

**VMware, Inc.**

3401 Hillview Ave, Palo Alto, CA 94304, USA, Tel: (877) 486-9273, [www.vmware.com](http://www.vmware.com)

## Guidance Supplement

# VMware ESXi 7.0 Update 3d

**Common Criteria (CC) Evaluation with Protection Profile (PP) for  
Virtualization Version 1.1 with PP-Module for Server Virtualization Version 1.1 and  
Functional Package for Transport Layer Security (TLS) Version 1.1**

Document Version: 1.0  
Document Date: July 25, 2022



**VMware, Inc.**  
3401 Hillview Ave  
Palo Alto, CA 94304  
United States of America

Phone: +1 (877) 486-9273  
<http://www.vmware.com>

VMware Security Advisories, Certifications and Guides

<http://www.vmware.com/security>

VMware Security Response Center

[http://www.vmware.com/support/policies/security\\_response.html](http://www.vmware.com/support/policies/security_response.html)  
[security@vmware.com](mailto:security@vmware.com)

# REVISION HISTORY

Ver #	Description of changes	Modified by	Date
1.0	Initial release of document	Leidos	July 25, 2022

# TABLE OF CONTENTS

<b>1</b>	<b><i>Introduction</i></b> .....	<b>8</b>
1.1	<b>Purpose</b> .....	<b>8</b>
1.2	<b>Document Reference</b> .....	<b>8</b>
1.3	<b>Features and Functions Not Included in the TOE Evaluation</b> .....	<b>8</b>
<b>2</b>	<b><i>Installation Guidelines and Preparative Procedures</i></b> .....	<b>11</b>
2.1	<b>Assumptions</b> .....	<b>11</b>
2.2	<b>Evaluated Configuration</b> .....	<b>11</b>
2.3	<b>TOE Components</b> .....	<b>12</b>
2.4	<b>Installing the TOE</b> .....	<b>13</b>
2.4.1	Configure Firmware.....	13
2.4.2	Obtain Software .....	13
2.4.3	Install or Update Software .....	14
2.4.4	Verify Software .....	15
2.4.5	Additional ESXi Configuration .....	15
2.4.6	Additional Device Configuration.....	17
2.5	<b>Configuring the TOE Environmental Components</b> .....	<b>17</b>
2.5.1	Install ESXCLI for Remote Management.....	18
2.5.2	Configure Auditing .....	18
2.6	<b>Operating Modes</b> .....	<b>19</b>
2.7	<b>Obtaining Support</b> .....	<b>19</b>
2.8	<b>Ongoing Tracking for Security Issues and Mitigations</b> .....	<b>20</b>
<b>3</b>	<b><i>Operational Guidance: Advanced Settings</i></b> .....	<b>21</b>
3.1	<b>Configuring Advanced Options Using the Host Client</b> .....	<b>21</b>
3.2	<b>Configuring Advanced Settings Using the VIM API</b> .....	<b>21</b>
3.2.1	Querying Advanced Settings .....	21
3.2.2	Setting Advanced Settings .....	21
3.3	<b>Selected Advanced Settings</b> .....	<b>22</b>
<b>4</b>	<b><i>Operational Procedures for Administrators</i></b> .....	<b>24</b>
4.1	<b>Audit Configuration (FAU)</b> .....	<b>24</b>
4.1.1	Configuring Local Audit Records.....	24
4.1.2	Configuring Remote Audit Server .....	24
4.1.3	Viewing Audit Records .....	26
4.2	<b>Cryptographic Configuration (FCS)</b> .....	<b>26</b>
4.2.1	Cryptographic Key Generation .....	26
4.2.2	Cryptographic Key Establishment .....	27
4.2.3	Cryptographic Key Destruction .....	27

4.2.4	Cryptographic Operation .....	27
4.2.5	Random Bit Generation .....	27
4.2.6	Entropy for Virtual Machines .....	27
4.2.7	HTTPS .....	27
4.2.8	TLS Protocol.....	27
4.2.8.1	TLS Protocol Versions .....	28
4.2.8.2	TLS Cipher Suites .....	28
4.2.8.3	ECC Choices in TLS .....	29
<b>4.3</b>	<b>Protection of User (VM) Data (FDP).....</b>	<b>29</b>
4.3.1	Virtual Networking .....	29
4.3.2	Physical Platform Resources.....	30
4.3.2.1	USB .....	30
4.3.2.2	Physical Network .....	31
4.3.3	Memory Zeroization .....	31
4.3.4	Hardware-based VM Isolation .....	31
<b>4.4</b>	<b>Authentication Configuration (FIA) .....</b>	<b>31</b>
4.4.1	Authentication Failure Handling.....	32
4.4.2	Password Management .....	32
4.4.3	X.509 Certificate Validation and Authentication.....	32
<b>4.5</b>	<b>Security Management (FMT) .....</b>	<b>33</b>
4.5.1	Default Sharing Configurations .....	33
4.5.2	Isolating VM Networks from the Management Network .....	33
4.5.3	Management APIs (Consolidated).....	34
<b>4.6</b>	<b>Hypervisor Integrity (FPT).....</b>	<b>37</b>
4.6.1	Trusted Updates .....	37
4.6.2	Removable Devices and Media .....	37
4.6.2.1	USB devices .....	37
4.6.2.2	CD-ROM devices.....	38
<b>4.7</b>	<b>Accessing the Hypervisor (FTA) .....</b>	<b>38</b>
4.7.1	Session Timeouts .....	38
4.7.2	Administrative Access Banner.....	38
<b>4.8</b>	<b>Secure Communication with the Hypervisor (FTP) .....</b>	<b>38</b>
4.8.1	Establishing Remote Administrative Sessions.....	38
4.8.2	Configuring Remote Audit Servers .....	39
4.8.3	User Interface Indicators.....	39
<b>Appendix A: Audit Information .....</b>		<b>40</b>
<b>A.1</b>	<b>Audit Record Format.....</b>	<b>40</b>
A.1.1	Audit Record Structure in Local Storage.....	40
A.1.2	Audit Record Structure for Remote Syslog Transmission .....	40
A.1.3	Structured Data Frame Description.....	41
<b>A.2</b>	<b>Audit Record Types .....</b>	<b>41</b>
A.2.1	account.locked .....	41
A.2.2	audit.net.failure .....	42
A.2.3	audit.storage.recycle .....	42
A.2.4	audit.start .....	42
A.2.5	audit.stop.....	42
A.2.6	https.connect .....	43

A.2.7	https.disconnect .....	43
A.2.8	login.connect.....	43
A.2.9	login.disconnect .....	43
A.2.10	rbg.entropy.failure .....	44
A.2.11	settings.advanced.set.....	44
A.2.12	syslog.net.connect.....	44
A.2.13	syslog.net.disconnect .....	45
A.2.14	syslog.net.link .....	45
A.2.15	syslog.reload .....	46
A.2.16	system.update.end.....	46
A.2.17	system.update.start.....	46
A.2.18	time.parameters.....	47
A.2.19	vm.change.....	48
A.2.20	vm.hypercall.access .....	48
A.2.21	vm.net.add.....	49
A.2.22	vm.net.edit .....	49
A.2.23	vm.net.remove .....	49
A.2.24	vm.storage.add .....	50
A.2.25	vm.storage.edit.....	50
A.2.26	vm.storage.remove.....	50
A.2.27	vm.usb.connect .....	51
A.2.28	vm.usb.disconnect.....	51
A.2.29	x509.cacert.add .....	51
A.2.30	x509.cacert.remove .....	52
A.2.31	x509.srvcert.generate .....	52
A.2.32	x509.srvcert.install.....	52
<b>A.3</b>	<b>Audit Record Examples .....</b>	<b>53</b>
A.3.1	Example Record Formatting .....	53
A.3.2	Security-Relevant Audit Records .....	53

# LIST OF TABLES

Table 1: Supporting Environmental Components.....18

Table 2: Advanced Options .....23

Table 3: VIM APIs for Certificate Management .....33

Table 4: Security-Relevant Management Functions .....36

Table 5: Sample Audit Records for Management Functions .....59

Table 6: Sample Audit Records for Other Security-Relevant Events.....65

# LIST OF FIGURES

Figure 1: The TOE Evaluated Configuration.....12



# 1 INTRODUCTION

## 1.1 Purpose

This document describes the operational guidance and preparative procedures for VMware ESXi™ 7.0 Update 3d. This document defines the necessary steps to configure the Target of Evaluation (TOE) for use and provides guidance for the ongoing secure usage of the TOE.

## 1.2 Document Reference

This document serves as a supplement to the standard VMware documentation set, and as such references (either implicitly or explicitly) the documents in this section. Note that both HTML and PDF versions of the documents are provided when applicable. The PDF documentation is the version of the documentation that was live as of the release of the product; the HTML versions are ‘living’ documents and as such may deviate from the PDFs.

- [VMware vSphere Documentation portal](#)
- [VMware ESXi Installation and Setup \(ESXi 7.0 Update 3 PDF\)](#)
- [VMware ESXi Upgrade \(ESXi 7.0 Update 3 PDF\)](#)
- [VMware vSphere Security \(ESXi 7.0 Update 3 PDF\)](#)
- [vSphere Single Host Management – VMware Host Client \(ESXi 7.0 Update 3 PDF\)](#)
- [vSphere Virtual Machine Administration \(ESXi 7.0 Update 3 PDF\)](#)

This document also references the following API and CLI command set documentation:

- [vSphere Management SDK, version 7.0](#)
- [vSphere 7.0U3 Web Services API Reference](#) (describes the VIM API)
- ESXCLI:
  - [Getting Started \(ESXi 7.0 PDF\)](#)
  - [Concepts and Examples \(ESXi 7.0 Update 3 PDF\)](#)

The following whitepapers describe the ESXi architecture:

- [Security of the VMware vSphere Hypervisor](#) (January 2014)
- [Timekeeping in VMware Virtual Machines](#) (November 2011)

This document also references various articles in the VMware Knowledge Base, located at <https://kb.vmware.com/s/>. Knowledge Base articles have the format “KB <number>.”

## 1.3 Features and Functions Not Included in the TOE Evaluation

In general, the evaluated functionality is limited to those security functions described in section 4 of this document. If a product function is not listed here, it is either non-interfering with respect to security or it is specifically excluded from the evaluated configuration of the TOE. Non-interfering functions may be used freely as their use has no impact on whether or not the claimed security functionality is implemented. Excluded functionality may adversely affect the claimed security functionality if used. Note that many of the excluded functions are disabled by default;

in these cases, no administrative action is needed other than to avoid deliberately enabling them. The excluded functions are as follows:

- AMD CPUs or Intel CPUs other than the Intel Xeon Gold 6230R. Support for other CPUs is implemented by ESXi but this evaluation covers only the Intel Xeon Gold 63230R.
- Physical optical drives and physical or virtual floppy devices. These have not been included in the evaluated hardware configuration.
- VIM Roles and Permissions. For the purposes of this evaluation, all VIM users are “Administrator” with full VIM permissions, and no lower-privileged roles are evaluated. This is to reduce the scope of evaluation in a way that reflects typical usage by vCenter Server, which always operates with full permissions.
- Active Directory integration for user account management. Active Directory integration must be left unconfigured in a NIAP-validated environment. This exclusion reflects usage of non-FIPS-validated cryptography. The NIAP-validated configuration uses only a local database of user accounts.
- RDM passthrough of storage LUNs. The isolation of raw device mappings is not covered by the evaluation as RDMs are not present in the TOE configuration.
- SCSI passthrough. SCSI devices available for passthrough are not present in the TOE configuration and are therefore not covered by the evaluation.
- PCI passthrough (DirectPath I/O). Testing PCI passthrough configurations is not covered by the evaluation as no devices suitable for PCI passthrough are present in the TOE configuration.
- vGPU passthrough of graphics cards. The passthrough mechanism used for vGPU does not provide isolation between virtual machines.
- Virtual Shared Disks (Multiwriter disks). Shared virtual disks are not covered by the evaluation and require explicit Administrator action to enable.
- vCenter Server. vCenter Server manages an ESXi host programmatically, using the VIM API evaluated here. This is outside the evaluated configuration because there are no security claims specifically related to its use. It is therefore non-interfering with respect to the product security.
- vSAN and NSX. vSAN is included but not enabled in the TOE due to being distributed as a separate license. NSX is installed as a separate product and is not included in the TOE. Usage of either product is not covered by this evaluation.
- vMotion (including SvMotion and XvMotion). This function was not evaluated by NIAP and is disallowed in a NIAP-validated environment by closing firewall ports. The vMotion wire protocol itself is not a trusted path and needs external mechanisms, possibly including physical network isolation, to establish a trusted path.
- IPSec. IPSec is not included in the TOE and is not evaluated for NIAP. IPSec is disabled by default and requires explicit configuration to enable, which should not be performed in a NIAP-validated environment. This exclusion reflects infrequent usage of IPSec in practice.
- CIM (Common Information Model) and SNMP (Simple Network Management Protocol). CIM and SNMP are not included in the TOE and are not evaluated for NIAP. These services are disabled by default and require explicit configuration to enable, which should not be performed in a NIAP-validated environment. This exclusion reflects limitations of

the software packages used to implement CIM. The SLP service is enabled by default; SLP is read-only and not sensitive, and Section 2.4.5 covers disabling SLP.

- SSH. The ESXi SSH interface is not evaluated for NIAP and should not be used. It is disabled by default. Administrative actions should be performed using remote esxcli, Host Client, or VIM.
- DCUI. The ESXi DCUI (Direct Console User Interface) is not evaluated for NIAP and should only be used for initial system setup prior to putting the system into its evaluated configuration.

## 2 INSTALLATION GUIDELINES AND PREPARATIVE PROCEDURES

### 2.1 Assumptions

The following assumptions are made with regards to the setup, installation, and ongoing operation.

- The platform has not been compromised prior to installation of ESXi.
- The ESXi system is provided with appropriate physical security.
- The IT environment specified in the Security Target (ST) is assumed to be properly implemented by a trained and competent administrator.
  - The administrator uses only designated interfaces to manage ESXi.
  - The administrator regularly installs software updates per VMware guidance.
  - The administrator follows guidance in Section 2 to properly configure ESXi security policies during to deployment.
  - The administrator follows guidance throughout this document to properly maintain ESXi security policies during normal operation.
- The administrator deploys workloads (virtual machines) appropriate to the risks of covert channels inherent in shared resources. For example, two virtual machines deployed to a single datastore carry a covert channel risk that information can be exchanged through high/low bandwidth usage on the datastore.
- The IT environment prevents willfully negligent or hostile actions from an administrator.

### 2.2 Evaluated Configuration

The evaluated configuration consists of a single instance of VMware ESXi and associated environmental components.

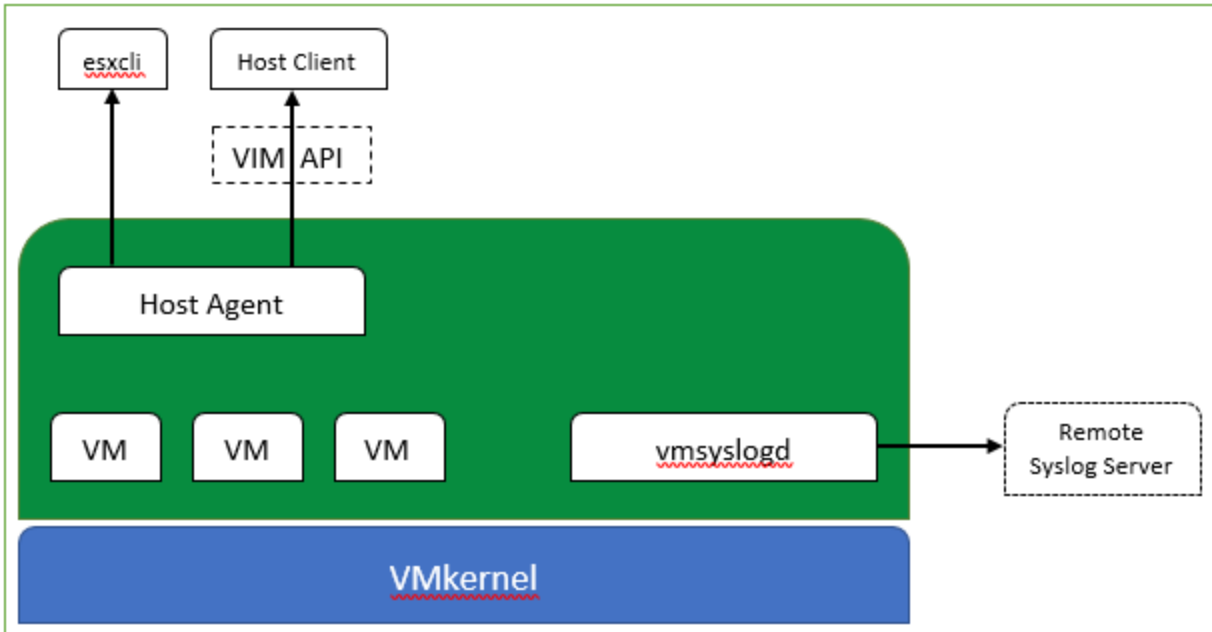


Figure 1: The TOE Evaluated Configuration

The evaluated configuration allows and authenticates incoming connections through the following interfaces:

- **VIM API:** Remote procedure call using SOAP (XML) over HTTPS. Authentication occurs using specific SOAP RPCs, for example `SessionManager.Login`, including HTTP cookies set by that interface.
- **Host Client:** Web interface for ESXi, built on the VIM API. Authentication occurs using the VIM API.
- **ESXCLI:** Remote `esxcli` interface for ESXi. Commands and parameters are encoded into an HTTP request over HTTPS. Authentication occurs using encoded parameters representing username and password.

