



Collecting and forwarding VMware events and alarms with Cloud Optimizer

2017/12/01

Thierry Ledent
thierry.ledent@microfocus.com

Get the latest updates of this document at <https://softwaresupport.softwaregrp.com/km/KM03028614>

Abstract

This paper describes how to configure Cloud Optimizer to collect VMware events and alarms from the vCenter and to forward these events and alarms to OMi, OMU, OML and OMW. It is divided into following sections:

1. [Terminology and scope of this paper](#)
2. [Basic configuration steps](#)
3. [Advanced configuration steps](#)
4. [Troubleshooting steps](#)

Most support cases related to the collection and forwarding of VMware events and alarms start with a misunderstanding of the differences between the concepts of events, alarms and alerts. The first section of this paper tries to clarify these concepts. This is a prerequisite to fully understand the rest of this paper.

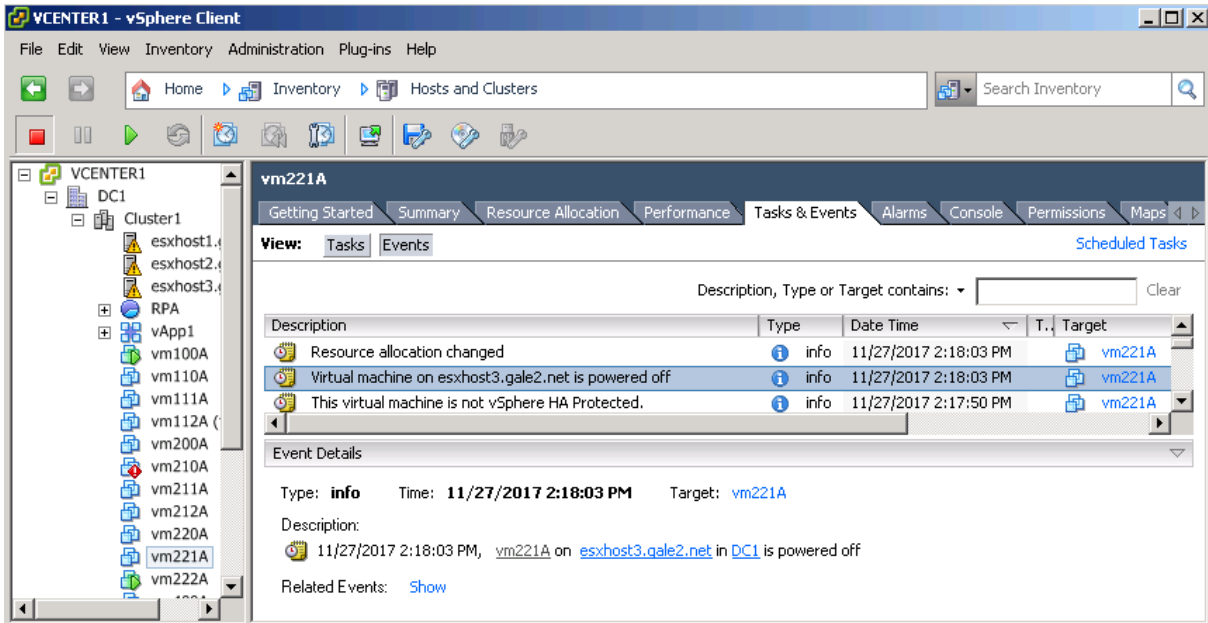
1 Terminology and scope of this paper

The topic of event forwarding through Cloud Optimizer generates some confusion because the words "events", "alerts" and "alarms" refer to different concepts depending on the context where they are used. In this document, we will use the terminology as defined below.

1.1 VMware events

VMware events are informational messages logged on the vCenter that report on activities in the vSphere environment. VMware events are visible in the vSphere client under the specific virtual machine, host, or other instance to which the event relates.

VMware provides events of many different types. For instance, the vSphere client screenshot below shows the events logged against the virtual machine vm221A. The highlighted event reports that this virtual machine has been powered off. This is an event of type `VmPoweredOffEvent`.

