VMware, Inc.
3401 Hillview Ave, Palo Alto, CA 94304, USA, Tel: (877) 486-9273, www.vmware.com

Guidance Supplement
Appendix A: Audit Events

VMware ESXi 6.7 Update 2

Common Criteria (CC) Evaluation with Protection Profile (PP) for Virtualization Version 1.0 with Server Virtualization Extended Package (EP) 1.0

Document Version: 1.0
Document Date: April 30, 2019

vmware®

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

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

VMware Security Advisories, Certifications and Guides

http://www.vmware.com/security

VMware Security Response Center

http://www.vmware.com/support/policies/security_response.html

security@vmware.com

REVISION HISTORY

Ver #	Description of changes	Modified by	Date
1.0	Initial release of document		April 30, 2019

APPENDIX A: AUDIT EVENTS

1.1 Introduction to audit record eventIDs

The subject of an audit eventID is the user associated with the eventide. When a daemon logs an audit message -- not due to a user's action -- the subject is "" (empty string) since the "system" did it.

The object of an audit event specifies the object involved in the operation (e.g. the path of a VMX file for identifying a VM) or "" (empty string) when no specific object is involved.

A comment parameter, unless specifically required by an eventID, is considered optional.

1.2 List of eventIDs

1.2.1 access.denied

This event is generated whenever an attempt to access a protected object is denied (e.g. system login, file access).

- The subject shall be the user that was denied access to the system if known.
- The object shall be the managed object on which the operation was invoked, in format <type:MoID>, e.g. "vim.HostSystem:ha-host".
- The result shall be "failure" since we track only unauthorized calls.
- The ip is the IP address from where the request is coming.
- The operation describes the API name, e.g. "GetHardware".
- The path contains the VMX file path if the target is a virtual machine, or the datastore name if the target object is a datastore.
- The reason, if present, shall describe additional details about the event.

1.2.2 audit.failure

This event is generated upon audit daemon restart after the audit daemon previously suffered a failure (e.g. unable to write to storage, networking link down, file system errors, etc.) and was unable to generate an audit record. This indicates that a loss of audit records may have occurred.

- The subject shall be "" (no user associated; the host itself).
- The object shall be "" (no user associated; the host itself).
- The result shall be "failure".

1.2.3 audit.network

This event is generated when the networking link to the external audit log record collector changes state. The "link down" transition records will only be found in the local storage.

- The subject shall be "" (no user associated; the host itself).
- The object shall be "" (no user associated; the host itself).
- When the link transitions from "up" to "down":
    - The result shall be "failure".

    - The reason shall be "link down".
- When the link transitions from "down" to "up":
    - The result shall be "success".
    - The reason shall be "link up".

1.2.4 audit.recycle

This event is generated when auditing returns to the beginning of its local storage.

- The subject shall be "" (no user associated; the host itself).
- The object shall be "" (no user associated; the host itself).
- The result shall be "success".

1.2.5 audit.start

This event is generated when auditing begins accepting audit records.

- The subject shall be "" (no user associated; the host itself).
- The object shall be "" (no user associated; the host itself).
- The result shall be "success".

1.2.6 audit.stop

This event is generated when auditing ceases to accept audit records.

- The subject shall be "" (no user associated; the host itself).
- The object shall be "" (no user associated; the host itself).
- The result shall be "success".
- The reason, if present, shall explain the reason for the stoppage.

1.2.7 https.connect

This event is generated when an HTTPS connection is made with the host.

- The subject shall be "" (no user associated; the host itself).
- The object shall be "" (no user associated; the host itself).
- The result shall be "success" or "failure"
- The ip shall be address of the remote peer trying to establish the connection
- The reason shall describe the reason for the failure or any side notes on the event.

1.2.8 https.disconnect

This event is generated when an HTTPS connection ends with the host.

- The subject shall be "" (no user associated; the host itself).
- The object shall be "" (no user associated; the host itself).
- The result shall be "success"
- The ip shall be address of the remote peer which is disconnecting

1.2.9 hypercall.access

This event is generated when a VM attempts to issue a hypercall that has been disabled.

- The subject shall be "" (no user associated; the host itself).
- The object shall be the path of the VMX file of the reporting VM
- The result shall be "failure"
- The reason shall describe the reason for the failure, including the hypercall interface which failed.

