Tripwire® ConfigCheck™
Remediation Guide

Security Assessment
and Remediation
for VMware ESX 3.5

tripwire™

Introduction

The Tripwire ConfigCheck Remediation Guide is intended for users of the free Tripwire® ConfigCheck™ Windows utility, designed to rapidly assesses the security of VMware ESX 3.5 using VMware's *Virtual Infrastructure 3 Security Hardening* guidelines. If you are unfamiliar with ConfigCheck, please visit **www.tripwire.com/configcheck**. Here you will learn in greater detail what it is, how to obtain your free copy, and why it should be an integral part of your ongoing VMware ESX security hardening strategy.

How ConfigCheck Works

The ConfigCheck utility contains a collection of individual "tests" that are used to assess security-related ESX 3.5 configuration settings. Each time the ConfigCheck application runs it will return one of the following results:

- **Passed**—The tested ESX 3.5 configuration meets the recommended VMware configuration guideline.
- **Failed**—The tested ESX 3.5 configuration does not meet the recommended VMware configuration guideline.
- **Unavailable**—There was a problem executing this test. Normally this result occurs because the root password fails, or the file that is attempting to be accessed is set to be unreadable by root.

About this Document

The *Tripwire ConfigCheck Remediation Guide* provides detailed test descriptions that cover the specific VMware ESX configuration setting being assessed by each test and why that configuration is considered important to ESX security hardening. In addition, you will also find step-by-step remediation instructions for each ConfigCheck test to help you quickly correct failures.

About Tripwire

Tripwire helps over 6,000 enterprises worldwide reduce security risk, attain compliance and increase operational efficiency throughout their virtual and physical environments. Using Tripwire's industry-leading configuration assessment and change auditing solutions, organizations successfully achieve and maintain IT configuration control. Tripwire is headquartered in Portland, Oregon, with offices worldwide.

Disclaimer

Remediation commands are derived from sources which (typically) include the system guidance from the publisher or manufacturer. Tripwire is relying on such third party information, and makes no warranties of any kind in relation to the accuracy or propriety of such information. Please note that these instructions are not guaranteed to work due to the specific nature of your environment and should only be treated as general guidance. Tripwire is not responsible, and expressly disclaims all liability, for any modification of settings, undesired behavior or any other results of your use of this remediation guidance. You assume all risk and responsibility therefore. In any case, all modifications to systems should be performed by trained, experienced and appropriate IT staff. Always apply appropriate backup measures prior to configuration change to allow systems to be returned to prior state.

SECTION: 1.5.1 Verify the Log Size Limit
TEST: Verify the Log Size Limit

DESCRIPTION

This test verifies that each virtual machine on the ESX Server is configured to use a log rotate size less than or equal to 500KB for the vmware.log file. Virtual machines log activity in their respective vmware.log files. If growth of these log files is not limited, it is possible for virtual machines to cause a denial of service on the ESX Server by filling up the VMFS volume. There are two options for preventing virtual machines from flooding the hard disk of the host; size-based log file rotation or disabling logging for the virtual machine. This policy checks for size-based log file rotation because disabling logging altogether limits troubleshooting options.

REMEDIATION

To remediate failure of this policy test, set the maximum size of log files to 500KB for virtual machines.

Setting the maximum size of log files to 500KB for virtual machines:

1. Login to the VirtualCenter or VI Client and select the ESX Server hosting the improperly configured virtual machine.
2. Select the virtual machine you wish to edit and click Edit Settings from the Summary tab.
3. Select the Options tab.
4. Select Advanced and click the Configuration Parameters button.
5. Look for a row with log.rotateSize and edit the value to be less than or equal to 50000.
6. If the row does not exist, then click the Add Row button.
7. In the Name field type log.rotateSize.
8. In the Value field type 500000.
9. Click OK to close the Configuration Parameters dialog.

FOR ADDITIONAL DETAILS, PLEASE REFER TO:

www.vmware.com/pdf/vi3_security_hardening_wp.pdf

SECTION: 1.5.2 Verify the Number of Log Files to Keep
TEST: Verify the Number of Log Files to Keep

DESCRIPTION

This test verifies that each virtual machine on the ESX Server is configured to keep at least 1 copy of the vmware.log when the log rotate size is exceeded. Virtual machines log activity in their respective vmware.log files. If growth of these log files is not limited, it is possible for virtual machines to cause a denial of service on the ESX Server by filling up the VMFS volume. There are two options for preventing virtual machines from flooding the hard disk of the host; size-based log file rotation or disabling logging for the virtual machine. This policy checks for size-based log file rotation because disabling logging altogether limits troubleshooting options.

REMEDIATION

To remediate failure of this policy test, set the maximum number of log files to keep for virtual machines to at least 1.

Setting the maximum number of log files to keep for virtual machines:

1. Login to the VirtualCenter or VI Client and select the ESX Server hosting the improperly configured virtual machine.
2. Select the virtual machine you wish to edit and click Edit Settings from the Summary tab.
3. Select the Options tab.
4. Select Advanced and click the Configuration Parameters button.
5. Look for a row with log.keepOld and edit the value to be greater than or equal to
6. If the row does not exist, then click the Add Row button.
7. In the Name field type log.keepOld.
8. In the Value field type 1
9. Click OK to close the Configuration Parameters dialog.

FOR ADDITIONAL DETAILS, PLEASE REFER TO:

www.vmware.com/pdf/vi3_security_hardening_wp.pdf

SECTION: 2.2.1 Check Firewall for Incoming Security Level
TEST: Check Firewall for Incoming Security Level

DESCRIPTION

This test determines if all incoming traffic is blocked by the service console firewall, with the exception of the management ports: 22, 902, 80, and 443. By default, ESX Server installs with the service console firewall configured at the high security level with all incoming and outgoing traffic blocked, except for management ports.

REMEDIATION

To remediate failure of this policy test, set the service console firewall to high security by blocking incoming and outgoing traffic.

Setting the service console firewall to high security by blocking incoming traffic:

1. Login to the Service Console via SSH using a non-privileged account.
2. Use the command su - and enter the root password.
3. Run the esxcfg-firewall -blockIncoming command to return the service console firewall to high security.
4. Run the service mgmt-vmware restart command to restart the vmware-hostd process.

FOR ADDITIONAL DETAILS, PLEASE REFER TO:

www.vmware.com/pdf/vi3_301_201_server_config.pdf

SECTION: 2.2.2 Check Firewall for Outgoing Security Level
TEST: Check Firewall for Outgoing Security Level

DESCRIPTION

This test determines if all outgoing traffic is blocked by the service console firewall, with the exception of the management ports: 22, 902, 80, and 443. By default, ESX Server installs with the service console firewall configured at the high security level with all incoming and outgoing traffic blocked, except for management ports.

REMEDIATION

To remediate failure of this policy test, set the service console firewall to high security by blocking incoming and outgoing traffic.

Setting the service console firewall to high security by blocking outgoing traffic:

1. Login to the Service Console via SSH using a non-privileged account.
2. Use the command su - and enter the root password.
3. Run the esxcfg-firewall -blockOutgoing command to return the service console firewall to high security.
4. Run the service mgmt-vmware restart command to restart the vmware-hostd process.