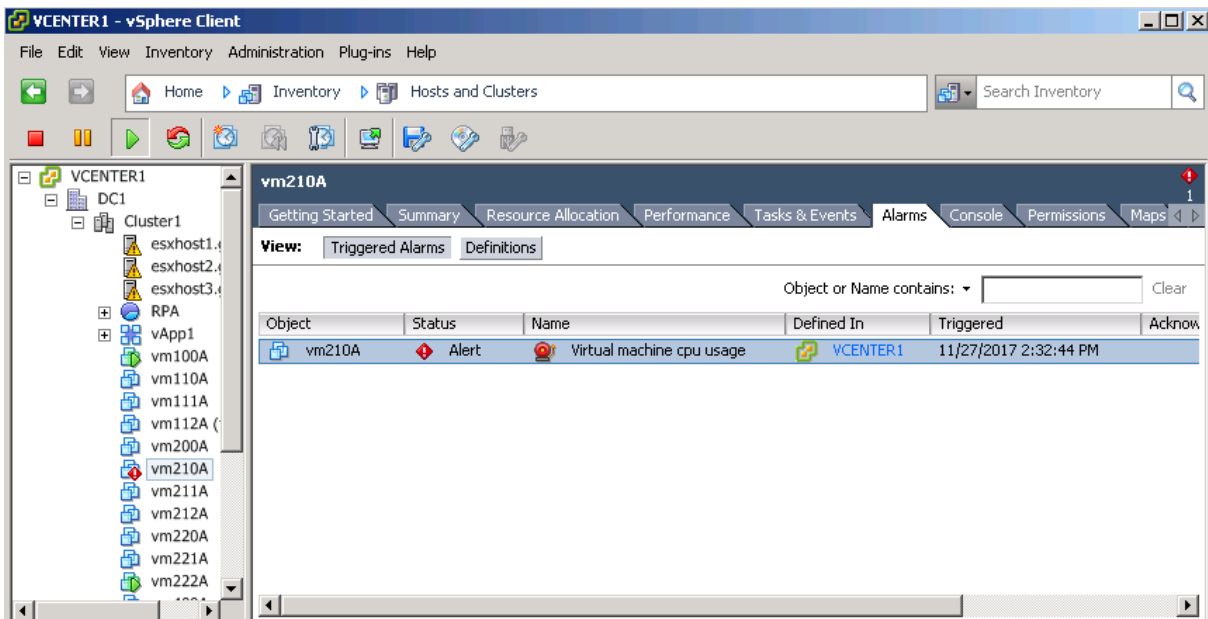


1.2 VMware alarms

VMware alarms are rules created on the vCenter to monitor the health, status and resource levels of virtual machines, hosts and other instances of the vSphere environment. VMware alarms are visible in the vSphere client under the specific virtual machine, host, or other instance to which it relates.

The status of a VMware alarm is represented by the colors green, yellow, red and grey as follows:

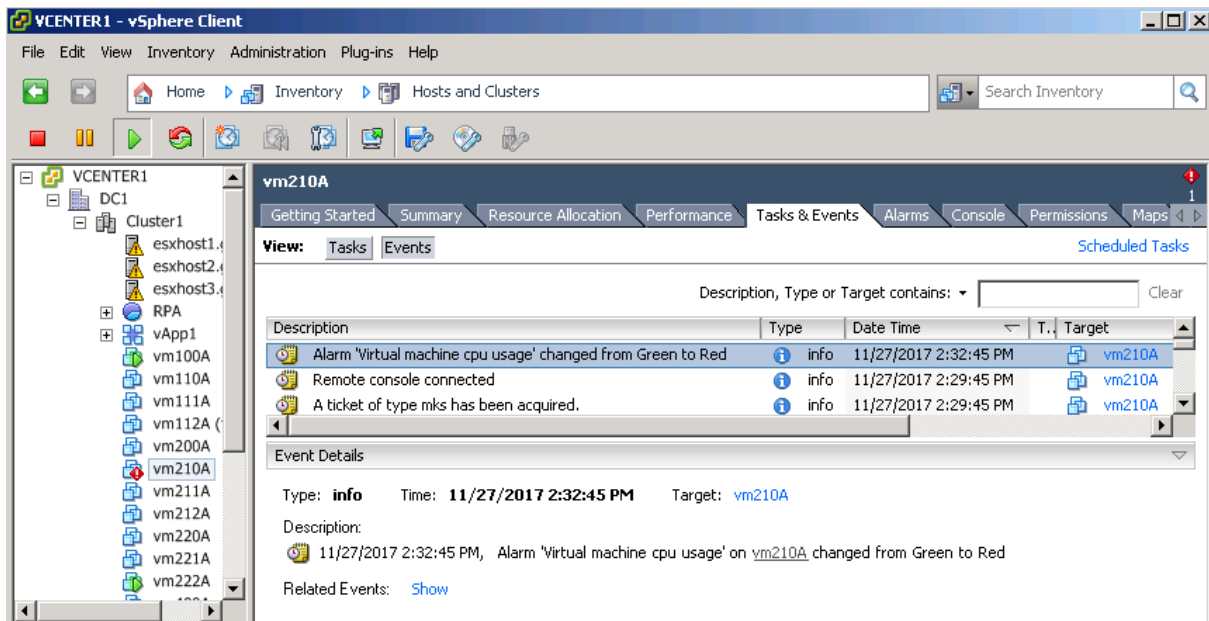
- **Green** The monitored item is below the defined warning threshold
- **Yellow** The monitored item is above the defined warning threshold
- **Red** The monitored item is above the defined critical threshold
- **Grey** The monitored item is not currently measurable (e.g. CPU usage of a virtual machine that is currently powered off)



