EventTracker

Actionable Security Intelligence

Integrate VMware ESX/ESXi and vCenter Server

EventTracker v8.x and above

Publication Date: September 24, 2018

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.

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

This document is for informational purposes only. EventTracker 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 EventTracker, if its content is unaltered, nothing is added to the content and credit to EventTracker is provided.

EventTracker 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 EventTracker, 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.

© 2018 EventTracker Security LLC. All rights reserved. The names of actual companies and products mentioned herein may be the trademarks of their respective owners.

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

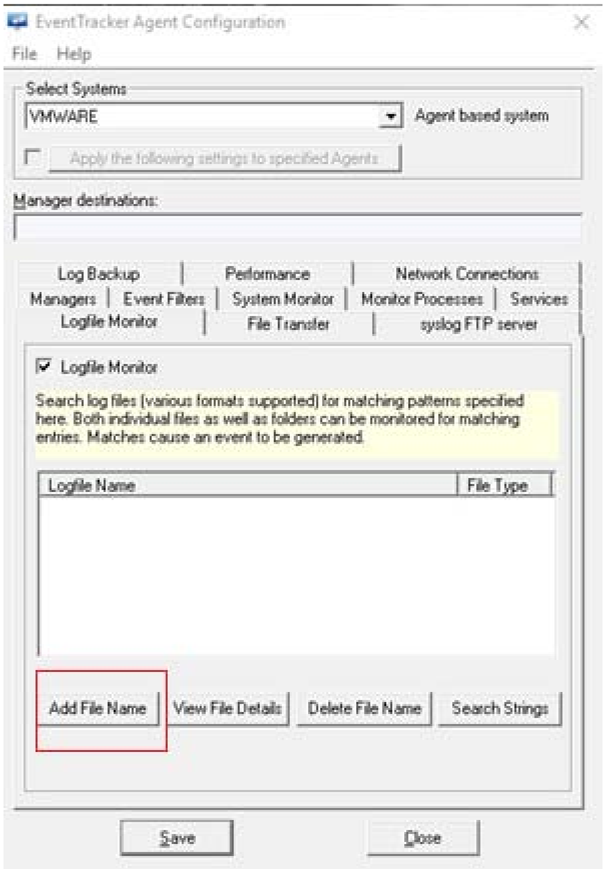
Configure VMware to forward logs to EventTracker

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.



Select Systems: VMWARE — Agent based system

□ Apply the following settings to specified Agents

Manager destinations:

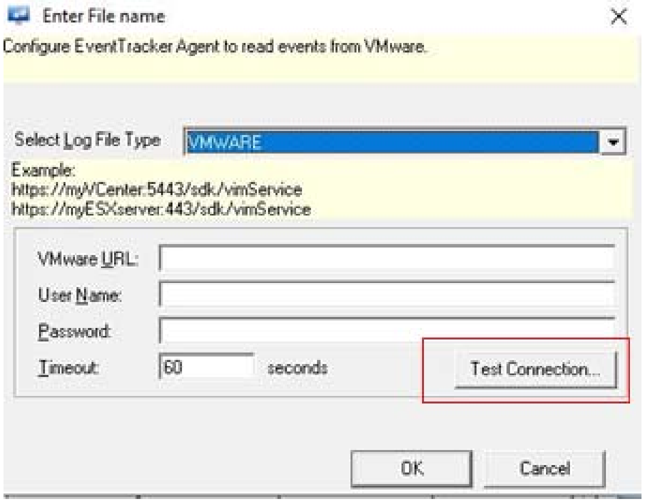
☑ Logfile Monitor

Search log files (various formats supported) for matching patterns specified here. Both individual files as well as folders can be monitored for matching entries. Matches cause an event to be generated.

Logfile Name	File Type

Figure 1

- 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.



Configure EventTracker Agent to read events from VMware.

Select Log File Type: VMWARE

Example:
https://myVCenter:5443/sdk/vimService
https://myESXserver:443/sdk/vimService

VMware URL:

User Name:

Password:

Timeout: 60 seconds

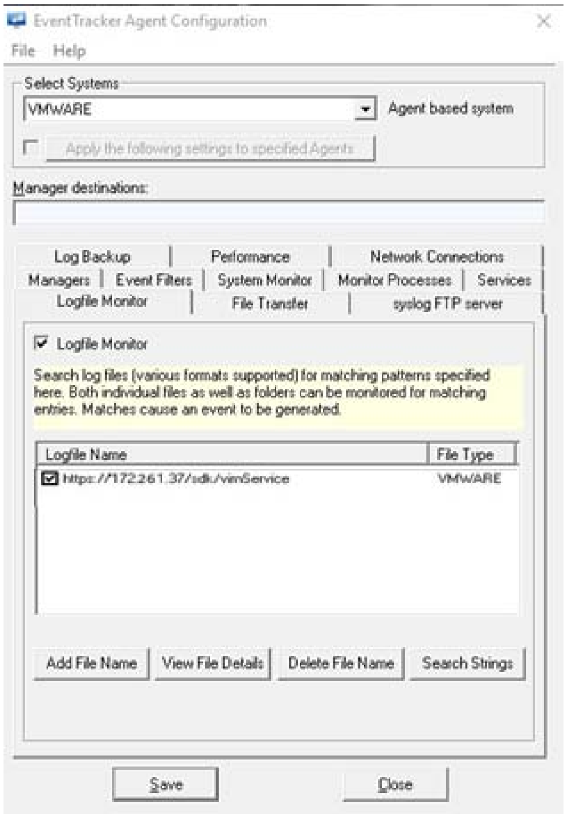
Figure 2

- Enter following details:

Field	Description
VMware URL	Type the FQDN/IP address of the Vcenter/ESXserver according to your infrastructure. e.g. https://<esxvcservername>/sdk/vimService.
User Name	Type Vcenter/ESXserver **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.



Select Systems: VMWARE — Agent based system

□ Apply the following settings to specified Agents

Manager destinations:

☑ Logfile Monitor

Search log files (various formats supported) for matching patterns specified here. Both individual files as well as folders can be monitored for matching entries. Matches cause an event to be generated.

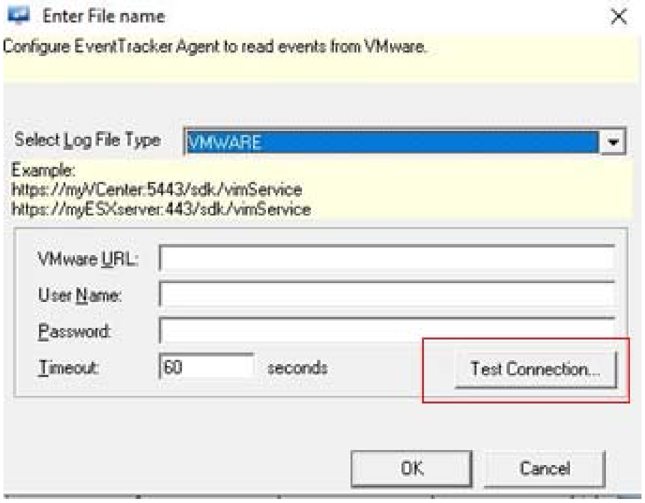
Logfile Name	File Type
☑ https://172.26.1.37/sdk/vimService	VMWARE

Figure 3

- Click **Save**.

Troubleshooting Techniques

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



Enter File name

Configure EventTracker Agent to read events from VMware.

Select Log File Type: VMWARE

Example:
https://myVCenter:5443/sdk/vimService
https://myESXserver:443/sdk/vimService

VMware URL:

User Name:

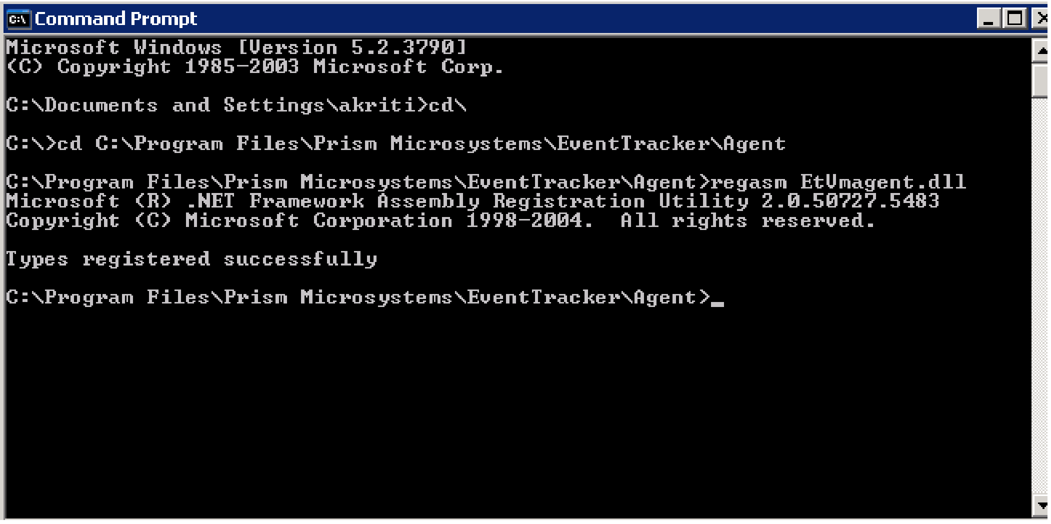
Password:

Timeout: 60 seconds

Figure 4

- Check if the entered URL is correct.
  Access **https://**<**Vcenter/ESXiservername**>:<**Port**>**sdk/vim.wsdl** 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**"



```
Microsoft Windows [Version 5.2.3790]
(C) Copyright 1985-2003 Microsoft Corp.

C:\Documents and Settings\akriti>cd\

C:\>cd C:\Program Files\Prism Microsystems\EventTracker\Agent

C:\Program Files\Prism Microsystems\EventTracker\Agent>regasm EtVmagent.dll
Microsoft (R) .NET Framework Assembly Registration Utility 2.0.50727.5483
Copyright (C) Microsoft Corporation 1998-2004.  All rights reserved.

Types registered successfully

C:\Program Files\Prism Microsystems\EventTracker\Agent>_
```

Figure 5

- 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-Datastore 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.

- **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 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.

- **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.

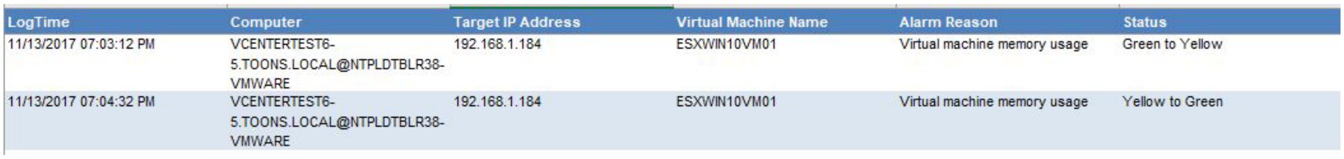
Knowledge Objects

- **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

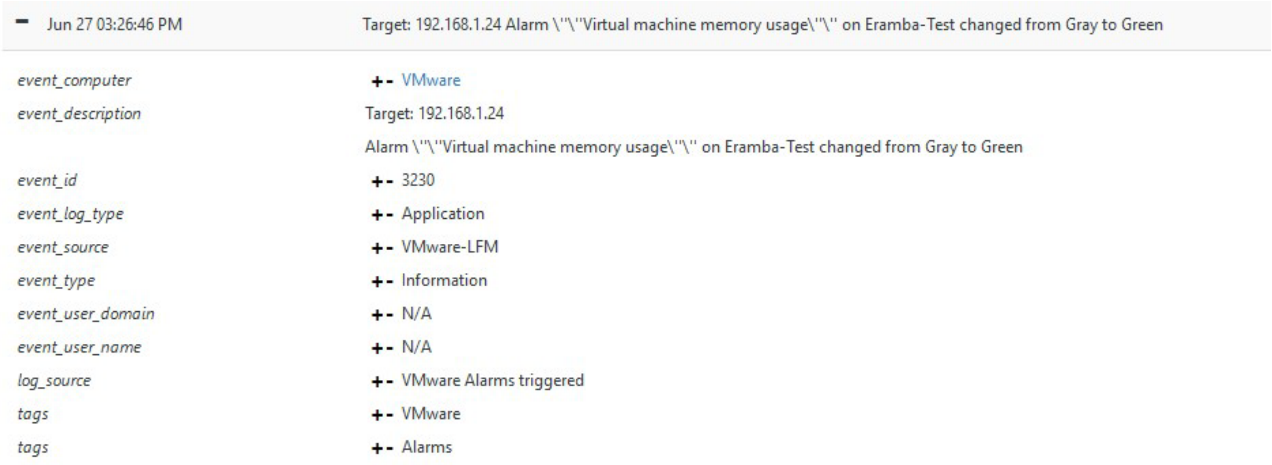
- **VMware- Alarms triggered:** This report provides information about the activities related to alarms triggered.



