Integrate VMware ESX/ESXi and vCenter Server
EventTracker v8.x and above
Abstract

This guide provides instructions to configure VMware to send the event logs to EventTracker Enterprise. Once events are configured to send to EventTracker Manager, alerts, dashboard and reports can be configured into EventTracker.

Scope

The configurations detailed in this guide are consistent with EventTracker Enterprise version 9.x and later, and VMware ESX 3-5.5 and vCenter 6.0 and 6.5.

Audience

VMware users, who wish to forward event logs to EventTracker Manager and monitor events using EventTracker Enterprise.
# Table of Contents

Abstract ............................................................................................................................................................. 1
Scope ................................................................................................................................................................. 1
Audience............................................................................................................................................................ 1
Overview................................................................................................................................................................ 3
Prerequisites.......................................................................................................................................................... 3
Configure VMware to forward logs to EventTracker ............................................................................................ 3
  Configure EventTracker Agent to receive VMware logs ................................................................................... 3
  Troubleshooting Techniques.................................................................................................................................... 6
EventTracker Knowledge Pack (KP) ....................................................................................................................... 7
  Categories.......................................................................................................................................................... 7
  Alerts ................................................................................................................................................................. 8
  Knowledge Objects............................................................................................................................................ 9
  Reports ............................................................................................................................................................ 10
Import Knowledge Pack into EventTracker ......................................................................................................... 20
  Import Category ........................................................................................................................................... 20
  Import Alerts ................................................................................................................................................ 21
  Import Tokens Template ................................................................................................................................. 22
  Import Knowledge Objects.............................................................................................................................. 23
  Import Flex Reports ...................................................................................................................................... 25
  Dashboards .................................................................................................................................................... 26
Verify Knowledge Pack in EventTracker .............................................................................................................. 29
  Category ....................................................................................................................................................... 29
  Alerts ............................................................................................................................................................ 30
  Token Values ............................................................................................................................................... 31
  Knowledge Object ....................................................................................................................................... 31
  Reports ........................................................................................................................................................ 32
  Dashboards ............................................................................................................................................... 33
Sample Flex Dashboards...................................................................................................................................... 34
Overview

VMware is a virtualization and cloud computing software provider for x86-compatible computers. VMware virtualization is based on the ESX/ESXi bare metal hypervisor, supporting virtual machines. The term "VMware" is often used about specific VMware Inc. products such as VMware vCenter, VMware Workstation, VMware View, VMware Horizon Application Manager and VMware vCloud Director.

Prerequisites

• EventTracker v9.x and later should be installed.
• VMware ESX/ESXi version 3-5.5 and vCenter version 6.0/6.5 Server should be installed.
• .NET Framework 3.5 should be installed on EventTracker Agent workstation where VMware is to be configured.

Configure VMware to forward logs to EventTracker

This configuration can be done on either EventTracker Manager or Agent.

Configure EventTracker Agent to receive VMware logs

• Go to the path where EventTracker Agent is installed and then locate and launch ETAconfig.exe as administrator. 
  (\%ET_Install_Path\Prism Microsystems\EventTracker\Agent\ETAconfig.exe)

• Click the Logfile Monitor tab and select respective checkbox. EventTracker displays the Logfile Monitor tab.
• Click **Add File Name**.
• Select the logfile type as **VMWARE** from the **Select Logfile Type** drop-down list. EventTracker displays the Enter File Name dialog box.
• Enter following details:

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
</table>
| VMware URL | Type the FQDN/IP address of the Vcenter/ESX server according to your infrastructure.  
  e.g. https://<esxvcservername>/sdk/vimService. |
| User Name  | Type Vcenter/ESX server Admin Credentials.                                  |
| Password   |                                                                             |
| Timeout    | Set appropriate connection timeout limit. Set to 60 by default.             |

**NOTE:** Configure vCenter URL only if multiple ESXi hosts are to be monitored. To monitor specific hosts, configure multiple LFMs with each ESXi host url.

• Click **Test Connection** to check if configuration parameters have been entered correctly.
• Click **OK**.  
  EventTracker displays the Agent Configuration Window.

![Figure 3](image)

• Click **Save**.
Troubleshooting Techniques

If you encounter any **Connection Errors** after you click **Test Connection**, follow the below mentioned steps.

![Figure 4](image)

- Check if the entered URL is correct.
  Access `https://<Vcenter/ESXiservername>:<Port>.sdk/vim.wsd` using a web browser, if you don’t get any connection errors’, the URL is correct. Otherwise please check the **URL** entered.

- Make sure you are using the valid credentials.
  Access the Web console UI (`https://<Vcenter/ESXiservername>:<Port>`) using the browser and type in the **admin** credentials entered in the configuration. If you are unable to login, the credentials entered are incorrect. Please verify and try again.