The vSphere client screenshot above shows the triggered alarms for the virtual machine vm210A. Triggered alarms are alarms that are currently in color yellow or red (above the warning or critical threshold). This example shows that the alarm named `Virtual machine cpu usage` currently has the color red for virtual machine vm210A.

Whenever the color of an alarm changes (e.g. from Yellow to Red, from Red to Green...), the vCenter generates a descriptive VMware event of type `AlarmStatusChangedEvent`. Events of this type are just one particular type among many possible event types like described in paragraph 1.1 above.

The vSphere client screenshot below shows the events logged against the virtual machine vm210A. The highlighted event is one of type `AlarmStatusChangedEvent`. This event reports that the alarm `Virtual machine cpu usage` changed from Green to Red for this virtual machine.



Cloud Optimizer does not explicitly collect any alarm information, but it can collect the events of type `AlarmStatusChangedEvent` and forward them to the OMi, OMu, OML or OMW server.

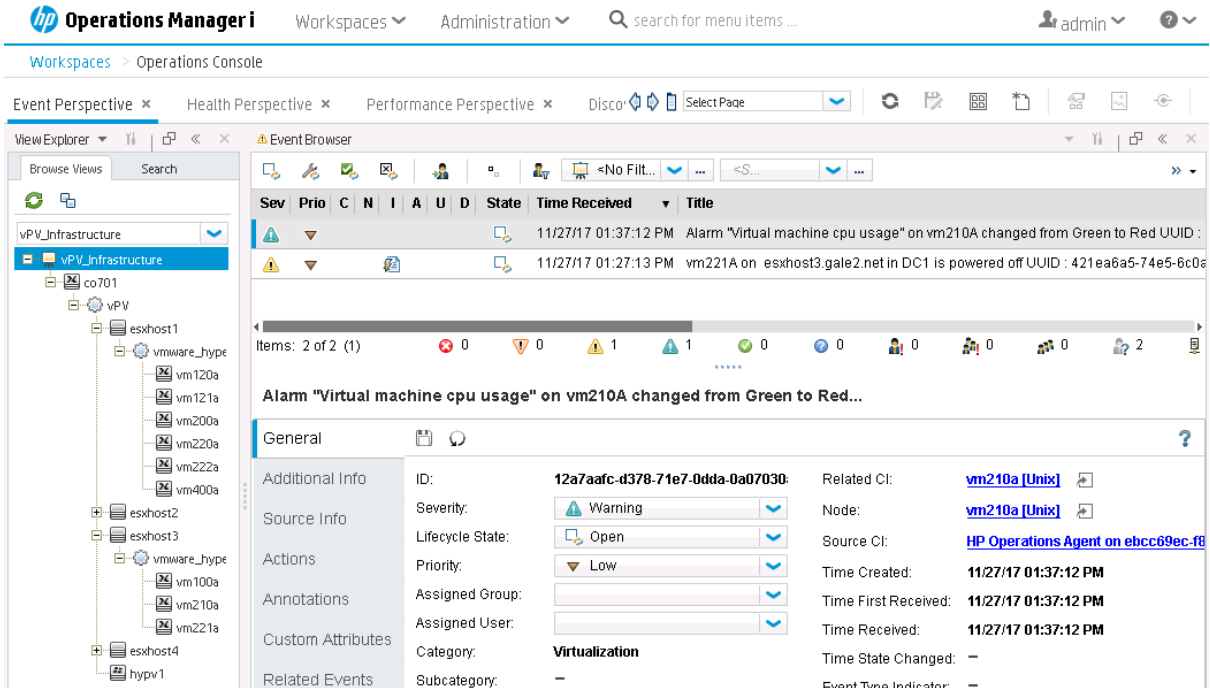
1.3 OMi events and OM messages

OMi events are informational messages originating from the monitored environment that can be viewed in the OMi event perspective. The OMi events include attributes such as a title, a severity, a related CI... OM messages are the counterpart of OMi events in the former products OMu, OML and OMW. This document will refer to the OMu, OML and OMW server as the OM server.

