forged Transmits, Promiscuous Mode])

14. Power off each guest, and in each guest:

    a. Select `Edit Settings`.

    b. Select the network adapter, on the right at the bottom there should be a `Network Connection`: Network Label title.

    c. Select the name of the new Network Label (PortGroup), created above, in the drop down the section box.

15. Restart the guest.

16. Configure network settings inside the guest (i.e. static IP addresses.)

Audit:
Evaluate network segmentation by reviewing vCenter displays of networking by performing the following:

1. Select the <*host*> in the navigation panel.

2. Select the `Configuration` tab.

3. Click the `Network Adapters` link, this will display a listing of the physical adapters in the host with each sequentially named <*vmnic**>.

4. Review the listing of each *<vmnic*>* and its association with a numbered virtual switch *<vSwitch*>* and the *<IP address range>* associated with the vSwitch/vmnic combination. Each of the 2 (or 3) traffic types should have their own unique *<vmnic*>* / *<vSwitch*>*/ *<IP address range>* pairing with no overlap in addressing.

5. If the preceding step indicates segregation is possible, then review the association of guests with virtual switches by selecting the `Networking` link.

6. In the networking screen, review each virtual switches and ensure all guests are on a virtual switch (or switches) that does not also have management traffic (Service Console) or data traffic.

On the ESX host, the following commands can be used to display networking information:

1. Review the vendor name of the NIC and its PCI location on the motherboard. Verify there are the appropriate number of 2 NICs to facilitate segregation and failover.

```
esxcfg-nics –l
```

2. Review the IP addresses associated with virtual software interfaces in ESX that the service console either uses for management or data traffic. Verify none of the IP network address ranges listed are available for guest use.

```
esxcfg-vswif –l
```

3. Review the sequentially numbered virtual switch (*<vSwitch*>*) and the *<vnic*>* that it is coupled with and the PortGroups that are associated with a *<vmnic*>* / *<vSwitch*>* pair. Verify there are at least 2 vSwitches, one connected to a Service Console PortGroup for management and another for connection to the production network for guest traffic, and a possible third connection to IP storage with a default PortGroup name of `VMkernel`.

4. Verify that an additional VMKernel PortGroup has been created for IP data traffic and kept isolated from other networks.

```
esxcfg-vswitch –l
```

5. Review which PortGroup a guest is associated with. Each available Ethernet connection contains a configuration line in each VM's .vmx file describing `ethernet*.networkName = <yournetworkname>`. Review the `<yournetworkname>` for each connection defined in the guest configuration file for association with the appropriate production network name and the absence of `Service Console`, `VMkernel` or other management related PortGroups

```
cat /vmfs/volumes/<storeagedevicename>/<guestname*> / <guestname.vmx | grep
".networkName ="
```

Note:
Unlike ESX 3.x, vSphere does not need a Service Console PortGroup on the vSwitch handling IP data traffic (iSCSI). The VMkernel PortGroup should be the only PortGroup on an iSCSI vSwitch.

1.8.2 Partition Disks to Avoid Consumption (Level1, Scorable)

Description:
During installation, the following file system structures should be configured on their own disk partitions with each having a minimum size greater than or equal to 5000 1K-blocks:

`/`	`5000`
`/boot`	`5000`
`/home`	`5000`
`swap`	
`/tmp`	`5000`
`/var`	`5000`
`/var/core`	`5000`
`/var/log`	`5000`

Rationale:
If these partitions fill up, it can cause a denial of service. The above partitions are in addition to the default `/`, `/boot`, swap, and `/var/log` partitions. Core files, which could be large as they may result from dump situations, are placed within the `/var/core/` directory. In a default partitioning scheme, these core files can fill up the root partition `/`. A separate partition for /`Home` will help ensure excessive user activity, if any, on the host does not fill production partitions. Having `/tmp` and `/var` in segregated partitions helps if s system processes generate unanticipated volumes of information.

Remediation:
If the default partition configuration was used during the installation process, that configuration process will consume the whole drive leaving no room for the suggested additional partitions. The affected host must either be reinstalled or an exception to policy granted. Establish installation procedures or installation scripts to modify the partitions and sizes to the recommendations during future installations and perform post-build independent certification of each host's construction.

Audit:
Verify the output of the `df` command and ensure the 8 partitions above, are configured on their own disk partition in the `Filesystem` column and their files sizes in the `1K-blocks` column is greater than or equal to `5000`.

```
df
```

Below is an example of a system that is configured as recommended.

```
# df
Filesystem           1K-blocks      Used Available Use% Mounted on
/dev/sda5              5162796   1392180   3508360  29% /
/dev/sda1               248895     30271    205774  13% /boot
/dev/sda9              4127076     32992   3884440   1% /home
/dev/sda8              4127076    311752   3605680   8% /opt
none                    134284         0    134284   0% /dev/shm
/dev/sda10             4127076    272108   3645324   7% /tmp
/dev/sda7              4127076    246568   3670864   7% /var
/dev/sda3              5162828     32828   4867740   1% /var/Core
/dev/sda6              4127076    142044   3775388   4% /var/log
```

1.9 Service Console/Hypervisor – Configuration

1.9.1 Minimize Boot services (Level 1, Scorable)

Description:
Services enabled at host startup should be limited to the vendor's default services and any authorized exceptions.

Rationale:
Any additional services running on an ESX host beyond, added or omitted, to the vendor's default configuration per the list below, could diminish host performance or introduce an attack vector.

Remediation:

1. Compare services discovered in the audit procedures with the recommended list of services presented. For enabled services not on the recommended list, determine whether any services designed to start at boot are required and disable unnecessary services with the `chkconfig` command.

   ```
   /sbin/chkconfig <servicename> off
   ```

   Note: Some services may also require a firewall rule change or rule addition. These items, such as NTP (see also section 1.3.2), are best changed using vCenter if available.

2. Enable services missing from the boot sequence with the `chkconfig` command for the list of services shown in the audit section.

   ```
   /sbin/chkconfig --level 3 <servicename> on
   ```

Audit:

1. Ensure only and all of the following 23 (22 if not using vCenter to manage the host) default services are scheduled to start at run level 3, any additions should be included in the organizations authorized build documents:

   ```
   acpid
   auditd
   crond
   firewall
   ip6tables
   lm_sensors
   mcstrans
   mgmt-vmware
   network
   restorecond
   rpcgssd
   rpcidmapd
   sfcbd-watchdog
   slpd
   sshd
   syslog
   usbarbitrator
   vmware
   ```

```
vmware-autostart
vmware-late
vmware-vmkauthd
vmware-vpxa          (this service is only present if using vCenter)
wsman
xinetd
```

Note: the services `vmware-authd` and `vmware-authd-mks` are added after `xinetd` is activated. Also, by default in vSphere `vmware-webAccess` should be off on all run levels unless specifically excepted by the organization's policy.

2. Compare the results from the following command to the list above and any additional approved services:

```
chkconfig --list | grep 3:on (for items scheduled to start at level 3)
chkconfig --list              (all services & xinetd list at the end)
```

1.9.2 Configure NTP (Level 1, Scorable)

Description:
Add configuration settings to enable system clock synchronization with Network Time Protocol (NTP) server(s).

Rationale:
Keeping your systems synchronized to a local or remote NTP server ensures log entries are date and time stamped consistently across systems allowing for accurate event correlation. This also ensures proper functioning on the system given its interaction to other systems (e.g. vCenter) and possibly third party tools. The default installation of an ESX host does not configure NTP, since the location of your NTP server varies by organization.

Remediation:
Adding NTP requires enabling the service, allowing the service through the firewall, and configuring the host's NTP client for the type and location of the NTP server.

1. Using vCenter, select the host from inventory.

2. Select the `Configuration` tab.

3. Select the `Security Profile` in the Software panel.

4. Click the `Properties` link and in the `Firewall Properties` pop up window, scroll down the ungrouped services to `NTP Client`,

5. Select the empty check box in front of `NTP Client`, then click `OK` and you will be returned to the configuration page where `NTP Client` is now showing in the `Outgoing Connections` list associated with port 123.

Note: These steps will both activate the service and open the related port through the firewall.

6. Select `Time Configuration` in the `Software` panel of the Configuration tab.

7. Click the `Properties` link and in the `Time Configuration` pop up window, click the `Options` button.

8. Select `NTP Settings` in the left panel,

9. In the NTP `Servers` dialog box, use the `Add...` button to add the address of an *<NTP server>*.

10. Repeat step 9 until three NTP servers are present.

11. Select the check box `Restart NTP service to apply changes` and click the `OK` button.

12. Click the `OK` button to close the `Time Configuration` dialog. On the Configuration panel you should see the NTP service as running and the three IP addresses you entered

Audit:

1. Verify the NTP service is running. If no output is present the test fails.

```
ps aux | grep ntp | grep –v grep
```

2. Verify the NTP service is allowed out through the firewall. If the status is `blocked` or the NTP service is not shown as `enabled` then the test fails.

```
esxcfg-firewall –q ntpClient
```

3. Review `/etc/ntp.conf` and verify only the following tokens are set:

    a. The first `restrict` token is set to `127.0.0.1`.

```
grep ^restrict[[:space:]]127\.0\.0\.1 /etc/ntp.conf
```

    b. The second `restrict` token is set to `kod nomodify notrap noquery nopeer.`

```
grep
^restrict[[:space:]]default[[:space:]]kod[[:space:]]nomodify[[:space:]]not
rap[[:space:]]noquery[[:space:]]nopeer /etc/ntp.conf
```

    c. The first `server` token is set to *`<authorized_NTP_server_primary>`*.

```
grep ^server[[:space:]]<authorized_NTP_server_primary> /etc/ntp.conf
```

    d. The second `server` token is set to *`<authorized_NTP_server_secondary>`*.

```
grep ^server[[:space:]]<authorized_NTP_server_secondary> \ /etc/ntp.conf
```

    e. The third `server` token is set to *`<authorized_NTP_server_tertiary>`*.

```
grep ^server[[:space:]]<authorized_NTP_server_tertiary> \ /etc/ntp.conf
```

4. Review `/etc/ntp/step-tickers` and verify only authorized NTP servers are present:

    a. The first server is set to `<authorized_NTP_server_primary>`.

```
grep ^<authorized_NTP_server_primary> /etc/ntp/step-tickers
```

    b. The second server is set to `<authorized_NTP_server_secondary>`.

```
grep ^<authorized_NTP_server_secondary> /etc/ntp/step-tickers
```

    c. The third server is set to `<authorized_NTP_server_tertiary>`.

```
grep ^<authorized_NTP_server_tertiary> /etc/ntp/step-tickers
```

1.9.3 Create Warning Banners (Level 1, Scorable)

Description:
Create warning banners for console and remote access.

Note: There are no default warning banners since your organization's exact wording is unknown at to the vendor.

Rationale:
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.

Remediation:
Log on to the service console; acquire `root` privileges and perform the following:

1. Create or edit Message of the Day warning banner.

```
vi /etc/motd
```

2. Create or edit login warning banner.

```
vi /etc/issue
```

3. Create or edit network login, warning banner.

```
vi /etc/issue.net
```

4. Create or edit the page first displayed when web browsing to the host. Even though the `vmware-webAccess` management functions to the host are disabled by default, the https service will display the page that allows the downloading of the Virtual Infrastructure Client (VIC) and would be an appropriate place for a warning banner.

```
vi /usr/lib/vmware/hostd/docroot/index.html
```

5. Create or edit the vCenter warning banner:
   a. Select the `Administration` menu name in vCenter.
   b. Select `Edit Message of the Day` to edit or create the text of your organization's warning content.

   Note: Also, if additional banners are specified in the `/etc/ssh/sshd_config` file, that specified banner file should include the organization's warning text.

Audit:
Verify system warning banners for message of the day, login, network login, GUI and vCenter are configured with the current version of your organizations warning banner language:

1. Verify the Message of the Day banner is properly configured.

```
cat /etc/motd
```

2. Verify the login banner is properly configured.

```
cat /etc/issue
```

3. Verify the network login banner is properly configured.

```
cat /etc/issue.net
```

4. Verify GUI-Based login banner is properly configured.

```
cat /usr/lib/vmware/hostd/docroot/index.html
```

5. Verify vCenter banners:

   a. Select the `Administration` menu name in vCenter.
   b. Select `Edit Message of the Day` to compare that text to your organization's content. (or alternately, observe the warning when logging into vCenter)

1.9.4 Maintain Vendor Patches (Level 1, Not Scorable)

Description:
A formal process for keeping up-to-date with applicable vendor patches is even more important for the host that services multiple guests. It is up to the organization to download and install

patches in accordance to their policies and any SLA requirements; some patches may require a reboot of the system. Patches should typically be evaluated in a test environment, before being implemented into a QA then Production environment. It is recommended that the VMware Update Manager be used for this purpose.

Note: Red Hat operating system patches should not be applied to the ESX host Console Operating System (COS).

Rationale:
Applying vendor supported patches minimizes vulnerabilities and utilizes the vendor's security research and their product knowledge regarding compatibility of changes with other components of the console operating system.

Remediation:
If Update Manager is installed, follow the procedures for that application to identify hosts and the patches needed, then stage and remediate as instructed by that software.

Log on to the service console; acquire `root` privileges and perform the following:

1. Run a test install to check dependencies and verify sufficient disk space:

```
esxupdate –d <url_of_update_repository> --test update
```

2. Install patches, via the command line, on the ESX host after the patches have been:

    - Evaluated as relevant to your organizations environment and prioritized (e.g. wait for the next update window or apply immediately.)
    - Downloaded and unzipped if needed.
    - Moved to the update repository.
    - Tested in a non-production environment.
    - Approved and documented including backup and roll-back plans in accordance with your organization's change management policies and procedure.