- Check the `<%ET_Install_Path%>\Prism Microsystems\EventTracker\Agent\ETAlog.txt` file, if you find errors,
  - Install **.NET Framework 3.5** on the system on the ET agent workstation where VMware integration was attempted.
  - Register **EtVMagent.dll**, To register the dll follow the below mentioned steps:
    - Open the **Command Prompt** as **Administrator**.
    - Change the directory of the command prompt to the directory where the agent is installed.
      ```
cd <%Eventracker_Install_Path%>\Prism Microsystems\EventTracker\Agent
```
    - Type the Command
      ```
      Regasm EtVMagent.dll
      ```
    - After registering a message will be displayed as shown below:
      “**Types registered successfully**”
Re-run the VMware Configuration.

EventTracker Knowledge Pack (KP)

Once logs are received in EventTracker; category, reports and dashboards can be configured in EventTracker.

Categories

- **VMware-Alarms triggered**: This category provides information about the logs related to alarms triggered.
- **VMware-Cluster created or removed**: This category provides information about the logs related to cluster created or removed.
- **VMware-Data center added or deleted**: This category provides information about the logs related to data center added or deleted.
- **VMware-Datstore creation or deletion**: This category provides information about the logs related to datastore creation or deletion.
- **VMware-ESXi host authentication failures**: This category provides information about the logs related to ESXi host authentication failures.
- **VMware-ESXi host login and logout**: This category provides information about the logs related to ESXi host login and logout.
- **VMware-Host added or removed**: This category provides information about the logs related to Host added or removed.
- **VMware-Policy and permission changes**: This category provides information about the logs related to policy and permission changes.
Integrate VMware ESXi and vCenter

- **VMware-vCenter auth failures**: This category provides information about the logs related to vCenter auth failures.
- **VMware-vCenter firewall configuration changes**: This category provides information about the logs related to vCenter firewall configuration changes.
- **VMware-vCenter login and logout**: This category provides information about the logs related to vCenter login and logout.
- **VMware-virtual machine connected and disconnected**: This category provides information about the logs related to virtual machine connected and disconnected.
- **VMware-virtual machine created or removed**: This category provides information about the logs related to virtual machine created or removed.
- **VMware-virtual machine installation errors**: This category provides information about the logs related to virtual machine installation errors.
- **VMware-virtual machine power on or off**: This category provides information about the logs related to virtual machine power on or off.

**Alerts**

- **VMware ESXi: Account created**: This alert is generated when an ESXi account is created.
- **VMware ESXi: Host added**: This alert is generated when an ESXi host is added.
- **VMware ESXi: Task failed**: This alert is generated when an ESXi Task fails.
- **VMware ESXi: Virtual machine created**: This alert is generated when an ESXi virtual machine is created.
- **VMware ESXi: Virtual machine reconfigured**: This alert is generated when an ESXi virtual machine is reconfigured.
- **VMware ESXi: User authentication failed**: This alert is generated when an ESXi authentication failure occurs.
- **VMware ESXi: User authentication success**: This alert is generated when an ESXi authentication is successful.
- **VMware ESXi: High resource usage alarm**: This alert is generated when utilization of ESXi resource is high.
- **VMware vCenter: User role deleted**: This alert is generated when a user role is deleted in vCenter.
- **VMware vCenter: User role modified**: This alert is generated when a user role is modified.
- **VMware vCenter: Virtual machine created**: This alert is generated when a virtual machine is created.
- **VMware vCenter: Virtual machine removed**: This alert is generated when a virtual machine is removed.
- **VMware vCenter: User permission removed**: This alert is generated when user permission on vCenter is removed.
- **VMware: Firewall configuration changed**: This alert is generated when firewall configuration changes are done.
Integrate VMware ESX/ESXi and vCenter

- **VMware ESX: Virtual machine created**: This alert is generated when an ESX virtual machine is created.