FOR ADDITIONAL DETAILS, PLEASE REFER TO:

www.vmware.com/pdf/vi3_301_201_server_config.pdf

SECTION: 2.4 Use a Directory Service for Authentication
TEST: Use a Directory Service for Authentication

DESCRIPTION

This test determines if a directory service is used for authentication. ESX Server is capable of using one of the following directory services for authentication: Active Directory, LDAP, or NIS. Using a directory service for authentication can provide additional security and ease administrative burden by ensuring that accounts disabled in your directory are not able to authenticate to the service console.

REMEDIATION

To remediate failure of this policy test, enable the option to use an LDAP, Active Directory, or NIS directory service for authentication.

Enabling the option to use a directory service for authentication:

1. Login to the Service Console via SSH using a non-privileged account.
2. Use the command su - and enter the root password.
3. Run the man esxcfg-auth command to print options.
4. Choose the appropriate type of directory service to use for authentication in your environment.
5. The authentication options for the esxcfg-auth command are:
   Active Directory
   --enablead --addomain=<domain> --addc=<domain controller>
   LDAP
   --enableldapauth --ldapbasedn=<basedn> --ldapserver=<server>
   NIS
   --enablenis --nisdomain=<domain> --nisserver=<server>
6. Enter the esxcfg-auth command with options specific to your environment.
7. Run the service mgmt-vmware restart command to restart the vmware-hostd process.

Note: When using stackable authentication modules, you may find that the service console starts prompting twice for logins. Adding the use_first_pass parameter to /etc/pam.d/system-auth can prevent multiple password requests:
auth sufficient /lib/security/$ISA/pam_unix.so use_first_pass
If you have to implement the multiple login workaround, be sure to remove it if you ever disable authentication using a directory service. Otherwise, it could cause authentication using pam_unix.so to fail and effectively lock users out of the server.

FOR ADDITIONAL DETAILS, PLEASE REFER TO:

www.vmware.com/pdf/vi3_security_hardening_wp.pdf

SECTION: 2.5.1 Direct 'root' Login via SSH is Disabled
TEST: Verify That sshd_config Disables PermitRootLogin

DESCRIPTION

This test determines whether or not direct root log in to the service console via SSH is disabled in /etc/ssh/sshd_confg. With this configuration an administrator would need to use a non-privileged user account to log in via SSH and then use sudo or su to perform tasks. By default ESX Server is configured to disallow remote root access via SSH to help prevent network-based attacks.

REMEDIATION

To remediate failure of this policy test, configure the SSH daemon to use safe defaults for the client and server by disabling root login via SSH.

Configuring the SSH Server to disable PermitRootLogin:

1. Login to the Service Console via SSH using a non-privileged account.
2. Use the command su - and enter the root password.
3. Open the /etc/ssh/sshd_config file.
4. Find the line PermitRootLogin <value>.
5. Set the line to PermitRootLogin no and save the file.
6. Restart the daemon using the service sshd restart command.

FOR ADDITIONAL DETAILS, PLEASE REFER TO:

kbase.redhat.com/faq/FAQ_80_7833.shtm

SECTION: 2.5.2 Direct 'root' Login at the Physical Console is Disabled
TEST: Direct 'root' Login at the Physical Console is Disabled

DESCRIPTION

This test determines whether or not direct root log in at the physical service console is disabled in /etc/securetty. With this configuration an administrator would need to use a non-privileged user account to log in to the server and then use sudo or su to perform tasks. By default ESX Server is configured to disallow remote root access via SSH to help prevent network-based attacks. Disabling direct root log in at the physical service console is an additional security measure you can take.

REMEDIATION

To remediate failure of this policy test, configure the /etc/securetty file to restrict root logins to the physical system console.

Configuring the /etc/securetty file to restrict root logins to the system console:

1. Login to the physical system console as root.
2. Run the mv /etc/securetty /etc/securetty_backup command to rename the existing file.
3. Run the cat /dev/null > /etc/securetty command to create an empty version of the file.
4. Logout of the service console.
5. Verify that you can no longer login to the physical system console as root.

FOR ADDITIONAL DETAILS, PLEASE REFER TO:

www.vmware.com/pdf/vi3_security_hardening_wp.pdf

SECTION: 2.6 Limiting Access to su
TEST: Limit Access to the 'root' Account from Super User

DESCRIPTION

This test checks the PAM configuration to verify that only members of the wheel group on the ESX Server are allowed to use the su command. This setting helps control access to the su command, which does not provide very extensive logging the way sudo does. Security best practice is to use sudo instead of su whenever possible.

REMEDIATION

To remediate failure of this policy test, configure pam.d to limit su access to the root account to users within the wheel group.

Configuring pam.d to limit su access to the root account:

1. Login to the Service Console via SSH using a non-privileged account.
2. Use the command su - and enter the root password.
3. Open the /etc/pam.d/su file.
4. Uncomment the line that contains auth required pam_wheel.so use_uid.

Note: You must first have a user configured in the wheel group before making the change or else it will not be possible to su to the root.

FOR ADDITIONAL DETAILS, PLEASE REFER TO:

www.vmware.com/pdf/vi3_security_hardening_wp.pdf

SECTION: 2.7.2 Use sudo Aliases
TEST: Use sudo Aliases

DESCRIPTION
This test checks the /etc/sudoers file on the ESX Server for evidence that user aliases are being utilized for the sudo authorization scheme. Utilizing sudo aliases eases administrative burden because a user alias can be listed in the command specification. When you need to add or remove users from the alias, it won't be necessary to update the command specifications.
REMEDIATION
To remediate failure of this policy test, configure sudo use user aliases to determine the authorization scheme. Configuring sudo to use user aliases: 1. Login to the Service Console via SSH using a non-privileged account. 2. Use the command su - and enter the root password. 3. Run the visudo command to open the /etc/sudoers file. 4. Find the line User_Alias <ALIAS_NAME> = <user_name>. 5. Set the <ALIAS_NAME> and the <user_name> and save the file.

FOR ADDITIONAL DETAILS, PLEASE REFER TO:

www.gratisoft.us/sudo/man/sudoers.html#sudoers_options

SECTION: 2.7.4 Authentication Using a Directory Service for sudo
TEST: Authentication Using a Directory Service for sudo

DESCRIPTION

This test verifies that sudo is configured to use a directory service for user authentication. The setting is defined in the /etc/pam.d/sudo file on the auth line. In general, using a directory service for authentication is a good security practice because it allows for centralized management of usernames and passwords. By default, sudo is configured to use the authentication method defined globally for the ESX Server.

REMEDIATION

To remediate failure of this policy test, configure sudo to authenticate using a directory service by setting the option globally with the esxcfg-auth command.

Configuring sudo to authenticate using a directory service:

1. Login to the Service Console via SSH using a non-privileged account.
2. Use the command su - and enter the root password.
3. Run the man esxcfg-auth command to print options.
4. Choose the appropriate type of directory service to use for authentication in your environment.
5. The authentication options for the esxcfg-auth command are:
   Active Directory
   --enablead --addomain=<domain> --addc=<domain controller>
   LDAP
   --enableldap --ldapbasedn=<basedn> --ldapserver=<server>
   NIS
   --enablenis --nisdomain=<domain> --nisserver=<server>
6. Enter the esxcfg-auth command with options specific to your environment.
7. Run the service mgmt-vmware restart command to restart the vmware-hostd process.
8. Open the file /etc/pam.d/sudo using and editor of your choice.
9. Verify the line auth required pam_stack.so service=system-auth exists and close the file.

