Compliance Self Test Plan for GENERIC, VMWare

vSphere 8.0 ESXi

05 DEC 2023

SIGNATURES

Information System Security Manager:

______________________________ ______________

Name **Date**
ISSM

Information System Security Officer:

______________________________ ______________

Name **Date**
ISSO

TABLE OF CONTENTS

1. INTRODUCTION

1.1 Purpose

The purpose of the GENERIC Test Plan is to provide all involved parties with a discrete set of measurement and expected outcomes in order to gauge successful security compliance self-testing for the GENERIC system at the installation location. Additionally, this document will outline the resources needed to successfully accomplish this test.

1.2 Scope

The scope of this test includes the test cases for the VMWare vSphere 8.0 ESXi on the GENERIC baseline system.

2. Environment (Target System)

The GENERIC system is comprised of the following sub-systems with associated operating systems and Original Equipment Manufacturer (OEM) as defined;

- INSERT SYSTEM (ABBREVIATION) [OPERATING SYSTEM, ORGANIZATION OWNER]
- LIST

The interface control systems that are testable in the target system include the account consoles to the GENERIC system, as defined by access through the sub-system.

2.1 Security Environment

The security environment will be at the [INSERT LEVEL OF SECURITY] level and will require the appropriate security and control measures suitable for the data being processed. All personnel will require access authorization to both the testing facility and the data produced on the system components. Any test materials, data, or reports identified as being classified will require the appropriate markings, protection, transmission, handling and storage procedures.

3. Responsibilities

3.1 Site ISSM

Organizational personnel will provide logistical and technical support to the OEM team during the installation and test period. Support should include any system administration or network administration that must be accomplished on the host environment in order to successfully integrate the test system into the [ORGANIZATIONAL] network.

3.2 Site ISSO

Implementation of appropriate security controls to maintain information system risk and associated mission risk at an acceptable level as determined by the Authorizing Authority (AO). The system controls, the particular controls with [ORGANIZATIONAL] defined parameters in Committee on National Security Systems Instruction (CNSSI) 1253 are referenced by the following list:

- INSERT SYSTEM CONTROL (ABBREVIATION) [OPERATING SYSTEM, ORGANIZATION OWNER] [PARAMETER]
- LIST

3.3 [ORGANIZATION]

Develop the cybersecurity compliance self-test plan. The test procedures contained in this document are referenced to VMWare vSphere 8.0 ESXi system.

4. Test Execution Instructions

i) The test procedure sheet may be filled out manually or electronically.
  (1) Complete the entries for target system, date, and test representative at the beginning of the procedure.
  (2) All information assurance security controls in the table must be marked as:
    (a) Pass:
      (i) the device passed the security test
    (b) Fail:
      (i) the device failed the test; or
      (ii) device lacks the capability and is not compensated by another device/measure
    (c) Not Evaluated:
      (i) no test provided; or
      (ii) the device is not available for testing; or
      (iii) the device lacks the capability but is compensated by another device/measure
  (3) Provide comments for any control not marked as Pass.
  (4) Upon completion, the score sheet is digitized if necessary, and uploaded as an exhibit to the appropriate [ORGANIZATION] project reference.

4.1 Test Procedure

The following pages provide the detailed test procedure required to perform the target system compliance self-test plan.

Step	Step Description	Expected Results/Comments	P/F
Security Test Case TEST SCENARIO: The test executioner will log onto a [access interface] workstation and execute a series of commands and check the results against the respective expected results that are listed below. TEST SETUP: 1. The test executioner will log into a [access interface] workstation with valid LDAP user with privileged access (account should have a ".priv" at the end of it). 2. Once logged on, the test executioner will open a shell by clicking on Hosts and selecting Console. 3. Within the shell, the test execution will execute the following shell commands;			
N/A	**Record Test Start Date/Time**	**Start Date: _______ Start Time: ________**	N/A

Step	Step Description	Expected Results/Comments	P/F
Test 1 CCI-000044 **Enforce the organization-defined limit of consecutive invalid logon attempts by a user during the organization-defined time period.** **NIST SP 800-53 Revision 5::AC-7 a**			
1	The ESXi host must enforce the limit of three consecutive invalid logon attempts by a user.	From the vSphere Client, go to Hosts and Clusters. Select the ESXi Host >> Configure >> System >> Advanced System Settings. Select the "Security.AccountLockFailures" value and verify it is set to "3". or From a PowerCLI command prompt while connected to the ESXi host, run the following command: Get-VMHost | Get-AdvancedSetting -Name Security.AccountLockFailures If the "Security.AccountLockFailures" setting is set to a value other than "3", this is a finding.	
Test 2 CCI-000048 **Display an organization-defined system use notification message or banner to users before granting access to the system that provides privacy and security notices consistent with applicable federal laws, Executive Orders, directives, policies, regulations, standards, and guidelines.** **NIST SP 800-53 Revision 5::AC-8 a**			

<table>
<tr><th>Step</th><th>Step Description</th><th>Expected Results/Comments</th><th>P/F</th></tr>
<tr><td>2</td><td>The ESXi host must display the Standard Mandatory DOD Notice and Consent Banner before granting access to the system via the Direct Console User Interface (DCUI).</td><td>From the vSphere Client, go to Hosts and Clusters.
Select the ESXi Host >> Configure >> System >> Advanced System Settings.
Select the "Annotations.WelcomeMessage" value and verify it contains the standard mandatory DOD notice and consent banner.
or
From a PowerCLI command prompt while connected to the ESXi host, run the following command:
Get-VMHost | Get-AdvancedSetting -Name Annotations.WelcomeMessage
If the "Annotations.WelcomeMessage" setting does not contain the standard mandatory DOD notice and consent banner, this is a finding.</td><td></td></tr>
<tr><td colspan="4"><b>Test 3 CCI-000054</b>
<b>Limit the number of concurrent sessions for each organization-defined account and/or account type to an organization-defined number.</b>
<b>NIST SP 800-53 Revision 5::AC-10</b></td></tr>
</table>

Step	Step Description	Expected Results/Comments	P/F
3	The ESXi host must enable lockdown mode.	For environments that do not use vCenter server to manage ESXi, this is not applicable. From the vSphere Client, go to Hosts and Clusters. Select the ESXi Host >> Configure >> System >> Security Profile. Scroll down to "Lockdown Mode" and verify it is set to "Enabled" (Normal or Strict). or From a PowerCLI command prompt while connected to the ESXi host, run the following command: `Get-VMHost | Select Name,@{N="Lockdown";E={$_.Extensiondata.Config.LockdownMode}}` If "Lockdown Mode" is disabled, this is a finding.	

Test 4 CCI-000057

The information system initiates a session lock after the organization-defined time period of inactivity.

NIST SP 800-53 Revision 5::AC-11 a

<table>
<tr><th>Step</th><th>Step Description</th><th>Expected Results/Comments</th><th>P/F</th></tr>
<tr><td>4</td><td>The ESXi host client must be configured with an idle session timeout.</td><td>From the vSphere Client, go to Hosts and Clusters.
Select the ESXi Host >> Configure >> System >> Advanced System Settings.
Select the "UserVars.HostClientSessionTimeout" value and verify it is set to "900" or less.
or
From a PowerCLI command prompt while connected to the ESXi host, run the following command:
Get-VMHost | Get-AdvancedSetting -Name UserVars.HostClientSessionTimeout
If the "UserVars.HostClientSessionTimeout" setting is not set to "900" or less, this is a finding.</td><td></td></tr>
<tr><td colspan="4"><b>Test 5 CCI-000068</b>
<b>Implement cryptographic mechanisms to protect the confidentiality of remote access sessions.</b>
<b>NIST SP 800-53 Revision 4::AC-17 (2)</b></td></tr>
</table>

Step	Step Description	Expected Results/Comments	P/F
5	The ESXi host Secure Shell (SSH) daemon must use FIPS 140-2 validated cryptographic modules to protect the confidentiality of remote access sessions.	From an ESXi shell, run the following command: # esxcli system security fips140 ssh get or From a PowerCLI command prompt while connected to the ESXi host, run the following commands: $esxcli = Get-EsxCli -v2 $esxcli.system.security.fips140.ssh.get.invoke() Expected result: Enabled: true If the FIPS mode is not enabled for SSH, this is a finding.	
Test 6 CCI-000130 **Ensure that audit records containing information that establishes what type of event occurred.** **NIST SP 800-53 Revision 5::AU-3 a**			

Step	Step Description	Expected Results/Comments	P/F
6	The ESXi must produce audit records containing information to establish what type of events occurred.	From the vSphere Client, go to Hosts and Clusters. Select the ESXi Host >> Configure >> System >> Advanced System Settings. Select the "Config.HostAgent.log.level" value and verify it is set to "info". or From a PowerCLI command prompt while connected to the ESXi host, run the following command: Get-VMHost | Get-AdvancedSetting -Name Config.HostAgent.log.level If the "Config.HostAgent.log.level" setting is not set to "info", this is a finding. Note: Verbose logging level is acceptable for troubleshooting purposes.	