- **VMware ESX: Virtual machine reconfigured**: This alert is generated when an ESX virtual machine is reconfigured.
- **VMware ESX: High resource usage alarm**: This alert is generated when utilization of ESX resource is high.
- **VMware ESX: Task failed**: This alert is generated when an ESX Task fails.
- **VMware ESX: User authentication failed**: This alert is generated when an ESX authentication failure occurs.

**Knowledge Objects**

- **VMware Alarms triggered**: This knowledge objects provides information about the logs related to alarms triggered.
- **VMware Cluster created or removed**: This knowledge objects provides information about the logs related to cluster created or removed.
- **VMware Data center added or deleted**: This knowledge objects provides information about the logs related to data center added or deleted.
- **VMware Datastore creation or deletion**: This knowledge objects provides information about the logs related to datastore creation or deletion.
- **VMware ESXi host authentication failures**: This knowledge objects provides information about the logs related to ESXi host authentication failures.
- **VMware ESXi host login and logout**: This knowledge objects provides information about the logs related to ESXi host login and logout.
- **VMware Host added or removed**: This knowledge objects provides information about the logs related to host added or removed.
- **VMware Policy and permission changes**: This knowledge objects provides information about the logs related to policy and permission changes.
- **VMware vCenter auth failures**: This knowledge objects provides information about the logs related to vCenter auth failures.
- **VMware vCenter firewall configuration changes**: This knowledge objects provides information about the logs related to vCenter firewall configuration changes.
- **VMware vCenter login and logout**: This knowledge objects provides information about the logs related to vCenter login and logout.
- **VMware Virtual machine connected and disconnected**: This knowledge objects provides information about the logs related virtual machine connected and disconnected.
- **VMware Virtual machine created or removed**: This knowledge objects provides information about the logs related virtual machine created or removed.
• **VMware Virtual machine installation errors**: This knowledge objects provides information about the logs related to virtual machine installation errors.

• **VMware Virtual machine power on or off**: This knowledge objects provides information about the logs related to virtual machine power on or off.

### Reports

• **VMware- Alarms triggered**: This report provides information about the activities related to alarms triggered.

#### Figure 6

**Logs Considered:**

<table>
<thead>
<tr>
<th>LogTime</th>
<th>Computer</th>
<th>Target IP-Address</th>
<th>Virtual Machine Name</th>
<th>Alarm Reason</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>11/13/2017 07:03:12 AM</td>
<td>VCENTERTESTS-5.TOOLS.LOCAL@INTRDL013S-VMWARE</td>
<td>192.168.1.164</td>
<td>ESXWX19VM801</td>
<td>Virtual machine memory usage</td>
<td>Green to Yellow</td>
</tr>
<tr>
<td>11/13/2017 07:04:32 AM</td>
<td>VCENTERTESTS-5.TOOLS.LOCAL@INTRDL013S-VMWARE</td>
<td>192.168.1.164</td>
<td>ESXWX19VM801</td>
<td>Virtual machine memory usage</td>
<td>Yellow to Green</td>
</tr>
</tbody>
</table>

#### Figure 7

- Jun 27 08:26:46 PM Target: 192.168.1.24 Alarm "Virtual machine memory usage" on Eamba-Test changed from Gray to Green

*event_computer* ➔ VMware

*event_description* ➔ Target: 192.168.1.24, Alarm "Virtual machine memory usage" on Eamba-Test changed from Gray to Green

*event_id* ➔ 3230

*event_log_type* ➔ Application

*event_source* ➔ VMware-LFM

*event_type* ➔ Information

*event_user_domain* ➔ N/A

*event_user_name* ➔ N/A

*log_source* ➔ VMware Alarms triggered

*tags* ➔ VMware

**tags** ➔ Alarms

• **VMware- Cluster created or removed**: This report provides information about the activities related to cluster created or removed.

#### Figure 8

<table>
<thead>
<tr>
<th>LogTime</th>
<th>Computer</th>
<th>Task Name</th>
<th>Target Machine</th>
<th>Status</th>
<th>Initiated By</th>
<th>Start Time</th>
<th>Completed Time</th>
</tr>
</thead>
<tbody>
<tr>
<td>11/09/2017 04:31:30 PM</td>
<td>VCENTERTESTS-5.TOOLS.LOCAL@INTRDL013S-VMWARE</td>
<td>Folder createCluster0</td>
<td>host</td>
<td>Running</td>
<td>VSHERE-LOCAL\Administrator</td>
<td>11/09/2017 4:31:30 PM</td>
<td>11/09/2017 4:53:00 AM</td>
</tr>
</tbody>
</table>
**Logs Considered:**

- **VMware- Data center added or deleted:** This report provides information about the activities related to data center added or deleted.

---