LogTime	Computer	Target IP Address	Virtual Machine Name	Alarm Reason	Status
11/13/2017 07:03:12 PM	VCENTERTEST6-5.TOONS.LOCAL@NTPLDTBLR38-VMWARE	192.168.1.184	ESXWIN10VM01	Virtual machine memory usage	Green to Yellow
11/13/2017 07:04:32 PM	VCENTERTEST6-5.TOONS.LOCAL@NTPLDTBLR38-VMWARE	192.168.1.184	ESXWIN10VM01	Virtual machine memory usage	Yellow to Green

Figure 6

Logs Considered:

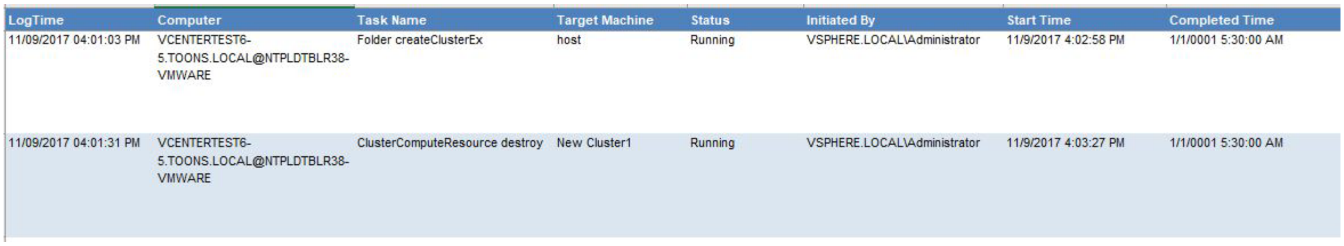


− Jun 27 03:26:46 PM Target: 192.168.1.24 Alarm \"\"Virtual machine memory usage\"\" on Eramba-Test changed from Gray to Green

event_computer	+- VMware
event_description	Target: 192.168.1.24 Alarm \"\"Virtual machine memory usage\"\" on Eramba-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

Figure 7

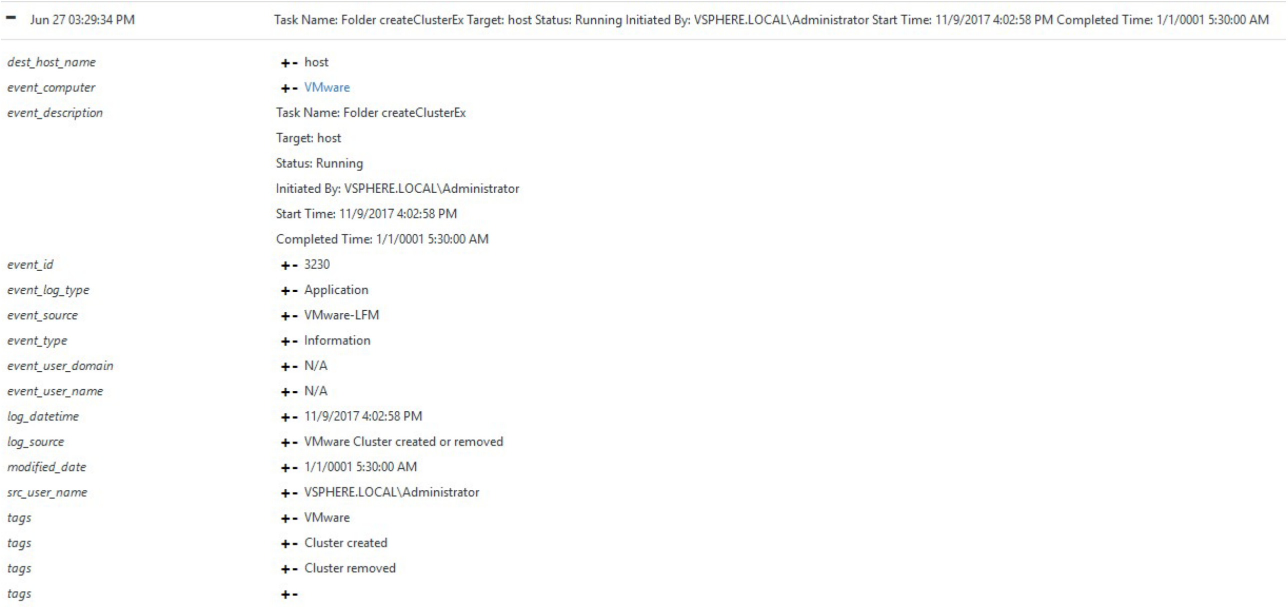
- **VMware- Cluster created or removed:** This report provides information about the activities related to cluster created or removed.



LogTime	Computer	Task Name	Target Machine	Status	Initiated By	Start Time	Completed Time
11/09/2017 04:01:03 PM	VCENTERTEST6-5.TOONS.LOCAL@NTPLDTBLR38-VMWARE	Folder createClusterEx	host	Running	VSPHERE.LOCAL\Administrator	11/9/2017 4:02:58 PM	1/1/0001 5:30:00 AM
11/09/2017 04:01:31 PM	VCENTERTEST6-5.TOONS.LOCAL@NTPLDTBLR38-VMWARE	ClusterComputeResource destroy	New Cluster1	Running	VSPHERE.LOCAL\Administrator	11/9/2017 4:03:27 PM	1/1/0001 5:30:00 AM

Figure 8

Logs Considered:

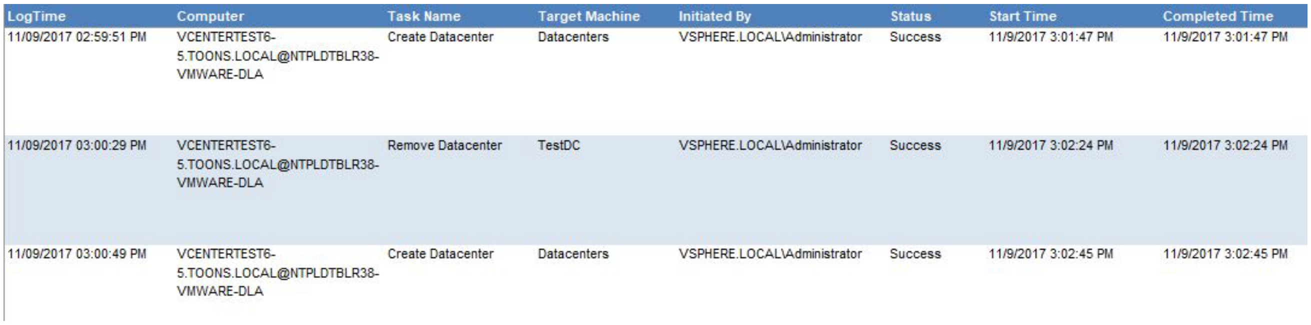


− Jun 27 03:29:34 PM   Task Name: Folder createClusterEx Target: host Status: Running Initiated By: VSPHERE.LOCAL\Administrator Start Time: 11/9/2017 4:02:58 PM Completed Time: 1/1/0001 5:30:00 AM

dest_host_name	+- host
event_computer	+- VMware
event_description	Task Name: Folder createClusterEx Target: host Status: Running Initiated By: VSPHERE.LOCAL\Administrator Start Time: 11/9/2017 4:02:58 PM Completed Time: 1/1/0001 5:30:00 AM
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_datetime	+- 11/9/2017 4:02:58 PM
log_source	+- VMware Cluster created or removed
modified_date	+- 1/1/0001 5:30:00 AM
src_user_name	+- VSPHERE.LOCAL\Administrator
tags	+- VMware
tags	+- Cluster created
tags	+- Cluster removed
tags	+-

Figure 9

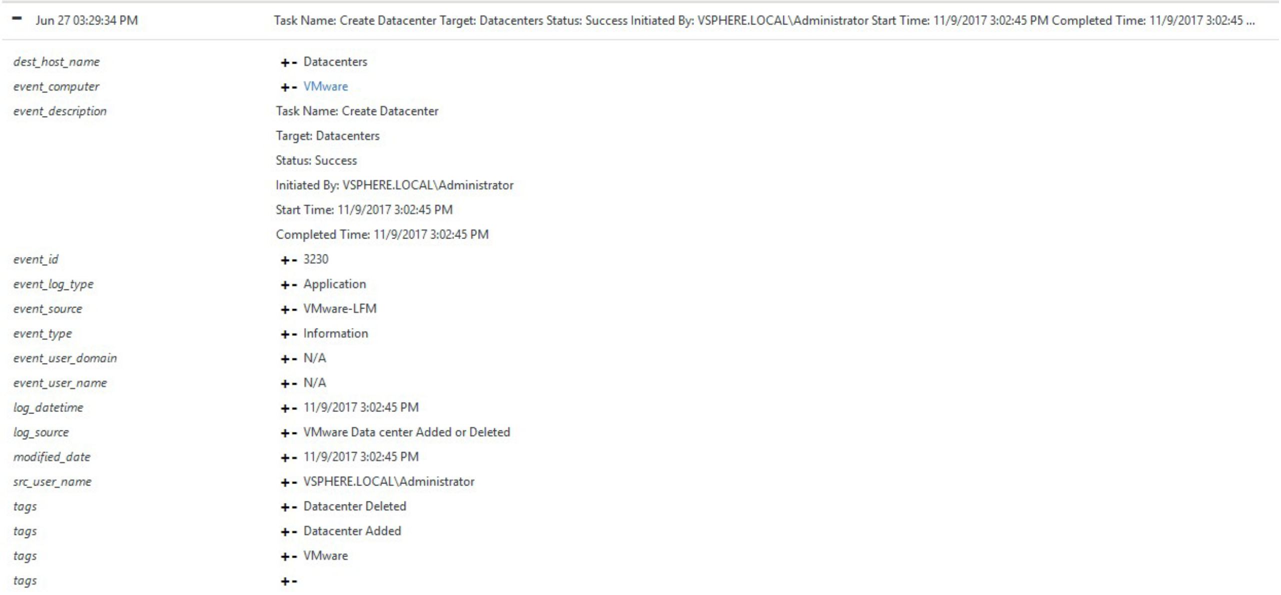
- **VMware- Data center added or deleted:** This report provides information about the activities related to data center added or deleted.



LogTime	Computer	Task Name	Target Machine	Initiated By	Status	Start Time	Completed Time
11/09/2017 02:59:51 PM	VCENTERTEST6-5.TOONS.LOCAL@NTPLDTBLR38-VMWARE-DLA	Create Datacenter	Datacenters	VSPHERE.LOCAL\Administrator	Success	11/9/2017 3:01:47 PM	11/9/2017 3:01:47 PM
11/09/2017 03:00:29 PM	VCENTERTEST6-5.TOONS.LOCAL@NTPLDTBLR38-VMWARE-DLA	Remove Datacenter	TestDC	VSPHERE.LOCAL\Administrator	Success	11/9/2017 3:02:24 PM	11/9/2017 3:02:24 PM
11/09/2017 03:00:49 PM	VCENTERTEST6-5.TOONS.LOCAL@NTPLDTBLR38-VMWARE-DLA	Create Datacenter	Datacenters	VSPHERE.LOCAL\Administrator	Success	11/9/2017 3:02:45 PM	11/9/2017 3:02:45 PM

Figure 10

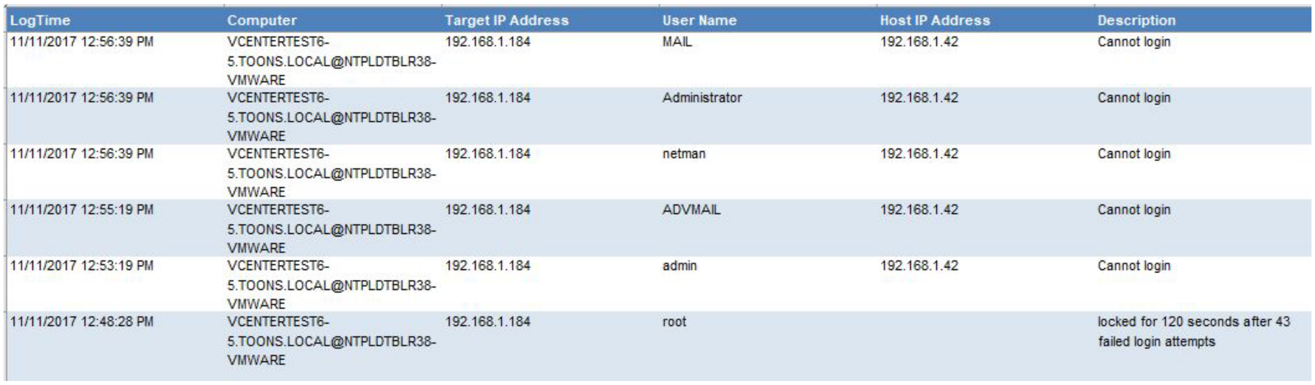
Logs Considered:



− Jun 27 03:29:34 PM	Task Name: Create Datacenter Target: Datacenters Status: Success Initiated By: VSPHERE.LOCAL\Administrator Start Time: 11/9/2017 3:02:45 PM Completed Time: 11/9/2017 3:02:45 ...
dest_host_name	+- Datacenters
event_computer	+- VMware
event_description	Task Name: Create Datacenter Target: Datacenters Status: Success Initiated By: VSPHERE.LOCAL\Administrator Start Time: 11/9/2017 3:02:45 PM Completed Time: 11/9/2017 3:02:45 PM
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_datetime	+- 11/9/2017 3:02:45 PM
log_source	+- VMware Data center Added or Deleted
modified_date	+- 11/9/2017 3:02:45 PM
src_user_name	+- VSPHERE.LOCAL\Administrator
tags	+- Datacenter Deleted
tags	+- Datacenter Added
tags	+- VMware
tags	+-

Figure 11

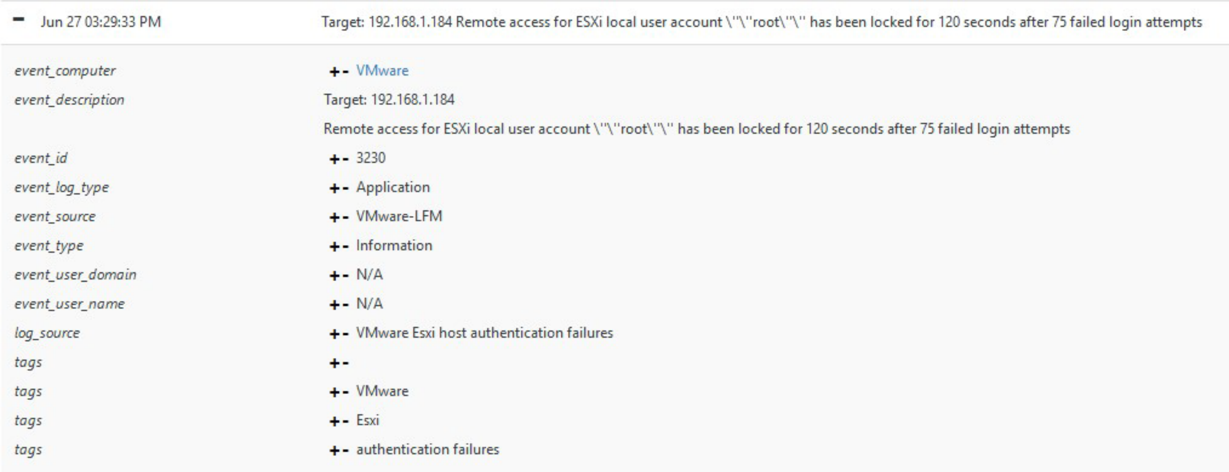
- **VMware- ESXi host authentication failures:** This report provides information about the activities related to ESXi host authentication failures.