<table>
<tr><th>Step</th><th>Step Description</th><th>Expected Results/Comments</th><th>P/F</th></tr>
<tr><td colspan="4">Test 7 CCI-000192
The information system enforces password complexity by the minimum number of upper case characters used.
NIST SP 800-53 Revision 4::IA-5 (1) (a)

CCI-000193
The information system enforces password complexity by the minimum number of lower case characters used.
NIST SP 800-53 Revision 4::IA-5 (1) (a)

CCI-000194
The information system enforces password complexity by the minimum number of numeric characters used.
NIST SP 800-53 Revision 4::IA-5 (1) (a)

CCI-000195
The information system, for password-based authentication, when new passwords are created, enforces that at least an organization-defined number of characters are changed.
NIST SP 800-53 Revision 4::IA-5 (1) (b)

CCI-000205
The information system enforces minimum password length.
NIST SP 800-53 Revision 4::IA-5 (1) (a)

CCI-001619
The information system enforces password complexity by the minimum number of special characters used.
NIST SP 800-53 Revision 4::IA-5 (1) (a)</td></tr>
</table>

Step	Step Description	Expected Results/Comments	P/F
7	The ESXi host must enforce password complexity by configuring a password quality policy.	From the vSphere Client, go to Hosts and Clusters. Select the ESXi Host >> Configure >> System >> Advanced System Settings. Select the "Security.PasswordQualityControl" value and verify it is set to "similar=deny retry=3 min=disabled,disabled,disabled,disabled,15". or From a PowerCLI command prompt while connected to the ESXi host, run the following command: Get-VMHost | Get-AdvancedSetting -Name Security.PasswordQualityControl If the "Security.PasswordQualityControl" setting is set to a value other than "similar=deny retry=3 min=disabled,disabled,disabled,disabled,15", this is a finding.	

Test 8 CCI-000200

The information system prohibits password reuse for the organization-defined number of generations.

NIST SP 800-53 Revision 4::IA-5 (1) (e)

Step	Step Description	Expected Results/Comments	P/F
8	The ESXi host must prohibit password reuse for a minimum of five generations.	From the vSphere Client, go to Hosts and Clusters. Select the ESXi Host >> Configure >> System >> Advanced System Settings. Select the "Security.PasswordHistory" value and verify it is set to "5" or greater. or From a PowerCLI command prompt while connected to the ESXi host, run the following command: Get-VMHost | Get-AdvancedSetting -Name Security.PasswordHistory If the "Security.PasswordHistory" setting is set to a value other than 5 or greater, this is a finding.	
Test 9 CCI-000381 **Configure the system to provide only organization-defined mission essential capabilities.** **NIST SP 800-53 Revision 5::CM-7 a**			

Step	Step Description	Expected Results/Comments	P/F
9	The ESXi host must be configured to disable nonessential capabilities by disabling the Managed Object Browser (MOB).	From the vSphere Client, go to Hosts and Clusters. Select the ESXi Host >> Configure >> System >> Advanced System Settings. Select the "Config.HostAgent.plugins.solo.enableMob" value and verify it is set to "false". or From a PowerCLI command prompt while connected to the ESXi host, run the following command: Get-VMHost | Get-AdvancedSetting -Name Config.HostAgent.plugins.solo.enableMob If the "Config.HostAgent.plugins.solo.enableMob" setting is not set to "false", this is a finding.	

Step	Step Description	Expected Results/Comments	P/F
Test 10 CCI-000764 **Uniquely identify and authenticate organizational users and associate that unique identification with processes acting on behalf of those users.** **NIST SP 800-53 Revision 5::IA-2** **CCI-000770** **The organization requires individuals to be authenticated with an individual authenticator when a group authenticator is employed.** **NIST SP 800-53 Revision 4::IA-2 (5)** **CCI-001682** **Automatically removes or disables emergency accounts after an organization-defined time period for each type of account.** **NIST SP 800-53 Revision 4::AC-2 (2)** **CCI-001941** **Implement replay-resistant authentication mechanisms for access to privileged accounts and/or non-privileged accounts.** **NIST SP 800-53 Revision 5::IA-2 (8)** **CCI-001942** **The information system implements replay-resistant authentication mechanisms for network access to non-privileged accounts.** **NIST SP 800-53 Revision 4::IA-2 (9)**			

Step	Step Description	Expected Results/Comments	P/F
10	The ESXi host must uniquely identify and must authenticate organizational users by using Active Directory.	For systems that do not use Active Directory and have no local user accounts other than root and/or service accounts, this is not applicable. From the vSphere Client, go to Hosts and Clusters. Select the ESXi Host >> Configure >> System >> Authentication Services. Verify the "Directory Services Type" is set to "Active Directory". or From a PowerCLI command prompt while connected to the ESXi host, run the following command: Get-VMHost | Get-VMHostAuthentication For systems that do not use Active Directory and do have local user accounts, other than root and/or service accounts, this is a finding. If the "Directory Services Type" is not set to "Active Directory", this is a finding.	
Test 11 CCI-000767 **The information system implements multifactor authentication for local access to privileged accounts.** **NIST SP 800-53 Revision 4::IA-2 (3)**			

Step	Step Description	Expected Results/Comments	P/F
11	The ESXi host Secure Shell (SSH) daemon must ignore .rhosts files.	From an ESXi shell, run the following command: # esxcli system ssh server config list -k ignorerhosts or From a PowerCLI command prompt while connected to the ESXi host, run the following commands: $esxcli = Get-EsxCli -v2 $esxcli.system.ssh.server.config.list.invoke() \| Where-Object {$_.Key -eq 'ignorerhosts'} Example result: ignorerhosts yes If "ignorerhosts" is not configured to "yes", this is a finding.	

Test 12 CCI-001133

Terminate the network connection associated with a communications session at the end of the session or after an organization-defined time period of inactivity.

NIST SP 800-53 Revision 5::SC-10

CCI-002361

Automatically terminate a user session after organization-defined conditions or trigger events requiring session disconnect.

NIST SP 800-53 Revision 5::AC-12

Step	Step Description	Expected Results/Comments	P/F
12	The ESXi host must set a timeout to automatically end idle shell sessions after fifteen minutes.	From the vSphere Client, go to Hosts and Clusters. Select the ESXi Host >> Configure >> System >> Advanced System Settings. Select the "UserVars.ESXiShellInteractiveTimeOut" value and verify it is set to less than "900" and not "0". or From a PowerCLI command prompt while connected to the ESXi host, run the following command: Get-VMHost | Get-AdvancedSetting -Name UserVars.ESXiShellInteractiveTimeOut If the "UserVars.ESXiShellInteractiveTimeOut" setting is set to a value greater than "900" or "0", this is a finding.	

