VMware ESX Audit Log Event Reference

October 24, 2025

VMware Cloud Foundation 9.0
VMware ESX 9.0

vmware by Broadcom

Table of Contents

Disclaimer

This document is intended to provide general guidance for organizations that are considering Broadcom solutions. The information contained in this document is for educational and informational purposes only. This document is not intended to provide advice and is provided “AS IS.” Broadcom makes no claims, promises, or guarantees about the accuracy, completeness, or adequacy of the information contained herein. Organizations should engage appropriate legal, business, technical, and audit expertise within their specific organization for review of requirements and effectiveness of implementations.

Introduction

This reference provides information about the audit records generated by VMware ESX in response to various security-related system events. This document also includes the parameters associated with each event. These audit records can be accessed locally on VMware ESX and can also be sent to remote log collectors. Both local storage and remote transmission are configurable capabilities of VMware ESX.

Download the Latest Version

Guidance does evolve as product releases occur. The most up-to-date version of this document can be found at:

https://brcm.tech/vcf-security

or for redirection-unfriendly environments, in the Features/Logging section of our GitHub repository:

https://github.com/vmware/vcf-security-and-compliance-guidelines

That repository also contains numerous additional resources to help your security and compliance efforts.

Security Hardening & Design

This document does not make specific security hardening recommendations. For baseline security guidance please consult the Security Configuration & Hardening Guides at https://github.com/vmware/vcf-security-and-compliance-guidelines

Feedback

The primary source for this document is within our repository at:

https://github.com/vmware/vcf-security-and-compliance-guidelines

Feedback and issues can be filed through the Issues mechanism in that repository or through your account team.

VMware ESXi versus VMware ESX

With the release of VMware Cloud Foundation 9.0 the name of the VMware Hypervisor was changed from ESXi back to ESX. Documents such as this, which use information that span a range of release versions, may use the names ESXi and ESX interchangeably, or refer to the hypervisor solely as ESX for simplicity. Unless you are running VMware vSphere 4.1, please consider both ESXi and ESX to be the same, and use the product version to determine applicability to your environment.

Enabling Audit Logging

Audit records are sent to the ESX vmsyslogd daemon for processing. Each record has a timestamp, the name of the reporting process, the PID of the reporting process, a syslog facility of 13 (audit), and a syslog severity (level) that is appropriate for the record. The vmsyslogd daemon, if enabled to do so, will store audit records locally and transmit audit records to external collectors (remote hosts). When transmitted, audit records also contain the name of the system from which they originated.

Audit logs on ESX are controlled by an additional set of parameters beyond traditional log forwarding. There is an order of operations for configuring these settings, and the parameters are listed in that order:

Syslog.global.logHost

A comma-delimited list of remote logging endpoints to forward logs, including audit logs. Should be formatted with the protocol and port number, such as tcp://hostname:514, udp://hostname:514, or ssl://hostname:1514.

Syslog.global.auditRecord.storageDirectory

Specifies the local ESX filesystem where audit logs will reside. By default, this will be set to /scratch/auditlog, which may be either a persistent filesystem or an in-memory filesystem, depending on the boot device for ESX.

You can detect if the scratch volume is temporary or persistent by querying the ScratchConfig.CurrentScratchLocation advanced parameter. If, when queried, it returns "/tmp/scratch" then the volume is temporary, and you should remap the audit record storage to a persistent device. USB and SD cards used as boot media should not be used as persistent devices as logging will wear them out.

If your only persistent device is a vSAN datastore you will need to configure syslog.global.vsanBacking to “TRUE” as well.

This parameter must be configured before enabling audit logging. To change it, disable audit logging.

Syslog.global.auditRecord.storageCapacity

Specifies the capacity of the audit record storage directory, in MiB. **You cannot decrease this allocation once set**. However, it can be grown at any time. By default it is set to 4 and is recommended that it be set to 100.

Syslog.global.auditRecord.storageEnable

Enables the local storage of audit records, into the directory specified by **s**yslog.global.auditRecord.storageDirectory. For best results configure the storage directory and the storage capacity before enabling audit logging.

This value is Boolean, TRUE or FALSE.

Syslog.global.auditRecord.remoteEnable

Enables the transmission of audit records to the log hosts specified in Syslog.global.logHost.

This value is Boolean, TRUE or FALSE.

PowerCLI Examples

VMware PowerCLI can be used to change these settings across multiple machines. As an example, this command will change a specific host’s log host setting:

```
Get-VMHost -Name $ESX | Get-AdvancedSetting Syslog.global.logHost | Set-AdvancedSetting -Value “tcp://hostname:514”
```

Or change all hosts (be careful!):

```
Get-VMHost | Get-AdvancedSetting Syslog.global.logHost | Set-AdvancedSetting -Value “tcp://hostname:514”
```

VMware PowerCLI is easy to use and learn. For more information visit https://developer.broadcom.com.

Additional Log Parameters

There are additional log handling parameters, please see the “ESX Syslog Options” chapter in the product documentation.

Audit Log Format

Audit logs are structured according to RFC 5424, and take the format:

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

RFC 5424 specifies that an SD-NAME must be a non-empty ASCII string which excludes whitespace, '=', ']', '"', and all control characters. It must be 32 characters or less in length.

“eventID@6876” is an RFC 5424 SD-ID (an SD-NAME). It consists of two parts: a name (which is used for the eventID) which additionally cannot contain an at-sign ('@'), and the VMware IANA private enterprise number of 6876, separated from the name by an at-sign ('@'). VMware restricts the length of the eventID such that the total SD-ID length is less than the maximum.

“paramName” is an RFC 5424 PARAM-NAME (an SD-NAME). The same paramName may be specified for multiple paramName="paramValue" entries.

“paramValue” is an RFC 5424 PARAM-VALUE, a UTF8 string. If the string contains '"' (double quotation mark), '\' (backslash), or ']' (right bracket), these characters will be escaped with a preceding backslash ('\'). A paramValue can be of any "reasonable" length (e.g. path names may be used). Note that a backslash followed by a character other than these characters is not an error from the standpoint of validation.

For example:

[syslog.mark@6876 subject="userName" object="syslog" result="success" comment="string"]

The order of parameters within the square brackets may change at any time. Do not depend on parameters having any specific order.

References

For more information on audit records, see the “Audit Records” subsection of the “Log File Formats” chapter of the product documentation.

For more information on configuring ESX log settings, visit the “ESX Syslog Options” chapter in the product documentation.

Logging inside VMware vSphere and VMware Cloud Foundation is standards-based and governed by several RFCs:

- RFC 3164: https://tools.ietf.org/html/rfc3164. Legacy (advisory) syslog format. Section 4.1.1 describes the PRI part (facility and severity) and also lists the numerical mappings (https://tools.ietf.org/html/rfc3164#section-4.1.1).
- RFC 3339: Date and Time on the Internet: Timestamps https://tools.ietf.org/html/rfc3339
- RFC 5234: Augmented BNF for Syntax Specifications: ABNF https://tools.ietf.org/html/rfc5234
- RFC 5424: https://tools.ietf.org/html/rfc5424. New syslog format. Section 6.2.1 describes the PRI part (facility and severity), and also lists the numerical mappings (https://tools.ietf.org/html/rfc5424#section-6.2.1) which clarifies that the "audit" is number 13.
- RFC 5425: Transport Layer Security (TLS) Transport Mapping for Syslog https://tools.ietf.org/html/rfc5425
- RFC 5427: https://tools.ietf.org/html/rfc5427. This describes the facility and severity names and numerical mappings.
- RFC 6587: Transmission of Syslog Messages over TCP [legacy] https://tools.ietf.org/html/rfc6587
- IANA Private Enterprise Numbers: https://www.iana.org/assignments/enterprise-numbers/enterprise-numbers. Catalog of all the private enterprise numbers when specifying the structured data. From the doc, the VMware private enterprise number is 6876.

Testing of log output can be done from the ESX command line. Please see the relevant Knowledge Base article (KB 342571).

Audit Events

account.changePassword

This event is generated when an attempt was made to change the password of a user account.

Severity

Success: Info
Failure: Notice

Parameters

Parameter	Description	Presence
subject	The name of the user who requested the operation.	Optional
object	The name of the target account.	Always present
result	"success" or "failure"	Always present
reason	Present when result is "failure" and indicates the reason for the failure.	Present when result is "failure"
ip	The network address of the originator of the operation.	Optional
opID	The operation ID.	Optional
comment	Provides additional information about the event.	Optional

account.create

This event is generated when an attempt was made to create a user account.

Severity

Success: Info

Failure: Notice

Parameters

Parameter	Description	Presence
subject	The name of the user who requested the operation.	Always present
object	The name of the new account.	Always present
result	"success" or "failure"	Always present
reason	Present when result is "failure" and indicates the reason for the failure.	Present when result is "failure"
ip	The network address of the originator of the operation.	Always present
opID	The operation ID.	Optional

account.delete

This event is generated when an attempt was made to delete a user account.

Severity

Success: Info

Failure: Notice

Parameters

Parameter	Description	Presence
subject	The name of the user who requested the operation.	Always present
object	The name of the target account.	Always present
result	"success" or "failure"	Always present
reason	Present when result is "failure" and indicates the reason for the failure.	Present when result is "failure"
ip	The network address of the originator of the operation.	Always present
opID	The operation ID.	Optional

account.edit

This event is generated when an attempt was made to edit an existing user account.

Severity

Success: Info

Failure: Notice

Parameters

Parameter	Description	Presence
subject	The name of the user who requested the operation.	Always present
object	The name of the target account.	Always present
result	"success" or "failure"	Always present
reason	Present when result is "failure" and indicates the reason for the failure.	Present when result is "failure"
ip	The network address of the originator of the operation.	Always present
opID	The operation ID.	Optional

account.locked

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

Severity

Success: Warning
Failure: Notice

Parameters

Parameter	Description	Presence
subject	The name of the user whose account was locked.	Always present
object	The value is always "account"	Always present
result	The value is always "success"	Always present

api.call

This event is generated when an attempt was made to call an API.