FOR ADDITIONAL DETAILS, PLEASE REFER TO:

www.vmware.com/pdf/vi3_security_hardening_wp.pdf

www.vmware.com/vmtn/resources/582

SECTION: 2.7.5.1 Verify That the rootpw Entry Does Not Exist in /etc/sudoers File
TEST: Verify That the ROOTPW Entry Does Not Exist in /etc/sudoers File

DESCRIPTION

This test verifies that sudo is configured to prompt for the password of the invoking user instead of the root password. The setting is defined using the rootpw tag in the /etc/sudoers file. It is a security risk to require sudo users to enter the root password because they could easily log in directly as root to avoid sudo logging.

REMEDIATION

To remediate failure of this policy test, remove the rootpw entry in the /etc/sudoers file so that sudo users enter their own password instead of the root password.

Removing the rootpw entry in the /etc/sudoers file so that sudo users enter their own password instead of the root password:

1. Login to the Service Console via SSH using a non-privileged account.
2. Use the command su - and enter the root password.
3. Run the visudo command to open the /etc/sudoers file.
4. Find the line contains rootpw.
5. Remove the rootpw entry and save the file.

FOR ADDITIONAL DETAILS, PLEASE REFER TO:

www.gratisoft.us/sudo/man/sudoers.html#sudoers_options

SECTION: 2.7.5.2 Verify That the NOPASSWD Entry Does Not Exist in /etc/sudoers File
TEST: Verify That the NOPASSWD Entry Does Not Exist in /etc/sudoers File

DESCRIPTION

This test verifies that sudo password checking enabled. The setting is defined using the nopasswd tag in the /etc/sudoers file. Allowing users to execute commands via sudo without authenticating is a security risk that could result in unauthorized activity.

REMEDIATION

To remediate failure of this policy test, remove the NOPASSWD entry in the /etc/sudoers file to enable password checking.

Removing the NOPASSWD entry in the /etc/sudoers file to enable password checking:

1. Login to the Service Console via SSH using a non-privileged account.
2. Use the command su - and enter the root password.
3. Run the visudo command to open the /etc/sudoers file.
4. Find the line contains NOPASSWD.
5. Remove the NOPASSWD entry and save the file.

FOR ADDITIONAL DETAILS, PLEASE REFER TO:

www.gratisoft.us/sudo/man/sudoers.html#sudoers_options

SECTION: 2.8.1.1.1 Verify Maximum Password Age in /etc/shadow
TEST: Verify Maximum Password Age in /etc/shadow

DESCRIPTION
This test verifies that accounts defined in /etc/shadow have a maximum passwords age that is less than or equal to 90 days. It is a best practice to change passwords frequently and this test checks for the default maximum password age. This setting should be tailored to match the password policy for your environment.
REMEDIATION
To remediate failure of this policy test, set the maximum number of days a password remains valid to less than or equal to 90 days. Setting the maximum number of days a password remains valid to less than or equal to 90 days: 1. Login to the Service Console via SSH using a non-privileged account. 2. Use the command su - and enter the root password. 3. Run the chage -M <number_of_days> <username> command where <number_of_days> is less than or equal to 90 and <username> is the account with the wrong password aging settings. **Note:** The instructions above configure the password aging policy for a specific account. Reset the global password aging policy used for new accounts with the esxcfg-auth --passmaxdays=<number_of_days> command.

FOR ADDITIONAL DETAILS, PLEASE REFER TO:

www.vmware.com/pdf/vi3_301_201_server_config.pdf

SECTION: 2.8.1.1.2 Verify PASS_MAX_DAYS Parameter in /etc/login.defs
TEST: Verify PASS_MAX_DAYS Parameter in /etc/login.defs

DESCRIPTION
This test verifies that the default maximum password age defined in /etc/login.defs is less than or equal to 90 days. This setting is used for creation of new accounts. It is a best practice to change passwords frequently and this test checks for the default maximum password age. This setting should be tailored to match the password policy for your environment.
REMEDIATION
To remediate failure of this policy test, set the PASS_MAX_DAYS parameter to define the maximum number of days a password may be used. Setting the PASS_MAX_DAYS parameter to define the maximum number of days a password may be used: 1. Login to the Service Console via SSH using a non-privileged account. 2. Use the command su - and enter the root password. 3. Use the esxcfg-auth --passmaxdays=<number_of_days> command where <number_of_days> is less than or equal to 90.

FOR ADDITIONAL DETAILS, PLEASE REFER TO:

www.vmware.com/pdf/vi3_301_201_server_config.pdf

SECTION: 2.8.1.2.1 Verify Minimum Password Age in /etc/shadow
TEST: Verify Minimum Password Age in /etc/shadow

DESCRIPTION
This test verifies that accounts defined in /etc/shadow have a minimum password age that is greater than or equal to 0 days. It is a best practice to change passwords frequently and this test checks for the default minimum password age. This setting should be tailored to match the password policy for your environment.

REMEDIATION
To remediate failure of this policy test, set the minimum number of days between password changes to greater than or equal to 0. Setting the minimum number of days between password changes to greater than or equal to 0: 1. Login to the Service Console via SSH using a non-privileged account. 2. Use the command su - and enter the root password. 3. Run the chage -m <number_of_days> <username> command where <number_of_days> is greater than or equal to 0 and <username> is the account with the wrong password aging settings. **Note:** The instructions above configure the password aging policy for a specific account. Reset the global password aging policy used for new accounts with the esxcfg-auth --passmindays=<number_of_days> command.

FOR ADDITIONAL DETAILS, PLEASE REFER TO:

www.vmware.com/pdf/vi3_301_201_server_config.pdf

SECTION: 2.8.1.2.2 Verify PASS_MIN_DAYS Parameter in /etc/login.defs

TEST: Verify PASS_MIN_DAYS Parameter in /etc/login.defs

DESCRIPTION
This test verifies that the minimum password age defined in /etc/login.defs is greater than or equal to 0 days. This setting is used for creation of new accounts. This test checks for the default minimum password age. This setting should be tailored to match the password policy for your environment.
REMEDIATION
To remediate failure of this policy test, set the PASS_MIN_DAYS parameter to define the minimum number of days allowed between password changes. Setting the PASS_MIN_DAYS parameter to define the minimum number of days allowed between password changes: 1. Login to the Service Console via SSH using a non-privileged account. 2. Use the command su - and enter the root password. 3. Use the esxcfg-auth --passmindays=<number_of_days> command where <number_of_days> is greater than or equal to 0.

FOR ADDITIONAL DETAILS, PLEASE REFER TO:

www.vmware.com/pdf/vi3_301_201_server_config.pdf

SECTION: 2.8.1.3.1 Verify Password Expiration Warning Age in /etc/shadow
TEST: Verify Password Expiration Warning Age in /etc/shadow

DESCRIPTION

This test verifies that the minimum password age defined in /etc/login.defs is greater than or equal to 0 days. This setting is used for creation of new accounts. This test checks for the default minimum password age. This setting should be tailored to match the password policy for your environment.

REMEDIATION

To remediate failure of this policy test, set the number of days a warning is given before a password expires to greater than or equal to 7.

Setting the number of days a warning is given before a password expires to greater than or equal to 7:

1. Login to the Service Console via SSH using a non-privileged account.
2. Use the command su - and enter the root password.
3. Run the chage -W <number_of_days> <username> command where <number_of_days> is equal to 7 and <user name> is the account with the wrong password aging settings.

Note: The instructions above configure the password aging policy for a specific account. Reset the global password aging policy used for new accounts with the esxcfg-auth --passwarnage=<number_of_days> command.