Cloud Optimizer can collect VMware events from the vCenter and forward them as OMi events to the OMi server or as OM messages to the OM server. Note that VMware events cannot be viewed in the CO user interface.

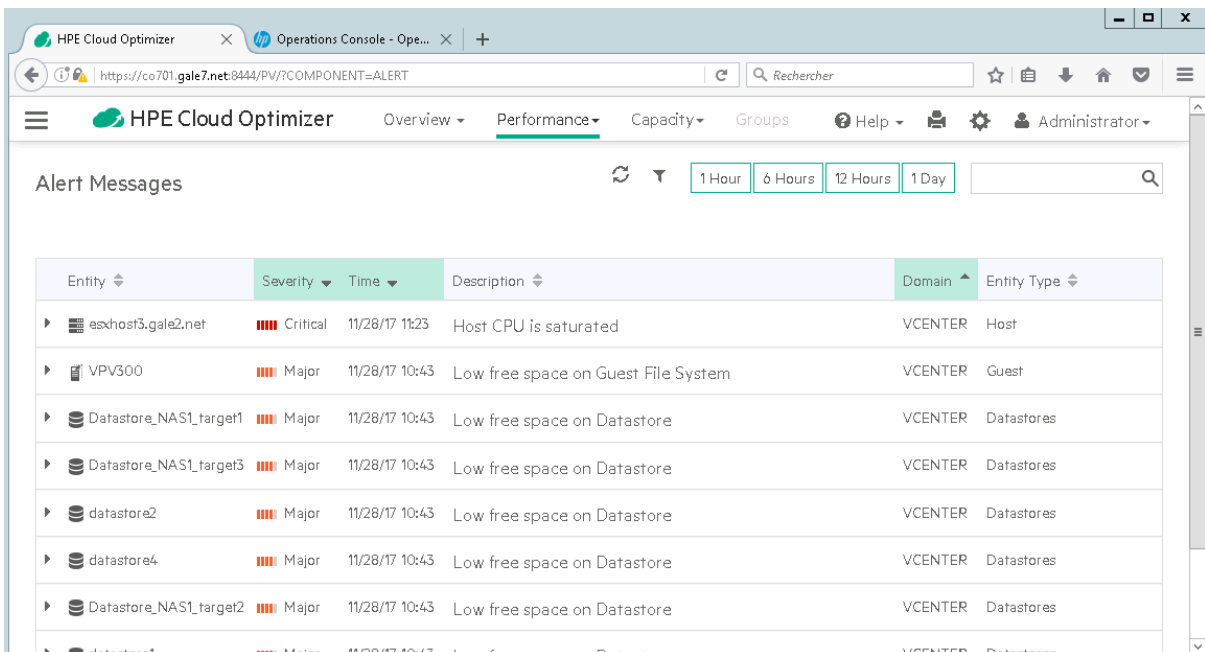
The screenshot of the OMi event perspective below shows two OMi events forwarded by the Cloud Optimizer server that report the same two VMware events that were shown in the screenshots above:

- An event of type `VmPoweredOffEvent` for virtual machine vm221A
- An event of type `AlarmStatusChangedEvent` for virtual machine vm210A



1.4 Cloud Optimizer alerts

Cloud Optimizer alerts are informational messages created by Cloud Optimizer that describe performance problems identified by pre-defined Cloud Optimizer rules and based on the metrics collected from the monitored virtualized environment. Cloud Optimizer alerts are visible in the Cloud Optimizer user interface (screenshot below) and can optionally be forwarded as OMi events to the OMi server or as OM messages to the OM server.



Cloud Optimizer alerts are stored in the events table of the Cloud Optimizer Vertica database, along with the VMware events. But apart from this, Cloud Optimizer alerts and VMware events are totally distinct concepts. Also their forwarding to the OMi server or OM server follows totally distinct processes.