LogTime	Computer	Target IP Address	User Name	Host IP Address	Description
11/11/2017 12:56:39 PM	VCENTERTEST6-5.TOONS.LOCAL@NTPLDTBLR38-VMWARE	192.168.1.184	MAIL	192.168.1.42	Cannot login
11/11/2017 12:56:39 PM	VCENTERTEST6-5.TOONS.LOCAL@NTPLDTBLR38-VMWARE	192.168.1.184	Administrator	192.168.1.42	Cannot login
11/11/2017 12:56:39 PM	VCENTERTEST6-5.TOONS.LOCAL@NTPLDTBLR38-VMWARE	192.168.1.184	netman	192.168.1.42	Cannot login
11/11/2017 12:55:19 PM	VCENTERTEST6-5.TOONS.LOCAL@NTPLDTBLR38-VMWARE	192.168.1.184	ADVMAIL	192.168.1.42	Cannot login
11/11/2017 12:53:19 PM	VCENTERTEST6-5.TOONS.LOCAL@NTPLDTBLR38-VMWARE	192.168.1.184	admin	192.168.1.42	Cannot login
11/11/2017 12:48:28 PM	VCENTERTEST6-5.TOONS.LOCAL@NTPLDTBLR38-VMWARE	192.168.1.184	root		locked for 120 seconds after 43 failed login attempts

Figure 12

Logs Considered:

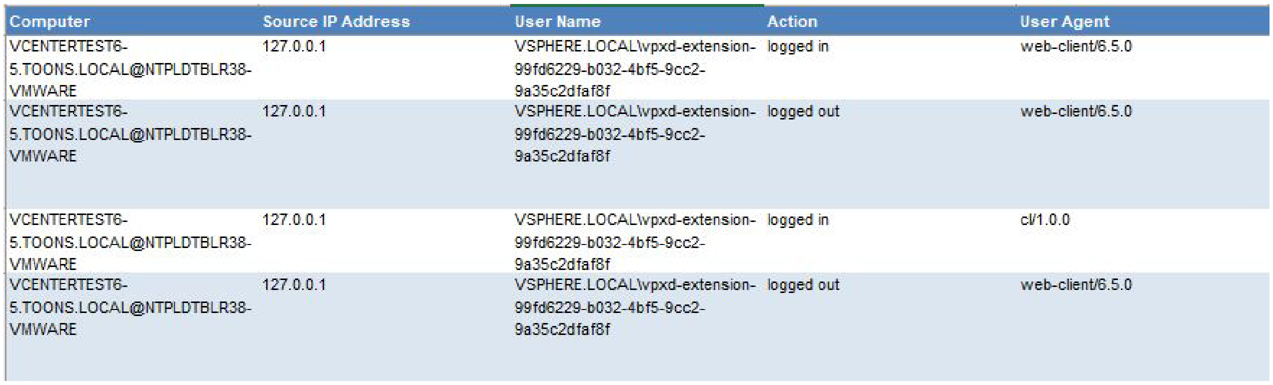


```
−  Jun 27 03:29:33 PM          Target: 192.168.1.184 Remote access for ESXi local user account \"\"root\"\" has been locked for 120 seconds after 75 failed login attempts

event_computer                 +- VMware
event_description              Target: 192.168.1.184
                               Remote access for ESXi local user account \"\"root\"\" has been locked for 120 seconds after 75 failed login attempts
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 Esxi host authentication failures
tags                           +-
tags                           +- VMware
tags                           +- Esxi
tags                           +- authentication failures
```

Figure 13

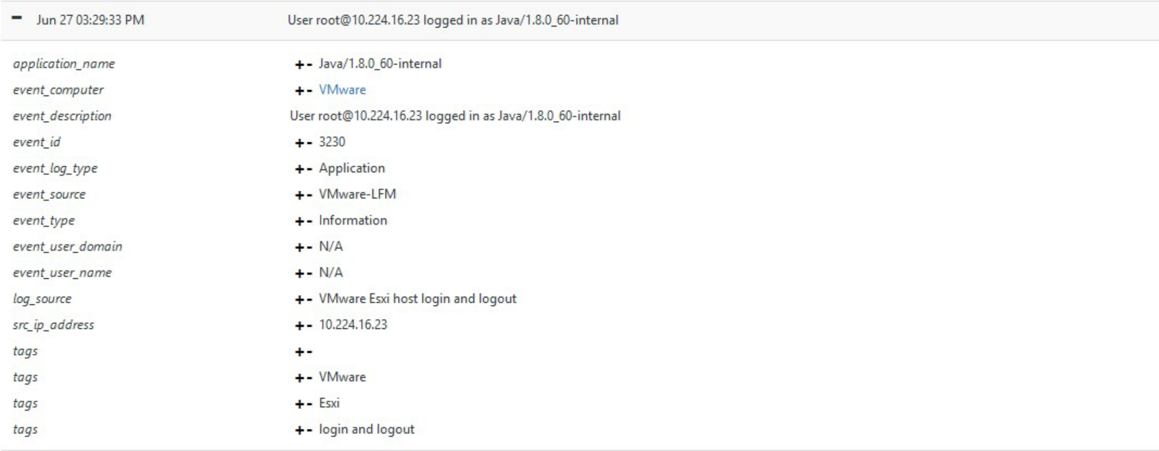
- **VMware- ESXi host login and logout:** This report provides information about the activities related to ESXi host login and logout.



Computer	Source IP Address	User Name	Action	User Agent
VCENTERTEST6-5.TOONS.LOCAL@NTPLDTBLR38-VMWARE	127.0.0.1	VSPHERE.LOCAL\vpxd-extension-99fd6229-b032-4bf5-9cc2-9a35c2dfaf8f	logged in	web-client/6.5.0
VCENTERTEST6-5.TOONS.LOCAL@NTPLDTBLR38-VMWARE	127.0.0.1	VSPHERE.LOCAL\vpxd-extension-99fd6229-b032-4bf5-9cc2-9a35c2dfaf8f	logged out	web-client/6.5.0
VCENTERTEST6-5.TOONS.LOCAL@NTPLDTBLR38-VMWARE	127.0.0.1	VSPHERE.LOCAL\vpxd-extension-99fd6229-b032-4bf5-9cc2-9a35c2dfaf8f	logged in	cl/1.0.0
VCENTERTEST6-5.TOONS.LOCAL@NTPLDTBLR38-VMWARE	127.0.0.1	VSPHERE.LOCAL\vpxd-extension-99fd6229-b032-4bf5-9cc2-9a35c2dfaf8f	logged out	web-client/6.5.0

Figure 14

Logs Considered:

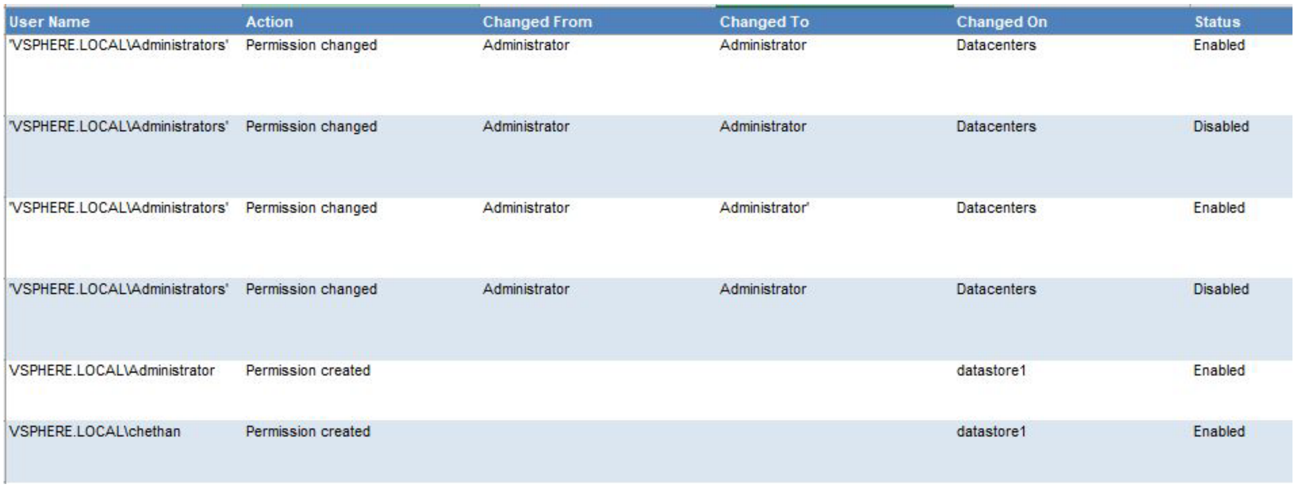


```
−  Jun 27 03:29:33 PM          User root@10.224.16.23 logged in as Java/1.8.0_60-internal

application_name               +- Java/1.8.0_60-internal
event_computer                 +- VMware
event_description              User root@10.224.16.23 logged in as Java/1.8.0_60-internal
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 Esxi host login and logout
src_ip_address                 +- 10.224.16.23
tags                           +-
tags                           +- VMware
tags                           +- Esxi
tags                           +- login and logout
```

Figure 15

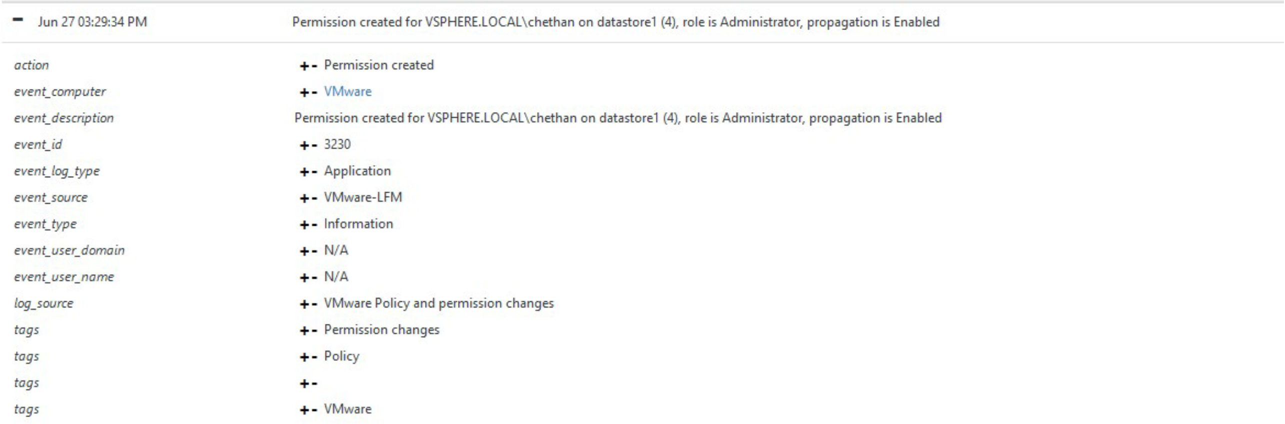
- **VMware- Policy and permission changes:** This report provides information about the activities related to policy and permission changes.