FOR ADDITIONAL DETAILS, PLEASE REFER TO:

www.vmware.com/pdf/vi3_301_201_server_config.pdf

SECTION: 2.8.1.3.2 Verify PASS_WARN_AGE Parameter in /etc/login.defs
TEST: Verify PASS_WARN_AGE Parameter in /etc/login.defs

DESCRIPTION
This test verifies that the password warn age defined in /etc/login.defs is greater than or equal to 7 days. This setting is used for creation of new accounts. Issuing password expiration warnings is best practice policy that encourages proactive user behavior and reduces administrative burden. This setting should be tailored to match the password policy for your environment.
REMEDIATION
To remediate failure of this policy test, set the PASS_WARN_AGE parameter to define the number of days warning given before a password expires. Setting the PASS_WARN_AGE parameter to define the number of days warning given before a password expires: 1. Login to the Service Console via SSH using a non-privileged account. 2. Use the command su - and enter the root password. 3. Use the esxcfg-auth --passwarnage=<number_of_days> command where <number_of_days> is greater than or equal to 7.

FOR ADDITIONAL DETAILS, PLEASE REFER TO:

www.vmware.com/pdf/vi3_301_201_server_config.pdf

SECTION: 2.8.2 Verify That the Minimum Password Length Is 8
TEST: Verify That the Minimum Password Length Is 8

DESCRIPTION
This test checks for the default password complexity requirements configured during ESX Server installation. By default ESX Server uses the pam_cracklib.so plugin with a minimum length parameter of 9. A user is required to enter at least 8 characters for a password if only one character class is used. Please refer to the ESX Server System Administration Guide for more information about how you can tailor this setting to match the password policy for your environment.

REMEDIATION
To remediate failure of this policy test, adjust the password complexity requirements for the ESX server to require password length of at least 8 if only one character class is used. Setting the password complexity requirements: 1. Login to the Service Console via SSH using a non-privileged account. 2. Use the command su - and enter the root password. 3. Reset the password complexity requirements using the esxcfg-auth --usecrack=<retries> <minimum_length> <lc_credit> <uc_credit> <d_credit> <oc_credit> command. **Note:** By default on an ESX Server the minimum length parameter is set to 9, but the actual minimum password length required is 8 when only one character class is used. For example, the default settings would be given by the esxcfg-auth --usecrack=3 9 1 1 1 1 command.

FOR ADDITIONAL DETAILS, PLEASE REFER TO:

www.vmware.com/pdf/vi3_301_201_server_config.pdf

SECTION: 2.9 Limit the Software and Services Running in the Service Console
TEST: Minimize Services Running

DESCRIPTION

This test checks that the default services installed with ESX Server are configured to start up during the boot process. These represent the minimum set of services required to manage an ESX Server. Failure of this test indicates that fewer or more services than the default set were found, which could indicate operational or security risks. Administrators are advised to strictly limit any additional services running on the server to minimize threat vectors. If additional services like NIS, CIM HTTPS, or SNMP are required, document any additional ports opened on the firewall.

REMEDIATION

To remediate failure of this policy test, minimize the list of services that start on boot to reduce the threat area of the ESX Server.

Minimizing the list of boot services:

1. Login to the Service Console via SSH using a non-privileged account.
2. Use the command su - and enter the root password.
3. Gotothe /etc/rc3.d/ directory.
4. View the list of boot services by using the ls command.
5. Disable any services not listed below using the chkconfig <service_name> off command as needed:
   S<id_number>microcode_ctl
   S<id_number>vmkstart
   S<id_number>vmware
   S<id_number>mptctlnode
   S<id_number>iptables
   S<id_number>firewall
   S<id_number>network
   S<id_number>syslog
   S<id_number>irqbalance
   S<id_number>random
   S<id_number>sshd
   S<id_number>vmware-late
   S<id_number>rawdevices
   S<id_number>xinetd
   S<id_number>ntpd
   S<id_number>gpm
   S<id_number>vmware-webAccess
   S<id_number>crond
   S<id_number>httpd.vmware
   S<id_number>vmware-vmkauthd
   S<id_number>mgmt-vmware
   S<id_number>local
   S<id_number>pegasus
   S<id_number>vmware-autostart

FOR ADDITIONAL DETAILS, PLEASE REFER TO:

www.vmware.com/pdf/vi3_security_hardening_wp.pdf

SECTION: 2.12.1.1.1 Verify All Access over the Loopback Interface
TEST: Verify All Access over the Loopback Interface

DESCRIPTION
This test verifies that NTP is configured to resolve hostnames using the loopback network. If this setting is not in place, /var/log/messages will report permission denied errors for the NTP daemon. Proper NTP configuration is a key factor in maintaining accurate log records used for incident handling.
REMEDIATION
To remediate failure of this policy test, set the restrict entry in the /etc/ntp.conf file to permit all access over the loopback interface. Setting the restrict entry in the /etc/ntp.conf file to permit all access over the loopback interface: 1. Login to the Service Console via SSH using a non-privileged account. 2. Use the command su - and enter the root password. 3. Open the /etc/ntp.conf file. 4. Find the line restrict <value>. 5. Set the <value> to 127.0.0.1 and save the file. 6. Restart the NTP daemon using the service ntpd restart command.

FOR ADDITIONAL DETAILS, PLEASE REFER TO:

http://kb.vmware.com/kb/1339

SECTION: 2.12.1.1.2 Check /etc/ntp.conf: Access Limited for Non-loopback Machines
TEST: Check /etc/ntp.conf: Access Limited for Non-loopback Machines

DESCRIPTION
This test verifies that NTP is configured to restrict access to non-loop back machines. Configuring NTP with kod, nomodify, and notrap provides protection against UDP spoofing of NTP for ESX Servers connected to the Internet. Proper NTP configuration is a key factor in maintaining accurate log records used for incident handling.
REMEDIATION
To remediate failure of this policy test, configure the NTP daemon to limit non-loopback machines. Configuring the NTP daemon to limit non-loopback machines: 1. Login to the Service Console via SSH using a non-privileged account. 2. Use the command su - and enter the root password. 3. Open the /etc/ntp.conf file. 4. Add the line restrict default kod nomodify notrap. 5. Save the file. 6. Restart the NTP daemon using the service ntpd restart command.

FOR ADDITIONAL DETAILS, PLEASE REFER TO:

http://kb.vmware.com/kb/1339

SECTION: 2.12.1.1.3 Check /etc/ntp.conf: At Least Three NTP Servers Defined
TEST: Check /etc/ntp.conf: At Least Three NTP Servers Defined

DESCRIPTION
This test verifies that NTP is configured to use three NTP pool servers. Using multiple NTP pool servers is a good practice for failover purposes. Proper NTP configuration is a key factor in maintaining accurate log records used for incident handling.
REMEDIATION
To remediate failure of this policy test, configure the NTP daemon to use at least three NTP servers. Configuring the NTP daemon to use at least three NTP servers: 1. Login to the Service Console via SSH using a non-privileged account. 2. Use the command su - and enter the root password. 3. Open the /etc/ntp.conf file. 4. Add at least three NTP servers to the /etc/ntp.conf file as shown in the following example: server 0.vmware.pool.ntp.org server 1.vmware.pool.ntp.org server 2.vmware.pool.ntp.org 5. Save the file. 6. Restart the NTP daemon using the service ntpd restart command.