The evaluated configuration establishes outgoing connections only for remote syslog servers using [RFC 3164](#)- and [RFC 5425](#)-compliant syslog connections.

## 2.3 TOE Components

The TOE consists of the ESXi hypervisor. For the TOE, the hypervisor is installed on top of a physical system (Dell PowerEdge R740) composed of CPUs (Intel Xeon Gold 6230R “Cascade Lake”), local storage and network adapters, and a keyboard and monitor.

The ESXi hypervisor is made up of a kernel (“VMkernel”), which runs virtual machines (“VM”), and a management agent (“Host Agent”). The Host Agent implements the VIM API and ESXCLI (both using HTTPS) over the network. The hypervisor can communicate with a remote syslog server over the network.

The hypervisor includes the Host Client, a web-based user interface implemented as an HTML5-based single-page application (JavaScript running in a web browser). The Host Client is implemented using calls to the VIM API.

## 2.4 Installing the TOE

The [VMware ESXi Installation and Setup](#) document provides general installation instructions.

### 2.4.1 Configure Firmware

Before installing the ESXi software, configure the system's firmware to support a secure hypervisor. On the TOE system (a Dell PowerEdge R740), press F2 during boot to enter System Setup. The following settings must be configured:

1. Ensure Boot Mode is set to UEFI (instead of Compatibility Mode BIOS). The firmware will require this be set for Secure Boot. Many systems default to this setting and might require a reboot after the setting is changed.
2. Enable Secure Boot. (System Security / SECURE BOOT, leave Secure Boot Policy as Standard.)
3. Confirm the following settings, which are generally enabled by default:
  - a. VT enabled (Hardware Virtualization)
  - b. VT-d enabled (IOMMU)
4. Boot Order. During installation, the system must boot from the virtual optical drive with installation media. After installation, this can be changed to boot from the physical disk.

*NOTE: Secure boot is itself not validated by the NIAP process due to usage of non-FIPS-validated cryptography during boot. Instead, using Secure Boot forces additional security checks when installing software updates (for example, unconditionally validating code signatures) that are necessary to satisfy NIAP requirements.*

### 2.4.2 Obtain Software

The software selected for the NIAP-evaluated configuration is ESXi 7.0 Update 3d. ESXi is VMware's vSphere Hypervisor, which is part of the VMware vSphere product family. This information is needed to identify the required software for purchase or evaluation. Note that Update 3d may have been superseded by a newer version of ESXi 7.0, which according to software update policy is also acceptable.

ESXi 7.0 Update 3d may be applied as a new installation or as an update to an existing ESXi 7.0 installation. The software for installation or update may be obtained either from an OEM or through VMware's [Customer Connect](#) portal. Using the portal requires an account. If an account does not yet exist, create one using the portal. Once an account is obtained, log into the portal to obtain the needed software.

Using the portal, if the software is to be applied as a new installation:

1. Select the portal's **Products and Accounts** entry from the top bar and click on **All Products**. This will display the **All Downloads** page.

2. Select the **Products A-Z** entry if it isn't already selected. (The **By Category** entry may have been selected by default.) This will show the **Products** list.
3. In the **Products** list find the **VMware vSphere** entry and click on the **Download Product** link for that entry. That will provide a list of downloads for the **VMware vSphere** product family.
4. In the list of downloads, find the entry for **VMware vSphere Hypervisor (ESXi) 7.0UN $p$** , where  $N$  is the update number and  $p$  is the letter for the patch release. Choose either **7.0U3d** (for Update 3d) or a more recent release and click on the entry's **GO TO DOWNLOADS** link. This will show the **Download Product** page.
5. On the **Download Product** page select the **VMware vSphere Hypervisor (ESXi ISO) image** entry and click on the entry's **Download Now** link.
6. An **End User License Agreement** page will be displayed. After reading the agreement, check the **I agree to the terms and conditions** checkbox and press **Accept**. The selected software will then be downloaded.

If the software is to be applied as an update to an existing installation, see either [KB 1021623](#), or through the portal:

1. Go to the [Customer Connect Product Patches](#) page.
2. From the **Select a Product** pulldown, select the **ESXi (Embedded and installable)** entry. (Do not select the **ESX** entry!)
3. In the version pulldown select **7.0** if it isn't selected already.
4. Press **SEARCH**. That will provide a list of patches associated with ESXi.
5. In the patch list find the entry **VMware-ESXi-7.0UN $p$ -XXXXXXXX-depot**, where  $N$  is the update number,  $p$  is the patch letter, and **XXXXXXXX** is the build number associated with the patch. As with a new installation, choose either **7.0U3d** or a more recent release. (The build number can be ignored since it is fixed for a specific patch release.)
6. Click on the selected entry's **DOWNLOAD NOW** link. The selected software will then be downloaded.

In addition to these two methods of obtaining the needed software, an evaluation copy may also be obtained through the portal:

1. Go to the [Customer Connect ESXi 7 Evaluation Center](#) page.
2. Find the **VMware vSphere Hypervisor (ESXi ISO) image** entry (which will be at least 7.0U3d) and click on the entry's **Manually Download** link. The selected software will then be downloaded.

Note that the Evaluation Center page for ESXi 7 provides an expiring evaluation license that can be used when evaluating the product. A permanent license can subsequently be purchased through an OEM or the portal.

### 2.4.3 Install or Update Software

As a new installation, the downloaded software can be installed in a variety of ways:

- Virtual media: The evaluated hardware configuration has an iDRAC interface (on a separate IP address), which can be used as a “remote console” to manage the host. The iDRAC can be configured to present the ESXi 7.0 ISO through firmware.
- USB: Described in *VMware ESXi Installation and Setup* documentation, not covered here.
- PXE: Described in *VMware ESXi Installation and Setup* documentation, not covered here.

*NOTE: PXE booting requires transferring sensitive system state using FTP or HTTP during boot and is not recommended for a secure installation, unless external measures are taken to ensure the security of the network used for PXE booting. Such measures are beyond the scope of this document.*

If updating an existing ESXi 7.0 installation, follow guidance in Section 4.6.1. To summarize:

1. Be running some version of ESXi 7.0.
2. Put the host in maintenance mode.
3. Use `esxcli software vib install` or `esxcli software vib update` to install the downloaded patch. The install command will forcibly install all contents of the specified patch; the update command will install only newer content.
4. Exit maintenance mode and reboot the system.
5. Confirm installation of the patch by verifying the build number. See Section 2.4.4.

*Note: patches of the core ESXi software always require a reboot.*

#### 2.4.4 Verify Software

To verify the installed ESXi software version, perform the following as an administrator:

- Log into the Host Client.
- From the top menu bar select Help→About.
- In the displayed About box note the ESXi version and build number.

For more information about determining the installed software version, see the VMware knowledge base article [KB 1022196](#).

#### 2.4.5 Additional ESXi Configuration

ESXi requires a few non-default parameters to be set for a NIAP configuration. Though ESXi attempts to be secure by default, some of these options come at a performance cost or disable common features and thus are not enabled by default.

**To enable eager memory zeroing (to minimize lifetime of cryptographic keys in memory; see Section 4.2.3):**

```
esxcli system settings advanced set -o "/Mem/MemEagerZero" --int-value "1"
```

**To disable features and associated services, close ports using firewall configuration:**

```
esxcli network firewall ruleset set -e false -r "CIMSLP"
```



```
esxcli network firewall ruleset set -e false -r "DVSSync"  
esxcli network firewall ruleset set -e false -r "faultTolerance"  
esxcli network firewall ruleset set -e false -r "iofiltervp"  
esxcli network firewall ruleset set -e false -r "vMotion"
```

*Note: this configuration will disable Distributed Virtual Switches, Fault Tolerance, SLP, vMotion, and Virtual Machine Encryption. Customers should evaluate their security exposure and functionality needs when choosing to disable features. See Section 1.3 for further information about why specific features are disabled.*

### **To configure the allowed TLS ciphers:**

Configuring the allowed cipher list requires enabling ssh on ESXi, logging into ESXi via ssh to modify the configuration file that provides the desired ciphers, restarting the reverse proxy daemon (rhttpproxy), and then disabling ssh.

*Note: SSH is only enabled temporarily to perform the needed configuration during system setup. After configuration is complete, SSH must be disabled.*

To enable ssh:

- Log into Host Client.
- Select Manage from the Navigator.
- Select the Services tab.
- Select the TSM-SSH service and press Start in the action bar. SSH logins will now be permitted.

To update the cipher list:

- Log into ESXi using ssh.
- Edit the file /etc/vmware/rhttpproxy/config.xml (using vi or any available text editor).
- Find the <cipherList></cipherList> entry or create it if it does not exist. It will be listed as:

```
<config>  
  <vmacore>  
    <ssl>  
      <cipherList></cipherList>  
    </ssl>  
  </vmacore>  
</config>
```

*Note: There is also another <ssl> tag in this file that is not under vmacore. Make sure to edit the one under <vmacore>.*

- Set the value to <cipherList>!aNULL:!ECDHE-RSA-AES256-SHA:!AES256-SHA:kECDH+AESGCM:ECDH+AESGCM:RSA+AESGCM:kECDH+AES:ECDH+AES:RSA+AES</cipherList>
- Save the file.

To restart the rhttpproxy daemon, from the ssh login execute:

```
# /etc/init.d/rhttpproxy restart
```

Once these steps are complete, log out of the ssh session and log into Host Client to disable the TSM-SSH service:

- From the Host Client login select **Manage** from the Navigator.
- Select the **Services** tab.
- Select the TSM-SSH service and press **Stop**. SSH logins will no longer be permitted.

#### 2.4.6 Additional Device Configuration

Several ESXi features are not evaluated within the TOE due to lack of available devices. The NIAP evaluation expects these features to be disabled, and not merely unused. To configure an ESXi system to ensure these features are unavailable:

- **PCI Passthrough:** Ensure all PCI devices are associated with the host only. No devices should be available for association with a virtual machine. This can be verified using Host Client by going to the **Hardware** tab under **Manage** in the **Navigator**. Scroll through the available devices and ensure none have **Enabled** in the **Passthrough** column. If any do, select the device and press **Toggle passthrough** to disable passthrough. That no devices are in fact available to any VM for passthrough can further be verified in Host Client by editing the settings of a powered off VM, selecting **Add other device**, and noting that the **PCI device** and **Dynamic PCI device** menu entries are not selectable.
- **vGPU:** Ensure nVidia GRID PCI devices are not installed in the TOE.
- **RDM passthrough of storage LUNs:** Ensure all local disks are formatted with VMFS volumes and mounted as datastores. No unmounted storage volumes should be available to the host. This can be verified using Host Client by going to **Storage** in the **Navigator**. Select **New Datastore**. In the **Select creation type** window select **Create new VMFS datastore**. In the **Select device** window, there should be no unclaimed devices listed. If there are, select each available device and continue to create a datastore on the device. That no RDM passthrough storage volumes are in fact available to any VM can further be verified in Host Client by editing the settings of a powered off VM, selecting **Add hard disk**, and noting that the **New raw disk** menu entry is not selectable.

## 2.5 Configuring the TOE Environmental Components

This section describes the steps involved when configuring the TOE environmental components.

The ESXi hypervisor is designed for self-contained operation. Few external components are needed. They are listed in Table 1 below, with guidance for their configuration and use included in the following sections.

Components	Description
Linux system for management	System from which to make VIM API calls or ESXCLI calls to configure and manage ESXi.

	<p><i>Any Linux distribution released after around 2014 should be sufficient. RHEL7 and Ubuntu 16.04 have been specifically tested.</i></p> <p><i>NOTE: In many deployments, vCenter Server is used to make VIM API calls.</i></p>
<b>Remote Syslog Server</b>	<p>A server which implements <a href="#">RFC 3164</a> “The BSD Syslog Protocol” and <a href="#">RFC 5425</a> “TLS Transport Mapping for Syslog.”</p> <p><i>NOTE: A remote syslog server is optional. However, usage of a remote syslog server is included in the NIAP-validated configuration.</i></p>

Table 1: Supporting Environmental Components

### 2.5.1 Install ESXCLI for Remote Management

The ESXCLI command set is available as a standalone ESXCLI download, available from:

<https://developer.vmware.com/web/tool/7.0/esxcli>

This guide covers using the ESXCLI standalone download. To install, download the provided script (for example `esxcli-7,0.0-15866526-lin64.sh` for Linux) onto a system separate from ESXi that will be used for remote administration. Then run the provided script as root. For example:

```
su # Install as root for all users
chmod +x ./esxcli-7.0.0-15866526-lin64.sh
./esxcli-7.0.0-15866526-lin64.sh
# During installation, accept the EULA to continue.
esxcli --version # Confirm successful installation
```

### 2.5.2 Configure Auditing

The following instructions assume ESXCLI is installed on a Linux system suitable for remote management of ESXi. To enable local auditing, execute the following command:

```
esxcli --server <host> system auditrecords local enable
```

To enable remote auditing, execute the following commands (using appropriate values for a CA and host name for the syslog server):

```
esxcli --server system security certificatestore add -f
cacert.pem
esxcli network firewall ruleset set --ruleset-id=syslog --
enabled=true
esxcli network firewall refresh
esxcli --server <host> system syslog \
  config set --loghost="ssl://syslog.example.com:1514"
esxcli --server <host> system syslog config set --crl-
check="true"
esxcli --server <host> system syslog config set --x509-
strict="true"
esxcli --server <host> system syslog reload
esxcli --server <host> system auditrecords remote enable
```

See Section 4.1 for further details.

CA roots can also be configured using ESXCLI commands:

```
esxcli system security certificatestore add --file=<local-file>
esxcli system security certificatestore list
esxcli system security certificatestore remove --issuer=<issuer>
--serial=<serial>
```

For more information about the esxcli system commands, see the [vSphere Command-Line Interface Reference](#).

## 2.6 Operating Modes

The ESXi hypervisor functions in several operating modes.

- **Installation.** During installation, security properties have not yet been configured and ESXi may be unable to offer management functionality until fully configured. For example, TLS keys may not yet be provisioned, and thus remote access may be inaccessible. Once installation completes, ESXi is fully usable.
- **Maintenance Mode.** ESXi can enter maintenance mode using the VIM API or the ESXi Host Client. Entering maintenance mode requires that no virtual machines currently be running. While in maintenance mode, virtual machines may not be powered on and attempting to power on a virtual machine will return an error. The intent of this mode is to assist administrators in disallowing conflicting operations while conducting maintenance activities, including applying system updates. While in maintenance mode, ESXi maintains all security properties (no security properties are weakened while in maintenance mode).
- **Normal operation.** All security and management functions are available as described in this document.

## 2.7 Obtaining Support

In the event of software failure, customers should engage with VMware Global Support Services to make use of any purchased support contract(s). See the [Support Contact Options](#) for more information.

VMware also offers self-service documentation and knowledge base articles at the [vSphere Support Center](#).

In the event of hardware failure, customers should communicate with the vendor who supplied the hardware platform for support options.

