Integrate Microsoft Hyper-V Server

EventTracker Enterprise
About this Guide

This guide will facilitate a Hyper-V user to send windows logs to EventTracker Enterprise.

Scope

The configurations detailed in this guide are consistent with EventTracker Enterprise 7.x or later and Hyper-V applies to version windows 2008 and later.

Audience

Administrators who want to monitor Hyper-V using EventTracker Enterprise.
# Table of Contents

About this Guide .......................................................................................................................... 1  
Scope ........................................................................................................................................... 1  
Audience ...................................................................................................................................... 1  
Introduction .................................................................................................................................. 3  
Pre-requisites ............................................................................................................................... 3  
Configuration ............................................................................................................................... 3  
EventTracker Knowledge Pack ...................................................................................................... 9  
Categories ................................................................................................................................. 9  
Alerts ........................................................................................................................................... 10  
Reports ....................................................................................................................................... 11  
Importing Hyper-V knowledge pack into EventTracker ............................................................. 16  
Category .................................................................................................................................... 17  
Alerts .......................................................................................................................................... 19  
Parsing rules ............................................................................................................................... 20  
Flex Reports ............................................................................................................................... 21  
Templates .................................................................................................................................. 22  
Verifying Hyper-V knowledge pack in EventTracker ................................................................. 23  
Categories ................................................................................................................................ 23  
Alerts .......................................................................................................................................... 24  
Tokens ....................................................................................................................................... 25  
Reports ...................................................................................................................................... 26  
Template .................................................................................................................................... 27  
Create Flex Dashboards in EventTracker .................................................................................. 28  
Schedule Reports ....................................................................................................................... 28  
Create Dashlets ........................................................................................................................ 31  
Sample Dashboards ................................................................................................................... 35
Introduction

The Hyper-V server role in Windows Server lets you create a virtualized server computing environment where you can create and manage virtual machines. You can run multiple operating systems on one physical computer and isolate the operating systems from each other. With this technology, you can improve the efficiency of your computing resources and free up your hardware resources.

Pre-requisites

- EventTracker 7.x or later should be installed.
- Hyper-V management tool should be installed.

Configuration

In order to send logs into the EventTracker Enterprise follow the below steps:-

**Step 1:** Open Event viewer in Hyper-V manager machine.

**Step 2:** Click on the following node as shown in the left side of the screen:

Expand Application and services logs>>Microsoft>>Windows and scroll down.

![Image of Event Viewer]

Figure 1
Step 3: Click on the required Hyper-V node in order to know the source like shown below:
Sources which are considered are:

- Hyper-V-VMMS
- Hyper-V-Hypervisor
- Hyper-V-VmSwitch
- Hyper-V-SynthNic
- Hyper-V-Worker
- Hyper-V-High-Availability

**NOTE:** Deploy EventTracker Agent in the Hyper-V manager machine in order to add the above sources into the EventTracker agent.


**NOTE:** We add the sources in order to receive real time logs into the EventTracker Enterprise.

To add the above specified source in agent configuration please follow the below steps.

**Step 4:** Select the **Start > All Programs > Prism Microsystems > EventTracker**.

**Step 5:** In **EventTracker Control Panel**, and select **EventTracker Agent Configuration**.

**Step 6:** Select **Event Filters** tab, and then click the **Filter Exception** button.
Filter Exception window displays.

**Step 7:** Click the **New** button.
Event Details window displays.

**Step 8:** In **Match in Source** box, enter ‘Microsoft-Windows-Hyper-V’.
Step 9: Click the OK button.
Step 10: Step 7, Step 8 and Step 9 must be followed in order to add the above sources which are mentioned into the filter exception.
Step 11: **Save** the configuration and **Close** the EventTracker Agent Configuration window.
EventTracker Knowledge Pack

Once Hyper-V events are enabled and Hyper-V events are received in EventTracker, Alerts and Reports can be configured in EventTracker.

The following Knowledge Packs are available in EventTracker to support Hyper-V monitoring.

Categories

- **Hyper V: Image management service status**
  This report provides information related to image management service, i.e whether the image management service has started or stopped.

- **Hyper V: Switch port created**
  This report provides information related to virtual switch port created.

- **Hyper V: Virtual machine operational message**
  This report provides information related to virtual machine operational messages which explains whether the machine was restored, started, saved, paused, resumed, reset and reset by the guest operating system.

- **Hyper V: Virtual SAN management**
  This report provides information related to SAN management, i.e. whether the Storage area network has been created or deleted.

- **Hyper V: Virtual switch created**
  This report provides information related to virtual switch which has been created.

- **Hyper V: Virtual switch deleted**
  This report provides information related to virtual switch which has been deleted.

- **Hyper V: Virtual switch setup started**
  This report provides information related to virtual switch whose setup has been started.

- **Hyper V: VM failed to unregister**
  This report provides information related to un-registered virtual machine that explains regarding the configuration of the machine where an error occurs to be failed.