FOR ADDITIONAL DETAILS, PLEASE REFER TO:

http://kb.vmware.com/kb/1339

SECTION: 2.12.1.1.4 Check for the Drift File
TEST: Check for the Drift File

DESCRIPTION
This test verifies that NTP is configured to use a driftfile. Driftfiles are used to store the current value of the frequency error used during initialization of the NTP daemon. It takes a day to compute the frequency error value, so using a drift file to store the previous version for use during NTP re-initialization is a good practice.
REMEDIATION
To remediate failure of this policy test, set the driftfile entry in the /etc/ntp.conf file to specify the location of the frequency file. Setting the driftfile entry in the /etc/ntp.conf file to specify the location of the frequency file: 1. Login to the Service Console via SSH using a non-privileged account. 2. Use the command su - and enter the root password. 3. Open the /etc/ntp.conf file. 4. Find the line driftfile <value>. 5. Set the <value> to /var/lib/ntp/drift and save the file. 6. Restart the NTP daemon using the service ntpd restart command.

FOR ADDITIONAL DETAILS, PLEASE REFER TO:

http://kb.vmware.com/kb/1339

SECTION: 2.12.1.2 Verify /etc/ntp/step-tickers Settings
TEST: Verify /etc/ntp/step-tickers Settings

DESCRIPTION
This test verifies that at least three NTP servers are defined in /etc/ntp/steptickers. Using step tickers helps speed up synchronization for the NTP daemon by using ntpdate to set the clock.

REMEDIATION
To remediate failure of this policy test, configure at least three trusted NTP servers in the /etc/ntp/step-tickers file. Configuring at least three trusted NTP servers in the /etc/ntp/steptickers file: 1. Login to the Service Console via SSH using a non-privileged account. 2. Use the command su - and enter the root password. 3. Open the /etc/ntp/step-tickers file. 4. Add at least three NTP servers to the file as shown in the example below: server 0.vmware.pool.ntp.org server 1.vmware.pool.ntp.org server 2.vmware.pool.ntp.org 5. Save the file.

FOR ADDITIONAL DETAILS, PLEASE REFER TO:

http://kb.vmware.com/kb/1339

SECTION: 2.12.1.3 Verify /etc/hosts Settings
TEST: Verify /etc/hosts Settings

DESCRIPTION
This test verifies that at least three NTP servers are defined in the /etc/hosts file. Adding the list of NTP pool servers to /etc/hosts helps minimize the impact of DNS resolution failures during NTP synchronization.

REMEDIATION
To remediate failure of this policy test, configure at least three trusted NTP servers in the /etc/hosts file. Configuring at least three trusted NTP servers in the /etc/hosts file: 1. Login to the Service Console via SSH using a non-privileged account. 2. Use the command su - and enter the root password. 3. Open the /etc/hosts file. 4. Add at least three NTP servers to the file as shown in the example below: 0.vmware.pool.ntp.org 1.vmware.pool.ntp.org 2.vmware.pool.ntp.org 5. Save the file.

FOR ADDITIONAL DETAILS, PLEASE REFER TO:

http://kb.vmware.com/kb/1339

SECTION: 2.12.1.4 Ensure That NTP Is Running
TEST: Ensure That NTP Is Running

DESCRIPTION
This test checks to see if the NTP daemon is currently running on the ESX Server. Proper NTP configuration is a key factor in maintaining accurate log records used for incident handling.

REMEDIATION
To remediate failure of this policy test, start the ntpd service if it is not running. Starting the ntpd service if it is not running: 1. Login to the Service Console via SSH using a non-privileged account. 2. Use the command su - and enter the root password. 3. Run the chkconfig --list ntpd command to check status of the service. 4. Run the service ntpd start command to start the service if it is not running.

FOR ADDITIONAL DETAILS, PLEASE REFER TO:

http://kb.vmware.com/kb/1339

SECTION: 2.12.1.5 Ensure Default NTP Port Is Open
TEST: Ensure Default NTP Port Is Open

DESCRIPTION
This test verifies that the default port used by the NTP daemon is open on the service console firewall. Proper NTP configuration is a key factor in maintaining accurate log records used for incident handling.
REMEDIATION
To remediate failure of this policy test, open port for NTP by enabling ntp Client service in the ESX firewall. Opening port for NTP by enabling ntpClient service in the ESX firewall: 1. Login to the Service Console via SSH using a non-privileged account. 2. Use the command su - and enter the root password. 3. Run the esxcfg-firewall -e ntpClient command to open port for the NTP. 4. Run the service mgmt-vmware restart command to restart the vmware-hostd process. 5. Restart the NTP daemon using the service ntpd restart command.

FOR ADDITIONAL DETAILS, PLEASE REFER TO:

http://kb.vmware.com/kb/1339

SECTION: 2.12.2.1.1 Verify the /etc/logrotate.d/vmkernel File Uses the 'compress' Option
TEST: Verify That /etc/logrotate.d/vmkernel Uses the 'compress' Option

DESCRIPTION
This test verifies that compression is enabled for the vmkernel log on the ESX Server. Using log compression helps control log growth by allowing more log data to be stored on the server.
REMEDIATION
To remediate failure of this policy test, configure the vmkernel file to use the compress mode. Configuring the vmkernel file to use the compress mode: 1. Login to the Service Console via SSH using a non-privileged account. 2. Use the command su - and enter the root password. 3. Open /etc/logrotate.d/vmkernel file. 4. Find the line nocompress . 5. Set the line to compress and save the file.

FOR ADDITIONAL DETAILS, PLEASE REFER TO:

http://kb.vmware.com/kb/1339

SECTION: 2.12.2.1.2 Verify the Size of the Log File Is Less than or Equals to 4096K in the /etc/logrotate.d/vmkernel File

TEST: Verify the Size of the Log File Is Less than or Equal to 4096K in the /etc/logrotate.d/vmkernel File

DESCRIPTION
This test verifies that size of the vmkernel log is less than or equal to 4096K. Putting a cap on log size can prevent the hard disk from filling up with log data. At the same time it is important to keep enough logging information to aid troubleshooting of system errors.
REMEDIATION
To remediate failure of this policy test, set the size entry to less than or equal to 4096KB in the /etc/logrotate.d/vmkernel file. Setting the size entry to less than or equal to 4096KB in the /etc/logrotate.d/vmkernel file: 1. Login to the Service Console via SSH using a non-privileged account. 2. Use the command su - and enter the root password. 3. Open the /etc/logrotate.d/vmkernel file. 4. Find the line size <value>. 5. Set the <value> to less than or equal to 4096K and save the file.

FOR ADDITIONAL DETAILS, PLEASE REFER TO:

www.vmware.com/pdf/vi3_security_hardening_wp.pdf

SECTION: 2.12.2.2.1 Verify the /etc/logrotate.d/vmksummary File Uses the 'compress' Option
TEST: Verify That /etc/logrotate.d/vmksummary Uses the 'compress' Option

DESCRIPTION
This test verifies that compression is enabled for the vmksummary log on the ESX Server. Using log compression helps control log growth by allowing more log data to be stored on the server.
REMEDIATION
To remediate failure of this policy test, configure the vmksummary file to use the compress mode. Configuring the vmksummary file to use the compress mode: 1. Login to the Service Console via SSH using a non-privileged account. 2. Use the command su - and enter the root password. 3. Open /etc/logrotate.d/vmksummary file. 4. Find the line nocompress. 5. Set the line to compress and save the file.