## 2.8 Ongoing Tracking for Security Issues and Mitigations

ESXi 7.0 Update 3d is part of an ongoing lifecycle, where security issues are found, resolved, or mitigated. Consult [VMware Security Advisories](#) (VMSAs) for information about VMware product security fixes, including those for ESXi. As of the publication of this document no applicable VMSAs were found that apply to the evaluated configuration of the product; a VMSA exists for ESXi PCI passthrough functionality but this is not relevant to the evaluated configuration of the product, which does not include any PCI passthrough devices in its operational environment.

## 3 OPERATIONAL GUIDANCE: ADVANCED SETTINGS

Advanced settings are specific key/value configuration settings that can be set to manipulate various settings. For more information about configuring advanced options, refer to [KB 1038578](#).

### 3.1 Configuring Advanced Options Using the Host Client

The ESXi Host Client (UI) contains a tab which allows directly editing advanced settings. This is also the best approach for discovering which settings exist and what their behaviors are. For more information about using the Host Client to configure advanced settings, see [Manage Advanced Settings in the VMware Host Client](#).

### 3.2 Configuring Advanced Settings Using the VIM API

Changing advanced settings on individual hosts using the Host Client can be impractical at scale. The VIM API offers a programmatic interface to manipulate advanced settings. The Host Client is built on top of this VIM API interface.

Advanced settings are controlled using the `OptionManager` managed object. This managed object can be accessed from the `HostSystem` managed object's `ConfigManager` field, as `HostSystem.configManager.advancedOption`.

For more information about using this managed object, see the following topics:

- [Managed Object - HostSystem\(vim.HostSystem\)](#)
- [Data Object - HostConfigManager\(vim.host.ConfigManager\)](#)
- [Managed Object - OptionManager\(vim.option.OptionManager\)](#)

#### 3.2.1 Querying Advanced Settings

The full list of advanced settings is available using the `OptionManager.supportedOption[]` field. The contents of this array are fixed for a particular ESXi build and do not change at runtime.

The list of currently set advanced settings (for example, those set to non-default values) is available using the `OptionManager.setting[]` field. The `OptionManager.UpdateOptions` method can be used to search for setting keys matching a particular string, as the full list of advanced settings might be too unwieldy for interactive use.

#### 3.2.2 Setting Advanced Settings

To set an advanced setting, invoke the `OptionManager.UpdateOptions` method with the desired key and value. The following pseudocode sets the advanced setting `Config.Etc.issue` to "Hello World\n":

```
MoRef optionMgr = hostSystem.configManager.advancedOption;  
settings = new OptionValue[]
```

```

settings[0].key = "Annotations.WelcomeMessage"
settings[0].value = "Hello World\n"
optionMgr.UpdateOptions(changedValue=settings)

```

### 3.3 Selected Advanced Settings

It is not possible to provide a full list of advanced settings since settings can be added or removed in any release. The best reference for the advanced settings a release supports is through the Host Client or VIM API exposed by that release, which includes a description of the provided advanced settings.

The following table describes advanced options which have a particular security effect.

Setting name	Default	Description
<b>Annotations.WelcomeMessage</b>	(empty)	Displayed in Host Client (UI) prior to login.
<b>Config.HostAgent.vma core.soap.sessionTime out</b>	30 (minutes)	Idle time in minutes before a VIM API session is automatically logged out. A value of zero disables the timeout. Applies to new sessions only.
<b>Mem.MemEagerZero</b>	0 (disabled)	Enable zeroing userworld and guest memory pages (including VMM) after VM exit.
<b>Security.AccountLock Failures</b>	5	Maximum number of failed login attempts before a user's account is locked. A value of zero disables account locking.
<b>Security.AccountUnlo ckTime</b>	900 (15 minutes)	Number of seconds that a user is locked out.
<b>Security.PasswordHis tory</b>	0	Number of passwords to remember for each user. This prevents duplicate or similar passwords.
<b>Security.PasswordMax Days</b>	99999	Maximum number of days between password changes.
<b>Security.PasswordQua lityControl</b>	retry=3 min=disabled,disabled,disabl ed,7,7	Password quality configuration.
<b>UserVars.HostClients essionTimeout</b>	900 (15 minutes)	Idle time in seconds before Host Client is automatically logged out. A value of zero disables the timeout.

<b>UserVars.HostClientWelcomeMessage</b>	(empty)	Displayed in Host Client following login, as a “hint”.
--	---------	--

Table 2: Advanced Options



## 4 OPERATIONAL PROCEDURES FOR ADMINISTRATORS

This section describes additional steps, clarifications, and exclusions that might not be documented in the public documentation for this product. The assumption is that the TOE and its environment have already been successfully set up and working before these next steps are performed.

### 4.1 Audit Configuration (FAU)

ESXi offers both local and remote audit recordkeeping. This is disabled by default and must be manually enabled for both local and remote modes.

The local audit log operates as a fixed-size buffer of recent audit messages. Once filled, new records overwrite the oldest records.

Remote audit servers (that is, remote syslog servers) receive audit records in a standard syslog format ([RFC 3164](#) “The BSD syslog protocol”), either unencrypted or encrypted ([RFC 5425](#) “TLS Transport Mapping for Syslog”). Audit message structured data complies with [RFC 5424](#) “The Syslog Protocol”, but general syslog messages only comply with [RFC 3164](#).

A generated audit message is sent simultaneously to the local store and remote audit servers. If the connection to a remote audit server is lost, any generated audit messages will be dropped from the perspective of the remote server. Upon reconnection, an audit message is generated indicating potential message loss.

#### 4.1.1 Configuring Local Audit Records

Configuration of local auditing is through either Host Client, or ESXCLI in the `esxcli system auditrecords local` namespace. To enable local auditing using Host Client, set the `Syslog.global.auditRecord.storageEnable` advanced setting to True. To enable local auditing using ESXCLI, execute the following command:

```
esxcli system auditrecords local enable.
```

For more information about using the Host Client to configure advanced options, see [Manage Advanced Settings in the VMware Host Client](#). For more information on configuring local audit using ESXCLI, see [Configuring and Managing the Audit System and Audit Data in ESXCLI 7.0 U3 Concepts and Examples](#).

#### 4.1.2 Configuring Remote Audit Server

Configuring ESXi to communicate with a remote audit server (that is, a syslog server) is either through Host Client, or ESXCLI using the `esxcli system syslog` and `esxcli system auditrecords remote` namespaces. During configuration, multiple syslog servers can be specified, separated by commas. The firewall must have been configured during system setup to permit outbound syslog access. Configuration of a remote syslog server for audit logging does not prevent logs from being generated and stored locally.

Communication with syslog servers is either encrypted (using TLS, required by the NIAP configuration) or unencrypted (using TCP). For TLS connections, a CA root suitable for each syslog server must be loaded into the ESXi certificate store. For more information, see Section 4.4.3.

When using TLS, the preferred port is 1514, and the syslog server configuration entry must be prefixed with “`ssl://`”. Otherwise the port should be 514 with a prefix of “`tcp://`”.

Audit events are transmitted in a format similar to RFC 3164 and RFC 5424. Audit records have the RFC-specified prefix range of <104> to <111>, which is a packed value reflecting audit facility 13 (for “audit”) at severities from 0 (“emerg”) to 7 (“debug”). Audit records are transmitted to a configured syslog server in real-time; in the event of a communications outage, no buffer is used to maintain remote availability of the records. Local audit logs can be used to monitor system activity during any outage.

For more information, see [Configure Syslog on ESXi Hosts](#) for configuring remote syslog servers using Host Client. Also see [Enable the Transmission of Audit Records to a Remote Host with ESXCLI](#).

The following example ESXCLI command enables remote audit logging:

```
esxcli system auditrecords remote enable
```

The following example ESXCLI command sequence sets the syslog server to `syslog.example.com`:

```
esxcli system syslog \  
  config set --loghost="ssl://syslog.example.com:port"  
esxcli system syslog reload
```

The following example ESXCLI command sequence clears the syslog server configuration:

```
esxcli system syslog config set --reset=loghost  
esxcli system syslog reload
```

The following ESXCLI example command sequence enables X.509 and CRL checking.

```
esxcli system syslog config set --crl-check="true"  
esxcli system syslog config set --x509-strict="true"  
esxcli system syslog reload
```

The ESXCLI `--crl-check` option (or the equivalent `Syslog.global.certificate.checkCRL` advanced option in Host Client) enables verification of X.509 CRLs, which are not checked by default in compliance with industry convention. The NIAP verified configuration, however, requires CRL checks. Due to implementation limitations, if CRL checks are enabled then **all** certificates in a certificate chain must provide a CRL link.

The ESXCLI `--x509-strict` option (or the equivalent `Syslog.global.certificate.strictX509Compliance` advanced option in Host Client) performs additional validity checks on CA root certificates during verification. These checks are generally not performed (CA roots are inherently trusted) and might cause incompatibilities with existing, misconfigured CA roots. The NIAP requirements, however, require even CA roots to pass validations.

VMware does not recommend enabling the “crl-check” or “x509-strict” options for non-certification-related installations because of the difficulty in properly configuring an environment that uses CRL checks.

### 4.1.3 Viewing Audit Records

Audit records can be viewed remotely using a remote audit server (see Section 4.1.2). The local audit may also be viewed remotely through the VIM API using a script provided as [sample code available from developer.vmware.com](#).

## 4.2 Cryptographic Configuration (FCS)

### 4.2.1 Cryptographic Key Generation

The Transport Layer Security (TLS) key is used to secure communication with the host using the TLS protocol. The TLS key is generated at first system boot as a 2048-bit RSA key. ESXi does not currently implement automatic generation of ECDSA keys for TLS. The TLS private key is not intended to be serviced by the administrator.

The default TLS certificate is self-signed, with a `subjectAltName` field matching the host name at installation. The administrator might want to install a different certificate, for example to make use of a different `subjectAltName` or to include a particular Certificate Authority (CA) in the verification chain.

The Host Client offers an interface for changing the TLS certificate. For more information, see [Import a New Certificate for an ESXi Host in the VMware Host Client](#).

The VIM API `HostCertificateManager` (`vim.host.CertificateManager`) managed object offers methods to manage the certificate. A typical workflow would call `GenerateCertificateSigningRequest` to fetch a Certificate Signing Request (CSR), use an external mechanism (beyond the scope of this document) to create a signed certificate, then would call `InstallServerCertificate` to install the signed certificate. For more information, see [Managed Object – HostCertificateManager\(vim.host.CertificateManager\)](#).

Ephemeral keys generated for TLS sessions are generated using algorithms and key sizes that depend on the negotiated TLS cipher suite; there is no mechanism by which the administrator controls the behavior of this function.

### 4.2.2 Cryptographic Key Establishment

Configuration of TLS cryptographic key establishment is governed by choice of TLS cipher suites, which select one of the RSA-based key transports (as specified in SP 800-56B) or ECC-based key agreements using ephemeral Elliptic Curve Diffie Hellman (ECDH) (as specified in SP 800-56A). The supported TLS cipher suites are configured as part of initial setup as described in section 2.4.5. The administrator has no direct control over the behavior of this function.

### 4.2.3 Cryptographic Key Destruction

In Host Client, the advanced setting `Mem.MemEagerZero (/Mem/MemEagerZero` in ESXCLI) can be used to enable zeroing out userworld and guest memory pages (including the VMM) when userworlds and guests exit. See Section 3 for further discussion of advanced settings. To enable the setting in Host Client, set the value to “1”. To enable the setting in ESXCLI, execute the command:

```
esxcli system settings advanced set -o "/Mem/MemEagerZero"
--int-value "1"
```

For more information, see [Configuring the Cryptographic Functionality](#) in [ESXCLI 7.0 U3 Concepts and Examples](#).

### 4.2.4 Cryptographic Operation

ESXi defaults to using FIPS-validated cryptography for all operations needing cryptography for security purposes. This includes remote access to management interfaces (for example, TLS), key generation, signature verification, and other use cases. Any parameters that would disable FIPS checking must not be changed.

There are no other configurable parameters relating to cryptographic operation. The NIAP certified functionality is enabled by default.

### 4.2.5 Random Bit Generation

There are no configurable parameters relating to random bit generation. The NIAP certified functionality is enabled by default.

### 4.2.6 Entropy for Virtual Machines

There are no configurable parameters relating to entropy for virtual machines. The NIAP certified functionality is enabled by default.

### 4.2.7 HTTPS

There are no configurable parameters relating to usage of HTTPS. The NIAP certified functionality is enabled by default.

### 4.2.8 TLS Protocol

ESXi uses a shared configuration for TLS Client and TLS Server protocols, though some TLS clients (including remote syslog) are not configurable. The default configuration is compliant with the TLS requirements in the TLS Functional Package as specified in the Security Target (ST). These settings are not generally expected to be serviced by an administrator, though in

practice public reports of TLS security vulnerabilities and company best-practices have necessitated manual configuration. VMware supports altering these settings only as directed by Global Support Services (GSS).

#### 4.2.8.1 *TLS Protocol Versions*

By default, ESXi allows TLS v1.2 only. ESXi supports configuration to enable TLS v1.1, TLS v1.0, and SSL v3 to support legacy clients and installations; this is not recommended and doing so is explicitly non-compliant with the Security Target. TLS v1.3 is not yet supported by ESXi.

The protocol list is configured using the UserVars.ESXiVPsDisabledProtocols advanced setting in Host Client (called /UserVars/ESXiVPsDisabledProtocols in ESXCLI). The advanced setting specifies the protocols to exclude, and thus by default has a value of “sslv3,tlsv1,tlsv1.1”.

ESXi does not support “holes” in the excluded protocol list.

For information on setting the protocol list using Host Client, see [Configure Advanced TLS/SSL Key Options](#) in [vSphere Single Host Management – VMware Host Client](#).

For information on setting the protocol list using ESXCLI, see [Configuring the Cryptographic Functionality](#) in [ESXCLI 7.0 U3 Concepts and Examples](#).

#### 4.2.8.2 *TLS Cipher Suites*

The default ESXi cipher suite permits a selection of high security protocols, with first preference to ciphers implementing GCM for better performance, and second preference to ciphers which use ephemeral key agreement (ECDHE) for Perfect Forward Secrecy.

Static key ciphers (RSA) are maintained for compatibility with the TLS 1.2 standard (which makes RSA+AES mandatory). ESXi does not use ECDSA server certificates, so ECDSA suites are only used as a client configuration.

The setup instructions in section 2.4.5 describe how to configure the TLS cipher suites that are supported by the evaluated configuration of ESXi.

The combination of applying the required cipher suite configuration and the fact that ECDSA server certificates cannot be loaded into ESXi result in the following cipher suites being offered by the TLS client and server:

TLS client:

- TLS\_RSA\_WITH\_AES\_128\_CBC\_SHA
- TLS\_RSA\_WITH\_AES\_128\_CBC\_SHA256
- TLS\_RSA\_WITH\_AES\_256\_CBC\_SHA256
- TLS\_RSA\_WITH\_AES\_128\_GCM\_SHA256
- TLS\_RSA\_WITH\_AES\_256\_GCM\_SHA384
- TLS\_ECDHE\_ECDSA\_WITH\_AES\_128\_CBC\_SHA256

- TLS\_ECDHE\_ECDSA\_WITH\_AES\_256\_CBC\_SHA384
- TLS\_ECDHE\_ECDSA\_WITH\_AES\_128\_GCM\_SHA256
- TLS\_ECDHE\_ECDSA\_WITH\_AES\_256\_GCM\_SHA384
- TLS\_ECDHE\_RSA\_WITH\_AES\_128\_CBC\_SHA256
- TLS\_ECDHE\_RSA\_WITH\_AES\_256\_CBC\_SHA384
- TLS\_ECDHE\_RSA\_WITH\_AES\_128\_GCM\_SHA256
- TLS\_ECDHE\_RSA\_WITH\_AES\_256\_GCM\_SHA384

TLS server:

- TLS\_RSA\_WITH\_AES\_128\_CBC\_SHA
- TLS\_RSA\_WITH\_AES\_128\_CBC\_SHA256
- TLS\_RSA\_WITH\_AES\_256\_CBC\_SHA256
- TLS\_RSA\_WITH\_AES\_128\_GCM\_SHA256
- TLS\_RSA\_WITH\_AES\_256\_GCM\_SHA384
- TLS\_ECDHE\_RSA\_WITH\_AES\_128\_CBC\_SHA256
- TLS\_ECDHE\_RSA\_WITH\_AES\_256\_CBC\_SHA384
- TLS\_ECDHE\_RSA\_WITH\_AES\_128\_GCM\_SHA256
- TLS\_ECDHE\_RSA\_WITH\_AES\_256\_GCM\_SHA384

#### 4.2.8.3 *ECC Choices in TLS*

ESXi provides a selection of strong prime curves, specifically "prime256v1:secp384r1:secp521r1". No interface is provided to change this configuration.

