VMware ESXi 8.0 Update 3e

NIAP Common Criteria Guidance Supplement

Document version 1.3

Table of contents

1 Introduction

This document describes the operational guidance and preparative procedures for VMware ESXi™ 8.0 Update 3e. 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.

1.1 Document References

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 8.0 Update 3 PDF)
- VMware ESXi Upgrade (ESXi 8.0 Update 3 PDF)
- VMware vSphere Security (ESXi 8.0 Update 3 PDF)
- vSphere Single Host Management – VMware Host Client (ESXi 8.0 Update 3 PDF)
- vSphere Virtual Machine Administration (ESXi 8.0 Update 3 PDF)

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

- vSphere Management SDK, version 8.0 (ESXI 8.0 Update 3 PDF)
- vSphere 8.0U3 Web Services API Reference (describes the VIM API)
- ESXCLI:
    - Getting Started (ESXi 8.0 PDF)
    - Concepts and Examples (ESXi 8.0 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://knowledge.broadcom.com/external/article?legacyId=<KB-ID >. Modifying the url with the "legacyId" field set to the KB ID is the easiest way to find a targeted KB article. e.g. https://knowledge.broadcom.com/external/article?legacyId=86447

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 6430. Support for other CPUs is implemented by ESXi but this evaluation covers only the Intel Xeon Gold 6430.

- 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 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.
- VMware PowerCLI Software
- USB Passthrough

- VM Encryption
- VM Virtual Disk Sharing
- 3rd Party VIBs(distributed independently of VMware ESXi)

1.2 Evaluated Configuration And TOE Overview

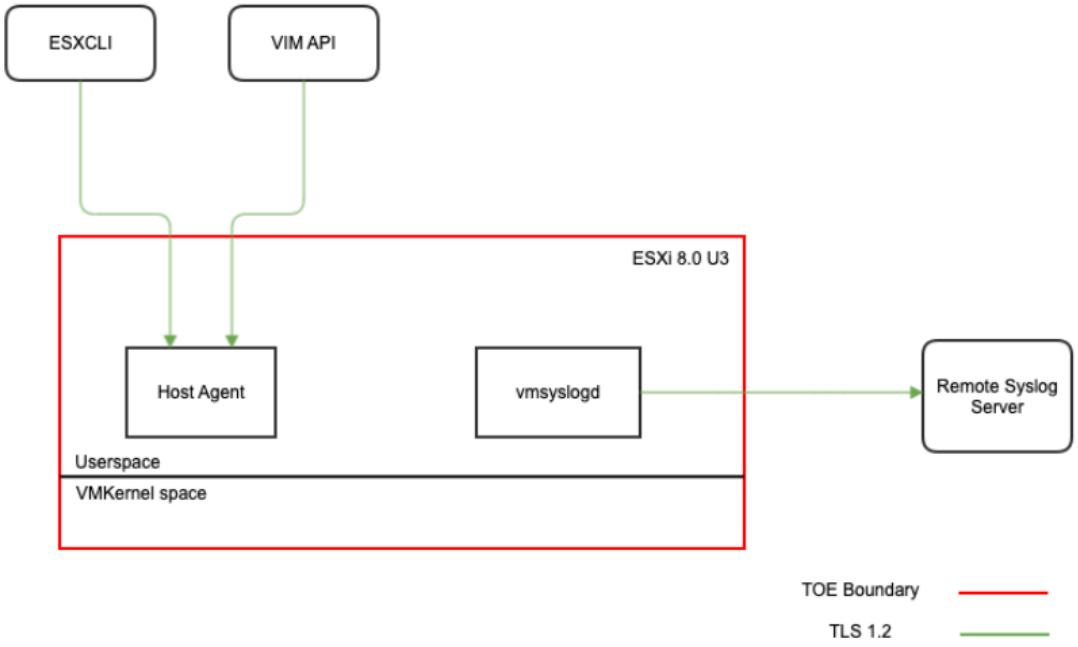

Figure 1: The TOE Evaluated Configuration

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 exclusively uses VIM API to perform actions.
- ESXCLI: Remote esx-cli 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.

The TOE consists of the ESXi hypervisor. For the TOE, the hypervisor is installed on top of a physical system (Dell PowerEdge R660) composed of CPUs (Intel Xeon Gold 6430), 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.

2 Installation Guidance 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. This includes any user interface which exclusively leverages the VIM api surface. Host Client UI is the Broadcom shipped UI which is served by ESXi which meets this standard.
    - The administrator regularly installs software updates per VMware guidance.
    - The administrator follows guidance in Section 2 to properly configure ESXi security policies during 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 Installing the TOE

The VMware ESXi Installation and Setup document provides general installation instructions.

2.2.1 Configure Firmware

Before installing the ESXi software, configure the system's firmware to support a secure hypervisor. On the TOE system (a Dell PowerEdge R660), 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.

2.2.2 Obtain Software

The software selected for the NIAP-evaluated configuration is ESXi 8.0 Update 3e. 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 3 may have been superseded by a newer version of ESXi 8.0U3e, which according to software update policy is also acceptable.

ESXi 8.0 Update 3e may be applied as a new installation or as an update to an existing ESXi 8.0 installation. The software for installation or update may be obtained from Broadcom Support 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. An active ESXi related license is required in order to download any version of ESXi 8.0.

Using the portal, if the software is to be applied as a new installation or an update from 8.0u2:

1. Select VMware Cloud Foundation from the Product Family dropdown list in the upper right part of the window (just to the left of the Profile dropdown with your login name).
2. Select My Downloads on the left navigation panel.
3. On the My Downloads - VMware Cloud Foundation panel select VMware vSphere. This is most easily found by entering "VMware vSphere" in the search textbox.
4. On the VMware vSphere panel select the appropriate entry for your license. Your license group will be VMware vSphere - Standard.
5. From the displayed list of versions select 8.0.
6. From the resulting Primary Downloads list find the VMware vSphere Hypervisor (ESXi) entry and press View Group for that entry.
7. From the version dropdown in the upper right of the panel select 8.0u3e. (Be sure this is selected, since a newer version may be selected by default.)

Please note that sub versions of ESXi 8.0 can also be selected from the same path supported above in the Broadcom Support Portal.

If the software is to be applied as an update to an existing installation, see the following Broadcom Downloads and Patch Support Article.

2.2.3 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 8.0 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 8.0 installation, follow guidance in Section 4.6.1. To summarize:

1. Be running some version of ESXi 8.0.
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 4.6.

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

2.2.4 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.

2.2.5 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.

2.2.5.1 Enablement of Audit Logging

ESXi does not come configured with audit logging enabled by default. In order for the ESXI to be properly configured, audit logging must be enabled. Please see Section 2.3.2 for logging enablement.

2.2.5.2 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
```

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

```
esxcli network firewall ruleset set -e false -r faultTolerance
esxcli network firewall ruleset set --allowed-all=false --ruleset-id=CIMSLP
esxcli network firewall ruleset set --allowed-all=false --ruleset-id=DVSSync
esxcli network firewall ruleset set --allowed-all=false --ruleset-id=iofiltervp
esxcli network firewall ruleset set --allowed-all=false --ruleset-id=vMotion
esxcli network firewall ruleset set --allowed-all=false --ruleset-id=NFC
```

NOTE: this configuration will disable Distributed Virtual Switches, Fault Tolerance, SLP, vMotion, storage vMotion, some external backup solutions, and Virtual Machine Encryption. Customers should evaluate their security exposure and functionality needs when choosing to disable features. See Section 1.2 for further information about why specific features are disabled.

2.2.5.4 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 ESXi server, 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.
- Execute the following esxcli commands for TLS configuration of inbound and outbound connections.
  - TLS Server configuration:
    - `esxcli system tls server set -p MANUAL`
    - `esxcli system tls server set -v "tls1.2"`
    - `esxcli system tls server set -c 'ECDHE+AESGCM:!ECDSA'`
    - `esxcli system tls server set -s 'ECDHE-RSA-AES256-GCM-SHA384:ECDHE-RSA-AES128-GCM-SHA256'`
    - `esxcli system tls server set -g 'prime256v1:secp384r1:secp521r1'`
  - TLS Client Configuration:
    - `esxcli system tls client set -p MANUAL`
    - `esxcli system tls client set -v "tls1.2"`
    - `esxcli system tls client set -c 'ECDHE+AESGCM:!AESCCM:!AESCCM8'`
    - `esxcli system tls client set -s 'ECDHE-ECDSA-AES256-GCM-SHA384:ECDHE-RSA-AES256-GCM-SHA384:ECDHE-ECDSA-AES128-GCM-SHA256:ECDHE-RSA-AES128-GCM-SHA256'`
    - `esxcli system tls client set -g 'prime256v1:secp384r1:secp521r1'`
- Reboot ESXi in order to pick up the TLS profile changes.

Note: Additional information and help can be found in the following documentation, Change the TLS Profile of an ESXi Host Using the CLI.

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.

2.2.6 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.

2.2.7 Configure Envoy Proxy For Operations

The envoy proxy in ESXi 8.0U3e requires additional configuration before the TOE can be considered configured. The TOE operator must enable explicit internal addresses in Envoy. To do this, the operator should execute the following steps:

1. SSH into the TOE.
2. Edit `/etc/vmware/envoy/config.yaml` to add `'envoy.reloadable_features.explicit_internal_address_config: true'` in `'layered_runtime->layers->static_layer'` section aligned to `'re2:'`

   Here is an example:

```
layered_runtime:
  layers:
    - name: static_layer_0
      static_layer:
        re2:
          max_program_size:
            warn_level: 256
            error_level: 256
        envoy.reloadable_features.explicit_internal_address_config: true
```

3. Restart envoy

```
$ /etc/init.d/envoy restart
```

4. Verify the following log in the file `/var/run/log/envoy.log:`

   a. `"2025-03-10T23:21:20.077Z In(166) envoy[526768]: envoy.reloadable_features.explicit_internal_address_config: true"`

2.3 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.

Table 1: Supporting Environmental Components

Components	Description
Linux system for management	System from which to make VIM API calls or ESXCLI calls to configure and manage ESXi. Any Linux distribution released after around 2014 should be sufficient. *NOTE: In many deployments, vCenter Server is used to make VIM API calls.*
Remote Syslog Server	A server which implements RFC 3164 "The BSD Syslog Protocol" and RFC 5425 "TLS Transport Mapping for Syslog." *NOTE: A remote syslog server is optional. However, usage of a remote syslog server is included in the NIAP-validated configuration.*

2.3.1 Install ESXCLI for Remote Management

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

https://developer.broadcom.com/tools/esxcli/8.0

Note: A Broadcom Support account is required for the download. There is no charge for signing up for a Broadcom Support and no purchase is required to obtain the ESXCLI binaries.

This guide covers using the ESXCLI standalone download. To install, download .tgz for Linux(e.g. esxcli-8.0.0-22179150.tgz) onto a system separate from ESXi that will be used for remote administration. Please follow the instructions provided in the above developer link for installation.

Note the generalized instructions are as follows:

```
$ pip install esxcli-*.tgz
```

2.3.2 Configure Auditing

Please ensure that your audit server certificates have been uploaded to a datastore in your ESXI server as the esxcli assumes you are referencing a certfile within a datastore.

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 <host> system security certificatestore add -f cacert.pem
esxcli --server <host> network firewall ruleset set --ruleset-id=syslog --
enabled=true
esxcli --server <host> 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 --server <host> system security certificatestore add --file=<local-file>
esxcli --server <host> system security certificatestore list
esxcli --server <host> system security certificatestore remove --issuer=<issuer> --
serial=<serial>
```

For more information about the ESXCLI system commands, see the ESXCLI reference guide. Additional guides and information can be found in the ESXi 8.0 ESXCLI developer tool reference page under the "development guide" subsection.