User Name	Action	Changed From	Changed To	Changed On	Status
'VSPHERE.LOCAL\Administrators'	Permission changed	Administrator	Administrator	Datacenters	Enabled
'VSPHERE.LOCAL\Administrators'	Permission changed	Administrator	Administrator	Datacenters	Disabled
'VSPHERE.LOCAL\Administrators'	Permission changed	Administrator	Administrator'	Datacenters	Enabled
'VSPHERE.LOCAL\Administrators'	Permission changed	Administrator	Administrator	Datacenters	Disabled
VSPHERE.LOCAL\Administrator	Permission created			datastore1	Enabled
VSPHERE.LOCAL\chethan	Permission created			datastore1	Enabled

Figure 16

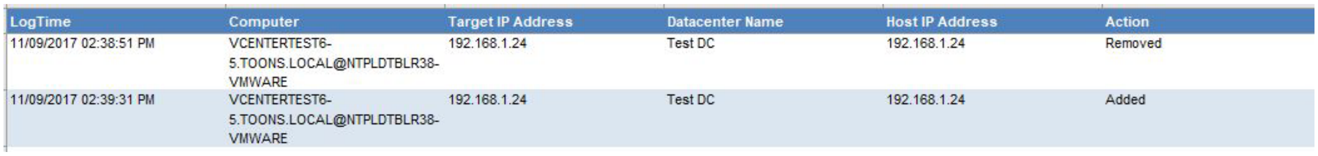
Logs Considered:



− Jun 27 03:29:34 PM	Permission created for VSPHERE.LOCAL\chethan on datastore1 (4), role is Administrator, propagation is Enabled
action	+- Permission created
event_computer	+- VMware
event_description	Permission created for VSPHERE.LOCAL\chethan on datastore1 (4), role is Administrator, propagation is Enabled
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 Policy and permission changes
tags	+- Permission changes
tags	+- Policy
tags	+-
tags	+- VMware

Figure 17

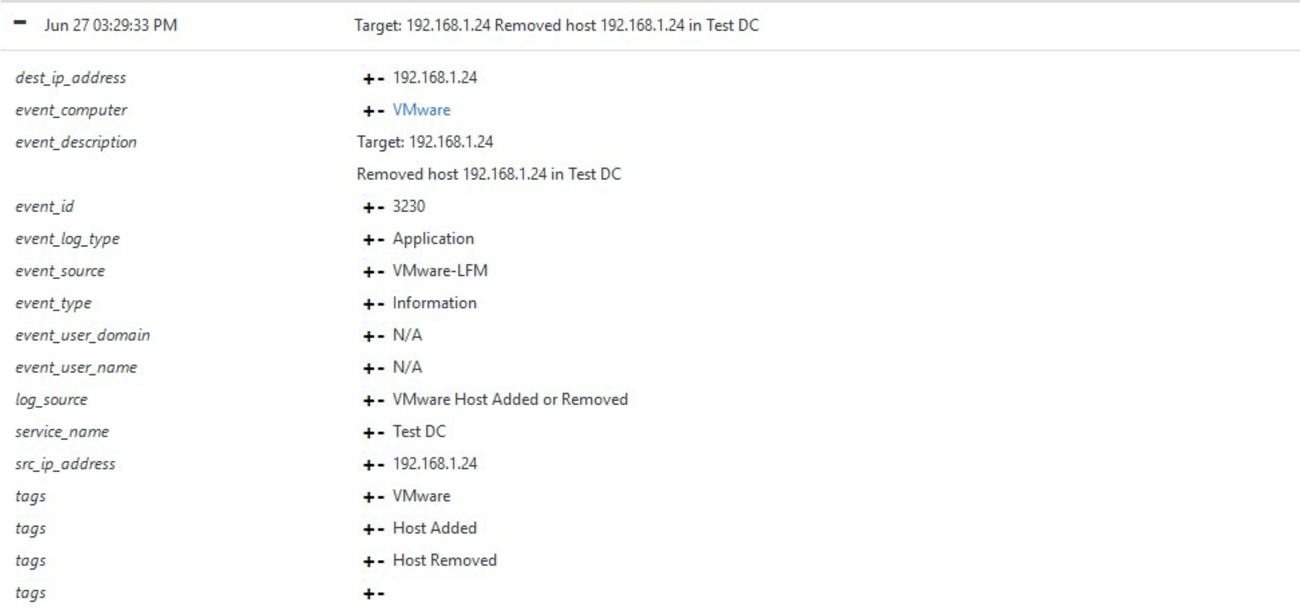
- **VMware- ESXi host added or removed:** This report provides information about the activities related to ESXi host added or removed.



LogTime	Computer	Target IP Address	Datacenter Name	Host IP Address	Action
11/09/2017 02:38:51 PM	VCENTERTEST6-5.TOONS.LOCAL@NTPLDTBLR38-VMWARE	192.168.1.24	Test DC	192.168.1.24	Removed
11/09/2017 02:39:31 PM	VCENTERTEST6-5.TOONS.LOCAL@NTPLDTBLR38-VMWARE	192.168.1.24	Test DC	192.168.1.24	Added

Figure 18

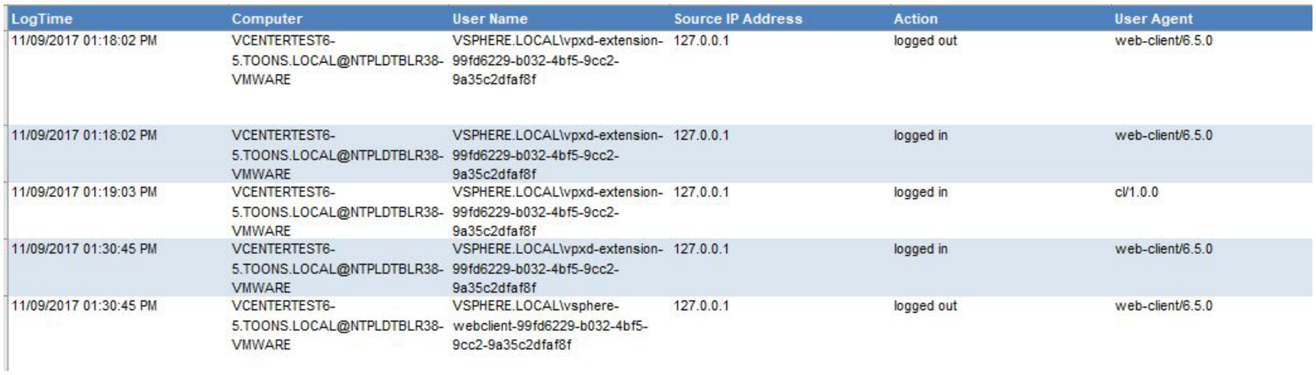
Logs Considered:



− Jun 27 03:29:33 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 Removed host 192.168.1.24 in Test DC
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 Host Added or Removed
service_name	+- Test DC
src_ip_address	+- 192.168.1.24
tags	+- VMware
tags	+- Host Added
tags	+- Host Removed
tags	+-

Figure 19

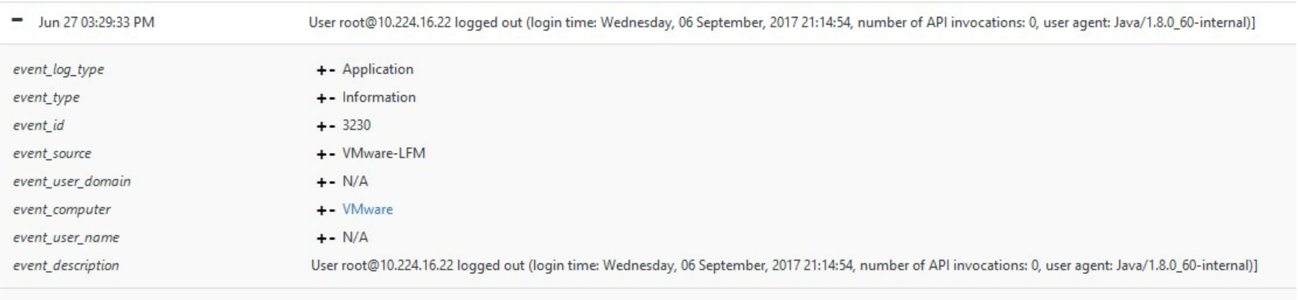
- **VMware- vCenter login and logout:** This report provides information about the activities related to vCenter login and logout.



LogTime	Computer	User Name	Source IP Address	Action	User Agent
11/09/2017 01:18:02 PM	VCENTERTEST6-5.TOONS.LOCAL@NTPLDTBLR38-VMWARE	VSPHERE.LOCAL\vpxd-extension-99fd6229-b032-4bf5-9cc2-9a35c2dfaf8f	127.0.0.1	logged out	web-client/6.5.0
11/09/2017 01:18:02 PM	VCENTERTEST6-5.TOONS.LOCAL@NTPLDTBLR38-VMWARE	VSPHERE.LOCAL\vpxd-extension-99fd6229-b032-4bf5-9cc2-9a35c2dfaf8f	127.0.0.1	logged in	web-client/6.5.0
11/09/2017 01:19:03 PM	VCENTERTEST6-5.TOONS.LOCAL@NTPLDTBLR38-VMWARE	VSPHERE.LOCAL\vpxd-extension-99fd6229-b032-4bf5-9cc2-9a35c2dfaf8f	127.0.0.1	logged in	cl/1.0.0
11/09/2017 01:30:45 PM	VCENTERTEST6-5.TOONS.LOCAL@NTPLDTBLR38-VMWARE	VSPHERE.LOCAL\vpxd-extension-99fd6229-b032-4bf5-9cc2-9a35c2dfaf8f	127.0.0.1	logged in	web-client/6.5.0
11/09/2017 01:30:45 PM	VCENTERTEST6-5.TOONS.LOCAL@NTPLDTBLR38-VMWARE	VSPHERE.LOCAL\vsphere-webclient-99fd6229-b032-4bf5-9cc2-9a35c2dfaf8f	127.0.0.1	logged out	web-client/6.5.0

Figure 20

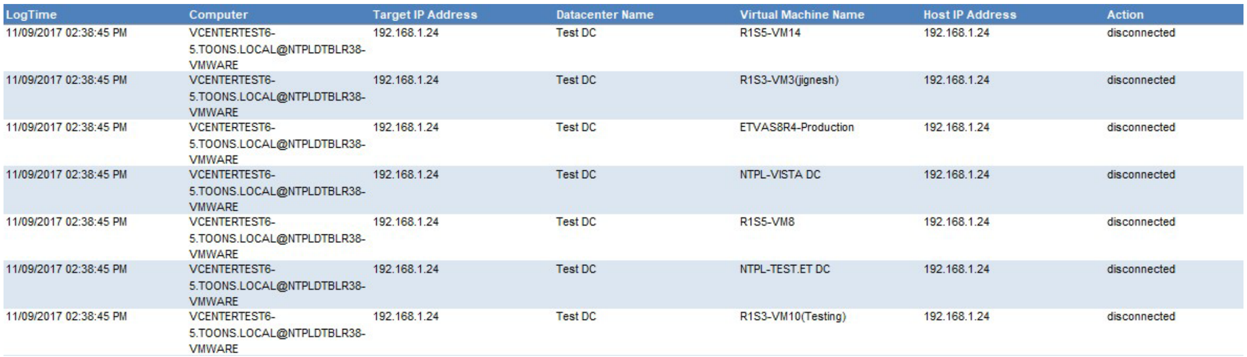
Logs Considered:



− Jun 27 03:29:33 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-internal)]
event_log_type	+- Application
event_type	+- Information
event_id	+- 3230
event_source	+- VMware-LFM
event_user_domain	+- N/A
event_computer	+- VMware
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-internal)]

Figure 21

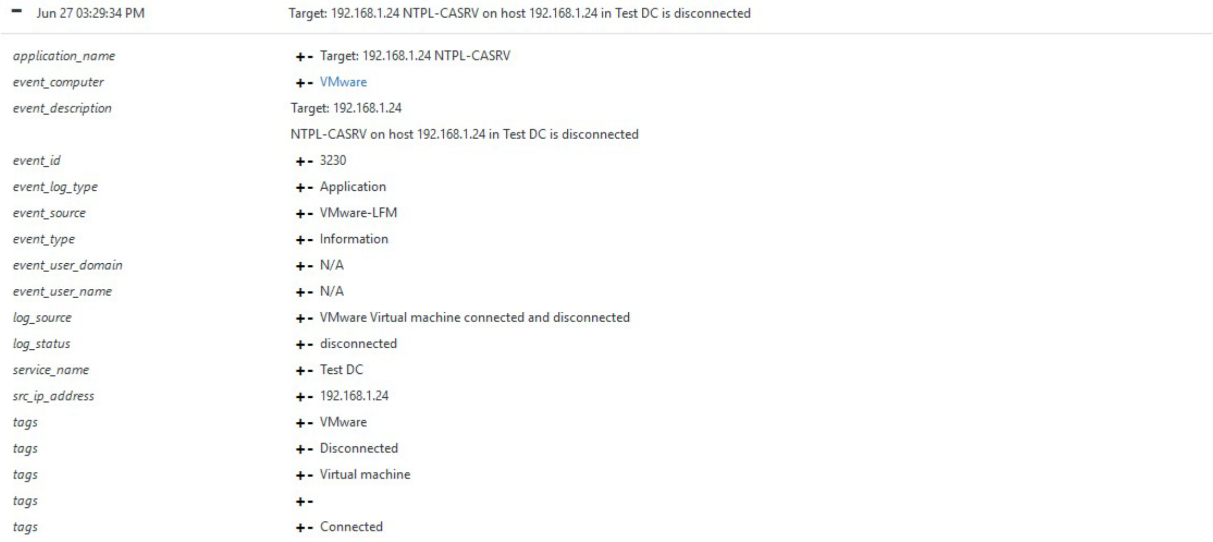
- **VMware- Virtual machine connected and disconnected:** This report provides information about the activities related to virtual machine connected and disconnected.