Severity

Success: Debug
Failure: Notice

Parameters

Parameter	Description	Presence
subject	The name of the user who requested the operation. For an operation initiated by the system, rather than a user, the subject is the defined value indicating activity performed by the system rather than a user. The subject may also be an empty string for operations initiated by a user anonymously (that is, operations that have the System.anonymous required privilege).	Always present
object	The name of the object and the method on which the operation is invoked (e.g. "vmodl.query.PropertyCollector.createFilter", "vim.EnvironmentBrowser.queryConfigOptionDescriptor", "vim.VirtualMachine.powerOn"). Consult the vSphere Web Servies API documentation for more information. Note that some objects are undocumented since they are internal-use only.	Always present
result	"success" or "failure"	Always present

audit.failure

This event is generated upon audit daemon restart after the audit daemon suffered a catastrophic failure. This indicates that a loss of audit records may have occurred.

Severity

Success: Info
Failure: Alert

Parameters

Parameter	Description	Presence
subject	The defined value indicating activity performed by the system rather than a user.	Always present
object	The value is always "audit”	Always present
result	The value is always "failure”	Always present
reason	The value is always "potential loss of audit records due to daemon crash”	Always present

audit.net.failure

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

Severity

Success: Info

Failure: Alert

Parameters

Parameter	Description	Presence
subject	The defined value indicating activity performed by the system rather than a user.	Always present
object	The affected remote host.	Always present
result	The value is always "failure"	Always present
reason	Reason for the network failure.	Always present

audit.start

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

Severity

Success: Info

Failure: Notice

Parameters

Parameter	Description	Presence
subject	The defined value indicating activity performed by the system rather than a user.	Always present
object	The value is always "audit”	Always present
result	The value is always "success”	Always present
directory	The path to the audit record storage area.	Always present
capacity	The storage capacity of the audit record storage area in MiB.	Always present

audit.stop

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

Severity

Success: Info

Failure: Notice

Parameters

Parameter	Description	Presence
subject	The defined value indicating activity performed by the system rather than a user.	Always present
object	The value is always "audit”	Always present
result	The value is always "success”	Always present

audit.storage.failure

This event is generated when an I/O error occurred while writing audit record storage. This indicates that a loss of audit records may have occurred.

Severity

Success: Info
Failure: Alert

Parameters

Parameter	Description	Presence
subject	The defined value indicating activity performed by the system rather than a user.	Always present
object	The audit record storage file where the I/O error occurred.	Always present
result	The value is always "failure”	Always present
reason	The value is always "I/O error”	Always present

audit.storage.recycle

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

Severity

Success: Info

Failure: Notice

Parameters

Parameter	Description	Presence
subject	The defined value indicating activity performed by the system rather than a user.	Always present
object	The value is always "audit”	Always present
result	The value is always "success”	Always present

cert.castore.add

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

Severity

Success: Info

Failure: Notice

Parameters

Parameter	Description	Presence
subject	The name of the user who requested the operation.	Always present
object	The value is always "cert"	Always present
result	"success" or "failure"	Always present
reason	Provides additional details about the event.	Optional
ip	The network address of the originator of the operation.	Optional
subjectDN	The subject distinguished name of the CA certificate.	Always present
opID	The operation ID.	Optional

cert.castore.remove

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

Severity

Success: Info

Failure: Notice

Parameters

Parameter	Description	Presence
subject	The name of the user who requested the operation.	Always present
object	The value is always "cert"	Always present
result	"success" or "failure"	Always present
reason	Provides additional details about the event.	Optional
subjectDN	The subject distinguished name of the CA certificate.	Always present
ip	The network address of the originator of the operation.	Optional
opID	The operation ID.	Optional

cert.client.generate

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

Severity

Success: Info

Failure: Notice

Parameters

Parameter	Description	Presence
subject	The name of the user who requested the operation.	Always present
object	The value is always "cert"	Always present
result	"success" or "failure"	Always present
reason	Provides additional details about the event.	Optional
ip	The network address of the originator of the operation.	Optional
opID	The operation ID.	Optional
type	Describes the type of client for which the signing request was generated.	Always present

cert.client.install

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

Severity

Success: Info

Failure: Notice

Parameters

Parameter	Description	Presence
subject	The name of the user who requested the operation.	Always present
object	The value is always "cert"	Always present
result	"success" or "failure"	Always present
reason	Provides additional details about the event.	Optional
subjectDN	The subject distinguished name of the server certificate.	Optional
ip	The network address of the originator of the operation.	Optional
opID	The operation ID.	Optional
type	Describes the type of client for which the signing request was generated. The value is "VASAClient"	Always present

cert.server.generate

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

Severity

Success: Info

Failure: Notice

Parameters

Parameter	Description	Presence
subject	The name of the user who requested the operation.	Always present
object	The value is always "cert"	Always present
result	"success" or "failure"	Always present
reason	Provides additional details about the event.	Optional
ip	The network address of the originator of the operation.	Optional
opID	The operation ID.	Optional

cert.server.install

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

Severity

Success: Info

Failure: Notice

Parameters

Parameter	Description	Presence
subject	The name of the user who requested the operation.	Always present
object	The value is always "cert"	Always present
result	"success" or "failure"	Always present
reason	Provides additional details about the event.	Optional
subjectDN	The subject distinguished name of the server certificate.	Optional
ip	The network address of the originator of the operation.	Optional
opID	The operation ID.	Optional

cert.server.provision

This event is generated when an attempt was made to provision a server private key.

Severity

Success: Info

Failure: Notice

Parameters

Parameter	Description	Presence
subject	The name of the user who requested the operation.	Always present
object	The value is always "cert"	Always present
result	"success" or "failure"	Always present
reason	Provides additional details about the event.	Optional
ip	The network address of the originator of the operation.	Optional
opID	The operation ID.	Optional

configenc.reqeio.disable

This event is generated when an attempt was made to disable the execInstalledOnly requirement for config encryption.

Severity

Success: Info

Failure: Notice

Parameters

Parameter	Description	Presence
subject	The name of the user who requested the operation.	Always present
object	The value is always "configenc"	Always present
result	"success" or "failure"	Always present
reason	Present when result is "failure" and indicates the reason for the failure.	Present when result is "failure"
ip	The network address of the originator of the operation.	Always present
opID	The operation ID.	Always present

configenc.reqeio.enable

This event is generated when an attempt was made to enable the execInstalledOnly requirement for config encryption.

Severity

Success: Info

Failure: Notice

Parameters

Parameter	Description	Presence
subject	The name of the user who requested the operation.	Always present
object	The value is always "configenc"	Always present
result	"success" or "failure"	Always present
reason	Present when result is "failure" and indicates the reason for the failure.	Present when result is "failure"
ip	The network address of the originator of the operation.	Always present
opID	The operation ID.	Always present

configenc.reqsb.disable

This event is generated when an attempt was made to disable the Secure Boot requirement for config encryption.

Severity

Success: Info

Failure: Notice

Parameters

Parameter	Description	Presence
subject	The name of the user who requested the operation.	Always present
object	The value is always "configenc"	Always present
result	"success" or "failure"	Always present
reason	Present when result is "failure" and indicates the reason for the failure.	Present when result is "failure"
ip	The network address of the originator of the operation.	Always present
opID	The operation ID.	Always present

configenc.reqsb.enable

This event is generated when an attempt was made to enable the Secure Boot requirement for config encryption.

Severity

Success: Info

Failure: Notice

Parameters

Parameter	Description	Presence
subject	The name of the user who requested the operation.	Always present
object	The value is always "configenc"	Always present
result	"success" or "failure"	Always present
reason	Present when result is "failure" and indicates the reason for the failure.	Present when result is "failure"
ip	The network address of the originator of the operation.	Always present
opID	The operation ID.	Always present

configenc.tpm.enable

This event is generated when an attempt was made to enable TPM mode for config encryption.

Severity

Success: Info

Failure: Notice

Parameters

Parameter	Description	Presence
subject	The name of the user who requested the operation.	Always present
object	The value is always "configenc"	Always present
result	"success" or "failure"	Always present
reason	Present when result is "failure" and indicates the reason for the failure.	Present when result is "failure"
ip	The network address of the originator of the operation.	Always present
opID	The operation ID.	Always present

dcui.login

This event is generated when an attempt was made to log in via the DCUI.

Severity

Success: Info

Failure: Notice

Parameters

Parameter	Description	Presence
subject	The name of the user who attempted to log in.	Always present
object	The value is always "dcui"	Always present
result	"success" or "failure"	Always present
reason	Present when result is "failure" and indicates the reason for the failure.	Present when result is "failure"

dcui.logout

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

Severity

Success: Info

Failure: Notice

Parameters

Parameter	Description	Presence
subject	The name of the user associated with the login.	Always present
object	The value is always "dcui"	Always present
result	"success" or "failure"	Always present
reason	Present when result is "failure" and indicates the reason for the failure.	Present when result is "failure"

entropy.data.exhausted

This event is generated when entropy in the memory and storage cache is exhausted.

Severity

Success: Info

Failure: Notice

Parameters

Parameter	Description	Presence
subject	The defined value indicating activity performed by the system rather than a user.	Always present
object	The value is always "entropy”	Always present
result	The value is always "failure”	Always present
reason	Indicates the reason for the failure.	Always present

entropy.data.received

This event is generated when the external entropy source provides entropy. It is generated the first time entropy is received, and also the first time after a timeout.

Severity

Success: Info
Failure: Notice

Parameters

Parameter	Description	Presence
subject	The user name specified by the external entropy source.	Always present
object	The IP address of the external entropy source.	Always present
result	The value is always "success"	Always present

entropy.data.timeout

This event is generated when the external entropy source does not provide entropy within the configured timeout period.

Severity

Success: Warning
Failure: Notice

Parameters

Parameter	Description	Presence
subject	The user name specified by the external entropy source.	Optional
object	The IP address of the external entropy source.	Optional
result	The value is always "success"	Always present
comment	Provides information about the event.	Optional

entropy.failure

This event is generated upon entropyd daemon restart after the daemon suffered a catastrophic failure (e.g. after the daemon or ESX crashed). It indicates that the daemon was not shut down quiesently.