**Log Time** | **Computer** | **Task Name** | **Target Machine** | **Initiated By** | **Status** | **Start Time** | **Completed Time**
--- | --- | --- | --- | --- | --- | --- | ---

11/09/2017 03:00:29 PM | VCSERTESTS-5.TOMKLS.LOCAL@MPRS-VWINWAR.BLA | Remove Datacenter | TestDC | VSPHERE LOCAL Administrator | Success | 11/09/2017 3:02:24 PM | 11/09/2017 3:02:24 PM

11/09/2017 03:00:49 PM | VCSERTESTS-5.TOMKLS.LOCAL@MPRS-VWINWAR.BLA | Create Datacenter | Datacenters | VSPHERE LOCAL Administrator | Success | 11/09/2017 3:02:45 PM | 11/09/2017 3:02:45 PM

---

**Figure 9**

- **VMware- Data center added or deleted:** This report provides information about the activities related to data center added or deleted.

---

**Figure 10**
Integrate VMware ESX/ESXi and vCenter

Logs Considered:

<table>
<thead>
<tr>
<th>Event Time</th>
<th>Computer</th>
<th>Target IP Address</th>
<th>User Name</th>
<th>Host IP Address</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1/11/2017 12:35:39 PM</td>
<td>VCenterTest-5T00NS LOCAL@NTPDFT/BLGSS-VMWARE</td>
<td>192.168.1.184</td>
<td>N/A</td>
<td>192.168.1.42</td>
<td>Cannot login</td>
</tr>
<tr>
<td>1/11/2017 12:36:30 PM</td>
<td>VCenterTest-5T00NS LOCAL@NTPDFT/BLGSS-VMWARE</td>
<td>192.168.1.184</td>
<td>Administrator</td>
<td>192.168.1.42</td>
<td>Cannot login</td>
</tr>
<tr>
<td>1/11/2017 12:37:30 PM</td>
<td>VCenterTest-5T00NS LOCAL@NTPDFT/BLGSS-VMWARE</td>
<td>192.168.1.184</td>
<td>netman</td>
<td>192.168.1.42</td>
<td>Cannot login</td>
</tr>
<tr>
<td>1/11/2017 12:38:30 PM</td>
<td>VCenterTest-5T00NS LOCAL@NTPDFT/BLGSS-VMWARE</td>
<td>192.168.1.184</td>
<td>ADMIN</td>
<td>192.168.1.42</td>
<td>Cannot login</td>
</tr>
<tr>
<td>1/11/2017 12:39:30 PM</td>
<td>VCenterTest-5T00NS LOCAL@NTPDFT/BLGSS-VMWARE</td>
<td>192.168.1.184</td>
<td>admin</td>
<td>192.168.1.42</td>
<td>Cannot login</td>
</tr>
<tr>
<td>1/11/2017 12:40:25 PM</td>
<td>VCenterTest-5T00NS LOCAL@NTPDFT/BLGSS-VMWARE</td>
<td>192.168.1.184</td>
<td>root</td>
<td>locked for 126 seconds after 43 failed login attempts</td>
<td></td>
</tr>
</tbody>
</table>

- **VMware-ESXi host authentication failures:** This report provides information about the activities related to ESXi host authentication failures.

Figure 11

Figure 12
Integrate VMware ESX/ESXi and vCenter

Logs Considered:

<table>
<thead>
<tr>
<th>Event</th>
<th>Computer</th>
<th>Source IP Address</th>
<th>User Name</th>
<th>Action</th>
<th>User Agent</th>
</tr>
</thead>
<tbody>
<tr>
<td>Jun 27 03:26:03 PM</td>
<td>VCENTERTESTB-5.TOUNS.LOCAL@NTPLDDBLS0-VMWARE</td>
<td>127.0.0.1</td>
<td>VSHERE.LOCAL\vsphere-extension-99180229-b032-41e5-9002-9a35c2d5a5bf</td>
<td>logged in</td>
<td>web-client/6.5.0</td>
</tr>
<tr>
<td>Jun 27 03:26:03 PM</td>
<td>VCENTERTESTB-5.TOUNS.LOCAL@NTPLDDBLS0-VMWARE</td>
<td>127.0.0.1</td>
<td>VSHERE.LOCAL\vsphere-extension-99180229-b032-41e5-9002-9a35c2d5a5bf</td>
<td>logged out</td>
<td>web-client/6.5.0</td>
</tr>
</tbody>
</table>

**Figure 13**

- **VMware-ESXi host login and logout**: This report provides information about the activities related to ESXi host login and logout.

Logs Considered:

<table>
<thead>
<tr>
<th>Event</th>
<th>User root@10.224.16.23 logged in as Java/1.8.0_60-internal</th>
<th>Source IP Address</th>
</tr>
</thead>
<tbody>
<tr>
<td>Jun 27 03:26:03 PM</td>
<td></td>
<td>10.224.16.23</td>
</tr>
</tbody>
</table>

**Figure 14**

**Figure 15**
• **VMware- Policy and permission changes:** This report provides information about the activities related to policy and permission changes.

<table>
<thead>
<tr>
<th>User Name</th>
<th>Action</th>
<th>Changed From</th>
<th>Changed To</th>
<th>Changed On</th>
<th>Status</th>
</tr>
</thead>
<tbody>
<tr>
<td>VSphere LOCALS\Administrators</td>
<td>Permission changed</td>
<td>Administrator</td>
<td>Administrator</td>
<td>Datacenters</td>
<td>Enabled</td>
</tr>
<tr>
<td>VSphere LOCALS\Administrators</td>
<td>Permission changed</td>
<td>Administrator</td>
<td>Administrator</td>
<td>Datacenters</td>
<td>Disabled</td>
</tr>
<tr>
<td>VSphere LOCALS\Administrators</td>
<td>Permission changed</td>
<td>Administrator</td>
<td>Administrator</td>
<td>Datacenters</td>
<td>Enabled</td>
</tr>
<tr>
<td>VSphere LOCALS\Administrators</td>
<td>Permission changed</td>
<td>Administrator</td>
<td>Administrator</td>
<td>Datacenters</td>
<td>Disabled</td>
</tr>
<tr>
<td>VSphere LOCALS\Administrator</td>
<td>Permission created</td>
<td>datastore1</td>
<td>datastore1</td>
<td>datastore1</td>
<td>Enabled</td>
</tr>
<tr>
<td>VSphere LOCALS\cheetah</td>
<td>Permission created</td>
<td>datastore1</td>
<td>datastore1</td>
<td>datastore1</td>
<td>Enabled</td>
</tr>
</tbody>
</table>

Figure 16

**Logs Considered:**