LogTime	Computer	Target IP Address	Datacenter Name	Virtual Machine Name	Host IP Address	Action
11/09/2017 02:38:45 PM	VCENTERTEST6-5.TOONS.LOCAL@NTPLDTBLR38-VMWARE	192.168.1.24	Test DC	R1S5-VM14	192.168.1.24	disconnected
11/09/2017 02:38:45 PM	VCENTERTEST6-5.TOONS.LOCAL@NTPLDTBLR38-VMWARE	192.168.1.24	Test DC	R1S3-VM3(jignesh)	192.168.1.24	disconnected
11/09/2017 02:38:45 PM	VCENTERTEST6-5.TOONS.LOCAL@NTPLDTBLR38-VMWARE	192.168.1.24	Test DC	ETVAS8R4-Production	192.168.1.24	disconnected
11/09/2017 02:38:45 PM	VCENTERTEST6-5.TOONS.LOCAL@NTPLDTBLR38-VMWARE	192.168.1.24	Test DC	NTPL-VISTA DC	192.168.1.24	disconnected
11/09/2017 02:38:45 PM	VCENTERTEST6-5.TOONS.LOCAL@NTPLDTBLR38-VMWARE	192.168.1.24	Test DC	R1S5-VM8	192.168.1.24	disconnected
11/09/2017 02:38:45 PM	VCENTERTEST6-5.TOONS.LOCAL@NTPLDTBLR38-VMWARE	192.168.1.24	Test DC	NTPL-TEST.ET DC	192.168.1.24	disconnected
11/09/2017 02:38:45 PM	VCENTERTEST6-5.TOONS.LOCAL@NTPLDTBLR38-VMWARE	192.168.1.24	Test DC	R1S3-VM10(Testing)	192.168.1.24	disconnected

Figure 22

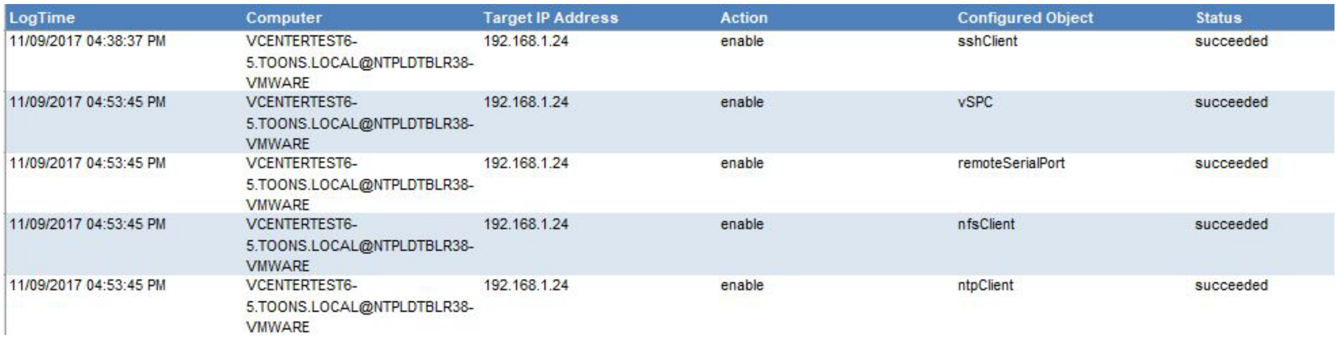
Logs Considered:



− Jun 27 03:29:34 PM	Target: 192.168.1.24 NTPL-CASRV on host 192.168.1.24 in Test DC is disconnected
application_name	+- Target: 192.168.1.24 NTPL-CASRV
event_computer	+- VMware
event_description	Target: 192.168.1.24 NTPL-CASRV on host 192.168.1.24 in Test DC is disconnected
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 Virtual machine connected and disconnected
log_status	+- disconnected
service_name	+- Test DC
src_ip_address	+- 192.168.1.24
tags	+- VMware
tags	+- Disconnected
tags	+- Virtual machine
tags	+-
tags	+- Connected

Figure 23

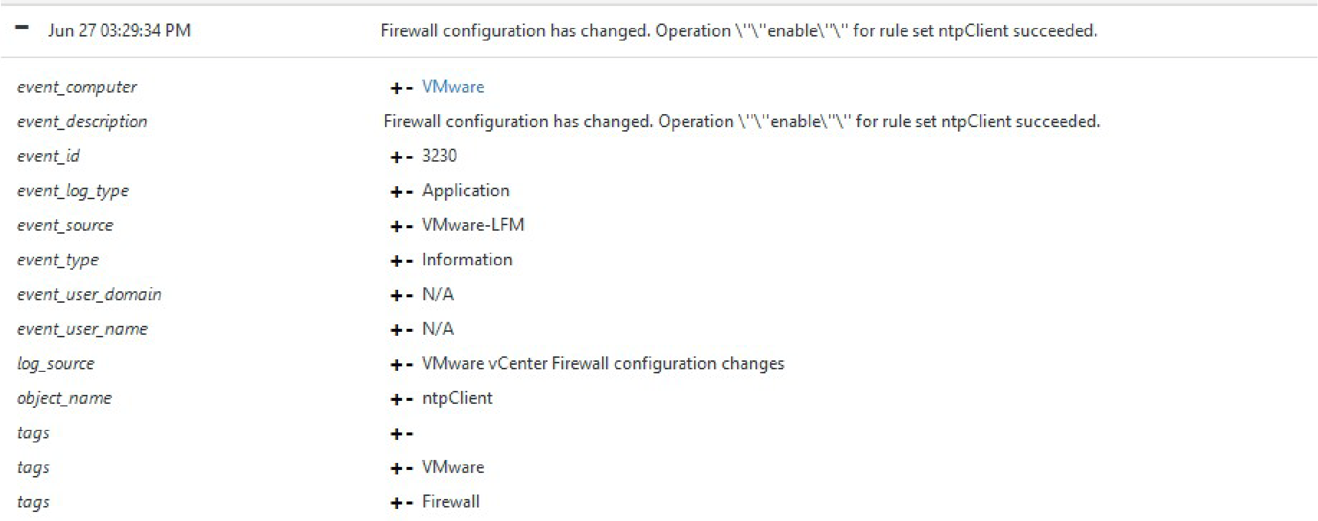
- **VMware- vCenter Firewall configuration changes:** This report provides information about the activities related to vCenter firewall configuration changes.



LogTime	Computer	Target IP Address	Action	Configured Object	Status
11/09/2017 04:38:37 PM	VCENTERTEST6-5.TOONS.LOCAL@NTPLDTBLR38-VMWARE	192.168.1.24	enable	sshClient	succeeded
11/09/2017 04:53:45 PM	VCENTERTEST6-5.TOONS.LOCAL@NTPLDTBLR38-VMWARE	192.168.1.24	enable	vSPC	succeeded
11/09/2017 04:53:45 PM	VCENTERTEST6-5.TOONS.LOCAL@NTPLDTBLR38-VMWARE	192.168.1.24	enable	remoteSerialPort	succeeded
11/09/2017 04:53:45 PM	VCENTERTEST6-5.TOONS.LOCAL@NTPLDTBLR38-VMWARE	192.168.1.24	enable	nfsClient	succeeded
11/09/2017 04:53:45 PM	VCENTERTEST6-5.TOONS.LOCAL@NTPLDTBLR38-VMWARE	192.168.1.24	enable	ntpClient	succeeded

Figure 24

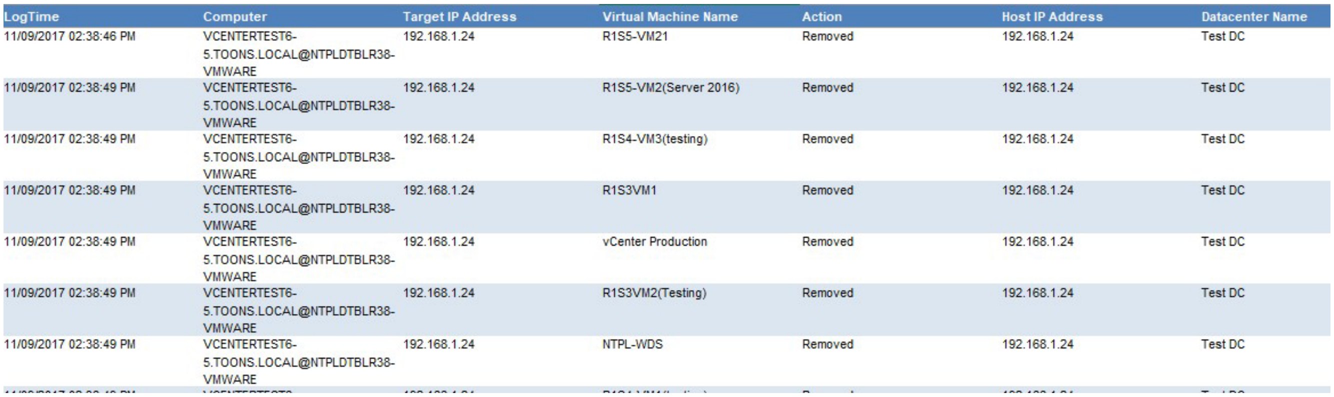
Logs Considered:



− Jun 27 03:29:34 PM	Firewall configuration has changed. Operation \"\"enable\"\" for rule set ntpClient succeeded.
event_computer	+- VMware
event_description	Firewall configuration has changed. Operation \"\"enable\"\" for rule set ntpClient succeeded.
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 vCenter Firewall configuration changes
object_name	+- ntpClient
tags	+-
tags	+- VMware
tags	+- Firewall

Figure 25

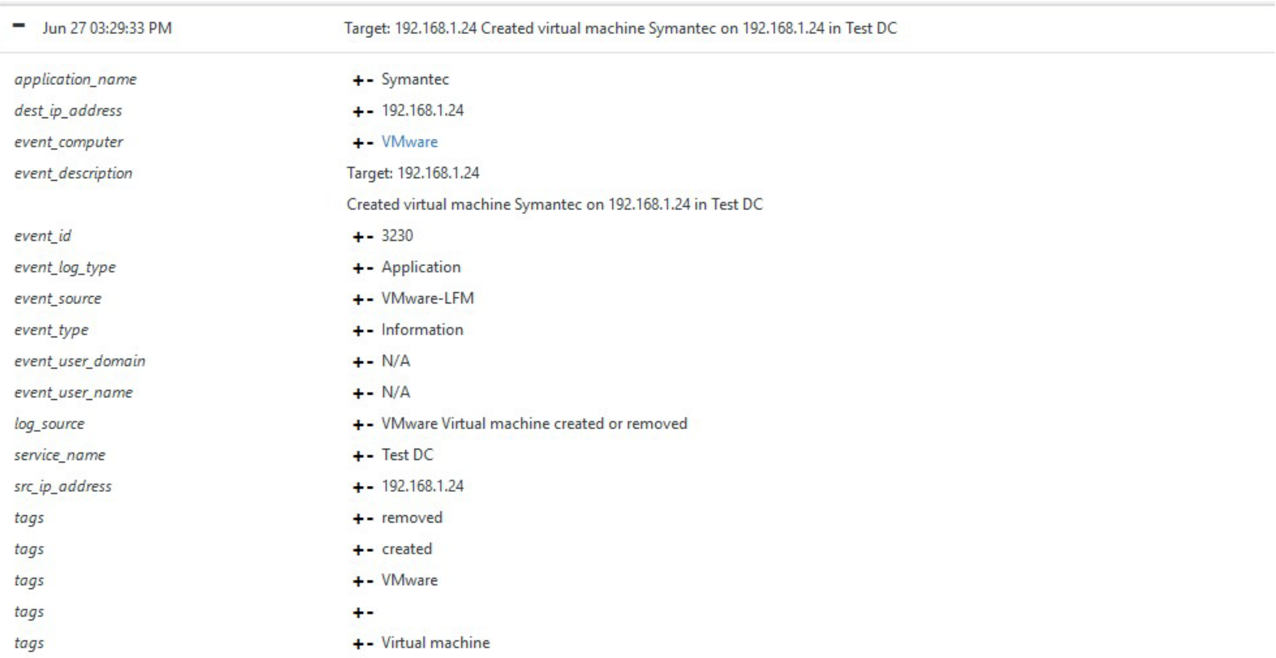
- **VMware- Virtual machine created or removed:** This report provides information about the activities related to virtual machine created or removed.