<table>
<tr><th>Step</th><th>Step Description</th><th>Expected Results/Comments</th><th>P/F</th></tr>
<tr><td colspan="4">Test 13 CCI-001494
Protect audit tools from unauthorized modification.
NIST SP 800-53 Revision 5::AU-9

CCI-001495
Protect audit tools from unauthorized deletion.
NIST SP 800-53 Revision 4::AU-9

CCI-002696
Verify correct operation of organization-defined security functions.
NIST SP 800-53 Revision 5::SI-6 a

CCI-002699
Perform verification of the correct operation of organization-defined security functions: when the system is in an organization-defined transitional state; upon command by a user with appropriate privileges; and/or on an organization-defined frequency.
NIST SP 800-53 Revision 5::SI-6 b</td></tr>
</table>

<table>
<tr><th>Step</th><th>Step Description</th><th>Expected Results/Comments</th><th>P/F</th></tr>
<tr><td>13</td><td>The ESXi host must implement Secure Boot enforcement.</td><td>If the ESXi host does not have a compatible TPM, this finding is downgraded to a CAT III.
From an ESXi shell, run the following command:
esxcli system settings encryption get
or
From a PowerCLI command prompt while connected to the ESXi host, run the following commands:
$esxcli = Get-EsxCli -v2
$esxcli.system.settings.encryption.get.invoke() | Select RequireSecureBoot
Expected result:
Require Secure Boot: true
If "Require Secure Boot" is not enable, this is a finding.</td><td></td></tr>
<tr><td colspan="4"><b>Test 14 CCI-001496</b>
<b>Implement cryptographic mechanisms to protect the integrity of audit tools.</b>
<b>NIST SP 800-53 Revision 5::AU-9 (3)</b></td></tr>
<tr><td>14</td><td>The ESXi host must enable Secure Boot.</td><td>From an ESXi shell, run the following command:
/usr/lib/vmware/secureboot/bin/secureBoot.py -s
If Secure Boot is not "Enabled", this is a finding.</td><td></td></tr>
</table>

Step	Step Description	Expected Results/Comments	P/F
Test 15 CCI-002238 **Automatically lock the account or node for either an organization-defined time period, until the locked account or node is released by an administrator, or delays the next logon prompt according to the organization-defined delay algorithm when the maximum number of unsuccessful logon attempts is exceeded.** **NIST SP 800-53 Revision 5::AC-7 b**			
15	The ESXi host must enforce an unlock timeout of 15 minutes after a user account is locked out.	From the vSphere Client, go to Hosts and Clusters. Select the ESXi Host >> Configure >> System >> Advanced System Settings. Select the "Security.AccountUnlockTime" value and verify it is set to less than "900" and not "0". or From a PowerCLI command prompt while connected to the ESXi host, run the following command: Get-VMHost | Get-AdvancedSetting -Name Security.AccountUnlockTime If the "Security.AccountUnlockTime" setting is less than 900 or 0, this is a finding.	
Test 16 CCI-001849 **Allocate audit log storage capacity to accommodate organization-defined audit record retention requirements.** **NIST SP 800-53 Revision 5::AU-4**			

Step	Step Description	Expected Results/Comments	P/F
16	The ESXi host must allocate audit record storage capacity to store at least one week's worth of audit records.	From the vSphere Client, go to Hosts and Clusters. Select the ESXi Host >> Configure >> System >> Advanced System Settings. Select the "Syslog.global.auditRecord.storageCapacity" value and verify it is set to "100". or From a PowerCLI command prompt while connected to the ESXi host, run the following command: Get-VMHost | Get-AdvancedSetting -Name Syslog.global.auditRecord.storageCapacity If the "Syslog.global.auditRecord.storageCapacity" setting is not set to 100, this is a finding.	

Step	Step Description	Expected Results/Comments	P/F
Test 17 CCI-001683 The information system notifies organization-defined personnel or roles for account creation actions. NIST SP 800-53 Revision 4::AC-2 (4) CCI-001684 The information system notifies organization-defined personnel or roles for account modification actions. NIST SP 800-53 Revision 4::AC-2 (4) CCI-001686 The information system notifies organization-defined personnel or roles for account removal actions. NIST SP 800-53 Revision 4::AC-2 (4) CCI-001851 Transfer audit logs per organization-defined frequency to a different system, system component, or media than the system or system component conducting the logging. NIST SP 800-53 Revision 5::AU-4 (1)			

Step	Step Description	Expected Results/Comments	P/F
17	The ESXi host must off-load logs via syslog.	From the vSphere Client, go to Hosts and Clusters. Select the ESXi Host >> Configure >> System >> Advanced System Settings. Select the "Syslog.global.logHost" value and verify it is set to a site-specific syslog server. Syslog servers are specified in the following formats: udp://<IP or FQDN>:514 tcp://<IP or FQDN>:514 ssl://<IP or FQDN>:1514 Multiple servers can also be specified when separated by commas. or From a PowerCLI command prompt while connected to the ESXi host, run the following command: Get-VMHost | Get-AdvancedSetting -Name Syslog.global.logHost If the "Syslog.global.logHost" setting is not set to a valid, site-specific syslog server, this is a finding.	

Test 18 CCI-001891

The information system compares internal information system clocks on an organization-defined frequency with an organization-defined authoritative time source.

NIST SP 800-53 Revision 4::AU-8 (1) (a)

CCI-002046

The information system synchronizes the internal system clocks to the authoritative time source when the time difference is greater than the organization-defined time period.

NIST SP 800-53 Revision 4::AU-8 (1) (b)

<table>
<tr><th>Step</th><th>Step Description</th><th>Expected Results/Comments</th><th>P/F</th></tr>
<tr><td>18</td><td>The ESXi host must synchronize internal information system clocks to an authoritative time source.</td><td>From the vSphere Client, go to Hosts and Clusters.
Select the ESXi Host >> Configure >> System >> Time Configuration.
Verify NTP or PTP are configured, and one or more authoritative time sources are listed.
From the vSphere Client, go to Hosts and Clusters.
Select the ESXi Host >> Configure >> System >> Services.
Verify the NTP or PTP service is running and configured to start and stop with the host.
or
From a PowerCLI command prompt while connected to the ESXi host, run the following commands:
Get-VMHost | Get-VMHostNTPServer
Get-VMHost | Get-VMHostService | Where {$_.Label -eq "NTP Daemon" -or $_.Label -eq "PTP Daemon"}
If the NTP service is not configured with authoritative DOD time sources or the service is not configured to start and stop with the host ("Policy" of "on" in PowerCLI) or is stopped, this is a finding.
If PTP is used instead of NTP, this is not a finding.</td><td></td></tr>
</table>

Step	Step Description	Expected Results/Comments	P/F
Test 19 CCI-001749 **The information system prevents the installation of organization-defined software components without verification the software component has been digitally signed using a certificate that is recognized and approved by the organization.** **NIST SP 800-53 Revision 4::CM-5 (3)** **CCI-001774** **Employ a deny-all, permit-by-exception policy to allow the execution of authorized software programs on the system.** **NIST SP 800-53 Revision 5::CM-7 (5) (b)**			
19	The ESXi Image Profile and vSphere Installation Bundle (VIB) acceptance level must be verified.	From the vSphere Client, go to Hosts and Clusters. Select the ESXi Host >> Configure >> System >> Security Profile. Under "Host Image Profile Acceptance Level" view the acceptance level. or From a PowerCLI command prompt while connected to the ESXi host, run the following commands: $esxcli = Get-EsxCli -v2 $esxcli.software.acceptance.get.Invoke() If the acceptance level is "CommunitySupported", this is a finding.	
Test 20 CCI-001967 **Authenticate organization-defined devices and/or types of devices before establishing a local, remote, and/or network connection using bidirectional authentication that is cryptographically based.** **NIST SP 800-53 Revision 5::IA-3 (1)**			

Step	Step Description	Expected Results/Comments	P/F
20	The ESXi host must enable bidirectional Challenge-Handshake Authentication Protocol (CHAP) authentication for Internet Small Computer Systems Interface (iSCSI) traffic.	If iSCSI is not used, this is not applicable. From the vSphere Client, go to Hosts and Clusters. Select the ESXi Host >> Configure >> Storage >> Storage Adapters. Select the iSCSI adapter >> Properties >> Authentication >> Method. View the CHAP configuration and verify CHAP is required for target and host authentication. or From a PowerCLI command prompt while connected to the ESXi host, run the following command: Get-VMHost | Get-VMHostHba | Where {$_.Type -eq "iscsi"} | Select AuthenticationProperties -ExpandProperty AuthenticationProperties If iSCSI is used and CHAP is not set to "required" for both the target and host, this is a finding. If iSCSI is used and unique CHAP secrets are not used for each host, this is a finding.	

Test 21 CCI-002418

Protect the confidentiality and/or integrity of transmitted information.

NIST SP 800-53 Revision 5::SC-8

Step	Step Description	Expected Results/Comments	P/F
21	The ESXi host must protect the confidentiality and integrity of transmitted information by isolating vMotion traffic.	For environments that do not use vCenter server to manage ESXi, this is not applicable. From the vSphere Client, go to Hosts and Clusters. Select the ESXi Host >> Configure >> Networking >> VMkernel adapters. Review the VLAN associated with any vMotion VMkernel(s) and verify they are dedicated for that purpose and are logically separated from other functions. If long distance or cross vCenter vMotion is used, the vMotion network can be routable but must be accessible to only the intended ESXi hosts. If the vMotion port group is not on an isolated VLAN and/or is routable to systems other than ESXi hosts, this is a finding.	