    Note: Some patches require rebooting the guests and or the host. Review each patch for reboot and other requirements or dependencies and communicate timelines to affected parties.

```
esxupdate –d <url_of_update_repository> update
```

Audit:
Log on to the service console; acquire `root` privileges and perform the following:

1. Determine the version and build of your ESX host:

```
vmware -v
```

2. Determine the patches that have been installed:

```
esxupdate query
```

3. Compare the installed patches to the list of vendor patches for the version and build number, obtained from the previous command, as shown per the vendor for ESX version 4 at: http://www.vmware.com/patch/download/. Assess any variance for applicability to the environment and any authorized exceptions.

Note: Optional audit steps.

4. Review the patch activity log for errors:

```
cat /var/log/vmware/esxupdate.log
```

5. Determine the list of CVEs resolved by installed patches (or to look for a specific CVE add the CVE year and number):

```
rpm –qa –changelog | grep CVE
```

References:

1. VMWare, Inc. (2009). *ESX 4 Patch Management Guide*. Available: http://www.vmware.com/pdf/vSphere4/r40/vsp_40_esxupdate.pdf

1.9.5 Utilize Host Profiles (Level 1, Not Scorable)

Description:
A vSphere host build, or a variety of risk-based builds, may be created and implemented on new hosts utilizing Host Profiles, standardizing the construction of new hosts.

Note: Host Profiles is not available on all vSphere product versions.

Rationale:
Consistent certified automated configurations of similar hosts may reduce errors, provide a similar security posture and speed deployment. Further, the Host Profiles tool may be used to monitor any host that varies from the standard and assist with the non-conforming host's remediation.

Remediation:
To create a host profile, first build an ESX host according to the organization's standards. Right click on that golden host in the Inventory panel of vCenter and select "Host Profile", then select "Create Profile from (this) Host", give the profile a name and description and click "Next" and "Finish".
To apply a host profile to another host, right click on that additional host in the Inventory panel of vCenter and select "Host Profile", then select "Manage Profile", in the "Attach profile" pop up panel, select the desired host profile previously created and click 'OK".

Audit:

To see how the host complies with the applied profile, right click on the host being evaluated, select “Host Profile”, and chose “Check Compliance”. In the host’s “Summary” tab, in the last two lines of the “General” section, the name of the profile applied to the selected host and its compliance status will be shown. If the host is not compliant with its profile, there will be a red “X” on the last line and a blue link to drill down to the list of issues causing the non-compliance.

1.9.6 Do Not Use Red Hat Based Vulnerability Scanners (Level 1, Not Scorable)

Description:
While it is recommended that Red Hat based operating system scanner not be used to assess the COS, any results provided by those tools should be carefully reviewed.

Rationale:
Scanning tools sometimes report vulnerabilities based on version information collected. If the component or service has been modified, which VMware does with many of the components in the COS, false positives may result, inefficiently consuming resources.

Remediation:
Define assessment procedures that use tools and techniques specifically designed for vSphere where possible.

Audit:
Review the current host assessment documentation and match tools and collection procedures used to the authorized process.

1.9.7 Do not Use Linux Based Configuration Commands (Level 1, Not Scorable)

Description:
Do not, if present, use Linux or Redhat based configuration commands (i.e.`redhat-config`, `system-config`, `authconfig`).

Rationale:
Since many of the components of the COS have been modified by VMware, use of non-approved configuration tools may degrade host performance or result in a vulnerability.

Remediation:
Review the current host management documentation and match tools and procedures used to the tools and procedures authorized by the vendor (vCenter, VIC, …).

Audit:
Review the current host management documentation and match observed tools and procedures used to the authorized process.

1.9.8 Monitor File Integrity (Level 1, Not Scorable)

Description:
Files critical to the configuration and operation of the host should have hash values calculated at installation, before deployment, and then periodically calculate the current hash value of those files and compare them to the known good values.

Rationale:
Any changes to critical files should be detected, and compared to the organizations change management records to determine appropriate authorization for the alteration.

Remediation:
System administrators and information security staff should determine a list of files critical to the security and operation of the host that are not subject to a high rate of automated change (i.e. log files). Those files should be hashed before deployment and those known good values stored on a non-writeable media for use in checking production host's values to detect changes.

Audit:
Review procedures to periodically evaluate critical file hashes against the known good values, the matching of changes to authorization, and the follow-up performed on changes not matching the authorization records.

Notes:
If using a third party tool for these procedures, verify with the vendor that the intended tools do not create support or warranty issues.

1.10 Service Console/Hypervisor – Access Control

1.10.1 Configure SSH Access (Level 1, Scorable)

Description:
Remote shell access to the console operating system should protect both the authentication credentials of the administrator and the content communicated between the ESX host and the administrator using secure shell (SSH). Do not enable Direct Root SSH. Do not enable direct `su` to `root`, only allow `sudo` (see section 1.4.2).

Note:
Direct console access should be mitigated with physical security controls. Also, other vendor supplied remote access tools may rely on the SSL protocol to protect browser based sessions. Review the vendor recommendations for replacing default, vendor-supplied certificates http://www.vmware.com/pdf/vi_vcserver_certificates.pdf.

Rationale:
Securing administrator login and communication sessions reduces the chance of unauthorized interception of privileged credentials or sensitive configuration information.

Remediation:

Note: Make a backup before editing configuration files.

If SSH server is not enabled, (it is enabled by default) then:

1. Using vCenter, select the <*host*> from inventory.

2. Select the `Configuration` tab.

3. Select the `Security Profile` in the Software panel.

4. Choose the `Properties` link and in the `Firewall Properties` pop up window, scroll down to the secure shell grouped services to `SSH Server`.

5. Select the empty check box in front `SSH server`, and you will be returned to the configuration page where `SSH Server` is now showing in the `Outgoing Connections` list associated with port 22. These steps will both activate the service and open the related port through the firewall.

6. Perform the following post-installation actions to secure the SSH (OpenSSH 4.3.p2) service:

    a. Change to the `/etc/ssh` directory.

    b. Edit `sshd_config.`

    c. Set the `Protocol` token to `2`. If it is absent, add and set it.

    d. Set the `IgnoreRhosts` token to `yes`. If it is absent, add and set it.

    e. Set the `StrictModes` token to `yes`. If it is absent, add and set it.

    f. Set the `PermitRootLogin` token to `no`. If it is absent, add and set it.

    g. Set the `PermitEmptyPasswords` token to `no`. If it is absent, add and set it.

    h. Set the `Banner` token to `/etc/issue`. If it is absent, add and set it.

    i. Save the updated `sshd_config` file.

    j. Ensure `root` is the owner of `sshd_config` and `ssh_config`.

    k. Ensure write access to `sshd_config` and `ssh_config` is limited to the file owner `root`.

7. Perform the following post installation actions to secure system-wide SSH client configuration (if SSH client is allowed as an exception, in the default ESX configuration SSH Client is turned off) :

    a. Change to the `/etc/ssh` directory.

    b. Edit `ssh_config.`

    c. Set the `Protocol` token to `2`. If it is absent, add and set it.

    d. Set the `Ciphers` token to `aes256-cbc,aes128-cbc`. If it is absent, add and set it.

    e. Save the `updated ssh_config` file.

8. Perform the following to allow inbound SSH connections through the ESX firewall

    a. `esxcfg-firewall -e sshServer`

9. Perform the following to prevent outbound SSH connections via the ESX firewall

    a. `esxcfg-firewall -d sshClient`

Audit:

1. Verify the SSHD service is running. If no output is present, SSHD is not configured as recommended.

```
ps aux | grep /usr/sbin/sshd | grep -v grep
```

2. Verify the configuration files `/etc/ssh/ssh_config` and `/etc/ssh/sshd_config` options and tokens are set as outlined in remediation steps 6 and 7 above.

```
cat /etc/ssh/ssh_config
cat /etc/ssh/sshd_config
```

3. Verify the ESX firewall permits inbound SSH connections.

```
esxcfg-firewall -q sshServer
```

   The above command will output **`Service`** `sshService` is `enabled` if configured as prescribed.

4. Verify the ESX firewall prevents outbound SSH connections.

```
esxcfg-firewall -q sshClient
```

   The above command will output `Service sshClient is blocked` if configured as prescribed unless an exception is allowed.

1.10.2 Implement SUDO (Level 1, Not Scorable)

Description:
SUDO allows non-root or non-administrative users to gain root or administrative access and commands, while providing logging that enhances user accountability.

Rationale:
SUDO enables associating users with powerful administrative commands and allowing root privileges. Further, SUDO provides logging of those users who access these advanced capabilities. SUDO is not configured on the default ESX installation, since the account and groups to be included vary by organization.

Remediation:
General SUDO configuration steps include identification of administrators and users and placing them in groups, assigning the groups to wheel status or assigning the groups to specific commands sets (i.e. such as those in the group that can execute esxcfg-* commands) based on their needs as agreed upon between the system administrators and information security..

Note:
Any changes to SUDO configurations must be made using the special editor `visudo` (not `vi`).

Audit:
Review the settings for SUDO alias specifications, wheel group membership, and user command combinations for appropriate functionality commensurate with the user's job functions. Also, SUDO messages are included in `/var/log/` messages, ensure this log file is included in the log reviews (section 1.5.2) and collection (section 1.5.3) procedures.

```
cat /etc/sudoers
```

1.10.3Set File Permissions (Level 1, Scorable)

Description:
Set file permissions on the ESX host for all `.vmx` configuration files to:

- Deny group write access
- Deny other write access

Set file ownership for all `.vmx` files to:

- Restrict owner and group file ownership to `root`

Set file permissions for all `.vmdk` disk files to:

- Deny group read, write and execute access
- Deny other read, write and execute access

Set file ownership for all `.vmdk` disk files to:

- Restrict owner and group file ownership to `root`

Note: Many additional files could be considered for reducing access from the default installed rights (log files, most files in the `/etc/` directory, and others). Each organization's system administration and information security teams should determine their list of critical files and the appropriate, individual, group, and other ownership rights, plus the appropriate read, write, and execute permissions for each item on that list.

Rational:
Limiting file permissions to and ownership of, configuration files helps prevent accidental or malicious changes to the system. Limiting file permissions-to- and ownership-of-, virtual disk files helps reduce unauthorized deletion or copying of a resource critical to the guest's operation.

Remediation:
Log on to the service console; acquire `root` privileges and perform the following:

1. Set file permissions for user and other to deny write access for all *<vmx_file_location>* files.

```
chmod go-w <vmdk_file_location>
```

Log on to the service console; acquire `root` privileges and perform the following:

1. Set file ownership parameters for owner and group to `root` for all *<vmx_file_location>* files:

```
chown root:root <vmx_file_location>
```

Log on to the service console; acquire `root` privileges and perform the following:

1. Set file permissions for user and other to deny read, write and execute access for all *<vmdk_file_location>* files.

```
chmod go-rwx <vmdk_file_location>
```

Log on to the service console; acquire `root` privileges and perform the following:

1. Set file ownership parameters for owner and group to `root` for all *<vmdk_file_location>* files:

```
chown root:root <vmdk_file_location>
```

Audit:
Log on to the service console; acquire `root` privileges and perform the following:

1. List all virtual machine file locations on your host (find is recursive by default):

```
find /vmfs/volumes/ -name *.vmx
```

2. Verify group and other file permissions for all *<vmx_file_location>* files have write access disabled, the rights string should contain `-rwx------`:

```
ls -l <vmx_file_location>
```

3. Verify file ownership as `root` and `root` for the owner and the group:

```
ls -l <vmx_file_location>
```

4. Verify group and other file permissions for all *<vmdk_file_location>* files have read, write and execute access disabled, the rights string should contain `-rwx------`:

```
ls -l <vmdk_file_location>
```

5. Verify file ownership as `root` and `root` for the owner and the group:

```
ls -l <vmdk_file_location>
```

6. For any other critical files, use the command below and review the permission string – `rwxrwxrwx` and ownership (`root:root`) and match to your organization's standard .

```
ls -l <critical_file_location>
```

1.10.4Strengthen Password Controls- History (Level 1, Scorable)

Description:
Retain a *history* of previous passwords used and configure the authentication controls to validate new passwords against greater than or equal to 10 recently used credentials.

Rationale:
Maintaining a history file containing previously used credentials for each user, along with an access control parameter limits continual reuse of recent passwords. Combined with minimum and maximum password life this control helps maintain password effectiveness.

Remediation:
Log on to the service console; acquire `root` privileges and perform the following:

1. A password history repository should exist on the vSphere host , but if it does not exist, then create it:

   ```
   touch /etc/security/opasswd
   ```

   Configure the file permissions:

   ```
   chmod 600 /etc/security/opasswd
   ```

   Change the file ownership:

   ```
   chown root:root /etc/security/opwasswd
   ```

2. Change to the `/etc/pam.d` directory.

3. Edit `system-auth-generic` per item 4

4. If absent, add the token `remember=10` to the line containing `password required /lib/security/$ISA/pam_unix.so`

5. Save the updated `system-auth-generic` file. (**note**: the `/etc/pam.d/system-auth-generic` file pertains to all users *except* the `vpx` vCenter account, the `/etc/pam.d/system-auth-local` file pertains to the `vpx` vCenter account)

Audit:
Verify password history is enabled and the value after `remember=`*`<password_history>`* is greater than or equal to `10`. If no results are returned then password history is not enabled.

```
grep -E 'password.*sufficient.*pam_unix.so.*remember='  \ /etc/pam.d/system-auth-generic
```

1.10.5Strengthen Password Controls – Composition Strength (Level 1, Scorable)

Description:
Password *strength/complexity* requirements:

- Ignored when 1 character class is used.
- Ignored when 2 character classes are used.
- Ignore passphrases.
- Greater than or equal to 12 characters in length when 3 character classes are used.
- Greater than or equal to 8 characters in length when 4 character classes are used.
- Ignore reuse of any number of characters from the old password unless the new password is exactly the same as the old password.