Severity

Success: Info
Failure: Notice

Parameters

Parameter	Description	Presence
subject	The defined value indicating activity performed by the system rather than a user.	Always present
object	The value is always "entropy”	Always present
result	The value is always "failure”	Always present
reason	Indicates the reason for the failure.	Always present

entropy.memory.exhausted

This event is generated when entropy in the memory cache is exhausted.

Severity

Success: Info

Failure: Notice

Parameters

Parameter	Description	Presence
subject	The defined value indicating activity performed by the system rather than a user.	Always present
object	The value is always "entropy”	Always present
result	The value is always "failure”	Always present
reason	Indicates the reason for the failure.	Always present

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.

Severity

Success: Info
Failure: Alert

Parameters

Parameter	Description	Presence
subject	The defined value indicating activity performed by the system rather than a user.	Always present
object	"entropy"	Always present
result	The value is always "failure"	Always present
reason	Indicates the reason for the failure. When testing for entropy failure, the reason is "test"	Always present

entropy.start

This event is generated when the entropy daemon starts.

Severity

Success: Info
Failure: Notice

Parameters

Parameter	Description	Presence
subject	The defined value indicating activity performed by the system rather than a user.	Always present
object	The value is always "entropy”	Always present
result	"success" or "failure”	Always present
reason	Present when the result is failure and indicates the reason for the failure.	Present when the result is failure

entropy.stop

This event is generated when the entropy daemon stopped.

Severity

Success: Info

Failure: Notice

Parameters

Parameter	Description	Presence
subject	The defined value indicating activity performed by the system rather than a user.	Always present
object	The value is always "entropy”	Always present
result	The value is always "success”	Always present

entropy.watermark.above

This event is generated when the amount of available entropy data has risen above the low water mark.

Severity

Success: Info

Failure: Notice

Parameters

Parameter	Description	Presence
subject	The defined value indicating activity performed by the system rather than a user.	Always present
object	The value is always "entropy”	Always present
result	The value is always "success”	Always present

entropy.watermark.below

This event is generated when the amount of available entropy data has fallen below the low water mark.

Severity

Success: Warning
Failure: Notice

Parameters

Parameter	Description	Presence
subject	The defined value indicating activity performed by the system rather than a user.	Always present
object	The value is always "entropy”	Always present
result	The value is always "success”	Always present

httpaccess.request

This event is generated when an HTTP request was made to the ESX host with the URL path beginning with one of the following prefixes: - /cgi-bin It is possible for a single HTTP request to generate more than one event. E.g. if the request headers have several authorization tokens or cookies then there will be one failure event for each invalid token or cookie.

Severity

Success: Info
Failure: Notice

Parameters

Parameter	Description	Presence
authorization	Of the request can be done in one of the following ways: - CGI ticket in HTTP header "vmware-cgi-ticket" or in cookie "vmware_cgi_ticket" - SOAP session cookie "vmware_soap_session" - user name and password - Oauth Bearer token in Authorization header (only for /cgi-bin)	Always present
subject	The name of the user who requested the operation.	Always present
object	The value is always "httpaccess"	Always present
result	"success" or "failure"	Always present
reason	Present when result is "failure" and indicates the reason for the failure.	Present when result is "failure"
ip	The network address of the originator of the connection.	Always present
port	The network port number of the originator of the connection.	Always present
url	The URL path of the HTTP request.	Always present
http	.method is the HTTP method involved in the connection attempt.	Always present
comment	Gives more details about the handling of the request.	Optional

message.invalid

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.

Severity

Success: Info
Failure: Notice

Parameters

Parameter	Description	Presence
subject	The name of user who requested the operation that has been found to contain problematic information.	Always present
object	The object that the operation was manipulating.	Always present
result	The value is always "failure"	Always present
origAuditID	The original eventID when eventID is valid or blank when the eventID is invalid.	Always present
file	The name of file where the audit record was emitted from.	Always present
line	The line number within the file where the audit record was emitted from.	Always present
reason	"One or more parameters were invalid" when one of more of the parameters are problematic or "Too long" when the parameters create an audit record that is too long to be handled by the host OS. As many of the original parameters, as practicable, will follow.	Always present

network.fw.defaultpolicy

This event is generated when an attempt was made to update the firewall default policy.

Severity

Success: Info

Failure: Notice

Parameters

Parameter	Description	Presence
subject	The name of the user who requested the operation.	Always present
object	The value is always "firewall"	Always present
result	"success" or "failure"	Always present
opID	The operation ID.	Optional
ip	The network address of the originator of the operation.	Optional
reason	Present when result is "failure" and indicates the reason for the failure.	Present when result is "failure"

network.fw.disable

This event is generated when an attempt was made to disable the firewall.

Severity

Success: Info

Failure: Notice

Parameters

Parameter	Description	Presence
subject	The name of the user who requested the operation.	Always present
object	The value is always "firewall"	Always present
result	"success" or "failure"	Always present
opID	The operation ID.	Optional
ip	The network address of the originator of the operation.	Optional
reason	Present when result is "failure" and indicates the reason for the failure.	Present when result is "failure"

network.fw.enable

This event is generated when an attempt was made to enable the firewall.

Severity

Success: Info

Failure: Notice

Parameters

Parameter	Description	Presence
subject	The name of the user who requested the operation.	Always present
object	The value is always "firewall"	Always present
result	"success" or "failure"	Always present
opID	The operation ID.	Optional
ip	The network address of the originator of the operation.	Optional
reason	Present when result is "failure" and indicates the reason for the failure.	Present when result is "failure"

network.fw.refresh

This event is generated when an attempt was made to refresh the firewall.

Severity

Success: Info

Failure: Notice

Parameters

Parameter	Description	Presence
subject	The name of the user who requested the operation.	Always present
object	The value is always "firewall"	Always present
result	"success" or "failure"	Always present
opID	The operation ID.	Optional
ip	The network address of the originator of the operation.	Optional
comment	Provides additional information about the event.	Optional
reason	Present when result is "failure" and indicates the reason for the failure.	Present when result is "failure"

network.fw.rule.disable

This event is generated when an attempt was made to disable a firewall ruleset.

Severity

Success: Info

Failure: Notice

Parameters

Parameter	Description	Presence
subject	The name of the user who requested the operation.	Always present
object	The name of the affected firewall ruleset.	Always present
result	"success" or "failure"	Always present
opID	The operation ID.	Optional
ip	The network address of the originator of the operation.	Optional
reason	Present when result is "failure" and indicates the reason for the failure.	Present when result is "failure"

network.fw.rule.enable

This event is generated when an attempt was made to enable a firewall ruleset.

Severity

Success: Info

Failure: Notice

Parameters

Parameter	Description	Presence
subject	The name of the user who requested the operation.	Always present
object	The name of the affected firewall ruleset.	Always present
result	"success" or "failure"	Always present
opID	The operation ID.	Optional
ip	The network address of the originator of the operation.	Optional
reason	Present when result is "failure" and indicates the reason for the failure.	Present when result is "failure"

network.fw.rule.update

This event is generated when an attempt was made to update a firewall ruleset.

Severity

Success: Info

Failure: Notice

Parameters

Parameter	Description	Presence
subject	The name of the user who requested the operation.	Always present
object	The name of the affected firewall ruleset.	Always present
result	"success" or "failure"	Always present
opID	The operation ID.	Optional
ip	The network address of the originator of the operation.	Optional
reason	Present when result is "failure" and indicates the reason for the failure.	Present when result is "failure"

network.nic.connect

This event is generated when an attempt was made to connect a host's NIC to a network switch.

Severity

Success: Info

Failure: Notice

Parameters

Parameter	Description	Presence
subject	The name of user who requested the operation.	Always present
object	The name of the affected physical NIC.	Always present
result	"success" or "failure"	Always present
opID	The operation ID.	Optional
type	"physical" or "vmkernel"	Always present
portGroup	The port group name.	Optional
networkID	The name of the affected vSphere Standard Switch or the uuid of the affected Distributed Virtual Switch.	Always present
reason	Present when result is "failure" and indicates the reason for the failure.	Present when result is "failure"

network.nic.disconnect

This event is generated when an attempt was made to disconnect a host's NIC from a network switch.

Severity

Success: Info

Failure: Notice

Parameters

Parameter	Description	Presence
subject	The name of user who requested the operation.	Always present
object	The name of the affected physical NIC.	Always present
result	"success" or "failure"	Always present
opID	The operation ID.	Optional
type	"physical" or "vmkernel"	Always present
portGroup	The port group name.	Optional
networkID	The name of the affected vSphere Standard Switch or the uuid of the affected Distributed Virtual Switch.	Always present
reason	Present when result is "failure" and indicates the reason for the failure.	Present when result is "failure"

network.switch.add

This event is generated when an attempt was made to add a virtual switch to the host.

Severity

Success: Info

Failure: Notice

Parameters

Parameter	Description	Presence
subject	The name of the user who requested the operation.	Always present
object	The name of the virtual switch.	Always present
type	"standard" or "distributed"	Always present
result	"success" or "failure"	Always present
opID	The operation ID.	Optional
reason	Provides additional details about the event.	Optional

network.switch.remove

This event is generated when an attempt was made to remove a virtual switch from the host.

Severity

Success: Info

Failure: Notice

Parameters

Parameter	Description	Presence
subject	The name of the user who requested the operation.	Always present
object	The name of the virtual switch.	Always present
type	"standard" or "distributed"	Always present
result	"success" or "failure"	Always present
opID	The operation ID.	Optional
reason	Provides additional details about the event.	Optional

product.issue

This event is generated when a product detects that an audit record should be issued but it is unable to do so for some reason. It is also generated for system issues like config store persistence errors that could put the system into an inconsistent or undesirable state. This audit event must only be used for issues that could affect system security and not other product issues.

Severity

Success: Info
Failure: Notice

Parameters

Parameter	Description	Presence
subject	The defined value indicating activity performed by the system rather than a user.	Always present
object	The name of the affected product (e.g. "esx")	Always present
result	The value is always "failure"	Always present
reason	Parameter is the reason why the the audit record could not be emitted, or the reason for the system failure.	Always present
location	Provides information about where in the product the issue occurred (e.g. a short description of the subsystem reporting the issue, like "VM state management").	Optional

proxy.connect

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

Severity

Success: Info

Failure: Notice

Parameters

Parameter	Description	Presence
subject	The defined value indicating activity performed by the system rather than a user.	Always present
object	The value is always "proxy"	Always present
result	"success" or "failure"	Always present
reason	Present when result is "failure" and indicates the reason for the failure.	Present when result is "failure"
ip	The network address of the originator of the connection.	Optional
port	The network port number of the originator of the connection.	Optional

proxy.disconnect

This event is generated when a proxy service connection was ended.