LogTime	Computer	Target IP Address	Virtual Machine Name	Action	Host IP Address	Datacenter Name
11/09/2017 02:38:46 PM	VCENTERTEST6-5.TOONS.LOCAL@NTPLDTBLR38-VMWARE	192.168.1.24	R1S5-VM21	Removed	192.168.1.24	Test DC
11/09/2017 02:38:49 PM	VCENTERTEST6-5.TOONS.LOCAL@NTPLDTBLR38-VMWARE	192.168.1.24	R1S5-VM2(Server 2016)	Removed	192.168.1.24	Test DC
11/09/2017 02:38:49 PM	VCENTERTEST6-5.TOONS.LOCAL@NTPLDTBLR38-VMWARE	192.168.1.24	R1S4-VM3(testing)	Removed	192.168.1.24	Test DC
11/09/2017 02:38:49 PM	VCENTERTEST6-5.TOONS.LOCAL@NTPLDTBLR38-VMWARE	192.168.1.24	R1S3VM1	Removed	192.168.1.24	Test DC
11/09/2017 02:38:49 PM	VCENTERTEST6-5.TOONS.LOCAL@NTPLDTBLR38-VMWARE	192.168.1.24	vCenter Production	Removed	192.168.1.24	Test DC
11/09/2017 02:38:49 PM	VCENTERTEST6-5.TOONS.LOCAL@NTPLDTBLR38-VMWARE	192.168.1.24	R1S3VM2(Testing)	Removed	192.168.1.24	Test DC
11/09/2017 02:38:49 PM	VCENTERTEST6-5.TOONS.LOCAL@NTPLDTBLR38-VMWARE	192.168.1.24	NTPL-WDS	Removed	192.168.1.24	Test DC

Figure 26

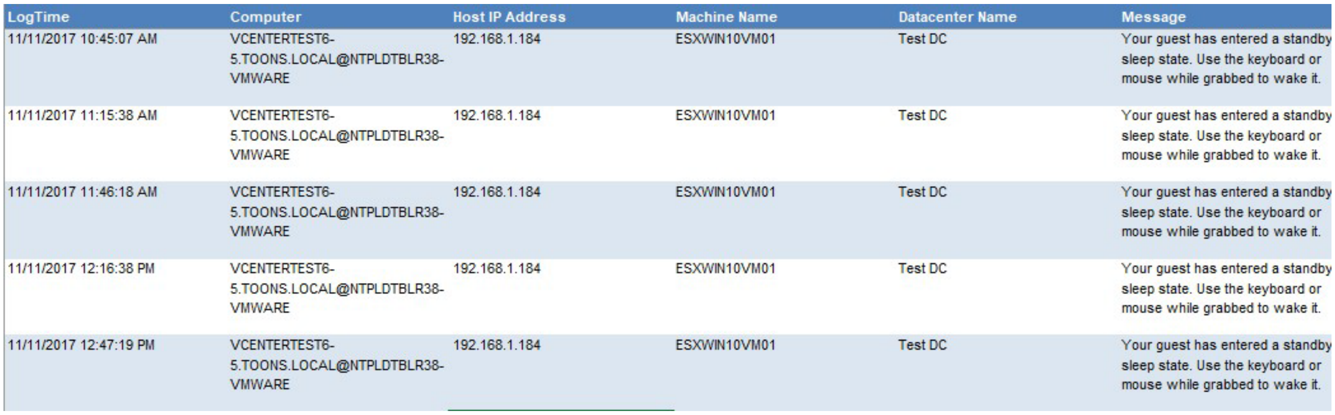
Logs Considered:



Jun 27 03:29:33 PM	Target: 192.168.1.24 Created virtual machine Symantec on 192.168.1.24 in Test DC
application_name	Symantec
dest_ip_address	192.168.1.24
event_computer	VMware
event_description	Target: 192.168.1.24 Created virtual machine Symantec on 192.168.1.24 in Test DC
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 Virtual machine created or removed
service_name	Test DC
src_ip_address	192.168.1.24
tags	removed
tags	created
tags	VMware
tags	
tags	Virtual machine

Figure 27

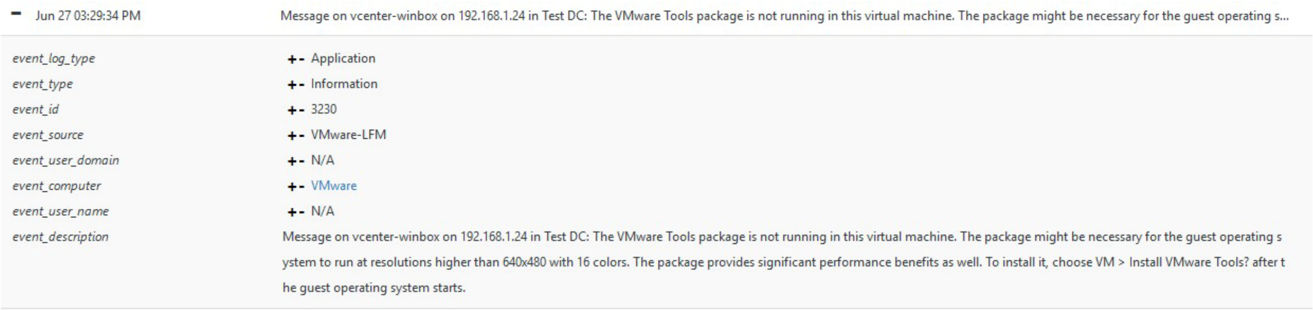
- **VMware- Virtual machine installation errors:** This report provides information about the activities related to virtual machine installation errors.



LogTime	Computer	Host IP Address	Machine Name	Datacenter Name	Message
11/11/2017 10:45:07 AM	VCENTERTEST6-5.TOONS.LOCAL@NTPLDTBLR38-VMWARE	192.168.1.184	ESXWIN10VM01	Test DC	Your guest has entered a standby sleep state. Use the keyboard or mouse while grabbed to wake it.
11/11/2017 11:15:38 AM	VCENTERTEST6-5.TOONS.LOCAL@NTPLDTBLR38-VMWARE	192.168.1.184	ESXWIN10VM01	Test DC	Your guest has entered a standby sleep state. Use the keyboard or mouse while grabbed to wake it.
11/11/2017 11:46:18 AM	VCENTERTEST6-5.TOONS.LOCAL@NTPLDTBLR38-VMWARE	192.168.1.184	ESXWIN10VM01	Test DC	Your guest has entered a standby sleep state. Use the keyboard or mouse while grabbed to wake it.
11/11/2017 12:16:38 PM	VCENTERTEST6-5.TOONS.LOCAL@NTPLDTBLR38-VMWARE	192.168.1.184	ESXWIN10VM01	Test DC	Your guest has entered a standby sleep state. Use the keyboard or mouse while grabbed to wake it.
11/11/2017 12:47:19 PM	VCENTERTEST6-5.TOONS.LOCAL@NTPLDTBLR38-VMWARE	192.168.1.184	ESXWIN10VM01	Test DC	Your guest has entered a standby sleep state. Use the keyboard or mouse while grabbed to wake it.

Figure 28

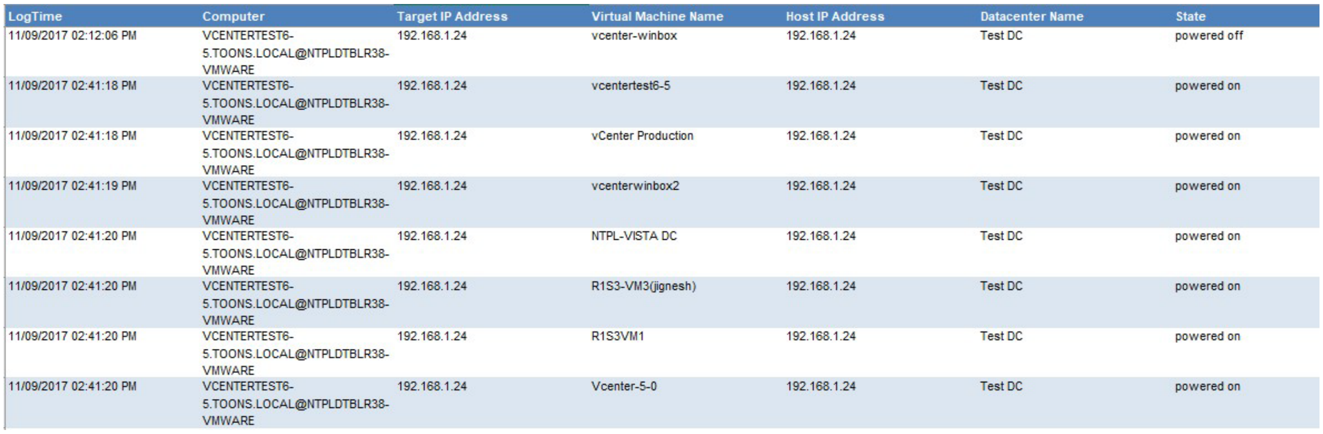
Logs Considered:



− Jun 27 03:29:34 PM	Message on vcenter-winbox on 192.168.1.24 in Test DC: The VMware Tools package is not running in this virtual machine. The package might be necessary for the guest operating s...
event_log_type	+- Application
event_type	+- Information
event_id	+- 3230
event_source	+- VMware-LFM
event_user_domain	+- N/A
event_computer	+- VMware
event_user_name	+- N/A
event_description	Message on vcenter-winbox on 192.168.1.24 in Test DC: The VMware Tools package is not running in this virtual machine. The package might be necessary for the guest operating system to run at resolutions higher than 640x480 with 16 colors. The package provides significant performance benefits as well. To install it, choose VM > Install VMware Tools? after the guest operating system starts.

Figure 29

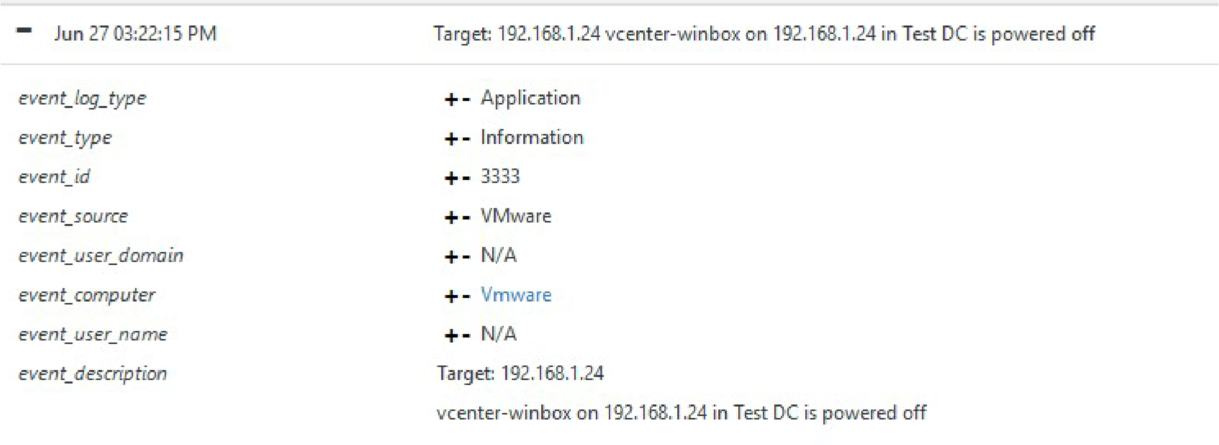
- **VMware- Virtual machine power on or off:** This report provides information about the activities related to virtual machine power on or off.



LogTime	Computer	Target IP Address	Virtual Machine Name	Host IP Address	Datacenter Name	State
11/09/2017 02:12:06 PM	VCENTERTEST6-5.TOONS.LOCAL@NTPLDTBLR38-VMWARE	192.168.1.24	vcenter-winbox	192.168.1.24	Test DC	powered off
11/09/2017 02:41:18 PM	VCENTERTEST6-5.TOONS.LOCAL@NTPLDTBLR38-VMWARE	192.168.1.24	vcentertest6-5	192.168.1.24	Test DC	powered on
11/09/2017 02:41:18 PM	VCENTERTEST6-5.TOONS.LOCAL@NTPLDTBLR38-VMWARE	192.168.1.24	vCenter Production	192.168.1.24	Test DC	powered on
11/09/2017 02:41:19 PM	VCENTERTEST6-5.TOONS.LOCAL@NTPLDTBLR38-VMWARE	192.168.1.24	vcenterwinbox2	192.168.1.24	Test DC	powered on
11/09/2017 02:41:20 PM	VCENTERTEST6-5.TOONS.LOCAL@NTPLDTBLR38-VMWARE	192.168.1.24	NTPL-VISTA DC	192.168.1.24	Test DC	powered on
11/09/2017 02:41:20 PM	VCENTERTEST6-5.TOONS.LOCAL@NTPLDTBLR38-VMWARE	192.168.1.24	R1S3-VM3(jignesh)	192.168.1.24	Test DC	powered on
11/09/2017 02:41:20 PM	VCENTERTEST6-5.TOONS.LOCAL@NTPLDTBLR38-VMWARE	192.168.1.24	R1S3VM1	192.168.1.24	Test DC	powered on
11/09/2017 02:41:20 PM	VCENTERTEST6-5.TOONS.LOCAL@NTPLDTBLR38-VMWARE	192.168.1.24	Vcenter-5-0	192.168.1.24	Test DC	powered on

Figure 30

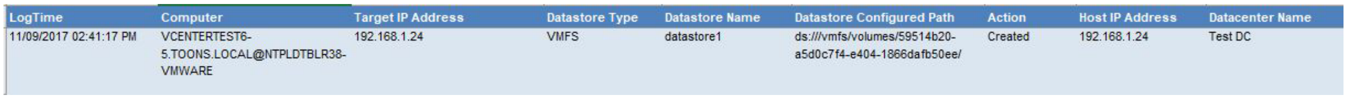
Logs Considered:



− Jun 27 03:22:15 PM	Target: 192.168.1.24 vcenter-winbox on 192.168.1.24 in Test DC is powered off
event_log_type	+- Application
event_type	+- Information
event_id	+- 3333
event_source	+- VMware
event_user_domain	+- N/A
event_computer	+- Vmware
event_user_name	+- N/A
event_description	Target: 192.168.1.24 vcenter-winbox on 192.168.1.24 in Test DC is powered off

Figure 31

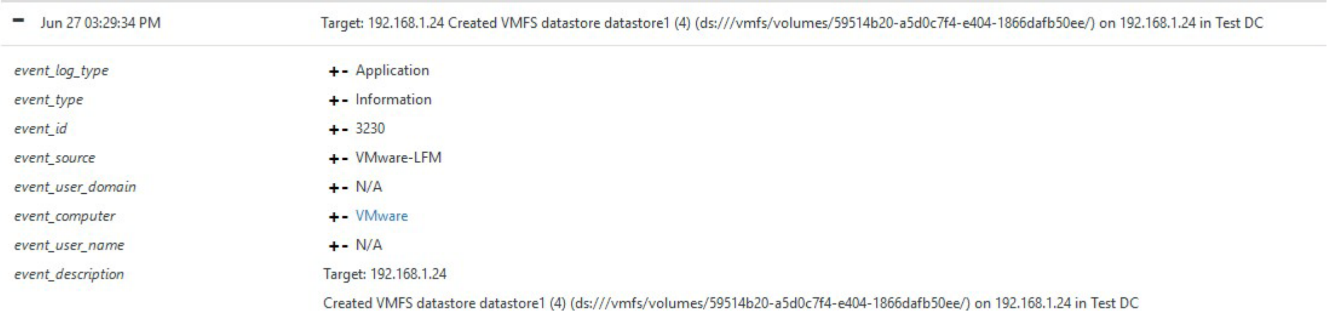
- **VMware- Datastore creation or deletion:** This report provides information about the activities related to datastore creation or deletion.