When looking at a forwarded Cloud Optimizer alert in the OMi event perspective or in the OM message browser, it is easy to distinguish it from a VMware event by looking at the detailed title or message text. The Cloud Optimizer alert will always include the reason why Cloud Optimizer decided to alert and what are the possible causes, e.g.:

```

CPU saturation is detected on host esxhost3.gale2.net

Reason:
MaxVmCpuReadyUtil [24.44] > VMCPUReadyUtilizationThreshold[15], and HostCPUDemand [771.0]
> Capacity [8800] - HeadRoom [99]

Possible Cause:
Multiple Virtual Machines with High CPU workload demand running on this Host.

Additional Details:
CPU Capacity =8800 MHz
CPU Demand =771.0 MHz
Virtual Machine Configured(Powered On) =2

Top 10 Virtual Machines by CPU Ready Time
CPU Ready Util(%)          VM Name
-----
Top 10 Virtual Machines by CPU Demand
CPU Demand(MHz)           VM Name
-----
436.0                      vm222A
335.0                      vm120A

References:
Allocation of Virtual Machines - https://10.7.3.10:8444/PV/...
Activity Status of Virtual Machines - https://10.7.3.10:8444/PV/...
Idle VMs - https://10.7.3.10:8444/PV/...
Host forecast graph - https://10.7.3.10:8444/PV/...

Recommendations:
a)Power-off the Virtual Machines that are in IDLE State.
b)If the selected host is under any cluster, and DRS is not enabled, migrate some of the
Virtual
    
```

On the other hand, an OMi event or OM message originating from a VMware event will include a very simple title or message text, e.g.:

```

vm221A on esxhost3.gale2.net in DC1 is powered off
UUID : 421ea6a5-74e5-6c0a-fc41-50270f7590d3
Element : vm221A
Time (UTC) : 2017-11-27T14:18:03+01:00
    
```

This paper does not cover Cloud Optimizer alerts.

2 Basic configuration steps

Follow the steps below to enable basic VMware event forwarding to the OM server. Advanced configuration steps are described in [Advanced configuration steps](#).

2.1 Version and patch level

Over time, there have been significant improvements to the collection of VMware events. It is important to remain up to date with the Cloud Optimizer versions, patch levels and hotfixes. At the time of this writing, it is recommended to run CO version 3.02.004 with hotfix CO_3.01.131_HF_VCENTER_4.

The forwarding of VMware events to OMi and OM is implemented through the policy `vPV-EventMonitor` and some instrumentation that are delivered through integration bits. The same bits also deliver the discovery policies and instrumentation that enable to create the guests, hosts, etc... as CIs on the OMi server or nodes on the OM server. The discovery must be operational for a functional forwarding of VMware events since the OMi and OM

server must be able to relate these events to the correct CI or node. Therefore, it is important to remain up to date with the integration bits. At the time of this writing, the following bits are recommended:

- CO/OMi integration
 - OMi Management Pack for Cloud Optimizer 1.25
 - Available at <https://marketplace.microfocus.com/itom/content/omi-management-pack-vpv>
- CO/OMU integration and CO/OML integration
 - CO_OMX_3.02.004 available through Microfocus support
- CO/OMW integration
 - CO_OMW_3.02.004 available through Microfocus support

2.2 Configuring the CO discovery

When the CO server forwards VMware events as OMi events or OM messages, the OMi server or OM server must be able to relate them to the correct CI or node. This requires the VMware instances to be created as CIs on OMi or nodes on OM. The CO discovery enables to automatically create these CIs or nodes. Some quick hints are provided below for a smoother discovery. For detailed information consult the OMi Management Pack for Cloud Optimizer and the Cloud Optimizer documentation.

Check some settings in the `agtrep` namespace of the CO server with:

```
# ovconfget agtrep
```

The variable `RESEND_RELATIONSHIP_INSTANCES` should have the value `TRUE`. Update the value with:

```
# ovconfchg -ns agtrep -set RESEND_RELATIONSHIP_INSTANCES TRUE
```

In large environments, it may be necessary to increase `ACTION_TIMEOUT` from the default 3 minutes to 15 minutes. There no harm doing this in small environments too:

```
# ovconfchg -ns agtrep -set ACTION_TIMEOUT 15
```

The discovery policy should be deployed to the CO server. This policy runs every hour at the half hour (e.g. at 00:30, 01:30, 02:30...). The policy name is `vpv-Discovery` for the OMi integration and `vpv-NodesDiscovery` for the OM integration. Both policies have version 302.0000 in the integration bits cited above in paragraph 2.1. The OM integration bits also provide a policy `vpv-TopologyDiscovery` that is not strictly required for VMware events forwarding.