```plaintext
<table>
<thead>
<tr>
<th>action</th>
<th>event_computer</th>
<th>event_description</th>
<th>event_id</th>
<th>event_log_type</th>
<th>event_source</th>
<th>event_type</th>
<th>event_user_domain</th>
<th>event_user_name</th>
<th>log_source</th>
<th>logs</th>
<th>tags</th>
<th>tags</th>
<th>logs</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td>123456</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Permission created</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
```

Figure 17

• **VMware- ESXi host added or removed:** This report provides information about the activities related to ESXi host added or removed.

<table>
<thead>
<tr>
<th>LogTime</th>
<th>Computer</th>
<th>Target IP Address</th>
<th>Datacenter Name</th>
<th>Host IP Address</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>1/10/2017 02:38:51 PM</td>
<td>VCENTERTEST\S-TOONS.LOCAL\TPlot\CDE-VMWARE</td>
<td>192.168.1.24</td>
<td>Test DC</td>
<td>192.168.1.24</td>
<td>Removed</td>
</tr>
<tr>
<td>1/10/2017 02:39:31 PM</td>
<td>VCENTERTEST\S-TOONS.LOCAL\TPlot\CDE-VMWARE</td>
<td>192.168.1.24</td>
<td>Test DC</td>
<td>192.168.1.24</td>
<td>Added</td>
</tr>
</tbody>
</table>

Figure 18
Integrate VMware ESX/ESXi and vCenter

Logs Considered:

- Jun 27 03:26:33 PM Target: 192.168.1.24 Removed host 192.168.1.24 in Test DC
  - dest_ip_address: 192.168.1.24
  - event_computer: VMware
  - event_description: Target: 192.168.1.24
  - event_id: 3230
  - event_log_type: Application
  - event_source: VMware-LPM
  - event_type: Information
  - event_user_domain: N/A
  - event_user_name: N/A
  - log_source: VMware Host Added or Removed
  - service_name: Test DC
  - src_ip_address: 192.168.1.24
  - tags: VMware
  - tags: Host Added
  - tags: Host Removed

Figure 19

- **VMware- vCenter login and logout:** This report provides information about the activities related to vCenter login and logout.

<table>
<thead>
<tr>
<th>LogTime</th>
<th>Computer</th>
<th>User Name</th>
<th>Source IP Address</th>
<th>Action</th>
<th>User Agent</th>
</tr>
</thead>
<tbody>
<tr>
<td>11/19/2017 01:18:02 PM</td>
<td>VCENTERTEST-5.TOONS.LOCAL@HTPBUMB-VMWARE</td>
<td>VSHERE.LOCAL</td>
<td>127.0.0.1</td>
<td>logged out</td>
<td>web-client8.5.0</td>
</tr>
<tr>
<td>11/19/2017 01:18:02 PM</td>
<td>VCENTERTEST-5.TOONS.LOCAL@HTPBUMB-VMWARE</td>
<td>VSHERE.LOCAL</td>
<td>127.0.0.1</td>
<td>logged in</td>
<td>web-client8.5.0</td>
</tr>
<tr>
<td>11/19/2017 01:19:03 PM</td>
<td>VCENTERTEST-5.TOONS.LOCAL@HTPBUMB-VMWARE</td>
<td>VSHERE.LOCAL</td>
<td>127.0.0.1</td>
<td>logged in</td>
<td>web-client8.5.0</td>
</tr>
<tr>
<td>11/19/2017 01:30:45 PM</td>
<td>VCENTERTEST-5.TOONS.LOCAL@HTPBUMB-VMWARE</td>
<td>VSHERE.LOCAL</td>
<td>127.0.0.1</td>
<td>logged in</td>
<td>web-client8.5.0</td>
</tr>
<tr>
<td>11/19/2017 01:30:45 PM</td>
<td>VCENTERTEST-5.TOONS.LOCAL@HTPBUMB-VMWARE</td>
<td>VSHERE.LOCAL</td>
<td>127.0.0.1</td>
<td>logged out</td>
<td>web-client8.5.0</td>
</tr>
</tbody>
</table>

Figure 20

Logs Considered:

- Jun 27 03:20:33 PM User root@10.224.16.22 logged out (Login time: Wednesday, 06 September, 2017 21:14:54, number of API invocations: 0, user agent: Java/1.8.0_60-interna0)
  - event_log_type: Application
  - event_type: Information
  - event_id: 3230
  - event_source: VMware-LPM
  - event_user_domain: N/A
  - event_user_name: N/A
  - event_description: User root@10.224.16.22 logged out (Login time: Wednesday, 06 September, 2017 21:14:54, number of API invocations: 0, user agent: Java/1.8.0_60-interna0)

Figure 21
• **VMware- Virtual machine connected and disconnected**: This report provides information about the activities related to virtual machine connected and disconnected.

<table>
<thead>
<tr>
<th>LogTime</th>
<th>Computer</th>
<th>Target IP Address</th>
<th>Datacenter Name</th>
<th>Virtual Machine Name</th>
<th>Host IP Address</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>11/08/2017 02:38:45 PM</td>
<td>VCENTERTESTS-5.TOONS LOCAL@HTPLD7B3S-VMWARE</td>
<td>192.168.1.24</td>
<td>Test DC</td>
<td>R155-VMI14</td>
<td>192.168.1.24</td>
<td>disconnected</td>
</tr>
<tr>
<td>11/08/2017 02:38:45 PM</td>
<td>VCENTERTESTS-5.TOONS LOCAL@HTPLD7B3S-VMWARE</td>
<td>192.168.1.24</td>
<td>Test DC</td>
<td>R155-VMI14 (guest)</td>
<td>192.168.1.24</td>
<td>disconnected</td>
</tr>
<tr>
<td>11/08/2017 02:38:45 PM</td>
<td>VCENTERTESTS-5.TOONS LOCAL@HTPLD7B3S-VMWARE</td>
<td>192.168.1.24</td>
<td>Test DC</td>
<td>ETVAS8BM-Production</td>
<td>192.168.1.24</td>
<td>disconnected</td>
</tr>
<tr>
<td>11/08/2017 02:38:45 PM</td>
<td>VCENTERTESTS-5.TOONS LOCAL@HTPLD7B3S-VMWARE</td>
<td>192.168.1.24</td>
<td>Test DC</td>
<td>NTPL-VI6TA DC</td>
<td>192.168.1.24</td>
<td>disconnected</td>
</tr>
<tr>
<td>11/08/2017 02:38:45 PM</td>
<td>VCENTERTESTS-5.TOONS LOCAL@HTPLD7B3S-VMWARE</td>
<td>192.168.1.24</td>
<td>Test DC</td>
<td>R155-VMI8</td>
<td>192.168.1.24</td>
<td>disconnected</td>
</tr>
<tr>
<td>11/08/2017 02:38:45 PM</td>
<td>VCENTERTESTS-5.TOONS LOCAL@HTPLD7B3S-VMWARE</td>
<td>192.168.1.24</td>
<td>Test DC</td>
<td>NTPL-TEST ET DC</td>
<td>192.168.1.24</td>
<td>disconnected</td>
</tr>
<tr>
<td>11/08/2017 02:38:45 PM</td>
<td>VCENTERTESTS-5.TOONS LOCAL@HTPLD7B3S-VMWARE</td>
<td>192.168.1.24</td>
<td>Test DC</td>
<td>R153-VMI10(Testing)</td>
<td>192.168.1.24</td>
<td>disconnected</td>
</tr>
</tbody>
</table>

**Figure 22**

**Logs Considered:**