2.4 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.

2.5 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.

2.6 Ongoing Tracking for Security Issues and Mitigations

ESXi 8.0 Update 3e 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.

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)

VMware by Broadcom maintains several repos for leveraging the VIM API on gitlab. Supported languages are as follows:

- Golang
- Python
- Java

The following links are provided as a resource for operators to familiarize themselves with the vsphere SDK support:

- Overview of vsphere APIs and SDKs
- Getting Started with vShere APIs and SDKs

Note: the provided samples are leveraging the python SDK.

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.

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.UpdateValues(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 which a specific release supports is through the VIM API exposed by that release. This includes a description of the provided advanced settings.

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

Table 2: Advanced Options

Setting Names	Default	Description
Config.HostAgent.vmacore.soap.sessionTimeout	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.
Mem.MemEagerZero	0 (disabled)	Enable zeroing userworld and guest memory pages (including VMM) after VM exit.
Security.AccountLockFailures	5	Maximum number of failed login attempts before a user's account is locked. A value of zero disables account locking.
Security.AccountUnlockTime	900 (15 minutes)	Number of seconds that a user is locked out.
Security.PasswordHistory	0	Number of passwords to remember for each user. This prevents duplicate or similar passwords.
Security.PasswordMaxDays	99999	Maximum number of days between password changes.
Security.PasswordQualityControl	retry=3 min=disabled,disabled,disabled ,7,7	Password quality configuration.
UserVars.HostClientSessionTimeout	900 (15 minutes)	Idle time in seconds before Host Client is automatically logged out. A value of zero disables the timeout.

UserVars.HostClientWelcomeMessage	(empty)	Displayed in Host Client following login, as a “hint”.

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

To enable local auditing using ESXCLI, execute the following command:

`esxcli system auditrecords local enable`.

For more information on configuring local audit using ESXCLI, see Configuring and Managing the Audit System and Audit Data in ESXCLI 8.0 U3e 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 done via 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 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

In general, the audit records can be viewed using 3 separate methods.

1. Locally on the ESXI leveraging the `/bin/viewAudit`
2. Remotely via configuring the remote audit server(see Section 4.1.2).

3. Remotely via the VIM API by leveraging the FetchAuditRecords API. See the VIM API for DiagnosticManagers subsection starting with FetchApiRecords.

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 1.2 protocol. ESXi currently implements 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 1.2 sessions are generated using algorithms and key sizes that depend on the negotiated TLS cipher suite.

4.2.2 Cryptographic Key Establishment

Configuration of TLS cryptographic key establishment is governed by choice of TLS 1.2 cipher suites, which select one of the ECC-based key agreements using ephemeral Elliptic Curve Diffie Hellman (ECDHE), as specified in SP 800-56Arev3. The supported TLS 1.2 cipher suites are configured as part of initial setup as described in section 2.3.5. The administrator has no direct control over the behavior of this function.

4.2.3 Cryptographic Key Destruction

The following command 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 ESXCLI, execute the command:

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

4.2.4 Cryptographic Operation

ESXi defaults to using FIPS 140 approved algorithms for all operations needing cryptography for security purposes. This includes remote access to management interfaces (for example, TLS 1.2), key generation, signature verification, and other use cases. Any parameters that would disable FIPS checking must not be changed. The NIAP evaluated functionalities are enabled by default.

4.2.5 Random Bit Generation

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

4.2.7 HTTPS

There are no configurable parameters relating to usage of HTTPS. The NIAP evaluated 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 1.2 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. Broadcom supports altering these settings only as directed by Global Support Services (GSS).

4.2.9 TLS Protocol Versions

By default, ESXi allows TLS v1.2 and TLS 1.3. TLS v1.3 is not in scope for the ESXI NIAP configuration for 8.0U3e. Section 2.3.5 disables TLS v1.3 along with unsupported TLS ciphers. TLS 1.3, TLS 1.1, TLS 1.0, and SSL 3.0 are not allowed and will not be supported by this guidance doc.

For information on setting the protocol list using ESXCLI, see VMware @ Broadcom's guide to configuring TLS on ESXi 8.0U3.

4.2.10 TLS Cipher Suites

The default ESXi cipher suite permits a selection of high security protocols. Ephemeral key agreement, ECDHE, is used 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 2.3.5 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_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256
- TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384
- TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256

- TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384

TLS server:

- TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256,
- TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384

4.2.11 ECC Choices in TLS

ESXi provides a selection of strong prime curves, specifically `"secp256r1:secp384r1:secp521r1"`.

4.3 Protection of User (VM) Data (FDP)

4.3.1 Virtual Networking

The configuration for virtual machine networking can be configured through 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).

To add a network adapter to a Virtual Switch, login to the host client as an administrator and perform the following workflow:

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. Click the **Virtual Hardware** tab and click **Add network adapter**.
4. In the network connection panel, select either a network with a specific label or a legacy network.
5. To configure the virtual Network Interface Card (NIC) to connect when the virtual machine is powered on, select **Connect at power on**.
6. Click **Save**.

To change the configuration of the Virtual Network Adaptor in the VMware Host Client:

- **Virtual Machine > Configuration > Modify device settings** for editing the MAC address and network.
- **Virtual Machine > Interaction > Device connection** for changing **Connect** and **Connect at power on**.
- **Network > Assign network**

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. Click the **Virtual Hardware** tab and select the appropriate Network Adapter (NIC) from the hardware list.
4. To connect the virtual NIC when the virtual machine is powered on, select **Connect at power on**.
5. Select the adapter type from the **Adapter Type** drop-down menu.
6. Select an option for MAC address configuration.

Option	Description
Automatic	vSphere assigns a MAC address automatically.
Manual	Enter the MAC address to use.

7. Click **Save**.

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.