Upon the initial execution, the discovery policy sends a complete set of CI/node information to the OMi/OM server. Upon the next executions, it updates the OMi or OM server with any changes discovered in the virtualized environments. When troubleshooting a discovery problem, it is sometimes necessary to force an initial complete discovery with below commands:

```
# /opt/OV/bin/ovagtrep -clearall
# /opt/OV/bin/ovagtrep -run vpv-Discovery (OMi integration)
# /opt/OV/bin/ovagtrep -run vpv-NodesDiscovery (OM integration)
```

Take care that the command `ovagtrep` is a troubleshooting tool that does not output a lot of information. It will fail silently when providing a wrong policy name.

2.3 Configuring VMware event collection

At each collection interval, the CO server collects the latest VMware events from the vCenter that are of a type listed in the file `/opt/OV/newconfig/OVPM/smepack/VCENTER/data/VIEEventsType.cfg`.

By default, this file contains only a limited list of event types, and some are commented out. For instance, the event type `AlarmStatusChangedEvent` is commented out. If you want to collect (and forward) events of this type, uncomment the corresponding line.

Changes to this file are picked up dynamically by the CO server, so that it is not necessary to restart any process when editing the file.

For a list of existing VMware event types, consult the VMware documentation.

Note that the CO server only collects VMware events related to hosts, virtual machines, datacenters, datastores and clusters.

2.4 Configuring VMware event forwarding

The policy `vPV-EventMonitor` converts the VMware events collected by CO into OMi events or OM messages and forwards them to the OMi/OM server. Before deploying this policy to the CO server, its policy interval must be set equal to the CO collection interval. Check the CO collection interval with:

```
# ovconfget pvcd CollectionInterval
```

The two possible values are 300 seconds and 900 seconds. If the variable is not set, or has a different value, it defaults to 300 seconds.

Failure to align the policy interval on the event collection interval can lead to missing a random amount of events.

The policy has several parameters. The below parameters are relevant to these basic configuration steps:

MessageGroup	This parameter specifies the value to fill into the message group attribute of the OMi event or OM message
AlarmFlag	This parameter must be set to <code>true</code> if events of type <code>AlarmStatusChangedEvent</code> should be forwarded to OMi/OM
Debug	Set this parameter to <code>2</code> in order to log debugging information into the log file <code>/var/opt/OV/log/vPV-EventMonitorLog.txt</code> . Since this log file grows rather slowly and rolls over when reaching 1MB, it is safe to keep this parameter with value <code>2</code> for an extended period of time.

2.5 Testing VMware event forwarding

After completing the steps 2.1 to 2.4, the desired VMware events should be collected and forwarded to OMi/OM.

When testing this feature keep in mind that:

- It can take up to 1 collection interval for a new VMware event to be collected, and then up to 1 more collection interval for the policy `vPV-EventMonitor` to forward the event.
- When the CO server processes are restarted, they will only collect VMware events that were created after the restart, so that any test VMware event should be created after the CO server processes have been started.

For testing purposes, make sure to generate a test VMware event of a type that is listed in the configuration file `/opt/OV/newconfig/OVPM/smepack/VCENTER/data/VIEventsType.cfg`. One type of VMware event that is very easy to generate is `VmRemoteConsoleConnectedEvent`. To generate such an event, just open the remote console of a virtual machine in the vSphere client. Note that this type is not included by default in the configuration file, so it must be added manually.

3 Advanced configuration steps

This section describes advanced configuration steps for VMware events collection and forwarding.

3.1 Configuring VMware events collection

At each collection interval, the CO server collects the latest VMware events from the vCenter that are of a type listed in the file `/opt/OV/newconfig/OVPM/smepack/VCENTER/data/VIEventsType.cfg`.

The file accepts a single event type per line, or two complementary events separated by a colon, e.g.:

```
HostShutdownEvent
VmPoweredOffEvent:VmPoweredOnEvent
```

Complementary events are also referred to as the *opted event* and the *normal event*, respectively `VmPoweredOffEvent` and `VmPoweredOnEvent` in above example. The opted events and normal events are handled in a slightly different manner in the policy `vPV-EventMonitor`.

In the special case that all event types are deleted or commented out in the configuration file `VIEventTypes.cfg`, the CO server will collect all VMware events related to hosts, virtual machines, datacenters, datastores and clusters, irrespective of their type. This has however an impact on the forwarding logic (see below).

3.2 Configuring VMware events forwarding to OM

The policy `vPV-EventMonitor` converts the VMware events collected by CO into OMi events or OM messages and forwards them to the OMi/OM server.