```
Jun 27 09:29:34 PM Target: 192.168.1.24 NTPL-CASRY on host 192.168.1.24 in Test DC is disconnected
```

- `application_name`: Target: 192.168.1.24 NTPL-CASRY
- `event_computer`: VMware
- `event_description`: NTPL-CASRY on host 192.168.1.24 in Test DC is disconnected
- `event_id`: 3230
- `event_log_type`: Application
- `event_source`: VMware-LM
- `event_type`: Information
- `event_user_domain`: N/A
- `event_user_name`: N/A
- `log_status`: VMware Virtual machine connected and disconnected
- `service_name`: Test DC
- `src_ip_address`: 192.168.1.24
- `tags`: Connected

**Figure 23**

• **VMware- vCenter Firewall configuration changes**: This report provides information about the activities related to vCenter firewall configuration changes.

<table>
<thead>
<tr>
<th>LogTime</th>
<th>Computer</th>
<th>Target IP Address</th>
<th>Action</th>
<th>Configured Object</th>
<th>Status</th>
</tr>
</thead>
<tbody>
<tr>
<td>11/09/2017 04:38:37 PM</td>
<td>VCENTERTESTS-5.TOONS LOCAL@HTPLD7B3S-VMWARE</td>
<td>192.168.1.24</td>
<td>enable</td>
<td>ssClient</td>
<td>succeeded</td>
</tr>
<tr>
<td>11/09/2017 04:38:45 PM</td>
<td>VCENTERTESTS-5.TOONS LOCAL@HTPLD7B3S-VMWARE</td>
<td>192.168.1.24</td>
<td>enable</td>
<td>VSIP</td>
<td>succeeded</td>
</tr>
<tr>
<td>11/09/2017 04:38:45 PM</td>
<td>VCENTERTESTS-5.TOONS LOCAL@HTPLD7B3S-VMWARE</td>
<td>192.168.1.24</td>
<td>enable</td>
<td>remoteSerialPort</td>
<td>succeeded</td>
</tr>
<tr>
<td>11/09/2017 04:38:45 PM</td>
<td>VCENTERTESTS-5.TOONS LOCAL@HTPLD7B3S-VMWARE</td>
<td>192.168.1.24</td>
<td>enable</td>
<td>nfsClient</td>
<td>succeeded</td>
</tr>
<tr>
<td>11/09/2017 04:38:45 PM</td>
<td>VCENTERTESTS-5.TOONS LOCAL@HTPLD7B3S-VMWARE</td>
<td>192.168.1.24</td>
<td>enable</td>
<td>ntpClient</td>
<td>succeeded</td>
</tr>
</tbody>
</table>

**Figure 24**
### Logs Considered:

<table>
<thead>
<tr>
<th>Log Time</th>
<th>Computer</th>
<th>Target IP Address</th>
<th>Virtual Machine Name</th>
<th>Action</th>
<th>Host IP Address</th>
<th>Datacenter Name</th>
</tr>
</thead>
<tbody>
<tr>
<td>11/06/2017 02:38:49 PM</td>
<td>VICTTEST5-5.TOOKS.LOCAL@NTPLOTBLS8-VMWARE</td>
<td>192.168.1.124</td>
<td>R155-VM21</td>
<td>Removed</td>
<td>192.168.1.24</td>
<td>Test DC</td>
</tr>
<tr>
<td>11/06/2017 02:38:49 PM</td>
<td>VICTTEST5-5.TOOKS.LOCAL@NTPLOTBLS8-VMWARE</td>
<td>192.168.1.124</td>
<td>R155-VM2(Server 2016)</td>
<td>Removed</td>
<td>192.168.1.24</td>
<td>Test DC</td>
</tr>
<tr>
<td>11/06/2017 02:38:49 PM</td>
<td>VICTTEST5-5.TOOKS.LOCAL@NTPLOTBLS8-VMWARE</td>
<td>192.168.1.124</td>
<td>R154-4433(2016)</td>
<td>Removed</td>
<td>192.168.1.24</td>
<td>Test DC</td>
</tr>
<tr>
<td>11/06/2017 02:38:49 PM</td>
<td>VICTTEST5-5.TOOKS.LOCAL@NTPLOTBLS8-VMWARE</td>
<td>192.168.1.124</td>
<td>R153-V81</td>
<td>Removed</td>
<td>192.168.1.24</td>
<td>Test DC</td>
</tr>
<tr>
<td>11/06/2017 02:38:49 PM</td>
<td>VICTTEST5-5.TOOKS.LOCAL@NTPLOTBLS8-VMWARE</td>
<td>192.168.1.124</td>
<td>vCenter Production</td>
<td>Removed</td>
<td>192.168.1.24</td>
<td>Test DC</td>
</tr>
<tr>
<td>11/06/2017 02:38:49 PM</td>
<td>VICTTEST5-5.TOOKS.LOCAL@NTPLOTBLS8-VMWARE</td>
<td>192.168.1.124</td>
<td>R153-V812(Testing)</td>
<td>Removed</td>
<td>192.168.1.24</td>
<td>Test DC</td>
</tr>
<tr>
<td>11/06/2017 02:38:49 PM</td>
<td>VICTTEST5-5.TOOKS.LOCAL@NTPLOTBLS8-VMWARE</td>
<td>192.168.1.124</td>
<td>NTP-LVD/2</td>
<td>Removed</td>
<td>192.168.1.24</td>
<td>Test DC</td>
</tr>
</tbody>
</table>

- **VMware** - **Virtual machine created or removed**: This report provides information about the activities related to virtual machine created or removed.
**Logs Considered:**

- Jun 27 03:29:33 PM Target: 192.168.1.24 Created virtual machine Symantec on 192.168.1.24 in Test DC

<table>
<thead>
<tr>
<th>Time</th>
<th>Computer</th>
<th>Host IP Address</th>
<th>Machine Name</th>
<th>Datacenter Name</th>
<th>Message</th>
</tr>
</thead>
<tbody>
<tr>
<td>11/1/2017 14:45:57 AM</td>
<td>VCENTERTEST-5.TODORO.LOOKOUT@3PITBLR8-VNWARE</td>
<td>192.168.1.184</td>
<td>ESXW01N1W01</td>
<td>Test DC</td>
<td>User has entered a standby sleep state. Use the keyboard or mouse while grabbed to wake it.</td>
</tr>
<tr>
<td>11/1/2017 11:15:26 AM</td>
<td>VCENTERTEST-5.TODORO.LOOKOUT@3PITBLR8-VNWARE</td>
<td>192.168.1.104</td>
<td>ESXW01N1W01</td>
<td>Test DC</td>
<td>User has entered a standby sleep state. Use the keyboard or mouse while grabbed to wake it.</td>
</tr>
<tr>
<td>11/1/2017 11:45:18 AM</td>
<td>VCENTERTEST-5.TODORO.LOOKOUT@3PITBLR8-VNWARE</td>
<td>192.168.1.104</td>
<td>ESXW01N1W01</td>
<td>Test DC</td>
<td>User has entered a standby sleep state. Use the keyboard or mouse while grabbed to wake it.</td>
</tr>
<tr>
<td>11/1/2017 12:18:32 PM</td>
<td>VCENTERTEST-5.TODORO.LOOKOUT@3PITBLR8-VNWARE</td>