Rationale:
The user should create a password that consists of a mix of character classes from the four choices; upper case, lower case, numeric, or special to reduce the use of common words as passwords and increase the difficulty of an unauthorized user guessing their credential.

Note:
The default installation of ESX uses the `pam_cracklib.so` plug-in for both password complexity (default is not configured) and number of failed login attempts before account lockout (default setting is 3.) This plug-in 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).

Remediation:
Log on to the service console; acquire `root` privileges and perform the following:

1. Configure password complexity:

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

Note: Setting the value of any of these options to `-1` ignores the requirement. Setting any of these options to `disabled` disqualifies passwords with the associated characteristic. The values used must be in descending order except for `-1` and `disabled`. The options for the command `esxcfg-auth --usepamqc=`*`<N0> <N1> <N2> <N3> <N4> <match>`* are:

- *`<N0>`* # of characters required for passwords using one character classes
- *`<N1>`* # of characters required for passwords using two character classes
- *`<N2>`* passphrases
- *`<N3>`* # of characters required for passwords using three character classes
- *`<N4>`* # of characters for passwords using all four character classes
- *`<match>`* # of character allowed to be reused from the old password

Note: When the `esxcfg-auth --usepamqc` command sets `pam_passwdqc.so` as the complexity control, the `pam_cracklib.so` plug-in is disabled, as is the 3-attempts control.

Audit:
Verify password complexity is enabled:

```
grep -i '^password[[:space:]]\+required[[:space:]]\+/lib/security/\$ISA/pam_passwdqc.so'
/etc/pam.d/system-auth-generic
```

If no text string is displayed, the complexity is not set. If the text string is displayed, verify the parameters meet the complexity requirements above.

1.10.6Strengthen Password Controls – Maximum Days (Level 1, Scorable)

Description:
Set the *maximum* number of days before a password is required to be changed to

- Less than or equal to 90 days.

Rationale:
Minimizing the life of a credential reduces the likelihood that the password will become compromised.

Remediation:
Log on to the service console, acquire `root` privileges and perform the following:

1. Set the maximum password life in days in `/etc/login.defs` to less than or equal to `90` days.

```
esxcfg-auth –passmaxdays=90
```

Note: The above command will not reset the remaining days in any existing user accounts. Therefore, if an account had more days remaining than the new standard, they retain those extra days of password life. The change above will be effective at the next time a new password is changed. Administrators should force service console users (with the appropriate advance communication) to change their password at the next login with the command below, thus implementing the new maximum standard.

2. Set a number of days since password was last changed **for each user account**.

```
chage –d 0 <useraccount>
```

Audit:

1. Verify the password maximum life setting is set to less than 90 days by running the following:

```
#!/bin/sh
# Audit password maximum life setting is less than or equal to 90
#
printf "Auditing the maximum number of days a password may be used is less
than or equal to 90 days...\n"

if [ `grep -i –c "^pass_max_days" /etc/login.defs` -eq 1 ]; then
  if [ `grep -i "^ pass_max_days” /etc/login.defs | awk '{print $2}'` -le 90
]; then
    printf "Password minimum life setting correctly configured.\n"
  else
    printf "Password minimum life setting incorrectly configured.\n"
    exit 1
  fi
```

```
else
  exit
fi
```

1.10.7Strengthen Password Controls – Minimum Days (Level 1, Scorable)

Description:
Set the ***minimum*** number of days a password must exist before it can be changed to:

- Greater than or equal to 7 days.

Rationale:
Combined with the password history setting, the minimum days setting will cause multiple days to transpire before a user can return to a favorite password, discouraging password reuse.

Remediation:
Log on to the service console; acquire `root` privileges and perform the following:

1. Set the minimum password life in days in `/etc/login.defs` to greater than or equal to 7 days.

```
esxcfg-auth –passmindays=7
```

Audit:
1. Verify the password minimum life setting, is set to greater than or equal to 7 days by running the following:

```
#!/bin/sh
# Audit password minimum life setting is greater than or equal to 7
#
printf "Auditing the minimum number of days allowed between password changes
is greater than or equal to 7 days...\n"

if [ `grep -i -c "^pass_min_days" /etc/login.defs` -eq 1 ]; then
  if [ `grep -i "^pass_min_days" /etc/login.defs | awk '{print $2}'` -ge 7 ];
then
    printf "Audit passed: Password minimum life setting correctly
configured.\n"
  else
    printf "Audit failed: Password minimum life setting.\n"
    exit 1
  fi
else
  printf "Audit failed: Password minimum life setting.\n"
  exit 1
fi
```

1.10.8Strengthen Password Controls – Length (Level 1, Scorable)

Description:
Set the minimum required number of characters the password ***length*** must be to:

- Greater than or equal to 8 characters (12 if only three out of the four character sets are required).

Note: `esxcfg-auth –passminlen` command option has been removed from ESX 4

Rationale:
The longer the password length the more iterations password guessing technique must process to determine the credential.

Remediation:
Use the pam quality parameters discussed above to set the minimum length for the three and four classes of characters that comprise the password. Use the command below to set the minimum password length in characters

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

Audit:
Verify the password minimum length setting is greater than 8 characters, (12 for the use of three character sets) by reviewing the output of the command below for the fourth and fifth parameters:

```
grep -i '^password[[:space:]]\+required[[:space:]]\+/lib/security/\$ISA/pam_passwdqc.so'
/etc/pam.d/system-auth-generic
```

1.10.9Ensure Host Direct Web Access is Disabled (level 1, Scorable)

Description:
The default setting of vSphere host web access should be retained. This access level allows only the display of the welcome screen with a link to download VMware Infrastructure client and links to VMware sites, but provides no host or guest management functionality.

Rationale:
The weaknesses of the http protocol and related browsers should be exposed as little as possible on the host. Administrator's logins and related traffic are better directed to other more secure access tools and protocols such as VMware infrastructure client and SSH.

Remediation:
The default setting of the service `vmware-webAccess` should remain off. If the service has been turned on, use the command below to set the service to not start at boot.

```
chkconfig –level 12345 vmware-webAccess off
```

Audit:
Observe the output from the command below and ensure the service is off for all run levels.

```
chkconfig --list vmware-webAccess
```

1.10.10 ESX User Accounts Not Synchronized (Level 1,Not Scorable)

Description:
User accounts on the ESX host and the vCenter management server are not synchronized in an automated fashion.

Rationale:
When changes or deletions are required in system administration staff, making alterations on one platform may not completely accomplish the desired result.

Remediation:
When removing or changing access rights of administrative users, procedures must be in place to determine the need for removal or changes the user's access levels of these types of accounts in both the ESX host and the vCenter server.

Audit:
Compare a listing of host users from `/etc/passwd`, a listing of users on the vCenter server to their responsibilities within the IT organization for appropriateness.

1.10.11 Use vCenter and vSphere Client for Administration (Level 1, Not Scorable)

Description:
The vendor supplied tools, vCenter, Command Line Interfaces (CLI) and the VIC directly accessing the host should be used for making changes on the host rather than commands run on the COS whenever possible.

Rationale:
Vendor designed panels in the tools provide a consistent interface for making changes, and provide information on other items related to the current change being made, all help reduce the chance of error.

Remediation:
Procedural documentation should require the use of vendor tools when making host changes and documented, approved exceptions when these tools cannot be used.

Audit:
Event log files can be sampled for items that may be compared to the change control documentation to verify methods used, both exception or pre-approved, to make the change were appropriate for that modification type.

1.10.12 Use Directory Service Authentication (Level 1, Scorable)

Description:
Use a central repository of authentication controls to the grant access to the host.

Rationale:
Host users, usually system administrators, access a variety of machines and applications in addition to the ESX host. Centralizing the authentication process provides for a consistent application of the organization's policies regarding credentials and user management.

Remediation:

After user accounts are created on the host, limited to a small group of host administrators, configure the host to use a directory service each time those users wish to access the host. Use the command below to set the `vmware-auth` service to use a directory service to authenticate users logging in to the host.

```
esxcfg-auth –enabled –addomain=<yourdomain>.com   \
–addc=<yourdomaincontroller>.<yourdomain>.com
```

Audit:
Verify the use of a directory service is enabled and the correct domain and directory controller are specified to the `vmware-auth` service by examining the `[realms]` section of the output of the command below.

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

References or Notes:
VMware *Enabling Active Directory Authentication with ESX Server*
Available: http://vmware.com/pdf/esx3_esxcfg_auth_tn.pdf

1.10.13 Use vCenter Automatic Password Change for vpxuser (Level 1, Scorable)

Description:
The password maximum days set on the host for the `vpxuser` account should be set to a value greater than or equal to the days provided in vCenter for automatically changing the password for `vpxuser`.

Rationale:
If the host has a shorter password maximum life set with esxcfg-auth, than the vCenter password autochange value, the vpxuser account could get locked out resulting in a denial of access to vCenter to help manage the host. The vpxuser account would then have to be unlocked from the host console to allow vCenter access to manage the host.

Remediation:
If the host password maximum days, which is compliant with your organization's policy, is shorter than the vCenter automatic change value, contact VMware support for instructions on how to edit the vpxd.cfg file on the vCenter server to set the `VirtualCenter.VimPasswordExpirationInDays` key value to the correct amount.

Audit:
To determine the current vCenter setting:

1. In vCenter, select the host in the navigator panel on the left that you wish to change the VIM password life
2. click on the name menu item "Administration"
3. select "vCenter Server Settings" from the drop down menu
4. from the list on the left, select the last choice "Advanced Settings"

5. from the list on the right, that is in alphabetical order, scroll down until you reach the Key field named `VirtualCenter.VimPasswordExpirationInDays` to read the current setting

To determine the current host setting run the following command:

```
grep -i "^pass_max_days" /etc/login.defs | awk '{print $2}'
```

If compliant, the first value will be less than or equal to the second value, and both values will be less than or equal to organization policy.

1.10.14 Require Authentication for Single User Mode (Level 1, Scorable)

Description:
Change the default installation boot configuration of the host to disallow the ability to boot into single user mode.

Rationale:
The single user boot mode, which is permitted in the default installation of the host, allows whoever enters this mode at the console to have root privileges without having to login and authenticate as root. Since the default installation also does not require a boot loader password (grub), anyone with console access to the host can edit to boot loader to direct the host to boot to the single user mode gaining escalated privileges. (see also 1.12.1 to configure a boot loader [grub] password)

Remediation:
To require a login with appropriate credentials at the single user mode boot levels, add the following line to the file `/etc/inittab`:

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

Audit:
Run the following command and if the output repeats the search string the correct command is included in `/etc/inittab` to require authentication for the single user mode, if the result is empty the configuration fails.

```
 grep ~~:S:wait:/sbin/sulogin /etc/inittab
```

1.10.15 Disable Console Root Login (Level 1, Scorable)

Description:
Root logins from the console, both attached and remote consoles, should be removed.

Rationale:
Removing `root` login from the console requires administrators to first identify and authenticate with their personal account, then use `sudo` to perform administrative functions. The will enhance accountability because of the logging performed by `sudo`.

Note: the configuration mentioned in this section will not mitigate the vulnerability described in section 1.4.14 related to booting into the single user mode.

Remediation:
At least one, or more as appropriate for their duties, user other than root must be created.

```
useradd <newuser>
```

That user(s) must be added to the wheel group.

```
usermod –G10 <newuser>
```

The wheel group must be activated.

```
visudo
i                        (to insert)
delete the # in front of the command line: # %wheel ALL=(ALL) ALL
press the escape key, then the “:wq” keys and hit enter to save the change
```

Finally, the sources from where root can log into can be removed (but retain the empty file).

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

Audit:
Verify the wheel group is active by reviewing the output of the command used in 1.4.2 for the presence of an uncommented line `%wheel ALL=(ALL) ALL`.

```
cat /etc/sudoers
```

Verify the appropriate users are members of the wheel group.

```
grep wheel /etc/group
```

Verify the locations from where root can login from are empty, the following command should produce empty results (`vc/1, vc/2`... and `tty1, tty2`,... entries should not be present)

```
cat /etc/securetty
```

1.11 Service Console/Hypervisor - Logging

1.11.1Establish Log Sizes and Compression (Level 1, Scorable)

Description:
Increase the file size to 2096K and enable compression for the log files `vmkwarning`, `vmkernel` and `vmksummary`.

Rationale:
The larger the log file the more events will be captured to help research system performance or security issues. Compression will allow more events to be captured in the file space provided. With the default history of 36 logs, the each set of log files will require just under 80 megabytes of storage.

Remediation:
Log on to the service console, acquire `root` privileges and perform the following:

1. Perform the following actions to configure global log compression and rotation:

    a. Change to the `/etc` directory

    b. Open `/etc/logrotate.conf` file with an editor

    c. Uncomment the `compress` token to enable the global log compression, remove the `#` (pound sign). If the `compress` token is absent, add it.

    d. Save the updated `logrotate.conf` file.