1.2.10 invalid.message

This event is generated when an event and its parameters prove problematic. Parameters from the problematic event form the body of this event in hopes that the information is sufficient to determine where the problem was created.

- If the eventID is valid, the VMW_PARAM_EVENTID parameter is present.
- Invalid parameter names are replaced with VMW_PARAM_BAD.
- Invalid parameter values (including subject and object values) are replaced with "" (the empty string).
- Any number of VMW_PARAM_REASON parameters will be present (including none).
- The result shall be "failure".

1.2.11 login.connect

This event is generated whenever an attempt is made to login into the system.

- The subject shall be the user authenticating with the system.
- The object shall be empty string.
- The result shall be "success" or "failure".
- The hostname is the name of the system whence the login originates, if present.
- The ip is the IP address from where the request is coming.
- The URL describes the URL of the authentication request if applicable, e.g. for CGI requests.
- The reason, if present, describes the reason for the failure.

1.2.12 login.disconnect

This event is generated when a logout occurs (explicit or time out).

- The subject shall be the user authenticating with the system.
- The object shall be empty string.
- The result shall be "success" or "failure".
- The hostname is the name of the system whence the login originates, if present.
- The ip is the IP address from where the request is coming.
- The URL describes the URL of the authentication request if applicable, e.g. for CGI requests.
- The reason, if present, shall describe additional details about the event.

1.2.13 mark

This event is generated whenever an admin explicitly requests this eventvia the command:
`esxcli system syslog mark -s "event message"`

- The subject shall be "userName" (the name of the user sending the mark)
- The object shall be "" (no user associated; the host itself).

- The result shall be "success".
- A "comment" parameter shall be present. The value may be an empty string.

1.2.14 network.add

This event is generated when a virtual network connection is attached to a virtual machine.

- The subject shall be the user name who configured this virtual network device.
- The object shall be the path of the VMX file of the affected VM.
- The result shall be "success" or "failure".
- The networkID shall be an identifier for the virtual network to which the affected virtual NIC is attached. This identifier may be a name or UUID, depending on the virtual network type.

1.2.15 network.edit

This event is generated when a change occurs to the virtual network connection associated with a virtual machine.

- The subject shall be the user name who configured this virtual network device.
- The object shall be the path of the VMX file of the affected VM.
- The result shall be "success" or "failure".
- The networkID shall be an identifier for the virtual network to which the affected virtual NIC is attached. This identifier may be a name or UUID, depending on the virtual network type.
- The oldID shall be an identifier for the old network from which a given NIC is detached or "" (empty string) when a change does not affect the network identifier.
- The status shall be "connected" or "disconnected" when a change affects device connectivity.

1.2.16 network.remove

This event is generated when a virtual network connection is removed from a virtual machine.

- The subject shall be the user name who configured this virtual network device.
- The object shall be the path of the VMX file of the affected VM.
- The result shall be "success" or "failure".
- The networkID shall be an identifier for the virtual network to which the affected virtual NIC is detached. This identifier may be a name or UUID, depending on the virtual network type.

1.2.17 rbg.entropy.failure

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

- The subject shall be "" (no user associated; the host itself).
- The object shall be "" (no user associated; the host itself).
- The result shall be "failure".
- The reason shall indicate whether the failure was due to a test.

1.2.18 storage.add

This event is generated when a virtual device is added to a VM.

- The subject shall be the user name who configured this virtual storage device.

- The object shall be the path of the VMX file of the affected VM.
- The result shall be "success" or "failure".
- The path shall be the path to the affected file or "" (empty string) when a local device is auto selected (e.g. CDROM).

1.2.19 storage.edit

This event is generated when the object (e.g. file, device) associated with a virtual device is changed.

- The subject shall be the user name who configured this virtual storage device.
- The object shall be the path of the VMX file of the affected VM.
- The result shall be "success" or "failure".
- The oldPath shall be the path to the detached file or "" (empty string) when a local device is auto selected (for example, CDROM).
- The path shall be the path to the attached file or "" (empty string) when a local device is auto selected (for example, CDROM).
- The status shall be "connected" or "disconnected" when a change affects device connectivity (for example, CDROM).