- **Hyper V: New partition created**
  This report provides information related to a partition which has been created.

- **Hyper V: Partition deleted**
This report provides information related to a partition which has been deleted.

- **Hyper V: Virtual disk compacted**  
  This report provides information related to virtual disk which has been compacted.

- **Hyper V: Virtual disk converted**  
  This report provides information related to virtual disk which has been converted.

- **Hyper V: Virtual disk create failed**  
  This report provides information related to virtual disk which has failed to create.

- **Hyper V: Virtual disk created**  
  This report provides information related to virtual disk which has been created.

- **Hyper V: Virtual disk expanded**  
  This report provides information related to virtual disk which has been expanded.

### Alerts

- **Hyper V: System create failed**  
  This alert is generated when a system fails to create for the given path.

- **Hyper V: Virtual machine deleted**  
  This alert is generated when virtual machine is deleted.

- **Hyper V: Virtual machine shutdown**  
  This alert is generated when virtual machine is shutdown.

- **Hyper V: Configuration error**  
  This alert is generated when a configuration error has occurred in the system.

- **Hyper V: Network adapter create failed**  
  This alert is generated when a network had failed to create a network adapter.

- **Hyper V: Network conflict**  
  This alert is generated when a network conflict has occurred at another adapter.

- **Hyper V: Network resource error**  
  This alert is generated when certain type of network resource error has occurred.
Reports

- **Hyper V-Virtual hard disk partition management**
  This report provides information related to hard disk partition management that explains about hard disk partition and the value of partition.

  **SAMPLE LOG:**

  ![Figure 8](image)

  **SAMPLE REPORT**

  ![Figure 9](image)

- **Hyper V-Virtual SAN management**
  This report provides information related to SAN management that is whether the Storage area network has been created or removed.

  **SAMPLE LOG:**

  ![Figure 10](image)
• **Hyper V-Virtual switch port created**
  This report provides information related to virtual switch created where it explains about which switch is created along with their port name.

**SAMPLE LOG**

![Sample Log Image](image)

**Figure 12**

**SAMPLE REPORT**

![Sample Report Image](image)

**Figure 13**

• **Hyper V-Virtual machine create**
  This report provides information related to virtual machine that is it explains about whether the virtual machine has been created.

**SAMPLE LOG**

![Sample Log Image](image)

**Figure 14**

**SAMPLE REPORT**
EventTracker: Integrate Microsoft Hyper-V Server

- **Hyper V-Virtual machine operational message**
  This report provides information related to virtual machine operational messages which explains whether the machine was restored, started, saved, paused, resumed, reset and reset by the guest operating system.

  **SAMPLE LOG**

  ![Figure 15](image)

  ![Figure 16](image)

  **SAMPLE REPORT**

  ![Figure 17](image)

- **Hyper V-VM failed to unregister**
  This report provides information related to un-registered virtual machine that explains regarding the configuration of the machine where an error occurs to be failed.

  **SAMPLE LOG**
• Hyper V-Image management service status
  This report provides information related to image management service that is whether the service has been started or stopped.

SAMPLE LOG

• Hyper V-Virtual disk image management
  This report provides information related to virtual disk image management which explains about different managements like create, convert, expand, compact, or failed to create etc.
• Hyper V-Virtual Switch management
  This report provides information related to virtual switch management that explains about whether the virtual switch has been created or deleted or set up.
SAMPLE REPORT

<table>
<thead>
<tr>
<th>LogTime</th>
<th>Computer</th>
<th>Machine Name</th>
<th>Status</th>
</tr>
</thead>
<tbody>
<tr>
<td>06/21/2016 12:53:57 PM</td>
<td>HYPER-V3</td>
<td>test</td>
<td>created</td>
</tr>
<tr>
<td>06/21/2016 12:53:58 PM</td>
<td>HYPER-V3</td>
<td>test</td>
<td>deleted</td>
</tr>
<tr>
<td>06/21/2016 12:53:58 PM</td>
<td>HYPER-V3</td>
<td>Virtual machine test</td>
<td>set up</td>
</tr>
<tr>
<td>06/21/2016 12:53:58 PM</td>
<td>HYPER-V3</td>
<td>Virtual machine test</td>
<td>set up</td>
</tr>
</tbody>
</table>

Figure 25

Importing Hyper-V knowledge pack into EventTracker

1. Launch EventTracker Control Panel.
2. Double click Export Import Utility, and then click Import tab.
   - Import
     I. Templates
     II. Category
     III. Alerts
     IV. Parsing rules
     V. Flex Reports

   **NOTE:** Importing should be in the same order as mentioned above.
Category

1. Click **Category** option, and then click the browse button.
2. Locate All Hyper V Categories.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.
Alerts

1. Click **Alerts** option, and then click the **browse** button.

![Figure 29]

2. Locate **All Hyper V Alerts.isalt** file, and then click the **Open** button.

3. To import alerts, click the **Import** button.
   
   EventTracker displays success message.