2. After host compression is enabled above, perform the following actions to set compression and log size for the two files `/etc/logrotate.d/vmkernel` and `/etc/logrotate.d/vmksummary` :

    a. Change to the `/etc/logrotate.d` directory

    b. Open `vmkernel` with an editor

    c. Change the `nocompress` option to `compress`. If it is absent, add it.

    d. Change the `size` token to `2096K`. If it is absent, add and set it.

    e. Save the updated `vmkernel` file.

    f. Open `vmksummary.`

    g. Change the `nocompress` option to `compress`. If it is absent, add it.

    h. Change the `size` token to `2096K`. If it is absent, add and set it.

    i. Save the updated `vmksummary` file.

3. Perform the following actions to set compression and log size for the file `/etc/logrotate.d/vmkwarning`:

    a. Change to the `/etc/logrotate.d` directory
    b. Open `vmkwarning`
    c. Add the `compress` option.
    d. Add the `size` token `2096K`.
    e. Save the updated `vmkwarning` file.

Audit:
The global settings for logging of host events is located in the `/etc/logrotate.conf` and individual settings for each log type (kernel, summary, warning) are located in separate files in the `/etc/logrotate.d/` directory. (For configuring and assessing guest event logging in the `/vmfs/volumes/` directory see section 1.11.4)

1. Verify host global settings for compression is enabled.

```
grep compress /etc/logrotate.conf
```

   If the command above yields no output then compression is not configured as recommended.

2. Review each of the log file's separate configuration files located in the `/etc/logrotate.d` directory to evaluate the presence of compression and the log size with the following command:

```
cat /etc/logrotate.d/<logfilename> | grep -E '(compress|size)'
```

   If the above command does not yield two lines, one for `compression` and another for `size`, then `logrotate` is not configured as recommended.

1.11.2 Review Logs (Level 1, Not Scorable)

Description:
Establish procedures defining the timing of and the staff responsibility for log reviews.

Note:
Host logs such as those mentioned in section 1.5.1 and messages, secure, and any log files in the `/var/log/vmware/` directory, and guest logs stored on the host in `/vmfs/volumes/<yourstoragedevice> /<yourguest>`, and vCenter logs (if in use) may help provide additional research sources related to ESX host analysis.

Rationale:
Reviewing logs in a timely manner may detect a performance or security issue in its early stages enabling the organization to take countermeasures to reduce the event's impact.

Remediation:
Establish documented review procedures for the logs listed above including: frequency, staff accountability, content to alert upon, escalation and communication, integration with other security information management tools and any other procedures.

Audit:
Review the documented procedure and verify those procedures for the logs listed above were implemented through interviews and review of procedural records that the following are working as intended including: frequency of the review with sign-offs, correct staff are performing the review from a confidentiality standpoint and the ability and authority to take appropriate action, action escalation and communication commensurate with the content of the alert, accurate hand-off of data to other security information management tools and any other procedures.

1.11.3 Configure syslogd to Send Logs to a Remote LogHost (Level 1, Scorable)

Description:
Configure `syslogd` to send a copy of ESX host logs to a separate hardened host.

Rationale:
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 a copy of the logs is stored off the machine that cannot be accessed with the compromised host's credentials, those logs can be analyzed for anomalies and used for prosecuting the attacker.

Remediation:
Log on to the service console; acquire `root` privileges and perform the following:

1. Perform the following actions to configure logging:

    a. Change to the `/etc` directory.

    b. Open `syslog.conf` with an editor

    c. Add the name of your log server(s) preceded by an ampersand (`@<yourlogserver1>`) to the end of each line that identifies a log file in the `/etc/syslog.conf` file.

    d. Save the updated `syslog.conf` file.

2. Perform the following actions to allow syslog traffic through the firewall, open the standard port with the commands below:

```
esxcfg-firewall -o 514,udp,out,syslog
esxcfg-firewall -l
```

Note: Syslog is one service ESX firewall does not have built-in when all known services are listed with the `esxcfg-firewall -s` command.

Audit:

1. Execute the following command to identify logging facilities that are not configured to send log entries to an authorized log server. If this command yields any output then syslog is not configured as recommended.

```
grep -Ev '(^#|<yourlogserver1>|<yourlogserver2>)' /etc/syslog.conf
```

2. Execute the following command to determine if your authorized syslog servers are configured. If this command does not yield any output then syslog is not configured as recommended.

```
grep -E '(<yourlogserver1>|<yourlogserver2>)' /etc/syslog.conf
```

3. The output of the command below will list of ports and related services that are controlled by the firewall as a known service and configurable by vCenter. The syslog service manually added above and not controlled by vCenter, should appear in the “Opened ports” section at the end of the list.

```
esxcfg-firewall -q
```

1.12 Networking – vSwitch and PortGroup

1.12.1 Protect Against MAC Address Spoofing (Level 1, Scorable)

Description:
Change the setting to `Reject` for the settings MAC Address Changes for virtual switches and PortGroups.

Note: The default setting is `accept` in virtual switches and in PortGroups for MAC Address Changes.

Rationale:
This setting provides the ability to not execute requests to alter a guest’s MAC address from the initial MAC address.

Remediation:

1. Perform the following actions in vCenter to set the MAC address spoofing setting from the default configuration of `Accept` (saved as `true` in the configuration files) to `Reject` (saved as `false` in the configuration files) using vCenter as follows:

    a. Select the <*host*> in the navigation panel,

    b. Select the `Configuration Tab` and click on the `Networking` link, this will display a listing of the vSwitches, port groups, physical NICs and the guest association.

    c. For each virtual switch, click on the `properties` link:

    d. In the `vSwitch` panel select each *vSwitch* or a *PortGroup* that needs modification.

    e. Click on the `Edit` button.

    f. Click on the `Security` tab.

   Note: The properties of the VSwitch are inherited by the PortGroup unless overridden in the PortGroup settings.

   g. Drop down the selector next to "MAC Address Changes:" and choose `Reject` instead of `Accept`.

2. Alternatively, change vSwitch, and all the PortGroups within that vSwitch, security policy settings at the command line using the `vimsh` command below:

```
vmware-vim-cmd hostscv/net/vswitch_setpolicy --securepolicy-macchange=false
<yourvswitch>
```

Audit:

1. In vCenter:

   a. Select the <*host*> in the navigation panel,

   b. Select the `Configuration Tab` and click on the `Networking` link, this will display a listing of the vswitches, port groups, physical NICs and the guest association.

   c. For each virtual switch, click on the `properties` link:

   d. In the vSwitch properties panel, select each vSwitch and PortGroup and review the "MAC Address Changes:" setting for the value `Reject` noting any settings of `Accept` for correction.

1.12.2 Protect Against Forged Transmits (Level 1, Scorable)

Description:
Change the flags to `Reject` for the settings Forged Transmits for virtual switches and PortGroups.

Note: The default setting is `accept` in virtual switches and in PortGroups for Forged Transmits.

Rationale:
This setting provides the ability to compare incoming and outgoing guest network packets guest MAC address in a packet to the initial MAC address specified in the guest configuration file (`.vmx`). If the MAC addresses differ, the packet is dropped with the `Reject` setting.

Remediation:

1. Perform the following actions in vCenter to set the forged transmits setting from the default configuration of `Accept` (saved as `true` in the configuration files) to `Reject` (saved as `false` in the configuration files) using vCenter as follows:

   a. Select the <*host*> in the navigation panel,

   b. Select the `Configuration Tab` and click on the `Networking` link, this will display a listing of the vswitches, port groups, physical NICs and the guest association.

c. For each virtual switch, click on the `properties` link:

d. In the `vSwitch` panel select each *vSwitch* or a *PortGroup* that needs modification.

e. Click on the `Edit` button.

f. Click on the `Security` tab.

Note: The properties of the VSwitch are inherited by the PortGroup unless overridden in the PortGroup settings.

g. Drop down the selector next to "Forged Transmits:" and choose `Reject` instead of `Accept`.

2. Alternatively, change vSwitch, and all the PortGroups within that vSwitch, security policy settings at the command line using the `vimsh` command below, replacing the [OPTIONS] with:

```
vmware-vim-cmd hostscv/net/vswitch_setpolicy --securepolicy-forgedxmit=false
<yourvswitch>
```

Audit:

1. In vCenter:

a. Select the <*host*> in the navigation panel,

b. Select the `Configuration Tab` and click on the `Networking` link, this will display a listing of the vswitches, port groups, physical NICs and the guest association.

c. For each virtual switch, click on the `properties` link:

d. In the vSwitch properties panel, select each vSwitch and PortGroup and review the "Forged Transmits:" setting for the value `Reject` noting any settings of `Accept` for correction.

1.12.3Protect Against Promiscuous Mode (Level 1, Scorable)

Description:
Ensure the `Reject` default setting for promiscuous mode has not been modified for virtual switches and PortGroups.

Rationale:
The `Accept` setting provide the ability guests utilizing that PortGroup or vSwitch to inspect packets not intended for that guest. For any security software in a guest that needs promiscuous mode to perform its monitoring function, ensure the guests utilizing the promiscuous PortGroup or vSwitch are authorized exceptions and the `Accept` setting is reflected in the approved and documented change control process.

Remediation:

1. If an approved authorized exception is needed for a guest functioning as a security device, perform the following actions in vCenter to change the Promiscuous Mode setting from the default configuration of `Reject` (saved as false in the configuration files) to `Accept` (saved as `true` in the configuration files) using vCenter as follows:

    a. Select the <*host*> in the navigation panel,

    b. Select the `Configuration Tab` and click on the `Networking` link, this will display a listing of the vSwitches, port groups, physical NICs and the guest association.

    c. For each virtual switch, click on the `properties` link:

    d. In the `vSwitch` panel select each *vSwitch* or a *PortGroup* that needs modification.

    e. Click on the `Edit` button.

    f. Click on the `Security` tab.

    Note: The properties of the VSwitch are inherited by the PortGroup unless overridden in the PortGroup settings.

    g. Drop down the selector next to "Promiscuous Mode:" and choose `Accept` instead of `Reject`.

2. Alternatively, change vSwitch, and all the PortGroups within that vSwitch, security policy settings at the command line using the `vimsh` command below, replacing the [OPTIONS] with `--securepolicy-promisc=true:`

```
vmware-vim-cmd hostscv/net/vswitch_setpolicy --securepolicy-promisc=true <yourvswitch>
```

Audit:

1. In vCenter:
    a. Select the <*host*> in the navigation panel,
    b. Select the `Configuration Tab` and click on the `Networking` link, this will display a listing of the vswitches, port groups, physical NICs and the guest association.
    c. For each virtual switch, click on the `properties` link:
    d. In the vSwitch properties panel, select each vSwitch and PortGroup and review the Promiscuous Mode setting for the value `Reject` noting any settings of `Accept` for correction. If there are any settings of Accept, compare the related guests to the approved security list.

1.13 Networking –Firewall

1.13.1 Configure the Firewall to Allow Only Authorized Traffic (Level 1, Not Scorable)

Description:

Configure the built-in firewall to ensure only authorized ports and related network traffic sources are allowed to and from the ESX host.

Note: In vCenter the known services can be managed along with their port numbers per the list below. However, firewall rules can be set outside of vCenter to enable services and ports that will not be displayed in vCenter (see section 1.5.3 regarding the syslogd service). Also, some services managed by vCenter will vary based on ESX host product levels (for example faultTolerance).

```
activeDirectorKerberos  caARCserve              CIMHttpServer
CIMHttpsServer          CIMSLP                  commvaultDynamic
commvaultStatic         esxupdate               faultTolerance
ftpClient               ftpServer               httpClient
kerberos                LDAP                    LDAPS
legatoNetWorker         nfsClient               nisClient
ntpClient               smbClient               snmpd
sshClient               sshServer               swISCSIClient
symantecBackupExec      symantecNetBackup       telnetClient
TSM   (TivoliStorage)   updateManager           VCB
vncServer               vpxHeartbeats           webAccess
```

Rationale:
If the firewall has not started or if unauthorized ports are opened to the ESX host by a firewall change, traffic containing disruptive or malicious payloads may negatively impact the host's performance or security

Remediation:

1. Using vCenter:

   a. Selecting the <*host*> in the navigation panel.

   b. Selecting the `Configuration Tab` and click on `Security Profile`.

   c. Select the `Properties` link.

   d. Navigate to the `Remote Access` panel.

   e. Check to enable or uncheck to disable the boxes in front of the services to allow or block related ports in the firewall based on the recommended services in the figure above.

Alternatively:
Log on to the service console; acquire `root` privileges and perform the following:

1. Enable known services defined in the list above by configuring the firewall.

```
esxcfg-firewall –e <servicename>
```

2. Disable known services not defined in the figure above by configuring the firewall.

```
esxcfg-firewall –d <servicename>
```

3. If the service you wish to enable is not on the `esxcfg-firewall` list above (`esxcfg-firewall -s`), it can be enabled with the open parameter of the command as shown below for example for syslogd services (see also section 1.5.3) that are not one of the predefined services.

```
# Example:  esxcfg-firewall -o 514,udp,out,syslog
```

Audit:

1. In vCenter:
   a. Selecting the *<host>* in the navigation panel.
   b. Selecting the `Configuration Tab` and click on `Security Profile.`
   c. Select the `Properties` link.
   d. Navigate to the `Remote Access` panel.
   e. Review the listing of incoming and outgoing connections with their related ports and compare that list to the list in the recommended services defined in the figure above.