## 4.3 Protection of User (VM) Data (FDP)

### 4.3.1 Virtual Networking

The configuration for virtual machine networking can be configured through Host Client or the VIM API. For Host Client, see [Network Virtual Machine Configuration](#) in [vSphere Single Host Management – VMware Host Client](#).

For the VIM API, the virtual machine managed object's configuration (`vim.VirtualMachine.config`) contains an array of devices (`vim.vm.ConfigInfo.hardware.device[]`). Within that array, some devices are network devices (classes derived from `vim.vm.device.VirtualEthernetCard`); these devices will have a `backing` property that contains the configured virtual network.

For more information on the required backing, see [Data Object – VirtualEthernetCardNetworkBackingInfo\(vim.vm.device.VirtualEthernetCard.NetworkBackingInfo\)](#). For more information on general VM configuration (of which the network configuration is a part), see [Data Object – VirtualMachineConfigSpec\(vim.vm.ConfigSpec\)](#).

Virtual machines can communicate if connected to the same Distributed Virtual Switch (or if the Distributed Virtual Switches are connected, either directly or indirectly). When using Distributed Virtual Switches, the virtual machine can only connect to the host's network address if the host's vmknic is connected to the same Distributed Virtual Switch.

To disable access to a virtual switch, either remove the virtual NIC from the virtual machine, or configure the virtual NIC to be “disconnected” (have no backing object).

### 4.3.2 Physical Platform Resources

Most devices are implemented as virtual devices, including the mouse and keyboard. However, ESXi allows direct access to physical devices in limited scenarios. To remain compliant with the Security Target, the only physical devices a virtual machine is allowed to access are USB devices and network adapters. Raw disks and other devices (such as PCI passthrough devices, vGPU devices, and SCSI passthrough devices) are not to be used.

#### 4.3.2.1 USB

Configuring a virtual machine's USB device access can be done through Host Client or the VIM API. For Host Client, to add a USB device to a virtual machine:

1. Click **Virtual Machines** in the VMware Host Client inventory.
2. Right-click a virtual machine in the list and select **Edit settings** from the pop-up menu.
3. On the **Virtual Hardware** tab, select **Add other device** and select **USB device** from the drop-down menu. Note: this option may be disabled if the virtual machine lacks a **USB controller**, which can be added using the same procedure. This option may also be disabled if the host has no available USB devices to add.
4. Available USB devices appear in the Virtual Hardware devices list. Select the desired one.
5. Press Save.

To delete an existing USB Device using Host Client, edit the virtual machine settings, find the USB Device entry, move the mouse pointer over the right side of the USB Device entry and click the **Remove** icon (X). Then press save.

The virtual machine's ConfigInfo contains an array of device objects (`vim.vm.ConfigInfo.hardware.devices[]`). Some instances in that array can be of type `vim.vm.device.VirtualUSB`; these devices can have a `backing` field, which specifies access to a particular backing device. Note: For connectivity, the virtual machine must also have a compatible virtual USB Controller configured for the virtual machine.

For more information on the required backing, see [Data Object – VirtualUSBUSBBackingInfo\(vim.vm.device.VirtualUSB.USBBackingInfo\)](#). For more information on general VM configuration (of which the USB configuration is a part), see [Data](#)



[Object – VirtualMachineConfigSpec\(vim.vm.ConfigSpec\)](#). For more information about virtual USB objects, see [Data Object – VirtualUSB\(vim.vm.device.VirtualUSB\)](#).

ESXCLI is used to obtain the VID (Vendor ID) and PID (Product ID) of USB devices available for virtual machine access. That information is required when creating the USBBackInfo. The command is:

```
esxcli hardware usb passthrough device list
```

#### 4.3.2.2 *Physical Network*

ESXi does not allow a guest to have direct access to a physical network except through the administrator configuring a virtual switch with a network interface attached to specific physical network interfaces. Any virtual machines expected to have external network access may be configured to have their virtual network interfaces connected to this virtual switch.

More commonly, the administrator can configure a virtual switch to connect to a specific VLAN on the physical network and then connect virtual machines to that virtual switch. This provides logical isolation of the virtual machines from the physical network. For guidance on configuring virtual machine networking using virtual switches, see [Managing Virtual Switches in the VMware Host Client](#) in the [vSphere Single Host Management – VMware Host Client](#) document.

#### 4.3.3 *Memory Zeroization*

There are no configurable parameters related to volatile memory zeroization.

There are no configurable parameters related to non-volatile memory zeroization while ESXi is operational. Note that as part of placing the product into its evaluated configuration, the eager memory setting must be applied as part of the initial setup process. This is described in section 2.4.5 above. Once this is enabled, no additional configuration is needed.

#### 4.3.4 *Hardware-based VM Isolation*

The only supported virtualization mode in ESXi 7.0 uses hardware-based virtualization (VT-x/VT-d/EPT or AMD-V, as the platform's CPU supports), in conjunction with hardware-based two-level page tables (Extended Page Tables).

*Note: the TOE is evaluated only on Intel CPUs with VT-x instructions with EPT. Thus, AMD-V is not included in this evaluation.*

Usage of hardware-based VM isolation mechanisms is always enabled. For more information, see [Binary Translation Deprecation](#).

## 4.4 *Authentication Configuration (FIA)*

Administrator authentication to ESXi uses locally-defined username and password credentials in the evaluated configuration. The administrator account name is 'root' and the password is specified during the initial installation and setup process.

Instructions for authenticating to each administrative interface is specified in section 4.8.1 below.



#### 4.4.1 Authentication Failure Handling

Authentication failure handling is available through several advanced settings. See the following settings in Section 3:

```
Security.AccountLockFailures  
Security.AccountUnlockTime
```

The `AccountLockFailures` option indicates the permitted number of failed login attempts before locking the account. For example, to lock the account on the 5<sup>th</sup> login failure, set this value to 4.

The `AccountUnlockTime` option describes a time interval following the last failed login attempt before a successful login for a given account is allowed. Any login attempt within the lock timeout will restart the lock timeout.

#### 4.4.2 Password Management

Password management is available through several advanced settings.

See the following options in Section 3.3:

```
Security.PasswordQualityControl  
Security.PasswordHistory  
Security.PasswordMaxDays
```

For more information, see [Configure the Passwords and Account Lockout Policy in the VMware Host Client](#).

The password history setting is only enforced for passwords changed through VIM API's `LocalAccountManager.changePassword`. So the administrator is required to use that interface (either directly, or indirectly through Host Client) to change the password in order to enforce password history. For more information, see [Update an ESXi User in the VMware Host Client](#) and [Managed Object – HostLocalAccountManager\(vim.host.LocalAccountManager\)](#).

To compose strong passwords, the `Security.PasswordQualityControl` setting should require a mix of characters from multiple character classes, and a minimum password length that satisfies the deployment's password requirements. In general, composition of strong passwords should require a mixture of at least three of the four character classes. This is the default.

#### 4.4.3 X.509 Certificate Validation and Authentication

ESXi offers methods to manage the certificate authorities trusted by the host. X.509 certificates presented by external services and by updates are verified against these certificate authorities.

In the NIAP-approved configuration, the only secure outbound connection from an ESXi host is for remote syslog using TLS. (All other connections relevant to the NIAP-approved configuration are inbound.) See Section 4.1.2 for information on how to configure CRL checking for remote syslog servers.

ESXi offers the ability to locally store CRLs at the same time as CA roots are configured. This is intended for scenarios where the ESXi host lacks network connectivity to the CA root's normal

CRL distribution mechanism (for example, ESXi operating in an isolated network environment); this is an advanced configuration not evaluated for NIAP, as NIAP requirements presume accessibility of CRLs.

CA roots can be configured using ESXCLI commands under the `esxcli system security certificatestore` command set. For more information, see [Manage CA Certificates with ESXCLI](#) in the [ESXCLI 7.0 U3 Concepts and Examples](#).

The VIM API `HostCertificateManager` (`vim.host.CertificateManager`) managed object offers methods to manage the certificate authorities trusted by the host. X.509 certificates presented by external services and by updates are verified against these certificate authorities.

Method	Purpose
<code>ListCACertificateRevocationLists</code>	Returns currently stored CRLs for CA roots used by this host.
<code>ListCACertificates</code>	Returns currently stored CA roots used by this host.
<code>ReplaceCACertificatesAndCRLs</code>	Installs new CA roots.

Table 3: VIM APIs for Certificate Management

For more information, see [Managed Object – HostCertificateManager\(vim.host.CertificateManager\)](#).

## 4.5 Security Management (FMT)

### 4.5.1 Default Sharing Configurations

Virtual machines default to a configuration that does not contain any mechanisms for sharing data between virtual machines. This is not configurable. (Virtual machines in general do not have a modifiable default configuration.) Administrators reconfiguring a VM (through the `vim.VirtualMachine.Reconfigure` VIM API) should use care to ensure any devices added to the virtual machine are configured correctly for sharing.

Virtual network configuration is discussed further in Section 4.3.1.

### 4.5.2 Isolating VM Networks from the Management Network

VMware’s published best practices for vSphere deployments recommend isolating the management network (generally, vCenter Server and all ESXi hosts) from unnecessary access. This best practice coincides with the “Trustworthy Administrator” assumption in Section 2.1.

Common network isolation mechanisms are:

- **Physical.** Provisions the ESXi host with multiple network devices. Configure ESXi to treat one or several (for redundancy) NICs as the management network and configure a

distinct set of NICs for attachment to virtual machines. The additional hardware and connection requirements make this a more resource-intensive configuration.

- **Logical (VLAN).** Allows ESXi to use the default NIC as a management network but configures virtual switches to operate over VLANs. In this way, virtual machine network traffic will be encapsulated and isolated from the management network. Configuring VLANs is beyond the scope of this document as configuration is also needed on devices external to the TOE.
- **None.** Virtual machines are connected to the same management network as the host. This is the default configuration; other modes require additional configuration.

For a more detailed discussion of configuration of the management network, see [Securing vSphere Networking](#) in the [vSphere Security](#) documentation.

A procedure for configuring virtual networking to place the management network and guest networking on physically isolated networks is:

1. Login to the VMware ESXi Host Client using an administrator account.
2. Click on the Networking entry in the Navigator pane.
3. Click on the “Virtual Switches” tab.
4. Click on “Add standard virtual switch”.
5. Enter a name of the new virtual switch (vSwitch1 in this example).
6. The new virtual switch (vSwitch1) will be assigned an unused physical NIC as the uplink adapter (vmnic1 in this example).
7. Select “Networking” in the left Navigator pane. Select the “Port groups” tab and click on the “Add port group” toolbar button.
8. Enter “Operational Network” for the name and select vSwitch1 for the “Virtual Switch.”
9. For all the virtual machines on this host, configure the VM’s network adapter so it is connected to “Operational Network”.
10. All VM traffic will now be physically separated from management traffic.

#### 4.5.3 Management APIs (Consolidated)

ESXi operates in a model where all authenticated access is administrative. Non-administrative users (e.g. access to virtual machines) do not have any host configuration privileges at all. Non-administrative user virtual machine configuration privileges are only non-security-sensitive. (For example, a user can disconnect or “eject” a virtual CD-ROM image but cannot choose a different CD-ROM image to connect. Or a user can change screen resolution, which has no security impact.)

The following table describes operations used to perform certain management functions on an ESXi system. Some apply to the ESXi host and some apply to virtual machines.

#	Function	Operation
1	Installing ESXi updates	See Section 4.6.1.
2	Configure password policy	See Section 4.4.2.
3	Create, configure, and delete VMs	For the VIM API, see: <ul style="list-style-type: none"><li>• <a href="#">vim.Folder.CreateVM Task</a></li></ul>

		<ul style="list-style-type: none"> <li>• <a href="#">vim.VirtualMachine.ReconfigVM_Task</a></li> <li>• <a href="#">vim.ManagedEntity.Destroy_Task</a></li> </ul> <p>Also see <a href="#">Managed Object – VirtualMachine(vim.VirtualMachine)</a></p> <p>For Host Client, see <a href="#">Virtual Machine Management with the VMware Host Client</a>.</p>
<b>4</b>	Set default initial VM configurations	<p>Default initial VM configurations are always “empty”. Overriding this “empty” configuration can be done through the config parameter to <a href="#">CreateVM_Task</a>.</p> <p>Overriding the default “empty” configuration can also be done through the Create VM wizard in the ESXi Host Client. See <a href="#">Create a Virtual Machine in the VMware Host Client</a>.</p>
<b>5</b>	Configure virtual networks	See Section 4.3.1.
<b>6</b>	Configure and manage audit system and audit data	See Section 4.1.
<b>7</b>	Configure VM access to physical devices	See Section 4.3.2.
<b>8</b>	Configure inter-VM data sharing	See “Configure virtual networks” in this table (item 5).
<b>9</b>	Enable/disable hypercalls	N/A – the PP-Module for Server Virtualization defines this as an optional management function and ESXi does not claim this. It has been included in the table for completeness.
<b>10</b>	Configure removable media policy	See Section 4.6.2.
<b>11</b>	Configure cryptographic functionality	See Section 4.1.3 and subsections.
<b>12</b>	Change default authorization factors	See Section 4.4.
<b>13</b>	Enable/disable screen lock	N/A – the PP-Module for Server Virtualization defines this as an optional management function and ESXi does not claim this. It has been included in the table for completeness.
<b>14</b>	Configure screen lock inactivity timeout	N/A – the PP-Module for Server Virtualization defines this as an optional management function and ESXi does not claim this. It has been included in the table for completeness.
<b>15</b>	Configure remote connection inactivity timeout	See Section 4.7.1.
<b>16</b>	Configure lockout policy for unsuccessful authentication attempts	See Section 4.4.1.

17	Configure directory server	N/A – the PP-Module for Server Virtualization defines this as an optional management function and ESXi does not claim this. It has been included in the table for completeness.
18	Configure audit/logging server	See Section 4.1.2.
19	Configure name/address of network time server	<p>For the VIM API, supply a list of time servers to <a href="#">UpdateDateTimeConfig</a> using <a href="#">HostDateTimeConfig</a>'s <a href="#">HostNtpConfig</a> or <a href="#">HostPtpConfig</a> object.</p> <p>For Host Client, see <a href="#">Edit the Time Configuration of an ESXi Host in the VMware Host Client</a>.</p> <p>Note that with Host Client the PTP Daemon must be explicitly started in order to use PTP. Enabling PTP when editing the PTP settings is insufficient. It is also important to manually refresh the <b>Time &amp; date</b> panel after making changes to see the updated settings in the summary (the summary is not automatically updated).</p>
20	Configure banner	See Section 4.7.2.
21	Connect/disconnect removable devices to/from a VM	See Sections 4.3.2 and 4.6.2.
22	Start a VM	<p>For the VIM API, see <a href="#">vim.VirtualMachine.PowerOn_Task</a>.</p> <p>For Host Client, see <a href="#">Power States of a Virtual Machine in the VMware Host Client</a>.</p>
23	Stop/halt a VM	<p>For the VIM API, see <a href="#">vim.VirtualMachine.PowerOffVM_Task</a>.</p> <p>For Host Client, see <a href="#">Power States of a Virtual Machine in the VMware Host Client</a>.</p>
24	Checkpoint a VM	<p>VMware uses the term “Snapshot”. For the VIM API, see <a href="#">vim.VirtualMachine.CreateSnapshot_Task</a>.</p> <p>For Host Client, see <a href="#">Using Snapshots to Manage Virtual Machines</a>.</p>
25	Suspend a VM	<p>For the VIM API, see <a href="#">vim.VirtualMachine.SuspendVM_Task</a>.</p> <p>For Host Client, see <a href="#">Power States of a Virtual Machine in the VMware Host Client</a>.</p>
26	Resume a VM	Resuming a VM is equivalent to starting a VM when the VM has a suspended state. See “Start a VM” in this table.

Table 4: Security-Relevant Management Functions

## 4.6 Hypervisor Integrity (FPT)

### 4.6.1 Trusted Updates

ESXi is made up of an “image profile” which describes a set of vSphere Installation Bundles (VIBs) that contain the actual software. A VIB is a signed ramdisk representing a component of the system, roughly analogous to an RPM or DEB on a Linux system. An “image profile” is a collection of VIBs; ESXi patches contain updated image profiles composed from a common set of VIBs.