The first rule (`Events from vCenter`) should not be modified. It reads the new events from the CO database and feeds them to the second rule (`Evaluate Events and send alert`). Don't let yourself be confused by the word "alert" in this rule's name - it is a shortcut for "OMi event" or "OM message" and has no relation with Cloud Optimizer alerts.

This second rule processes each collected VMware event sequentially through a set of 44 predefined thresholds:

- | | |
|---|--|
| 1. VM Removed Event | 23. VM Suspended Event |
| 2. DRS VM Migrated Event | 24. VM Resuming Event |
| 3. VM BeingHotMigrated Event | 25. VM GuestReboot Event |
| 4. VM Migrated Event | 26. Failover Level Restored |
| 5. VM Failed Migrated Event | 27. General HostError Event |
| 6. VM Disk Failed Event | 28. General VmError Event |
| 7. VM UUID Changed Event | 29. HealthStatus Changed Event |
| 8. VM UUID Conflict Event | 30. Host CnxFailedNetworkError Event |
| 9. VM Failover Failed Event | 31. Host LicenseExpired Event |
| 10. VM No Network Access Event | 32. License NonCompliance Event |
| 11. VM Orphaned Event | 33. MigrationError Event |
| 12. VM Renamed Event | 34. VM DasBeingReset Event |
| 13. Not Enough ResourcesTo StartVmEvent | 35. VM DasResetFailed Event |
| 14. Host Removed Event | 36. VC CannotFindMaster Event |
| 15. Host Shutdown Event | 37. Cluster Failover ActionCompleted Event |
| 16. DRS VM Powered On Event | 38. Failed Restart AfterIsolation Event |
| 17. VM Powered Off Event | 39. License CapacityExceeded Event |
| 18. VM Powered On Event | 40. VC HealthStateChanged Event |
| 19. DRS Disabled Event | 41. Das HostFailed Event |
| 20. DRS Enabled Event | 42. AlarmStatus Changed Event |
| 21. DRS Entered Standby Mode Event | 43. Alarm Normal State |
| 22. DRS Exited Standby Mode Event | 44. Warning Alert - Event Occured |

The logic of the thresholds 1 to 41 is straightforward. For instance, a VMware event of type `VmRenamedEvent` will match the threshold 12. This threshold creates and forwards an OMi event or OM message descriptive of this VMware event and related to the corresponding virtual machine. Note that, if the FQDN of the virtual machine is not known to CO, the OMi event or OM message will be related to the CO server.

The thresholds 42 and 43 manage the VMware events of type `AlarmStatusChangedEvent`. Their logic is explained in more detail in [Configuring the forwarding of alarms](#).

The last threshold is a catch-all threshold that will act on VMware events that did not match with any of the previous thresholds. It compares the event type against the types listed in the configuration file `VIEventsType.cfg`. If the type can be found in the file, the threshold creates and forwards an OMi event or OM message descriptive of this VMware event. Note that in case of complementary events (see [Configuring VMware events collection](#)), only the opted event is forwarded.

Note that the above logic implies that the catch-all threshold will not forward any VMware event if all event types are deleted or commented out in `VIEventTypes.cfg`. Only the VMware events of a type matched by the thresholds 1 to 43 will be forwarded. In this scenario, it is probably desirable to add thresholds for any additional desired event type, between the current thresholds 43 and 44.

3.3 Configuring the forwarding of alarms

Recent versions of the policy `vPV-EventMonitor` come with 4 parameters that enable to configure how VMware events of type `AlarmStatusChangedEvent` should be forwarded to OMi or OM:

3.3.1 Parameter AlarmFlag

This parameter should be set to `true` to enable the thresholds 42 and 43 that forward the events of type `AlarmStatusChangedEvent` as OMi events or OM messages to the OMi/OM server. By default, this parameter is set to `false`, which effectively disables the forwarding of these VMware events.

3.3.2 Parameter AlarmFilterByText

This parameter is unset by default, which means that all events of type `AlarmStatusChangedEvent` are forwarded.

When this parameter is set, it should list the names of VMware alarms for which the corresponding VMware events of type `AlarmStatusChangedEvent` should be forwarded, with the names separated by commas. For instance, if one wants to forward events of type `AlarmStatusChangedEvent` that originate from the alarms named 'Virtual machine cpu usage' and 'Virtual machine memory usage', then the parameter should be set as:

```
AlarmFilterByText=Virtual machine cpu usage,Virtual machine memory usage
```

The alarm name comparison with the list provided in this parameter is case-insensitive, but accepts no wildcards and no extra leading or trailing blanks.

