

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.

The information contained in this document represents the current view of Prism Microsystems Inc. on the issues discussed as of the date of publication. Because Prism Microsystems must respond to changing market conditions, it should not be interpreted to be a commitment on the part of Prism Microsystems, and Prism Microsystems cannot guarantee the accuracy of any information presented after the date of publication.

This document is for informational purposes only. Prism Microsystems MAKES NO WARRANTIES, EXPRESS OR IMPLIED, AS TO THE INFORMATION IN THIS DOCUMENT.

Complying with all applicable copyright laws is the responsibility of the user. Without limiting the rights under copyright, this paper may be freely distributed without permission from Prism, as long as its content is unaltered, nothing is added to the content and credit to Prism is provided.

Prism Microsystems may have patents, patent applications, trademarks, copyrights, or other intellectual property rights covering subject matter in this document. Except as expressly provided in any written license agreement from Prism Microsystems, the furnishing of this document does not give you any license to these patents, trademarks, copyrights, or other intellectual property.

The example companies, organizations, products, people and events depicted herein are fictitious. No association with any real company, organization, product, person or event is intended or should be inferred.

© 2016 Prism Microsystems Corporation. All rights reserved. The names of actual companies and products mentioned herein may be the trademarks of their respective owners.

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.

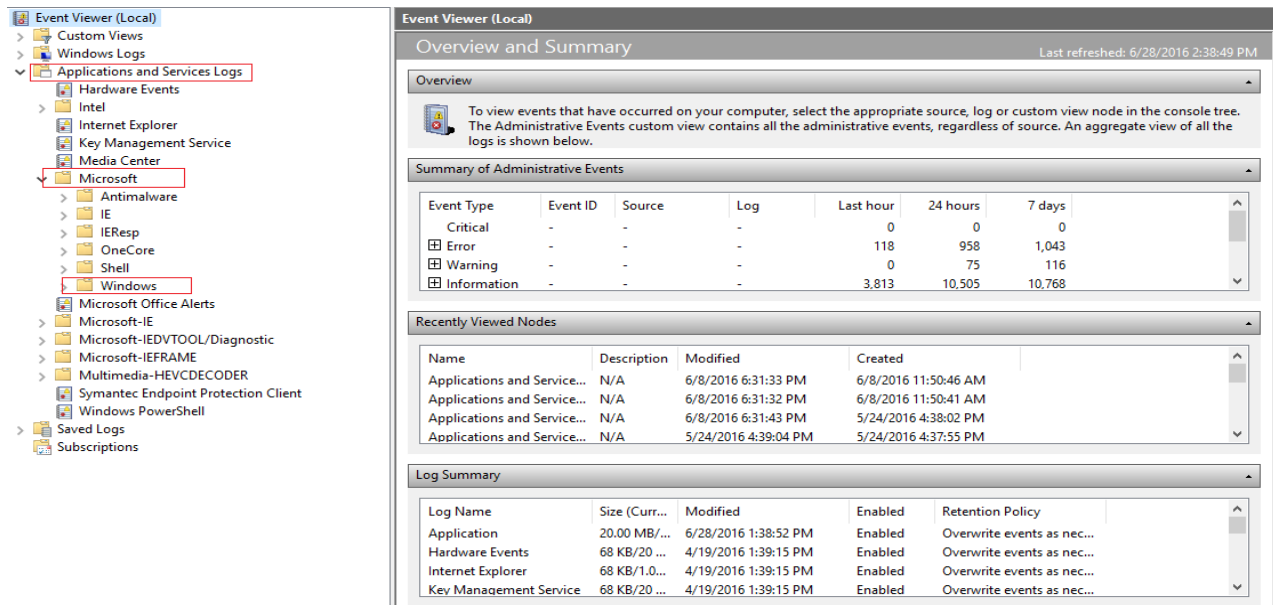


Figure 1

EventTracker: Integrate Microsoft Hyper-V Server

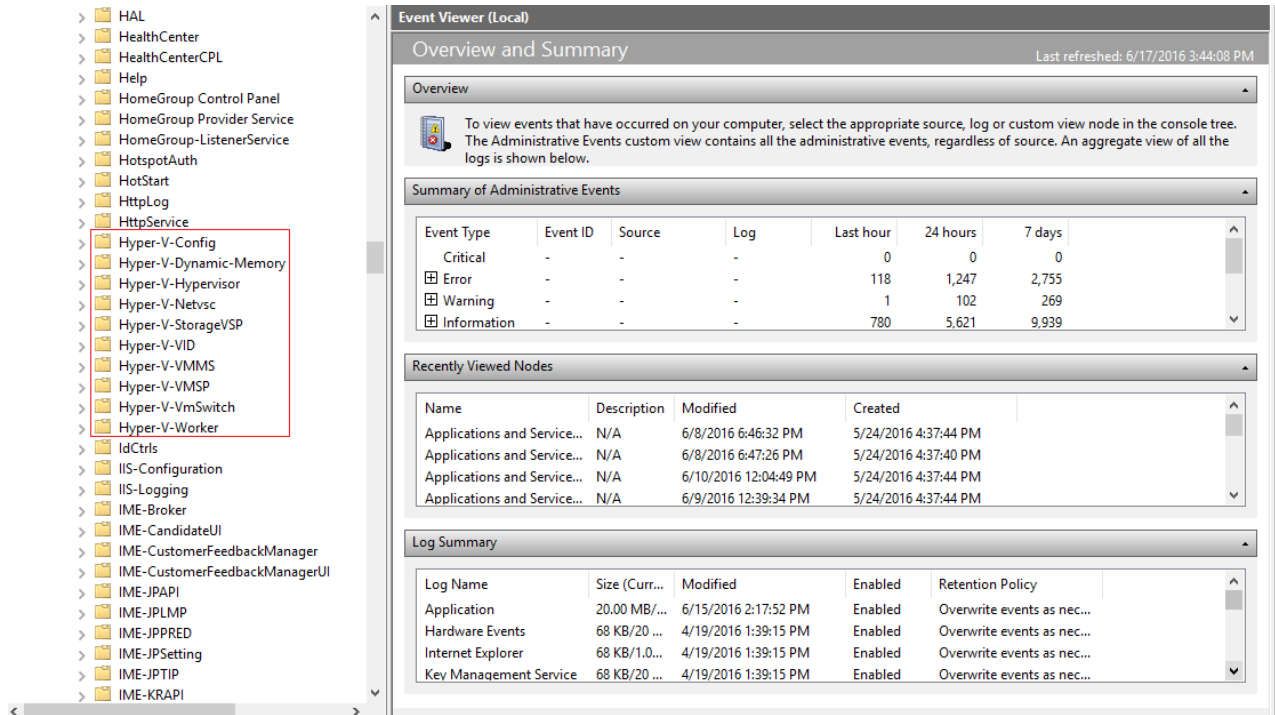


Figure 2

Step 3: Click on the required Hyper-V node in order to know the source like shown below:

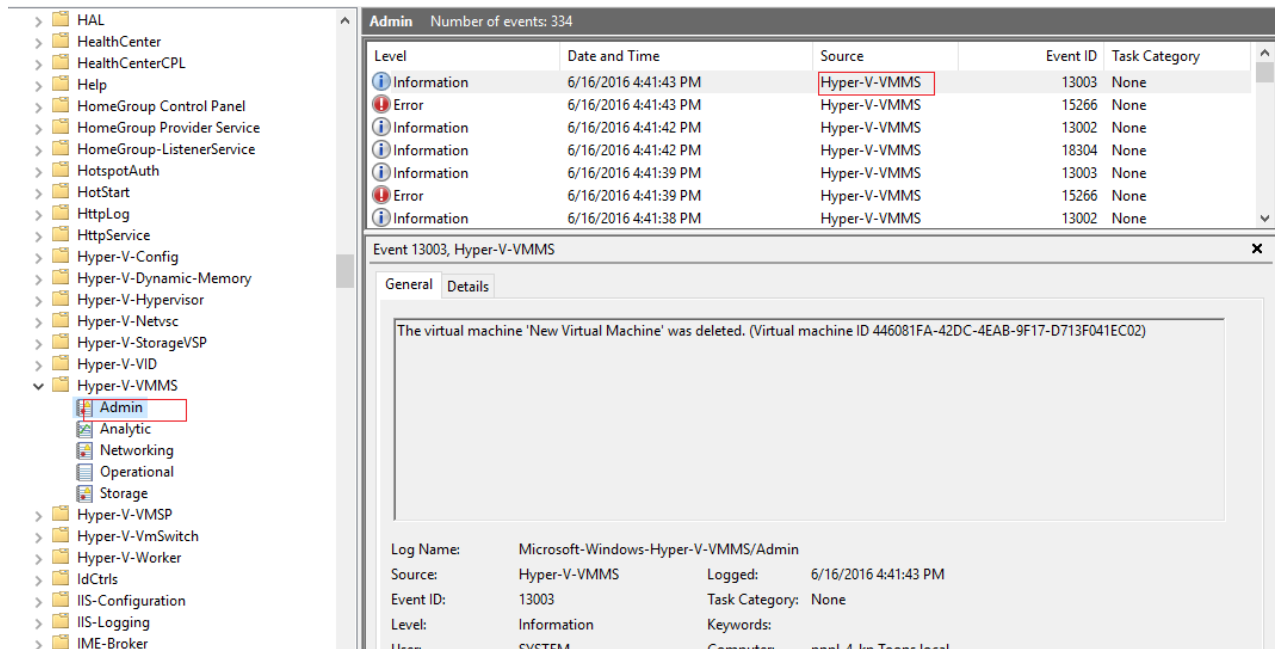


Figure 3

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.

<https://www.eventtracker.com/wp-content/support-docs/How-to-Install-EventTracker-and-Change-Audit-Agent.pdf>

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.