SECTION: 2.12.2.2.2 Verify the Size of the Log File Is Less than or Equals to 4096K in the /etc/logrotate.d/vmksummary File

TEST: Verify the Size of the Log File Is Less than or Equal to 4096K in the /etc/logrotate.d/vmk summary File

DESCRIPTION
This test verifies that size of the vmksummary log is less than or equal to 4096K. Putting a cap on log size can prevent the hard disk from filling up with log data. At the same time it is important to keep enough logging information to aid troubleshooting of system errors.
REMEDIATION
To remediate failure of this policy test, set the size entry to less than or equal to 4096KB in the /etc/logrotate.d/vmksummary file. Setting the size entry to less than or equal to 4096KB in the /etc/logrotate.d/vmksummary file: 1. Login to the Service Console via SSH using a non-privileged account. 2. Use the command su - and enter the root password. 3. Open the /etc/logrotate.d/vmksummary file. 4. Find the line size <value>. 5. Set the <value> to less than or equal to 4096K and save the file.

FOR ADDITIONAL DETAILS, PLEASE REFER TO:

www.vmware.com/pdf/vi3_security_hardening_wp.pdf

SECTION: 2.12.2.3.1 Verify the /etc/logrotate.d/vmkwarning File Uses the 'compress' Option
TEST: Verify That /etc/logrotate.d/vmkwarning Uses the 'compress' Option

DESCRIPTION
This test verifies that compression is enabled for the vmkwarning log on the ESX Server. Using log compression helps control log growth by allowing more log data to be stored on the server.
REMEDIATION
To remediate failure of this policy test, configure the vmkwarning file to use the compress mode. Configuring the vmkwarning file to use the compress mode: 1. Login to the Service Console via SSH using a non-privileged account. 2. Use the command su - and enter the root password. 3. Open /etc/logrotate.d/vmkwarning file. 4. Find the line nocompress . 5. Set the line to compress and save the file.

SECTION: 2.12.2.3.2 Verify the Size of the Log File Is Less than or Equals to 4096K in the /etc/logrotate.d/vmkwarning File

TEST: Verify the Size of the Log File Is Less than or Equal to 4096K in the /etc/logrotate.d/vmk warning File

DESCRIPTION
This test verifies that size of the vmkwarning log is less than or equal to 4096K. Putting a cap on log size can prevent the hard disk from filling up with log data. At the same time it is important to keep enough logging information to aid troubleshooting of system errors.
REMEDIATION
To remediate failure of this policy test, set the size entry to less than or equal to 4096KB in the /etc/logrotate.d/vmkwarning file. Setting the size entry to less than or equal to 4096KB in the /etc/logrotate.d/vmkwarning file: 1. Login to the Service Console via SSH using a non-privileged account. 2. Use the command su - and enter the root password. 3. Open the /etc/logrotate.d/vmkwarning file. 4. Find the line size <value>. 5. Set the <value> to less than or equal to 4096K and save the file.

FOR ADDITIONAL DETAILS, PLEASE REFER TO:

www.vmware.com/pdf/vi3_security_hardening_wp.pdf

SECTION: 2.12.3 Use Remote syslog Logging
TEST: Use Remote syslog Logging

DESCRIPTION
This test verifies that syslog is configured to send logs to a remote host. Using a centralized host to store log data allows for monitoring of all servers from a single location.

REMEDIATION
To remediate failure of this policy test, configure /etc/syslog.conf to send messages to a remote host for each log. Configuring /etc/syslog.conf to send messages to a remote host for each log: 1. Login to the Service Console via SSH using a non-privileged account. 2. Use the command su - and enter the root password. 3. Open the /etc/syslog.conf file. 4. Add the line @<loghost.company.com> after each log name in the file. Where the <loghost.company.com> is the name of a host configured to record remote log files. 5. Save the file. 6. Open the /etc/hosts file. 7. Add the <loghost.company.com> to the file if needed and save the file. 8. Run the kill -SIGHUP `cat /var/run/syslogd.pid` command to reload the syslog daemon.

FOR ADDITIONAL DETAILS, PLEASE REFER TO:

www.vmware.com/pdf/vi3_security_hardening_wp.pdf

SECTION: 2.12.4 Display Different Log Level Messages on Different Screens
TEST: Display Different Log Level Messages on Different Screens

DESCRIPTION
This test verifies that critical, error, and warning level log messages are directed to different terminals. Displaying different level log messages on separate terminals can help the administrator easily distinguish between different error levels. Customize the terminal number used for each type of message based on the needs of your environment.
REMEDIATION
To remediate failure of this policy test, enable separation of log message display for critical level messages. Enable separation of log message display for critical level messages: 1. Login to the Service Console via SSH using a non-privileged account. 2. Use the command su - and enter the root password. 3. Open the /etc/syslog.conf file. 4. Add the line *.crit /dev/tty11 to the file and save the file. 5. Run the kill -SIGHUP `cat /var/run/syslogd.pid` command to reload the syslog daemon.

FOR ADDITIONAL DETAILS, PLEASE REFER TO:

www.vmware.com/pdf/vi3_security_hardening_wp.pdf

SECTION: 2.12.5.1 Verify /etc/sudoers Settings
TEST: Verify That syslog Is Configured in /etc/sudoers File

DESCRIPTION
This test verifies that sudo is configured to use syslog for logging all activities looking for a syslog entry in /etc/sudoers. Using sudo to perform tasks that are beyond the normal administrative capability of a user is preferred to using su because all sudo activity can be logged and access to commands can be controlled.
REMEDIATION
To remediate failure of this policy test, configure the sudo to use syslog to record all occurrences of its use. Configuring the sudo to use syslog to record all occurrences of its use: 1. Login to the Service Console via SSH using a non-privileged account. 2. Use the command su - and enter the root password. 3. Run the visudo command to open the /etc/sudoers file. 4. Set the line Defaults syslog=<value>. 5. Save the file.

FOR ADDITIONAL DETAILS, PLEASE REFER TO:

vmware.com/pdf/vi3_security_hardening_wp.pdf

SECTION: 2.12.5.2 Verify That /etc/syslog.conf Contains Proper Settings for Logging sudo Activity
TEST: Verify That syslog Daemon Sends the Logging Information to File

DESCRIPTION
This test verifies the syslog daemon is configured to send the sudo logging information to a file. If the syslog daemon does not direct the sudo logging information to a file, then sudo activities are not logged as expected.
REMEDIATION
To remediate failure of this policy test, add an entry to the /etc/syslog.conf file to send the logging information to a file. Adding an entry to the /etc/syslog.conf file to send the logging information to a file: 1. Login to the Service Console via SSH using a non-privileged account. 2. Use the command su - and enter the root password. 3. Run the visudo command to open the /etc/sudoers file. 4. Find the line Defaults syslog=<value>. 5. Open the /etc/syslog.conf file. 6. Add the line <value> <log_file_name> and save the file.

FOR ADDITIONAL DETAILS, PLEASE REFER TO:

vmware.com/pdf/vi3_security_hardening_wp.pdf

SECTION: 2.12.6.1 Change the Permissions of the snmpd.conf File to 700
TEST: Verify /etc/snmp/snmpd.conf Permissions

DESCRIPTION
This test verifies that the 'root' user owns /etc/snmp/snmpd.conf and permissions are equal to 700. By default when ESX Server is installed the root user and root group are assigned ownership of the /etc/snmp/snmpd.conf file. Using permissions of 700 ensures that only the owner can read, write, and execute the file.