There is also a host configuration file for the firewall at `/etc/sysconfig/iptables-config`. The settings in this file mostly relate to saving of rules and the eight settings are listed below with their default values. If any of these lines have been removed or their settings altered, they should be matched with the organization's change control documentation.

```
IPTABLES_MODULES=""
IPTABLES_MODULES_UNLOAD="yes"
IPTABLES_SAVE_ON_STOP="no"
IPTABLES_SAVE_ON_RESTART="no"
IPTABLES_SAVE_COUNTER="no”
IPTABLES_STATUS_NUMERIC="yes"
IPTABLES_STATUS_VERBOSE="no"
IPTABLES_STATUS_LINENUMBERS="yes"
```

```
grep -v ^# /etc/sysconfig/iptables-config
```

There is also a configuration file for IPV6 `iptables` at `/etc/sysconfig/ip6tables-config`. The same 8 settings are present with the same 8 default values. If IPV6 is in use, verify the settings in this file also match the defaults or match authorized change control documentation.

Vendor supplied commands can be used to assess the status of those services that have been pre-defined by the vendor. The first command (`-s`) shows all pre-defined services controlled by the vendor's command `esxcfg-firewall`. The second command shows the status of the service specified.

```
esxcfg-firewall -s
esxcfg-firewall -q <servicename>
```

For a complete listing of all rules employed by the firewall, the command below will identify all traffic rules similar to the output from issuing a `iptables -L` command, including those services not defined in `esxcfg-firewall -s`. For example, the syslog service and port described above will be on the output of the command below, but would not be in the vCenter screens or in the `esxcfg-firewall` command options.

```
esxcfg-firewall -q
```

1.14 Networking – Other

1.14.1 Ensure all Host Browser Sessions are https (Level 1, Scorable)

Description:
By default all browser sessions with the host are initiated with a secure protocol (HTTPS) using SSL.

Rationale:
If this session protection were not used, sensitive authentication or configuration information may be intercepted between the administrator's endpoint and the ESX host.

Remediation:
None, by default SSL is enabled, see the audit section for confirmation.

Audit:
Review the contents of the `/etc/vmware/hostd/config.xml` file between the tags `<ssl> … </ssl>` and ensure the two lines regarding key and certificate storage are present and have not been commented out.

References or Notes: Contained within the above configuration file, are instructions on how to disable SSL.

1.14.2 Ensure there are No Unused PortGroups (Level 1,Scorable)

Description:
Multiple PortGroups (512 per virtual standard switch) and multiple ports (1,016 active ports per host) allow for the flexibility to configure more networking than may be required.

Rationale:
Extra or dormant network objects could lead to errors in deployment and misconnection within the organization's network.

Remediation:
In vCenter for each host in the "Configuration" tab, select all virtual switches, and all PortGroups on each host and compare to the organization's authorized network structure for any extra paths. If any virtual switches or PortGroups need correction, select the "Properties" blue link and remove any unneeded components.

Audit:
In vCenter for each host in the "Configuration" tab, select all virtual switches, and all PortGroups on each host and compare to the organization's authorized network structure for any extra paths.

1.14.3 Avoid PortGroup VLAN Numbering that Conflicts with Native VLANs (Level 1, NonScorable)

Description:

External networking devices handle native traffic that is not on a specified VLAN and may specify a VLAN number, for example "1", to be associated with such traffic. Generally external networking devices do not place a VLAN tag inside the packets on this path. Virtual switch PortGroups can be configured to use the same VLAN number as the external native VLAN number, but will place VLAN tags in the packet.

Rationale:
If VLAN numbers internally in a vSwitch PortGroup, conflict with the external switch native VLAN numbers, the mixture of tagged and un-tagged packets will not be delivered.

Remediation:
Review the configuration of external switches that are connected to an uplink from a virtual switch and note that external VLAN number used for native traffic. In vCenter for each host, from the "Configuration" tab, select "Networking" link ion the "Hardware" section. For each vSwitch, select the "Properties" link. in the "<yourvswitch> Properties" panel select each PortGroup and review the number (if any) next to "VLAN ID:". If that number conflicts with the external native VLAN number, click on the "Edit" button at the bottom to make changes.

Audit:
Perform the same steps as in the remediation section stopping at the "Edit" step.

1.14.4 Match vSwitch VLANs to Physical Switch Port Trunk VLANs (Level 1, NonScorable)

Description:
There is no mechanism to automatically synchronize numbering of VLANs inside virtual switch PortGroups, with VLAN numbers configured on external physical switches trunk ports.

Rationale:
If internal PortGroup VLAN numbers are not configured with the same VLAN numbers on the linked external physical switch, traffic may not get routed. If extra VLANs are available on the external physical switch, connections may be made to paths that are not of the intended risk or security classification.

Remediation:
Review the configuration of external switches that are connected to an uplink from a virtual switch and note that external VLAN numbers configured to the trunk port.. In vCenter for each host, from the "Configuration" tab, select "Networking" link ion the "Hardware" section. For each vSwitch, select the "Properties" link in the "*<yourvswitch>* Properties" panel select each PortGroup and review the number (if any) next to "VLAN ID:". The VLAN numbers from all of the PortGroups should exactly match the list of VLANs configured on the external switch trunk port where the vSwitch uplinks.

If the two VLAN number lists are not exactly equal, assuming the internal virtual VLAN list is correct, see the external physical switch vendor documentation on how to increase or decrease the VLAN numbers associated with the trunk port to which this vSwitch uplinks.

Audit:
Perform the same steps as in the remediation section stopping at the end of the first paragraph.

1.15 Storage

1.15.1 Use Bi-directional CHAP to Access iSCSI Devices (Level 1, Scorable)

Description:
Configure connections to iSCSI storage devices to use the CHAP protocol for both authentication of the target storage devices to the host initiator, and authenticate the host initiator to the storage target.

Rationale:
Use of the CHAP protocol ensures ESX hosts and storage devices are communicating with known endpoints.

Note:
It is also recommended if iSCSI is in use the network segment that iSCSI clear data traffic traverses, also be isolated from the general user network (see section 1.2.1 on how to create a segregated network path).

Remediation:
Perform the following to enable CHAP in vCenter:

1. Select the <*host*> from inventory.
2. Select the `Configuration` tab.
3. Then select the `Storage Adapters` in the Hardware panel.
4. Chose the <*iSCSI adapter number*> in the blue `Properties` link and in the `iSCSI Initiator Properties` panel
5. In the General tab, Select the `CHAP` button.
6. In the `CHAP Credentials` panel.
7. Enter the `CHAP Credentials` (the host authenticates to the storage target)
8. Enter the `Mutual CHAP Credentials` (the storage target authenticates to the host) and click OK

Audit:
1. Verify CHAP authentication is enabled by executing the following command.

```
vmware-vim-cmd hostsvc/storage/info | grep chap
```

2. If the `chapAuthEnabled` value is set to `false`, the host does not have CHAP enabled and fails this requirement.

1.15.2 Do Not Include vmkernel on a iSCSI vSwitch (Level 1, Scorable)

Description:

Do not add a Service Console network PortGroup to the vSwitch communicating with the iSCSI storage.

Rationale:
In prior versions of the ESX host, the vSwitch handling iSCSI traffic, which by default was the PortGroup `VMkernel` that handled data traffic, also needed to have a `Service Console` PortGroup on the same vSwitch to handle messaging traffic between the host and the storage device. With ESX 4 all traffic types can be handled by the `VMkernel` PortGroup. Removing the second `Service Console` PortGroup removes an unneeded path into the COS.

Remediation:
If a vSwitch designed to handle iSCSI traffic has a Service Console PortGroup, in vCenter:

1. In vCenter, select the host, and click on the `Configuration` tab
2. Select `Networking` from the hardware list
3. Scroll to the vSwitch handling the iSCSI traffic, if that vSwitch has unneeded PortGroups, select `Properties`
4. On the left, select the unneeded PortGroup
5. Click on the `Remove` button at the bottom

Audit:
Use steps 1. through 3. in this section's **Remediation** content and compare PortGroups listed with this sections requirements.

1.15.3Unique CHAP Secret for Each Host (Level 1, Scorable)

Description:
The secret used by the host to authenticate itself to the iSCSI target should be different for each host.

Rationale:
If the password were known to other hosts, those hosts could impersonate the correct host and possibly gain unauthorized access to data.

Remediation:
Build procedures for setting up hosts should include instructions not to use a common secret for Chap authentication.

Audit:
This cannot be tested without compromising the secret, the cryptograms are masked with a string of "X"s when retrieved with the following command.

```
vim-cmd hostsvc/storage/info | grep Secret
```

1.15.4 Disable Managed Object Browser (Level 1, Scorable)

Description:

The Managed Object Browser enumerates the VMware Web Services System Development Kit (SDK) inventory using a browser. Resources, objects, and settings related to a host can be viewed and possibly changed with this tool.

Rationale:
Using this browser tool does not enforce the roles and access controls present when using the vCenter Server with the VI Client.

Remediation:
Log in to the ESX service console and backup the `proxy.xml` configuration file located in the `/etc/vmware/hostd` directory.

```
cp /etc/vmware/hostd/proxy.xml /etc/vmware/hostd/proxy.xml.old
```

Edit the file `/etc/vmware/hostd/proxy.xml` with the vi editor. Reduce the length value `<_length>10</length>` on line three of the file by 1 (default value is ten, if no other modifications have been made, the new value will be 9).

```
vi /etc/vmware/hostd/proxy.xml
i
<_length>9</length>
```

Comment out the section of the file related to the tags `<e id=”3”>` and `</e>`, unless the file has been modified the id will equal 3 and the lines will look like the following after the edit:

```
<!–
   <e id="3">
      <_type>vim.ProxyService.NamedPipeServiceSpec</_type>
      <accessMode>httpsWithRedirect</accessMode>
      <pipeName>/var/run/vmware/proxy-mob</pipeName>
      <serverNamespace>/mob</serverNamespace>
    </e>
 -->

*** while in the editor, also decrement each succeeding <e id=”n”>  by 1 ***
```

When saving the file, place the override symbol “`!`” after `:wq` when exiting the editor since this is a read-only file.

Restart management services for the change to take effect.

```
service  mgmt-vmware restart
service  vmware-vpxa restart
```

Note: A separate benchmark will be developed for vCenter. vCenter also has managed object browser capability that should be disabled for the same reasons it is on the host. To change the setting on the vCenter server, the `vpxd.cfg` file is located on the VMware vCenter Server by default at:

```
%ALLUSERPROFILE%\Application Data\VMware\VMware VirtualCenter\vpxd.cfg
```

- On Windows Server 2008, this would generally be `C:\ProgramData\VMware\VMware VirtualCenter\vpxd.cfg`

- On Windows Server 2003, this would generally be `C:\Documents and Settings\All Users\Application Data\VMware\VMware VirtualCenter\vpxd.cfg`

Using Wordpad or another editor, add the following line to the file `vpxd.cfg`, between the tags `<vpxd>` and `</vpxd>`:

```
<enableDebugBrowse>false<enableDebugBrowse/>
```

Use Windows' `services.msc` program from the vCenter server command line, locate the VMware VirtualCenter Management Webservices service, and chose restart.

Audit:
Open a browser and type in the ESX host address in the URL bar. On the home page in the lower right hand corner click on the link to "Browse objects managed by this host". The result should be a page not found error.

Alternately, review the contents of the `/etc/vmware/hostd/proxy.xml` file on the host for evidence the managed objects browser (mob) section has been commented out and succeeding id's appropriately decremented.

```
cat /etc/vmware/hostd/proxy.xml | more
```

On the vCenter server, use file explorer to navigate to the directory shown above where the file `vpxd.cfg` is located, open that file with an editor and review for the presence of the setting below:

```
<enableDebugBrowse>false<enableDebugBrowse/>
```

1.16 Virtual Machine Settings

1.16.1 Remove Guest Control of Hardware Devices (Level 1, Scorable)

Description:
Do not allow guests to control hardware devices outside of ESX or vCenter.

Rationale:
Guest control of hardware devices could lead to resource conflicts and possible poor performance, or access to unauthorized devices and data stored there.

Remediation:
Perform the following actions using the vCenter management console to set guest control:

1. If running, shut down the virtual machine within the guest using the appropriate procedure.

2. Right click on the <*guest name*> in the navigation tree.

3. Select `Edit Settings`.

4. Select the `Options` tab.

5. Select the `General` line item indented from the `Advanced` line (not the General Options line item).

6. Click on the `Configuration Parameters` button.

   Note: The configuration parameters panel will pop up with each setting listed with a Name and Value pair per line.

7. Add the name value pair below:

```
isolation.device.connectable.disable    true
```

Audit:
Validate the settings in the guest configuration file `(*.vmx)`.

Login to the vCenter management console:

1. Select a *<guest virtual machine>* to assess in the `Inventory` tree.

2. If running, shut down the virtual machine within the guest using the appropriate procedure.

3. Right click on the *<guest virtual machine>* in the navigation tree.

4. Select `Edit Settings`.

5. Select the `Options` tab.

6. Select the `General` line item indented from the `Advanced` line (not the General Options line item).

7. Click on the `Configuration Parameters` button.

   Note: The configuration parameters panel will pop up with each setting listed with a Name and Value pair per line.