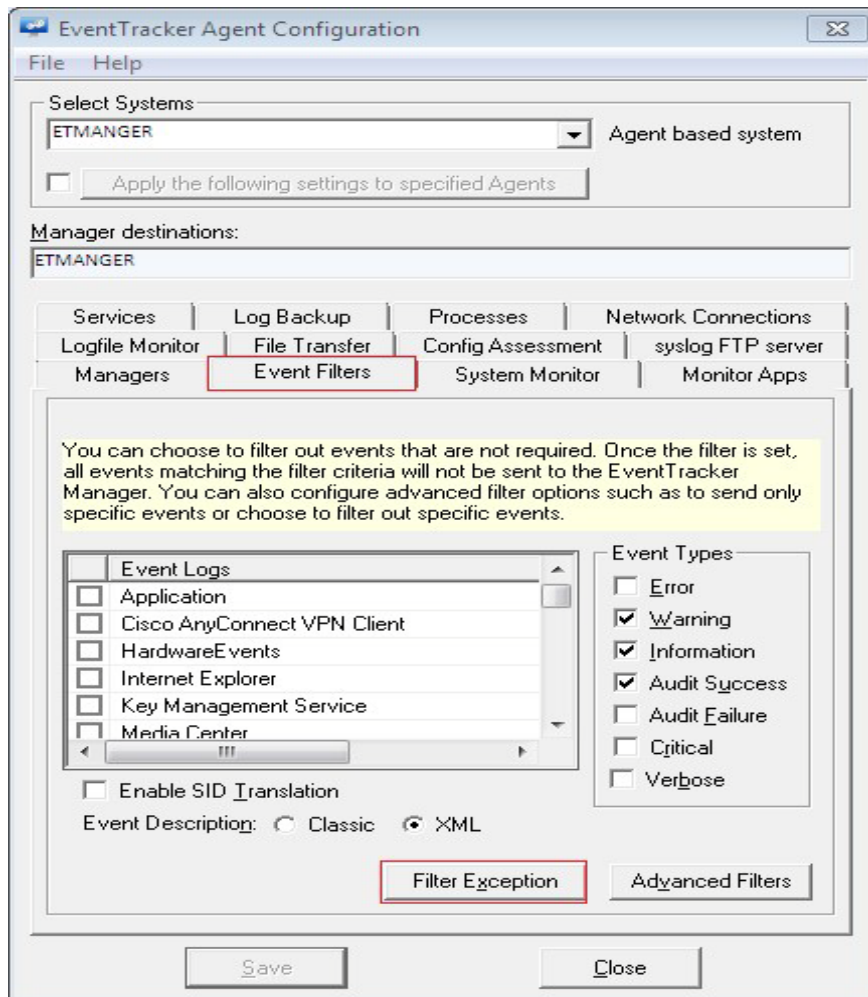


Figure 4

Filter Exception window displays.

Step 7: Click the **New** button.

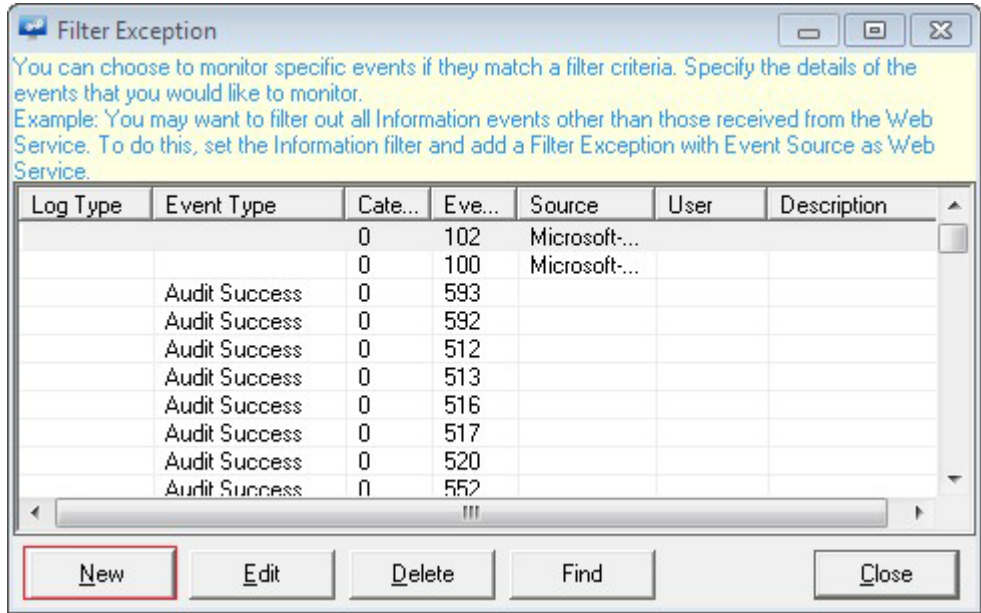


Figure 5

Event Details window displays.

Step 8: In **Match in Source:** box, enter 'Microsoft-Windows-Hyper-V'.

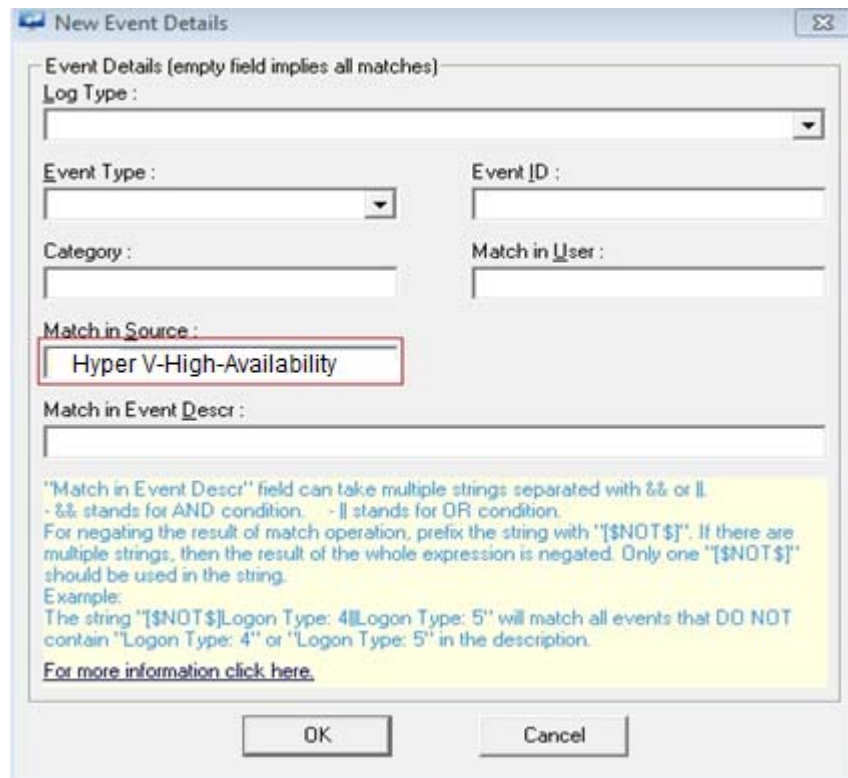


Figure 6

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.

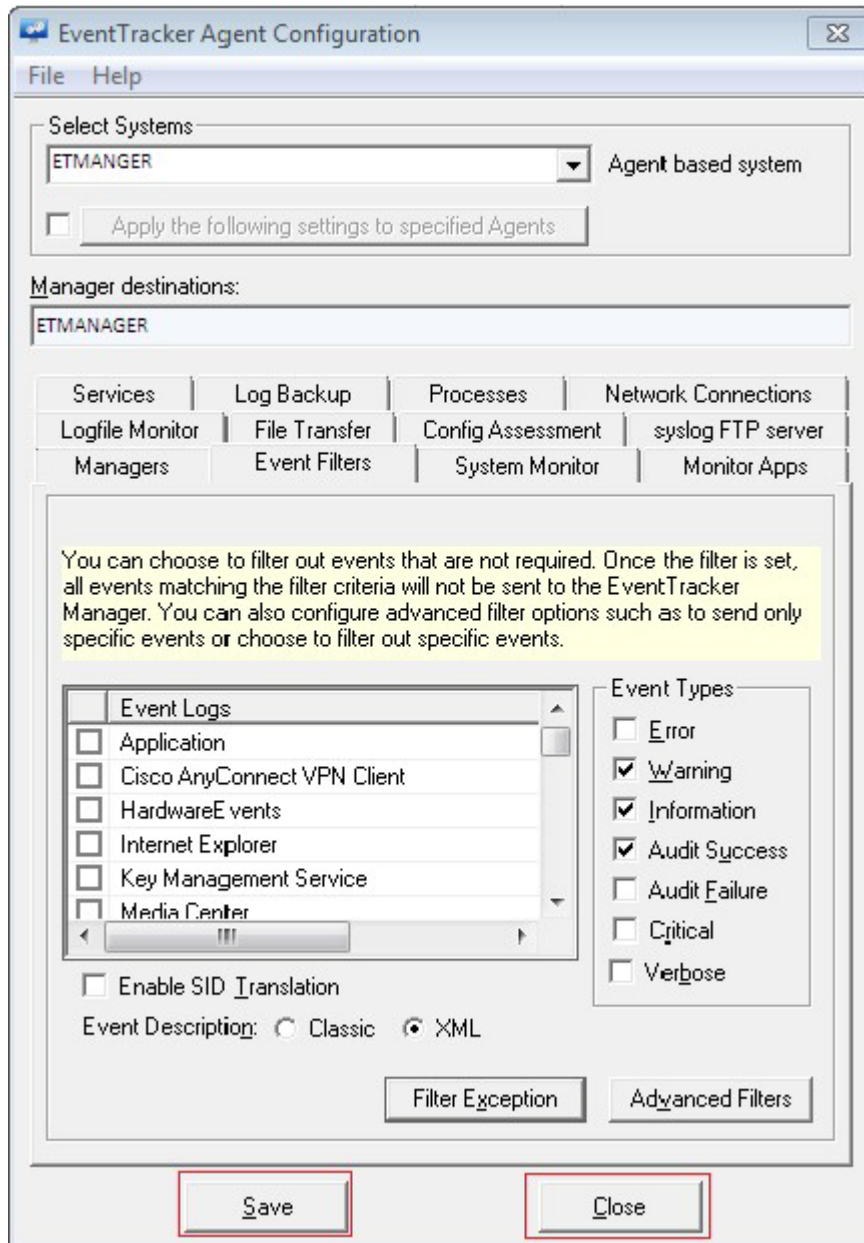


Figure 7

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:

6/16/2016 2:23:00 PM	16641	PNPL-4-KP / VMESX3	SYSTEM	NT AUTHORITY	Microsoft-Windows-Hyper-V-Hypervisor
Event Type: Information Log Type: Microsoft-Windows-Hyper-V-Hypervisor-Operational Category Id: 0		Description: Hyper-V successfully created a new partition (partition 6). <EventData><Data Name="PartitionId">6</Data></EventData>			
6/16/2016 1:56:27 PM	16642	PNPL-4-KP / VMESX3	SYSTEM	NT AUTHORITY	Microsoft-Windows-Hyper-V-Hypervisor
Event Type: Information Log Type: Microsoft-Windows-Hyper-V-Hypervisor-Operational Category Id: 0		Description: Hyper-V successfully deleted a partition (partition 41). <EventData><Data Name="PartitionId">41</Data></EventData>			