With the above parameter setting, if a VMware event of type `AlarmStatusChangedEvent` is collected that originates from a different alarm, say the alarm named 'Host memory usage', it will not be forwarded.

Each alarm name listed in the parameter can be expanded with the severities that should be attributed to the forwarded OMi event or OM message, in function of the new alarm color. For instance, assume the below setting for the parameter:

```
AlarmFilterByText=Virtual machine cpu usage:Major|Minor|Warning,
                  Virtual machine memory usage:Minor|-|-
```

With this setting, the severities of the OMi events or OM message will be as per below table:

Alarm name	New alarm color	OMi event or OM message severity
Virtual machine cpu usage	Red	Major
Virtual machine cpu usage	Yellow	Minor
Virtual machine cpu usage	Grey	Warning
Virtual machine memory usage	Red	Minor
Virtual machine memory usage	Yellow	Not forwarded
Virtual machine memory usage	Grey	Not forwarded

3.3.3 Parameter IncidentBased

This parameter defines the severity of the OMi events or OM messages related to VMware events of type `AlarmStatusChangedEvent` as per below table. Note that if the severities are defined with the parameter `AlarmFilterByText`, as described above, they overwrite any setting of the parameter `IncidentBased`.

IncidentBased	New alarm color	OMi event or OM message severity
false (default)	Red	Warning
false (default)	Yellow	Warning
false (default)	Grey	Warning
true	Red	Critical
true	Yellow	Warning
true	Grey	Unknown

3.3.4 Parameter ForwardGreenAlarms

If this parameter is set to 1 (default), VMware events of type `AlarmStatusChangedEvent` originating from alarms that changed to color green will be forwarded as OMi events or OM messages to OMi/OM with the severity Normal. If the parameter `AlarmFilterByText` is also set, then only the events resulting from an alarm listed in the parameter will be forwarded.

If this parameter is set to 0, VMware events of type `AlarmStatusChangedEvent` originating from alarms that changed to color green will not be forwarded.

4 Troubleshooting steps

When troubleshooting a VMware event collection or forwarding problem, the following questions should always be clarified:

1. What type of events should be collected and forwarded?

This question implies to distinguish between VMware events, VMware alarms and CO alerts. Remember that VMware alarms are never collected, but the events of type `AlarmStatusChangedEvent` that result from an alarm color change can be collected and forwarded. Don't assume that such an event has been recently created just because the color of an alarm is currently red or yellow. An alarm that is in color red or yellow, may be in this color since a long time. Alarms can be repeated in the vSphere client, but only when the color changed will a new event of type `AlarmStatusChangedEvent` be created. Therefore, if you are missing such an event, confirm in the vSphere client that it was effectively created and when it was created.

Remember that CO alerts are a totally different concept that follows distinct processes.

2. Are the desired event types listed in `VIEventsType.cfg`?

This configuration file, located in folder `/opt/OV/newconfig/OVPM/smepack/VCENTER/data`, only contains a limited number of event types by default. It should be updated with any desired additional event type. Remember also that the type `AlarmStatusChangedEvent` is listed but commented out by default and should be uncommented if events of this type should be collected.

If all event types are deleted or commented out, then remember that only the events matching one of the thresholds 1 to 43 will be forwarded unless you updated the policy `vPV-EventMonitor` with your custom thresholds (see [Configuring VMware events forwarding to OM](#)).

3. Is the policy `vPV-EventMonitor` deployed with the correct policy interval?

This policy is responsible for forwarding the VMware events. The policy interval must be set equal to the collection interval, else a random amount of events will not be forwarded.

4. Are the parameters of policy `vPV-EventMonitor` set correctly?

Especially if VMware events of type `AlarmStatusChangedEvent` should be forwarded, it is mandatory to set the policy parameter `AlarmFlag` to `true`. Additional parameters are explained in this paper in [Configuring the forwarding of alarms](#).

5. Are we facing a VMware event collection problem or a VMware event forwarding problem?

The collection of VMware events and the forwarding of VMware events are two distinct processes that require distinct troubleshooting steps. The troubleshooting toolkit PVTk 2.0 includes a command that enables to quickly view which VMware events have been collected:

```
# /opt/OV/contrib/PVTk/pvdump -events
```

Analyzing the output of this command enables to distinguish between a collection and a forwarding problem.

For more hints on troubleshooting this type of problems, consult the PVTk 2.0 User and Reference Manual on page 24. This troubleshooting toolkit is available at <https://softwaresupport.softwaregrp.com/km/KM02600652>.

Send feedback to thierry.ledent@microfocus.com