8. Review the settings list, if the name / value pair below is not present, the guest fails the test:

```
isolation.device.connectable.disable    true
```

Alternatively, at the command line, each guest's `.vmx` configuration file can be queried for this setting:

```
grep "isolation.device.connectable.disable = \"true\""         \
/vmfs/volumes/<yourstorage>/<yourguest>.vmx
```

1.16.2 Appropriately Size the Information a Guest Can Store in a Configuration File. (Level 1, Scorable)

Description:
ESX 4 has added the ability to limit the amount of data that can be stored in a guest's `vmx` configuration files. The default limit is 1 mb of storage. If your guest has extensive custom configurations and is sending many `setinfo` type messages to the configuration file, the file could become full. Appropriately provide sufficient space for the `vmx` configuration file.

Rationale:
If configuration settings or `setinfo` messages cannot be written to the vm configuration file, the next startup of the guest may be missing components needed for its operation.

Remediation:
After determining the appropriate size for the `vmx` configuration file, if more than 1 mg, perform the following actions using the vCenter management console to size the vmx file

1. If running, shut down the virtual machine from within the guest using the appropriate procedure.
2. Right click on the guest name in the navigation tree.
3. Select `Edit Settings`.
4. Select the `Options` tab.
5. Select the `General` line item indented from the `Advanced` line (not the General Options line item).
6. Click on the `Configuration Parameters` button.

   Note: The configuration parameters panel will pop up with each setting listed with a Name and Value pair per line.

7. While on the configuration parameters pop-up panel, click on the `Add` button and add Name and Value pairs:

```
tools.setinfo.sizeLimit = nnnnnnn      (in bytes)
```

Audit:
Validate the settings in the guest configuration file (`*.vmx`).

Login to the vCenter management console:

1. Select a <*guest virtual machine*> to assess in the Inventory tree.

2. If running, shut down the virtual machine within the guest using the appropriate procedure from within the guest.

3. Right click on the <*guest virtual machine*> name in the navigation tree.

4. Select `Edit Settings`.

5. Select the `Options` tab.

6. Select the `General` line item indented from the `Advanced` line (not the General Options line item).

7. Click on the `Configuration Parameters` button.

   Note: The configuration parameters panel will pop up with each setting listed with a Name and Value pair per line.

8. Review the settings list for an entry of a Name and Value pair per the text below, if the string pair below is not present the guest fails the test. Compare the value shown to the documented build standard for this guest.

```
tools.setinfo.sizeLimit       nnnnnnn             (in bytes)
```

1.16.3Disable Cut and Paste (Level 1, Scorable)

Description:
Disable the ability of data to be cut and paste from the guest to the hosts that is enabled when `vmware-tools` are installed in a guest.

Rationale:
The cut and paste capability provides the ability to place executable files on a destination without logging to trace actions to users.

Remediation:
Perform the following actions using the vCenter management console to set guest control:

1. If running, shut down the virtual machine within the guest using the appropriate procedure.

2. Right click on the <*guest virtual machine*> name in the navigation tree.

3. Select `Edit Settings`.

4. Select the `Options` tab.

5. Select the `General` line item indented from the `Advanced` line (not the General Options line item).

6. Click on the `Configuration Parameters` button.

Note: The configuration parameters panel will pop up with each setting listed with a Name and Value pair per line.

7. While on the configuration parameters pop-up panel, compare each of the three setting shown below to the Value field:

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

Audit:
Validate the settings in the guest configuration file (`*.vmx`).

Login to the vCenter management console:

1. Select a *<guest virtual machine>* to assess in the Inventory tree.

2. If running, shut down the virtual machine within the guest using the appropriate procedure.

3. Right click on the *<guest virtual machine>* name in the navigation tree.

4. Select `Edit Settings`.

5. Select the `Options` tab.

6. Select the `General` line item indented from the `Advanced` line (not the General Options line item).

7. Click on the `Configuration Parameters` button.

   Note: The configuration parameters panel will pop up with each setting listed with a Name and Value pair per line.

8. Review the settings list for an entry of a Name and Value pair for each of the three pairs listed below.

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

1.16.4 Rotate VM Log Files on the Host and Limit Their Size (Level 1, Scorable)

Description:
Set the maximum size of each log file and number of log files to retain in each guest directory under `/vmfs/volumes/<yourstoragedevice>/` to:

- Rotate the current log file when the size is greater than or equal to `10000000` Bytes.

- Retain less than or equal to `30` historical log files.

Rationale:
Limiting the size of the log files will help minimize possible denial of service attacks on log file data-store should they become full.

Remediation:
Perform the following actions using the vCenter management console to set guest control:

1. If running, shut down the virtual machine within the guest using the appropriate procedure.
2. Right click on the *<guest virtual machine>* name in the navigation tree
3. Select `Edit Settings`.
4. Select the `Options` tab.
5. Select the `General` line item indented from the `Advanced` line (not the General Options line item).
6. Click on the `Configuration Parameters` button.

   Note: The configuration parameters panel will pop up with each setting listed with a Name and Value pair per line.

7. While on the configuration parameters pop-up panel, double click on any of the two settings shown below to change the Value field to your organization's standard. If the settings are not present, click on the Add button to create a new Name and Value pair as shown below:

```
log.rotateSize                    10000000
log.keepOld                       30
```

Audit:
Validate the settings in the guest configuration file (`*.vmx`).

Login to the vCenter management console:

1. Select a *<guest virtual machine>* to assess in the `Inventory` tree.
2. If running, shut down the virtual machine within the guest using the appropriate procedure.
3. Right click on the *<guest virtual machine>* name in the navigation tree, select Edit Settings.
4. Select the `Options` tab.
5. Select the `General` line item indented from the `Advanced` line (not the General Options line item).

6. Click on the `Configuration Parameters` button.

   Note: The configuration parameters panel will pop up with each setting listed with a Name and Value pair per line.

7. Review the settings list for an entry of a Name and Value pair per the text below. If both of the string pair settings below are present and the metrics match organization standards, the guest passes the test.

```
log.rotateSize                    10000000
log.keepOld                       30
```

1.16.5 Virtual Machine Communications Interface (VCMI) (Level 1, Not Scorable)

Description:
The Virtual Machine Communications Interface (VMCI) used in VMware virtual hardware version 7 is a virtual Peripheral Component Interconnect (PCI) equivalent socket layer device that allows virtual machines to communicate directly to each other and the ESX host, without the need to traverse the network layer.

Rationale:
Direct communication bypasses traditional network firewalls and monitoring techniques. The default setting of disabled should be retained unless a specific there is an authorized exception.

Remediation:
No action is needed if the default setting has not been altered. If the default setting has been altered:

Login to the vCenter management console:

1. Select a *<guest virtual machine>* to edit in the `Inventory` tree.

2. Right click on the *<guest virtual machine>* name in the navigation tree, select Edit Settings.

3. Read the `VCMI device` line (if not visible, check the “Show All Devices” box in the upper left) the default should read “Restricted” on the right side of the VCMI line.

4. If the right side of the VCMI lines reads “Unrestricted”

5. If running, shut down the virtual machine within the guest using the appropriate procedure.

6. Uncheck the “Enable VCMI Between VMs” box to the right

7. Restart the virtual machine

Audit:
Verify the setting of VCMI using steps 1-4 in the remediation section above.

1.16.6 Prevent Virtual Disk Shrinkage (Level 1, Scorable)

Description:
The installation of VMware Tools within a VM, commonly done to obtain higher performance drivers, also enables disk shrinkage functionality.

Rationale:
If a user inside a VM can access the tools interface, possibly without administrative or root privileges, they may be able to perform a disk shrinkage function that could take the VM off line and create a denial of service situation.

Remediation:
Disable the disk shrinkage functionality of VMware Tools (while leaving the other benefits in place, by editing the VM configuration.

Login to the vCenter management console:

1. Select a *<guest virtual machine>* to assess in the `Inventory` tree.

2. If running, shut down the virtual machine within the guest using the appropriate procedure.

3. Right click on the *<guest virtual machine>* name in the navigation tree, select Edit Settings.

4. Select the `Options` tab.

5. Select the `General` line item indented from the `Advanced` line (not the General Options line item).

6. Click on the `Configuration Parameters` button.

   Note: The configuration parameters panel will pop up with each setting listed with a Name and Value pair per line.

7. Scroll to the end of the list and to add the two new pairs below, click on the "Add Row" button

   ```
   isolation.tools.diskWiper.disable      TRUE
   isolation.tools.diskShrink.disable     TRUE
   ```

8. Click "OK" to approve each pair

9. Click "OK" again to update the VM configuration file

10. Restart the VM

Audit:
Verify the setting of VCMI using steps 1-4 in the remediation section above. Alternatively, review the contents of the VM configuration file (`*.vmx`) for each VM,

```
cat /vmfs/volumes/<yourstorage>/<yourguest>.vmx
```

for the lines:

```
isolation.tools.diskWiper.disable=TRUE
isolation.tools.diskShrink.disable=TRUE
```

1.16.7Set RemoteDisplay.maxConnections to One (Level 1, Scorable)

Description:

The `RemoteDisplay.maxConnections` setting defines the number of remote consoles allowed to simultaneously access a particular virtual machine.

Rationale:

There is no default setting for remote display connections which allows multiple consoles to be open simultaneously. With multiple consoles open, a second user, who may be of a lower access rights group, could observe the actions of an administrator.

Remediation:

Login to the vCenter management console:

1. Select a *<guest virtual machine>* to assess in the `Inventory` tree.
2. If running, shut down the virtual machine within the guest using the appropriate procedure.
3. Right click on the *<guest virtual machine>* name in the navigation tree, select Edit Settings.
4. Select the `Options` tab.
5. Select the `General` line item indented from the `Advanced` line (not the General Options line item).
6. Click on the `Configuration Parameters` button.

   Note: The configuration parameters panel will pop up with each setting listed with a Name and Value pair per line.
7. Scroll to the end of the list and to add the new pair below, click on the "Add Row" button:

   ```
   RemoteDisplay.maxConnections  1
   ```
8. Click "OK" to approve the pair
9. Click "OK" again to update the VM configuration file
10. Restart the VM

Audit:
If the VM is powered off, verify the correct setting use steps 3 through 7 shown in the remediation section and review the contents of the `RemoteDisplay.maxConnections` line.
If the VM is powered on, on the host issue the following command, all on one line, for each VM:

```
grep RemoteDisplay.maxConnections /vmfs/volumes/<datastore>/<vmname>/<vmname>.vmx
```

1.16.8 Disconnect Unneeded Devices (i.e. floppy drive) (Level 1, Not Scorable)

Description:
vSphere has the ability to present a variety of virtual hardware devices to the VM, some of which may not be needed by the VM, either permanently or after initial installation.

Rationale:
Devices not needed are an unnecessary point of entry to the VM and should be removed to reduce access to the VM. Devices that may be removed, depending on the intended use of the VM include serial ports, parallel ports, CD's, USBs and floppy drives.

Remediation:
To add or delete devices available to the VM: first shutdown the guest operating system:

1. Log into vCenter and in the Inventory panel, Hosts and Clusters view, right click on a VM name

2. Select "Edit settings"

3. Within the "Virtual Machine Properties" panel, in the "Hardware" tab review the list of devices for appropriateness

4. If a device that needs to be removed, highlight that device, click on "Remove",

5. Repeat the steps in item 4 for any other devices needing removal

6. Then click on "OK" in the Properties panel to complete the removal of the device(s)

Audit:
Verify the list of devices assigned to a VM by performing steps 1 through 3 in the prior remediation section, this can be done with the VM running or the VM powered off.

1.16.9 Remotely Log VM's with Nonpersistent Disks (Level 1, Scorable)

Description:
VM disks have a configuration option of Independent Mode which is not affected by snapshots. In this mode changes to the VM are discarded when the VM is rebooted or powered off if the Nonpersistent option is selected.

Rationale:
While potentially useful in a development environment, when using VMs in production it is recommended not to use the Independent Nonpersistent Mode. If the Independent Nonpersistent

Mode is required, it is recommended that VM remotely log relevant system events to a external log server, if not, a record of the activity on the VM between reboots or shutdowns will be lost

Remediation:
To change disk options, first shutdown the guest operating system:

1. Log into vCenter and in the Inventory panel, Hosts and Clusters view, right click on a VM name

2. Select "Edit settings"

3. Within the "Virtual Machine Properties" panel, in the "Hardware" tab review the list of disks for appropriateness

4. Highlight the disk, and review the settings in the Mode section on the right

5. If "Independent" mode is appropriate click on the "Persistent" radio button

6. If "Independent" mode is not appropriate, uncheck the box next to "Independent"

7. Repeat the steps in items 4-6 for any additional disks

8. Then click on "OK" in the Properties panel to complete disk configuration

9. If requirements dictate an Independent Nonpersistent disk, then, within the guest, configure copying of the appropriate logs to a remote server with the designated tools

Audit:
Verify the list of devices assigned to a VM by performing steps 1 through 3 in the prior remediation section, this can be done with the VM running or the VM powered off.

Alternatively, search each VM's configuration file for evidence of the independent-nonpersistent mode setting by entering the following at the command line of the host for each VM and the result should contain no output:

```
grep -i independent-nonpersistent        /vmfs/volumes/<yourdatastore>/<yourVM>/<yourVM>.vmx
```

1.16.10 Disable VIX API (Level 1, Scorable)

Description:
The VMware VIX application programming interface allows for control of VM operations (i.e. power-on, power-off, copy files, run programs, and other functions) on the guest containing the VIX tools or another guest.