The ESXi upgrade process is described in the [VMware ESXi Upgrade](#) documentation. ESXi updates are installed using ESXCLI, with commands in the `esxcli software` namespace. See [Upgrading Hosts by Using ESXCLI Commands](#). ESXi software updates are validated using code signing certificates. The root CAs used for update verification are loaded automatically during initial installation of ESXi; no administrator configuration is necessary for this.

ESXCLI may be used to list all installed VIBs and their current version, or the current image profile, using the following commands:

```
esxcli software vib list
esxcli software profile get
```

The general upgrade process is:

- Put the ESXi host into maintenance mode.
- Run an `esxcli software profile update` command (pointing to a URL, or a .zip file transferred to the host).
- Reboot the system.
- Take the system out of maintenance mode.

Secure transfer of VIBs or the entire depot is not necessary, as the VIBs themselves are cryptographically signed by VMware and the update process will verify these signatures.

*Note: Other upgrade mechanisms as described by the VMware ESXi Upgrade documentation might work correctly. However, these mechanisms require external services (for example, PXE booting), which are either not available in a NIAP configuration or where security cannot be evaluated.*

The Host Client may be used to install individual VIBs, but not entire patch releases. See [Update Your VMware Host Client Environment to the Latest Version](#).

Once the update process has completed, the newly installed version can be verified following the process described in section 2.4.4 above.

### 4.6.2 Removable Devices and Media

#### 4.6.2.1 USB devices

Removable USB devices (and any associated media) are covered in Section 4.3.2.1.

#### 4.6.2.2 CD-ROM devices

CD-ROM images in the form of files within a datastore (ISO format) can be connected to a virtual machine. This is most commonly used to install a guest operating system. CD-ROM images support read access only.

These configurations may be supplied through the VIM API by adding a [vim.vm.device.VirtualCdrom](#) to the virtual machine's device list with the corresponding [vim.vm.device.VirtualCdrom.IsoBackingInfo](#) backing.

To make the CD-ROM image available to a virtual machine using Host Client, see [Add a CD or DVD Drive to a Virtual Machine in the VMware Host Client](#).

*Note that ISO files are the only mechanism by which a CD-ROM logical interface is supported in the evaluated configuration; support for physical optical drives is not claimed.*

## 4.7 Accessing the Hypervisor (FTA)

### 4.7.1 Session Timeouts

Timeouts for VIM and Host Client are configurable through advanced options.

See the following options in Section 3.3:

```
Config.HostAgent.vmacore.soap.sessionTimeout  
UserVars.HostClientSessionTimeout
```

### 4.7.2 Administrative Access Banner

ESXi has two configurable access “banners” before beginning a Host Client interactive administrative session, one displayed before login and one after. The contents are stored as strings, in Advanced Options on the system. The strings permit embedded newlines and support reasonable line lengths. When unset or set to an empty string, no message is displayed.

See the following options in Section 3.3:

```
Annotations.WelcomeMessage  
UserVars.HostClientWelcomeMessage
```

## 4.8 Secure Communication with the Hypervisor (FTP)

### 4.8.1 Establishing Remote Administrative Sessions

ESXi implements several login mechanisms.

- VIM API: Use VIM's `SessionManager.Login` method to supply a user name and password. This will set an HTTPS cookie for the HTTPS client containing a session ID, which may be used to authenticate future VIM API calls using distinct HTTPS connections during the same login session.

The VIM API operates as SOAP method calls over HTTPS using the standard HTTPS port (443). Connections may be made based on hostname or IP address; ESXi's self-



signed TLS certificate specifies hostname only (Subject Alt Name DNS), but a customer-supplied TLS certificate may specify more.

- **Host Client (UI):** Enabled by default. The Host Client’s web page accepts credentials (user name and password).  
Connections may be made based on hostname or IP address; ESXi’s self-signed TLS certificate specifies hostname only (Subject Alt Name DNS), but a customer-supplied TLS certificate may specify more.
- **ESXCLI:** The ESXCLI client accepts username and password parameters using the `--username` and `--password` flags.  
ESXCLI authenticates the server using TLS certificates when connecting. Clients should either install a corresponding CA certificate on the client, use the `--cacertsfile` flag to specify a CA certificate manually, or use the `--thumbprint` flag to specify a certificate thumbprint.

#### 4.8.2 **Configuring Remote Audit Servers**

Configuration of remote audit servers is covered in Section 4.1.2.

#### 4.8.3 **User Interface Indicators**

The only interface that supports direct viewing of a VM console is the Host Client (UI). Using that interface, administrators can open the VM console window as either an embedded window within the UI, as a distinct browser tab, as a distinct browser window, or through the VMware Remote Client (VMRC). Usage of VMRC is outside the scope of this evaluation.

Within the Host Client (UI), VM consoles are identified by the name of the VM in the window’s title bar. The VM with input focus is the top-most window.

The VIM API identifies virtual machines with a Managed Object Identifier (MOID), which is the unique identifier used within the API. The MOID is assigned automatically and uniquely within the TOE and may not be changed. As this identifier is meaningless to a user, the Host Client uses the human-readable “name” field within the Managed Object.



## APPENDIX A: AUDIT INFORMATION

Local audit log files are pre-allocated when configured. This prevents any error due to out-of-space during ordinary operation.

### A.1 Audit Record Format

This section describes the format of audit events in local and remote audit logs. Specific events are documented in Appendix A: Audit Events.

#### A.1.1 Audit Record Structure in Local Storage

Local storage of audit records follows the format defined by [RFC 5424](#). Each record is composed of the following fields (all in ASCII except the structured data frame which can contain UTF-8):

- 1) A '<' character, followed by digits that express the message PRI (facility and severity), followed by a '>' character. For all audit messages the facility is 13 and the severity is from 0 to 7. This results in a PRI with values from 104 to 111.
- 2) The digit 1 (representing Version 1 of the syslog protocol specification)
- 3) A SPACE character
- 4) An [RFC 3339](#) time stamp (the time when the audit record was generated)
- 5) A SPACE character
- 6) A dash ('-') character (representing a missing hostname, since the records are local)
- 7) A SPACE character
- 8) The name of the program issuing the audit record
- 9) A SPACE character
- 10) The process ID (PID) of the issuing program
- 11) A SPACE character
- 12) A dash ('-') character (representing a missing MSGID, since audit records do not use this field)
- 13) A SPACE character
- 14) A structured data frame (which contains the audit record parameters)
- 15) A LF character (that is, a new line)

#### A.1.2 Audit Record Structure for Remote Syslog Transmission

An audit record for remote syslog transmission follows the format defined by [RFC 3164](#), with the message following the structured data definition in [RFC 5424](#). Each record is composed of the following fields (all in ASCII except the structured data frame which can contain UTF-8):

- 1) A '<' character, followed by digits that express the message PRI (facility and severity), followed by a '>' character. For all audit messages the facility is 13 and the severity is from 0 to 7. This results in a PRI with values from 104 to 111.
- 2) An [RFC 3339](#) time stamp (the time when the audit record was generated)
- 3) A SPACE character
- 4) The identification string of the TOE (the "system name")
- 5) A SPACE character
- 6) The name of the program issuing the audit record

- 7) A '[' character
- 8) The process ID (PID) of the issuing program
- 9) A ']' character
- 10) A ':' character
- 11) A SPACE character
- 12) A structured data frame (which contains the audit record parameters)
- 13) A LF character (that is, a new line)

### A.1.3 Structured Data Frame Description

The language used for describing an audit record structured data frame is taken from [RFC 5424](#). A structured data frame is delimited by an open and a close square bracket ('[' and ']'). The format of the data within is:

```
[name@6876 paramName="paramValue" paramName="paramValue" ...]
```

- name@6876  
This is an RFC 5424 SD-ID. The RFC specifies that an SD-ID must be a non-empty ASCII string which excludes whitespace, '=', ']', '"', and all control characters. It must be 32 characters or less in length. It consists of two parts, a name (which VMware is using for the audit event identifier, i.e. an `eventID`) which additionally cannot contain an at sign ('@'), and an IANA [Private Enterprise Number](#) separated from the name by an at sign ('@'). The IANA private enterprise number for VMware is 6876, so all ESXi-generated audit events have that number in the SD-ID.
- paramName="paramValue"  
This is an RFC 5424 PARAM-NAME and PARAM-VALUE. The PARAM-NAME has the same character restrictions as an SD-ID. The same PARAM-NAME can be specified for multiple paramName="paramValue" entries. The PARAM-VALUE is surrounded by '"' and is a UTF-8 string (which can contain ASCII LF characters). If the string contains '"', '\', or ']', these characters must be escaped with a preceding backslash ('\'). A PARAM-VALUE can be of any "reasonable" length (e.g. path names are OK). Note that a backslash followed by a character other than '"', '\', or ']', is not an error from the standpoint of validation. For such cases the '\' is dropped.

The possible parameters that may be present in a structured data frame are described by the descriptions of the audit record types in Appendix A.2 below.

## A.2 Audit Record Types

This section identifies all of the audit record types that VMware ESXi generates and the events that trigger the generation of these records. The parameters associated with each event are also listed. Specific examples of these events are shown in Appendix A.3 below, organized by product functional behavior rather than by event type.

### A.2.1 account.locked

This event is generated when an account was locked due to too many failed login attempts.

Parameters:

- The `subject` is the name of the user whose account was locked.
- The `object` is an empty string (the host itself).
- The `result` is "success" since the account was successfully locked.

### A.2.2 `audit.net.failure`

This event is generated when remote host connectivity was lost. This indicates that a loss of audit records may have occurred.

Parameters:

- The `subject` is an empty string (the host itself).
- The `object` is the affected remote host.
- The `result` is "failure".
- The `reason` is reason for the network failure.

### A.2.3 `audit.storage.recycle`

This event is generated when the audit record storage FIFO returned to its beginning (and older records are dropped).

Parameters:

- The `subject` is an empty string (the host itself).
- The `object` is "audit".
- The `result` is "success".

### A.2.4 `audit.start`

This event is generated when audit records storage and/or transmission was started.

Parameters:

- The `subject` is an empty string (the host itself).
- The `object` is "audit".
- The `result` is "success".

### A.2.5 `audit.stop`

This event is generated when audit record storage and/or transmission was stopped.

Parameters:

- The `subject` is an empty string (the host itself).
- The `object` is "audit".
- The `result` is "success".

### A.2.6 `https.connect`

This event is generated when an attempt was made to establish an HTTPS connection.

Parameters:

- The `subject` is an empty string (the host itself).
- The `object` is an empty string (the host itself).
- The `result` is "success" or "failure".
- The `reason`, if present, provides additional details about the event.
- The `ip` is the network address of the originator of the connection.

### A.2.7 `https.disconnect`

This event is generated when an HTTPS connection was ended.

Parameters:

- The `subject` is an empty string (the host itself).
- The `object` is an empty string (the host itself).
- The `result` is "success".
- The `ip` is the network address of the originator of the connection.

### A.2.8 `login.connect`

This event is generated whenever an attempt was made to log in.

Parameters:

- The `subject` is the name of the user attempting to log in.
- The `object` is an empty string (the host itself).
- The `result` is "success" or "failure".
- The `reason`, if present, provides additional details about the event.
- The `ip` is the network address of the originator of the connection.
- The `opID`, if present, is the operation ID.

### A.2.9 `login.disconnect`

This event is generated when a login was ended (explicit or time out).

Parameters:

- The `subject` is the name of the user associated with the login.
- The `object` is an empty string (the host itself).
- The `result` is "success" or "failure".
- The `reason`, if present, provides additional details about the event.
- The `ip` is the network address of the originator of the operation.
- The `opID`, if present, is the operation ID.

### A.2.10 `rbg.entropy.failure`

This event is generated when the host was unable to provide a sufficient amount of entropy for cryptographically secure random number generation.

Parameters:

- The `subject` is an empty string (the host itself).
- The `object` is "rbg".
- The `result` is "failure".
- The `reason`, if present, indicates the reason for the failure. When testing for entropy failure, the reason is "test".

### A.2.11 `settings.advanced.set`

This event is generated when an attempt was made to change an advanced option.

Parameters:

- The `subject` is the name of the user who requested the operation.
- The `object` is the name of the advanced option.
- The `result` is "success" or "failure".
- The `reason` is present when `result` is "failure" and indicates the reason for the failure.
- The `value` is the new value specified for the advanced option.
- The `ip` is the network address of the originator of the operation.
- The `opID`, if present, is the operation ID.

### A.2.12 `syslog.net.connect`

This event is generated when the ESXi syslog daemon, `vmsyslogd`, establishes a connection (e.g. UDP, TCP, TLS (SSL)) to a remote host.

Parameters:

- The `subject` is an empty string (the host itself).
- The `object` is the remote host (a syslog collector) identifier (e.g. DNS address, IPV4 or IPV6 address).
- The `result` is "success" or "failure".
- The `reason`, if present, provides additional details about the event.
- The `subjectDN` is present when `result` is "failure" and the root cause of the failure was due to a TLS (SSL) connection failure. The `subjectDN` is the subject of the presented peer certificate in Distinguished Name (DN) form, e.g. "C=US,L=Palo Alto,O=VMware".
- The `subjectAltName` is present when `result` is "failure" and the root cause of the failure was due to a TLS (SSL) connection failure. The `subjectAltName` is the subject alternate name extension of the presented peer certificate. e.g. "IP:10.128.169.4".
- The `referenceID` is present when `result` is "failure" and the root cause of the failure was due to a TLS (SSL) connection failure. The `referenceID` is the address of the remote server (DNS, IPv4) from the client configuration. This is the reference identifier that is matched with the presented identifier.

### A.2.13 `syslog.net.disconnect`

This event is generated when the ESXi syslog daemon, `vm syslogd`, terminates a connection (e.g. UDP, TCP, TLS (SSL)) with a remote host.

Parameters:

- The `subject` is an empty string (the host itself).
- The `object` is the remote host (a syslog collector) identifier (e.g. DNS address, IPV4 or IPV6 address).
- The `result` is "success" or "failure".
- The `reason`, if present, provides additional details about the event.

### A.2.14 `syslog.net.link`

This event is generated when a remote host network connection changes state.

Parameters:

- The `subject` is an empty string (the host itself).
- The `object` is the remote host (a syslog collector) identifier (e.g. DNS address, IPv4 or IPv6 address).

When the link transitions from "up" to "down":

- The `result` is "failure".
- The `reason` is "link down".

When the link transitions from "down" to "up":

- The `result` is "success".
- The `reason` is "link up".

### A.2.15 `syslog.reload`

This event is generated when an attempt was made to force the syslog/audit daemon to reload its parameters.

Parameters:

- The `subject` is the name of the user who requested the operation.
- The `object` is "syslog".
- The `result` is "success" or "failure".
- The `reason` is present when `result` is "failure" and indicates the reason for the failure.
- The `ip` is the network address of the originator of the operation.

### A.2.16 `system.update.end`

This event is generated at the end of a system update.

Parameters:

- The `subject` is the name of the user who requested the operation.
- The `object` is an empty string (the host itself).
- The `result` is "success" or "failure".
- The `reason`, if present, provides additional details about the event.
- The `vib` describes the identity of the update.

### A.2.17 `system.update.start`

This event is generated when an attempt was made to initiate a system update.

Parameters:

- The `subject` is the name of the user who requested the operation.
- The `object` is an empty string (the host itself).
- The `result` is "success" or "failure".
- The `reason`, if present, provides additional details about the event.
- The `vib` describes the identity of the update.

## A.2.18 time.parameters

This event is generated when an attempt was made to change an NTP/PTP (clock synchronization) configuration parameter.