4.3.3 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
```

4.3.4 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.

4.3.5 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.

4.3.6 Hardware-based VM Isolation

The only supported virtualization mode in ESXi 8.0U3e 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 5th login failure, set this value to 5.

The `AccountUnlockTime` option describes a time interval(in seconds) 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`

The `Security.PasswordQualityControl` option defines the complexity requirements for ESXi user passwords. It allows you to specify the minimum length, required character classes (lowercase, uppercase, numbers, special characters), and whether passphrases are allowed.

The `Security.PasswordHistory` option determines how many previous passwords the system remembers for each user. By enabling this and setting it to a value greater than 0, you can prevent users from reusing old passwords.

The `Security.PasswordMaxDays` option enforces password expiration by setting the maximum number of days a password can be used before the user is required to change it.

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 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 4.1.3 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.

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
`ListCACertificateRevocationLists`	Returns currently stored CRLs for CA roots used by this host.
`ListCACertificates`	Returns currently stored CA roots used by this host.
`ReplaceCACertificatesAndCRLs`	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. For more detailed information on how this may be achieved, please see Securing Virtual Machines with VLANs. 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	Initiation of Update	See Section 4.6.1.
2	Configure password policy	See Section 4.4.2.

3	Create, configure, and delete VMs	**For the VIM API**, Please follow the examples below and see:
		• vim.Folder.CreateVM_Task
		• vim.VirtualMachine.ReconfigVM_Task
		• vim.ManagedEntity.Destroy_Task
		
		create a VM ConfigSpec(required for creation and reconfiguration):
		
		The VM ConfigSpec is used both for initial configuration and reconfiguration of virtual machines. Please see the below example on how to create a VM ConfigSpec in PyVMomi.
		
		`config = vim.vm.ConfigSpec()`
		`config.annotation = <annotation>`
		`config.memoryMB = <desired memory amount>`
		`config.guestId = <desired guest id>`
		`config.name = <vm name>`
		`config.numCPUs = <desired number of CPUs>`
		`files = vim.vm.FileInfo()`
		`files.vmPathName = <path desired including datastore to the .vmx and vm configuration files>`
		`config.files = files`
		
		Create VM(VIM):
		
		1. Obtain a reference to the desired Datacenter's vmFolder.
		2. Call vm_folder.CreateVM(<constructed ConfigSpec, <target Resource Pool>, <desired host>)
		
		Reconfigure VM(VIM):
		
		1. Obtain a reference to the target VM.
		2. Create a VM ConfigSpec containing the desired config changes.
		3. Call `vm_ref.ReconfigVM_task(config_spec)`
		
		Delete VM(VIM):
		
		1. Obtain a reference to the target VM.
		2. Call `vm.destroy()` on the vm.
		
		Please note, vm.destroy does not perform a graceful shutdown of the VM. If the user is concerned about data loss, or communication disruption then a graceful shutdown of the VM should be completed before vm.destroy is called.
		
		Also see Managed Object – VirtualMachine(vim.VirtualMachine)
		
		For Host Client,
		Please follow the procedures laid out below.
		
		Create VM:
		1. Right-click Host in the VMware Host Client inventory and select Create/Register VM.
		2. The New Virtual Machine wizard opens.
		3. Select Create a new virtual machine and click Next.
		4. On the Select a name and guest OS page, provide a unique name for the virtual machine and configure the guest operating system.
		5. Click Next.
		6. On the Select storage page, select the storage type for the virtual machine and a datastore where to store the virtual machine files.
		7. On the Customize settings page, configure the virtual machine hardware and options and click Next.
		8. For information about virtual machine options and virtual disk configuration, including instructions for adding different types of devices, see vSphere Virtual Machine Administration.
		9. On the Ready to complete page, review the details and click Finish.

		Reconfigure VM: 1. Right-click a virtual machine in the inventory and select Edit Settings. 2. Navigate the appropriate tab for the configuration in question(e.g. for memory you would select the "Virtual Hardware" tab 3. Make the reconfiguration modifications being sure to follow any onscreen instructions. 4. Click **Ok**. **Delete VM:** 1. Click Virtual Machines in the VMware Host Client inventory. 2. Select one or multiple check boxes next to the virtual machines that you want to remove and select Actions > Delete. 3. The Delete VMs dialog box opens. 4. Click Delete. For more information on the Host Client use case, see Virtual Machine Management with the VMware Host Client.
4	Set default initial VM configurations	**For VIM APIs**, the initial VM configurations are always "empty". Overriding this "empty" configuration can done through the `config` parameter to `CreateVM_Task`. Please see Item #3 of this table for VIM configuration guidance. **For Host Client**, override the default "empty" configuration can also be done through the Create VM wizard in the ESXi Host Client. This process can be started via the process described in Item #3 of this table within the Host client's "create vm" section. For more information on the Host Client use case, See Create a Virtual Machine in the VMware Host Client.
5	Configure virtual networks	See Section 4.3.1.
6	Configure and manage audit system and audit data	See Section 4.1.
7	Configure VM access to physical devices	See Section 4.3.2.
8	Configure inter-VM data sharing	See "Configure virtual networks" in this table (item 5).
9	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.
10	Configure removable media policy	See Section 4.6.2.
11	Configure cryptographic functionality	See Section 4.2 and subsections.
12	Change default authorization factors	See Section 4.4.
13	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.
14	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.
15	Configure remote connection inactivity timeout	See Section 4.7.1.
16	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 4.1.3.

19	Configure name/address of network time server	For the VIM API, supply a list of time servers to `UpdateDateTimeConfig` using `HostDateTimeConfig`'s `HostNtpConfig` or `HostPtpConfig` object.
		
		Sample code for this would look like the following
		
		NTP example:
		`< Obtain reference to Esxi Host target>`
		`time_config =hostRef.configManager.queryHostDateTimeSystem()`
		`ntpConfig = vim.host.ntpConfig()`
		`ntpConfig.server=[<list of string based ips>]`
		`new_time_config.ntpConfig=ntpConfig`
		`hostRef.configManager.UpdateDateTimeConfig(new_time_config)`
		
		For Host Client,
		
		1. Click **Manage** in the VMware Host Client inventory.
		2. On the **System** tab, click Time & date.
		3. Set the **time** and **date** for the host.
		
		The user will be presented with three options from here.
		
		1. Manually configure the date and time on this host
		a. Click Edit NTP Settings.
		b. The Edit NTP Settings dialog box will appear.
		c. Set the time and date for the host manually.
		d. Click Save.
		2. Use Network Time Protocol (Enable NTP client)
		a. Click Edit NTP Settings.
		b. The Edit NTP Settings dialog box will appear.
		c. Select the Use Network Time Protocol radio button.
		d. In the NTP Servers text box, enter the IP addresses or host names of the NTP servers that you want to use.
		e. From the NTP Service Startup Policy drop-down menu, select an option for starting and stopping the NTP service on the host.
		i. **Start and stop with port usage.** Starts or stops the NTP service when the NTP client port is activated or deactivated for access in the security profile of the host.
		ii. **Start and stop with host**. Starts and stops the NTP service when the host powers on and shuts down.
		iii. **Start and stop manually.** Enables manual starting and stopping of the NTP service. If you select the Start and stop manually policy, the status of the NTP service changes only when you use the UI controls.
		f. Click Save.
		3. Use Precision Time Protocol (Enable PTP client)
		a. Click Edit PTP Settings.
		b. Select the Enable check box.
		c. From the Network interface drop-down menu, select a network interface.
		d. The IPv4 and Subnet mask will appear.
		e. Click Save.
		
		For more information, see Edit the Time Configuration of an ESXi Host in the VMware Host Client.
		
		Important Notes:
		• When using the 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 important to manually refresh the **Time & date** panel after making changes to see the updated settings in the summary (the summary is not automatically updated).

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	For the VIM API, see vim.VirtualMachine.PowerOn_Task. For example, to invoke this via the PYVMOMI api library the user would invoke the following code. 1. Obtain a reference to the target VM. 2. Call `vm.PowerOn()` For Host Client, 1. In the VMware Host Client inventory, click **Virtual Machines**. 2. Right-click a virtual machine and select the "Power On" power operation. For more information, see Power States of a Virtual Machine in the VMware Host Client.
23	Stop/halt a VM	For the VIM API, see `vim.VirtualMachine.PowerOffVM_Task`. For example, to invoke this via the PYVMOMI api library the user would invoke the following code. 1. Obtain a reference to the target VM. 2. Call `vm.PowerOff()` For Host Client, 1. In the VMware Host Client inventory, click **Virtual Machines**. 2. Right-click a virtual machine and select the "Power Off" power operation. For more information, see Power States of a Virtual Machine in the VMware Host Client.

24	Checkpoint a VM	**For the VIM API,** VMware uses the term "Snapshot". see `vim.VirtualMachine.CreateSnapshot_Task`. For example, to invoke this via the PYVMOMI api library the user would invoke the following code. 1. Obtain a reference to the target VM. 2. Call `vm.CreateSnapshot(self, name: str, description: Optional[str], memory: bool, quiesce: bool) -> Task` with the desired correct inputs. **For Host Client,** 1. In the VMware Host Client inventory, click **Virtual Machines**. 2. Right-click a virtual machine from the list and select Snapshots > Take snapshot. 3. Enter a name for the snapshot. 4. (Optional) Type a description for the snapshot. 5. (Optional) Select the Snapshot the virtual machine's memory check box to capture the memory of the virtual machine. 6. (Optional) Deselect Snapshot the virtual machine's memory and select Quiesce guest file system (needs VMware Tools installed) check box to pause running processes on the guest operating system so that file system contents are in a known consistent state when you take the snapshot. 7. Quiesce the virtual machine files only when the virtual machine is powered on and you do not want to capture the virtual machine's memory. 8. Click Take snapshot For more information on snapshots and their nuances, see Using Snapshots to Manage Virtual Machines.
25	Suspend a VM	**For the VIM API,** See `vim.VirtualMachine.SuspendVM_Task`. For example, to invoke this via the PYVMOMI api library the user would invoke the following code. 1. Obtain a reference to the target VM. 2. Call `vm.Suspend()` **For Host Client,** 1. In the VMware Host Client inventory, click **Virtual Machines**. 2. Right-click a virtual machine and select the "Suspend" power operation. For Host For more information, please see Power States of a Virtual Machine in the VMware Host Client
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 digital signature verification. The public keys used for update verification are loaded automatically during initial installation of ESXi. If necessary, Updates to the public keys are made by the standard upgrade process without any additional configuration from administrators.

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.

ESXCLI may be used to list all installed VIBs and their current version, or the current image profile, using the following commands. The technical steps for the core part of ESXi Upgrades are as follows:

3. `esxcli software vib list`
4. `esxcli software sources profile list`
5. See Section 3 of Procedures in Upgrade or Update a Host with Image Profiles
    1. Broadcom Support Depot:
       `esxcli software profile update --depot=<depot_location> --profile=<profile_name>`
    2. Local Zip file copied onto a Datastore:
       `esxcli --server=<server_name> software profile update --depot=file:///<path_to_profile_ZIP_file>/<profile_ZIP_file> --profile=<profile_name>`
    3. For other support options please see the above documentation.
6. Reboot the ESXi host immediately if in the ESXCLI output you see `Reboot Required: true`.
7. Verify the VIBs are installed on your ESXi Host.
    1. `esxcli --server=<server_name> software vib list`

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 processes described above for listing VIBs.

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.
- 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 4.1.3.

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.

4.9 VMM Isolation from VM (VIV)

4.9.1 Configuring VM Hypercall isolation

Each individual backdoor command can be disabled or enabled using the VM configuration setting:

```
config.name.disable = "true" # to disable
```

or:

```
config.name.disable = "false" # to enable
```

The config.name.disable setting for each command is defined in the configuration column of the Commands table. This setting must be applied to
the configuration file before the VM is powered on (or resumed). Note that disabling a command disables all its subcommands.

To disable the entire backdoor facility for a VM, set in the VM's configuration:

```
monitor_control.restrict_backdoor = "true"
```

4.10 Removable Devices and Media

4.10.1 USB devices

Removable USB devices (and any associated media) are covered in Section 4.3.3.

4.10.2 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.

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 the PP-relevant 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 is locked due to too many failed login attempts.

Parameters:

- The `subject` is the name of the user whose account was locked.
- The `object` is “account”
- The `ip` is the network address of the originator of the operation.
- The `result` is "success" since the account was successfully locked.

A.2.2 audit.storage.recycle

This event is generated when the audit record storage FIFO returns 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.2.3 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 `directory` is the location where the rolling log archives will be stored.
- The `capacity` is the amount of storage the audit directory will consume in megabytes before initiating archive rollover.
- The `reason`, if present, provides additional details about the event.
- The `result` is "success".

A.2.4 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 `reason` is “administrative action”.
- The `result` is "success".’

A.2.5 cert.castore.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 "cert".
- The `result` is "success" or "failure".
- The `reason`, if present, provides additional details about the event.
- The `ip`, if present, is the network address of the originator of the operation.
- The `subjectDN` is the subject distinguished name of the CA certificate.
- The `opID`, if present, is the operation ID.

A.2.6 cert.castore.remove

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

Parameters:

- The `subject` is the name of the user who requested the operation.
- The `object` is "cert".
- The `result` is "success" or "failure".
- The `reason`, if present, provides additional details about the event.
- The `ip`, if present, is the network address of the originator of the operation.
- The `subjectDN` is the subject distinguished name of the CA certificate.

- The `opID`, if present, is the operation ID.

A.2.7 cert.server.generate

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

Parameters:

- The `subject` is the name of the user who requested the operation.
- The `object` is "cert".
- The `result` is "success" or "failure".
- The `reason`, if present, provides additional details about the event.
- The `ip`, if present, is the network address of the originator of the operation.
- The `opID`, if present, is the operation ID.

A.2.8 cert.server.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 "cert".
- The `result` is "success" or "failure".
- The `reason`, if present, provides additional details about the event.
- The `ip`, if present, is the network address of the originator of the operation.
- The `subjectDN`, if present, is the subject distinguished name of the server certificate.
- The `opID`, if present, is the operation ID.

A.2.9 entropy.rbg.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 "entropy"
- The `result` is "failure".

- The `reason`, if present, indicates the reason for the failure. When testing for entropy failure, the reason is "test".

A.2.10 proxy.connect

This event is generated when an attempt is made to establish a proxy service connection.

Parameters:

- The `subject` is an empty string (the host itself).
- The `object` is "proxy".
- The `result` is "success" or "failure".
- The `reason` is present when the result is "failure" and indicates the reason for the failure.
- The `ip`, if present, is the network address of the originator of the connection.
- The `port`, if present, is the network port number of the originator of the connection.

A.2.11 proxy.disconnect

This event is generated when a proxy service connection ends.

Parameters:

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

A.2.12 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 the `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.2.13 ssh.connect

This event is generated when an attempt to establish an ssh connection is made to the ESXi server.

Parameters:

- The `subject` is the name of the user who requested the operation.
- The `object` is “ssh”.
- The `result` is "success" or "failure".
- The `ip` is the network address of the originator of the operation.
- The `reason` provides additional details about the event.

A.2.14 syslog.net.close

This event is generated when vmsyslogd closes a socket (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".

A.2.15 syslog.net.link.down

This event is generated when the TCP/SSL connection to a remote host is lost.

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 "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.2.16 syslog.net.link.up

This event is generated when a TCP/SSL connection to a remote host is established. For the sake of consistency, it is also generated for UDP.

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".

A.2.17 syslog.net.open

This event is generated when vmsyslogd opens a socket (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".

A.2.18 system.update.add

This event is generated when a new VIB is added to the inventory of the ESXi.

Parameters:

- The `subject` is the name of the user who requested the operation.
- The `object` is the VIB which is being added to ESXi.
- The `result` is "success" or "failure".
- The `reason`, if present, provides additional details about the event. Including details regarding failure related to the provided VIB.

A.2.19 system.update.end

This event is generated at the end of a system update. The severity on success depends on whether signature validation has been overridden. If it has then the severity is LOG_NOTICE. Otherwise it is the default (LOG_INFO).

Parameters:

- The `subject` is the name of the user who requested the operation.
- The `object` is “system”.
- The `result` is "success" or "failure".
- The `reason` is present when the result is “failure” and indicates the reason for the failure.

A.2.20 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 “system”.
- The `result` is "success" or "failure".
- The `reason`, if present, provides additional details about the event.

A.2.21 time.ntp.set.servers

This event is generated when an attempt was made to set the NTP server configuration. On success, all existing NTP servers are replaced with the time server(s) indicated by the value parameter(s).

Parameters:

- The `subject` is the name of the user who requested the operation.
- The `object` is "time".
- The `result` is "success" or "failure".
- The `reason` is present when result is "failure" and indicates the reason for the failure.
- The `ip`, if present, is the network address of the originator of the operation.
- The `max`, if present, indicates the maximum number of allowed servers when the result is "failure".
- The `value`, if present, is the new value of server(s) configured for for NTP. May be specified multiple times, one for each NTP server.
- The `opID`, if present, is the operation ID.

A.2.22 tls.clt.set.profile

This event is generated when an attempt is made to set the client TLS profile.

Parameters:

- The `subject` is the name of the user who requested the operation.
- The `object` is “tls”.
- The `result` is "success" or "failure".
- The `reason` is present when the result is "failure" and indicates the reason for the failure.
- The `value` is the new profile value (one of "COMPATIBLE","MANUAL").
- The `ip` is the network address of the originator of the operation.
- The `comment`, if present, provides information about the event.

- The `opID`, if present, is the operation ID.

A.2.23 tls.clt.set.protocols

This event is generated when an attempt is made to set the client TLS protocols.

Parameters:

- The `subject` is the name of the user who requested the operation.
- The `object` is “tls”.
- The `result` is "success" or "failure".
- The `reason` is present when the result is "failure" and indicates the reason for the failure.
- The `value` is the new value specified for the protocols.
- The `ip` is the network address of the originator of the operation.
- The `comment`, if present, provides information about the event.
- The `opID`, if present, is the operation ID.

A.2.24 tls.clt.set.cipherlist

This event is generated when an attempt was made to set the ciphers for outgoing connections, where ESXi is acting as a client, and if the negotiated protocol is TLS 1.2.

Parameters:

- The `subject` is the name of the user who requested the operation.
- The `object` is “tls”.
- The `result` is "success" or "failure".
- The `reason` is present when the result is "failure" and indicates the reason for the failure.
- The `value` is the new value specified for the new cipherlist.
- The `ip` is the network address of the originator of the operation.
- The `comment`, if present, provides information about the event.
- The `opID`, if present, is the operation ID.

A.2.25 tls.clt.set.ciphersuites

This event is generated when an attempt was made to set the ciphers for outgoing connections, where ESXi is acting as a client, and if the negotiated protocol is TLS 1.3.

Parameters:

- The `subject` is the name of the user who requested the operation.
- The `object` is “tls”.
- The `result` is "success" or "failure".
- The `reason` is present when the result is "failure" and indicates the reason for the failure.
- The `value` is the new value specified for the new ciphersuites.
- The `ip` is the network address of the originator of the operation.
- The `comment`, if present, provides information about the event.
- The `opID`, if present, is the operation ID.

A.2.26 tls.clt.set.groups

This event is generated when an attempt was made to set the client TLS ECC groups.

Parameters:

- The `subject` is the name of the user who requested the operation.
- The `object` is “tls”.
- The `result` is "success" or "failure".
- The `reason` is present when the result is "failure" and indicates the reason for the failure.
- The `value` is the new value specified for the ECC Groups.
- The `ip` is the network address of the originator of the operation.
- The `comment`, if present, provides information about the event.
- The `opID`, if present, is the operation ID.

A.2.27 tls.svr.set.profile

This event is generated when an attempt was made to set the server TLS profile.

Parameters:

- The `subject` is the name of the user who requested the operation.
- The `object` is “tls”.
- The `result` is "success" or "failure".
- The `reason` is present when the result is "failure" and indicates the reason for the failure.