Rationale:
The functions above should be limited to skilled and trained virtualization administrators and this capability generally does not need to be provided within a VM as sufficient tools (i.e. VI Client to vCenter, vMA, PowerCLI) are available on an administrators workstation outside of a VM for management of VMs.

Remediation:

Disable the ability of a VM to issue commands that may affect itself adversely or other VMs by performing the following:

Login to the vCenter management console:

1. Select a <*guest virtual machine*> to edit in the `Inventory` tree.
2. If running, shut down the virtual machine within the guest using the appropriate procedure.
3. Right click on the powered-off <*guest virtual machine*> name in the navigation tree, select Edit Settings.
4. Select the `Options` tab.
5. Select the `General` line item indented from the `Advanced` line (not the General Options line item).
6. Click on the `Configuration Parameters` button.
7. Click on "`Add Row`" , this will take you to the bottom of the list
8. Enter "`guest.command.enabled`" on the left side of the entry
9. Enter "`FALSE`" on the right side of the entry
10. Click "OK", and "OK" once more to save the entry
11. Restart the VM

Audit:
With the VM powered either on or off:

1. Select a <*guest virtual machine*> to edit in the `Inventory` tree.
2. Right click on the <*guest virtual machine*> name in the navigation tree, select Edit Settings.
3. Select the `Options` tab.
4. Select the `General` line item indented from the `Advanced` line (not the General Options line item).
5. Click on the `Configuration Parameters` button.
6. Scroll to the bottom of the parameters list
7. Review for the presence of a "`guest.command.enabled`" on the left side and a "`FALSE`" on the right side

Alternatively, search each VM's configuration file for evidence of disabling the VIX setting by entering the following at the command line of the host for each VM and the result should contain one line with the setting. If this command returns no results, then run the command again changing the "FALSE" to "TRUE" (not case sensitive) and if you receive one line result with the "TRUE" setting the VM fails this requirement:

```
grep -i guest.command.enabled=FALSE       /vmfs/volumes/<yourdatastore>/<yourVM>/<yourVM>.vmx
```

1.16.11 Disable ESX Host Performance Data Delivery to a VM (Level 1, Scorable)

Description:
Host performance data may be sent to VMs, by default this setting is disabled.

Rationale:
If a VM obtains performance data from the host without an approved purpose, that data may be available to a broader audience than authorized. The host information could be used for footprinting and planning possible future attacks against the host.

Remediation:
Login to the vCenter management console:

1. Select a *<guest virtual machine>* to edit in the `Inventory` tree.
2. If running, shut down the virtual machine within the guest using the appropriate procedure.
3. Right click on the powered-off *<guest virtual machine>* name in the navigation tree, select Edit Settings.
4. Select the `Options` tab.
5. Select the `General` line item indented from the `Advanced` line (not the General Options line item).
6. Click on the `Configuration Parameters` button.
7. Click on "`Add Row`" , this will take you to the bottom of the list
8. Enter "`tools.guestlib.enableHostInfo`" on the left side of the entry
9. Enter "`FALSE`" on the right side of the entry
10. Click "OK", and "OK" once more to save the entry
11. Restart the VM

Audit:
With either the VM powered on or off:

1. Select a *<guest virtual machine>* to edit in the `Inventory` tree.
2. Right click on the *<guest virtual machine>* name in the navigation tree, select Edit Settings.

3. Select the `Options` tab.

4. Select the `General` line item indented from the `Advanced` line (not the General Options line item).

5. Click on the `Configuration Parameters` button.

6. Scroll to the bottom of the parameters list

7. Review for the presence of a "`tools.guestlib.enableHostInfo`" on the left side and a "`FALSE`" on the right side

Alternatively, search each VM's configuration file for evidence of disabling the host data collection setting by entering the following at the command line of the host for each VM and the result should contain one line with the setting. If this command returns no results, then run the command again changing the "FALSE" to "TRUE" (not case sensitive) and if you receive one line result with the "TRUE" setting the VM fails this requirement:

```
grep –i tools.guestlib.enableHostInfo=FALSE
/vmfs/volumes/<yourdatastore>/<yourVM>/<yourVM>.vmx
```

1.17 Other Virtual Machine Considerations

1.17.1 Disable VMsafe, Except for Approved Appliances/Applications (Level 1, Scorable)

Description:
VMsafe allows one VM acting as a security device to inspect CPU/Memory or Networking resource usage of other VMs.

Rationale:
These security devices gather a large volume of information about a VM; much of which is sensitive and should be limited to approved devices. If an unauthorized VMsafe VM were deployed it could gather information about another VM that could lead to data theft or privilege escalation.

Remediation:
VMs acting as a security appliance/application must be expressly defined to VMsafe. For each VM approved to inspect resources on other guests to enable VMsafe:

Login to the vCenter management console:

1. Select a <*guest virtual machine*> to edit in the `Inventory` tree.

2. If running, shut down the virtual machine within the guest using the appropriate procedure.

3. Right click on the powered-off <*guest virtual machine*> name in the navigation tree, select Edit Settings.

4. Select the `Options` tab.

5. Select the `General` line item indented from the `Advanced` line (not the General Options line item).

6. Click on the `Configuration Parameters` button.

7. Click on "`Add Row`" , this will take you to the bottom of the list

8. To enable CPU/Memory introspection:
   a.) Enter "`ethernetX.networkName`" on the left side of the entry where X is the NIC number
   b.) Enter "`VMsafe-appliances`" on the right side of the entry
   c.) Click "`OK`" to approve this entry

9. To enable Network introspection:
   a.) Enter "`ethernetX.networkName`" on the left side of the entry where X is the NIC number
   b.) Enter "`dvfilter-appliances`" on the right side of the entry
   c.) Click "`OK`" to approve this entry

10. Click "`OK`", once more to save the entry

11. Restart the VM

Audit:
With the VM powered either on or off:

1. Select a *<guest virtual machine>* to edit in the `Inventory` tree.

2. Right click on the *<guest virtual machine>* name in the navigation tree, select Edit Settings.

3. Select the `Options` tab.

4. Select the `General` line item indented from the `Advanced` line (not the General Options line item).

5. Click on the `Configuration Parameters` button.

6. Scroll to the bottom of the parameters list

7. For a CPU/Memory appliance, review for the presence of a "`ethernetX.networkName`" on the left side and a "`VMsafe-appliances`" on the right side

8. For a Network appliance, review for the presence of a "`ethernetX.networkName`" on the left side and a "`dvfilter-appliances`" on the right side

9. If either entry, or both appear, compare this VM for appearance on the list of authorized VMsafe appliances

Alternatively, search each VM's configuration file for evidence of monitoring on either introspection channel by entering the following at the command line of the host for each VM and the result should contain one or two lines if the VM is a VMsafe appliance. If one or two lines are present compare this VM to managements approved list of VMsafe appliances.

```
grep –i ‘.networkName=”VMsafe-appliances”|.networkName=”dvfilter-appliances”’
/vmfs/volumes/<yourdatastore>/<yourVM>/<yourVM>.vmx
```

1.17.2 Disable VM Participation in VMsafe Introspection Unless Approved (Level 1,Scorable)

Description:
VMsafe allows one VM acting as a security device to inspect CPU/Memory or Networking resource usage of other VMs.

Rationale:
Any VM that does not meet the requirements for the type of resource usage that is monitored by a VMsafe appliance, should not be monitored by that VMsafe appliance or inappropriate data leakage may occur.

Remediation:
VMs being monitored by a security appliance/application must be expressly configured to pass information to the VMsafe device. For each VM approved to be inspected, activate VMsafe on this monitored VM by:

Login to the vCenter management console:

1. Select a *<guest virtual machine>* to edit in the `Inventory` tree.

2. If running, shut down the virtual machine within the guest using the appropriate procedure.

3. Right click on the powered-off *<guest virtual machine>* name in the navigation tree, select Edit Settings.

4. Select the `Options` tab.

5. Select the `General` line item indented from the `Advanced` line (not the General Options line item).

6. Click on the `Configuration Parameters` button.

7. Click on “`Add Row`” , this will take you to the bottom of the list

8. To enable CPU/Memory introspection of this VM:
   a.) Enter “`VMsafe.enable`” on the left side of the entry
   b.) Enter “`TRUE`” on the right side of the entry

   c.) Enter “`VMsafe.agentAddress`” on the left side of the entry
   d.) Enter “`xxx.xxx.xxx.xxx`” on the right side of the entry representing the IP address of the approved VMsafe monitoring appliance
   e.) Enter “`VMsafe.agentPort`” on the left side of the entry

f.) Enter “xxxxx” on the right side of the entry representing the port number of the approved VMsafe monitoring appliance
g.) Click “OK” to approve these three entries

9. To enable Network introspection of this VM:
   a.) Enter “ethernetX.filterY.name” on the left side of the entry where X is the NIC number Y is the VMsafe path number
   b.) Enter “dv-filterY” on the right side of the entry where Y is the VMsafe path number
   c.) Click “OK” to approve this entry

10. Click “OK”, once more to save the 4 entries

11. Restart the VM

Audit:
With the VM powered either on or off:

1. Select a <*guest virtual machine*> to edit in the Inventory tree.

2. Right click on the <*guest virtual machine*> name in the navigation tree, select Edit Settings.

3. Select the Options tab.

4. Select the General line item indented from the Advanced line (not the General Options line item).

5. Click on the Configuration Parameters button.

6. Scroll to the bottom of the parameters list

7. For a CPU/Memory appliance, review for the presence of a the three entries:
   ```
   VMsafe.enable=”TRUE”
   VMsafe.agentAddress=“xxx.xxx.xxx.xxx”
   VMsafe.agentPort=“xxxxx”
   ```

8. For a Network appliance, review for the presence of a “ethernetX.filterY.name” on the left side and a “dv-filterY” on the right side, where Y is the VMsafe path

9. If any of the 4 entries appear, compare this VM for appearance on the list of authorized VMs intended to be monitored by the particular VMsafe appliance(s)

Alternatively, search each VM’s configuration file for evidence of being monitored on either introspection channel by entering the following at the command line of the host for each VM and the result should contain one or more lines if the VM is being monitored by a VMsafe appliance. If one or more lines are present compare this VM to managements approved list of VMsafe appliances.

```
grep –i ‘VMsafe.enable=”TRUE”|VMsafe.agentAddress|VMsafe.agentPort|dv-filter’
/vmfs/volumes/<yourdatastore>/<yourVM>/<yourVM>.vmx
```

1.17.3 Disable VMDirectPath I/O Devices Unless Approved (Level 1, Scorable)

Description:
VMDiectPath allows a VM to communicate with a qualifying host device, usually storage or network related, without hypervisor involvement. Generally this results in enhanced throughput performance.

Rationale:
Utilizing VMDirectPath, thus bypassing the hypervisor, may reduce the ability of the host to balance loads and resolve contention. Furthermore, certain hypervisor functionality such as VMotion and Distributed Resource Scheduling (DRS) is disabled if VMDirectPath is enabled for a VM, reducing continuity options for any VMs using VMDirectPath.

Remediation:
To configure a VM to utilize VMDirectPath login to the vCenter management console:

1. Select a *<guest virtual machine>* to edit in the `Inventory` tree.
2. If running, shut down the virtual machine within the guest using the appropriate procedure.
3. Right click on the powered-off *<guest virtual machine>* name in the navigation tree, select Edit Settings.
4. Select the `Hardware` tab.
5. Select the desired device, click "Next" and select other settings appropriate for this device, click "OK"
6. Restart the VM

Audit:
With either the VM powered on or off perform steps 1 through 4 above in the remediation section and compare the VMDirectPath enabled devices to the approved list of devices authorized for this VM.

References or Notes:
If none of the VMs supported by a host require VMDirectPath, VMDirectPath can be disabled on the host, then:

1. Select a *<host>* to edit in the `Inventory` tree.
2. If running, shut down all virtual machines supported by this host within the guest using the appropriate procedure.
3. click on the *<host>* name in the navigation tree, select the "Configuration" tab
4. Select the `Advanced Settings` link within the "Hardware" section
5. A list of supported devices appears for enabling or disabling as needed

6. Restart the host

7. Restart the VMs

1.17.4 Ensure Linked Clones are of Equal Security Classification (Level 1, Scorable)

Description:
Using the VMware vSphere Web Services Software Development Kit (SDK) or additional products like Lab Manager, shared or base virtual disks (.VMDK) can be created that contain a common set of operating system and application bytes that are shared between multiple VMs. The VMs then create differential or delta disks containing the content that is unique to them.

Rationale:
A VM using a linked cloned disk will not have unique access to that portion of VM residing on the linked cloned base disk. The resulting information sharing should only take place between machine authorized to do so and of the same security class. Further, VMs using a linked cloned base disk cannot use VMware's High Availability (HA) mirroring, reducing continuity options for affected VMs.

Remediation:
Use Lab Manager or a similar product, or write custom API scripts to create linked clone disks (`vmdk`).

Audit:
Lab Manager uses snapshot methods to create linked clones. Use the following command to locate linked clone VM ID numbers which will be the non-zero digits in the front of the returned file name as "`000000nnn-<yourtemplate>-delta.vmdk`". Then in Lab Manager use the VM ID "nnn" to determine the linked VMs, then review that list for appropriate grouping.

```
find /vmfs/volumes/<lanmangerdirectory>/ -name *delta.vmdk
```

1.17.5 Use Active Directory Authentication with vMA 4.1 (Level 1,Scorable)

Description:
The vSphere Management Assistant (vMA) appliance 4.1 added the capability to authenticate against an active directory server.