Test 22 CCI-002420

Maintain the confidentiality and/or integrity of information during preparation for transmission.

NIST SP 800-53 Revision 5::SC-8 (2)

CCI-002422

Maintain the confidentiality and/or integrity of information during reception.

NIST SP 800-53 Revision 5::SC-8 (2)

<table>
<tr><th>Step</th><th>Step Description</th><th>Expected Results/Comments</th><th>P/F</th></tr>
<tr><td>22</td><td>The ESXi host must maintain the confidentiality and integrity of information during transmission by exclusively enabling Transport Layer Security (TLS) 1.2.</td><td>From the vSphere Client, go to Hosts and Clusters.
Select the ESXi Host >> Configure >> System >> Advanced System Settings.
Select the "UserVars.ESXiVPsDisabledProtocols" value and verify it is set to "sslv3,tlsv1,tlsv1.1".
or
From a PowerCLI command prompt while connected to the ESXi host, run the following command:
Get-VMHost | Get-AdvancedSetting -Name UserVars.ESXiVPsDisabledProtocols
If the "UserVars.ESXiVPsDisabledProtocols" setting is set to a value other than "sslv3,tlsv1,tlsv1.1", this is a finding.</td><td></td></tr>
<tr><td colspan="4"><b>Test 23 CCI-002450</b>
<b>Implement organization-defined types of cryptography for each specified cryptography use.</b>
<b>NIST SP 800-53 Revision 5::SC-13 b</b></td></tr>
</table>

<table>
<tr><th>Step</th><th>Step Description</th><th>Expected Results/Comments</th><th>P/F</th></tr>
<tr><td>23</td><td>The ESXi host Secure Shell (SSH) daemon must be configured to only use FIPS 140-2 validated ciphers.</td><td>From an ESXi shell, run the following command:
esxcli system ssh server config list -k ciphers
or
From a PowerCLI command prompt while connected to the ESXi host, run the following commands:
$esxcli = Get-EsxCli -v2
$esxcli.system.ssh.server.config.list.invoke() | Where-Object {$_.Key -eq 'ciphers'}
Expected result:
ciphers aes256-gcm@openssh.com,aes128-gcm@openssh.com,aes256-ctr,aes192-ctr,aes128-ctr
If the output matches the ciphers in the expected result or a subset thereof, this is not a finding.
If the ciphers in the output contain any ciphers not listed in the expected result, this is a finding.</td><td></td></tr>
</table>

Test 24 CCI-000366

Implement the security configuration settings.

NIST SP 800-53 Revision 5::CM-6 b

Step	Step Description	Expected Results/Comments	P/F
24	The ESXi host DCUI.Access list must be verified.	For environments that do not use vCenter server to manage ESXi, this is not applicable. From the vSphere Client, go to Hosts and Clusters. Select the ESXi Host >> Configure >> System >> Advanced System Settings. Select the "DCUI.Access" value and verify only the root user is listed. or From a PowerCLI command prompt while connected to the ESXi host, run the following command: Get-VMHost | Get-AdvancedSetting -Name DCUI.Access and verify it is set to root. If the "DCUI.Access" is not restricted to "root", this is a finding. Note: This list is only for local user accounts and should only contain the root user.	

Test 25 CCI-000048

Display an organization-defined system use notification message or banner to users before granting access to the system that provides privacy and security notices consistent with applicable federal laws, Executive Orders, directives, policies, regulations, standards, and guidelines.

NIST SP 800-53 Revision 5::AC-8 a

Step	Step Description	Expected Results/Comments	P/F
25	The ESXi host must display the Standard Mandatory DOD Notice and Consent Banner before granting access to the system via Secure Shell (SSH).	From the vSphere Client, go to Hosts and Clusters. Select the ESXi Host >> Configure >> System >> Advanced System Settings. Select the "Config.Etc.issue" value and verify it contains the standard mandatory DOD notice and consent banner. or From a PowerCLI command prompt while connected to the ESXi host, run the following command: Get-VMHost | Get-AdvancedSetting -Name Config.Etc.issue If the "Config.Etc.issue" setting does not contain the standard mandatory DOD notice and consent banner, this is a finding.	

Test 26 CCI-000048

Display an organization-defined system use notification message or banner to users before granting access to the system that provides privacy and security notices consistent with applicable federal laws, Executive Orders, directives, policies, regulations, standards, and guidelines.

NIST SP 800-53 Revision 5::AC-8 a

Step	Step Description	Expected Results/Comments	P/F
26	The ESXi host Secure Shell (SSH) daemon must display the Standard Mandatory DOD Notice and Consent Banner before granting access to the system.	From an ESXi shell, run the following command: # esxcli system ssh server config list -k banner or From a PowerCLI command prompt while connected to the ESXi host, run the following commands: $esxcli = Get-EsxCli -v2 $esxcli.system.ssh.server.config.list.invoke() \| Where-Object {$_.Key -eq 'banner'} Example result: banner /etc/issue If "banner" is not configured to "/etc/issue", this is a finding.	

Test 27 CCI-000381

Configure the system to provide only organization-defined mission essential capabilities.

NIST SP 800-53 Revision 5::CM-7 a

CCI-002314

Employ automated mechanisms to control remote access methods.

NIST SP 800-53 Revision 5::AC-17 (1)

CCI-002322

Provide the capability to disconnect or disable remote access to the system within the organization-defined time period.

NIST SP 800-53 Revision 5::AC-17 (9)

Step	Step Description	Expected Results/Comments	P/F
27	The ESXi host must be configured to disable nonessential capabilities by disabling Secure Shell (SSH).	From the vSphere Client, go to Hosts and Clusters. Select the ESXi Host >> Configure >> System >> Services. Under Services, locate the "SSH" service and verify it is "Stopped". or From a PowerCLI command prompt while connected to the ESXi host, run the following command: Get-VMHost | Get-VMHostService | Where {$_.Label -eq "SSH"} If the SSH service is "Running", this is a finding.	

Test 28 CCI-000381

Configure the system to provide only organization-defined mission essential capabilities.

NIST SP 800-53 Revision 5::CM-7 a

Step	Step Description	Expected Results/Comments	P/F
28	The ESXi host must be configured to disable nonessential capabilities by disabling the ESXi shell.	From the vSphere Client, go to Hosts and Clusters. Select the ESXi Host >> Configure >> System >> Services. Under Services, locate the "ESXi Shell" service and verify it is "Stopped". or From a PowerCLI command prompt while connected to the ESXi host, run the following command: Get-VMHost | Get-VMHostService | Where {$_.Label -eq "ESXi Shell"} If the ESXi Shell service is "Running", this is a finding.	

Test 29 CCI-001133

Terminate the network connection associated with a communications session at the end of the session or after an organization-defined time period of inactivity.

NIST SP 800-53 Revision 5::SC-10

Step	Step Description	Expected Results/Comments	P/F
29	The ESXi host must automatically stop shell services after 10 minutes.	From the vSphere Client, go to Hosts and Clusters. Select the ESXi Host >> Configure >> System >> Advanced System Settings. Select the "UserVars.ESXiShellTimeOut" value and verify it is set to less than "600" and not "0". or From a PowerCLI command prompt while connected to the ESXi host, run the following command: Get-VMHost | Get-AdvancedSetting -Name UserVars.ESXiShellTimeOut If the "UserVars.ESXiShellTimeOut" setting is set to a value greater than "600" or "0", this is a finding.	

Test 30 CCI-001133

Terminate the network connection associated with a communications session at the end of the session or after an organization-defined time period of inactivity.

NIST SP 800-53 Revision 5::SC-10

Step	Step Description	Expected Results/Comments	P/F
30	The ESXi host must set a timeout to automatically end idle DCUI sessions after 10 minutes.	From the vSphere Client, go to Hosts and Clusters. Select the ESXi Host >> Configure >> System >> Advanced System Settings. Select the "UserVars.DcuiTimeOut" value and verify it is set to less than "600" and not "0". or From a PowerCLI command prompt while connected to the ESXi host, run the following command: Get-VMHost | Get-AdvancedSetting -Name UserVars.DcuiTimeOut If the "UserVars.DcuiTimeOut" setting is set to a value greater than "600" or "0", this is a finding.	

Test 31 CCI-002418

Protect the confidentiality and/or integrity of transmitted information.