- The `value` is the new profile value (one of "COMPATIBLE","MANUAL","NIST_2024").
- The `ip` is the network address of the originator of the operation.
- The `comment`, if present, provides information about the event.
- The `opID`, if present, is the operation ID.

A.2.28 tls.svr.set.protocols

This event is generated when an attempt was made to set the server TLS protocols.

Parameters:

- The `subject` is the name of the user who requested the operation.
- The `object` is “tls”.
- The `result` is "success" or "failure".
- The `reason` is present when the result is "failure" and indicates the reason for the failure.
- The `value` is the new value specified for the protocols.
- The `ip` is the network address of the originator of the operation.
- The `comment`, if present, provides information about the event.
- The `opID`, if present, is the operation ID.

A.2.29 tls.svr.set.cipherlist

This event is generated when an attempt was made to set the ciphers for incoming connections, where ESXi is acting as a server, and if the negotiated protocol is TLS 1.2.

Parameters:

- The `subject` is the name of the user who requested the operation.
- The `object` is “tls”.
- The `result` is "success" or "failure".
- The `reason` is present when the result is "failure" and indicates the reason for the failure.
- The `value` is the new value specified for the new cipherlist.
- The `ip` is the network address of the originator of the operation.
- The `comment`, if present, provides information about the event.
- The `opID`, if present, is the operation ID.

A.2.30 tls.svr.set.ciphersuites

This event is generated when an attempt was made to set the ciphers for outgoing connections, where ESXi is acting as a server, and if the negotiated protocol is TLS 1.3.

Parameters:

- The `subject` is the name of the user who requested the operation.
- The `object` is “tls”.
- The `result` is "success" or "failure".
- The `reason` is present when the result is "failure" and indicates the reason for the failure.
- The `value` is the new value specified for the new ciphersuites.
- The `ip` is the network address of the originator of the operation.
- The `comment`, if present, provides information about the event.
- The `opID`, if present, is the operation ID.

A.2.31 tls.svr.set.groups

This event is generated when an attempt was made to set the server TLS ECC groups.

Parameters:

- The `subject` is the name of the user who requested the operation.
- The `object` is “tls”.
- The `result` is "success" or "failure".
- The `reason` is present when the result is "failure" and indicates the reason for the failure.
- The `value` is the new value specified for the ECC Groups.
- The `ip` is the network address of the originator of the operation.
- The `comment`, if present, provides information about the event.
- The `opID`, if present, is the operation ID.

A.2.32 vim.connect

This event is generated when an attempt to connect to the VIM endpoint is attempted.

Parameters:

- The `subject` is the name of the user who requested the operation.
- The `object` is “vim”.
- The `result` is "success" or "failure".
- The `ip` is the network address of the originator of the operation.
- The `uniqueID` is only present on success, it indicates the session ID from the vim connection.
- The `opID`, if present, is the operation ID.

A.2.33 vim.disconnect

This event is generated when an attempt to disconnect from the VIM endpoint is attempted.

Parameters:

- The `subject` is the name of the user who requested the operation.
- The `object` is “vim”.
- The `result` is "success" or "failure".
- The `reason` provides additional details about the event.
- The `ip` is the network address of the originator of the operation.
- The `uniqueID` is only present on success, it indicates the session ID from the vim connection.
- The `opID`, if present, is the operation ID.

A.2.34 vm.create

This event is generated when an attempt is made to create 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 `opID`, if present, is the operation ID.

A.2.35 vm.delete

This event is generated when an attempt is made to create 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 `opID`, if present, is the operation ID.

A.2.36 vm.hypercall.denied

This event is generated when an attempt to use a hypercall is denied.

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 the 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.2.37 vm.net.add

This event is generated when an attempt is 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 `reason` is present when the result is "failure" and indicates the reason for the failure. B
- 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.2.38 vm.net.edit

This event is generated when an attempt is 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 `networkID` is the name of the new network.
- The `connect` is “at power-on” or “not at power-on”
- The `oldID`, if present, 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.2.39 vm.power.off

This event is generated when an attempt is made to power off a VM.

Parameters:

- The `subject` is the name of the user powering off a VM.
- 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`, if present, is the network address of the originator of the operation.
- The `opID`, if present, is the operation ID.

A.2.40 vm.power.on

This event is generated when an attempt is made to power on a VM.

Parameters:

- The `subject` is the name of the user powering on a VM.
- 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`, if present, is the network address of the originator of the operation.
- The `opID`, if present, is the operation ID.

A.2.41 vm.power.suspend

This event is generated when an attempt is made to suspend 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`, if present, is the network address of the originator of the operation.
- The `opID`, if present, is the operation ID.

A.2.42 vm.reconfigure

This event is generated when a new configuration is submitted as an updated configuration to a targeted VM.

Parameters:

- The `subject` is an empty string (the host itself).
- The `object` is the VMX file of the target VM..
- The `reason`, if present, provides additional details about the event.
- The `result` is an indicator of whether the configuration update was applied or rejected.
- The `ip` is the network address of the originator of the connection
- The `opID`, if present, is the operation ID.

A.2.43 vm.snapshot.create

This event is generated when an attempt is made to create a VM snapshot.

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 result is "failure" and indicates the reason for the failure.
- The `ip` is the network address of the originator of the operation.
- The `name` is the display name of the snapshot.
- The `uniqueID` is the unique ID of the snapshot or an empty string.
- The `parent` is the unique ID of the parent snapshot or an empty string when the snapshot is the root of the tree.
- The `opID`, if present, is the operation ID.

A.2.44 vm.snapshot.remove

This event is generated when an attempt is made to remove a VM snapshot.

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 `name` is the display name of the snapshot.
- The `uniqueID` is the unique ID of the snapshot or an empty string.
- The `parent` is the unique ID of the parent snapshot or an empty string when the snapshot is the root of the tree.
- The `opID`, if present, is the operation ID.

A.2.45 vm.snapshot.removeAll

This event is generated when an attempt is made to remove all VM snapshots.

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 `opID`, if present, is the operation ID.

A.2.46 vm.storage.add

This event is generated when an attempt is 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 `reason`, if present, provides additional details about the event.
- 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.2.47 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 `connect` is “at power-on” or “not at power-on”
- 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 `reason` is present when the result is “failure” and indicates the reason for the failure
- The `status` is "connected" or "disconnected" when a change affects device connectivity.
- The `opID`, if present, is the operation ID.

A.2.48 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.2.49 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.
- The `name`, if present, is the user-friendly name of the device.
- The `type`, if present, is the type of the device. "generic" means the device is attached to the local ESX host. "remote" means the device may reside on another host (or a client machine) and has been attached to the VM through a network connection. The other values are specific for the virtual devices ("hid", "hub", etc.)

A.2.50 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 identifing 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 `name`, if present, is the user-friendly name of the device.
- The `type`, if present, is the type of the device. "generic" means the device is attached to the local ESX host. "remote" means the device may reside on another host (or a client machine) and has been attached to the VM through a network connection. The other values are specific for the virtual devices ("hid", "hub", etc.)
- The `deviceID`, if present, is the device ID of the device.

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

Initiation of update	**FPT_TUD_EXT.1 – Event 1** <110>1 2024-09-05T23:19:47.212Z - esxupdate 2104948 - [system.update.start@6876 subject="root" object="system" result="success"] <110>1 2024-09-05T23:19:47.214Z - esxupdate 2104948 - [system.update.add@6876 subject="root" object="VMW_bootbank_atlantic_1.0.3.0-13vmw.803.0.0.24022510" result="success"] <110>1 2024-09-05T23:19:47.218Z - esxupdate 2104948 - [system.update.end@6876 subject="root" object="system" result="success"]
Configure password policy	**FMT_MOF_EXT.1** **FIA_PMG_EXT.1** <110>1 2024-09-05T23:22:36.283Z - Hostd 2099295 - [settings.advanced.set@6876 subject="root" object="Security.PasswordMaxDays" value="3" ip="10.4.25.25" opID="esxui-229-ccd1" result="success"]
Create, configure, and delete VMs	**FMT_MOF_EXT.1** <110>1 2024-10-11T19:57:41.773Z - Hostd 2099295 - [vm.create@6876 subject="root" object="/vmfs/volumes/668eddb5-b1324e77-6e22-00620b94eaa0/Ubuntu 1/Ubuntu 1.vmx" ip="10.4.25.83" opID="esxui-6682-7dcf" result="success"] <110>1 2024-10-11T19:58:24.218Z - Hostd 2099295 - [vm.reconfigure@6876 subject="root" object="/vmfs/volumes/668eddb5-b1324e77-6e22-00620b94eaa0/Ubuntu 1/Ubuntu 1.vmx" ip="10.4.25.83" opID="esxui-9529-7e11" result="success"] <110>1 2024-10-11T19:58:53.321Z - Hostd 2099295 - [vm.delete@6876 subject="root" object="/vmfs/volumes/668eddb5-b1324e77-6e22-00620b94eaa0/Ubuntu 1/Ubuntu 1.vmx" ip="10.4.25.83" opID="esxui-3da9-7e30" result="success"]