Figure 8

SAMPLE REPORT

LogTime	Computer	Partition Status	Partition Number
06/03/2016 09:38:35 AM	VMESX3	deleted	partition 90
06/03/2016 09:38:35 AM	VMESX3	deleted	partition 90
06/03/2016 09:38:35 AM	VMESX3	created	partition 94
06/03/2016 09:38:35 AM	VMESX3	created	partition 94

Figure 9

- **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:

6/14/2016 5:29:46 PM	32190	PNPL-4-KP / PNPL-4-K...	Michel	TOONS	Microsoft-Windows-Hyper-V-VMMS
Event Type: Information Log Type: Microsoft-Windows-Hyper-V-VMMS-Admin Category Id: 0		Description: A new virtual SAN with name Computing was created			
6/14/2016 5:29:11 PM	32191	PNPL-4-KP / PNPL-4-K...	Michel	TOONS	Microsoft-Windows-Hyper-V-VMMS
Event Type: Information Log Type: Microsoft-Windows-Hyper-V-VMMS-Admin Category Id: 0		Description: Virtual SAN with name Computing was removed			

Figure 10

SAMPLE REPORT

LogTime	EventUser	Computer	Storage Area Network Name	Status
06/09/2016 12:39:26 PM	Michel	PNPL-4-KP	Computing	created
06/09/2016 12:39:31 PM	Michel	PNPL-4-KP	Computing	removed

Figure 11

- **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

6/15/2016 11:58:58 AM 26004 PNPL-4-KP / PNPL-4-K... SYSTEM NT AUTHORITY Microsoft-Windows-Hyper-V-VMMS

Event Type: Information
Log Type: Microsoft-Windows-Hyper-V-VMMS-Networking
Category Id: 0

Description:
 Switch port created, switch name = "2BBE2297-BE5B-45E2-9F0E-0BE748E69688", switch friendly name = "switch 1", port name = "53F7ECAE-51C6-4346-994A-BBD6D6A4DC64", port friendly name="switch 1".

Figure 12

SAMPLE REPORT

LogTime	Computer	Switch Name	Port Name
06/01/2016 06:04:36 PM	PNPL-4-KP	New Virtual Switch	New Virtual Switch
06/07/2016 03:04:34 PM	PNPL-4-KP	New Virtual Switch	New Virtual Switch
06/07/2016 03:04:34 PM	PNPL-4-KP	New Virtual Switch	New Virtual Switch_External
06/07/2016 04:19:12 PM	PNPL-4-KP	New Virtual Switch	New Virtual Switch
06/07/2016 04:19:41 PM	PNPL-4-KP	New Virtual Switch	New Virtual Switch

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

LOG TIME	EVENT ID	SITE / COMPUTER	USER	DOMAIN	SOURCE
6/30/2016 6:47:20 PM	8024	PNPL-4-KP / PNPL-4-K...	Michel	TOONS	Microsoft-Windows-Hyper-V-VMMS

Event Type: Information
Log Type: Application
Category Id: 0

Description:
 The system successfully created "D:\may\hyperv\roover.vhdx". A new virtual machine "roover" was created. (Virtual machine ID 491F5B9F-217A-40FF-972D-069511B454F6)

Figure 14

SAMPLE REPORT

LogTime	EventUser	Computer	Machine Name	File Path Of Hard Disk
06/30/2016 06:47:20 PM	michel	PNPL-4-KP	roover	D:\may\hyperv\roover.vhdx

Figure 15

- **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

6/16/2016 1:55:24 PM	18510	PNPL-4-KP / VMESX3	Michel	NT VIRTUAL MACH...	Microsoft-Windows-Hyper-V-Worker
Event Type: Information Log Type: Microsoft-Windows-Hyper-V-Worker-Admin Category Id: 0 Description: "Vmesx3-vm9" saved successfully. (Virtual machine ID CFCFA073C-4B2B-46C6-8EB6-E054380D4B8A)					
6/16/2016 11:31:08 AM	18512	PNPL-4-KP / VMESX3	Michel	NT VIRTUAL MACH...	Microsoft-Windows-Hyper-V-Worker
Event Type: Information Log Type: Microsoft-Windows-Hyper-V-Worker-Admin Category Id: 0 Description: "Vmesx3-vm9" was reset. (Virtual machine ID CFCFA073C-4B2B-46C6-8EB6-E054380D4B8A)					

Figure 16

SAMPLE REPORT

LogTime	Computer	EventUser	Machine Name	Operation Message
05/27/2016 04:12:23 PM	VMESX3	michel	Vmesx3-vm9	reset by the guest operating system.
05/27/2016 07:08:39 PM	VMESX3	michel	Vmesx3-VM2- Testing	turned off.
05/27/2016 07:09:14 PM	VMESX3	rachel	Vmesx3-VM2- Testing	started successfully
05/30/2016 05:59:38 PM	VMESX3	ronaldino	vmesx3-vm1	reset.
06/03/2016 09:41:13 AM	PNPL-4-KP	donald	windows 7	saved successfully
06/03/2016 09:43:29 AM	PNPL-4-KP	johnathan	windows 7	restored successfully.
06/08/2016 04:20:20 PM	PNPL-4-KP	roger	windows 7	paused.
06/08/2016 04:20:27 PM	PNPL-4-KP	johnathan	windows 7	resumed.

Figure 17

- **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

6/27/2016 12:07:59 PM 21502 PNPL-4-KP / Hyperv3 SYSTEM N/A Microsoft-Windows-Hyper-V-High-Availabil...

Event Type: Error
Log Type: Application
Category Id: 0

Description:
"Virtual Machine Configuration Server1_VM" failed to unregister the virtual machine with the Virtual Machine Management Service.

Figure 18

SAMPLE REPORT

LogTime	Computer	Machine Name
06/21/2016 07:00:30 PM	HYPERV3	"Virtual Machine Configuration Server1_VM"

Figure 19

- **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

6/27/2016 12:09:57 PM 15201 PNPL-4-KP / Hyperv2 SYSTEM N/A Microsoft-Windows-Hyper-V-Image-Managemen...

Event Type: Information
Log Type: Application
Category Id: 0

Description:
The Hyper-V Image Management service stopped.

6/27/2016 12:09:57 PM 15200 PNPL-4-KP / Hyperv2 SYSTEM N/A Microsoft-Windows-Hyper-V-Image-Managemen...

Event Type: Information
Log Type: Application
Category Id: 0

Description:
The Hyper-V Image Management Service started.

Figure 20

SAMPLE REPORT

LogTime	Computer	Status
06/21/2016 03:23:24 PM	HYPERV2	started
06/21/2016 03:23:24 PM	HYPERV2	started
06/21/2016 03:23:24 PM	HYPERV2	started
06/21/2016 03:23:24 PM	HYPERV2	started
06/21/2016 03:23:24 PM	HYPERV2	stopped
06/21/2016 03:23:24 PM	HYPERV2	stopped

Figure 21

- **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.

SAMPLE LOG

6/27/2016 12:11:48 PM	15105	PNPL-4-KP / Hyper-V...	SYSTEM	N/A	Microsoft-Windows-Hyper-V-Image-Manageme...
Event Type: Error					
Log Type: Application					
Category Id: 0					
Description: The system successfully expanded "E:\VMachine\Virtual Machines est5.vhd".					
6/27/2016 12:11:48 PM	15101	PNPL-4-KP / Hyper-V...	SYSTEM	N/A	Microsoft-Windows-Hyper-V-Image-Manageme...
Event Type: Error					
Log Type: Application					
Category Id: 0					
Description: The system successfully compacted "E:\VMachine\Virtual Machines est1.vhd".					
6/27/2016 12:11:48 PM	15107	PNPL-4-KP / Hyper-V...	SYSTEM	N/A	Microsoft-Windows-Hyper-V-Image-Manageme...
Event Type: Error					
Log Type: Application					
Category Id: 0					
Description: The system successfully converted "E:\VMachine\Virtual Machines est3.vhd".					

Figure 22

SAMPLE REPORT

LogTime	Computer	File Path Name	Status
06/20/2016 06:49:12 PM	HYPERR-V2	E:\VMachine\Virtual Machinesest2.vhd	failed to create
06/20/2016 06:49:12 PM	HYPERR-V2	E:\VMachine\Virtual Machinesest3.vhd	successfully converted
06/20/2016 06:49:12 PM	HYPERR-V2	E:\VMachine\Virtual Machinesest4.vhd	successfully created
06/20/2016 06:49:12 PM	HYPERR-V2	E:\VMachine\Virtual Machinesest5.vhd	successfully expanded
06/20/2016 06:49:12 PM	HYPERR-V2	E:\VMachine\Virtual Machinesest1.vhd	successfully compacted

Figure 23

- **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 LOG

6/27/2016 12:15:49 PM	26000	PNPL-4-KP / Hyper-V3	SYSTEM	N/A	Microsoft-Windows-Hyper-V-VMMS
Event Type: Information					
Log Type: Application					
Category Id: 0					
Description: Switch created, name="DFC3A82F-C7CF-4F49-B470-9F64004DD1B2", friendly name="test".					
6/27/2016 12:15:49 PM	14020	PNPL-4-KP / Hyper-V3	SYSTEM	N/A	Microsoft-Windows-Hyper-V-VMMS
Event Type: Information					
Log Type: Application					
Category Id: 0					
Description: Switch set up, name="DFC3A82F-C7CF-4F49-B470-9F64004DD1B2", external port="9F64004DD1B2", internal port="69F3266F9EB0", NIC="C7CF-4F49-B470", internal name="D03C-4B49-8171", internal friendly name="Virtual machine test".					
6/27/2016 12:15:49 PM	26000	PNPL-4-KP / Hyper-V3	SYSTEM	N/A	Microsoft-Windows-Hyper-V-VMMS

Figure 24

SAMPLE REPORT

LogTime	Computer	Machine Name	Status
06/21/2016 12:53:57 PM	HYPER-V3	test	created
06/21/2016 12:53:58 PM	HYPER-V3	test	deleted
06/21/2016 12:53:58 PM	HYPER-V3	Virtual machine test	set up
06/21/2016 12:53:58 PM	HYPER-V3	Virtual machine test	set up

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.