NIST SP 800-53 Revision 5::SC-8

Step	Step Description	Expected Results/Comments	P/F
31	The ESXi host must protect the confidentiality and integrity of transmitted information by isolating ESXi management traffic.	From the vSphere Client, go to Hosts and Clusters. Select the ESXi Host >> Configure >> Networking >> VMkernel adapters. Review each VMkernel adapter that is used for management traffic and view the "Enabled services". Review the VLAN associated with each VMkernel that is used for management traffic. Verify with the system administrator that they are dedicated for that purpose and are logically separated from other functions. If any services other than "Management" are enabled on the Management VMkernel adapter, this is a finding. If the network segment is accessible, except to networks where other management-related entities are located such as vCenter, this is a finding. If there are any other systems or devices such as VMs on the ESXi management segment, this is a finding.	

Test 32 CCI-002418

Protect the confidentiality and/or integrity of transmitted information.

NIST SP 800-53 Revision 5::SC-8

Step	Step Description	Expected Results/Comments	P/F
32	The ESXi host must protect the confidentiality and integrity of transmitted information by isolating IP-based storage traffic.	If IP-based storage is not used, this is not applicable. From the vSphere Client, go to Hosts and Clusters. Select the ESXi Host >> Configure >> Networking >> VMkernel adapters. Review each VMkernel adapter that is used for IP-based storage traffic and view the "Enabled services". Review the VLAN associated with each VMkernel that is used for IP-based storage traffic. Verify with the system administrator that they are dedicated for that purpose and are logically separated from other functions. If any services are enabled on an NFS or iSCSI IP-based storage VMkernel adapter, this is a finding. If any services are enabled on a vSAN VMkernel adapter other than vSAN, this is a finding. If any IP-based storage networks are not isolated from other traffic types, this is a finding.	

Test 33 CCI-000366

Implement the security configuration settings.

NIST SP 800-53 Revision 5::CM-6 b

Step	Step Description	Expected Results/Comments	P/F
33	The ESXi host lockdown mode exception users list must be verified.	For environments that do not use vCenter server to manage ESXi, this is not applicable. From the vSphere Client, go to Hosts and Clusters. Select the ESXi Host >> Configure >> System >> Security Profile. Under "Lockdown Mode", review the Exception Users list. or From a PowerCLI command prompt while connected to the ESXi host, run the following script: $vmhost = Get-VMHost | Get-View $lockdown = Get-View $vmhost.ConfigManager.HostAccessManager $lockdown.QueryLockdownExceptions() If the Exception Users list contains accounts that do not require special permissions, this is a finding. Note: The Exception Users list is empty by default and should remain that way except under site-specific circumstances.	

Test 34 CCI-000366

Implement the security configuration settings.

NIST SP 800-53 Revision 5::CM-6 b

Step	Step Description	Expected Results/Comments	P/F
34	The ESXi host Secure Shell (SSH) daemon must not allow host-based authentication.	From an ESXi shell, run the following command: # esxcli system ssh server config list -k hostbasedauthentication or From a PowerCLI command prompt while connected to the ESXi host, run the following commands: $esxcli = Get-EsxCli -v2 $esxcli.system.ssh.server.config.list.invoke() \| Where-Object {$_.Key -eq 'hostbasedauthentication'} Example result: hostbasedauthentication no If "hostbasedauthentication" is not configured to "no", this is a finding.	
Test 35 CCI-000366 **Implement the security configuration settings.** **NIST SP 800-53 Revision 5::CM-6 b**			

Step	Step Description	Expected Results/Comments	P/F
35	The ESXi host Secure Shell (SSH) daemon must not permit user environment settings.	From an ESXi shell, run the following command: # esxcli system ssh server config list -k permituserenvironment or From a PowerCLI command prompt while connected to the ESXi host, run the following commands: $esxcli = Get-EsxCli -v2 $esxcli.system.ssh.server.config.list.invoke() \| Where-Object {$_.Key -eq 'permituserenvironment'} Example result: permituserenvironment no If "permituserenvironment" is not configured to "no", this is a finding.	
Test 36 CCI-000366 **Implement the security configuration settings.** **NIST SP 800-53 Revision 5::CM-6 b**			

Step	Step Description	Expected Results/Comments	P/F
36	The ESXi host Secure Shell (SSH) daemon must be configured to not allow gateway ports.	From an ESXi shell, run the following command: # esxcli system ssh server config list -k gatewayports or From a PowerCLI command prompt while connected to the ESXi host, run the following commands: $esxcli = Get-EsxCli -v2 $esxcli.system.ssh.server.config.list.invoke() \| Where-Object {$_.Key -eq 'gatewayports'} Example result: gatewayports no If "gatewayports" is not configured to "no", this is a finding.	
Test 37 CCI-000366 **Implement the security configuration settings.** **NIST SP 800-53 Revision 5::CM-6 b**			

Step	Step Description	Expected Results/Comments	P/F
37	The ESXi host Secure Shell (SSH) daemon must not permit tunnels.	From an ESXi shell, run the following command: # esxcli system ssh server config list -k permittunnel or From a PowerCLI command prompt while connected to the ESXi host, run the following commands: $esxcli = Get-EsxCli -v2 $esxcli.system.ssh.server.config.list.invoke() \| Where-Object {$_.Key -eq 'permittunnel'} Example result: permittunnel no If "permittunnel" is not configured to "no", this is a finding.	
Test 38 CCI-000366 **Implement the security configuration settings.** **NIST SP 800-53 Revision 5::CM-6 b**			

Step	Step Description	Expected Results/Comments	P/F
38	The ESXi host Secure Shell (SSH) daemon must set a timeout count on idle sessions.	From an ESXi shell, run the following command: # esxcli system ssh server config list -k clientalivecountmax or From a PowerCLI command prompt while connected to the ESXi host, run the following commands: $esxcli = Get-EsxCli -v2 $esxcli.system.ssh.server.config.list.invoke() \| Where-Object {$_.Key -eq 'clientalivecountmax'} Example result: clientalivecountmax 3 If "clientalivecountmax" is not configured to "3", this is a finding.	

Test 39 CCI-000366

Implement the security configuration settings.

NIST SP 800-53 Revision 5::CM-6 b

Step	Step Description	Expected Results/Comments	P/F
39	The ESXi host Secure Shell (SSH) daemon must set a timeout interval on idle sessions.	From an ESXi shell, run the following command: # esxcli system ssh server config list -k clientaliveinterval or From a PowerCLI command prompt while connected to the ESXi host, run the following commands: $esxcli = Get-EsxCli -v2 $esxcli.system.ssh.server.config.list.invoke() \| Where-Object {$_.Key -eq 'clientaliveinterval'} Example result: clientaliveinterval 200 If "clientaliveinterval" is not configured to "200", this is a finding.	
Test 40 CCI-000366 **Implement the security configuration settings.** **NIST SP 800-53 Revision 5::CM-6 b**			

Step	Step Description	Expected Results/Comments	P/F
40	The ESXi host must disable Simple Network Management Protocol (SNMP) v1 and v2c.	From an ESXi shell, run the following command: # esxcli system snmp get or From a PowerCLI command prompt while connected to the ESXi host, run the following command: Get-VMHostSnmp | Select * If SNMP is not in use and is enabled, this is a finding. If SNMP is enabled and is not using v3 targets with authentication, this is a finding. Note: SNMP v3 targets can only be viewed and configured via the "esxcli" command.	

Test 41 CCI-000366

Implement the security configuration settings.

NIST SP 800-53 Revision 5::CM-6 b

Step	Step Description	Expected Results/Comments	P/F
41	The ESXi host must disable Inter-Virtual Machine (VM) Transparent Page Sharing.	From the vSphere Client, go to Hosts and Clusters. Select the ESXi Host >> Configure >> System >> Advanced System Settings. Select the "Mem.ShareForceSalting" value and verify it is set to "2". or From a PowerCLI command prompt while connected to the ESXi host, run the following command: Get-VMHost | Get-AdvancedSetting -Name Mem.ShareForceSalting If the "Mem.ShareForceSalting" setting is not set to 2, this is a finding.	

Test 42 CCI-000366

Implement the security configuration settings.