<td>192.168.1.184</td>
<td>ESXW01N1W01</td>
<td>Test DC</td>
<td>User has entered a standby sleep state. Use the keyboard or mouse while grabbed to wake it.</td>
</tr>
<tr>
<td>11/1/2017 12:47:19 PM</td>
<td>VCENTERTEST-5.TODORO.LOOKOUT@3PITBLR8-VNWARE</td>
<td>192.168.1.184</td>
<td>ESXW01N1W01</td>
<td>Test DC</td>
<td>User has entered a standby sleep state. Use the keyboard or mouse while grabbed to wake it.</td>
</tr>
</tbody>
</table>

**Figure 27**

- **VMware- Virtual machine installation errors:** This report provides information about the activities related to virtual machine installation errors.

**Figure 28**
Integrate VMware ESX/ESXi and vCenter

Logs Considered:

**Figure 29**

- **VMware- Virtual machine power on or off:** This report provides information about the activities related to virtual machine power on or off.

<table>
<thead>
<tr>
<th>LogTime</th>
<th>Computer</th>
<th>Target IP Address</th>
<th>Virtual Machine Name</th>
<th>Host IP Address</th>
<th>Datacenter Name</th>
<th>State</th>
</tr>
</thead>
<tbody>
<tr>
<td>11/95/2017 02:13:56 PM</td>
<td>vCenter-TestVM</td>
<td>192.168.1.24</td>
<td>vcenter-vbox</td>
<td>192.168.1.24</td>
<td>Test DC</td>
<td>powered off</td>
</tr>
<tr>
<td>11/95/2017 02:14:15 PM</td>
<td>vCenter-TestVM</td>
<td>192.168.1.24</td>
<td>vcenter-testVM</td>
<td>192.168.1.24</td>
<td>Test DC</td>
<td>powered on</td>
</tr>
<tr>
<td>11/95/2017 02:14:15 PM</td>
<td>vCenter-TestVM</td>
<td>192.168.1.24</td>
<td>vCenter-TestVM</td>
<td>192.168.1.24</td>
<td>Test DC</td>
<td>powered on</td>
</tr>
<tr>
<td>11/95/2017 02:14:20 PM</td>
<td>vCenter-TestVM</td>
<td>192.168.1.24</td>
<td>vCenter-TestVM</td>
<td>192.168.1.24</td>
<td>Test DC</td>
<td>powered on</td>
</tr>
<tr>
<td>11/95/2017 02:14:20 PM</td>
<td>vCenter-TestVM</td>
<td>192.168.1.24</td>
<td>vCenter-TestVM</td>
<td>192.168.1.24</td>
<td>Test DC</td>
<td>powered on</td>
</tr>
<tr>
<td>11/95/2017 02:14:20 PM</td>
<td>vCenter-TestVM</td>
<td>192.168.1.24</td>
<td>vCenter-TestVM</td>
<td>192.168.1.24</td>
<td>Test DC</td>
<td>powered on</td>
</tr>
<tr>
<td>11/95/2017 02:14:20 PM</td>
<td>vCenter-TestVM</td>
<td>192.168.1.24</td>
<td>vCenter-TestVM</td>
<td>192.168.1.24</td>
<td>Test DC</td>
<td>powered on</td>
</tr>
</tbody>
</table>

**Figure 30**

- **Logs Considered:**

<table>
<thead>
<tr>
<th>LogTime</th>
<th>Target: 192.168.1.24 vcenter-vbox on 192.168.1.24 in Test DC is powered off</th>
</tr>
</thead>
<tbody>
<tr>
<td>event_log_type</td>
<td>Application</td>
</tr>
<tr>
<td>event_type</td>
<td>Information</td>
</tr>
<tr>
<td>event_id</td>
<td>3333</td>
</tr>
<tr>
<td>event_source</td>
<td>VMware</td>
</tr>
<tr>
<td>event_user_domain</td>
<td>N/A</td>
</tr>
<tr>
<td>event_computer</td>
<td>VMware</td>
</tr>
<tr>
<td>event_user_name</td>
<td>N/A</td>
</tr>
<tr>
<td>event_description</td>
<td>Target: 192.168.1.24 vcenter-vbox on 192.168.1.24 in Test DC is powered off</td>
</tr>
</tbody>
</table>

**Figure 31**
• **VMware - Datastore creation or deletion:** This report provides information about the activities related to datastore creation or deletion.

<table>
<thead>
<tr>
<th>Log Time</th>
<th>Computer</th>
<th>Target IP Address</th>
<th>Datastore Type</th>
<th>Datastore Name</th>
<th>Datastore Configured Paths</th>
<th>Action</th>
<th>Host IP Address</th>
<th>Datacenter Name</th>
</tr>
</thead>
<tbody>
<tr>
<td>11/06/2017 22:41:17 PM</td>
<td>VCENTERTEST2-5STGNS.LOCAL\VPMS\BLA52-VVMWARE</td>
<td>192.168.1.24</td>
<td>VMFS</td>
<td>datastore1</td>
<td>ds://vmfs/volumes/59514b20-a5d3b7f4-e6f4-1866da68b50ee/</td>
<td>Created</td>
<td>192.168.1.24</td>
<td>Test DC</td>
</tr>
</tbody>
</table>

**Figure 32**

**Logs Considered:**

<table>
<thead>
<tr>
<th>Event Log Type</th>
<th>Event Type</th>
<th>Event ID</th>
<th>Event Source</th>
<th>Event User Domain</th>
<th>Event Computer</th>
<th>Event User Name</th>
<th>Event Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Application</td>
<td>Information</td>
<td>3230</td>
<td>VMware-ERM</td>
<td>N/A</td>
<td>VMware</td>
<td>N/A</td>
<td>Target: 192.168.1.24 Created VMFS datastore datastore1 (ds://vmfs/volumes/59514b20-a5d3b7f4-e6f4-1866da68b50ee/) on 192.168.1.24 in Test DC</td>
</tr>
</tbody>
</table>

**Figure 33**

**Import Knowledge Pack into EventTracker**

**NOTE:** Import knowledge pack items in the following sequence:

- Categories
- Alerts
- Parsing Rules/Token Template
- Knowledge Objects
- Flex Reports
- Dashboards

**Import Category**

1. Click **Category** option, and then click the browse button.
2. Locate **Category_VMware.iscat** file, and then click the **Open** button.

3. To import categories, click the **Import** button.

   EventTracker displays success message.

4. Click **OK**, and then click the **Close** button.