Figure 26

Category

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

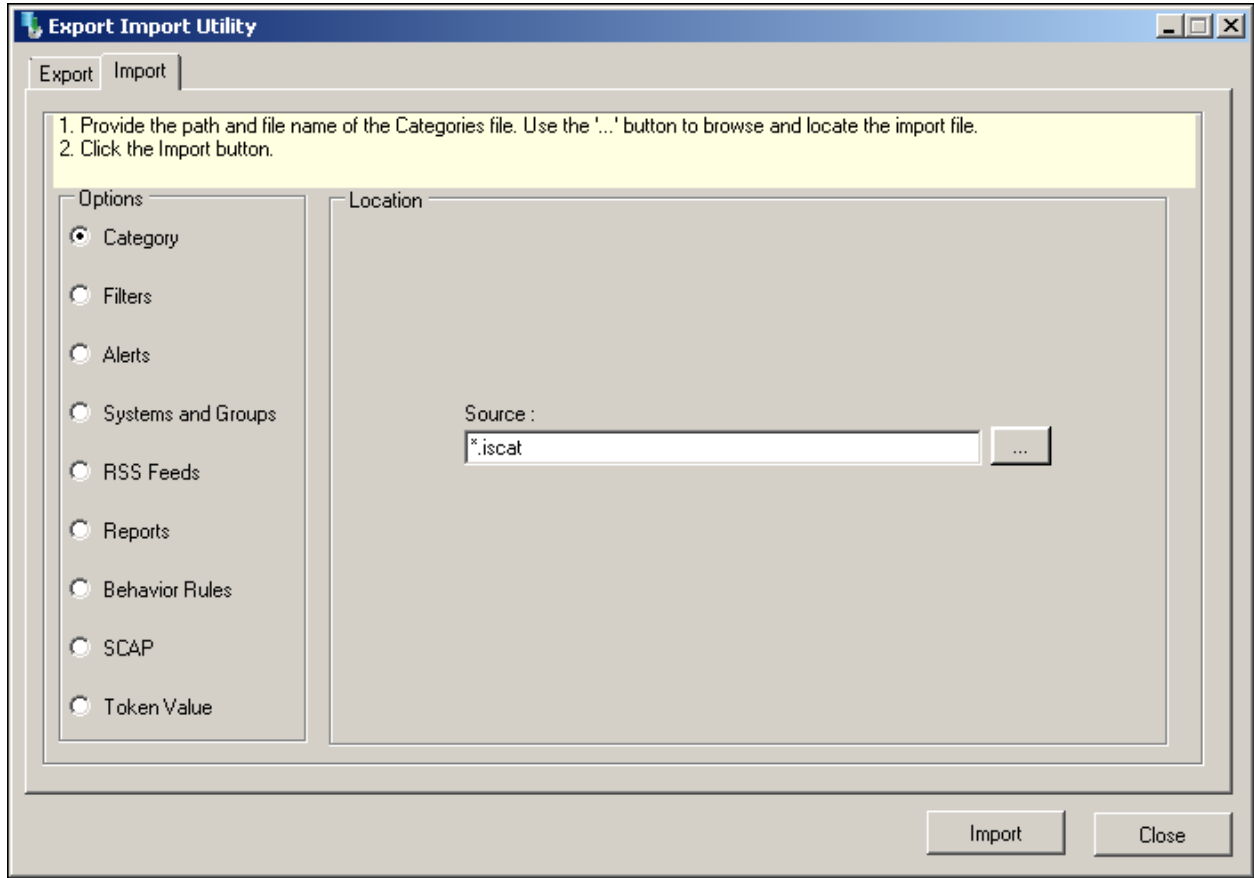


Figure 27

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.

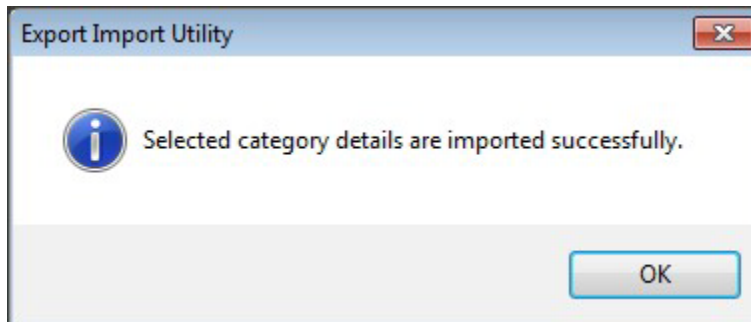



Figure 28

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

Alerts

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

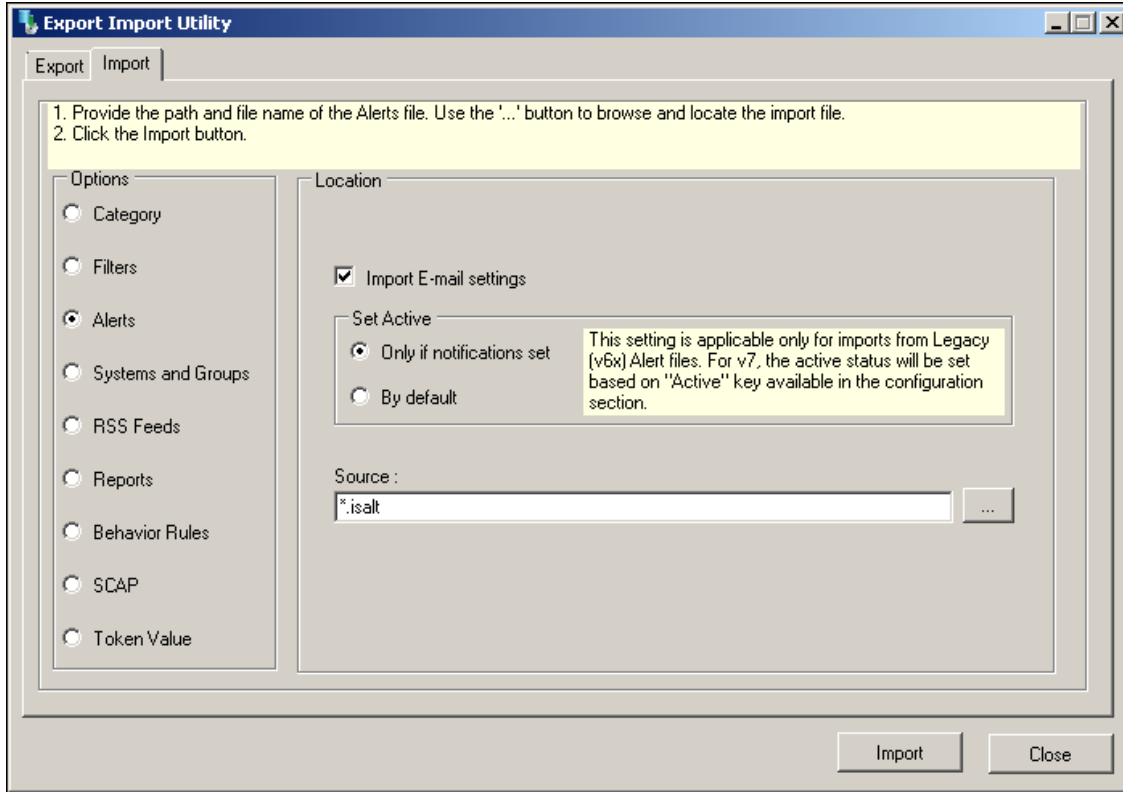


Figure 29

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.

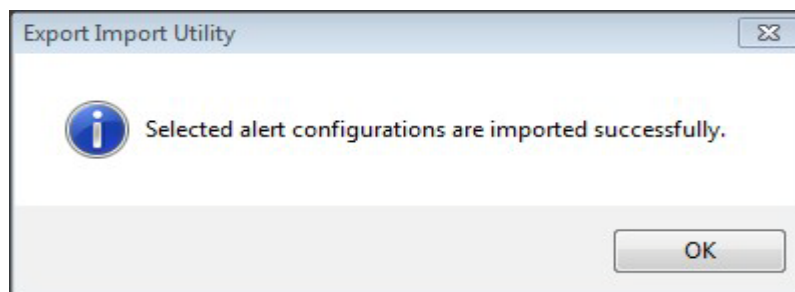



Figure 30

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

Parsing rules

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

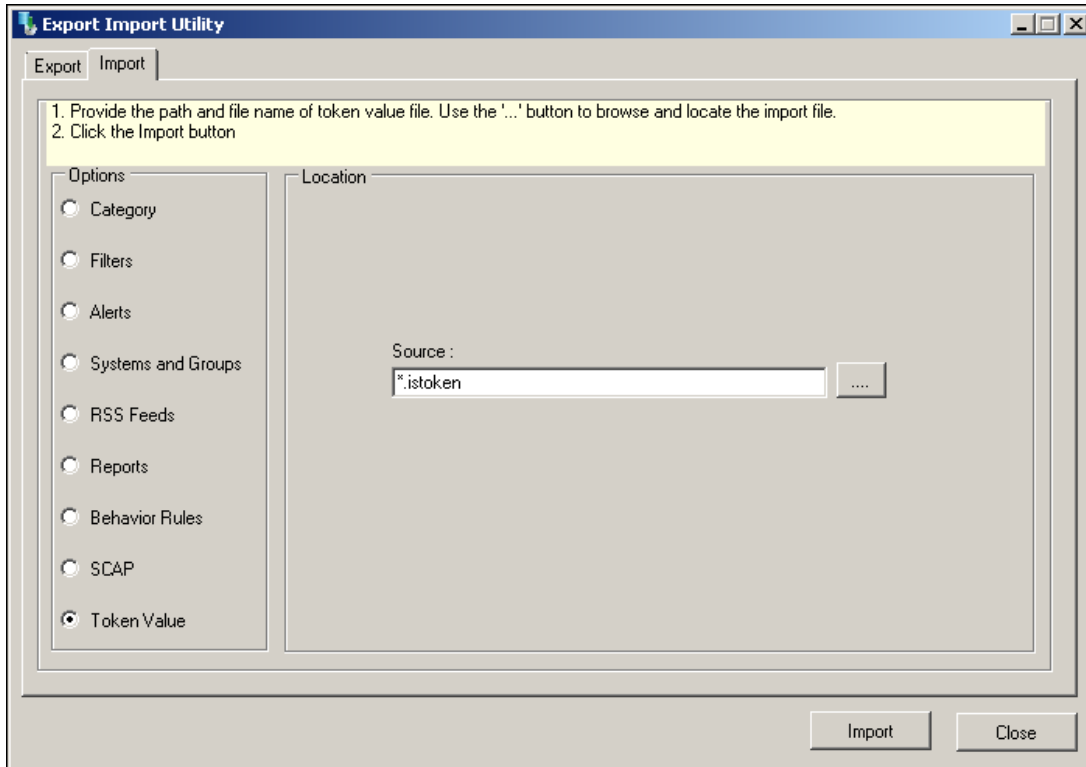


Figure 31

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.