Rationale:
In vMA version 4.0 and prior, and in version 4.1 if `adauth` is not used, authentication information is stored locally on the vMA appliance.

Remediation:
To specify a host or vCenter server that is accessed by a vMA appliance specify the adauth method when establishing the connection to the host or vCenter server. In the vMA appliance enter:

```
vifp <youtservername> --authpolicy adauth --username <yourdomain>\\<youruser>
```

Audit:

To determine which authentication mode is used with each host or vCenter server that is connected to a vMA appliance, in the vMA appliance enter:

```
vifp listservers -l
```

Any server listed that does not show "`adauth`" as the last parameter on each line is not using active directory for authentication.

1.17.6 Monitor Thin Provisioned Use to Avoid Storage Over-commitment (Level 1, Scorable)

Description:
Thin disk provisioning consumes storage space when the VM requires that resource. The space is not committed entirely at VM creation. The total of all provisioned disk space can exceed the physical size of the storage device because only the amount actually used by the VM is decremented from the datastore "Free" measurement as shown in vCenter, not the provisioned (higher) amount.

Rationale:
If the total thinly provisioned , but unused, disk space total exceeds the "Free" disk space physically available on a storage device, and enough VM events require additional provisioned space exceeding remaining physical space, VMs could suffer shutdowns.

Remediation:
Monitor uncommitted space potential additional space requests of thinly provisioned VMs. In vCenter server, select each VM and on the "Summary" tab, note the data storage device(s) used by the guest. For each guest, click on the "Refresh Storage Usage" to obtain a current measure of disk consumption. Subtract the "Used Storage" amount from the "Provisioned Storage" amount to obtain the uncommitted storage amount. Add the uncommitted storage amount for each VM per storage device and compare the total per storage device to the "Free" physical storage space shown in the "Datastore" section. Any per-VM total that exceeds the device "Free" value should be reviewed for possible storage capacity additions or VM movement to other devices. Additionally, alarms could be defined to warn of disk overcommitment above certain levels (i.e. 150%) and provisioned space consumption (i.e.75%)

Audit:
To compare uncommitted space requirements with the remaining "Free" physical space, perform the steps shown in the remediation section above. Also, review alarms for appropriate warning before consumption exceeds available space.

1.18 Other

1.18.1Password Protect the Boot Loader (GRUB) (Level 1, Scorable)

Description:
Protect the configuration of the boot loader GRUB, which controls the operating systems used at host startup and parameters used by those operating system to initialize the host.

Rationale:

This loader and its parameters need password protection (see sections 1.4.5 through 1.4.8 for password configuration guidance) to avoid booting from unauthorized operating systems, or the passing of unauthorized parameters to an authorized operating system at startup. The controls suggested in this section also help mitigate the risk of booting the system into the privileged single user mode described in section 1.4.10. The default installation of ESX 4 provides no GRUB password.

Remediation:
To create a GRUB password use the command below to generate a 32 character hash of your chosen password:

```
/sbin/grub-md5-crypt <yourpassword>
```

Open the `/boot/grub/grub.conf` file with an editor and add the 32 character hash by adding the line `password` –md5 <*thehashgeneratedabove*> after the `timeout` line:

```
password –md5 <thehashgeneratedabove>:
```

Audit:
Observe the system administrator during the ESX boot process enter the letter "`e`" to edit the GRUB settings during boot and a request for password should appear. Alternately, review the contents of the `grub.conf` file for the requirement to enter a password to enter the GRUB edit shell.

```
grep password /boot/grub/grub.conf
```

1.18.2 Replace Vendor SSL certificates (Level 1,Not Scorable)

Description:
Replace the certificates used during SSL network encryption from the vendor defaults to a trusted certificate authority, internal or external.

Rationale:
If default self-signed certificates are used, while unique to each server, they create additional exposure to man-in-the-middle attacks without independent verification that the signed certificate's value is valid.

Remediation:
Replacing the default certificates and using your choice of trusted certificate authority, internal and external. Use the vendors guide shown in the reference below and your organizations procedures for certificates, internal or external, to deploy a secure certificate.

Audit:
Review configuration documentation or change control records for evidence the certificates were changed and a trusted authority is in use. Review the contents of the SSL configuration file `/etc/pki/tls/openssl.cnf` for conformance with the organization's standards.

References or Notes:

1. VMware *(2010) ESX Configuration Guide* [Security chapter, Authentication and User Management section, Encryption and Security Certificates for ESX subsection] http://www.vmware.com/pdf/vSphere4/r40_U1/esx_server_config.pdf

2. VMware (2009) Replacing vCenter Server Certificates[also covers ESX 4 and ESXi 4] http://www.vmware.com/pdf/vsp_4_vcserver_certificates.pdf

1.18.3 Configure Security Event Logging (auditd) (Level 1, Not Scorable)

Description:
The security event daemon `auditd`, is enabled at start up on ESX 4 to log actions of users into the file `/var/log/audit/audit.log`. The size and location and other behaviors of this daemon are controlled with parameters in the file `/etc/audit/auditd.conf`. Custom rules specified by your organization can be created in the file `/etc/audit/audit.rules` using the command `auditctl`.

Rationale:
The configuration of the `auditd` daemon should be reviewed to ensure the log file location, actions upon space limits, and other configuration settings are aligned with the organization's policy to avoid the disk being consumed by log entries. Any custom rules should be created to track high risk activities (not captured in other logs) or events generated by specific users to allow for research.

Remediation:
To review or change the `auditd` daemon configuration open the file `/etc/audit/auditd.conf` with an editor and add or change entries such that the configuration agrees with the organization's policy.

To add or change custom rules, use the `auditctl` command to add to the list of the cistom audit rules in `/etc/audit/audit.rules`

Audit:
Verify the configuration of the `auditd` daemon from the output of the command below to the organization's policy.

```
cat /etc/audit/auditd.conf
```

Match the construction of any custom `auditd` rules with the authorizing change control documentation using the output of the following command.

```
auditctl -l
```

Appendix A: References

1. CIS. (2008). *VMWare ESX Server 3.x Benchmark.* Available: http://community.cisecurity.org/download/. Last accessed 1 October 2009.

2. DISA. (20089). *ESX server – Security Technical Implementation Guide*. Available: http://iase.disa.mil/stigs/stig/esx_server_stig_v1r1_final.pdf. Last accessed 1 October 2009.

3. NSA. (2008). *VMWare ESX Server 3 Configuration Guide*. Available: http://www.nsa.gov/ia/_files/support/I733-009R-2008.pdf. Last accessed 1 October.

4. VMWare, Inc. (2009). *Basic System Administration*. Available: http://www.vmware.com/pdf/vi3_35/esx_3/r35/vi3_35_25_admin_guide.pdf. Last accessed 1 October 2009.

5. VMWare, Inc. (2008). *ESX Patch Management Guide*. Available: http://www.vmware.com/pdf/vi3_35/esx_3/r35/vi3_35_25_esxupdate.pdf. Last accessed 1 October 2009.

6. VMWare, Inc. (2009). *ESX Configuration Guide*. Available: http://www.vmware.com/pdf/. Last accessed 1 October 2009.

7. VMWare, Inc. (2009). *ESX Installation Guide, Update 2 and Later*. Available: http://www.vmware.com/pdf/.pdf. Last accessed 1 October 2009.

8. VMWare, Inc. (2009). *Replacing VirtualCenter Server Certificates*. Available: http://www.vmware.com/pdf/vi_vcserver_certificates.pdf. Last access 1 October 2009.

9. VMWare, Inc. (2009). *Security Hardening - VMware Infrastructure 3*. Available: http://www.vmware.com/files/pdf/vi35_security_hardening_wp.pdf. Last accessed 1 October 2009.

10. VMWare, Inc. (2009). *VMware Update Manager Administration Guide*. Available: http://www.vmware.com/pdf/vi3_vum_10_admin_guide.pdf.

11. VMware Knowledgebase article on NTP: http://kb.vmware.com/kb/1339. Last accessed 1 October 2009.

12. VMware Support Center -Download Patches: https://www.vmware.com/mysupport/download/. Last accessed 1 October 2009. Guidance on the configuration of SUDO see the main page for the software provider. Available: http://www.gratisoft.us/sudo/. Last accessed 1 October 2009

13. Ed Haletky. *VMware vSphere(TM) and Virtual Infrastructure Security.* Available: http://www.astroarch.com/wiki/index.php/VMware_Virtual_Infrastructure_Security

14. Ed Haletky. *VMWare ESX Server in the Enterprise.* Available: http://www.astroarch.com/wiki/index.php/VMWare_ESX_Server_in_the_Enterprise

Appendix B: Acronyms

Component	Code	Description
VMware VirtualCenter Management Server **Renamed vCenter by the vendor**	VCMS Or vCenter	**VMware VirtualCenter Server centrally manages and monitors multiple Virtual Infrastructure Nodes. It runs on a windows-based server platform and requires network connectivity to all VMware ESX hosts that it manages.**
VirtualCenter Database Server	VCDB	**VMware VirtualCenter Database Server is an approved and supported database server that contains the information needed by VMware VirtualCenter to manage its environment.**
VMware Virtual Infrastructure License Server	VILS	**VMware Virtual Infrastructure License Server manages licensing of Virtual Infrastructure features throughout the enterprise. This software is typically installed on the same server as the VirtualCenter Server.**
Console Operating System	COS	
VMware ESX Server Host	ESX or Host	**VMware ESX host is the platform on which the Virtual Infrastructure is executed. It runs a proprietary kernel with a Linux console for direct management**
VMware VCB Proxy Server	VPRX	**The VMware VCB proxy server is used to provide off network backups to the VMware Virtual Infrastructure. This host must be a windows host and should be attached to the backup SAN.**
VMware Virtual Machine Guest	VM Or Guest	**This is a VMware Virtual Machine instance housed on a VMware ESX host. Guests can be saved as Templates to facilitate future deployments.**
Storage	VIS	**Storage used by Virtual Infrastructure**
VMware Infrastructure Client	**VIC**	**This is the Client used to manage VMware ESX hosts and VMware VirtualCenter Management Servers.**

Appendix C: CIS Red Hat Enterprise Linux 5 Benchmark

Apply all recommendations except the following:

Section 4.6: disable IPMI, network, ntpd, these are required services for VMware ESX

Appendix D: Other Considerations

Depending on your organization's security environment, additional items that may be considered include:

1. Any remediation changes suggested in this benchmark should be preceded by a backup of the item affected, and a current search of the vendor's documentation and other releases, plus appropriate updating, if necessary, of the organization's standards or policies and integration with the organization's change control processes.
2. Naming Conventions – using vendor default names is not recommended because should an unauthorized person gain access to the environment, it would be easier for them to navigate to their desired object. Also, object titles not congruent with the organization's infrastructure naming conventions may lead to deployment mistakes.
3. Installation of additional software on the ESX host – The vendor generally recommends avoiding installing other software on the ESX host., However the vendor does mention certain security software products as acceptable for host installations in some versions of their documentation. Any software installed should be approved by your organization's policy and communicated to VMware to determine its effect on support. A recommendation is to maintain a default installation of an ESX server. Running the `rpm –qa | sort` command on a default build host will give a standard list of items installed by the rpm command, running the same command on a production host and using `diff` to compare the two lists will give a indication of noncompliant software. (**Note:** executable binary files not installed with the rpm command will not show up on either list).
4. `/etc/vmware/hostd/config.xml` – This configuration file contains settings for web access related to performance, storage, function and also governs SSL behavior. The contents of this file on a production ESX host should be compared to the same file contained in the default build and any changes matched to the organization's documented and authorized change management process.
5. `sysstat` logging – Consideration may be given to adding this logging facility for a more focused collection of messages related to performance events.
6. Data Residing on the ESX host – While the intent of the ESX host is not to store production applications or data, if there is a malfunction it is possible a dump may deposit data in the `/var/core/` directory. A periodic review of the `/var/core/`, `/home` (and other directories if additional software is found above) is in order to ensure, and if present remove, duplicate, sensitive customer or other organization data from the ESX host.
7. SNMP Community Strings – The SNMP read community string in ESX is "Public". Some organizations policies or some compliance requirements state default authentication credentials be changed.
8. Kernel Routing – Some organizations prohibit operating systems from performing certain network functions. In most Linux distributions the parameters for accept_redirects, send_redirects, accept_source-route may be set to the value `0` or disabled. In ESX these setting are sometimes set to `1` or enabled, at the `all` , `default`, or interface (i.e. /`vswif0/`) subdirectories of `/proc/sys/net/ipv4/conf/`. Given the internal network routing functions expected to be performed by an ESX host, it is recommended if your security policy prohibits these settings, an exception to policy may be considered for an ESX host.
9. Encryption Certificates - "Enabling Server-Certificate Verification for Virtual Infrastructure Clients":http://kb.VMware.com/kb/4646606
10. Trusted Platform Module (TPM) – this is a chip on the host motherboard that employs cryptography to validate systems and devices. This capability is limited to the ESXi hypervisor.

11. vNetwork Distributed Switch (vDS)- Multiple ports (1,016 active ports per host) allow for the flexibility to configure more networking than may be required. Extra ports can result in extra VMs of dissimilar requirements and security classification being attached to this type of switch. A vDS has the capability to configure the number of ports and this value should be set to the number necessary to support the appropriate attached VMs. Note: vNetwork Standard Switches (vSS) do not have the ability to adjust the number of ports offered from the default of 120.

Appendix E: Change History

Date	Version	Changes for this version
December 30th,, 2010	1.0.0	Initial Public Release