REMEDIATION
To remediate failure of this policy test, set appropriate permissions and ownership on the /etc/snmp/snmpd.conf file. Setting appropriate permissions and ownership on the /etc/snmp/snmpd.conf file: 1. Login to the Service Console via SSH using a non-privileged account. 2. Use the command su - and enter the root password. 3. Check the permissions and ownership of the files using the ls -lL /etc/snmp/snmpd.conf command. 4. Change permissions to 700 using the chmod 700 /etc/snmp/snmpd.conf command. 5. Change ownership to root using the chown root:root /etc/snmp/snmpd.conf command.

SECTION: 2.12.6.4 Do Not Change Mode from Read-only
TEST: SNMP in Read-only Mode

DESCRIPTION
This test verifies that the default SNMP community created during installation is configured to have read-only access. To minimize SNMP security risks, do not change the mode from read-only unless you have a specific need and are aware of the implications.
REMEDIATION
To remediate failure of this policy test, set the SNMP community to read-only. Setting the SNMP community to read-only: 1. Login to the Service Console via SSH using a non-privileged account. 2. Use the command su - and enter the root password. 3. Open the /etc/snmp/snmpd.conf file. 4. Find the line contains the rwcommunity string. 5. Change rwcommunity to rocommunity and save the file. 6. Restart the SNMP daemon using the service snmpd restart command.

FOR ADDITIONAL DETAILS, PLEASE REFER TO:

www.vmware.com/pdf/vi3_301_201_admin_guide.pdf

SECTION: 3.2 Do Not Create a Default Port Group
TEST: Do Not Create a Default Port Group

DESCRIPTION

This test determines if the default network was created during installation. Choosing the "Create Default Network" option during ESX Server installation creates an insecure configuration where service console traffic is visible to the virtual machine network. It is a security best practice to isolate the service console network from the virtual machine networks.

REMEDIATION

To remediate failure of this policy test, configure the service console on a network interface that is isolated from the network interface used by virtual machines.

Configuring the service console on a network interface that is isolated from the network for virtual machines using one of the following options:

1. Login to VirtualCenter or the VI Client to access the ESX Server.
2. Select the Configuration tab.
3. From the Hardware pane, select Networking.
4. Click Properties for vSwitch0 and configure using one of the following options:

   Remove the VM Network port group from vSwitch0 and create a new virtual switch on a different subnet for virtual machines.

   Configure isolated VLAN IDs for the service console and virtual machine port groups if they must remain on the same virtual switch.

FOR ADDITIONAL DETAILS, PLEASE REFER TO:

www.vmware.com/pdf/vi3_301_201_server_config.pdf

SECTION: 3.4 Do Not Use Promiscuous Mode on Network Interfaces
TEST: Verify That Promiscuous Mode Is Set to Reject

DESCRIPTION

This test checks that the layer 2 network security policy is configured to reject promiscuous mode. While promiscuous mode can be useful for troubleshooting, it is not advisable to enable it on the virtual switches of the ESX Server. When it is enabled, any virtual machines on the host could intercept packets sent across the virtual switch.

REMEDIATION

To remediate failure of this policy test, configure the layer 2 security policy for all of the virtual switches and port groups on the ESX Server to reject promiscuous mode.

Configuring the ESX Server to reject promiscuous mode:

1. Login to VirtualCenter or the VI Client to access the ESX Server.
2. Select the Configuration tab.
3. From the Hardware pane, select Networking.
4. Click Properties for the virtual switch you would like to reconfigure.
5. On the Ports tab select vSwitch and click Edit.
6. Select the Security tab.
7. Set Promiscuous Mode: to Reject.
8. Click OK.
9. For each port group on the virtual switch click Properties, select the Security tab.
10. Uncheck the Promiscuous Mode: option for Policy Exceptions as needed.
11. Click Close.
12. Repeat steps 4 -11 for each virtual switch on the ESX Server as needed.

FOR ADDITIONAL DETAILS, PLEASE REFER TO:

www.vmware.com/pdf/vi3_301_201_server_config.pdf

SECTION: 3.5.1 MAC Address Changes
TEST: Verify That MAC Address Changes Is Set to Reject

DESCRIPTION

This test checks that the layer 2 network security policy is configured to reject MAC address changes. Rejecting MAC address changes helps protect against MAC address spoofing. With this option set, the ESX Server will not honor requests to change the effective MAC address.

REMEDIATION

To remediate failure of this policy test, configure the layer 2 security policy for all of the virtual switches and port groups on the ESX Server to reject MAC address changes.

Configuring the ESX Server to reject MAC address changes:

1. Login to VirtualCenter or the VI Client to access the ESX Server.
2. Select the Configuration tab.
3. From the Hardware pane, select Networking.
4. Click Properties for the virtual switch you would like to reconfigure.
5. On the Ports tab select vSwitch and click Edit.
6. Select the Security tab.
7. Set MAC Address Changes: to Reject.
8. Click OK.
9. For each port group on the virtual switch click Properties, select the Security tab.
10. Uncheck the MAC Address Changes: option for Policy Exceptions as needed.
11. Click Close.
12. Repeat steps 4–11 for each virtual switch on the ESX Server as needed.

FOR ADDITIONAL DETAILS, PLEASE REFER TO:

www.vmware.com/pdf/vi3_301_201_server_config.pdf

SECTION: 3.5.2 Forged Transmissions
TEST: Verify That Forged Transmits Is Set to Reject

DESCRIPTION
This test checks that the layer 2 network security policy is configured to reject forged transmits. Setting this option to reject causes the ESX Server to drop packets if the source MAC address does not match the effective MAC address of the virtual machine.

REMEDIATION
To remediate failure of this policy test, configure the layer 2 security policy for all of the virtual switches and port groups on the ESX Server to reject forged transmits. Configuring the ESX Server to reject forged transmits: 1. Login to VirtualCenter or the VI Client to access the ESX Server. 2. Select the Configuration tab. 3. From the Hardware pane, select Networking. 4. Click Properties for the virtual switch you would like to reconfigure. 5. On the Ports tab select vSwitch and click Edit. 6. Select the Security tab. 7. Set Forged Transmits: to Reject. 8. Click OK. 9. For each port group on the virtual switch click Properties, select the Security tab. 10. Uncheck the Forged Transmits: option for Policy Exceptions as needed. 11. Click Close. 12. Repeat steps 4–11 for each virtual switch on the ESX Server as needed.

FOR ADDITIONAL DETAILS, PLEASE REFER TO:

www.vmware.com/pdf/vi3_301_201_server_config.pdf

SECTION: 3.6.1 Verify /etc/grub.conf Settings
TEST: Verify /etc/grub.conf Settings

DESCRIPTION

This test verifies that a password is required when a user attempts to modify the boot process by passing commands to GRUB. If a password is not required an attacker might be able to subvert the normal boot process on the server.

REMEDIATION

To remediate failure of this policy test, configure grub mode to require a password when a user attempts to modify the boot process.

Configuring the grub mode to set a password when a user attempts to modify the boot process:

1. Login to the Service Console via SSH using a non-privileged account.
2. Use the command su - and enter the root password.
3. Run the grub command to enter the grub mode.
4. In the grub mode, run the md5crypt command to encrypt the password.
5. Enter the grub password.
6. Copy down the encrypted password.
7. Run the quit command to exit grub mode.
8. Open the /etc/grub.conf file.
9. Add the line password --md5 <encrypted_password> and save the file.