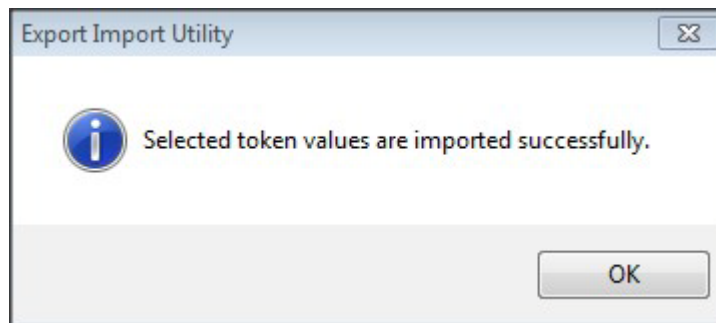



Figure 32

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

Flex Reports

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

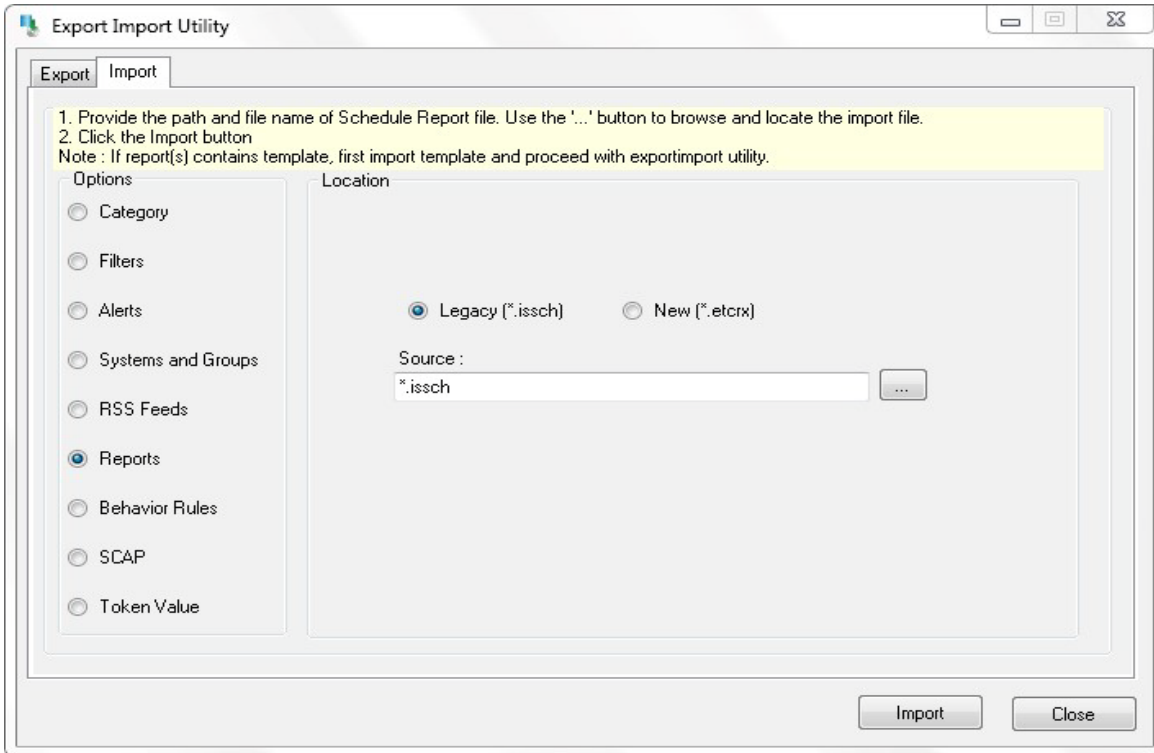


Figure 33

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.

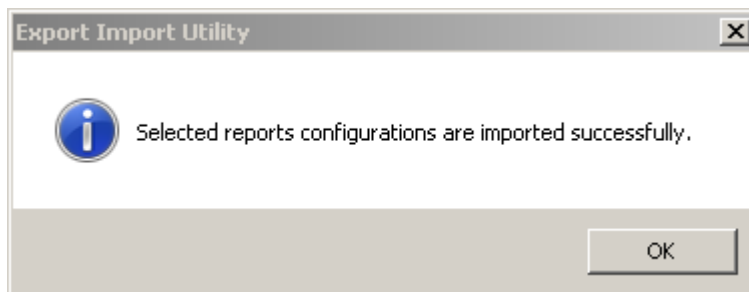



Figure 34

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

Templates

1. Click the **Admin** menu, and then click **Parsing rule**.
2. Select **Template** tab, and then click on  'Import' option.

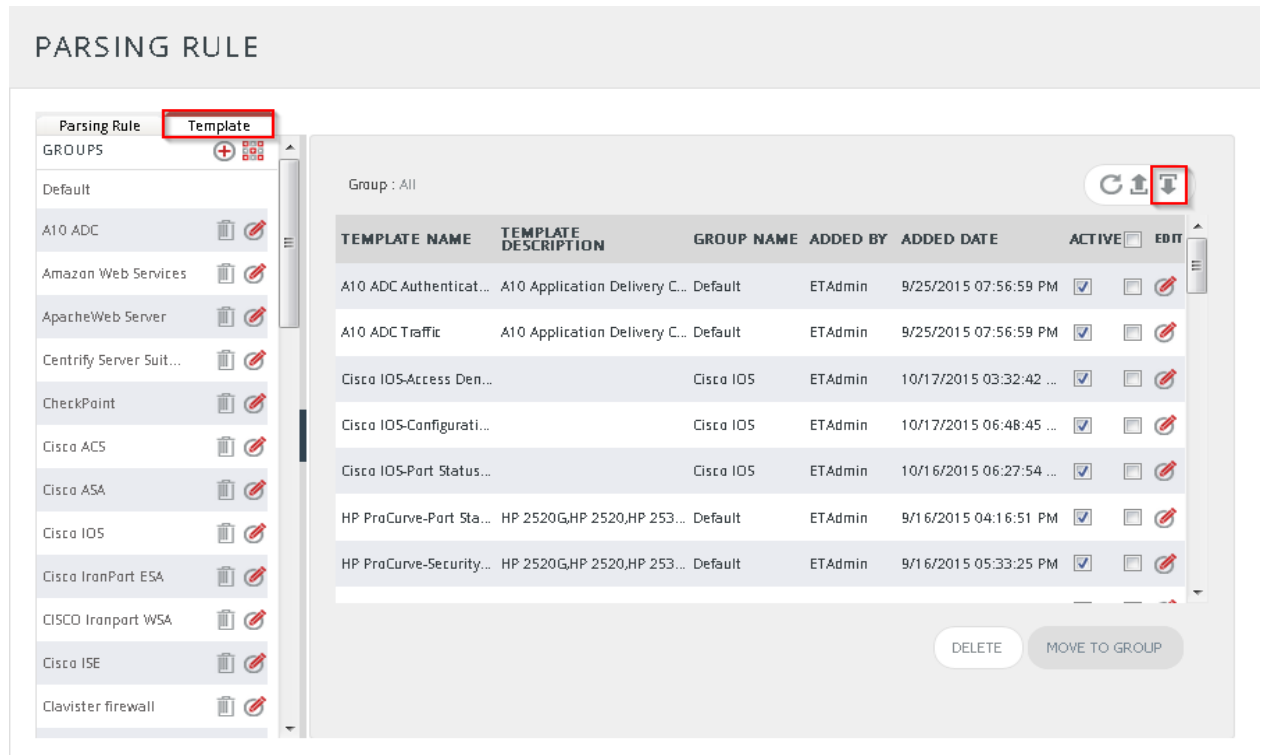


Figure 35

3. Click on **Browse** button.

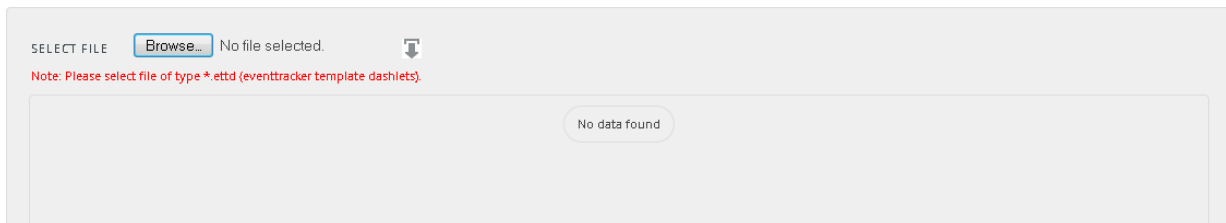



Figure 36

4. Locate **All Hyper V Template.ettd** file, and then click the **Open** button

SELECTED FILE IS: All Microsoft Windows Hyper-V Token Template.ettd

<input type="checkbox"/> TEMPLATE NAME	SEPARATOR	TEMPLATE DESCRIPTION	ADDED DATE	ADDED BY	GROUP NAME
<input type="checkbox"/> Microsoft Windows Hyper V-Partition created and deleted	\n	Hyper-V successfully deleted a partition (partition 109).	6/10/2016 4:12:28 PM	ETAdmin	Microsoft Windows Hyper V
<input type="checkbox"/> Microsoft Windows Hyper V: Resource management	\n	The system successfully created "C:\Users\Public\Documents\Hyper-V\Virtual Hard Disks\New Virtual Machine.vhdx".	6/10/2016 6:34:15 PM	ETAdmin	Microsoft Windows Hyper V
<input type="checkbox"/> Microsoft Windows Hyper V: SAN management	\n	A new virtual SAN with name Computing was created	6/14/2016 6:48:11 PM	ETAdmin	Microsoft Windows Hyper V
<input type="checkbox"/> Microsoft Windows Hyper V: Virtual machine management	\n	A new virtual machine "windows" was created. (Virtual machine ID 1006F171-102E-470E-8488-64FA737929E5)	6/13/2016 3:38:08 PM	ETAdmin	Microsoft Windows Hyper V
<input type="checkbox"/> Microsoft Windows Hyper V: Virtual machine operational message	\n	'Vmesx3-VM2- Testing' was reset by the guest operating system. (Virtual machine ID D4405665-9BFD-49B3-9511-ED4F07E6E84C)	6/10/2016 3:46:47 PM	ETAdmin	Microsoft Windows Hyper V