![Figure 30]

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

1. Click **Token value** option, and then click the **browse** button.

   ![Figure 31](image)

2. Locate **All Hyper V Parsing rules.istoken** file, and then click the **Open** button.

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

   EventTracker displays success message.

   ![Figure 32](image)

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

1. Click **Report** option, and then click the **browse** button.

![Figure 33](image)

2. Locate **All Hyper V Report.issch** file, and then click the **Open** button.

3. To import scheduled reports, click the **Import** button.

EventTracker displays success message.

![Figure 34](image)

4. Click **OK**, and then click the **Close** button.
EventTracker: Integrate Microsoft Hyper-V Server

Templates

1. Click the Admin menu, and then click Parsing rule.

2. Select Template tab, and then click on ‘Import’ option.

3. Click on Browse button.

4. Locate All Hyper V Template.ettld file, and then click the Open button.
5. Now select the check box and then click on 'Import' option. EventTracker displays success message.

![Template(s) imported successfully](image)

6. Click on OK button.

**Verifying Hyper-V knowledge pack in EventTracker Categories**

1. Logon to EventTracker Enterprise web interface.
2. Click the Admin menu, and then click Categories.
3. In **Category Tree** to view imported categories, scroll down and expand **Hyper V** group folder to view the imported categories.

![Category Tree](image)

**Figure 39**

### Alerts

1. Logon to **EventTracker Enterprise** web interface.
2. Click the **Admin** menu, and then click **Alerts**.
3. In **Search** field, type ‘**Hyper V**’, and then click the **Go** button.

   Alert Management page will display all the imported **Hyper V** alerts.
4. To activate the imported alerts, select the respective checkbox in the **Active** column.

   EventTracker displays message box.

   ![Successful activation message]

   **Figure 41**

5. Click **OK**, and then click the **Activate Now** button.

   **NOTE:**

   You can select alert notification such as Beep, Email, and Message etc. For this, select the respective checkbox in the Alert management page, and then click the **Activate Now** button.

**Tokens**

1. Logon to **EventTracker Enterprise** web interface.

2. Click the **Admin** menu, and then click **Parsing Rules**.

   The imported **Hyper V** tokens are added in Token-Value Groups list.
Reports

1. Logon to EventTracker Enterprise.
2. Click the Reports menu, and then select Configuration.
3. In Reports Configuration pane, select Defined option.
   EventTracker displays Defined page.
4. In search box enter Hyper V, and then click the Search button.
   EventTracker displays Flex reports of Hyper V.
Template

1. Logon to **EventTracker Enterprise** web interface.

2. Click the **Admin** menu, and then click **Parsing Rules** and click **Template**.
Create Flex Dashboards in EventTracker

**NOTE:** To configure the flex dashboards, schedule and generate the reports. Flex dashboard feature is available from EventTracker Enterprise v8.0 and later.

**Schedule Reports**

1. Open EventTracker in browser and logon.

![Figure 44: Create Flex Dashboards in EventTracker](image)
2. Navigate to Reports>Configuration.

3. Select Hyper V in report groups. Check Defined dialog box.

4. Click on ‘schedule’ to plan a report for later execution.
Figure 47
5. Check column names to persist using PERSIST checkboxes beside them. Choose suitable Retention period.
6. Proceed to next step and click Schedule button.
7. Wait till the reports get generated.

Create Dashlets

1. Open EventTracker in browser and logon.
3. Navigate to Dashboard>Flex. Flex Dashboard pane is shown.

4. Fill suitable title and description and click Save button.

5. Click ☰ to configure a new flex dashlet. Widget configuration pane is shown.
6. Locate earlier scheduled report in **Data Source** dropdown.
7. Select **Chart Type** from dropdown.
8. Select extent of data to be displayed in **Duration** dropdown.
9. Select computation type in **Value Field Setting** dropdown.
10. Select evaluation duration in **As Of** dropdown.
11. Select comparable values in **X Axis** with suitable label.
12. Select numeric values in **Y Axis** with suitable label.
13. Select comparable sequence in **Legend**.
14. Click **Test** button to evaluate. Evaluated chart is shown.
2. If satisfied, click **Configure** button

3. Click ‘customize’ 📠 to locate and choose created dashlet.
4. Click 🔄 to add dashlet to earlier created dashboard.
Sample Dashboards

For below dashboard DATA SOURCE: Hyper-V-Virtual machine operational

**WIDGET TITLE:** Hyper-V-Virtual machine operational  
**CHART TYPE:** Stacked Column  
**AXIS LABELS [X-AXIS]:** Operation message  
**Label Text:** User Name  
**FILTER:** Machine Name  
**FILTER VALUES:** Vmesx3-VM2- Testing

1. Hyper-V-Virtual machine operational message.

![Figure 54](image-url)