**Import Alerts**

1. Click Alert option, and then click the browse button.

2. Locate **Alert_Trend Micro CM.isalt** file, and then click the **Open** button.
3. To import alerts, click the **Import** button.

![Figure 36](image)

4. Click **OK**, and then click the **Close** button.

![Figure 37](image)

**Import Tokens Template**

- Logon to **EventTracker Enterprise**.
- Click the **Admin** menu, and then click **Parsing Rules**.
• Select **Template** tab, locate the **Token_Template_VMware.ettd** file.
• Select all the reports by clicking on the check box.
• Click on the **Import** icon.

![Import](Figure 38)

![Import](Figure 39)

• **Templates are now imported successfully.**

![Import](Figure 40)

**Import Knowledge Objects**

1. Click **Knowledge objects** under Admin option in the EventTracker manager page.
2. Locate the file named `KO_VMware.etko`.

![Figure 41](image)

3. Now select all the check box and then click on ‘Import’ option.

![Figure 42](image)

4. Knowledge objects are now imported successfully.
Import Flex Reports

1. Click **Reports** option, and select new (.etcrx) from the option.

2. Locate the file named **Reports_VMware.etcrx**, and select all the check box.
3. Click the **Import** button to import the reports. EventTracker displays success message.

![Figure 45](image)

### Dashboards

**Note:** If you have EventTracker Enterprise version v9.0, you can import dashboards.

1. Open **EventTracker Enterprise**.
2. Navigate to Dashboard>My Dashboard. My Dashboard pane is shown.

3. Click the ‘Import’ button to import the dashlets.
4. Locate the **Dashboard_Trend Micro CM.etwd** file.
5. Click the ‘Upload’ option.

![Figure 49](image)

6. Now select all the check box and then click on ‘Import’ option. Dashlets are now imported successfully.
7. Click the ‘Add’ button to create a new dashlet.

![Figure 50](image)
8. Fill suitable Title and Description and click Save button.

9. Click ‘Customize’ to locate Trend Micro CM dashlets and choose all created dashlets for Trend Micro CM and choose all created dashlets.

10. Click ‘Add’ dashlet to create dashboard.

**Verify Knowledge Pack in EventTracker**

**Category**

1. Logon to EventTracker Enterprise.
2. Click the Admin menu, and then click Category.
3. In Category Group Tree to view imported category, scroll down and click VMware group folder.

Category are displayed in the pane.
Integrate VMware ESX/ESXi and vCenter

Figure 52

Alerts

1. In the EventTracker Enterprise web interface, click the Admin dropdown, and then click Alerts.
2. In search box, enter VMware and then click the Search button.

EventTracker displays alert of VMware.
Token Values

1. Logon to EventTracker Enterprise.
2. Click the Admin menu, and then click Parsing Rules.
3. In Token Value Group Tree to view imported token values, scroll down and click VMware group folder. Token values are displayed in the token value pane.

Knowledge Object

1. Logon to EventTracker Enterprise.
2. Click the Admin menu, and then click Knowledge Object.
3. In Knowledge Object Group Tree to view imported knowledge object, scroll down and click VMware group folder.

Knowledge Object are displayed in the pane.
Integrate VMware ESX/ESXi and vCenter

1. Logon to EventTracker Enterprise.
2. Click the Reports menu, and then Configuration.
4. In Report Groups Tree to view imported Scheduled Reports, scroll down and click VMware group folder.

Reports are displayed in the Reports configuration pane.
Integrate VMware ESX/ESXi and vCenter

Dashboards

1. Open EventTracker Enterprise in browser and logon.
2. Navigate to Dashboard>My Dashboard.
   My Dashboard pane is shown.
Sample Flex Dashboards

**VMware - Cluster created or removed by username:** This dashboard provides information related to cluster created or removed.

![Figure 58](image)

**VMware - VMs created or removed:** This dashboard provides information related to VMs created or removed.

![Figure 59](image)
VMware - VMware ESXi login logout details by source IP address: This dashboard provides information related to ESXi login logout details.

![Figure 60](image)

VMware - vCenter firewall configuration changes by username: This dashboard provides information related to firewall configuration changes.

![Figure 61](image)
VMware - Host Added or Removed by source IP address: This dashboard provides information related hosts added or removed.

Figure 62

VMware - vCenter authentication failures by username: This dashboard provides information related to vCenter Authentication failures.

Figure 63
**VMware - ESXi host login and logout by username:** This dashboard provides information related to vCenter host login and logout.

![Pie chart showing login logout details](image)

**Figure 64**