Figure 37

5. Now select the check box and then click on  'Import' option. EventTracker displays success message.

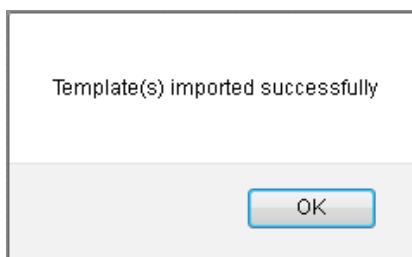


Figure 38

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 MANAGEMENT

Total category groups: 356 Total categories: 3,161
Last 10 modified categories

NAME	MODIFIED DATE	MODIFIED BY
Microsoft Windows Hyper V-Import and export	6/16/2016 11:52:55 AM	ETAdmin
Microsoft Windows Hyper V-SAN management	6/14/2016 6:51:36 PM	ETAdmin
Microsoft Windows Hyper V-Configuration store	6/14/2016 4:31:02 PM	ETAdmin
Microsoft Windows Hyper V-Switch created	6/14/2016 2:58:46 PM	ETAdmin
Microsoft Windows Hyper V-Integration service	6/14/2016 12:48:33 PM	ETAdmin
Microsoft Windows Hyper V-Virtual machine deleted	6/13/2016 5:15:02 PM	ETAdmin
Microsoft Windows Hyper V-Virtual machine created	6/13/2016 4:21:56 PM	ETAdmin
Microsoft Windows Hyper V: System created	6/10/2016 6:36:50 PM	ETAdmin
Microsoft Windows Hyper V: System create failed	6/10/2016 5:46:02 PM	ETAdmin
Microsoft Windows Hyper V: Virtual machine operational message	6/10/2016 12:49:43 PM	ETAdmin

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.

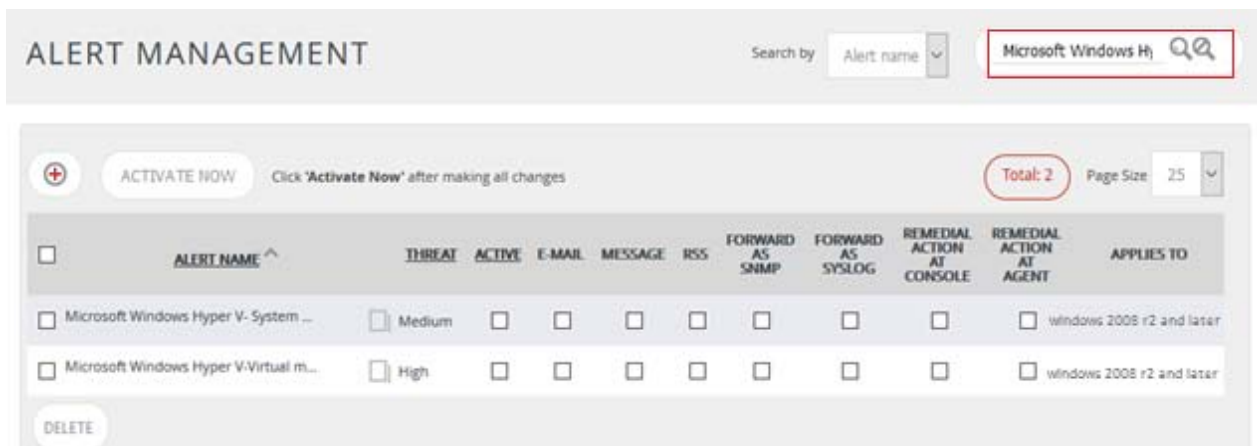


Figure 40

- To activate the imported alerts, select the respective checkbox in the **Active** column. EventTracker displays message box.

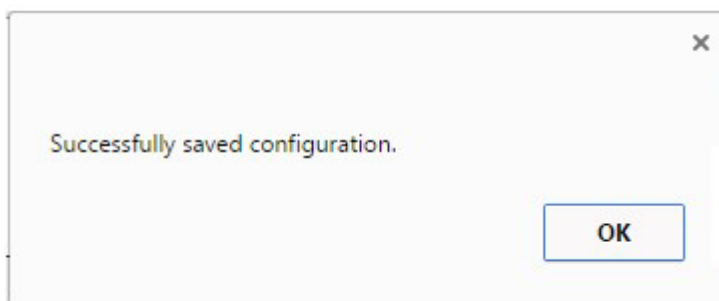


Figure 41

- 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

- Logon to **EventTracker Enterprise** web interface.
- Click the **Admin** menu, and then click **Parsing Rules**.

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

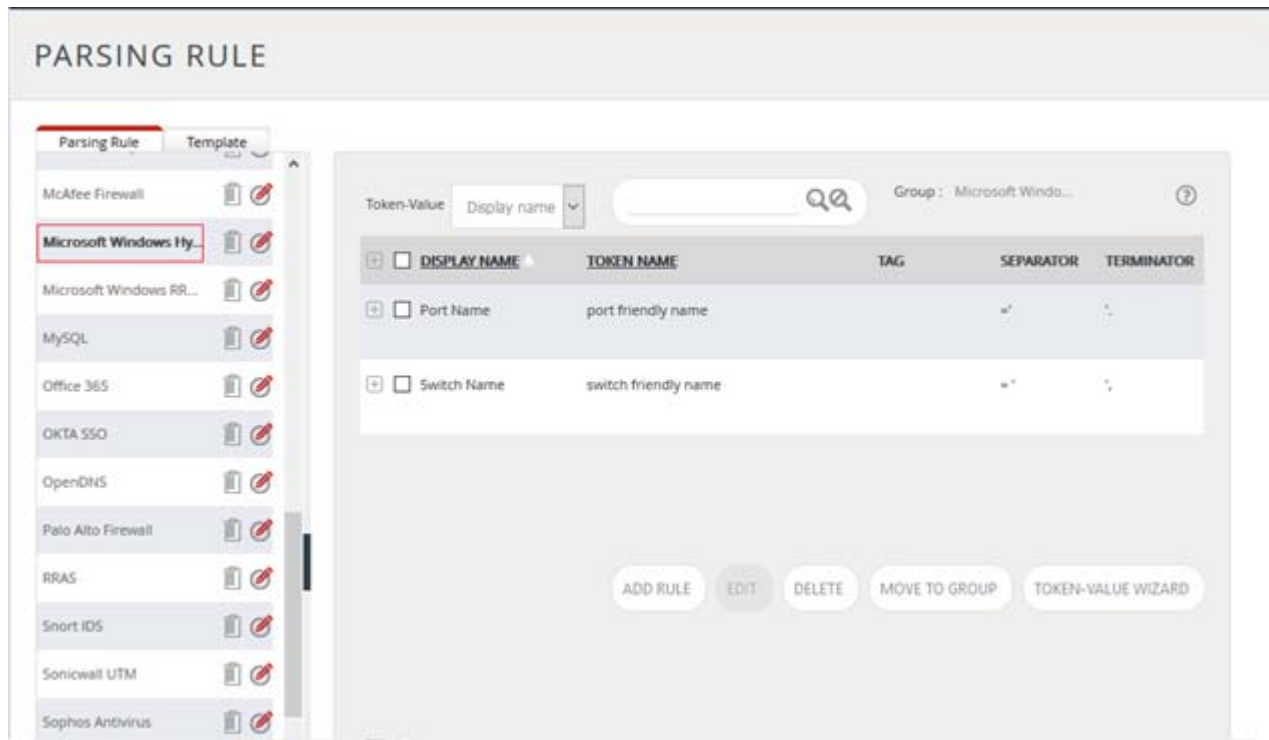


Figure 42

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**.

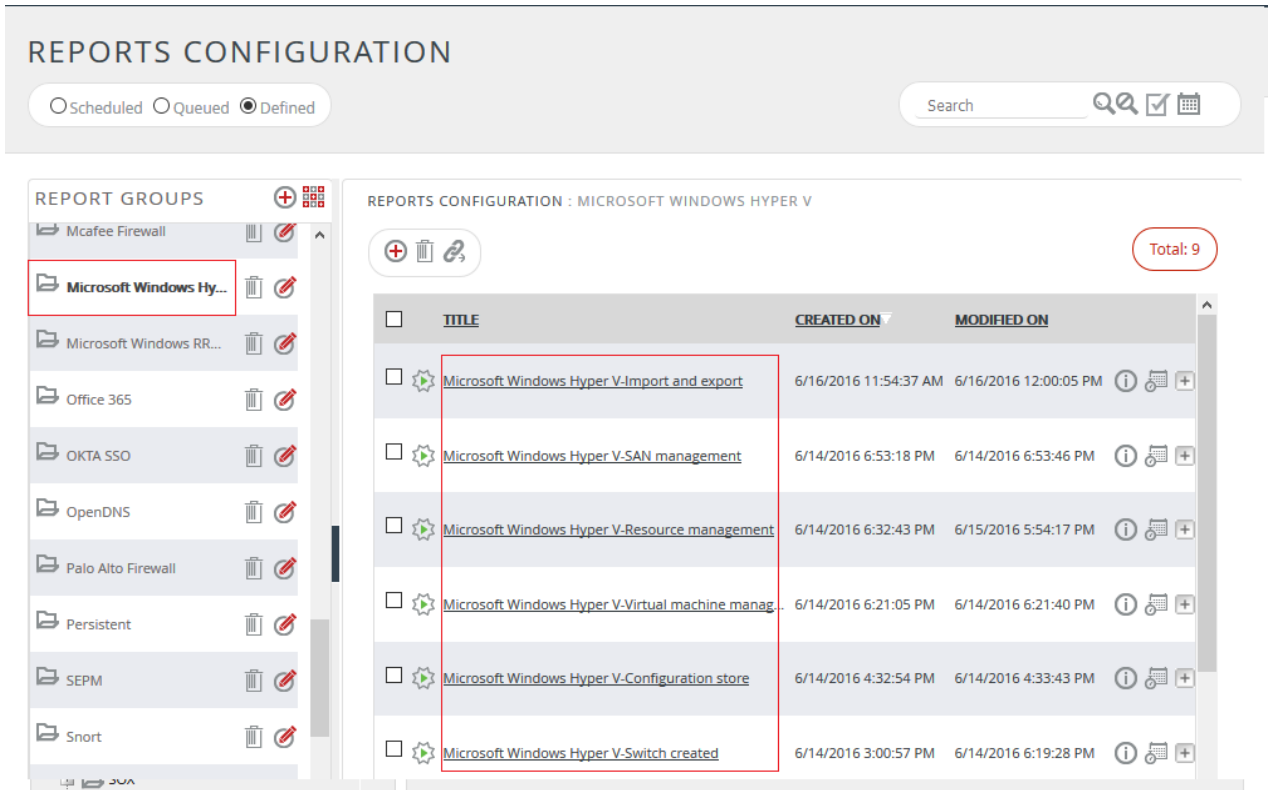


Figure 43

Template

1. Logon to **EventTracker Enterprise** web interface.
2. Click the **Admin** menu, and then click **Parsing Rules** and click **Template**.