Parameters:

- The `subject` is the name of the user who requested the operation.
- The `object` is an empty string (the host itself).
- The `result` is "success" or "failure".
- The `reason` is present when `result` is "failure" and indicates the reason for the failure.
- The `ip` is the network address of the originator of the operation.
- The `operation` provides which setting is being affected.
  - "SetEnabled" Enable/Disable the service (NTP,PTP)
  - "SetServers" Set the list of servers or none if no servers (NTP)
  - "UpdateFirewallRule" Update the firewall rule (NTP,PTP)
  - "SetLogLevel" Set the logging level (NTP,PTP)
  - "ResetToFactory" Reset to factory settings (NTP,PTP)
  - "LoadConfig" Load a new NTP configuration file (NTP)
  - "SetDomain" Set the domain (PTP)
  - "SetPort" Set the port (PTP)
  - "SetIpConfig" Set the IP configuration (PTP)
  - "ValidatePciPassthruDev" Validate the pic passthru device (PTP)
  - "SetDevice" Set the network device type (PTP)
  - "SetEvent" Enable sending events to VC (TIME)
  - "SetFallback" Enable fallback to NTP from PTP
  - "UpdateConfig" Update the time configuration (TIME, PTP, NTP)
  - "ConfigureSettings" Configure time settings. (TIME)
  - "DaemonStateChange" Values for this operation include "start", "stop" and "restart". (NTP, PTP)
- The `value` is the value that the setting is being changed to.
- The `comment`, if present, provides information about the event.
- The `type`, if present, provides information about the specific type of daemon (PTP, NTP) or TIME to specify a common parameter.
- The `enabled`, if present, provides information that pertains to enabled/disabled setting.
- The `servers`, if present, is a list of servers.
- The `level`, if present, is the logging level.
- The `path`, if present, is the path of an NTP configuration file.
- The `index`, if present, is the port's index in PTP.
- The `deviceLabel`, if present, is the PTP port device name.
- The `deviceID`, if present, is the type of the device in PTP.
- The `domain`, if present, is the domain of PTP.
- The `netmask`, if present, is the subnet mask.



- The `protocol`, if present, is set to one of "DHCP", "static IP address", or "none" if no protocol applies.
- The `event`, if present, is the time service that was sending events when failure was detected.
- The `backup`, if present, specifies the use of NTP as fallback upon a PTP service failure.

### A.2.19 `vm.change`

This event is generated when an attempt was made to change a VM.

Parameters:

- The `subject` is the name of the user who requested the operation.
- The `object` is the path of the VMX file of the affected VM.
- The `result` is "success" or "failure".
- The `reason` is present when the result is "failure" and indicates the reason for the failure.
- The `ip` is the network address of the originator of the operation.
- The `operation` indicates what change was involved:
  - "checkpoint" Snapshot a VM
  - "create" Create a VM
  - "delete" Delete a VM
  - "powerOff" Power off a VM
  - "powerOn" Power on a VM
  - "reconfigure" Reconfigure a VM
  - "reset" Reset a VM
  - "suspend" Suspend a VM
- The `opID`, if present, is the operation ID.

### A.2.20 `vm.hypercall.access`

This event is generated when an attempt was made by a VM to use a disabled hypercall.

Parameters:

- The `subject` is an empty string (the host itself).
- The `object` is the path of the VMX file of the reporting VM.
- The `result` is "failure".
- The `reason` is present when `result` is "failure" and indicates the reason for the failure.
- The `type` is "Backdoor" or "HbBackdoor".
- The `value` is the hypercall number.
- The `name`, if present, is the name of the hypercall.
- The `opID`, if present, is the operation ID.

### A.2.21 vm.net.add

This event is generated when an attempt was made to attach a network to a VM.

Parameters:

- The `subject` is the name of the user requesting the operation.
- The `object` is the path of the VMX file of the affected VM.
- The `result` is "success" or "failure".
- The `ip` is the network address of the originator of the operation.
- The `networkID` is the name of the network that was to be attached.
- The `opID`, if present, is the operation ID.

### A.2.22 vm.net.edit

This event is generated when an attempt was made to modify a network attached to a VM.

Parameters:

- The `subject` is the name of the user who requested the operation.
- The `object` is the path of the VMX file of the affected VM.
- The `result` is "success" or "failure".
- The `ip` is the network address of the originator of the operation.
- The `networkID` is the name of the new network.
- The `oldID` is the name of the old network.
- The `status` is "connected" or "disconnected" when a change affects device connectivity.
- The `opID`, if present, is the operation ID.

### A.2.23 vm.net.remove

This event is generated when an attempt was made to detach a network from a VM.

Parameters:

- The `subject` is the name of the user who requested the operation.
- The `object` is the path of the VMX file of the affected VM.
- The `result` is "success" or "failure".
- The `ip` is the network address of the originator of the operation.
- The `networkID` is the name of the network that was to be detached.
- The `opID`, if present, is the operation ID.

### A.2.24 vm.storage.add

This event is generated when an attempt was made to add a virtual storage device to a VM.

Parameters:

- The `subject` is the name of the user who requested the operation.
- The `object` is the path of the VMX file of the affected VM.
- The `result` is "success" or "failure".
- The `ip` is the network address of the originator of the operation.
- The `path` is the path to the affected file or an empty string when a local device is auto selected.
- The `opID`, if present, is the operation ID.

### A.2.25 vm.storage.edit

This event is generated when an attempt was made to modify the "backing" (e.g. file, device) of a virtual storage device associated with a VM.

Parameters:

- The `subject` is the name of the user who requested the operation.
- The `object` is the path of the VMX file of the affected VM.
- The `result` is "success" or "failure".
- The `ip` is the network address of the originator of the operation.
- The `oldPath` is the path to the detached file or an empty string when a local device is auto selected.
- The `path` is the path to the attached file or an empty string when a local device is auto selected.
- The `status` is "connected" or "disconnected" when a change affects device connectivity.
- The `opID`, if present, is the operation ID.

### A.2.26 vm.storage.remove

This event is generated when an attempt was made to remove a virtual storage device from a VM.

Parameters:

- The `subject` is the name of the user who requested the operation.
- The `object` is the path of the VMX file of the affected VM.
- The `result` is "success" or "failure".
- The `ip` is the network address of the originator of the operation.

- The `path` is the path to the affected file or an empty string when a local device is auto selected.
- The `opID`, if present, is the operation ID.

### A.2.27 `vm.usb.connect`

This event is generated when an attempt was made to connect a USB device to a VM.

Parameters:

- The `subject` is an empty string (the host itself).
- The `object` is the path of the VMX file of the reporting VM.
- The `result` is "success" or "failure".
- The `reason`, if present, provides additional details about the event.
- The `opID`, if present, is the operation ID.
- The `deviceLabel`, if present, is "usb:<N>" for usb 1.1, "ehci:<N>" for usb 2.0, or "usb\_xhci:<N>" for usb 3.x. The "<N>" is a small integer, uniquely identifying the USB controller involved.
- The `vendorID` is the vendor ID of the device.
- The `productID` is the product ID of the device.

### A.2.28 `vm.usb.disconnect`

This event is generated when an attempt was made to disconnect a USB device from a VM.

Parameters:

- The `subject` is an empty string (the host itself).
- The `object` is the path of the VMX file of the reporting VM.
- The `result` is "success" or "failure".
- The `reason`, if present, provides additional details about the event.
- The `opID`, if present, is the operation ID.
- The `deviceLabel`, if present, is "usb:<N>" for usb 1.1, "ehci:<N>" for usb 2.0, or "usb\_xhci:<N>" for usb 3.x. The "<N>" is a small integer, uniquely identifying the USB controller involved.
- The `vendorID`, if present, is the vendor ID of the device.
- The `productID`, if present, is the product ID of the device.
- The `deviceID`, if present, is the device ID of the device.

### A.2.29 `x509.cacert.add`

This event is generated when an attempt was made to add a CA certificate to the host CA store.

Parameters:

- The `subject` is the name of the user who requested the operation.
- The `object` is an empty string (empty string) since the "system" did it.
- The `result` is "success" or "failure".
- The `reason`, if present, provides additional details about the event.
- The `subjectDN` is the subject distinguished name of the CA certificate.

### A.2.30 x509.cacert.remove

This event is generated when an attempt was made to remove a CA certificate from the host CA store.

Parameters:

- The `subject` is the name of the user who requested the operation.
- The `object` is an empty string (empty string) since the "system" did it.
- The `result` is "success" or "failure".
- The `reason`, if present, provides additional details about the event.
- The `subjectDN` is the subject distinguished name of the CA certificate.

### A.2.31 x509.srvcert.generate

This event is generated when an attempt was made to generate a certificate signing request.

Parameters:

- The `subject` is the name of the user who requested the operation.
- The `object` is an empty string (empty string) since the "system" did it.
- The `result` is "success" or "failure".
- The `reason`, if present, provides additional details about the event.
- The `ip` is the network address of the originator of the operation.

### A.2.32 x509.srvcert.install

This event is generated when an attempt was made to install a new server certificate.

Parameters:

- The `subject` is the name of the user who requested the operation.
- The `object` is an empty string (empty string) since the "system" did it.
- The `result` is "success" or "failure".
- The `reason`, if present, provides additional details about the event.
- The `ip` is the network address of the originator of the operation.
- The `subjectDN`, if present, is the subject distinguished name of the server certificate.

## A.3 Audit Record Examples

The following section lists examples of audit records for various security-relevant events as a reference for what to expect when these events occur.

### A.3.1 Example Record Formatting

Locally-stored records will differ slightly in their format from the records exported to an external syslog. See below for an example of this.

An audit record within local storage:

```
<110>1 2022-10-31T17:43:11Z - vmsyslogd 1000347563 -
[audit.start@6876 subject="root" object="" result="success"]
```

The equivalent audit record as transmitted off the TOE:

```
<110>2022-10-31T17:43:11Z esx-host.example.com
vmsyslogd[1000347563]: [audit.start@6876 subject="root"
object="" result="success"]
```

### A.3.2 Security-Relevant Audit Records

The following tables include lists of events that must be audited per the claimed CC requirements along with sample records that show what an audit record for that event may look like. Note that the first table shows audit records that correspond to the execution of the management functions listed in section 4.5.3 above while the second table shows records for generalized security-relevant behavior.

Function	Sample Record
Installing ESXi updates	<pre>&lt;19&gt;1 2022-07-25T14:11:24.700Z - esxupdate 2101211 - [system.update.start@6876 subject="root" object="" result="success" reason="" vib="add: {VMW_bootbank_lpfc_14.0.169.25- 5vmw.703.0.35.19482537,VMW_bootbank_nvmetcp_1.0.0.1- 1vmw.703.0.35.19482537,VMware_bootbank_bmcad_7.0.3- 0.35.19482537,VMware_bootbank_cpu-microcode_7.0.3- 0.35.19482537,VMware_bootbank_crx_7.0.3- 0.35.19482537,VMware_bootbank_esx-base_7.0.3- 0.35.19482537,VMware_bootbank_esx-dvfilter-generic- fastpath_7.0.3-0.35.19482537,VMware_bootbank_esx- update_7.0.3-0.35.19482537,VMware_bootbank_esx- xserver_7.0.3-0.35.19482537,VMware_bootbank_esxio- combiner_7.0.3-0.35.19482537,VMware_bootbank_gc_7.0.3- 0.35.19482537,VMware_bootbank_loadesx_7.0.3- 0.35.19482537,VMware_bootbank_lsuv2-lsiv2-drivers- plugin_1.0.0- 10vmw.703.0.35.19482537,VMware_bootbank_native-misc- drivers_7.0.3-0.35.19482537,VMware_bootbank_trx_7.0.3- 0.35.19482537,VMware_bootbank_vdfs_7.0.3- 0.35.19482537,VMware_bootbank_vsan_7.0.3- 0.35.19482537,VMware_bootbank_vsanhealth_7.0.3- 0.35.19482537} remove: {VMW_bootbank_lpfc_14.0.169.25- 5vmw.703.0.20.19193900,VMW_bootbank_nvmetcp_1.0.0.0- 1vmw.703.0.20.19193900,VMware_bootbank_bmcad_7.0.3-</pre>

```
0.30.19482531,VMware_bootbank_cpu-microcode_7.0.3-
0.30.19482531,VMware_bootbank_crx_7.0.3-
0.30.19482531,VMware_bootbank_esx-base_7.0.3-
0.30.19482531,VMware_bootbank_esx-dvfilter-generic-
fastpath_7.0.3-0.30.19482531,VMware_bootbank_esx-
update_7.0.3-0.30.19482531,VMware_bootbank_esx-
xserver_7.0.3-0.30.19482531,VMware_bootbank_esxio-
combiner_7.0.3-0.30.19482531,VMware_bootbank_gc_7.0.3-
0.30.19482531,VMware_bootbank_loadesx_7.0.3-
0.30.19482531,VMware_bootbank_lsuv2-lsiv2-drivers-
plugin_1.0.0-
9vmw.703.0.20.19193900,VMware_bootbank_native-misc-
drivers_7.0.3-0.30.19482531,VMware_bootbank_trx_7.0.3-
0.30.19482531,VMware_bootbank_vdfs_7.0.3-
0.30.19482531,VMware_bootbank_vsan_7.0.3-
0.30.19482531,VMware_bootbank_vsanhealth_7.0.3-
0.30.19482531}]"]

<19>1 2022-07-25T14:11:37.336Z - esxupdate 2101211 -
[system.update.end@6876 subject="root" object=""
result="success" reason="" vib="add:
{VMW_bootbank_lpfc_14.0.169.25-
5vmw.703.0.35.19482537,VMW_bootbank_nvmetcp_1.0.0.1-
1vmw.703.0.35.19482537,VMware_bootbank_bmcad_7.0.3-
0.35.19482537,VMware_bootbank_cpu-microcode_7.0.3-
0.35.19482537,VMware_bootbank_crx_7.0.3-
0.35.19482537,VMware_bootbank_esx-base_7.0.3-
0.35.19482537,VMware_bootbank_esx-dvfilter-generic-
fastpath_7.0.3-0.35.19482537,VMware_bootbank_esx-
update_7.0.3-0.35.19482537,VMware_bootbank_esx-
xserver_7.0.3-0.35.19482537,VMware_bootbank_esxio-
combiner_7.0.3-0.35.19482537,VMware_bootbank_gc_7.0.3-
0.35.19482537,VMware_bootbank_loadesx_7.0.3-
0.35.19482537,VMware_bootbank_lsuv2-lsiv2-drivers-
plugin_1.0.0-
10vmw.703.0.35.19482537,VMware_bootbank_native-misc-
drivers_7.0.3-0.35.19482537,VMware_bootbank_trx_7.0.3-
0.35.19482537,VMware_bootbank_vdfs_7.0.3-
0.35.19482537,VMware_bootbank_vsan_7.0.3-
0.35.19482537,VMware_bootbank_vsanhealth_7.0.3-
0.35.19482537} remove: {VMW_bootbank_lpfc_14.0.169.25-
5vmw.703.0.20.19193900,VMW_bootbank_nvmetcp_1.0.0.0-
1vmw.703.0.20.19193900,VMware_bootbank_bmcad_7.0.3-
0.30.19482531,VMware_bootbank_cpu-microcode_7.0.3-
0.30.19482531,VMware_bootbank_crx_7.0.3-
0.30.19482531,VMware_bootbank_esx-base_7.0.3-
0.30.19482531,VMware_bootbank_esx-dvfilter-generic-
fastpath_7.0.3-0.30.19482531,VMware_bootbank_esx-
update_7.0.3-0.30.19482531,VMware_bootbank_esx-
xserver_7.0.3-0.30.19482531,VMware_bootbank_esxio-
combiner_7.0.3-0.30.19482531,VMware_bootbank_gc_7.0.3-
0.30.19482531,VMware_bootbank_loadesx_7.0.3-
0.30.19482531,VMware_bootbank_lsuv2-lsiv2-drivers-
plugin_1.0.0-
9vmw.703.0.20.19193900,VMware_bootbank_native-misc-
drivers_7.0.3-0.30.19482531,VMware_bootbank_trx_7.0.3-
0.30.19482531,VMware_bootbank_vdfs_7.0.3-
```