Severity

Success: Info

Failure: Notice

Parameters

Parameter	Description	Presence
subject	The defined value indicating activity performed by the system rather than a user.	Always present
object	The value is always "proxy"	Always present
result	The value is always "success"	Always present
ip	The network address of the originator of the connection.	Optional
port	The network port number of the originator of the connection.	Optional

service.access.denied

This event is generated when an attempt to access a service was denied due to failing authorization checks.

Severity

Success: Info

Failure: Notice

Parameters

Parameter	Description	Presence
subject	The name of the user who was denied access.	Always present
object	The name of the service operation that was invoked.	Always present
result	The value is always "failure"	Always present
reason	Provides additional details about the event.	Optional
ip	The network address of the originator of the connection.	Optional
opID	The operation ID.	Optional

service.apikey.get

This event is generated when an attempt was made to create an API key.

Severity

Success: Info

Failure: Notice

Parameters

Parameter	Description	Presence
subject	The name of the user who requested the new API key.	Always present
object	The name of the service operation that was invoked.	Always present
result	"success" or "failure"	Always present
uniqueId	The identifier of the created API key.	Optional
reason	Provides additional details about the event.	Optional
ip	The network address of the originator of the connection.	Optional
opID	The operation ID.	Optional

service.apikey.use

This event is generated when an attempt was made to authenticate with an API key.

Severity

Success: Info

Failure: Notice

Parameters

Parameter	Description	Presence
subject	The name of the user who requested the API key authentication.	Always present
object	The name of the service operation that was invoked.	Always present
result	"success" or "failure"	Always present
uniqueId	The identifier of the used API key.	Always present
reason	Provides additional details about the event.	Optional
ip	The network address of the originator of the connection.	Optional
opID	The operation ID.	Optional

service.exttoken.use

This event is generated when an attempt to use an external token for authentication.

Severity

Success: Info

Failure: Notice

Parameters

Parameter	Description	Presence
subject	The name of the user who requested the operation.	Always present
object	The name of the service operation that was invoked.	Always present
result	"success" or "failure"	Always present
reason	Provides additional details about the event.	Optional
ip	The network address of the originator of the connection.	Optional
opID	The operation ID.	Optional

service.lcticket.get

This event is generated when a Lifecycle service authorization ticket is requested. Typically for settingsd. It is generated for the following service URL paths: - /lifecycle-api

Severity

Success: Info
Failure: Notice

Parameters

Parameter	Description	Presence
subject	The name of the user who requested the operation.	Always present
object	The target operation or resource.	Always present
result	"success" or "failure"	Always present
reason	Provides additional details about the failure.	Optional
ip	The network address of the originator of the operation.	Optional
opID	The operation ID.	Optional
uniqueID	The identifier of the created ticket.	Optional

service.lcticket.use

This event is generated when an attempt was made to use a Lifecycle service authorization ticket. Typically in settingsd. It is generated for the service URL paths listed under service.lcticket.get.

Severity

Success: Info
Failure: Notice

Parameters

Parameter	Description	Presence
subject	"@unknown" - Usage of Lifecycle service ticket does not provide a subject identity.	Always present
object	The target operation or resource.	Always present
result	"success" or "failure"	Always present
reason	Provides additional details about the failure.	Optional
ip	The network address of the originator of the connection.	Optional
opID	The operation ID.	Optional
uniqueID	The identifier of the used ticket.	Optional

service.password.use

This event is generated when an attempt was made to authenticate a user with a password.

Severity

Success: Info

Failure: Notice

Parameters

Parameter	Description	Presence
subject	The name of the user who requested the operation.	Always present
object	The name of the service operation that was invoked.	Always present
result	"success" or "failure"	Always present
reason	Provides additional details about the event.	Optional
ip	The network address of the originator of the connection.	Optional
opID	The operation ID.	Optional

service.restart

This event is generated when an attempt was made to restart a host service.

Severity

Success: Info

Failure: Notice

Parameters

Parameter	Description	Presence
subject	The name of the user who requested the operation.	Always present
object	The service identifier.	Always present
result	"success" or "failure"	Always present
reason	Present when result is "failure" and indicates the reason for the failure.	Present when result is "failure"
ip	The network address of the originator of the connection.	Optional
opID	The operation ID.	Optional
comment	Provides additional information about the event.	Optional

service.start

This event is generated when an attempt was made to start a host service.

Severity

Success: Info

Failure: Notice

Parameters

Parameter	Description	Presence
subject	The name of the user who requested the operation.	Always present
object	The service identifier.	Always present
result	"success" or "failure"	Always present
reason	Present when result is "failure" and indicates the reason for the failure.	Present when result is "failure"
ip	The network address of the originator of the connection.	Optional
opID	The operation ID.	Optional
comment	Provides additional information about the event.	Optional

service.stop

This event is generated when an attempt was made to stop a host service.

Severity

Success: Info

Failure: Notice

Parameters

Parameter	Description	Presence
subject	The name of the user who requested the operation.	Always present
object	The service identifier.	Always present
result	"success" or "failure"	Always present
reason	Present when result is "failure" and indicates the reason for the failure.	Present when result is "failure"
ip	The network address of the originator of the connection.	Optional
opID	The operation ID.	Optional
comment	Provides additional information about the event.	Optional

service.ticket.get

This event is generated when a service authorization ticket was requested. It is generated for the following service URL paths: - /cgi-bin - /folder - /host - /screen - /tmp

Severity

Success: Info
Failure: Notice

Parameters

Parameter	Description	Presence
subject	The name of the user who requested the operation.	Always present
object	The ticket ID with most of its fields masked out.	Always present
result	The value is always "success"	Always present
ip	The network address of the originator of the operation.	Always present
url	The URL the ticket was acquired for.	Always present
http	.method is the HTTP method the ticket was acquired for, or empty string if not specified.	Always present
opID	The operation ID.	Optional

service.ticket.use

This event is generated when an attempt was made to use a service authorization ticket. It is generated for the service URL paths listed under service.ticket.get.

Severity

Success: Info
Failure: Notice

Parameters

Parameter	Description	Presence
subject	The name of the user who requested the operation if the ticket is valid and an empty string otherwise.	Always present
object	The ticket ID with most of its fields masked out.	Always present
result	"success" or "failure"	Always present
reason	Provides additional details about the event.	Optional
url	The URL path of the incoming request.	Always present
http	.method is the HTTP method of the incoming request.	Always present
opID	The operation ID.	Optional

service.token.get

This event is generated when an attempt was made to request an ESX access token from user credentials or another security token. It is generated for the following service URL paths: - /cgi-bin - /api - /sdk - /observability - /gdp - /stats

Severity

Success: Info
Failure: Notice

Parameters

Parameter	Description	Presence
subject	The name of the user who requested the operation.	Always present
object	The name of the service operation that was invoked.	Always present
result	"success" or "failure"	Always present
uniqueId	The masked signature of the new token, or an empty string if the signature could not be generated.	Optional
reason	Provides additional details about the event.	Optional
ip	The network address of the originator of the connection.	Optional
opID	The operation ID.	Optional

service.token.use

This event is generated when an attempt was made to execute an operation by passing a previously created access token. It is generated for the service URL paths listed under service.token.get.

Severity

Success: Info
Failure: Notice

Parameters

Parameter	Description	Presence
subject	The name of the user who requested the operation.	Always present
object	The name of the service operation that was invoked.	Always present
result	"success" or "failure"	Always present
uniqueId	The masked signature of the new token, or an empty string if the signature could not be determined.	Optional
reason	Present when the result is "failure" and indicates the the reason for the failure.	Present when the result is "failure"
ip	The network address of the originator of the operation.	Optional
opID	The operation ID.	Optional

service.uninstall

This event is generated when an attempt was made to uninstall a host service.

Severity

Success: Info

Failure: Notice

Parameters

Parameter	Description	Presence
subject	The name of the user who requested the operation.	Always present
object	The service identifier.	Always present
result	"success" or "failure"	Always present
reason	Present when result is "failure" and indicates the reason for the failure.	Present when result is "failure"
ip	The network address of the originator of the connection.	Optional
opID	The operation ID.	Optional

service.updatepolicy

This event is generated when an attempt was made to update the policy of a host service.

Severity

Success: Info

Failure: Notice

Parameters

Parameter	Description	Presence
subject	The name of the user who requested the operation.	Always present
object	The service identifier.	Always present
result	"success" or "failure"	Always present
reason	Present when result is "failure" and indicates the reason for the failure.	Present when result is "failure"
value	The policy value ("automatic", "on", or "off").	Always present
ip	The network address of the originator of the connection.	Optional
opID	The operation ID.	Optional
comment	Provides information about the event.	Optional

settings.advanced.add

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

Severity

Success: Info
Failure: Notice

Parameters

Parameter	Description	Presence
subject	The name of the user who requested the operation.	Always present
object	The name of the advanced option.	Always present
result	"success" or "failure"	Always present
reason	Present when result is "failure" and indicates the reason for the failure.	Present when result is "failure"
ip	The network address of the originator of the operation.	Optional
type	"int" or "string"	Always present
min	Present only when adding an integer (type "int") advanced setting. It denotes the minimum legal value.	Always present
max	Present only when adding an integer (type "int") advanced setting. It denotes the maximum legal value.	Always present
defaultValue	The default value of the new option.	Always present
description	The description of the new option.	Always present
isHidden	Indicates whether the option is hidden, i.e. 0 (not hidden) or 1 (hidden).	Always present
opID	The operation ID.	Optional

settings.advanced.delete

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

Severity

Success: Info

Failure: Notice

Parameters

Parameter	Description	Presence
subject	The name of the user who requested the operation.	Always present
object	The name of the advanced option.	Always present
result	"success" or "failure"	Always present
reason	Present when result is "failure" and indicates the reason for the failure.	Present when result is "failure"
ip	The network address of the originator of the operation.	Optional
opID	The operation ID.	Optional

settings.advanced.reset

This event is generated when an attempt was made to reset (to default) an advanced option.