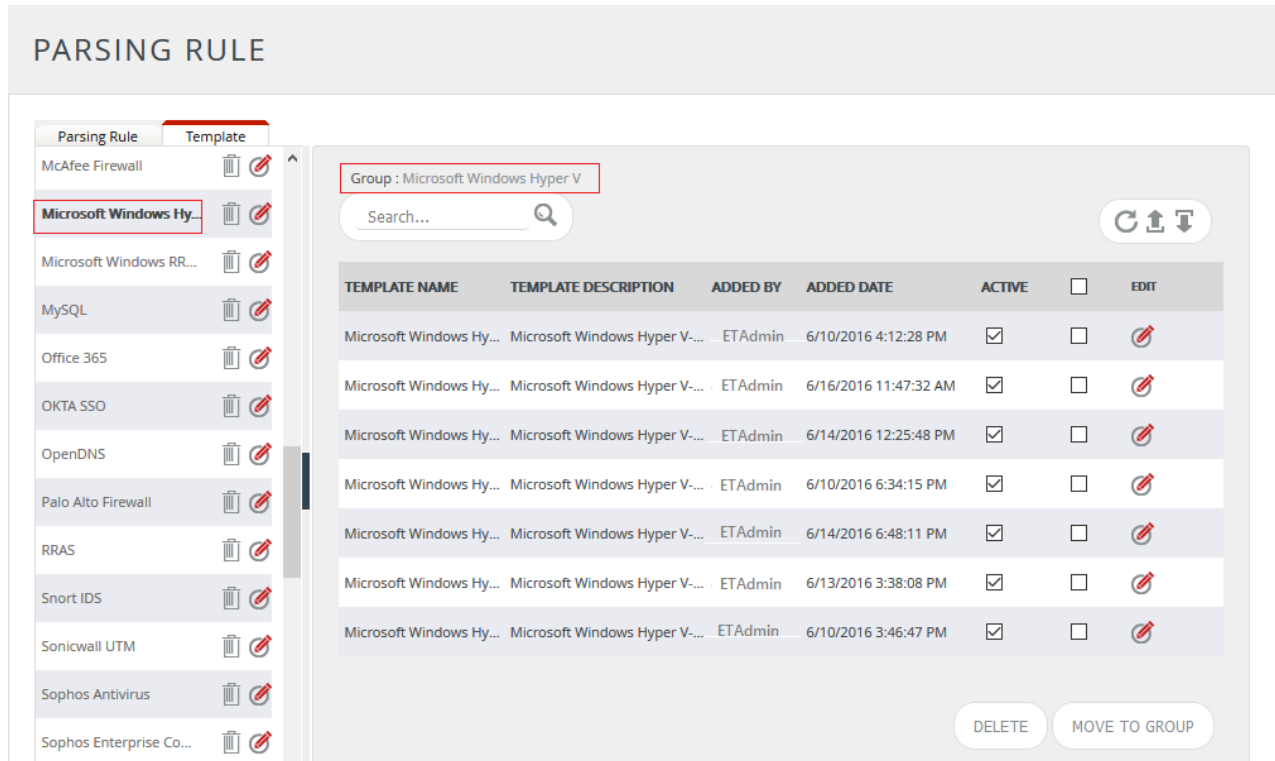


Figure 44

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.

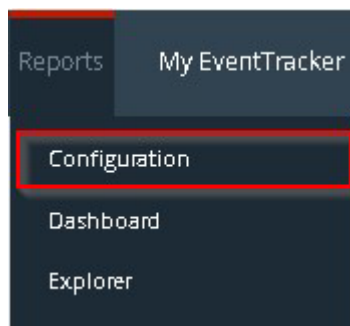


Figure 45

2. Navigate to **Reports>Configuration**.

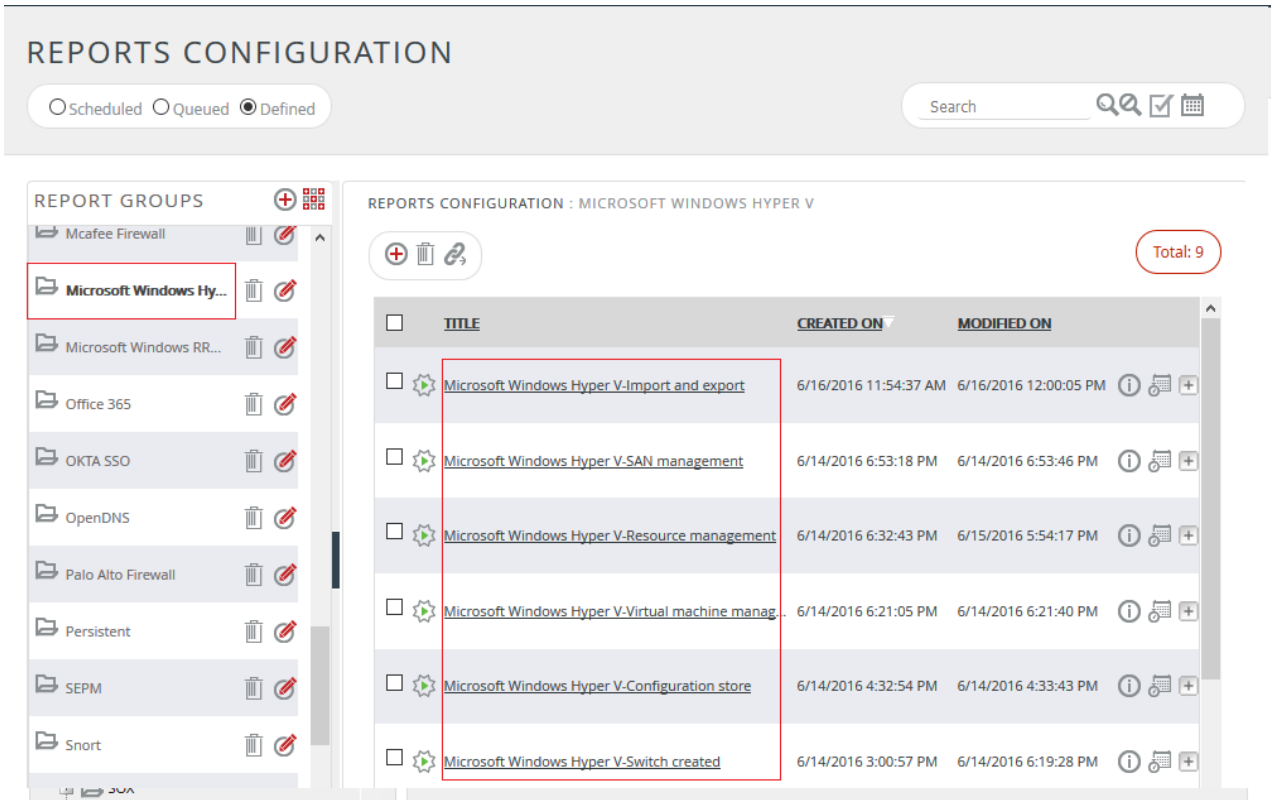



Figure 46

3. Select **Hyper V** in report groups. Check **Defined** dialog box.
4. Click on 'schedule'  to plan a report for later execution.

REPORT WIZARD

TITLE: MICROSOFT WINDOWS HYPER V-VIRTUAL MACHINE MANAGEMENT

LOGS

CANCEL < BACK NEXT >

Review cost details and configure the publishing options. Step 8 of 10

DISK COST ANALYSIS

Estimated time for completion: 00:00:50(HH:MM:SS)
Number of cab(s) to be processed: 10
Available disk space: 245 GB
Required disk space: 50 MB

Enable publishing option (Configure SMTP Server in manager configuration screen to use this option)
 Deliver results via E-mail
 Notify results via E-mail

To E-mail: [Use comma(,) to separate multiple e-mail recipients]

Update status via RSS:

Show in:

Persist data in Eventvault Explorer

Figure 47

REPORT WIZARD

TITLE: Microsoft Windows Hyper-V
DATA PERSIST DETAIL

CANCEL < BACK NEXT >

Select columns to persist Step 9 of 10

RETENTION SETTING

Retention period: days ⓘ

Persist in database only *[Reports will not be published and will only be stored in the respective database]*

SELECT COLUMNS TO PERSIST

COLUMN NAME	PERSIST
Event Time	<input checked="" type="checkbox"/>
Computer	<input checked="" type="checkbox"/>
Admin Name	<input checked="" type="checkbox"/>
Source IP Address	<input checked="" type="checkbox"/>
Destination IP Address	<input checked="" type="checkbox"/>
Session Status	<input checked="" type="checkbox"/>

Figure 48

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.