Note: Where the <encrypted_password> is copied from the encrypted password in grub mode.

FOR ADDITIONAL DETAILS, PLEASE REFER TO:

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

SECTION: 3.6.2 Verify /etc/grub.conf Permissions
TEST: Verify /etc/grub.conf Permissions

DESCRIPTION
This test verifies that the 'root' user owns /etc/grub.conf and permissions are equal to 600. To help protect the GRUB configuration from unauthorized changes, only the 'root' user should have read and write access to the grub.conf file.

REMEDIATION
To remediate failure of this policy test, set appropriate permissions and ownership on the /etc/grub.conf file. Setting appropriate permissions and ownership on the /etc/grub.conf file: 1. Login to the Service Console via SSH using a non-privileged account. 2. Use the command su - and enter the root password. 3. Check the permissions and ownership of the file using the ls -lL /etc/grub.conf command. 4. Change permissions to 600 using the chmod 600 /etc/grub.conf command. 5. Change ownership to root using the chown root:root /etc/grub.conf command.

SECTION: 3.8.1 Protect against the Root File System Filling up from /var/log
TEST: Protect against the Root File System Filling up from /var/log

DESCRIPTION

This test verifies that the system log directory (/var/log) is isolated from the root partition. It is recommended to create a separate partition for /var/log to prevent a denial of service scenario where the root partition fills up.

REMEDIATION

To remediate failure of this policy test, move the /var/log directory to a separate partition from / to prevent it from filling the root partition.

Configuring a new partition the /var/log directory:

1. Login to the physical Service Console using a non-privileged account.
2. Use the command su - and enter the root password.
3. If needed, create and format a new ext3 partition that is at least 2000MB, taking note of the target partition name.
    1. Create a partition as needed using fdisk /dev/<devicename> to start fdisk.
    2. Create the filesystem on the new partition using the mkfs.ext3 /dev/<device name> command. Where <device name> is the target partition name.
4. Create a mount point.
    1. Create a new directory using mkdir /mnt/<mount point> where <mount point> is a name of your choosing.
    2. Mount the new filesystem with the mount /dev/<devicename> /mnt/<mount point> command.
5. Copy the contents of /var/log to the new mount point.
    1. Enter single-user mode with the init 1 command.
    2. Change to the /var/log directory using the cd /var/log command.
    3. Copy the contents of the directory with the cp -ax * /mnt/<mount point> command.
6. Move the existing directory and mount the new partition.
    1. Go to the root directory using cd / command.
    2. Enter mv /var/log /var/log.old to make a backup copy of the existing directory.
    3. Create a new directory using the mkdir /var/log command.
    4. Mount the new directory on the new partition with the mount /dev/<device name> /var/log command.
    5. Exit single-user mode by pressing the Ctrl-D keys.
7. Edit /etc/fstab so the new partition is loaded automatically on the next reboot: /dev/<mount point> /var/log ext3 defaults 1 2
8. Reload fstab using the mount -a command.

FOR ADDITIONAL DETAILS, PLEASE REFER TO:

www.vmware.com/pdf/vi3_301_201_installation_guide.pdf

SECTION: 3.8.2 Protect against the Root File System Filling up from /home
TEST: Protect against the Root File System Filling up from /home

DESCRIPTION
This test verifies that the user data directory (/home) is isolated from the root partition. It is recommended to create a separate partition for /home to prevent a denial of service scenario where the root partition fills up.

REMEDIATION

To remediate failure of this policy test, move the /home directory to a separate partition from / to prevent it from filling the root partition.

Configuring a new partition the /home directory:

1. Login to the physical Service Console using a non-privileged account.
2. Use the command su - and enter the root password.
3. If needed, create and format a new ext3 partition that is at least 512MB, taking note of the target partition name.
    1. Create a partition as needed using fdisk /dev/<devicename> to start fdisk.
    2. Create the filesystem on the new partition using the mkfs.ext3 /dev/<device name> command. Where <device name> is the target partition name.
4. Create a mount point.
    1. Create a new directory using mkdir /mnt/<mount point> where <mount point> is a name of your choosing.
    2. Mount the new filesystem with the mount /dev/<devicename> /mnt/<mount point> command.
5. Copy the contents of /home to the new mount point.
    1. Enter single-user mode with the init 1 command.
    2. Change to the /home directory using the cd /home command.
    3. Copy the contents of the directory with the cp -ax * /mnt/<mount point> command.
6. Move the existing directory and mount the new partition.
    1. Go to the root directory using the cd / command.
    2. Enter mv /home /home.old to make a backup copy of the existing directory.
    3. Create a new directory using the mkdir /home command.
    4. Mount the new directory on the new partition with the mount /dev/<device name> /home command.
    5. Exit single-user mode by pressing the Ctrl-D keys.
7. Edit /etc/fstab so the new partition is loaded automatically on the next reboot: /dev/<mount point> /home ext3 defaults 1 2
8. Reload fstab using the mount -a command.

FOR ADDITIONAL DETAILS, PLEASE REFER TO:

www.vmware.com/pdf/vi3_301_201_installation_guide.pdf

SECTION: 3.8.3 Protect against the Root File System Filling up from /tmp
TEST: Protect against the Root File System Filling up from /tmp

DESCRIPTION

This test verifies that the temporary file directory (/tmp) is isolated from the root partition. It is recommended to create a separate partition for /tmp to prevent a denial of service scenario where the root partition fills up.

REMEDIATION

To remediate failure of this policy test, move the /tmp directory to a separate partition from / to prevent it from filling the root partition.

Configuring new partition for the /tmp directory:

1. Login to the physical Service Console using a non-privileged account.
2. Use the command su - and enter the root password.
3. If needed, create and format a new ext3 partition that is at least 1024MB, taking note of the target partition name.
    1. Create a partition as needed using fdisk /dev/<devicename> to start fdisk.
    2. Create the filesystem on the new partition using the mkfs.ext3 /dev/<device name> command. Where <device name> is the target partition name.
4. Create a mount point.
    1. Create a new directory using mkdir /mnt/<mount point> where <mount point> is a name of your choosing.
    2. Mount the new filesystem with the mount /dev/<devicename> /mnt/<mount point> command.
5. Copy the contents of /tmp to the new mount point.
    1. Enter single-user mode with the init 1 command.
    2. Change to the /tmp directory using the cd /tmp command.
    3. Copy the contents of the directory with the cp -ax * /mnt/ <mount point> command.
6. Move the existing directory and mount the new partition.
    1. Go to the root directory using the cd / command.
    2. Enter mv /tmp /tmp.old to make a backup copy of the existing directory.
    3. Create a new directory using mkdir /tmp.
    4. Mount the new directory on the new partition with the mount /dev/<device name> /tmp command.
    5. Exit single-user mode by pressing the Ctrl-D keys.
7. Edit /etc/fstab so the new partition is loaded automatically on the next reboot:
   /dev/<mount point> /tmp ext3 defaults 1 2
8. Reload fstab using the mount -a command.

FOR ADDITIONAL DETAILS, PLEASE REFER TO:

www.vmware.com/pdf/vi3_301_201_installation_guide.pdf

www.tripwire.com
US TOLL FREE: 1.800.TRIPWIRE **MAIN:** 503.276.7500 **FAX:** 503.223.0182
326 SW Broadway, 3rd Floor Portland, OR 97205 USA