	0.30.19482531,VMware_bootbank_vsan_7.0.3-0.30.19482531,VMware_bootbank_vsanhealth_7.0.3-0.30.19482531}"]
Configure password policy	<110>1 2022-07-22T20:40:39.664Z - Hostd 2099692 - [settings.advanced.set@6876 subject="root" object="Security.PasswordMaxDays" value="365" ip="172.16.1.50" opID="esxui-83ff-67ae" result="success"]
Create, configure, and delete VMs	<pre>&lt;110&gt;1 2022-07-22T20:47:53.822Z - Hostd 2099692 - [vm.storage.add@6876 subject="root" object="/vmfs/volumes/6148ce85-f29c9ebe-ad18-78ac4428ad30/Testing2/Testing2.vmx" opID="esxui-4de0-6810" ip="172.16.1.50" path="/vmfs/volumes/6148ce85-f29c9ebe-ad18-78ac4428ad30/Testing2/Testing2.vmdk" result="success"]  &lt;110&gt;1 2022-07-22T20:47:53.822Z - Hostd 2099692 - [vm.net.add@6876 subject="root" object="/vmfs/volumes/6148ce85-f29c9ebe-ad18-78ac4428ad30/Testing2/Testing2.vmx" opID="esxui-4de0-6810" ip="172.16.1.50" networkID="network-00" result="success"]  &lt;110&gt;1 2022-07-22T20:47:53.822Z - Hostd 2099692 - [vm.storage.add@6876 subject="root" object="/vmfs/volumes/6148ce85-f29c9ebe-ad18-78ac4428ad30/Testing2/Testing2.vmx" opID="esxui-4de0-6810" ip="172.16.1.50" path="[datastore1\\] ubuntu-22.04-desktop-amd64.iso" result="success"]  &lt;110&gt;1 2022-07-22T20:47:53.822Z - Hostd 2099692 - [vm.net.edit@6876 subject="root" object="/vmfs/volumes/6148ce85-f29c9ebe-ad18-78ac4428ad30/Testing2/Testing2.vmx" opID="esxui-4de0-6810" ip="172.16.1.50" networkID="network-00" status="connected" result="success"]  &lt;110&gt;1 2022-07-22T20:47:53.822Z - Hostd 2099692 - [vm.storage.edit@6876 subject="root" object="/vmfs/volumes/6148ce85-f29c9ebe-ad18-78ac4428ad30/Testing2/Testing2.vmx" opID="esxui-4de0-6810" ip="172.16.1.50" path="[datastore1\\] ubuntu-22.04-desktop-amd64.iso" status="connected" result="success"]  &lt;110&gt;1 2022-07-22T20:47:53.864Z - Hostd 2099692 - [vm.change@6876 subject="root" object="/vmfs/volumes/6148ce85-f29c9ebe-ad18-78ac4428ad30/Testing2/Testing2.vmx" ip="172.16.1.50" operation="create" opID="esxui-4de0-6810" result="success"]  &lt;110&gt;1 2022-07-22T21:18:36.168Z - Hostd 2099692 - [vm.change@6876 subject="root" object="/vmfs/volumes/6148ce85-f29c9ebe-ad18-78ac4428ad30/Testing2/Testing2.vmx" ip="172.16.1.50"</pre>



	<pre>operation="delete" opID="esxui-9059-692a" result="success"]</pre>
<p><b>Set default initial VM configurations</b></p>	<pre>&lt;110&gt;1 2022-07-22T20:47:53.822Z - Hostd 2099692 - [vm.storage.add@6876 subject="root" object="/vmfs/volumes/6148ce85-f29c9ebe-ad18- 78ac4428ad30/Testing2/Testing2.vmx" opID="esxui-4de0- 6810" ip="172.16.1.50" path="/vmfs/volumes/6148ce85- f29c9ebe-ad18-78ac4428ad30/Testing2/Testing2.vmdk" result="success"]  &lt;110&gt;1 2022-07-22T20:47:53.822Z - Hostd 2099692 - [vm.net.add@6876 subject="root" object="/vmfs/volumes/6148ce85-f29c9ebe-ad18- 78ac4428ad30/Testing2/Testing2.vmx" opID="esxui-4de0- 6810" ip="172.16.1.50" networkID="network-00" result="success"]  &lt;110&gt;1 2022-07-22T20:47:53.822Z - Hostd 2099692 - [vm.net.edit@6876 subject="root" object="/vmfs/volumes/6148ce85-f29c9ebe-ad18- 78ac4428ad30/Testing2/Testing2.vmx" opID="esxui-4de0- 6810" ip="172.16.1.50" networkID="network-00" status="connected" result="success"]  &lt;110&gt;1 2022-07-22T20:47:53.822Z - Hostd 2099692 - [vm.storage.add@6876 subject="root" object="/vmfs/volumes/6148ce85-f29c9ebe-ad18- 78ac4428ad30/Testing2/Testing2.vmx" opID="esxui-4de0- 6810" ip="172.16.1.50" path="[datastore1\\] ubuntu- 22.04-desktop-amd64.iso" result="success"]  &lt;110&gt;1 2022-07-22T20:47:53.822Z - Hostd 2099692 - [vm.storage.edit@6876 subject="root" object="/vmfs/volumes/6148ce85-f29c9ebe-ad18- 78ac4428ad30/Testing2/Testing2.vmx" opID="esxui-4de0- 6810" ip="172.16.1.50" path="[datastore1\\] ubuntu- 22.04-desktop-amd64.iso" status="connected" result="success"]  &lt;110&gt;1 2022-07-22T20:47:53.864Z - Hostd 2099692 - [vm.change@6876 subject="root" object="/vmfs/volumes/6148ce85-f29c9ebe-ad18- 78ac4428ad30/Testing2/Testing2.vmx" ip="172.16.1.50" operation="create" opID="esxui-4de0-6810" result="success"]</pre>
<p><b>Configure virtual networks</b></p>	<pre>&lt;110&gt;1 2022-07-22T21:20:58.301Z - Hostd 2099692 - [vm.net.add@6876 subject="root" object="/vmfs/volumes/6148ce85-f29c9ebe-ad18- 78ac4428ad30/Kali Test 1/Kali Test 1.vmx" opID="esxui- 24fe-69f3" ip="172.16.1.50" networkID="network-00" result="success"]  &lt;110&gt;1 2022-07-22T21:20:58.301Z - Hostd 2099692 - [vm.net.edit@6876 subject="root" object="/vmfs/volumes/6148ce85-f29c9ebe-ad18- 78ac4428ad30/Kali Test 1/Kali Test 1.vmx" opID="esxui-</pre>

	<pre>24fe-69f3" ip="172.16.1.50" networkID="network-00" status="connected" result="success"]  &lt;110&gt;1 2022-07-22T21:20:58.726Z - Hostd 2099692 - [vm.change@6876 subject="root" object="/vmfs/volumes/6148ce85-f29c9ebe-ad18- 78ac4428ad30/Kali Test 1/Kali Test 1.vmx" ip="172.16.1.50" operation="reconfigure" opID="esxui- 24fe-69f3" result="success"]</pre>
Configure and manage audit system and audit data	<pre>&lt;110&gt;1 2022-07-24T15:10:18.011Z - Hostd 2099692 - [settings.advanced.set@6876 subject="root" object="Syslog.global.auditRecord.storageCapacity" ip="172.16.0.161" value="8" result="success"]</pre>
Configure VM access to physical devices	<pre>&lt;110&gt;1 2022-07-22T18:59:02.789Z - vmx 2431848 - [vm.usb.connect@6876 subject="" object="/vmfs/volumes/6148ce85-f29c9ebe-ad18- 78ac4428ad30/efi_test_vm/niaptest.vmx" vendorID="0e0f" productID="0003" deviceLabel="usb_xhci:4" result="success"]</pre>
Configure inter-VM data sharing	<pre>&lt;110&gt;1 2022-07-22T20:13:41.914Z - Hostd 2099692 - [vm.net.add@6876 subject="root" object="/vmfs/volumes/6148ce85-f29c9ebe-ad18- 78ac4428ad30/Ubuntu Test 1/Ubuntu Test 1.vmx" opID="esxui-3282-655d" ip="172.16.1.50" networkID="network-00" result="success"]  &lt;110&gt;1 2022-07-22T20:13:41.914Z - Hostd 2099692 - [vm.net.edit@6876 subject="root" object="/vmfs/volumes/6148ce85-f29c9ebe-ad18- 78ac4428ad30/Ubuntu Test 1/Ubuntu Test 1.vmx" opID="esxui-3282-655d" ip="172.16.1.50" networkID="network-00" status="connected" result="success"]  &lt;110&gt;1 2022-07-22T20:13:42.402Z - Hostd 2099692 - [vm.change@6876 subject="root" object="/vmfs/volumes/6148ce85-f29c9ebe-ad18- 78ac4428ad30/Ubuntu Test 1/Ubuntu Test 1.vmx" ip="172.16.1.50" operation="reconfigure" opID="esxui- 3282-655d" result="success"]</pre>
Configure removable media policy	<pre>&lt;110&gt;1 2022-07-22T20:12:03.175Z - Hostd 2099692 - [vm.change@6876 subject="root" object="/vmfs/volumes/6148ce85-f29c9ebe-ad18- 78ac4428ad30/Ubuntu Test 1/Ubuntu Test 1.vmx" ip="172.16.1.50" operation="reconfigure" opID="esxui- 2e0c-64f8" result="success"]</pre>
Configure cryptographic functionality	<pre>&lt;110&gt;1 2022-07-22T20:10:37.844Z - Hostd 2099692 - [settings.advanced.set@6876 subject="root" object="/UserVars/ESXiVPsAllowedCiphers" ip="172.16.1.50" value="!aNULL:kECDH+AESGCM:ECDH+AESGCM:RSA+AESGCM:kECD H+AES:ECDH+AES:RSA+AES" comment="no change" result="success"]</pre>
Change default authorization factors	<pre>&lt;110&gt;1 2022-07-24T16:22:05.475Z - Hostd 2099692 - [x509.cacert.add@6876 subject="root" object=""]</pre>

	<pre>ip="172.16.0.161" subjectDN="CN=esxiroot2.test.domain" result="success"]  &lt;110&gt;1 2022-07-24T16:23:20.374Z - Hostd 2099692 - [x509.cacert.remove@6876 subject="root" object="" ip="172.16.0.161" subjectDN="CN=esxiroot2.test.domain" result="success"]  &lt;110&gt;1 2022-07-24T16:30:04.781Z - Hostd 2099692 - [x509.srvcert.generate@6876 subject="root" object="" ip="172.16.1.50" result="success"]  &lt;110&gt;1 2022-07-24T16:32:36.788Z - Hostd 2099692 - [x509.srvcert.install@6876 subject="root" object="" ip="172.16.1.50" subjectDN="C=US, ST=California, L=Palo Alto, O=VMware, Inc, OU=VMware ESX Server Default Certificate/emailAddress=ssl- certificates@vmware.com, CN=172.16.23.1/unstructuredName=1637248603,564d7761726 520496e632e" result="success"]</pre>
Configure remote connection inactivity timeout	<pre>&lt;110&gt;1 2022-07-22T20:01:40.320Z - Hostd 2099692 - [settings.advanced.set@6876 subject="root" object="/UserVars/HostClientSessionTimeout" ip="172.16.1.50" value="1000" result="success"]</pre>
Configure lockout policy for unsuccessful authentication attempts	<pre>&lt;110&gt;1 2022-07-22T20:23:55.879Z - Hostd 2099692 - [settings.advanced.set@6876 subject="root" object="Security.AccountLockFailures" value="6" ip="172.16.1.50" opID="esxui-8936-6695" result="success"]</pre>
Configure audit/logging server	<pre>&lt;110&gt;1 2022-07-22T20:26:41.563Z - Hostd 2099692 - [settings.advanced.set@6876 subject="root" object="Syslog.global.logHost" ip="127.0.0.1" value="ssl://test.tlss.test.domain:1515" result="success"]  &lt;110&gt;1 2022-07-24T15:59:38.930Z - Hostd 2099692 - [syslog.reload@6876 subject="root" object="syslog" ip="172.16.0.161" value="2" result="success"]</pre>
Configure name/address of network time server	<pre>&lt;110&gt;1 2022-07-22T20:30:14.037Z - Hostd 2099692 - [time.parameters@6876 subject="root" object="" ip="172.16.1.50" operation="SetServers" type="NTP" value="172.16.1.150" result="success"]  &lt;110&gt;1 2022-07-22T20:30:14.037Z - Hostd 2099692 - [time.parameters@6876 subject="root" object="" ip="172.16.1.50" operation="SetServers" type="NTP" value="172.16.1.150" result="success"]</pre>
Configure banner	<pre>&lt;110&gt;1 2022-07-22T19:58:03.098Z - Hostd 2099692 - [settings.advanced.set@6876 subject="root" object="/UserVars/HostClientWelcomeMessage" ip="172.16.1.50" value="CommonCriteriaTestBanner" result="success"]</pre>
Connect/disconnect removable devices to/from a VM	<pre>&lt;110&gt;1 2022-07-22T18:59:02.789Z - vmx 2431848 - [vm.usb.connect@6876 subject="" object="/vmfs/volumes/6148ce85-f29c9ebe-ad18- 78ac4428ad30/efi_test_vm/niaptest.vmx" vendorID="0e0f"</pre>

	<pre>productID="0003" deviceLabel="usb_xhci:4" result="success"]  &lt;110&gt;1 2022-07-22T18:59:02.786Z - vmx 2431848 - [vm.usb.disconnect@6876 subject="" object="/vmfs/volumes/6148ce85-f29c9ebe-ad18- 78ac4428ad30/efi_test_vm/niaptest.vmx" vendorID="0000" productID="0000" deviceLabel="usb_xhci:4" result="success"]</pre>
Start a VM	<pre>&lt;110&gt;1 2022-07-22T18:59:02.825Z - Hostd 2099692 - [vm.change@6876 subject="root" object="/vmfs/volumes/6148ce85-f29c9ebe-ad18- 78ac4428ad30/efi_test_vm/niaptest.vmx" ip="172.16.1.50" operation="powerOn" opID="esxui-a2f9- 61a2" result="success"]</pre>
Stop/halt a VM	<pre>&lt;110&gt;1 2022-07-22T19:30:15.183Z - Hostd 2099692 - [vm.change@6876 subject="root" object="/vmfs/volumes/6148ce85-f29c9ebe-ad18- 78ac4428ad30/efi_test_vm/niaptest.vmx" ip="172.16.1.50" operation="powerOff" opID="esxui- c406-621e" result="success"]</pre>
Checkpoint a VM	<pre>&lt;110&gt;1 2022-07-22T19:51:47.469Z - Hostd 2099692 - [vm.change@6876 subject="root" object="/vmfs/volumes/6148ce85-f29c9ebe-ad18- 78ac4428ad30/efi_test_vm/niaptest.vmx" ip="172.16.1.50" operation="checkpoint" opID="esxui- f4b-62b4" result="success"]</pre>
Suspend a VM	<pre>&lt;110&gt;1 2022-07-22T19:54:13.949Z - Hostd 2099692 - [vm.change@6876 subject="root" object="/vmfs/volumes/6148ce85-f29c9ebe-ad18- 78ac4428ad30/efi_test_vm/niaptest.vmx" ip="172.16.1.50" operation="suspend" opID="esxui-8d2b- 631a" result="success"]</pre>
Resume a VM	<pre>&lt;110&gt;1 2022-07-22T19:55:32.376Z - Hostd 2099692 - [vm.change@6876 subject="root" object="/vmfs/volumes/6148ce85-f29c9ebe-ad18- 78ac4428ad30/efi_test_vm/niaptest.vmx" ip="172.16.1.50" operation="powerOn" opID="esxui-a3c2- 6367" result="success"]</pre>

Table 5: Sample Audit Records for Management Functions

Event	Sample Record
Start-up and shutdown of the audit functions	<pre>&lt;110&gt;1 2021-08-10T07:13:59.468Z - vmsyslogd 1001397645 - [audit.start@6876 subject="" object="" result="success" reason="administrative action"]  &lt;110&gt;1 2021-08-10T07:16:07.601Z - vmsyslogd 1001397645 - [audit.stop@6876 subject="" object="" result="success" reason="administrative action"]</pre>
Failure of audit data capture because of pre-defined limits	<pre>&lt;109&gt;1 2022-07-24T15:21:21.583Z - Hostd 2099692 - [settings.advanced.set@6876 subject="root" object="Syslog.global.auditRecord.storageCapacity"]</pre>