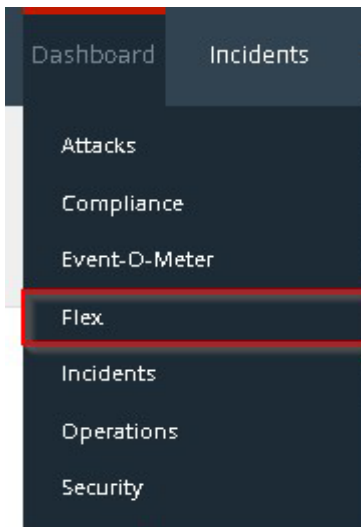


Figure 49

3. Navigate to **Dashboard>Flex**.
Flex Dashboard pane is shown.

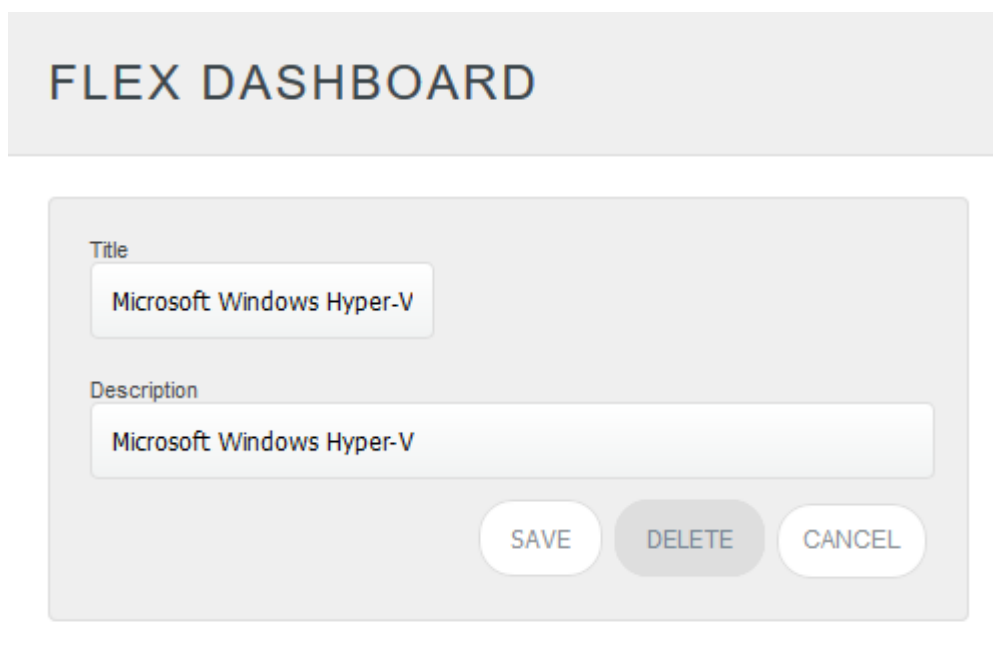



Figure 50

4. Fill suitable title and description and click **Save** button.
5. Click  to configure a new flex dashlet. Widget configuration pane is shown.

WIDGET CONFIGURATION

WIDGET TITLE: Windows Hyper-V-Virtual machine operational message

NOTE: [Empty text box]

DATA SOURCE: Microsoft Windows Hyper V-Virtual machine operational messag

CHART TYPE: Donut

DURATION: 12 Hours

VALUE FIELD SETTING: COUNT

AS OF: Recent

AXIS LABELS [X-AXIS]: Operation Message

LABEL TEXT: [Empty text box]

VALUES [Y-AXIS]: Select column

VALUE TEXT: [Empty text box]

FILTER: Select column

FILTER VALUES: [Empty dropdown]

LEGEND [SERIES]: Select column

SELECT: All

[TEST] [CONFIGURE] [CLOSE]

Figure 51

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.

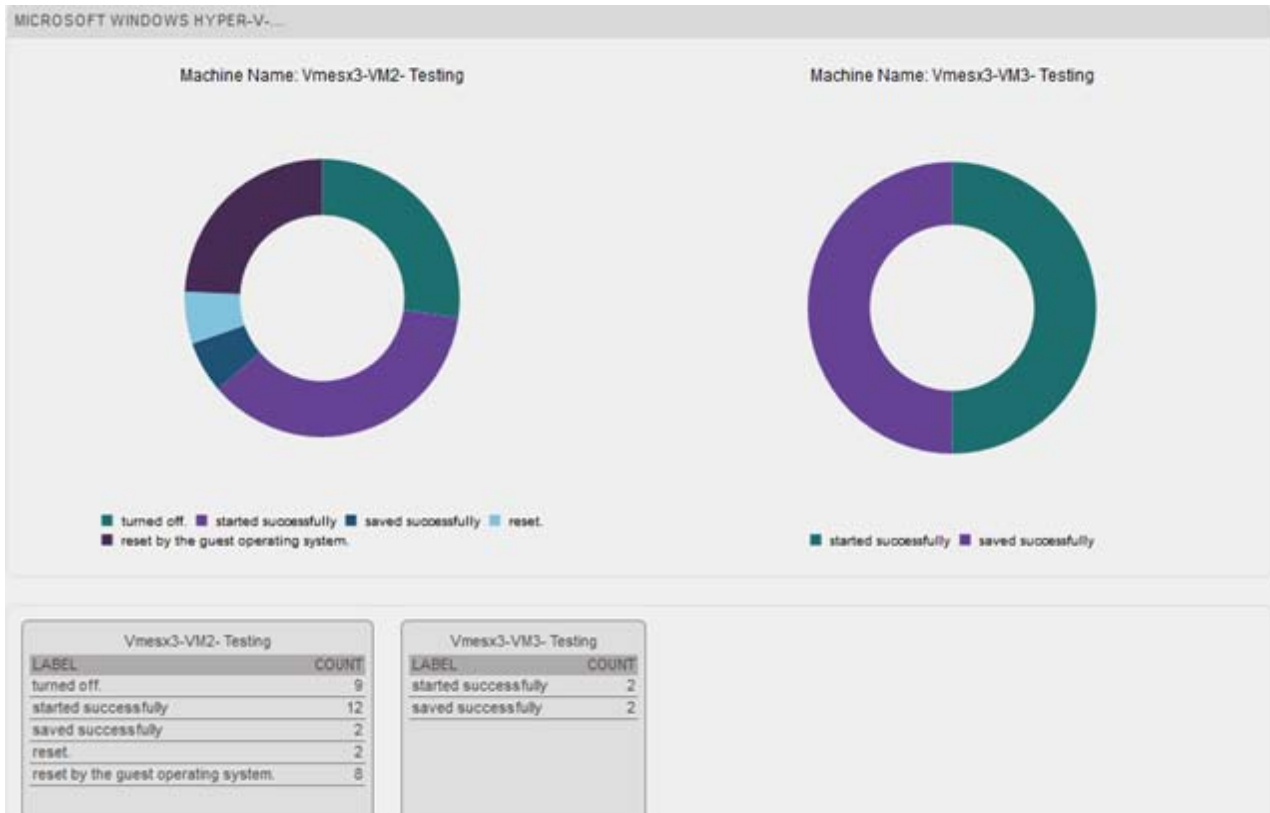


Figure 52

2. If satisfied, click **Configure** button

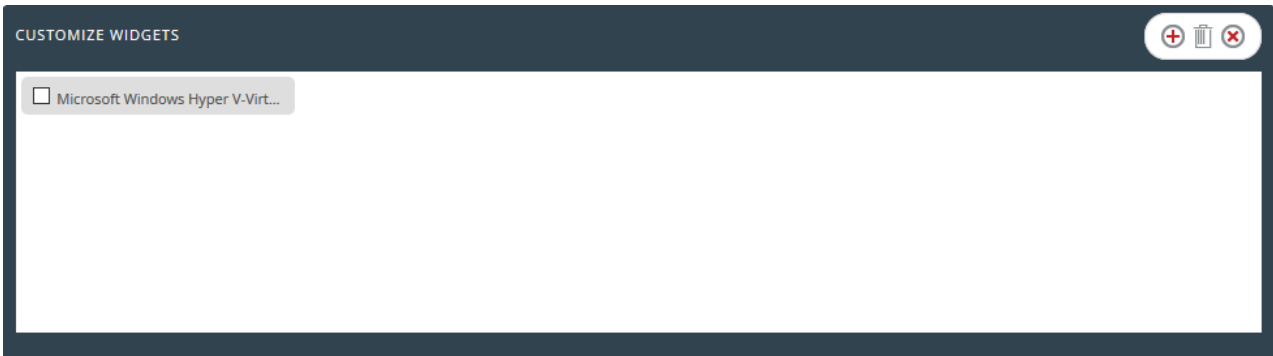




Figure 53

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.

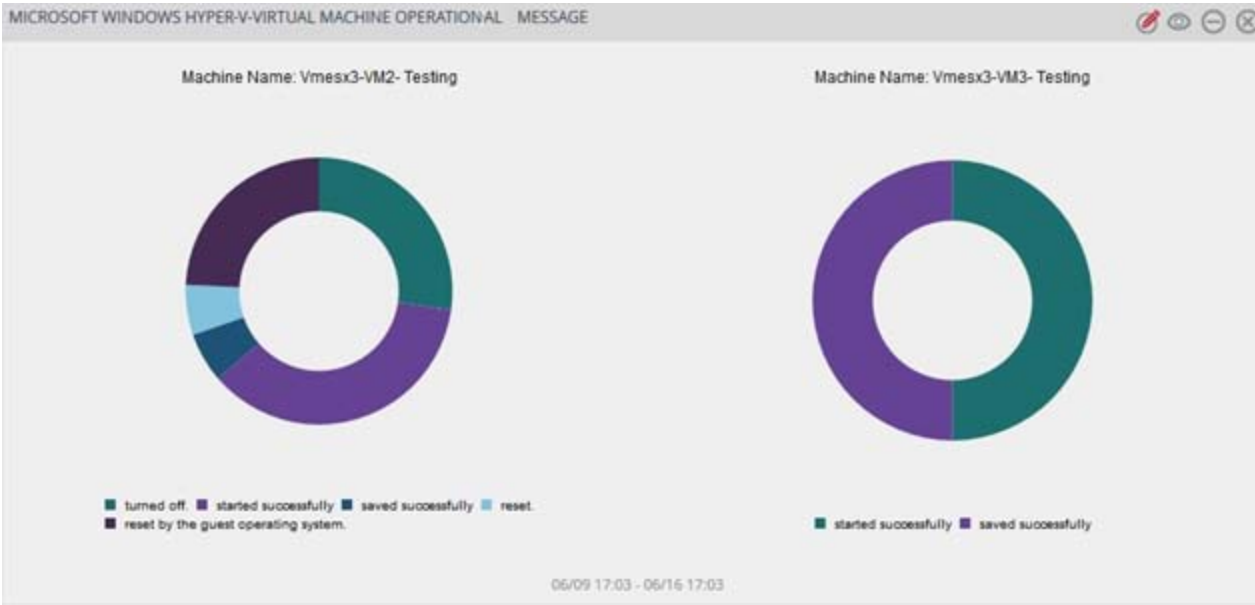


Figure 54