Severity

Success: Info
Failure: Notice

Parameters

Parameter	Description	Presence
subject	The name of the user who requested the operation.	Always present
object	The name of the advanced option.	Always present
result	"success" or "failure"	Always present
reason	Present when result is "failure" and indicates the reason for the failure.	Present when result is "failure"
ip	The network address of the originator of the operation.	Optional
value	May not be present for some failures. When present, it is the default value for the option.	Always present
opID	The operation ID.	Optional

settings.advanced.set

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

Severity

Success: Info

Failure: Notice

Parameters

Parameter	Description	Presence
subject	The name of the user who requested the operation.	Always present
object	The name of the advanced option.	Always present
result	"success" or "failure"	Always present
reason	Present when result is "failure" and indicates the reason for the failure.	Present when result is "failure"
ip	The network address of the originator of the operation.	Optional
value	The new value specified for the advanced option.	Always present
opID	The operation ID.	Optional

settings.kernel.set

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

Severity

Success: Info

Failure: Notice

Parameters

Parameter	Description	Presence
subject	The name of the user who requested the operation.	Always present
object	The name of the setting.	Always present
result	"success" or "failure"	Always present
reason	Present when result is "failure" and indicates the reason for the failure.	Present when result is "failure"
ip	The network address of the originator of the operation.	Optional
value	The new value specified for the kernel setting.	Always present
opID	The operation ID.	Optional

shell.cmd

This event is generated whenever a command, issued via a shell, completes.

Severity

Success: Info
Failure: Notice

Parameters

Parameter	Description	Presence
subject	The name of the user who requested the operation.	Always present
object	The value is always "shell"	Always present
result	"success" or "failure" (representing 0 or not 0 respectively, as returned by shell $?).	Always present
command	The command line.	Always present
status	The exit code of the command. It will be present when the result is "failure"	Present when the result is "failure"

ssh.cmd

This event is generated whenever a shell command was issued by sshd.

Severity

Success: Info

Failure: Notice

Parameters

Parameter	Description	Presence
subject	The name of the user who requested the operation.	Always present
object	The value is always "ssh"	Always present
result	"success" as the command is always passed successfully to the shell.	Always present
command	The command passed to the shell.	Always present

ssh.connect

This event is generated when an attempt was made to begin an SSH connection.

Severity

Success: Info

Failure: Notice

Parameters

Parameter	Description	Presence
subject	The name of the user who requested the operation.	Always present
object	The value is always "ssh"	Always present
result	"success" or "failure"	Always present
reason	Present when result is "failure" and indicates the reason for the failure.	Present when result is "failure"
ip	The network address of the originator of the connection.	Always present

ssh.disconnect

This event is generated when an attempt was made to end an SSH connection.

Severity

Success: Info

Failure: Notice

Parameters

Parameter	Description	Presence
subject	The name of the user who requested the operation.	Always present
object	The value is always "ssh"	Always present
result	"success" or "failure"	Always present
reason	Present when result is "failure" and indicates the reason for the failure.	Present when result is "failure"
ip	The network address of the originator of the connection.	Always present

ssh.session.begin

This event is generated when an attempt was made to begin an SSH session.

Severity

Success: Info

Failure: Notice

Parameters

Parameter	Description	Presence
subject	The name of the user who requested the operation.	Always present
object	The value is always "ssh"	Always present
result	"success" or "failure"	Always present
reason	Present when result is "failure" and indicates the reason for the failure.	Present when result is "failure"
ip	The network address of the originator of the session.	Always present
hostname	The origin host name (or the ip address if the host name could not be resolved).	Always present

ssh.session.end

This event is generated when an attempt was made to end an SSH session.

Severity

Success: Info

Failure: Notice

Parameters

Parameter	Description	Presence
subject	The name of the user who requested the operation.	Always present
object	The value is always "ssh"	Always present
result	"success" or "failure"	Always present
reason	Present when result is "failure" and indicates the reason for the failure.	Present when result is "failure"
ip	The network address of the originator of the session.	Always present
hostname	The origin host name (or the ip address if the host name could not be resolved).	Always present

syslog.mark

This event is generated when a mark message is issued to syslog and the audit trail.

Severity

Success: Info

Failure: Notice

Parameters

Parameter	Description	Presence
subject	The name of the user who requested the operation.	Always present
object	The value is always "syslog”	Always present
result	The value is always "success”	Always present
comment	Parameter is the "event message” The text may be an empty string.	Always present
ip	The network address of the originator of the session.	Optional
opID	The operation ID.	Optional

syslog.net.close

This event is generated when vmsyslogd closes a socket (UDP, TCP, TLS (SSL)) to a remote host.

Severity

Success: Info

Failure: Notice

Parameters

Parameter	Description	Presence
subject	The defined value indicating activity performed by the system rather than a user.	Always present
object	The remote host (a syslog collector) identifier (e.g. DNS address, IPV4 or IPV6 address).	Always present
result	The value is always "success"	Always present

syslog.net.link.down

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

Severity

Success: Info
Failure: Notice

Parameters

Parameter	Description	Presence
subject	The defined value indicating activity performed by the system rather than a user.	Always present
object	The remote host (a syslog collector) identifier (e.g. DNS address, IPV4 or IPV6 address).	Always present
result	"failure"	Always present
reason	Provides additional details about the event.	Optional
subjectDN	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"	Present when result is "failure"
subjectAltName	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"	Present when result is "failure"
referenceID	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.	Present when result is "failure"

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.

Severity

Success: Info
Failure: Notice

Parameters

Parameter	Description	Presence
subject	The defined value indicating activity performed by the system rather than a user.	Always present
object	The remote host (a syslog collector) identifier (e.g. DNS address, IPV4 or IPV6 address).	Always present
result	"success"	Always present

syslog.net.open

This event is generated when vmsyslogd opens a socket (UDP, TCP, TLS (SSL)) to a remote host.

Severity

Success: Info

Failure: Notice

Parameters

Parameter	Description	Presence
subject	The defined value indicating activity performed by the system rather than a user.	Always present
object	The remote host (a syslog collector) identifier (e.g. DNS address, IPV4 or IPV6 address).	Always present
result	"success"	Always present

syslog.reload

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

Severity

Success: Info

Failure: Notice

Parameters

Parameter	Description	Presence
subject	The name of the user who requested the operation.	Always present
object	The value is always "syslog"	Always present
result	"success" or "failure"	Always present
reason	Present when result is "failure" and indicates the reason for the failure.	Present when result is "failure"
ip	The network address of the originator of the operation.	Optional
opID	The operation ID.	Optional

system.update.add

This event is generated upon completion of a VIB installation attempt.

Severity

Success: Info
Failure: Notice

Parameters

Parameter	Description	Presence
severity	On success depends on whether an attempt has been made to override signature validation. If it has then the severity is LOG_NOTICE. Otherwise it is the default (LOG_INFO).	Always present
subject	The name of the user who requested the operation.	Always present
object	The VIB being installed.	Always present
result	"success" or "failure" If "failure", the reason is indicated by the system.update.end event.	Always present

system.update.end

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

Severity

Success: Info

Failure: Notice

Parameters

Parameter	Description	Presence
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).	Always present
subject	The name of the user who requested the operation.	Always present
object	The value is always "system"	Always present
result	"success" or "failure"	Always present
reason	Present when result is "failure" and indicates the reason for the failure.	Present when result is "failure"

system.update.remove

This event is generated upon completion of a VIB removal attempt.

Severity

Success: Info
Failure: Notice

Parameters

Parameter	Description	Presence
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).	Always present
subject	The name of the user who requested the operation.	Always present
object	The VIB being removed.	Always present
result	"success" or "failure" If "failure", the reason is indicated by the system.update.end event.	Always present

system.update.start

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

Severity

Success: Info

Failure: Notice

Parameters

Parameter	Description	Presence
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).	Always present
subject	The name of the user who requested the operation.	Always present
object	The value is always "system"	Always present
result	"success" or "failure"	Always present
reason	Provides additional details about the event.	Optional

time.monitoring.disable

This event is generated when an attempt was made to disable time service monitoring.

Severity

Success: Info

Failure: Notice

Parameters

Parameter	Description	Presence
subject	The name of the user who requested the operation.	Always present
object	The value is always "time"	Always present
result	"success" or "failure"	Always present
reason	Present when result is "failure" and indicates the reason for the failure.	Present when result is "failure"
ip	The network address of the originator of the operation.	Optional
opID	The operation ID.	Optional

time.monitoring.enable

This event is generated when an attempt was made to enable time service monitoring.

Severity

Success: Info

Failure: Notice

Parameters

Parameter	Description	Presence
subject	The name of the user who requested the operation.	Always present
object	The value is always "time"	Always present
result	"success" or "failure"	Always present
reason	Present when result is "failure" and indicates the reason for the failure.	Present when result is "failure"
ip	The network address of the originator of the operation.	Optional
opID	The operation ID.	Optional

time.ntp.disable

This event is generated when an attempt was made to disable NTP.

Severity

Success: Info

Failure: Notice

Parameters

Parameter	Description	Presence
subject	The name of the user who requested the operation.	Always present
object	The value is always "time"	Always present
result	"success" or "failure"	Always present
reason	Present when result is "failure" and indicates the reason for the failure.	Present when result is "failure"
ip	The network address of the originator of the operation.	Optional
opID	The operation ID.	Optional

time.ntp.enable

This event is generated when an attempt was made to enable NTP.

Severity

Success: Info

Failure: Notice

Parameters

Parameter	Description	Presence
subject	The name of the user who requested the operation.	Always present
object	The value is always "time"	Always present
result	"success" or "failure"	Always present
reason	Present when result is "failure" and indicates the reason for the failure.	Present when result is "failure"
ip	The network address of the originator of the operation.	Optional
opID	The operation ID.	Optional

time.ntp.set.loglevel

This event is generated when an attempt was made to set the loggging level of NTP.

