

VMware

Table of Contents

1. [Restrict Owner and Group File Ownership to Root for .vmdk Files](#)
2. [Restrict Owner and Group file ownership to Root for .vmx Files](#)
3. [Disable Group and Other Read, Write and Execute File Permissions for .vmdk Files](#)
4. [Disable Group and Other Write File Permissions for .vmx Files](#)
5. [Implement logon warning banners](#)
6. [Use CHAP protocol to connect to iSCSI devices](#)
7. [Harden firewall settings to allow only authorized traffic](#)
8. [Protect against MAC address spoofing, forged transmits, and promiscuous mode](#)
9. [Enable BIOS passwords](#)
10. [Isolate service console management traffic](#)
11. [Configure syslogd to send logs to a remote LogHost](#)
12. [Review logs periodically](#)
13. [Enable compression and rotation for log files](#)
14. [Minimum password length](#)
15. [Enable password minimum days parameter](#)
16. [Enable maximum password life parameter](#)
17. [Failed login attempts](#)
18. [Implement strong password complexity](#)
19. [Implement strong password controls](#)
20. [Restrict SSH Access](#)
21. [Configure system clock synchronization with NTP](#)
22. [Disable unnecessary services](#)
23. [Apply critical security patches](#)

1. Restrict Owner and Group File Ownership to Root for .vmdk Files

Restricting file ownership for virtual machine disk files helps prevent accidental or malicious changes to application data. Set file ownership for all .vmdk disk files to:

Restrict owner and group file ownership to root

MAINOPTIONS

checkedTagID[]: undefined, undefined, undefined

2. Restrict Owner and Group file ownership to Root for .vmx Files

Restricting file ownership for configuration files helps prevent accidental or malicious changes to the system. Set file ownership for all .vmx files to:

Restrict owner and group file ownership to root

MAINOPTIONS

checkedTagID[]: undefined, undefined, undefined

3. Disable Group and Other Read, Write and Execute File Permissions for .vmdk Files

Disabling file permissions for virtual machine disk files helps prevent accidental or malicious changes to application data.

Set file permissions for all .vmdk disk files to:

Deny group read, write and execute access

Deny other read, write and execute access

MAINOPTIONS

checkedTagID[]: undefined, undefined, undefined

4. Disable Group and Other Write File Permissions for .vmx Files

Disabling file permissions for configuration files helps prevent accidental or malicious changes to the system.

Set file permissions for all .vmx configuration files to:

Deny group write access

Deny other write access

MAINOPTIONS

checkedTagID[]: undefined, undefined, undefined

5. Implement logon warning banners

There are no default warning banners since your organization's exact wording is unknown at installation. 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. Create warning banners for console and remote access.

MAINOPTIONS

checkedTagID[]: undefined, undefined, undefined

6. Use CHAP protocol to connect to iSCSI devices

Use of the CHAP protocol ensures ESX hosts and storage devices are communicating with known endpoints. Configure connections to iSCSI storage devices to use the CHAP protocol for authentication.

MAINOPTIONS

checkedTagID[]: undefined, undefined, undefined

7. Harden firewall settings to allow only authorized traffic

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

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

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.

REFERENCE

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 are all commented out in a default installation. If any of these lines have been activated ("`#`" removed from the start of a line) they should be matched with the organization change control documentation. Any activated lines can be found with the following command.