Set default initial VM configurations	**FMT_MOF_EXT.1** <110>1 2024-09-04T22:13:30.698Z - Hostd 2099293 - [vm.storage.add@6876 subject="root" object="/vmfs/volumes/668eddb5-b1324e77-6e22-00620b94eaa0/Ubuntu 1/Ubuntu 1.vmx" path="/vmfs/volumes/668eddb5-b1324e77-6e22-00620b94eaa0/Ubuntu 1/Ubuntu 1_1.vmdk" ip="10.4.25.35" opID="esxui-f5a7-b45c" result="success"] <110>1 2024-09-04T23:37:10.199Z - Hostd 2099293 - [vm.storage.edit@6876 subject="root" object="/vmfs/volumes/668eddb5-b1324e77-6e22-00620b94eaa0/Ubuntu 1/Ubuntu 1.vmx" oldPath="" path="/vmfs/volumes/668eddb5-b1324e77-6e22-00620b94eaa0/ubuntu-24.04-desktop-amd64.iso" ip="10.4.25.35" opID="esxui-60ab-b6b0" result="success"] <110>1 2024-09-05T22:54:21.831Z - Hostd 2099295 - [vm.net.add@6876 subject="root" object="/vmfs/volumes/668eddb5-b1324e77-6e22-00620b94eaa0/Ubuntu 1/Ubuntu 1.vmx" networkID="VM Network" ip="10.4.25.25" opID="esxui-7a0-caf4" result="success"] <110>1 2024-09-05T22:54:21.831Z - Hostd 2099295 - [vm.net.edit@6876 subject="root" object="/vmfs/volumes/668eddb5-b1324e77-6e22-00620b94eaa0/Ubuntu 1/Ubuntu 1.vmx" networkID="VM Network" connect="at power-on" ip="10.4.25.25" opID="esxui-7a0-caf4" result="success"]
Configure virtual networks	**FMT_MOF_EXT.1** **FDP_VNC_EXT.1** <110>1 2024-08-14T20:23:28.718Z - Hostd 2099211 - [vm.net.add@6876 subject="root" object="/vmfs/volumes/668eddb5-b1324e77-6e22-00620b94eaa0/TestVM_1/TestVM_1.vmx" networkID="" ip="10.4.146.35" opID="f48eacb9" result="success"] <109>1 2024-09-05T22:27:14.478Z - Hostd 2099295 - [vm.net.add@6876 subject="root" object="/vmfs/volumes/668eddb5-b1324e77-6e22-00620b94eaa0/Ubuntu 2/Ubuntu 2.vmx" networkID="VM Network" ip="10.4.25.25" opID="esxui-b59d-c07d" reason="Number of virtual devices exceeds the maximum for a given controller." result="failure"] <110>1 2024-08-14T20:23:28.718Z - Hostd 2099211 - [vm.net.edit@6876 subject="root" object="/vmfs/volumes/668eddb5-b1324e77-6e22-00620b94eaa0/TestVM_1/TestVM_1.vmx" networkID="" connect="at power-on" ip="10.4.146.35" opID="f48eacb9" result="success"] <110>1 2024-09-04T22:13:30.698Z - Hostd 2099293 - [vm.reconfigure@6876 subject="root" object="/vmfs/volumes/668eddb5-b1324e77-6e22-00620b94eaa0/Ubuntu 1/Ubuntu 1.vmx" ip="10.4.25.35" opID="esxui-f5a7-b45c" result="success"]

Configure and manage audit system and audit data	**FMT_MOF_EXT.1** <110>1 2024-09-04T21:51:22.710Z - vmsyslogd 2098124 - [audit.start@6876 subject="" object="audit" result="success" reason="administrative action" directory="/scratch/auditLog" capacity="4"] <110>1 2024-09-04T21:51:15.628Z - vmsyslogd 2098124 - [audit.stop@6876 subject="" object="audit" result="success" reason="administrative action"] <110>1 2024-09-05T23:25:40.715Z - Hostd 2099295 - [settings.advanced.set@6876 subject="root" object="Syslog.global.auditRecord.storageCapacity" value="8" ip="127.0.0.1" opID="esxcli-bc-cd72" result="success"]
Configure VM access to physical devices	**FDP_PPR_EXT.1** <109>1 2024-09-05T21:45:33.526Z - Hostd 2099295 - [vm.reconfigure@6876 subject="root" object="/vmfs/volumes/668eddb5-b1324e77-6e22-00620b94eaa0/Ubuntu 1/Ubuntu 1.vmx" ip="10.4.25.25" opID="esxui-2dbc-a968" reason="Unable to access file since it is locked" result="failure"] <109>1 2024-09-05T21:45:33.526Z - Hostd 2099295 - [vm.storage.add@6876 subject="root" object="/vmfs/volumes/668eddb5-b1324e77-6e22-00620b94eaa0/Ubuntu 1/Ubuntu 1.vmx" path="/vmfs/volumes/668eddb5-b1324e77-6e22-00620b94eaa0/Ubuntu 2/Ubuntu 2.vmdk" ip="10.4.25.25" opID="esxui-2dbc-a968" reason="Unable to access file since it is locked" result="failure"] <109>1 2024-09-05T21:48:54.886Z - vmx 2102131 - [vm.usb.connect@6876 subject="" object="/vmfs/volumes/668eddb5-b1324e77-6e22-00620b94eaa0/Ubuntu 1/Ubuntu 1.vmx" reason="The device is already connected to another virtual machine." name="SanDisk Ultra Fit" vendorID="0781" productID="5583" deviceLabel="ehci:0" type="generic" result="failure"] **FMT_MOF_EXT.1** <110>1 2024-09-05T21:47:32.398Z - vmx 2102131 - [vm.usb.connect@6876 subject="" object="/vmfs/volumes/668eddb5-b1324e77-6e22-00620b94eaa0/Ubuntu 1/Ubuntu 1.vmx" name="SanDisk Ultra Fit" vendorID="0781" productID="5583" deviceLabel="ehci:0" type="generic" result="success"]

Configure inter-VM data sharing	**FMT_MOF_EXT.1** <110>1 2024-08-14T20:23:28.718Z - Hostd 2099211 - [vm.net.add@6876 subject="root" object="/vmfs/volumes/668eddb5-b1324e77-6e22-00620b94eaa0/TestVM_1/TestVM_1.vmx" networkID="" ip="10.4.146.35" opID="f48eacb9" result="success"] <110>1 2024-08-14T20:23:28.718Z - Hostd 2099211 - [vm.net.edit@6876 subject="root" object="/vmfs/volumes/668eddb5-b1324e77-6e22-00620b94eaa0/TestVM_1/TestVM_1.vmx" networkID="" connect="at power-on" ip="10.4.146.35" opID="f48eacb9" result="success"] <110>1 2024-09-04T22:13:30.698Z - Hostd 2099293 - [vm.reconfigure@6876 subject="root" object="/vmfs/volumes/668eddb5-b1324e77-6e22-00620b94eaa0/Ubuntu 1/Ubuntu 1.vmx" ip="10.4.25.35" opID="esxui-f5a7-b45c" result="success"]

Configure cryptographic functionality	**FMT_MOF_EXT.1** <110>1 2024-09-05T23:28:04.248Z - Hostd 2099295 - [tls.svr.set.profile@6876 subject="root" object="tls" value="MANUAL" ip="127.0.0.1" opID="esxcli-47-cda7" result="success"] <110>1 2024-09-05T23:28:04.248Z - Hostd 2099295 - [tls.svr.set.protocols@6876 subject="root" object="tls" value="tls1.2" comment="unchanged" ip="127.0.0.1" opID="esxcli-47-cda7" result="success"] <110>1 2024-09-05T23:28:04.248Z - Hostd 2099295 - [tls.svr.set.cipherlist@6876 subject="root" object="tls" value="ECDHE+AESGCM:!ECDSA" comment="unchanged" ip="127.0.0.1" opID="esxcli-47-cda7" result="success"] <110>1 2024-09-05T23:28:04.248Z - Hostd 2099295 - [tls.svr.set.ciphersuites@6876 subject="root" object="tls" value="ECDHE-RSA-AES256-GCM-SHA384:ECDHE-RSA-AES128-GCM-SHA256" comment="unchanged" ip="127.0.0.1" opID="esxcli-47-cda7" result="success"] <110>1 2024-09-05T23:28:04.248Z - Hostd 2099295 - [tls.svr.set.groups@6876 subject="root" object="tls" value="prime256v1:secp384r1:secp521r1" ip="127.0.0.1" opID="esxcli-47-cda7" result="success"] <110>1 2024-09-05T23:28:17.978Z - Hostd 2099295 - [tls.clt.set.profile@6876 subject="root" object="tls" value="MANUAL" ip="127.0.0.1" opID="esxcli-ed-cdbb" result="success"] <110>1 2024-09-05T23:28:17.978Z - Hostd 2099295 - [tls.clt.set.protocols@6876 subject="root" object="tls" value="tls1.2" comment="unchanged" ip="127.0.0.1" opID="esxcli-ed-cdbb" result="success"] <110>1 2024-09-05T23:28:17.978Z - Hostd 2099295 - [tls.clt.set.cipherlist@6876 subject="root" object="tls" value="ECDHE+AESGCM:!AESCCM:!AESCCM8" comment="unchanged" ip="127.0.0.1" opID="esxcli-ed-cdbb" result="success"] <110>1 2024-09-05T23:28:17.978Z - Hostd 2099295 - [tls.clt.set.ciphersuites@6876 subject="root" object="tls" value="ECDHE-ECDSA-AES256-GCM-SHA384:ECDHE-RSA-AES256-GCM-SHA384:ECDHE-ECDSA-AES128-GCM-SHA256:ECDHE-RSA-AES128-GCM-SHA256" comment="unchanged" ip="127.0.0.1" opID="esxcli-ed-cdbb" result="success"] <110>1 2024-09-05T23:28:17.978Z - Hostd 2099295 - [tls.clt.set.groups@6876 subject="root" object="tls" value="prime256v1:secp384r1:secp521r1" ip="127.0.0.1" opID="esxcli-ed-cdbb" result="success"]

Change default authorization factors	**FMT_MOF_EXT.1** <110>1 2024-09-05T23:30:50.379Z - Hostd 2099295 - [cert.castore.remove@6876 subject="root" object="cert" ip="127.0.0.1" opID="esxcli-d4-cdcc" subjectDN="C=US, ST=Texas, O=atsec, OU=rsyslog, CN=rsyslog CA" result="success"] <110>1 2024-09-05T23:30:55.117Z - Hostd 2099295 - [cert.castore.add@6876 subject="root" object="cert" ip="127.0.0.1" opID="esxcli-9b-cdd6" subjectDN="C=US, ST=Texas, O=atsec, OU=rsyslog, CN=rsyslog CA" result="success"] <110>1 2024-09-05T23:32:36.720Z - Hostd 2099295 - [cert.server.generate@6876 subject="root" object="cert" ip="10.4.25.25" opID="esxui-371-cde5" result="success"] <109>1 2024-09-05T23:32:49.008Z - Hostd 2099295 - [cert.server.install@6876 subject="root" object="cert" ip="10.4.25.25" opID="esxui-4c58-cdf5" reason="Cannot change the host configuration." result="failure"]
Configure remote connection inactivity timeout	**FMT_MOF_EXT.1** <110>1 2024-09-05T23:33:48.084Z - Hostd 2099295 - [settings.advanced.set@6876 subject="root" object="/UserVars/HostClientSessionTimeout" value="1000" ip="10.4.25.25" opID="esxui-8906-ce23" result="success"]
Configure lockout policy for unsuccessful authentication attempts	**FMT_MOF_EXT.1** <110>1 2024-09-05T23:34:24.891Z - Hostd 2099295 - [settings.advanced.set@6876 subject="root" object="Security.AccountLockFailures" value="6" ip="10.4.25.25" opID="esxui-2324-ce38" result="success"]
Configure audit/logging server	**FMT_MOF_EXT.1** <110>1 2024-09-02T23:00:38.350Z - Hostd 2099293 - [settings.advanced.set@6876 subject="root" object="Syslog.global.logHost" value="ssl://10.4.146.35:6514" ip="10.4.146.35" opID="esxcli-ee-8fb1" result="success"]
Configure name/address of network time server	**FMT_MOF_EXT.1** <110>1 2024-09-05T23:38:14.037Z - Hostd 2099295 - [time.ntp.set.servers@6876 subject="root" object="time" value="0.pool.ntp.org" result="success"]

Configure banner	**FMT_MOF_EXT.1** <110>1 2024-09-05T23:38:53.434Z - Hostd 2099295 - [settings.advanced.set@6876 subject="root" object="/UserVars/HostClientWelcomeMessage" value="Welcome to Common Criteria {{hostname}}" ip="10.4.25.25" opID="esxui-42a-ce77" result="success"]
Connect/disconnect removable devices to/from a VM	**FMT_MOF_EXT.1** <110>1 2024-09-05T22:29:15.687Z - vmx 2103806 - [vm.usb.connect@6876 subject="" object="/vmfs/volumes/668eddb5-b1324e77-6e22-00620b94eaa0/Ubuntu 2/Ubuntu 2.vmx" name="SanDisk Ultra Fit" vendorID="0781" productID="5583" deviceLabel="ehci:0" type="generic" result="success"] <110>1 2024-09-05T22:29:15.681Z - vmx 2103555 - [vm.usb.disconnect@6876 subject="" object="/vmfs/volumes/668eddb5-b1324e77-6e22-00620b94eaa0/Ubuntu 2/Ubuntu 2.vmx" name="SanDisk Ultra Fit" vendorID="0781" productID="5583" deviceLabel="ehci:0" type="generic" result="success"]
Start a VM	**FMT_MOF_EXT.1** <110>1 2024-09-04T15:39:07.221Z - Hostd 2099293 - [vm.power.on@6876 subject="root" object="/vmfs/volumes/668eddb5-b1324e77-6e22-00620b94eaa0/Ubuntu 1/Ubuntu 1.vmx" ip="10.4.25.15" opID="esxui-b564-a6de" result="success"]
Stop/halt a VM	**FMT_MOF_EXT.1** <110>1 2024-09-04T15:39:04.442Z - Hostd 2099293 - [vm.power.off@6876 subject="root" object="/vmfs/volumes/668eddb5-b1324e77-6e22-00620b94eaa0/Ubuntu 1/Ubuntu 1.vmx" ip="10.4.25.15" opID="esxui-f1a-a6b9" result="success"]