Severity

Success: Info

Failure: Notice

Parameters

Parameter	Description	Presence
subject	The name of the user who requested the operation.	Always present
object	The value is always "time"	Always present
result	"success" or "failure"	Always present
reason	Present when result is "failure" and indicates the reason for the failure.	Present when result is "failure"
ip	The network address of the originator of the operation.	Optional
value	The new value specified for the NTP logging level.	Optional
comment	Provides additional information about the event.	Optional
opID	The operation ID.	Optional

time.ntp.set.rawconfig

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

Severity

Success: Info
Failure: Notice

Parameters

Parameter	Description	Presence
subject	The name of the user who requested the operation.	Always present
object	The value is always "time"	Always present
result	"success" or "failure"	Always present
reason	Present when result is "failure" and indicates the reason for the failure.	Present when result is "failure"
ip	The network address of the originator of the operation.	Optional
max	Indicates the maximum number of lines allowed for the NTP raw configuration.	Optional
value	The new value of raw NTP configuration(s). May be specified multiple times, one for each raw configuration.	Optional
opID	The operation ID.	Optional

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).

Severity

Success: Info
Failure: Notice

Parameters

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

time.ptp.disable

This event is generated when an attempt was made to disable PTP.

Severity

Success: Info

Failure: Notice

Parameters

Parameter	Description	Presence
subject	The name of the user who requested the operation.	Always present
object	The value is always "time"	Always present
result	"success" or "failure"	Always present
reason	Present when result is "failure" and indicates the reason for the failure.	Present when result is "failure"
ip	The network address of the originator of the operation.	Optional
opID	The operation ID.	Optional

time.ptp.enable

This event is generated when an attempt was made to enable PTP.

Severity

Success: Info

Failure: Notice

Parameters

Parameter	Description	Presence
subject	The name of the user who requested the operation.	Always present
object	The value is always "time"	Always present
result	"success" or "failure"	Always present
reason	Present when result is "failure" and indicates the reason for the failure.	Present when result is "failure"
ip	The network address of the originator of the operation.	Optional
opID	The operation ID.	Optional

time.ptp.set.device

This event is generated when an attempt was made to set the network device for PTP.

Severity

Success: Info

Failure: Notice

Parameters

Parameter	Description	Presence
subject	The name of the user who requested the operation.	Always present
object	The value is always "time"	Always present
result	"success" or "failure"	Always present
reason	Present when result is "failure" and indicates the reason for the failure.	Present when result is "failure"
ip	The network address of the originator of the operation.	Optional
type	The new device type for PTP, and can be set to "virtualNic", "pciPassthruNic", or "none"	Optional
deviceLabel	The new name specified for the PTP device.	Optional
opID	The operation ID.	Optional

time.ptp.set.domain

This event is generated when an attempt was made to set the domain for PTP.

Severity

Success: Info

Failure: Notice

Parameters

Parameter	Description	Presence
subject	The name of the user who requested the operation.	Always present
object	The value is always "time"	Always present
result	"success" or "failure"	Always present
reason	Present when result is "failure" and indicates the reason for the failure.	Present when result is "failure"
ip	The network address of the originator of the operation.	Optional
value	The new value of the PTP domain.	Optional
opID	The operation ID.	Optional

time.ptp.set.fallback

This event is generated when an attempt was made to set the fallback option for PTP.

Severity

Success: Info

Failure: Notice

Parameters

Parameter	Description	Presence
subject	The name of the user who requested the operation.	Always present
object	The value is always "time"	Always present
result	"success" or "failure"	Always present
reason	Present when result is "failure" and indicates the reason for the failure.	Present when result is "failure"
ip	The network address of the originator of the operation.	Optional
value	The new value specified to set PTP fallback.	Always present
comment	Provides additional information about the event.	Optional
opID	The operation ID.	Optional

time.ptp.set.ip

This event is generated when an attempt was made to set the IP configuration for PTP.

Severity

Success: Info

Failure: Notice

Parameters

Parameter	Description	Presence
subject	The name of the user who requested the operation.	Always present
object	The value is always "time"	Always present
result	"success" or "failure"	Always present
reason	Present when result is "failure" and indicates the reason for the failure.	Present when result is "failure"
ip	The network address of the originator of the operation.	Optional
type	Set to one of "DHCP", "static IP address", or "none" if no protocol applies.	Optional
value	The network address of the device.	Optional
netmask	The subnet mask for the device ip.	Optional
opID	The operation ID.	Optional

time.ptp.set.loglevel

This event is generated when an attempt was made to set the loggging level of PTP.

Severity

Success: Info

Failure: Notice

Parameters

Parameter	Description	Presence
subject	The name of the user who requested the operation.	Always present
object	The value is always "time"	Always present
result	"success" or "failure"	Always present
reason	Present when result is "failure" and indicates the reason for the failure.	Present when result is "failure"
ip	The network address of the originator of the operation.	Optional
value	The new value specified for the PTP logging level.	Optional
comment	Provides additional information about the event.	Optional
opID	The operation ID.	Optional

time.set.systemclock

This event is generated when an attempt was made to manually set the system clock time.

Severity

Success: Info
Failure: Notice

Parameters

Parameter	Description	Presence
subject	The name of the user who requested the operation.	Always present
object	The value is always "time"	Always present
result	"success" or "failure"	Always present
reason	Present when result is "failure" and indicates the reason for the failure.	Present when result is "failure"
ip	The network address of the originator of the operation.	Optional
value	On success, is the new system clock time. On failure, it is the value that caused the failure.	Always present
opID	The operation ID.	Optional

tls.clt.set.cipherlist

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

Severity

Success: Info
Failure: Notice

Parameters

Parameter	Description	Presence
subject	The name of the user who requested the operation.	Always present
object	"tls"	Always present
result	"success" or "failure"	Always present
reason	Present when result is "failure" and indicates the reason for the failure.	Present when result is "failure"
ip	The network address of the originator of the operation.	Always present
value	The new value specified for the cipher list.	Always present
comment	Provides information about the event.	Optional

tls.clt.set.ciphersuites

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

Severity

Success: Info
Failure: Notice

Parameters

Parameter	Description	Presence
subject	The name of the user who requested the operation.	Always present
object	"tls"	Always present
result	"success" or "failure"	Always present
reason	Present when result is "failure" and indicates the reason for the failure.	Present when result is "failure"
ip	The network address of the originator of the operation.	Always present
value	The new value specified for the cipher suites.	Always present
comment	Provides information about the event.	Optional

tls.clt.set.groups

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

Severity

Success: Info

Failure: Notice

Parameters

Parameter	Description	Presence
subject	The name of the user who requested the operation.	Always present
object	"tls"	Always present
result	"success" or "failure"	Always present
reason	Present when result is "failure" and indicates the reason for the failure.	Present when result is "failure"
ip	The network address of the originator of the operation.	Always present
value	The new value specified for the ECC groups.	Always present
comment	Provides information about the event.	Optional

tls.clt.set.profile

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

Severity

Success: Info
Failure: Notice

Parameters

Parameter	Description	Presence
subject	The name of the user who requested the operation.	Always present
object	"tls"	Always present
result	"success" or "failure"	Always present
reason	Present when result is "failure" and indicates the reason for the failure.	Present when result is "failure"
ip	The network address of the originator of the operation.	Optional
value	The new profile value (one of "COMPATIBLE", "MANUAL")	Always present
comment	Provides information about the event.	Optional
opID	The operation ID.	Optional

tls.clt.set.protocols

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

Severity

Success: Info

Failure: Notice

Parameters

Parameter	Description	Presence
subject	The name of the user who requested the operation.	Always present
object	"tls"	Always present
result	"success" or "failure"	Always present
reason	Present when result is "failure" and indicates the reason for the failure.	Present when result is "failure"
ip	The network address of the originator of the operation.	Always present
value	The new value specified for the protocols.	Always present
comment	Provides information about the event.	Optional

tls.svr.set.cipherlist

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

Severity

Success: Info
Failure: Notice

Parameters

Parameter	Description	Presence
subject	The name of the user who requested the operation.	Always present
object	"tls"	Always present
result	"success" or "failure"	Always present
reason	Present when result is "failure" and indicates the reason for the failure.	Present when result is "failure"
ip	The network address of the originator of the operation.	Always present
value	The new value specified for the cipher list.	Always present
comment	Provides information about the event.	Optional

tls.svr.set.ciphersuites

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

Severity

Success: Info
Failure: Notice

Parameters

Parameter	Description	Presence
subject	The name of the user who requested the operation.	Always present
object	"tls"	Always present
result	"success" or "failure"	Always present
reason	Present when result is "failure" and indicates the reason for the failure.	Present when result is "failure"
ip	The network address of the originator of the operation.	Always present
value	The new value specified for the cipher suites.	Always present
comment	Provides information about the event.	Optional

tls.svr.set.groups

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

Severity

Success: Info
Failure: Notice

Parameters

Parameter	Description	Presence
subject	The name of the user who requested the operation.	Always present
object	"tls"	Always present
result	"success" or "failure"	Always present
reason	Present when result is "failure" and indicates the reason for the failure.	Present when result is "failure"
ip	The network address of the originator of the operation.	Always present
value	The new value specified for the ECC groups.	Always present
comment	Provides information about the event.	Optional

tls.svr.set.profile

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

Severity

Success: Info
Failure: Notice

Parameters

Parameter	Description	Presence
subject	The name of the user who requested the operation.	Always present
object	"tls"	Always present
result	"success" or "failure"	Always present
reason	Present when result is "failure" and indicates the reason for the failure.	Present when result is "failure"
ip	The network address of the originator of the operation.	Optional
value	The new profile value (one of "COMPATIBLE","MANUAL","NIST_2024", "NIST_2024_TLS_13_ONLY").	Always present
comment	Provides information about the event.	Optional
opID	The operation ID.	Optional

tls.svr.set.protocols

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

Severity

Success: Info

Failure: Notice

Parameters

Parameter	Description	Presence
subject	The name of the user who requested the operation.	Always present
object	"tls"	Always present
result	"success" or "failure"	Always present
reason	Present when result is "failure" and indicates the reason for the failure.	Present when result is "failure"
ip	The network address of the originator of the operation.	Always present
value	The new value specified for the protocols.	Always present
comment	Provides information about the event.	Optional

usb.passthru.disable

This event is generated when an attempt was made to make a connected USB device unavailable for passthrough to a VM.