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

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
```

MAINOPTIONS

checkedTagID[]: undefined, undefined, undefined, undefined, undefined

8. Protect against MAC address spoofing, forged transmits, and promiscuous mode

Change the flags to reject for the settings MAC Address Changes and Forged Transmits for a <vSwitch> or a <PortGroup>.

The default setting is accept in virtual switches and in portgroups.

These settings provide the ability to drop incoming and outgoing guest network packets if a guest MAC address in a packet is different from the MAC address specified in the guest configuration file (vmx).

MAINOPTIONS

checkedTagID[]: undefined, undefined, undefined, undefined

9. Enable BIOS passwords

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.

MAINOPTIONS

checkedTagID[]: undefined, undefined, undefined, undefined

10. Isolate service console management traffic

During the installation, un-select the default option to create a default network for virtual machines. This default installation option will combine the virtual machine network with the virtual infrastructure service console management network. This could potentially allow network-based access to the service console to a wider population of users than just system administrators, possibly allowing access to sensitive configuration traffic. The service console management traffic should always be isolated on a separate network.

REFERENCE

MAINOPTIONS

checkedTagID[]: undefined, undefined

11. Configure syslogd to send logs to a remote LogHost

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.

Configure syslogd to send a copy of ESX host logs to a remote location.

MAINOPTIONS

checkedTagID[]: undefined, undefined, undefined, undefined

12. Review logs periodically

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.

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

MAINOPTIONS

checkedTagID[]: undefined, undefined, undefined, undefined, undefined

13. Enable compression and rotation for log files

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. Increase the file size 2096K and enable compression for the log files vmkernel and vmksummary.

MAINOPTIONS

checkedTagID[]: undefined, undefined, undefined

14. Minimum password length

The longer the total character length of a password, the more difficult it is to guess by unauthorized users.

Set the minimum required number of characters a password must contain to:

Greater than or equal to 8 characters.

MAINOPTIONS

checkedTagID[]: undefined, undefined, undefined

15. Enable password minimum days parameter

Combined with the history setting (see section 1.3.4), the minimum days setting will cause multiple days to transpire before a user can return to a favorite password, discouraging password reuse. Set the minimum number of days a password must exist before it can be changed to:

Greater than or equal to 7 days.

MAINOPTIONS

checkedTagID[]: undefined, undefined, undefined

16. Enable maximum password life parameter

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

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

Less than or equal to 90 days.

MAINOPTIONS

checkedTagID[]: undefined, undefined, undefined

17. Failed login attempts

For user accounts, setting the failed attempt number at a low level discourages repetitive tries, which may be automated, to guess a user's password.

Set the number of login attempts allowed before the account is locked / disabled to:

Less than or equal to 3 failed logins.

MAINOPTIONS

checkedTagID[]: undefined, undefined, undefined, undefined, undefined

18. Implement strong password complexity

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.

Recommended password 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.

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).

MAINOPTIONS

checkedTagID[]: undefined, undefined, undefined, undefined, undefined

19. Implement strong password controls

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.

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.

MAINOPTIONS

checkedTagID[]: undefined, undefined, undefined, undefined, undefined

20. Restrict SSH Access

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

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.

MAINOPTIONS

checkedTagID[]: undefined, undefined, undefined, undefined, undefined

21. Configure system clock synchronization with NTP

Add configuration settings to enable system clock synchronization with Network Time Protocol (NTP) server(s). Keeping 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). The default installation of an ESX host does not configure NTP, since the location of your NTP server varies by organization.

REFERENCE

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

MAINOPTIONS

checkedTagID[]: undefined, undefined, undefined, undefined, undefined

22. Disable unnecessary services

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

REFERENCE

http://www.vmware.com/pdf/vi3_35/esx_3/r35/vi3_35_25_3_server_config.pdf.
http://www.vmware.com/files/pdf/vi35_security_hardening_wp.pdf

MAINOPTIONS

checkedTagID[]: undefined, undefined, undefined, undefined, undefined

23. Apply critical security patches

It is critical that an organization develop a formal process for keeping up-to-date with applicable VMware

patches. VMware uses three categories for patches: Security, Critical, and General. The patch # refers to KB (knowledge base) article number that goes into more detail. VMware will (usually) issue a KB article when they become aware of security vulnerabilities and other serious functionality issues before they issue a patch. However, it is up to the organization to actually download and install these patches in accordance to their policies and 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/Production environment. It is recommended that the VMware Update Manager be used for this purpose.

REFERENCE

VMware Support Center -Download Patches: <https://www.vmware.com/mysupport/download/>.

MAINOPTIONS

checkedTagID[]: undefined, undefined, undefined, undefined, undefined