Checkpoint a VM	**FMT_MOF_EXT.1** <110>1 2024-10-31T02:09:18.444Z - Hostd 2099295 - [vm.snapshot.create@6876 subject="root" object="/vmfs/volumes/668eddb5-b1324e77-6e22-00620b94eaa0/Ubuntu-1/Ubuntu-1.vmx" ip="10.4.25.6" opID="esxui-d03d-2b1b" name="test" uniqueID="1" parent="" result="success"] <110>1 2024-10-31T02:10:06.075Z - Hostd 2099295 - [vm.snapshot.remove@6876 subject="root" object="/vmfs/volumes/668eddb5-b1324e77-6e22-00620b94eaa0/Ubuntu-1/Ubuntu-1.vmx" ip="10.4.25.6" opID="esxui-f991-2b73" name="test" uniqueID="1" comment="remove all children" result="success"] <110>1 2024-10-31T02:10:11.220Z - Hostd 2099295 - [vm.snapshot.removeAll@6876 subject="root" object="/vmfs/volumes/668eddb5-b1324e77-6e22-00620b94eaa0/Ubuntu-1/Ubuntu-1.vmx" ip="10.4.25.6" opID="esxui-e24-2b83" result="success"]
Suspend a VM	**FMT_MOF_EXT.1** <110>1 2024-09-05T23:39:50.032Z - Hostd 2099295 - [vm.power.suspend@6876 subject="root" object="/vmfs/volumes/668eddb5-b1324e77-6e22-00620b94eaa0/Ubuntu 1/Ubuntu 1.vmx" ip="10.4.25.25" opID="esxui-fb21-cec3" result="success"]
Resume a VM	**FMT_MOF_EXT.1** <110>1 2024-09-04T15:39:07.221Z - Hostd 2099293 - [vm.power.on@6876 subject="root" object="/vmfs/volumes/668eddb5-b1324e77-6e22-00620b94eaa0/Ubuntu 1/Ubuntu 1.vmx" ip="10.4.25.15" opID="esxui-b564-a6de" result="success"]

Table 5: Sample Audit Records for Management Functions

Event	Sample Record
Start-up and shutdown of the audit functions	**FMT_MOF_EXT.1** <110>1 2024-09-04T21:51:22.710Z - vmsyslogd 2098124 - [audit.start@6876 subject="" object="audit" result="success" reason="administrative action" directory="/scratch/auditLog" capacity="4"] <110>1 2024-09-04T21:51:15.628Z - vmsyslogd 2098124 - [audit.stop@6876 subject="" object="audit" result="success" reason="administrative action"] <110>1 2024-09-05T23:25:40.715Z - Hostd 2099295 - [settings.advanced.set@6876 subject="root" object="Syslog.global.auditRecord.storageCapacity" value="8" ip="127.0.0.1" opID="esxcli-bc-cd72" result="success"]
On failure of logging function, capture record of failure and record upon restart of logging function	**FAU_STG_EXT.1 – Event 2** <110>1 2024-09-04T16:08:15.648Z - vmsyslogd 2098124 - [audit.storage.recycle@6876 subject="" object="audit" result="success"]
Failure of randomization	**FCS_RBG_EXT.1** <105>1 2024-09-09T21:19:32.761Z - Hostd 2099378 - [entropy.rbg.failure@6876 subject="" object="entropy" reason="test" result="failure"]

Security policy violations	**FDP_PPR_EXT.1** <109>1 2024-09-05T21:45:33.526Z - Hostd 2099295 - [vm.reconfigure@6876 subject="root" object="/vmfs/volumes/668eddb5-b1324e77-6e22-00620b94eaa0/Ubuntu 1/Ubuntu 1.vmx" ip="10.4.25.25" opID="esxui-2dbc-a968" reason="Unable to access file since it is locked" result="failure"] <109>1 2024-09-05T21:45:33.526Z - Hostd 2099295 - [vm.storage.add@6876 subject="root" object="/vmfs/volumes/668eddb5-b1324e77-6e22-00620b94eaa0/Ubuntu 1/Ubuntu 1.vmx" path="/vmfs/volumes/668eddb5-b1324e77-6e22-00620b94eaa0/Ubuntu 2/Ubuntu 2.vmdk" ip="10.4.25.25" opID="esxui-2dbc-a968" reason="Unable to access file since it is locked" result="failure"] <109>1 2024-09-05T21:48:54.886Z - vmx 2102131 - [vm.usb.connect@6876 subject="" object="/vmfs/volumes/668eddb5-b1324e77-6e22-00620b94eaa0/Ubuntu 1/Ubuntu 1.vmx" reason="The device is already connected to another virtual machine." name="SanDisk Ultra Fit" vendorID="0781" productID="5583" deviceLabel="ehci:0" type="generic" result="failure"] **FDP_VNC_EXT.1 – Event 2** <109>1 2024-09-05T22:21:16.544Z - Hostd 2099295 - [vm.reconfigure@6876 subject="test" object="/vmfs/volumes/668eddb5-b1324e77-6e22-00620b94eaa0/Ubuntu 2/Ubuntu 2.vmx" ip="10.4.25.25" opID="esxui-3a2c-bed5" reason="Permission to perform this operation was denied." result="failure"] <109>1 2024-09-05T22:27:14.478Z - Hostd 2099295 - [vm.reconfigure@6876 subject="root" object="/vmfs/volumes/668eddb5-b1324e77-6e22-00620b94eaa0/Ubuntu 2/Ubuntu 2.vmx" ip="10.4.25.25" opID="esxui-b59d-c07d" reason="Number of virtual devices exceeds the maximum for a given controller." result="failure"]

Successful and failed attempts to connect VMs to physical and virtual networking components	**FDP_VNC_EXT.1** Success: <110>1 2024-08-14T20:23:28.718Z - Hostd 2099211 - [vm.net.add@6876 subject="root" object="/vmfs/volumes/668eddb5-b1324e77-6e22-00620b94eaa0/TestVM_1/TestVM_1.vmx" networkID="" ip="10.4.146.35" opID="f48eacb9" result="success"] <110>1 2024-08-14T20:23:28.718Z - Hostd 2099211 - [vm.net.edit@6876 subject="root" object="/vmfs/volumes/668eddb5-b1324e77-6e22-00620b94eaa0/TestVM_1/TestVM_1.vmx" networkID="" connect="at power-on" ip="10.4.146.35" opID="f48eacb9" result="success"] <110>1 2024-09-04T22:13:30.698Z - Hostd 2099293 - [vm.reconfigure@6876 subject="root" object="/vmfs/volumes/668eddb5-b1324e77-6e22-00620b94eaa0/Ubuntu 1/Ubuntu 1.vmx" ip="10.4.25.35" opID="esxui-f5a7-b45c" result="success"] Failure: <109>1 2024-09-05T22:27:14.478Z - Hostd 2099295 - [vm.net.add@6876 subject="root" object="/vmfs/volumes/668eddb5-b1324e77-6e22-00620b94eaa0/Ubuntu 2/Ubuntu 2.vmx" networkID="VM Network" ip="10.4.25.25" opID="esxui-b59d-c07d" reason="Number of virtual devices exceeds the maximum for a given controller." result="failure"]

Successful and failed attempts to connect VMs to physical devices where connection is governed by configurable policy	**FDP_PPR_EXT.1 – Event 1** <109>1 2024-09-05T21:45:33.526Z - Hostd 2099295 - [vm.reconfigure@6876 subject="root" object="/vmfs/volumes/668eddb5-b1324e77-6e22-00620b94eaa0/Ubuntu 1/Ubuntu 1.vmx" ip="10.4.25.25" opID="esxui-2dbc-a968" reason="Unable to access file since it is locked" result="failure"] <109>1 2024-09-05T21:45:33.526Z - Hostd 2099295 - [vm.storage.add@6876 subject="root" object="/vmfs/volumes/668eddb5-b1324e77-6e22-00620b94eaa0/Ubuntu 1/Ubuntu 1.vmx" path="/vmfs/volumes/668eddb5-b1324e77-6e22-00620b94eaa0/Ubuntu 2/Ubuntu 2.vmdk" ip="10.4.25.25" opID="esxui-2dbc-a968" reason="Unable to access file since it is locked" result="failure"] <110>1 2024-09-05T21:47:32.398Z - vmx 2102131 - [vm.usb.connect@6876 subject="" object="/vmfs/volumes/668eddb5-b1324e77-6e22-00620b94eaa0/Ubuntu 1/Ubuntu 1.vmx" name="SanDisk Ultra Fit" vendorID="0781" productID="5583" deviceLabel="ehci:0" type="generic" result="success"] <109>1 2024-09-05T21:48:54.886Z - vmx 2102131 - [vm.usb.connect@6876 subject="" object="/vmfs/volumes/668eddb5-b1324e77-6e22-00620b94eaa0/Ubuntu 1/Ubuntu 1.vmx" reason="The device is already connected to another virtual machine." name="SanDisk Ultra Fit" vendorID="0781" productID="5583" deviceLabel="ehci:0" type="generic" result="failure"]

Administrator configuration of inter-VM communications channels	**FDP_VNC_EXT.1** <110>1 2024-09-04T14:35:26.741Z - Hostd 2099293 - [vm.net.add@6876 subject="root" object="/vmfs/volumes/668eddb5-b1324e77-6e22-00620b94eaa0/Ubuntu 2/Ubuntu 2.vmx" networkID="VM Network" ip="10.4.25.15" opID="esxui-bf70-9fff" result="success"] <110>1 2024-09-04T14:35:26.741Z - Hostd 2099293 - [vm.net.edit@6876 subject="root" object="/vmfs/volumes/668eddb5-b1324e77-6e22-00620b94eaa0/Ubuntu 2/Ubuntu 2.vmx" networkID="VM Network" connect="not at power-on" ip="10.4.25.15" opID="esxui-bf70-9fff" result="success"] <110>1 2024-09-04T15:14:59.840Z - Hostd 2099293 - [vm.reconfigure@6876 subject="root" object="/vmfs/volumes/668eddb5-b1324e77-6e22-00620b94eaa0/Ubuntu 2/Ubuntu 2.vmx" ip="10.4.25.15" opID="esxui-6c91-a5cf" result="success"] <110>1 2024-09-05T22:54:21.831Z - Hostd 2099295 - [vm.net.add@6876 subject="root" object="/vmfs/volumes/668eddb5-b1324e77-6e22-00620b94eaa0/Ubuntu 1/Ubuntu 1.vmx" networkID="VM Network" ip="10.4.25.25" opID="esxui-7a0-caf4" result="success"] <110>1 2024-09-05T22:54:21.831Z - Hostd 2099295 - [vm.net.edit@6876 subject="root" object="/vmfs/volumes/668eddb5-b1324e77-6e22-00620b94eaa0/Ubuntu 1/Ubuntu 1.vmx" networkID="VM Network" connect="at power-on" ip="10.4.25.25" opID="esxui-7a0-caf4" result="success"] <110>1 2024-09-05T22:54:21.830Z - Hostd 2099295 - [vm.reconfigure@6876 subject="root" object="/vmfs/volumes/668eddb5-b1324e77-6e22-00620b94eaa0/Ubuntu 1/Ubuntu 1.vmx" ip="10.4.25.25" opID="esxui-7a0-caf4" result="success"]
Unsuccessful login attempts limit is met or exceeded	**FIA_AFL_EXT.1** <109>1 2024-09-05T23:09:58.802Z - Hostd 2099295 - [vim.connect@6876 subject="test" object="vim" opID="esxcli-b0-cc27" ip="10.4.146.35" reason="Invalid login" result="failure"] <108>1 2024-09-05T23:10:07.399Z - auditAccountLocked 2104780 - [account.locked@6876 subject="test" object="account" ip="10.4.146.35" result="success"]

Administrator authentication attempts	**FIA_UIA_EXT.1** <109>1 2024-09-04T23:21:53.531Z - Hostd 2099293 - [vim.connect@6876 subject="root" object="vim" opID="esxui-dc65-b5c8" ip="10.4.25.35" reason="Invalid login" result="failure"] <110>1 2024-09-04T23:24:49.928Z - Hostd 2099293 - [vim.connect@6876 subject="root" object="vim" opID="ace4b60f" ip="10.4.146.35" uniqueID="52d748bd-b622-fdbe-13b6-4d5237b6abe8" result="success"] <110>1 2024-09-05T21:36:05.549Z - sshd 2101906 - [ssh.connect@6876 subject="root" object="ssh" result="failure" ip="10.4.25.35" reason="AUTH_FAIL_PUBKEY"] <110>1 2024-09-05T21:36:14.696Z - sshd 2101906 - [ssh.connect@6876 subject="root" object="ssh" result="failure" ip="10.4.25.35" reason="AUTH_FAIL_KBDINT"] <110>1 2024-09-05T21:36:19.728Z - sshd 2101906 - [ssh.connect@6876 subject="root" object="ssh" result="success" ip="10.4.25.35" reason="AUTH_SUCCESS"]
All use of the identification and authentication mechanism	**FIA_UIA_EXT.1** <109>1 2024-09-04T23:21:53.531Z - Hostd 2099293 - [vim.connect@6876 subject="root" object="vim" opID="esxui-dc65-b5c8" ip="10.4.25.35" reason="Invalid login" result="failure"] <110>1 2024-09-04T23:24:49.928Z - Hostd 2099293 - [vim.connect@6876 subject="root" object="vim" opID="ace4b60f" ip="10.4.146.35" uniqueID="52d748bd-b622-fdbe-13b6-4d5237b6abe8" result="success"] <110>1 2024-09-05T21:36:05.549Z - sshd 2101906 - [ssh.connect@6876 subject="root" object="ssh" result="failure" ip="10.4.25.35" reason="AUTH_FAIL_PUBKEY"] <110>1 2024-09-05T21:36:14.696Z - sshd 2101906 - [ssh.connect@6876 subject="root" object="ssh" result="failure" ip="10.4.25.35" reason="AUTH_FAIL_KBDINT"] <110>1 2024-09-05T21:36:19.728Z - sshd 2101906 - [ssh.connect@6876 subject="root" object="ssh" result="success" ip="10.4.25.35" reason="AUTH_SUCCESS"]

Start and end of administrator session	**FIA_UIA_EXT.1** <110>1 2024-09-05T23:01:46.405Z - Hostd 2099295 - [vim.connect@6876 subject="root" object="vim" opID="efbecc0f" ip="127.0.0.1" uniqueID="52b50263-fe98-248d-2aeb-c8a2be9b569a" result="success"] <110>1 2024-09-05T23:01:46.429Z - Hostd 2099295 - [vim.disconnect@6876 subject="root" object="vim" opID="efbecc10" ip="127.0.0.1" uniqueID="52b50263-fe98-248d-2aeb-c8a2be9b569a" reason="User logout" result="success"]