Severity

Success: Info

Failure: Notice

Parameters

Parameter	Description	Presence
subject	The name of the user who requested the operation.	Always present
object	A reference to the affected USB device, in the form "bus:device:vendorID:productID", where all values are represented in hex form.	Always present
result	"success" or "failure"	Always present
reason	Provides additional details about the event.	Optional
ip	The network address of the originator of the operation.	Optional
comment	Provides information about the event.	Optional
opID	The operation ID.	Optional

usb.passthru.enable

This event is generated when an attempt was made to make a connected USB device available for passthrough to a VM.

Severity

Success: Info
Failure: Notice

Parameters

Parameter	Description	Presence
subject	The name of the user who requested the operation.	Always present
object	A reference to the affected USB device, in the form "bus:device:vendorID:productID", where all values are represented in hex form.	Always present
result	"success" or "failure"	Always present
reason	Provides additional details about the event.	Optional
ip	The network address of the originator of the operation.	Optional
comment	Provides information about the event.	Optional
opID	The operation ID.	Optional

vim.access.denied

This event is generated when an attempt to access a protected VIM object was denied.

Severity

Success: Info

Failure: Notice

Parameters

Parameter	Description	Presence
subject	The name of the user who was denied access.	Always present
object	The name of the object on which the operation was invoked (e.g. "vim.HostSystem:ha-host", "vim.host.StorageSystem:storageSystem", "vmodl.query.PropertyCollector:ha-property-collector"). Consult the vSphere Web Servies API documentation for more information. Note that some objects are undocumented since they are internal-use only.	Always present
result	The value is always "failure"	Always present
reason	Provides additional details about the event.	Optional
ip	The network address of the originator of the connection.	Always present
apiName	Describes the internal API name of the operation that was invoked (e.g. "GetStorageDeviceInfo", "waitForUpdatesEx"). To understand the meaning of this value, consult the vSphere Web Servies API documentation, starting with the object value as a reference. Note that property retrieval operations are prefixed with "Is" for boolean properties and "Get" for all other properties. Also note that some operations are undocumented since they are internal-use only.	Always present
path	The VMX file path if the target is a virtual machine, or the datastore name if the target object is a datastore.	Always present
opID	The operation ID.	Optional

vim.connect

This event is generated when an attempt was made to create a VIM connection.

Severity

Success: Info
Failure: Notice

Parameters

Parameter	Description	Presence
subject	The user authenticating with the system.	Always present
object	The value is always "vim"	Always present
result	"success" or "failure"	Always present
reason	Present when result is "failure" and indicates the reason for the failure.	Present when result is "failure"
ip	The network address of the originator of the connection.	Always present
uniqueID	A unique ID representing the session that was established. It is present when the result is "success"	Present when the result is "success"
opID	The operation ID.	Optional

vim.disconnect

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

Severity

Success: Info

Failure: Notice

Parameters

Parameter	Description	Presence
subject	The user who is the owner of the connection.	Always present
object	The value is always "vim”	Always present
result	The value is always "success”	Always present
reason	The reason for the connection ending, e.g. logout, timeout expired, or terminated by administrator.	Always present
ip	The network address of the originator of the connection.	Always present
uniqueID	A unique ID representing the closed session.	Always present
opID	The operation ID.	Optional

vim.terminate

This event is generated when a VIM connection was terminated by an administrator.

Severity

Success: Info

Failure: Notice

Parameters

Parameter	Description	Presence
subject	The user who is terminating the connection.	Always present
object	The user who is the owner of the terminated connection.	Always present
result	The value is always "success"	Always present
ip	The network address of the originator of the connection.	Always present
uniqueID	A unique ID representing the terminated session.	Always present
opID	The operation ID.	Optional

vm.create

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

Severity

Success: Info

Failure: Notice

Parameters

Parameter	Description	Presence
subject	The name of the user who requested the operation.	Always present
object	The path of the VMX file of the affected VM.	Always present
result	"success" or "failure"	Always present
reason	Present when result is "failure" and indicates the reason for the failure.	Present when result is "failure"
ip	The network address of the originator of the operation.	Always present

vm.delete

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

Severity

Success: Info

Failure: Notice

Parameters

Parameter	Description	Presence
subject	The name of the user who requested the operation.	Always present
object	The path of the VMX file of the affected VM.	Always present
result	"success" or "failure"	Always present
reason	Present when result is "failure" and indicates the reason for the failure.	Present when result is "failure"
ip	The network address of the originator of the operation.	Always present
opID	The operation ID.	Optional

vm.guestrpc.denied

This event is generated when an attempt to use a privileged Guest RPC was denied.

Severity

Success: Info

Failure: Notice

Parameters

Parameter	Description	Presence
subject	The defined value indicating activity performed by the system rather than a user.	Always present
object	The path of the VMX file of the reporting VM.	Always present
result	The value is always "failure”	Always present
reason	The value is always "permission denied”	Always present
name	The Guest RPC command.	Always present
value	The Guest RPC number.	Always present

vm.hypercall.denied

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

Severity

Success: Info

Failure: Notice

Parameters

Parameter	Description	Presence
subject	The defined value indicating activity performed by the system rather than a user.	Always present
object	The path of the VMX file of the reporting VM.	Always present
result	The value is always "failure”	Always present
reason	Indicates the reason for the denial.	Always present
type	"Backdoor" or "HbBackdoor”	Always present
value	The hypercall number.	Always present
name	The name of the hypercall.	Optional

vm.kill

This event is generated when an attempt was made to forcibly terminate a virtual machine.

Severity

Success: Info

Failure: Notice

Parameters

Parameter	Description	Presence
subject	The name of the user who requested the operation.	Always present
object	The path of the VMX file of the affected VM.	Always present
result	"success" or "failure"	Always present
reason	Present when result is "failure" and indicates the reason for the failure.	Present when result is "failure"
ip	The network address of the originator of the operation.	Optional
opID	The operation ID.	Optional

vm.net.add

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

Severity

Success: Info

Failure: Notice

Parameters

Parameter	Description	Presence
subject	The name of the user who requested the operation.	Always present
object	The path of the VMX file of the affected VM.	Always present
result	"success" or "failure"	Always present
ip	The network address of the originator of the operation.	Always present
networkID	The name of the network that was to be attached.	Always present
opID	The operation ID.	Optional

vm.net.edit

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

Severity

Success: Info

Failure: Notice

Parameters

Parameter	Description	Presence
subject	The name of the user who requested the operation.	Always present
object	The path of the VMX file of the affected VM.	Always present
result	"success" or "failure"	Always present
ip	The network address of the originator of the operation.	Always present
networkID	The name of the new network.	Always present
oldID	The name of the old network, or an empty string if not applicable.	Always present
connect	"at power-on" or "not at power-on" when a change affects device setup.	Optional
opID	The operation ID.	Optional

vm.net.remove

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

Severity

Success: Info

Failure: Notice

Parameters

Parameter	Description	Presence
subject	The name of the user who requested the operation.	Always present
object	The path of the VMX file of the affected VM.	Always present
result	"success" or "failure"	Always present
ip	The network address of the originator of the operation.	Always present
networkID	The name of the network that was to be detached.	Always present
opID	The operation ID.	Optional

vm.power.off

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

Severity

Success: Info

Failure: Notice

Parameters

Parameter	Description	Presence
subject	The name of the user powering off a VM.	Always present
object	The path of the VMX file of the affected VM.	Always present
result	"success" or "failure"	Always present
reason	Present when result is "failure" and indicates the reason for the failure.	Present when result is "failure"
ip	The network address of the originator of the operation.	Optional
opID	The operation ID.	Optional

vm.power.on

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

Severity

Success: Info

Failure: Notice

Parameters

Parameter	Description	Presence
subject	The name of the user who requested the operation.	Always present
object	The path of the VMX file of the affected VM.	Always present
result	"success" or "failure"	Always present
reason	Present when result is "failure" and indicates the reason for the failure.	Present when result is "failure"
ip	The network address of the originator of the operation.	Optional
opID	The operation ID.	Optional

vm.power.reset

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

Severity

Success: Info

Failure: Notice

Parameters

Parameter	Description	Presence
subject	The name of the user who requested the operation.	Always present
object	The path of the VMX file of the affected VM.	Always present
result	"success" or "failure"	Always present
reason	Present when result is "failure" and indicates the reason for the failure.	Present when result is "failure"
ip	The network address of the originator of the operation.	Optional
opID	The operation ID.	Optional

vm.power.suspend

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

Severity

Success: Info

Failure: Notice

Parameters

Parameter	Description	Presence
subject	The name of the user who requested the operation.	Always present
object	The path of the VMX file of the affected VM.	Always present
result	"success" or "failure"	Always present
reason	Present when result is "failure" and indicates the reason for the failure.	Present when result is "failure"
ip	The network address of the originator of the operation.	Optional
opID	The operation ID.	Optional

vm.reconfigure

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

Severity

Success: Info

Failure: Notice

Parameters

Parameter	Description	Presence
subject	The name of the user who requested the operation.	Always present
object	The path of the VMX file of the affected VM.	Always present
result	"success" or "failure"	Always present
reason	Present when result is "failure" and indicates the reason for the failure.	Present when result is "failure"
ip	The network address of the originator of the operation.	Optional
opID	The operation ID.	Optional

vm.register

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

Severity

Success: Info

Failure: Notice

Parameters

Parameter	Description	Presence
subject	The name of the user who requested the operation.	Always present
object	The path of the VMX file of the affected VM.	Always present
result	"success" or "failure"	Always present
reason	Present when result is "failure" and indicates the reason for the failure.	Present when result is "failure"
ip	The network address of the originator of the operation.	Always present
opID	The operation ID.	Optional