1.2.20 storage.remove

This event is generated when a virtual device is removed from a VM.

- The subject shall be the user name who configured this virtual storage device.
- The object shall be the path of the VMX file of the affected VM.
- The result shall be "success" or "failure".
- The path shall be the path to the affected file or "" (empty string) when a local device is auto selected (for example, CDROM).

1.2.21 system.update.end

This event is generated upon the completion of a system update.

- The subject shall be the userName of the person requesting the update
- The object shall be "" (no user associated; the host itself).
- The result shall be "success" or "failure"
- The vib shall be the identifying information of the update
- The reason shall describe the reason for the failure or any side notes on the event.

1.2.22 system.update.start

This event is generated when a system update is initiated.

- The subject shall be the userName of the person requesting the update
- The object shall be "" (no user associated; the host itself).
- The result shall be "success" or "failure"
- The vib shall be the identifying information of the update
- The reason shall describe the reason for the failure or any side notes on the event.

1.2.23 ticket.get

This event is generated when a ticket is requested from the host.

- The subject shall be the user requesting a ticket.

- The object shall be the ticket ID with most of its fileds masked out.
- The result shall be "success". We don't log failures here.
- The ip is the IP address from where the request is coming.
- The URL describes the URL the ticket was acquired for.
- The HTTP.method contains the HTTP method the ticket was acquired for or empty string if not specified.

1.2.24 ticket.use

This event is generated when a previously requested ticket is used by the host.

- The subject shall be the user associated with the ticket if the ticket is valid.
- The object shall be the ticket ID with most of its fileds masked out.
- The result shall be "success" or "failure".
- The ip is the IP address of the incoming request.
- The URL describes the URL path of the incoming request.
- The HTTP.method contains the HTTP method of the incoming request.
- The reason describes the reason for the failure.

1.2.25 tls.client.connect

This event is generated when a TLS connection is initiated.

- The subject shall be “” (empty string) as the connection is initiated by the ESXi system.
- The object shall be the network address (DNS, IPv4 or IPv6) of the remote server.
- The result shall be "success" or "failure".
- The reason is optional and shall describe any additional details about the event.

1.2.26 tls.client.disconnect

This event is generated when a TLS connection is terminated.

- The subject shall be “” (empty string) as the connection is initiated by the ESXi system.
- The object shall be the network address (DNS, IPv4 or IPv6) of the remote server.
- The result shall be "success" or "failure".
- The reason is optional and shall describe any additional details about the event.

1.2.27 usb.connect

This event is generated when a USB device is connected to a VM.

- The subject shall be "" (no user associated; the host itself).
- The object shall be the path of the VMX file of the reporting VM
- The deviceLabel shall be usb:<N> for usb 1.1; ehci:<N> for usb 2.0; or usb_xhci:<N> for usb 3.x
- The vid shall be the vendor ID of the device
- The pid shall be the product ID of the device
- The result shall be "success" or "failure"
- The reason shall describe the reason for the failure

1.2.28 usb.disconnect

This event is generated when a USB device is disconnected from a VM.

- The subject shall be "" (no user associated; the host itself).

- The object shall be the path of the VMX file of the reporting VM
- The deviceLabel shall be usb:<N> for usb 1.1; ehci:<N> for usb 2.0; or usb_xhci:<N> for usb 3.x
- The vid shall be the vendor ID of the device
- The pid shall be the product ID of the device
- The result shall be "success" or "failure"
- The reason shall describe the reason for the failure

1.2.29 x509.cacert.add

This event is generated when a CA certificate is added to the host Certificate Authority store.

- The subject shall be the user authenticating with the system.
- The object shall be “” (empty string) as the host Certificate Authority store is unique.
- The result shall be "success" or "failure".
- The subjectDN shall be the Distinguished Name of the CA certificate.
- The reason, if present, describes additional details about the event.

1.2.30 x509.cacert.remove

This event is generated when a CA certificate is removed from the host CA store.

- The subject shall be the user authenticating with the system.
- The object shall be “” (empty string) as the host Certificate Authority store is unique.
- The result shall be "success" or "failure".
- The subjectDN shall be the distinguished name of the CA certificate.
- The reason, if present, describes additional details about the event.