NIST SP 800-53 Revision 5::CM-6 b

Step	Step Description	Expected Results/Comments	P/F
42	The ESXi host must configure the firewall to block network traffic by default.	From an ESXi shell, run the following command: # esxcli network firewall get If the "Default Action" does not equal "DROP", this is a finding. If "Enabled" does not equal "true", this is a finding. or From a PowerCLI command prompt while connected to the ESXi host, run the following command: Get-VMHostFirewallDefaultPolicy If the Incoming or Outgoing policies are "True", this is a finding.	
Test 43 CCI-000366 **Implement the security configuration settings.** **NIST SP 800-53 Revision 5::CM-6 b**			

Step	Step Description	Expected Results/Comments	P/F
43	The ESXi host must enable Bridge Protocol Data Units (BPDU) filter on the host to prevent being locked out of physical switch ports with Portfast and BPDU Guard enabled.	From the vSphere Client, go to Hosts and Clusters. Select the ESXi Host >> Configure >> System >> Advanced System Settings. Select the "Net.BlockGuestBPDU" value and verify it is set to "1". or From a PowerCLI command prompt while connected to the ESXi host, run the following command: Get-VMHost | Get-AdvancedSetting -Name Net.BlockGuestBPDU If the "Net.BlockGuestBPDU" setting is not set to "1", this is a finding.	
Test 44 CCI-000366 **Implement the security configuration settings.** **NIST SP 800-53 Revision 5::CM-6 b**			

Step	Step Description	Expected Results/Comments	P/F
44	The ESXi host must configure virtual switch security policies to reject forged transmits.	Note: This control addresses ESXi standard switches. Distributed switches are addressed in the vCenter STIG. If there is no standard switch on the ESXi host, this is not applicable. From the vSphere Client, go to Hosts and Clusters. Select the ESXi Host >> Configure >> Networking >> Virtual Switches. On each standard switch, click the '...' button next to each port group and select "Edit Settings". Click the "Security" tab. Verify that "Forged transmits" is set to "Reject" and that "Override" is not checked. or From a PowerCLI command prompt while connected to the ESXi host, run the following commands: Get-VirtualSwitch | Get-SecurityPolicy Get-VirtualPortGroup | Get-SecurityPolicy | Select-Object * If the "Forged Transmits" policy is set to "Accept" (or "true", via PowerCLI) or the security policy inherited from the virtual switch is overridden, this is a finding.	

Test 45 CCI-000366

Implement the security configuration settings.

NIST SP 800-53 Revision 5::CM-6 b

Step	Step Description	Expected Results/Comments	P/F
45	The ESXi host must configure virtual switch security policies to reject Media Access Control (MAC) address changes.	This control addresses ESXi standard switches. Distributed switches are addressed in the vCenter STIG. If there is no standard switch on the ESXi host, this is not applicable. From the vSphere Client, go to Hosts and Clusters. Select the ESXi Host >> Configure >> Networking >> Virtual Switches. On each standard switch, click the '...' button next to each port group and select "Edit Settings". Click the "Security" tab. Verify that "MAC Address Changes" is set to "Reject" and that "Override" is not checked. or From a PowerCLI command prompt while connected to the ESXi host, run the following commands: Get-VirtualSwitch | Get-SecurityPolicy Get-VirtualPortGroup | Get-SecurityPolicy | Select-Object * If the "MAC Address Changes" policy is set to "Accept" (or "true", via PowerCLI) or the security policy inherited from the virtual switch is overridden, this is a finding.	

Test 46 CCI-000366

Implement the security configuration settings.

NIST SP 800-53 Revision 5::CM-6 b

Step	Step Description	Expected Results/Comments	P/F
46	The ESXi host must configure virtual switch security policies to reject promiscuous mode requests.	This control addresses ESXi standard switches. Distributed switches are addressed in the vCenter STIG. If there is no standard switch on the ESXi host, this is not applicable. From the vSphere Client, go to Hosts and Clusters. Select the ESXi Host >> Configure >> Networking >> Virtual Switches. On each standard switch, click the '...' button next to each port group and select "Edit Settings". Click the "Security" tab. Verify that "Promiscuous Mode" is set to "Reject" and that "Override" is not checked. or From a PowerCLI command prompt while connected to the ESXi host, run the following commands: Get-VirtualSwitch | Get-SecurityPolicy Get-VirtualPortGroup | Get-SecurityPolicy | Select-Object * If the "Promiscuous Mode" policy is set to "Accept" (or "true", via PowerCLI) or the security policy inherited from the virtual switch is overridden, this is a finding.	

Test 47 CCI-000366

Implement the security configuration settings.

NIST SP 800-53 Revision 5::CM-6 b

Step	Step Description	Expected Results/Comments	P/F
47	The ESXi host must restrict use of the dvFilter network application programming interface (API).	From the vSphere Client, go to Hosts and Clusters. Select the ESXi Host >> Configure >> System >> Advanced System Settings. Select the "Net.DVFilterBindIpAddress" value and verify the value is blank or the correct IP address of a security appliance if in use. or From a PowerCLI command prompt while connected to the ESXi host, run the following command: Get-VMHost | Get-AdvancedSetting -Name Net.DVFilterBindIpAddress If the "Net.DVFilterBindIpAddress" setting is not blank and security appliances are not in use on the host, this is a finding.	
Test 48 CCI-000366 **Implement the security configuration settings.** **NIST SP 800-53 Revision 5::CM-6 b**			

Step	Step Description	Expected Results/Comments	P/F
48	The ESXi host must restrict the use of Virtual Guest Tagging (VGT) on standard switches.	This control addresses ESXi standard switches. Distributed switches are addressed in the vCenter STIG. If there is no standard switch on the ESXi host, this is not applicable. From the vSphere Client, go to Hosts and Clusters. Select the ESXi Host >> Configure >> Networking >> Virtual Switches. For each standard switch, review the "VLAN ID" on each port group and verify it is not set to "4095". or From a PowerCLI command prompt while connected to the ESXi host, run the following command: Get-VirtualPortGroup | Select Name, VLanID If any port group is configured with VLAN 4095 and is not documented as a needed exception, this is a finding.	

Test 49 CCI-000366

Implement the security configuration settings.

NIST SP 800-53 Revision 5::CM-6 b

Step	Step Description	Expected Results/Comments	P/F
49	The ESXi host must have all security patches and updates installed.	Determine the current version and build: From the vSphere Client, go to Hosts and Clusters. Select the ESXi Host >> Summary. Note the version string next to "Hypervisor:". or From a Secure Shell (SSH) session connected to the ESXi host, or from the ESXi shell, run the following command: # vmware -v If the ESXi host does not have the latest patches, this is a finding. If the ESXi host is not on a supported release, this is a finding. The latest ESXi versions and their build numbers can be found here: https://kb.vmware.com/s/article/2143832 VMware also publishes advisories on security patches and offers a way to subscribe to email alerts for them. Go to: https://www.vmware.com/support/policies/security_response	

Test 50 CCI-000366

Implement the security configuration settings.

NIST SP 800-53 Revision 5::CM-6 b

Step	Step Description	Expected Results/Comments	P/F
50	The ESXi host must not suppress warnings that the local or remote shell sessions are enabled.	From the vSphere Client, go to Hosts and Clusters. Select the ESXi Host >> Configure >> System >> Advanced System Settings. Select the "UserVars.SuppressShellWarning" value and verify it is set to "0". or From a PowerCLI command prompt while connected to the ESXi host, run the following command: Get-VMHost | Get-AdvancedSetting -Name UserVars.SuppressShellWarning If the "UserVars.SuppressShellWarning" setting is not set to "0", this is a finding.	
Test 51 CCI-000366 **Implement the security configuration settings.** **NIST SP 800-53 Revision 5::CM-6 b**			

Step	Step Description	Expected Results/Comments	P/F
51	The ESXi host must not suppress warnings about unmitigated hyperthreading vulnerabilities.	From the vSphere Client go to Hosts and Clusters. Select the ESXi Host >> Configure >> System >> Advanced System Settings. Select the "UserVars.SuppressHyperthreadWarning" value and verify it is set to "0". or From a PowerCLI command prompt while connected to the ESXi host, run the following command: Get-VMHost | Get-AdvancedSetting -Name UserVars.SuppressHyperthreadWarning If the "UserVars.SuppressHyperthreadWarning" setting is not set to "0", this is a finding.	

Test 52 CCI-000366

Implement the security configuration settings.