vm.snapshot.create

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

Severity

Success: Info
Failure: Notice

Parameters

Parameter	Description	Presence
subject	The name of the user who requested the operation.	Always present
object	The path of the VMX file of the affected VM.	Always present
result	"success" or "failure"	Always present
reason	Present when result is "failure" and indicates the reason for the failure.	Present when result is "failure"
ip	The network address of the originator of the operation.	Always present
name	The display name of the snapshot.	Always present
uniqueID	The unique ID of the snapshot or an empty string.	Always present
parent	The unique ID of the parent snapshot or an empty string. when the snapshot is the root of the tree.	Always present
opID	The operation ID.	Optional

vm.snapshot.remove

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

Severity

Success: Info

Failure: Notice

Parameters

Parameter	Description	Presence
subject	The name of the user who requested the operation.	Always present
object	The path of the VMX file of the affected VM.	Always present
result	"success" or "failure"	Always present
reason	Present when result is "failure" and indicates the reason for the failure.	Present when result is "failure"
ip	The network address of the originator of the operation.	Always present
name	The display name of the snapshot.	Always present
uniqueID	The unique ID of the snapshot.	Always present
opID	The operation ID.	Optional
comment	Provides information about the event.	Optional

vm.snapshot.removeAll

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

Severity

Success: Info

Failure: Notice

Parameters

Parameter	Description	Presence
subject	The name of the user who requested the operation.	Always present
object	The path of the VMX file of the affected VM.	Always present
result	"success" or "failure"	Always present
reason	Present when result is "failure" and indicates the reason for the failure.	Present when result is "failure"
ip	The network address of the originator of the operation.	Always present
opID	The operation ID.	Optional

vm.snapshot.rename

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

Severity

Success: Info

Failure: Notice

Parameters

Parameter	Description	Presence
subject	The name of the user who requested the operation.	Always present
object	The path of the VMX file of the affected VM.	Always present
result	"success" or "failure"	Always present
reason	Present when result is "failure" and indicates the reason for the failure.	Present when result is "failure"
ip	The network address of the originator of the operation.	Always present
name	The current display name of the snapshot.	Always present
newName	The new display name of the snapshot.	Always present
uniqueID	The unique ID of the snapshot.	Always present
opID	The operation ID.	Optional
comment	Provides information about the event.	Optional

vm.snapshot.revert

This event is generated when an attempt was made to revert to VM snapshot.

Severity

Success: Info

Failure: Notice

Parameters

Parameter	Description	Presence
subject	The name of the user who requested the operation.	Always present
object	The path of the VMX file of the affected VM.	Always present
result	"success" or "failure"	Always present
reason	Present when result is "failure" and indicates the reason for the failure.	Present when result is "failure"
ip	The network address of the originator of the operation.	Always present
name	The current display name of the snapshot.	Always present
uniqueID	The unique ID of the snapshot.	Always present
opID	The operation ID.	Optional

vm.storage.add

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

Severity

Success: Info
Failure: Notice

Parameters

Parameter	Description	Presence
subject	The name of the user who requested the operation.	Always present
object	The path of the VMX file of the affected VM.	Always present
result	"success" or "failure"	Always present
ip	The network address of the originator of the operation.	Always present
path	The path to the affected file or an empty string when a local device is auto selected (e.g. CDROM/DVD).	Always present
opID	The operation ID.	Optional
reason	Present when result is "failure" and indicates the reason for the failure.	Present when result is "failure"

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.

Severity

Success: Info
Failure: Notice

Parameters

Parameter	Description	Presence
subject	The name of the user who requested the operation.	Always present
object	The path of the VMX file of the affected VM.	Always present
result	"success" or "failure"	Always present
ip	The network address of the originator of the operation.	Always present
path	The path to the attached file or an empty string when a local device is auto selected (e.g. CDROM/DVD).	Always present
oldPath	The path to the detached file or an empty string when a local device is auto selected (e.g. CDROM/DVD).	Optional
connect	"at power-on" or "not at power-on" when a change affects device setup.	Optional
opID	The operation ID.	Optional
reason	Present when result is "failure" and indicates the reason for the failure.	Present when result is "failure"

vm.storage.remove

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

Severity

Success: Info

Failure: Notice

Parameters

Parameter	Description	Presence
subject	The name of the user who requested the operation.	Always present
object	The path of the VMX file of the affected VM.	Always present
result	"success" or "failure"	Always present
ip	The network address of the originator of the operation.	Always present
path	The path to the affected file or an empty string when a local device is auto selected (e.g. CDROM/DVD).	Always present
opID	The operation ID.	Optional
reason	Present when result is "failure" and indicates the reason for the failure.	Present when result is "failure"

vm.unregister

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

Severity

Success: Info

Failure: Notice

Parameters

Parameter	Description	Presence
subject	The name of the user who requested the operation.	Always present
object	The path of the VMX file of the affected VM.	Always present
result	"success" or "failure"	Always present
reason	Present when result is "failure" and indicates the reason for the failure.	Present when result is "failure"
ip	The network address of the originator of the operation.	Always present
opID	The operation ID.	Optional

vm.usb.connect

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

Severity

Success: Info
Failure: Notice

Parameters

Parameter	Description	Presence
subject	The defined value indicating activity performed by the system rather than a user.	Always present
object	The path of the VMX file of the reporting VM.	Always present
result	"success" or "failure"	Always present
reason	Provides additional details about the event.	Optional
opID	The operation ID.	Optional
deviceLabel	"usb:" for usb 1.1, "ehci:" for usb 2.0, or "usb_xhci:" for usb 3.x. The "" is a small integer, uniquely identifying the USB controller involved.	Optional
vendorID	The vendor ID of the device.	Always present
productID	The product ID of the device.	Always present
name	The user-friendly name of the device.	Optional
type	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.)	Optional

vm.usb.disconnect

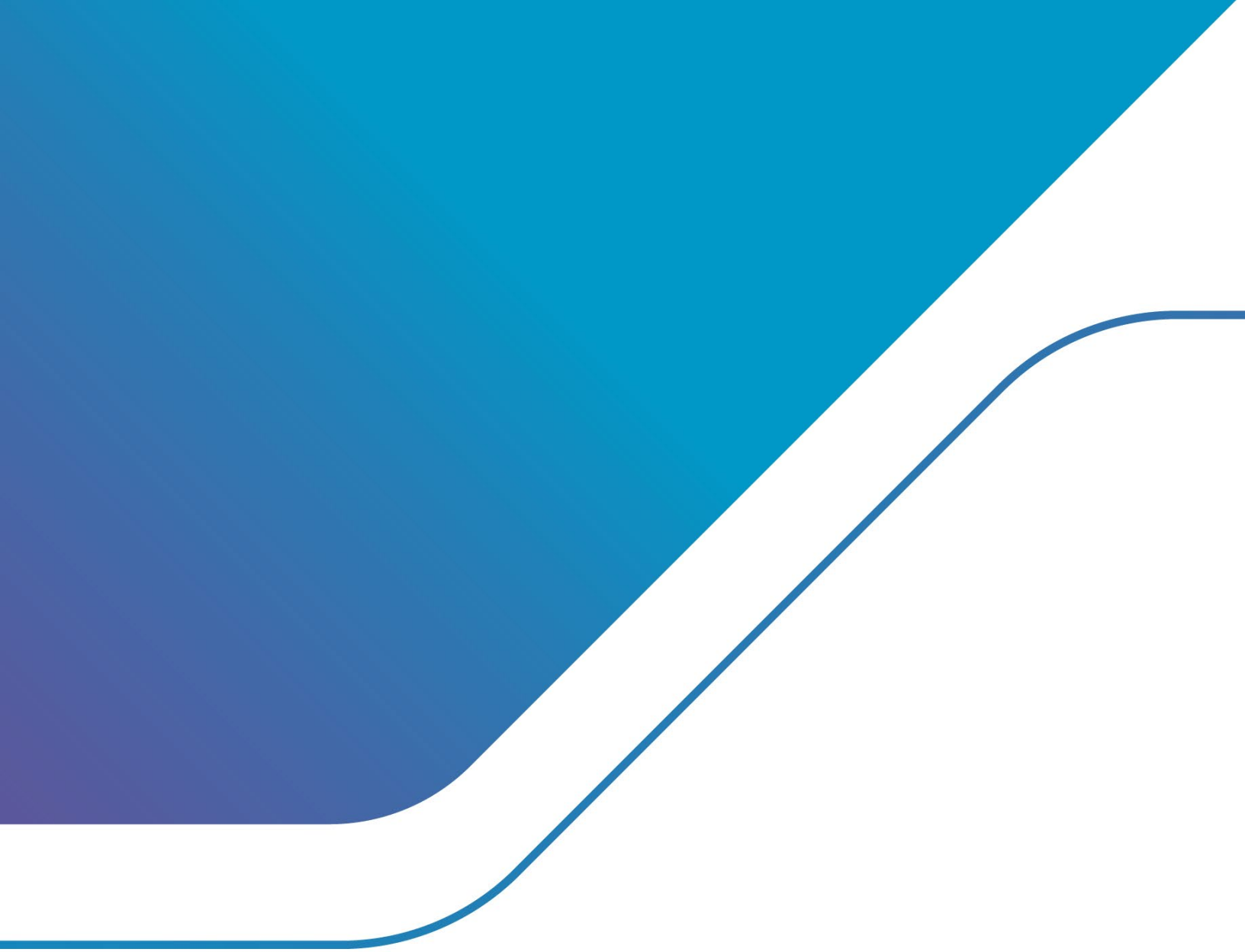
This event is generated when an attempt was made to disconnect a USB device from a VM.

Severity

Success: Info
Failure: Notice

Parameters

Parameter	Description	Presence
subject	The defined value indicating activity performed by the system rather than a user.	Always present
object	The path of the VMX file of the reporting VM.	Always present
result	"success" or "failure"	Always present
reason	Provides additional details about the event.	Optional
opID	The operation ID.	Optional
deviceLabel	"usb:" for usb 1.1, "ehci:" for usb 2.0, or "usb_xhci:" for usb 3.x. The "" is a small integer, uniquely identifying the USB controller involved.	Optional
vendorID	The vendor ID of the device.	Optional
productID	The product ID of the device.	Optional
deviceID	The device ID of the device.	Optional
name	The user-friendly name of the device.	Optional
type	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.)	Optional



vmware® by Broadcom