LogTime	Computer	Target IP Address	Datastore Type	Datastore Name	Datastore Configured Path	Action	Host IP Address	Datacenter Name
11/09/2017 02:41:17 PM	VCENTERTEST6-5.TOONS.LOCAL@NTPLDTBLR38-VMWARE	192.168.1.24	VMFS	datastore1	ds:///vmfs/volumes/59514b20-a5d0c7f4-e404-1866dafb50ee/	Created	192.168.1.24	Test DC

Figure 32

Logs Considered:



```
- Jun 27 03:29:34 PM    Target: 192.168.1.24 Created VMFS datastore datastore1 (4) (ds:///vmfs/volumes/59514b20-a5d0c7f4-e404-1866dafb50ee/) on 192.168.1.24 in Test DC

event_log_type       +- Application
event_type           +- Information
event_id             +- 3230
event_source         +- VMware-LFM
event_user_domain    +- N/A
event_computer       +- VMware
event_user_name      +- N/A
event_description    Target: 192.168.1.24
                     Created VMFS datastore datastore1 (4) (ds:///vmfs/volumes/59514b20-a5d0c7f4-e404-1866dafb50ee/) on 192.168.1.24 in Test DC
```

Figure 33

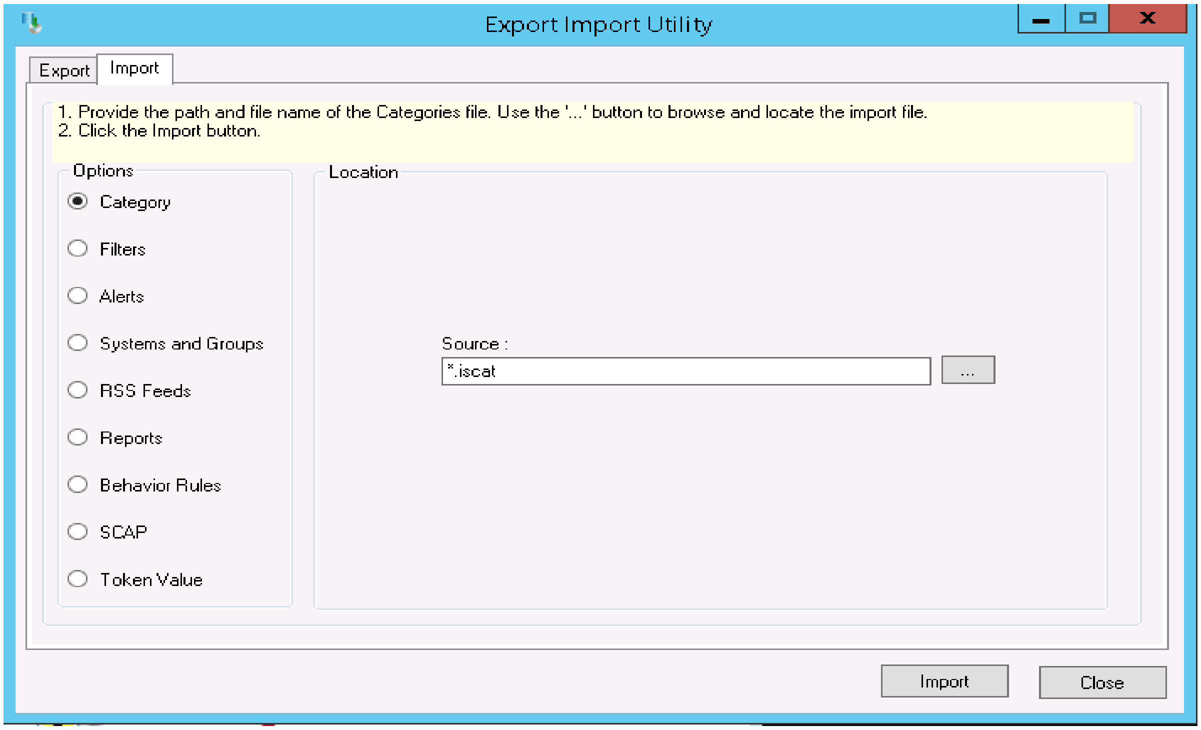
Import Knowledge Pack into EventTracker

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.



1. Provide the path and file name of the Categories file. Use the '...' button to browse and locate the import file.
2. Click the Import button.

● Category
○ Filters
○ Alerts
○ Systems and Groups
○ RSS Feeds
○ Reports
○ Behavior Rules
○ SCAP
○ Token Value

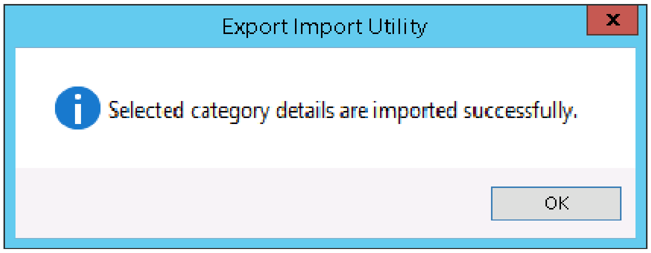
Source : *.iscat

Figure 34

2. Locate **Category_VMware.iscat** file, and then click the **Open** button.

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

   EventTracker displays success message.



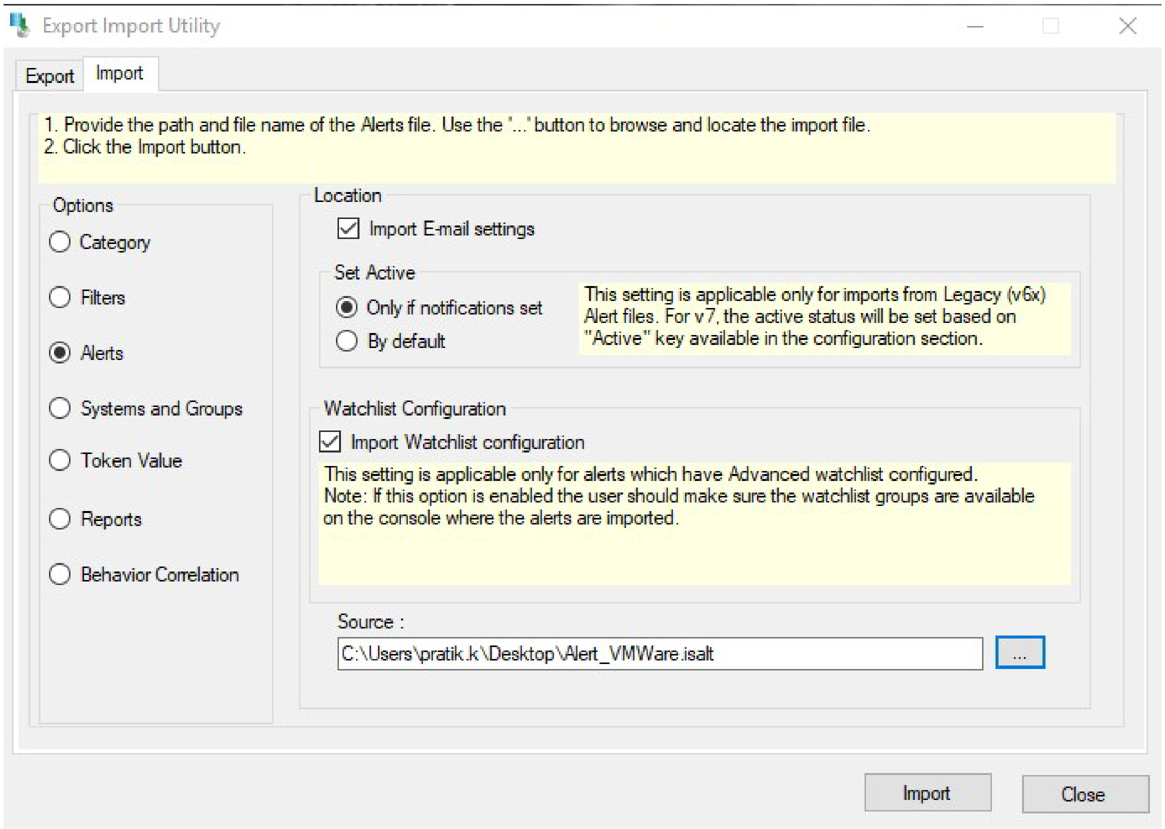
Selected category details are imported successfully.

Figure 35

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.



1. Provide the path and file name of the Alerts file. Use the "..." button to browse and locate the import file.
2. Click the Import button.

Options
○ Category
○ Filters
● Alerts
○ Systems and Groups
○ Token Value
○ Reports
○ Behavior Correlation

Location
☑ Import E-mail settings

Set Active
● Only if notifications set
○ By default

This setting is applicable only for imports from Legacy (v6x) Alert files. For v7, the active status will be set based on "Active" key available in the configuration section.

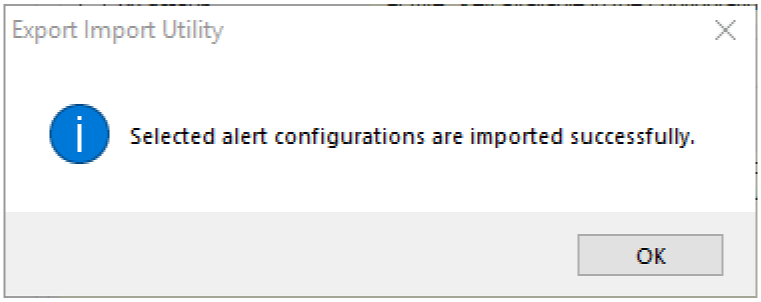
Watchlist Configuration
☑ Import Watchlist configuration

This setting is applicable only for alerts which have Advanced watchlist configured.
Note: If this option is enabled the user should make sure the watchlist groups are available on the console where the alerts are imported.

Source : C:\Users\pratik.k\Desktop\Alert_VMWare.isalt

Figure 36

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



Selected alert configurations are imported successfully.

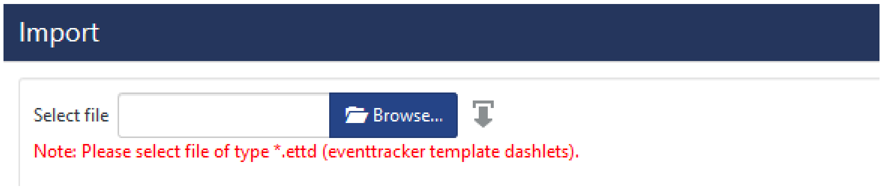
Figure 37

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

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.

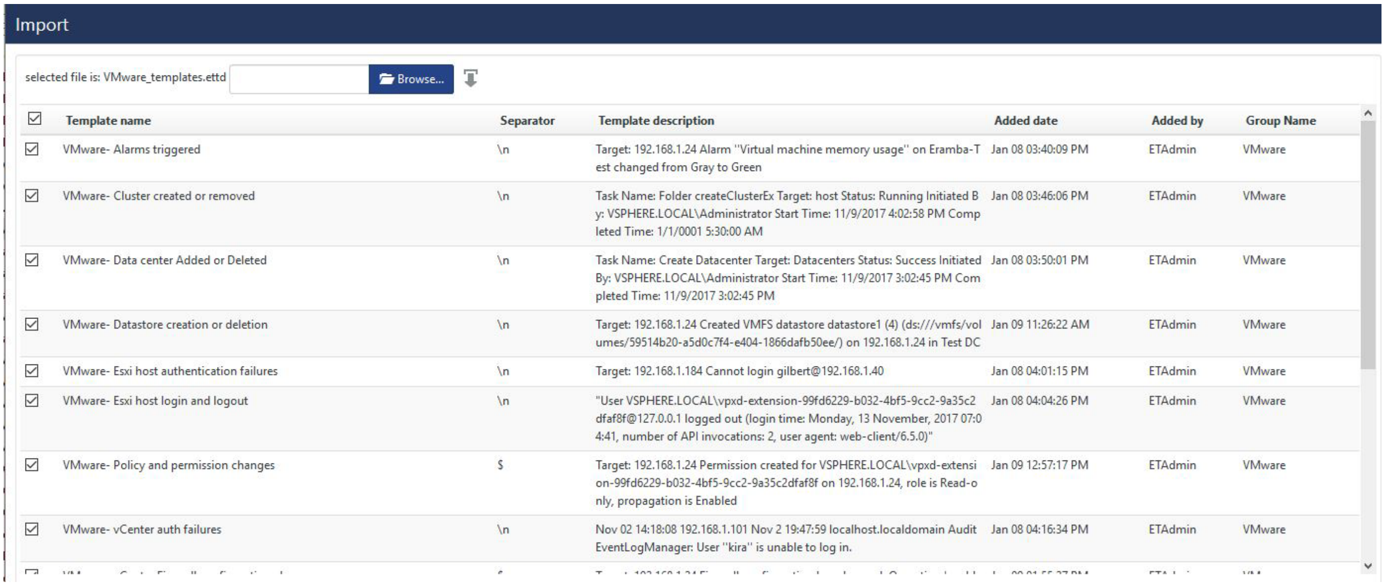


Import

Select file

Note: Please select file of type *.ettd (eventtracker template dashlets).