NIST SP 800-53 Revision 5::CM-6 b

Step	Step Description	Expected Results/Comments	P/F
52	The ESXi host must verify certificates for SSL syslog endpoints.	If SSL is not used for a syslog target, this is not applicable. From the vSphere Client, go to Hosts and Clusters. Select the ESXi Host >> Configure >> System >> Advanced System Settings. Select the "Syslog.global.logCheckSSLCerts" value and verify it is set to "true". or From a PowerCLI command prompt while connected to the ESXi host, run the following command: Get-VMHost | Get-AdvancedSetting -Name Syslog.global.logCheckSSLCerts If the "Syslog.global.logCheckSSLCerts" setting is not set to "true", this is a finding.	

Test 53 CCI-000366

Implement the security configuration settings.

NIST SP 800-53 Revision 5::CM-6 b

Step	Step Description	Expected Results/Comments	P/F
53	The ESXi host must enable volatile key destruction.	From the vSphere Client, go to Hosts and Clusters. Select the ESXi Host >> Configure >> System >> Advanced System Settings. Select the "Mem.MemEagerZero" value and verify it is set to "1". or From a PowerCLI command prompt while connected to the ESXi host, run the following command: Get-VMHost | Get-AdvancedSetting -Name Mem.MemEagerZero If the "Mem.MemEagerZero" setting is not set to "1", this is a finding.	

Test 54 CCI-000366

Implement the security configuration settings.

NIST SP 800-53 Revision 5::CM-6 b

Step	Step Description	Expected Results/Comments	P/F
54	The ESXi host must configure a session timeout for the vSphere API.	From the vSphere Client, go to Hosts and Clusters. Select the ESXi Host >> Configure >> System >> Advanced System Settings. Select the "Config.HostAgent.vmacore.soap.sessionTimeout" value and verify it is set to "30". or From a PowerCLI command prompt while connected to the ESXi host, run the following command: Get-VMHost | Get-AdvancedSetting -Name Config.HostAgent.vmacore.soap.sessionTimeout If the "Config.HostAgent.vmacore.soap.sessionTimeout" setting is not set to "30", this is a finding.	
Test 55 CCI-000366 **Implement the security configuration settings.** **NIST SP 800-53 Revision 5::CM-6 b**			

Step	Step Description	Expected Results/Comments	P/F
55	The ESXi host must be configured with an appropriate maximum password age.	From the vSphere Client, go to Hosts and Clusters. Select the ESXi Host >> Configure >> System >> Advanced System Settings. Select the "Security.PasswordMaxDays" value and verify it is set to "90". or From a PowerCLI command prompt while connected to the ESXi host, run the following command: Get-VMHost | Get-AdvancedSetting -Name Security.PasswordMaxDays If the "Security.PasswordMaxDays" setting is not set to "90", this is a finding.	

Test 56 CCI-000366

Implement the security configuration settings.

NIST SP 800-53 Revision 5::CM-6 b

Step	Step Description	Expected Results/Comments	P/F
56	The ESXi Common Information Model (CIM) service must be disabled.	From the vSphere Client, go to Hosts and Clusters. Select the ESXi Host >> Configure >> System >> Services. Under "Services", locate the "CIM Server" service and verify it is "Stopped" and the "Startup Policy" is set to "Start and stop manually". or From a PowerCLI command prompt while connected to the ESXi host, run the following command: Get-VMHost | Get-VMHostService | Where {$_.Label -eq "CIM Server"} If the "CIM Server" service does not have a "Policy" of "off" or is running, this is a finding.	
Test 57 CCI-000366 **Implement the security configuration settings.** **NIST SP 800-53 Revision 5::CM-6 b**			
57	The ESXi host must use DOD-approved certificates.	From the vSphere Client, go to Hosts and Clusters. Select the ESXi Host >> Configure >> System >> Certificate. If the issuer is not a DOD-approved certificate authority, this is a finding. If the host will never be accessed directly (virtual machine console connections bypass vCenter), this is not a finding.	
Test 58 CCI-000366 **Implement the security configuration settings.** **NIST SP 800-53 Revision 5::CM-6 b**			

Step	Step Description	Expected Results/Comments	P/F
58	The ESXi host Secure Shell (SSH) daemon must disable port forwarding.	From an ESXi shell, run the following command: # esxcli system ssh server config list -k allowtcpforwarding or From a PowerCLI command prompt while connected to the ESXi host, run the following commands: $esxcli = Get-EsxCli -v2 $esxcli.system.ssh.server.config.list.invoke() \| Where-Object {$_.Key -eq 'allowtcpforwarding'} Example result: allowtcpforwarding no If "allowtcpforwarding" is not configured to "no", this is a finding.	

Test 59 CCI-000366

Implement the security configuration settings.

NIST SP 800-53 Revision 5::CM-6 b

Step	Step Description	Expected Results/Comments	P/F
59	The ESXi host OpenSLP service must be disabled.	From the vSphere Client go to Hosts and Clusters. Select the ESXi Host >> Configure >> System >> Services. Under "Services", locate the "slpd" service and verify it is "Stopped" and the "Startup Policy" is set to "Start and stop manually". or From a PowerCLI command prompt while connected to the ESXi host, run the following command: Get-VMHost | Get-VMHostService | Where {$_.Label -eq "slpd"} If the slpd service does not have a "Policy" of "off" or is running, this is a finding.	
Test 60 CCI-000366 **Implement the security configuration settings.** **NIST SP 800-53 Revision 5::CM-6 b**			

Step	Step Description	Expected Results/Comments	P/F
60	The ESXi host must enable audit logging.	From the vSphere Client, go to Hosts and Clusters. Select the ESXi Host >> Configure >> System >> Advanced System Settings. Select the "Syslog.global.auditRecord.storageEnable" value and verify it is set to "true". or From a PowerCLI command prompt while connected to the ESXi host, run the following command: Get-VMHost | Get-AdvancedSetting -Name Syslog.global.auditRecord.storageEnable If the "Syslog.global.auditRecord.storageEnable" setting is not set to "true", this is a finding.	

Test 61 CCI-001851

Transfer audit logs per organization-defined frequency to a different system, system component, or media than the system or system component conducting the logging.

NIST SP 800-53 Revision 5::AU-4 (1)

Step	Step Description	Expected Results/Comments	P/F
61	The ESXi host must off-load audit records via syslog.	From the vSphere Client, go to Hosts and Clusters. Select the ESXi Host >> Configure >> System >> Advanced System Settings. Select the "Syslog.global.auditRecord.remoteEnable" value and verify it is set to "true". or From a PowerCLI command prompt while connected to the ESXi host, run the following command: Get-VMHost | Get-AdvancedSetting -Name Syslog.global.auditRecord.remoteEnable If the "Syslog.global.auditRecord.remoteEnable" setting is not set to "true", this is a finding.	
Test 62 CCI-000366 **Implement the security configuration settings.** **NIST SP 800-53 Revision 5::CM-6 b**			

Step	Step Description	Expected Results/Comments	P/F
62	The ESXi host must enable strict x509 verification for SSL syslog endpoints.	If SSL is not used for a syslog target, this is not applicable. From the vSphere Client, go to Hosts and Clusters. Select the ESXi Host >> Configure >> System >> Advanced System Settings. Select the "Syslog.global.certificate.strictX509Compliance" value and verify it is set to "true". or From a PowerCLI command prompt while connected to the ESXi host, run the following command: Get-VMHost | Get-AdvancedSetting -Name Syslog.global.certificate.strictX509Compliance If the "Syslog.global.certificate.strictX509Compliance" setting is not set to "true", this is a finding.	
Test 63 CCI-000130 **Ensure that audit records containing information that establishes what type of event occurred.** **NIST SP 800-53 Revision 5::AU-3 a**			

Step	Step Description	Expected Results/Comments	P/F
63	The ESXi host must forward audit records containing information to establish what type of events occurred.	From the vSphere Client, go to Hosts and Clusters. Select the ESXi Host >> Configure >> System >> Advanced System Settings. Select the "Syslog.global.logLevel" value and verify it is set to "info". or From a PowerCLI command prompt while connected to the ESXi host, run the following command: Get-VMHost | Get-AdvancedSetting -Name Syslog.global.logLevel If the "Syslog.global.logLevel" setting is not set to "info", this is a finding. Note: Verbose logging level is acceptable for troubleshooting purposes.	
Test 64 CCI-000366 **Implement the security configuration settings.** **NIST SP 800-53 Revision 5::CM-6 b**			
64	The ESXi host must not be configured to override virtual machine (VM) configurations.	From an ESXi shell, run the following command: # stat -c "%s" /etc/vmware/settings Expected result: 0 If the output does not match the expected result, this is a finding.	
Test 65 CCI-000366 **Implement the security configuration settings.** **NIST SP 800-53 Revision 5::CM-6 b**			

Step	Step Description	Expected Results/Comments	P/F
65	The ESXi host must not be configured to override virtual machine (VM) logger settings.	From an ESXi shell, run the following command: # grep "^vmx\.log" /etc/vmware/config If the command produces any output, this is a finding.	