	<pre>ip="172.16.1.50" reason="Audit record storage capacity must be between 4 and 100 (MiB)." value="150" result="failure"]  &lt;110&gt;1 2022-07-22T04:23:15.465Z - vmsyslogd 2424830 - [audit.storage.recycle@6876 subject="" object="audit" result="success"]</pre>
Failure of randomization	<pre>&lt;105&gt;1 2021-08-18T20:56:51.717Z - Hostd 1001392706 - [rbg.entropy.failure@6876 subject="" object="" reason="test" result="failure"]</pre>
Successful and failed attempts to connect VMs to physical and virtual networking components	<pre><b>Success:</b> &lt;110&gt;1 2022-07-22T20:13:41.914Z - Hostd 2099692 - [vm.net.add@6876 subject="root" object="/vmfs/volumes/6148ce85-f29c9ebe-ad18- 78ac4428ad30/Ubuntu Test 1/Ubuntu Test 1.vmx" opID="esxui- 3282-655d" ip="172.16.1.50" networkID="network-00" result="success"]  &lt;110&gt;1 2022-07-22T20:13:41.914Z - Hostd 2099692 - [vm.net.edit@6876 subject="root" object="/vmfs/volumes/6148ce85-f29c9ebe-ad18- 78ac4428ad30/Ubuntu Test 1/Ubuntu Test 1.vmx" opID="esxui- 3282-655d" ip="172.16.1.50" networkID="network-00" status="connected" result="success"]  &lt;110&gt;1 2022-07-22T20:13:42.402Z - Hostd 2099692 - [vm.change@6876 subject="root" object="/vmfs/volumes/6148ce85-f29c9ebe-ad18- 78ac4428ad30/Ubuntu Test 1/Ubuntu Test 1.vmx" ip="172.16.1.50" operation="reconfigure" opID="esxui-3282- 655d" result="success"  <b>Failure:</b> &lt;109&gt;1 2022-07-25T20:26:18.431Z - Hostd 2099805 - [vm.change@6876 subject="root" object="/vmfs/volumes/6148ce85-f29c9ebe-ad18- 78ac4428ad30/Kali Test 1/Kali Test 1.vmx" ip="172.16.1.50" operation="reconfigure" reason="Failed to connect virtual device \'ethernet1\'. " opID="esxui-9835-055b" result="failure"]  &lt;109&gt;1 2022-07-25T20:26:18.432Z - Hostd 2099805 - [vm.net.edit@6876 subject="root" object="/vmfs/volumes/6148ce85-f29c9ebe-ad18- 78ac4428ad30/Kali Test 1/Kali Test 1.vmx" ip="172.16.1.50" networkID="New port group" opID="esxui-9835-055b" result="failure"]</pre>
Security policy violations	<pre>&lt;109&gt;1 2022-07-22T21:33:13.904Z - Hostd 2099692 - [vm.change@6876 subject="root" object="/vmfs/volumes/6148ce85-f29c9ebe-ad18- 78ac4428ad30/Kali Test 1/Kali Test 1.vmx" ip="172.16.1.50" operation="reconfigure" reason="Failed to add disk \'scsi0:1\'. " opID="esxui-e097-6b30" result="failure"]</pre>

	<pre>&lt;109&gt;1 2022-07-22T21:33:13.905Z - Hostd 2099692 - [vm.storage.add@6876 subject="root" object="/vmfs/volumes/6148ce85-f29c9ebe-ad18- 78ac4428ad30/Kali Test 1/Kali Test 1.vmx" ip="172.16.1.50" path="[datastore1\] Ubuntu Test 1/Ubuntu Test 1.vmdk" opID="esxui-e097-6b30" result="failure"]</pre>
<p>Administrator configuration of inter-VM communications channels</p>	<pre>&lt;110&gt;1 2022-07-22T20:13:41.914Z - Hostd 2099692 - [vm.net.add@6876 subject="root" object="/vmfs/volumes/6148ce85-f29c9ebe-ad18- 78ac4428ad30/Ubuntu Test 1/Ubuntu Test 1.vmx" opID="esxui- 3282-655d" ip="172.16.1.50" networkID="network-00" result="success"]  &lt;110&gt;1 2022-07-22T20:13:41.914Z - Hostd 2099692 - [vm.net.edit@6876 subject="root" object="/vmfs/volumes/6148ce85-f29c9ebe-ad18- 78ac4428ad30/Ubuntu Test 1/Ubuntu Test 1.vmx" opID="esxui- 3282-655d" ip="172.16.1.50" networkID="network-00" status="connected" result="success"]  &lt;110&gt;1 2022-07-22T20:13:42.402Z - Hostd 2099692 - [vm.change@6876 subject="root" object="/vmfs/volumes/6148ce85-f29c9ebe-ad18- 78ac4428ad30/Ubuntu Test 1/Ubuntu Test 1.vmx" ip="172.16.1.50" operation="reconfigure" opID="esxui-3282- 655d" result="success"]  &lt;110&gt;1 2022-07-22T21:20:58.301Z - Hostd 2099692 - [vm.net.add@6876 subject="root" object="/vmfs/volumes/6148ce85-f29c9ebe-ad18- 78ac4428ad30/Kali Test 1/Kali Test 1.vmx" opID="esxui- 24fe-69f3" ip="172.16.1.50" networkID="network-00" result="success"]  &lt;110&gt;1 2022-07-22T21:20:58.301Z - Hostd 2099692 - [vm.net.edit@6876 subject="root" object="/vmfs/volumes/6148ce85-f29c9ebe-ad18- 78ac4428ad30/Kali Test 1/Kali Test 1.vmx" opID="esxui- 24fe-69f3" ip="172.16.1.50" networkID="network-00" status="connected" result="success"]  &lt;110&gt;1 2022-07-22T21:20:58.726Z - Hostd 2099692 - [vm.change@6876 subject="root" object="/vmfs/volumes/6148ce85-f29c9ebe-ad18- 78ac4428ad30/Kali Test 1/Kali Test 1.vmx" ip="172.16.1.50" operation="reconfigure" opID="esxui-24fe-69f3" result="success"]</pre>
<p>Unsuccessful login attempts limit is met or exceeded</p>	<pre>&lt;109&gt;1 2022-07-22T13:53:26.053Z - Hostd 2099692 - [login.connect@6876 subject="LoginTest" object="" ip="172.16.0.161" reason="Invalid Login" opID="esxcli-ae- 5dca" result="failure"]  &lt;109&gt;1 2022-07-22T13:53:26.033Z - vobd 2097881 - [account.locked@6876 subject="LoginTest" object="" result="success"]</pre>

<p>Administrator authentication attempts</p>	<pre>&lt;110&gt;1 2021-08-18T03:34:25.063Z - sshd 1001395395 - [login.connect@6876 subject="root" object="" result="failure" ip="172.16.23.2" reason="AUTH_FAIL_KBDINT"]  &lt;110&gt;1 2021-08-18T03:34:30617Z - sshd 1001395395 - [login.connect@6876 subject="root" object="" result="failure" ip="172.16.23.2" reason="AUTH_FAIL_NONE"]  &lt;110&gt;1 2021-08-18T03:34:32.094Z - sshd 1001395395 - [login.connect@6876 subject="root" object="" result="failure" ip="172.16.23.2" reason="AUTH_FAIL_PASSWD"]  &lt;109&gt;1 2021-08-12T16:39:54.931Z - Hostd 1001392629 - [login.connect@6876 subject="aadmin" `object="" `ip=172.16.1.150" reason="Invalid Login" opID="esxui-d8aa- 6e09" result="failure"]  &lt;110&gt;1 2021-08-18T03:37:02.469Z - Hostd 1001392490 - [login.connect@6876 subject="root" object="" ip="127.0.0.1" opID="esxcli-2d-c125" result="success"]</pre>
<p>All use of the identification and authentication mechanism</p>	<pre>&lt;110&gt;1 2021-08-18T03:34:32.111Z - sshd 1001395395 - [login.disconnect@6876 subject="root" object="" result="success" ip="172.16.23.2"]</pre>
<p>Invalid parameter to hypercall detected</p>	<pre>&lt;109&gt;1 2022-07-20T18:51:14.615Z - vmx 2412639 - [vm.hypercall.access@6876 subject="" object="/vmfs/volumes/6148ce85-f29c9ebe-ad18- 78ac4428ad30/Ubuntu Test 1/Ubuntu Test 1.vmx" type="Backdoor" value="2" reason="ignored due to inappropriate mode" result="failure"]</pre>
<p>Hypercall interface invoked when documented preconditions are not met</p>	<pre>&lt;109&gt;1 2022-07-20T18:58:05.002Z - vmx 2412639 - [vm.hypercall.access@6876 subject="" object="/vmfs/volumes/6148ce85-f29c9ebe-ad18- 78ac4428ad30/Ubuntu Test 1/Ubuntu Test 1.vmx" type="Backdoor" value="8" reason="hypercall is disabled" name="copyDisable" result="failure"]</pre>
<p>Connection/disconnection of removable media or device to/from a VM</p>	<pre>&lt;110&gt;1 2022-07-22T18:59:02.789Z - vmx 2431848 - [vm.usb.connect@6876 subject="" object="/vmfs/volumes/6148ce85-f29c9ebe-ad18- 78ac4428ad30/efi_test_vm/niaptest.vmx" vendorID="0e0f" productID="0003" deviceLabel="usb_xhci:4" result="success"]  &lt;110&gt;1 2022-07-22T18:59:02.786Z - vmx 2431848 - [vm.usb.disconnect@6876 subject="" object="/vmfs/volumes/6148ce85-f29c9ebe-ad18- 78ac4428ad30/efi_test_vm/niaptest.vmx" vendorID="0000" productID="0000" deviceLabel="usb_xhci:4" result="success"]</pre>
<p>Ejection/insertion of removable media or device</p>	<pre>&lt;110&gt;1 2022-07-22T22:35:24.519Z - Hostd 2099692 - [vm.storage.edit@6876 subject="root"]</pre>

<p>from/to an already connected VM</p>	<pre>object="/vmfs/volumes/6148ce85-f29c9ebe-ad18-78ac4428ad30/Kali Test 1/Kali Test 1.vmx" opID="esxui-895-6e97" ip="172.16.1.50" oldPath="[datastore1\\] Kali Test 1/_deviceImage-0.iso" path="" result="success"]  &lt;110&gt;1 2022-07-22T22:35:24.519Z - Hostd 2099692 - [vm.storage.edit@6876 subject="root" object="/vmfs/volumes/6148ce85-f29c9ebe-ad18-78ac4428ad30/Kali Test 1/Kali Test 1.vmx" opID="esxui-895-6e97" ip="172.16.1.50" path="" status="disconnected" result="success"]  &lt;110&gt;1 2022-07-22T22:35:24.593Z - Hostd 2099692 - [vm.change@6876 subject="root" object="/vmfs/volumes/6148ce85-f29c9ebe-ad18-78ac4428ad30/Kali Test 1/Kali Test 1.vmx" ip="172.16.1.50" operation="reconfigure" opID="esxui-895-6e97" result="success"]\n'</pre>
<p>Initiation of update</p>	<pre>&lt;19&gt;1 2021-2021-08-18T16:20:44.161Z - esxupdate 1001402274 - [system.update.start@6876 subject="root" object="" result="success" reason="" vib="add: {VMware_bootbank_vmware-esx-esxcli-nvme-plugin_1.2.0.23-2.50.8294258} remove: {VMware_bootbank_vmware-esx-esxcli-nvme-plugin_1.2.0.43-1vmw.703.0.0.18256574}"]</pre>
<p>Failure of update signature verification</p>	<pre>&lt;19&gt;1 2022-07-25T13:16:11.513Z - esxupdate 2455973 - [system.update.end@6876 subject="root" object="" result="failure" reason="CRC check failed 0x72c7b4e5 != 0x9681a9cf" vib="add: {VMware_bootbank_vmware-esx-esxcli-nvme-plugin_1.2.0.32-2.50.8294253} remove: {VMware_bootbank_vmware-esx-esxcli-nvme-plugin_1.2.0.44-1vmw.703.0.20.19193900}"]</pre>
<p>Initiation of trusted channel</p>	<pre>&lt;110&gt;1 2022-07-22T14:19:16.075Z - vmsyslogd 2424830 - [syslog.net.connect@6876 subject="" object="tlss.test.domain:1515" result="success"]  &lt;110&gt;1 2022-07-22T14:19:16.076Z - vmsyslogd 2424830 - [syslog.net.link@6876 subject="" object="tlss.test.domain:1515" result="success" reason="link up"]  &lt;110&gt;1 2022-07-22T14:08:20.238Z - Hostd 2099692 - [login.connect@6876 subject="root" object="" ip="172.16.1.50" opID="esxui-62e4-5e7b" result="success"]  &lt;110&gt;1 2022-07-22T14:08:20.564Z - Rhttpproxy 2099235 - [https.connect@6876 subject="" object="" ip="172.16.1.50" result="success"]</pre>
<p>Termination of trusted channel</p>	<pre>&lt;110&gt;1 2022-07-22T17:47:14.908Z - vmsyslogd 2424830 - [syslog.net.disconnect@6876 subject="" object="tlss.test.domain:1515" result="success"]</pre>



	<pre>&lt;110&gt;1 2022-07-22T17:47:14.909Z - vmsyslogd 2424830 - [syslog.net.link@6876 subject="" object="tlss.test.domain:1515" result="failure" reason="link down"]  &lt;110&gt;1 2022-07-22T17:49:43.755Z - Hostd 2099692 - [login.disconnect@6876 subject="root" object="" ip="172.16.1.50" reason="Session closed" opID="esxui-c90f- 6020" result="success"]</pre>
Failure of trusted channel functions	<pre>&lt;110&gt;1 2022-07-22T18:46:44.633z - vmsyslogd 2424830 - [syslog.net.connect@6876 subject="" object="tlss.test.domain:1515" result="failure" reason="[SSL: CERTIFICATE_VERIFY_FAILED] certificate verify failed: Hostname mismatch, certificate is not valid for 'tlss.test.domain'. (_ssl.c:1125)" subjectDN="Unknown" subjectAltName="Unknown" referenceID="tlss.test.domain"  &lt;109&gt;2022-06-16T18:25:30.428Z vmware-esxi-1 Rhttpproxy[2099235]: [https.connect@6876 subject="" object="" ip="172.16.0.25" reason="SSL Handshake failed" result="failure"]  &lt;110&gt;1 2022-07-24T15:15:30.846Z - vmsyslogd 2424830 - [audit.net.failure@6876 subject="" object="tlss.test.domain:1515" result="failure" reason="tlss.test.domain:1515 was down"]</pre>
Failure to establish a HTTPS session.	<pre>&lt;109&gt;1 2021-08-18T16:45:20.137Z - Rhttpproxy 1001391993 - [https.connect@6876 subject="" object="" ip="172.16.13.105" reason="SSL Handshake failed" result="failure"]</pre>
Establishment/Termination of an HTTPS session	<pre>&lt;110&gt;1 2021-08-10T07:01:06.985Z - Rhttpproxy 1001392101 - [https.connect@6876 subject="" object="" ip="172.16.1.50" result="success"]  &lt;110&gt;1 2021-08-10T07:01:55.811Z - Rhttpproxy 1001392101 - [https.disconnect@6876 subject="" object="" ip="172.16.1.50" result="success"]</pre>
Failure to establish a TLS session	<pre>&lt;110&gt;1 2022-07-24T15:15:25.833Z - vmsyslogd 2424830 - [syslog.net.connect@6876 subject="" object="tlss.test.domain:1515" result="failure" subjectDN="Unknown" subjectAltName="Unknown" referenceID="tlss.test.domain"]</pre>
Failure to verify presented TLS identifier	<pre>&lt;110&gt;2022-06-07T18:38:33.725Z vmware-esxi-1 vmsyslogd[2097858]: [syslog.net.connect@6876 subject="" object="tlss.test.domain:1515" result="failure" reason="[SSL: CERTIFICATE_VERIFY_FAILED] certificate verify failed: Hostname mismatch, certificate is not valid for 'tlss.test.domain'. (_ssl.c:1125)" subjectDN="CN=wrong.test.domain" subjectAltName="None" referenceID="tlss.test.domain"]</pre>

<p>Establishment/Termination of a TLS session</p>	<pre>&lt;110&gt;1 2022-07-22T14:19:16.075Z - vmsyslogd 2424830 - [syslog.net.connect@6876 subject="" object="tlss.test.domain:1515" result="success"]  &lt;110&gt;1 2022-07-22T14:19:16.076Z - vmsyslogd 2424830 - [syslog.net.link@6876 subject="" object="tlss.test.domain:1515" result="success" reason="link up"]  &lt;110&gt;1 2022-07-22T14:08:20.238Z - Hostd 2099692 - [login.connect@6876 subject="root" object="" ip="172.16.1.50" opID="esxui-62e4-5e7b" result="success"]  &lt;110&gt;1 2022-07-22T14:08:20.564Z - Rhttpproxy 2099235 - [https.connect@6876 subject="" object="" ip="172.16.1.50" result="success"]</pre>
---	---

Table 6: Sample Audit Records for Other Security-Relevant Events