Invalid parameter to hypercall detected	**FPT_HCL_EXT.1** <109>1 2024-09-04T14:35:57.322Z - vmx 2413438 - [vm.hypercall.denied@6876 subject="" object="/vmfs/volumes/668eddb5-b1324e77-6e22-00620b94eaa0/Ubuntu 1/Ubuntu 1.vmx" type="Backdoor" value="89" reason="File size of zero" result="failure"]
Hypercall interface invoked when documented preconditions are not met	**FPT_HCL_EXT.1** <109>1 2024-09-10T23:04:51.519Z - vmx 2102457 - [vm.hypercall.denied@6876 subject="" object="/vmfs/volumes/668eddb5-b1324e77-6e22-00620b94eaa0/Ubuntu 2/Ubuntu 2.vmx" type="Backdoor" value="92" reason="ignored due to inappropriate mode" result="failure"] <109>1 2024-09-10T12:59:42.646Z - vmx 2102279 - [vm.hypercall.denied@6876 subject="" object="/vmfs/volumes/668eddb5-b1324e77-6e22-00620b94eaa0/efi_test_vm/niaptest.vmx" type="Backdoor" value="89" reason="Secure boot blocked by admin" result="failure"]

Connection/disconnection of removable media or device to/from a VM	**FPT_RDM_EXT.1** <110>1 2024-09-05T21:47:32.398Z - vmx 2102131 - [vm.usb.connect@6876 subject="" object="/vmfs/volumes/668eddb5-b1324e77-6e22-00620b94eaa0/Ubuntu 1/Ubuntu 1.vmx" name="SanDisk Ultra Fit" vendorID="0781" productID="5583" deviceLabel="ehci:0" type="generic" result="success"] <110>1 2024-09-05T22:29:15.681Z - vmx 2103555 - [vm.usb.disconnect@6876 subject="" object="/vmfs/volumes/668eddb5-b1324e77-6e22-00620b94eaa0/Ubuntu 2/Ubuntu 2.vmx" name="SanDisk Ultra Fit" vendorID="0781" productID="5583" deviceLabel="ehci:0" type="generic" result="success"]
Ejection/insertion of removable media or device from/to an already connected VM	**FPT_RDM_EXT.1** <110>1 2024-09-11T15:34:23.087Z - Hostd 2099424 - [vm.storage.add@6876 subject="root" object="/vmfs/volumes/668eddb5-b1324e77-6e22-00620b94eaa0/Ubuntu 1/Ubuntu 1.vmx" path="/vmfs/volumes/668eddb5-b1324e77-6e22-00620b94eaa0/ubuntu-24.04-desktop-amd64.iso" ip="10.4.25.9" opID="esxui-3c11-05cd" result="success"] <110>1 2024-09-11T22:54:01.088Z - Hostd 2099424 - [vm.storage.remove@6876 subject="root" object="/vmfs/volumes/668eddb5-b1324e77-6e22-00620b94eaa0/Ubuntu 1/Ubuntu 1.vmx" path="" ip="10.4.25.9" opID="esxui-b19-165a" result="success"]
Failure of update signature verification	**FPT_TUD_EXT.1 – Event 2** <106>1 2024-09-09T21:43:38.305Z - esxupdate 2101733 - [system.update.start@6876 subject="root" object="system" result="failure" reason="('VMware_bootbank_vsan_8.0.3-0.30.24262648', 'The VIB VMware_bootbank_vsan_8.0.3-0.30.24262648 does not contain a signature.')"] <106>1 2024-09-09T22:01:18.457Z - esxupdate 2102341 - [system.update.start@6876 subject="root" object="system" result="failure" reason="('VMware_bootbank_vsan_8.0.3-0.30.24262648', 'Invalid PKCS7 digest.')"] <106>1 2024-09-09T22:15:49.349Z - esxupdate 2102624 - [system.update.start@6876 subject="root" object="system" result="failure" reason="('VMware_bootbank_vsan_8.0.3-0.30.24262648', 'Could not find a trusted signer: self-signed certificate')"]

Initiation of trusted channel	**FTP_ITC_EXT.1** <110>1 2024-09-02T23:00:12.765Z - vmsyslogd 2098124 - [syslog.net.open@6876 subject="" object="10.4.146.35:6514" result="success"] <110>1 2024-09-02T23:00:12.825Z - vmsyslogd 2098124 - [syslog.net.link.up@6876 subject="" object="10.4.146.35:6514" result="success"] <110>1 2024-09-11T23:20:54.091Z - Hostd 2099424 - [vim.connect@6876 subject="root" object="vim" opID="c0ab16d6" ip="10.4.146.35" uniqueID="52f224b9-d615-cd3a-9ba2-c72a2b0777d7" result="success"] **FTP_TRP.1** <110>1 2024-09-11T23:20:54.091Z - Hostd 2099424 - [vim.connect@6876 subject="root" object="vim" opID="c0ab16d6" ip="10.4.146.35" uniqueID="52f224b9-d615-cd3a-9ba2-c72a2b0777d7" result="success"]
Termination of trusted channel	**FTP_ITC_EXT.1** <110>1 2024-09-02T23:00:36.069Z - vmsyslogd 2098124 - [syslog.net.close@6876 subject="" object="10.4.146.35:6514" result="success"] <110>1 2024-09-11T23:20:54.108Z - Hostd 2099424 - [vim.disconnect@6876 subject="root" object="vim" opID="c0ab16d9" ip="10.4.146.35" uniqueID="52f224b9-d615-cd3a-9ba2-c72a2b0777d7" reason="User logout" result="success"] **FTP_TRP.1** <110>1 2024-09-11T23:20:54.108Z - Hostd 2099424 - [vim.disconnect@6876 subject="root" object="vim" opID="c0ab16d9" ip="10.4.146.35" uniqueID="52f224b9-d615-cd3a-9ba2-c72a2b0777d7" reason="User logout" result="success"]

Failure of trusted channel functions 1/2	**FTP_ITC_EXT.1** `<109>1 2024-09-02T22:18:33.886Z - envoy 2098920 - [proxy.connect@6876 subject="" object="proxy" result="failure" reason="TLS_error:|268435640:SSL routines:OPENSSL_internal:NO_SHARED_CIPHER" ip="10.4.146.35" port="57784"]` `<109>1 2024-09-02T22:21:12.560Z - envoy 2098920 - [proxy.connect@6876 subject="" object="proxy" result="failure" reason="TLS_error:|268435696:SSL routines:OPENSSL_internal:UNSUPPORTED_PROTOCOL" ip="10.4.146.35" port="60874"]` `<110>1 2024-09-02T22:13:47.848Z - vmsyslogd 2098124 - [syslog.net.link.down@6876 subject="" object="server:50443" result="failure" reason="[SSL: UNKNOWN_CIPHER_RETURNED\] unknown cipher returned (_ssl.c:1006)" subjectDN="Unknown" subjectAltName="Unknown" referenceID="server"]` `<110>1 2024-09-02T22:14:13.607Z - vmsyslogd 2098124 - [syslog.net.link.down@6876 subject="" object="server:50443" result="failure" reason="[SSL: DIGEST_CHECK_FAILED\] digest check failed (_ssl.c:1006)" subjectDN="Unknown" subjectAltName="Unknown" referenceID="server"]` `<110>1 2024-09-02T22:45:17.351Z - vmsyslogd 2098124 - [syslog.net.link.down@6876 subject="" object="server:50443" result="failure" reason="[SSL: CERTIFICATE_VERIFY_FAILED\] certificate verify failed: unable to get local issuer certificate (_ssl.c:1006)" subjectDN="C=US,ST=Texas,O=atsec,OU=PP_VIRTUALIZATION_BASE Test RSA 20240902174502,CN=server" subjectAltName="DNS:server" referenceID="server"]`  `<110>1 2024-09-02T22:56:03.073Z - vmsyslogd 2098124 - [syslog.net.link.down@6876 subject="" object="server:50443" result="failure" reason="[SSL: CERTIFICATE_VERIFY_FAILED\] certificate verify failed: certificate revoked (_ssl.c:1006)" subjectDN="C=US,ST=Texas,O=atsec,OU=PP_VIRTUALIZATION_BASE Test RSA 20240902175549,CN=server" subjectAltName="DNS:server" referenceID="server"]`  `<109>1 2024-09-11T23:20:57.260Z - envoy 2099024 - [proxy.connect@6876 subject="" object="proxy" result="failure" reason="TLS_error:|268435612:SSL routines:OPENSSL_internal:HTTP_REQUEST" ip="10.4.146.35" port="60922"]`

Failure of trusted channel functions 2/2	**FTP_TRP.1** <109>1 2024-09-11T23:20:57.260Z - envoy 2099024 - [proxy.connect@6876 subject="" object="proxy" result="failure" reason="TLS_error:|268435612:SSL routines:OPENSSL_internal:HTTP_REQUEST" ip="10.4.146.35" port="60922"]
Failure to establish a HTTPS session.	**FCS_HTTPS_EXT.1** <109>1 2024-09-02T22:18:33.886Z - envoy 2098920 - [proxy.connect@6876 subject="" object="proxy" result="failure" reason="TLS_error:|268435640:SSL routines:OPENSSL_internal:NO_SHARED_CIPHER" ip="10.4.146.35" port="57784"] <109>1 2024-09-02T22:21:12.560Z - envoy 2098920 - [proxy.connect@6876 subject="" object="proxy" result="failure" reason="TLS_error:|268435696:SSL routines:OPENSSL_internal:UNSUPPORTED_PROTOCOL" ip="10.4.146.35" port="60874"]
Establishment/Termination of an HTTPS session	**FCS_HTTPS_EXT.1** <110>1 2024-09-04T15:52:55.119Z - envoy 2098920 - [proxy.connect@6876 subject="" object="proxy" result="success" ip="10.4.25.15" port="58518"] <110>1 2024-09-04T17:00:55.668Z - envoy 2098920 - [proxy.disconnect@6876 subject="" object="proxy" result="success" ip="10.4.25.15" port="58518"]

Failure to establish a TLS session	**FCS_TLSC_EXT.1** <110>1 2024-09-02T22:13:47.848Z - vmsyslogd 2098124 - [syslog.net.link.down@6876 subject="" object="server:50443" result="failure" reason="[SSL: UNKNOWN_CIPHER_RETURNED\] unknown cipher returned (_ssl.c:1006)" subjectDN="Unknown" subjectAltName="Unknown" referenceID="server"] <110>1 2024-09-02T22:14:13.607Z - vmsyslogd 2098124 - [syslog.net.link.down@6876 subject="" object="server:50443" result="failure" reason="[SSL: DIGEST_CHECK_FAILED\] digest check failed (_ssl.c:1006)" subjectDN="Unknown" subjectAltName="Unknown" referenceID="server"] **FCS_TLSS_EXT.1** <109>1 2024-09-02T22:18:33.886Z - envoy 2098920 - [proxy.connect@6876 subject="" object="proxy" result="failure" reason="TLS_error:|268435640:SSL routines:OPENSSL_internal:NO_SHARED_CIPHER" ip="10.4.146.35" port="57784"] <109>1 2024-09-02T22:21:12.560Z - envoy 2098920 - [proxy.connect@6876 subject="" object="proxy" result="failure" reason="TLS_error:|268435696:SSL routines:OPENSSL_internal:UNSUPPORTED_PROTOCOL" ip="10.4.146.35" port="60874"]
Failure to verify presented TLS identifier	**FCS_TLSC_EXT.1** <110>1 2024-09-02T22:45:17.351Z - vmsyslogd 2098124 - [syslog.net.link.down@6876 subject="" object="server:50443" result="failure" reason="[SSL: CERTIFICATE_VERIFY_FAILED\] certificate verify failed: unable to get local issuer certificate (_ssl.c:1006)" subjectDN="C=US,ST=Texas,O=atsec,OU=PP_VIRTUALIZATION_BASE Test RSA 20240902174502,CN=server" subjectAltName="DNS:server" referenceID="server"] <110>1 2024-09-02T22:56:03.073Z - vmsyslogd 2098124 - [syslog.net.link.down@6876 subject="" object="server:50443" result="failure" reason="[SSL: CERTIFICATE_VERIFY_FAILED\] certificate verify failed: certificate revoked (_ssl.c:1006)" subjectDN="C=US,ST=Texas,O=atsec,OU=PP_VIRTUALIZATION_BASE Test RSA 20240902175549,CN=server" subjectAltName="DNS:server" referenceID="server"]

Establishment/Termination of a TLS session	**FCS_TLSC_EXT.1** <110>1 2024-09-02T23:00:12.765Z - vmsyslogd 2098124 - [syslog.net.open@6876 subject="" object="10.4.146.35:6514" result="success"] <110>1 2024-09-02T23:00:36.069Z - vmsyslogd 2098124 - [syslog.net.close@6876 subject="" object="10.4.146.35:6514" result="success"]
Failure To validate a certificate	**FIA_X509_EXT.1** <110>1 2024-09-02T22:45:17.351Z - vmsyslogd 2098124 - [syslog.net.link.down@6876 subject="" object="server:50443" result="failure" reason="[SSL: CERTIFICATE_VERIFY_FAILED\] certificate verify failed: unable to get local issuer certificate (_ssl.c:1006)" subjectDN="C=US,ST=Texas,O=atsec,OU=PP_VIRTUALIZATION_BASE Test RSA 20240902174502,CN=server" subjectAltName="DNS:server" referenceID="server"] <110>1 2024-09-02T22:56:03.073Z - vmsyslogd 2098124 - [syslog.net.link.down@6876 subject="" object="server:50443" result="failure" reason="[SSL: CERTIFICATE_VERIFY_FAILED\] certificate verify failed: certificate revoked (_ssl.c:1006)" subjectDN="C=US,ST=Texas,O=atsec,OU=PP_VIRTUALIZATION_BASE Test RSA 20240902175549,CN=server" subjectAltName="DNS:server" referenceID="server"]

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

vmware by Broadcom