Test 66 CCI-000366

Implement the security configuration settings.

NIST SP 800-53 Revision 5::CM-6 b

66	The ESXi host must require TPM-based configuration encryption.	If the ESXi host does not have a compatible TPM, this finding is downgraded to a CAT III. From an ESXi shell, run the following command: # esxcli system settings encryption get or From a PowerCLI command prompt while connected to the ESXi host, run the following commands: $esxcli = Get-EsxCli -v2 $esxcli.system.settings.encryption.get.invoke() | Select Mode Expected result: Mode: TPM If the "Mode" is not set to "TPM", this is a finding.	

Test 67 CCI-000366

Implement the security configuration settings.

NIST SP 800-53 Revision 5::CM-6 b

<table>
<tr><th>Step</th><th>Step Description</th><th>Expected Results/Comments</th><th>P/F</th></tr>
<tr><td>67</td><td>The ESXi host must configure the firewall to restrict access to services running on the host.</td><td>From the vSphere Client, go to Hosts and Clusters.

Select the ESXi Host >> Configure >> System >> Firewall.

Under the "Allowed IP addresses" column, review the allowed IPs for each service.

Check this for "Incoming" and "Outgoing" sections.

or

From a PowerCLI command prompt while connected to the ESXi host, run the following command:

Get-VMHost | Get-VMHostFirewallException | Where {$_.Enabled -eq $true} | Select Name,Enabled,@{N="AllIPEnabled";E={ $_.ExtensionData.AllowedHosts.AllIP }}

If for an enabled service "Allow connections from any IP address" is selected, this is a finding.</td><td></td></tr>
<tr><td colspan="4"><b>Test 68 CCI-000366</b>
<b>Implement the security configuration settings.</b>
<b>NIST SP 800-53 Revision 5::CM-6 b</b></td></tr>
</table>

<table>
<tr><th>Step</th><th>Step Description</th><th>Expected Results/Comments</th><th>P/F</th></tr>
<tr><td>68</td><td>The ESXi host when using Host Profiles and/or Auto Deploy must use the vSphere Authentication Proxy to protect passwords when adding themselves to Active Directory.</td><td>For environments that do not use vCenter server to manage ESXi, this is not applicable.

If the organization is not using Host Profiles to join Active Directory, this is not applicable.

From the vSphere Client, go to Home >> Policies and Profiles >> Host Profiles.

Click a Host Profile >> Configure >> Security and Services >> Security Settings >> Authentication Configuration >> Active Directory Configuration >> Join Domain Method.

If the method used to join hosts to a domain is not set to "Use vSphere Authentication Proxy to add the host to domain", this is a finding.

or

From a PowerCLI command prompt while connected to vCenter, run the following command:

Get-VMHost | Select Name, `<br>@{N="HostProfile";E={$_ | Get-VMHostProfile}}, `
@{N="JoinADEnabled";E={($_ | Get-VmHostProfile).ExtensionData.Config.ApplyProfile.Authentication.ActiveDirectory.Enabled}}, `
@{N="JoinDomainMethod";E={(($_ | Get-VMHostProfile).ExtensionData.Config.ApplyProfile.Authentication.ActiveDirectory | Select -ExpandProperty Policy | Where {$_.Id -eq "JoinDomainMethodPolicy"}).Policyoption.Id}}
If "JoinADEnabled" is "True" and "JoinDomainMethod" is not "FixedCAMConfigOption", this is a finding.</td><td></td></tr>
</table>

Step	Step Description	Expected Results/Comments	P/F
Test 69 CCI-000366 **Implement the security configuration settings.** **NIST SP 800-53 Revision 5::CM-6 b**			
69	The ESXi host must not use the default Active Directory ESX Admin group.	For systems that do not use Active Directory, this is not applicable. From the vSphere Client, go to Hosts and Clusters. Select the ESXi Host >> Configure >> System >> Advanced System Settings. Select the "Config.HostAgent.plugins.hostsvc.esxAdminsGroup" value and verify it is not set to "ESX Admins". or From a PowerCLI command prompt while connected to the ESXi host, run the following command: Get-VMHost | Get-AdvancedSetting -Name Config.HostAgent.plugins.hostsvc.esxAdminsGroup If the "Config.HostAgent.plugins.hostsvc.esxAdminsGroup" setting is set to "ESX Admins", this is a finding.	
Test 70 CCI-001849 **Allocate audit log storage capacity to accommodate organization-defined audit record retention requirements.** **NIST SP 800-53 Revision 5::AU-4**			

Step	Step Description	Expected Results/Comments	P/F
70	The ESXi host must configure a persistent log location for all locally stored logs.	From the vSphere Client, go to Hosts and Clusters. Select the ESXi Host >> Configure >> System >> Advanced System Settings. Select the "Syslog.global.logDir" value and verify it is set to a persistent location. If the value of the setting is "[] /scratch/logs", verify the advanced setting "ScratchConfig.CurrentScratchLocation" is not set to "/tmp/scratch". This is a nonpersistent location. If "Syslog.global.logDir" is not configured to a persistent location, this is a finding. or From a PowerCLI command prompt while connected to the ESXi host, run the following commands: $esxcli = Get-EsxCli -v2 $esxcli.system.syslog.config.get.Invoke() | Select LocalLogOutput,LocalLogOutputIsPersistent If the "LocalLogOutputIsPersistent" value is not true, this is a finding.	
Test 71 CCI-000366 **Implement the security configuration settings.** **NIST SP 800-53 Revision 5::CM-6 b**			

<table>
<tr><th>Step</th><th>Step Description</th><th>Expected Results/Comments</th><th>P/F</th></tr>
<tr><td>71</td><td>The ESXi host must enforce the exclusive running of executables from approved VIBs.</td><td>If the ESXi host does not have a compatible TPM, this finding is downgraded to a CAT III.
From the vSphere Client, go to Hosts and Clusters.
Select the ESXi Host >> Configure >> System >> Advanced System Settings.
Select the "VMkernel.Boot.execInstalledOnly" value and verify that it is "true".
or
From a PowerCLI command prompt while connected to the ESXi host, run the following command:
Get-VMHost | Get-AdvancedSetting -Name VMkernel.Boot.execInstalledOnly
If the "VMkernel.Boot.execInstalledOnly" setting is not "true", this is a finding.</td><td></td></tr>
<tr><td colspan="4"><b>Test 72 CCI-000366</b>
<b>Implement the security configuration settings.</b>
<b>NIST SP 800-53 Revision 5::CM-6 b</b></td></tr>
</table>

<table>
<tr><th>Step</th><th>Step Description</th><th>Expected Results/Comments</th><th>P/F</th></tr>
<tr><td>72</td><td>The ESXi host must use sufficient entropy for cryptographic operations.</td><td>From an ESXi shell, run the following commands:
esxcli system settings kernel list -o disableHwrng
esxcli system settings kernel list -o entropySources
or
From a PowerCLI command prompt while connected to the ESXi host, run the following commands:
$esxcli = Get-EsxCli -v2
$esxcli.system.settings.kernel.list.invoke() | Where {$_.Name -eq "disableHwrng" -or $_.Name -eq "entropySources"}
If "disableHwrng" is not set to "false", this is a finding.
If "entropySources" is not set to "0", this is a finding.</td><td></td></tr>
<tr><td colspan="4"><b>Test 73 CCI-000366</b>
<b>Implement the security configuration settings.</b>
<b>NIST SP 800-53 Revision 5::CM-6 b</b></td></tr>
</table>

Step	Step Description	Expected Results/Comments	P/F
73	The ESXi host must not enable log filtering.	From an ESXi shell, run the following command: # esxcli system syslog config logfilter get or From a PowerCLI command prompt while connected to the ESXi host, run the following commands: $esxcli = Get-EsxCli -v2 $esxcli.system.syslog.config.logfilter.get.invoke() If "LogFilteringEnabled" is not set to "false", this is a finding.	
Notes:			

4.2 Reporting

A final After Action Report (AAR) will be provided to all [ORGANIZATION] stakeholders within 30 days of completion of demonstration execution.