Figure 38



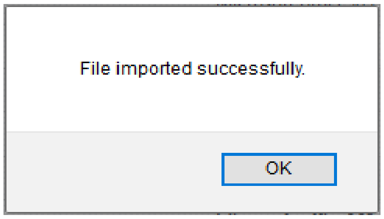
Import

selected file is: VMware_templates.ettd

☑	Template name	Separator	Template description	Added date	Added by	Group Name
☑	VMware- Alarms triggered	\n	Target: 192.168.1.24 Alarm "Virtual machine memory usage" on Eramba-Test changed from Gray to Green	Jan 08 03:40:09 PM	ETAdmin	VMware
☑	VMware- Cluster created or removed	\n	Task Name: Folder createClusterEx Target: host Status: Running Initiated By: VSPHERE.LOCAL\Administrator Start Time: 11/9/2017 4:02:58 PM Completed Time: 1/1/0001 5:30:00 AM	Jan 08 03:46:06 PM	ETAdmin	VMware
☑	VMware- Data center Added or Deleted	\n	Task Name: Create Datacenter Target: Datacenters Status: Success Initiated By: VSPHERE.LOCAL\Administrator Start Time: 11/9/2017 3:02:45 PM Completed Time: 11/9/2017 3:02:45 PM	Jan 08 03:50:01 PM	ETAdmin	VMware
☑	VMware- Datastore creation or deletion	\n	Target: 192.168.1.24 Created VMFS datastore datastore1 (4) (ds:///vmfs/volumes/59514b20-a5d0c7f4-e404-1866dafb50ee/) on 192.168.1.24 in Test DC	Jan 09 11:26:22 AM	ETAdmin	VMware
☑	VMware- Esxi host authentication failures	\n	Target: 192.168.1.184 Cannot login gilbert@192.168.1.40	Jan 08 04:01:15 PM	ETAdmin	VMware
☑	VMware- Esxi host login and logout	\n	"User VSPHERE.LOCAL\vpxd-extension-99fd6229-b032-4bf5-9cc2-9a35c2dfaf8f@127.0.0.1 logged out (login time: Monday, 13 November, 2017 07:04:41, number of API invocations: 2, user agent: web-client/6.5.0)"	Jan 08 04:04:26 PM	ETAdmin	VMware
☑	VMware- Policy and permission changes	$	Target: 192.168.1.24 Permission created for VSPHERE.LOCAL\vpxd-extension-99fd6229-b032-4bf5-9cc2-9a35c2dfaf8f on 192.168.1.24, role is Read-only, propagation is Enabled	Jan 09 12:57:17 PM	ETAdmin	VMware
☑	VMware- vCenter auth failures	\n	Nov 02 14:18:08 192.168.1.101 Nov 2 19:47:59 localhost.localdomain Audit EventLogManager: User "kira" is unable to log in.	Jan 08 04:16:34 PM	ETAdmin	VMware

Figure 39

- Templates are now imported successfully.



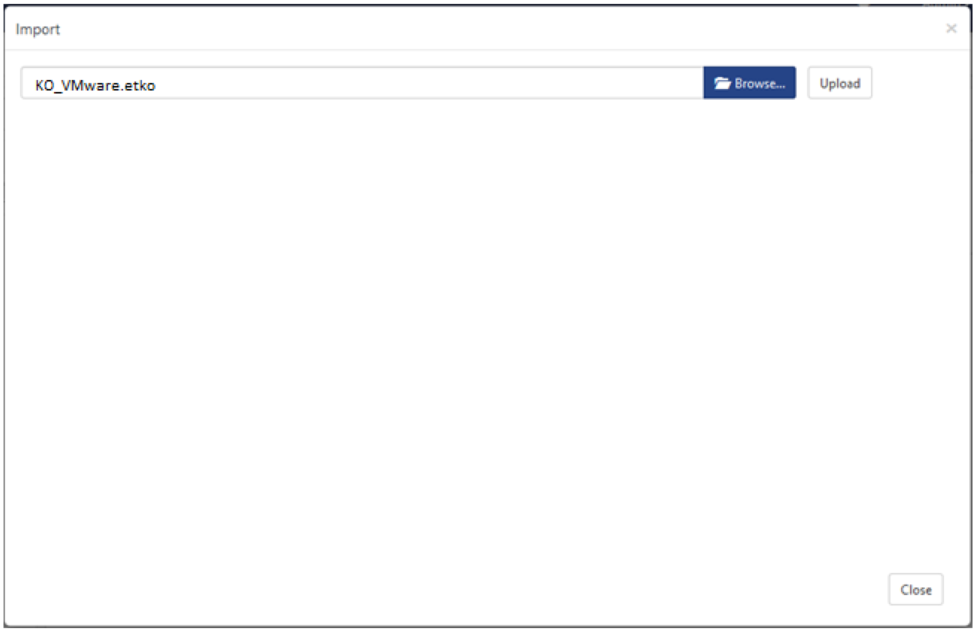
File imported successfully.

Figure 40

Import Knowledge Objects

1. Click **Knowledge objects** under Admin option in the EventTracker manager page.

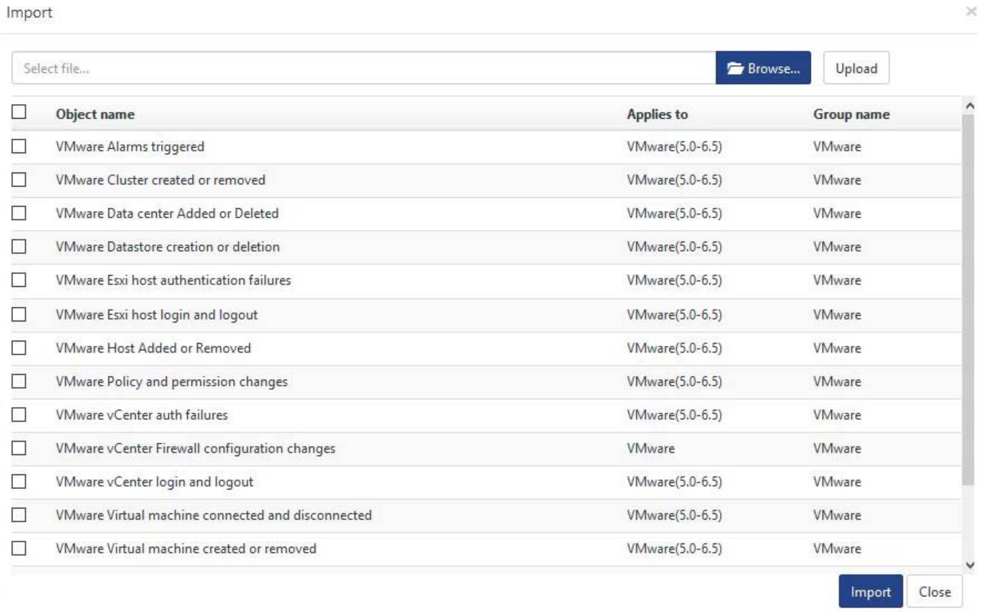
2. Locate the file named **KO_VMware.etko**.



KO_VMware.etko

Figure 41

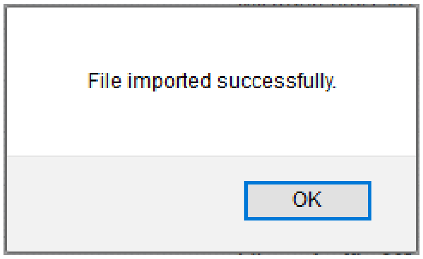
3. Now select all the check box and then click on ‘**Import**’ option.



□	Object name	Applies to	Group name
□	VMware Alarms triggered	VMware(5.0-6.5)	VMware
□	VMware Cluster created or removed	VMware(5.0-6.5)	VMware
□	VMware Data center Added or Deleted	VMware(5.0-6.5)	VMware
□	VMware Datastore creation or deletion	VMware(5.0-6.5)	VMware
□	VMware Esxi host authentication failures	VMware(5.0-6.5)	VMware
□	VMware Esxi host login and logout	VMware(5.0-6.5)	VMware
□	VMware Host Added or Removed	VMware(5.0-6.5)	VMware
□	VMware Policy and permission changes	VMware(5.0-6.5)	VMware
□	VMware vCenter auth failures	VMware(5.0-6.5)	VMware
□	VMware vCenter Firewall configuration changes	VMware	VMware
□	VMware vCenter login and logout	VMware(5.0-6.5)	VMware
□	VMware Virtual machine connected and disconnected	VMware(5.0-6.5)	VMware
□	VMware Virtual machine created or removed	VMware(5.0-6.5)	VMware

Figure 42

4. Knowledge objects are now imported successfully.

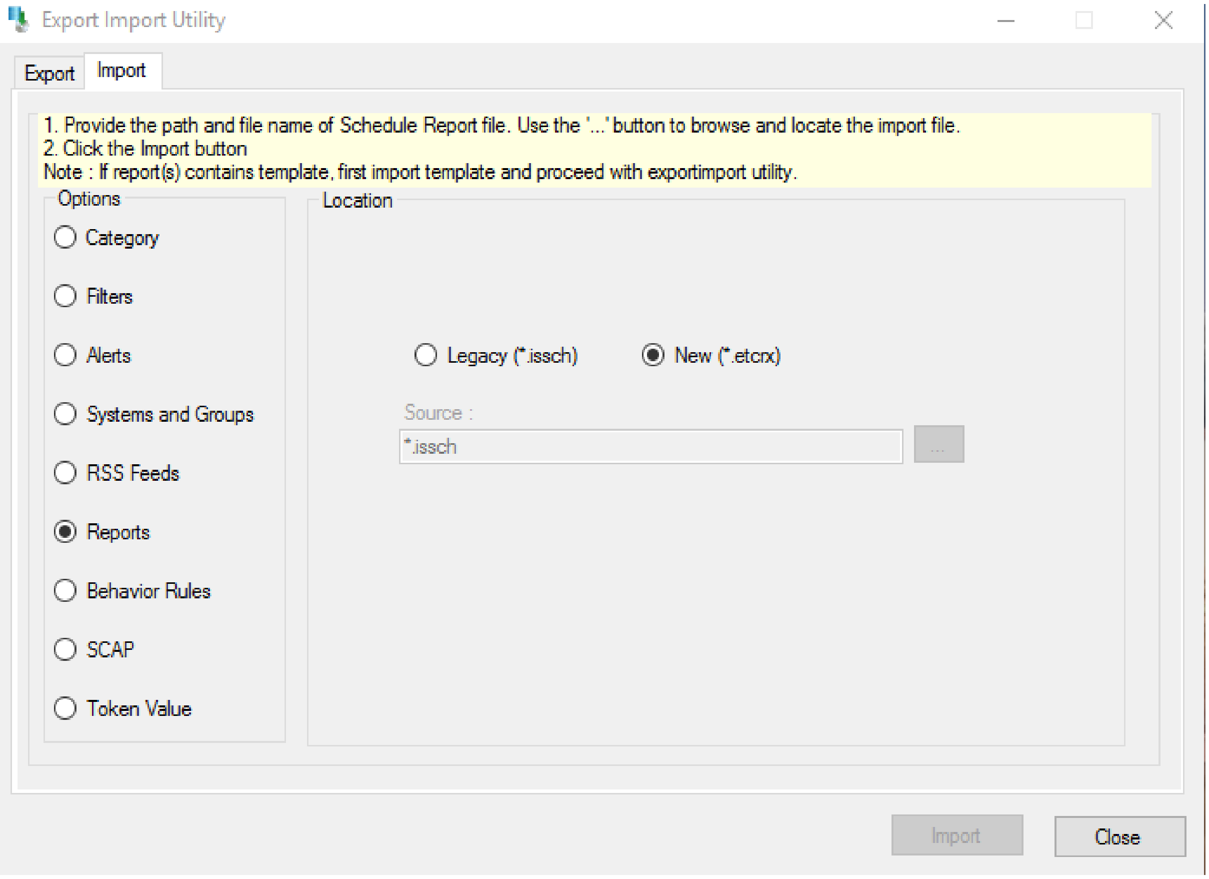


File imported successfully.

Figure 43

Import Flex Reports

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



1. Provide the path and file name of Schedule Report file. Use the '...' button to browse and locate the import file.
2. Click the Import button
Note : If report(s) contains template, first import template and proceed with exportimport utility.

Options

○ Category
○ Filters
○ Alerts
○ Systems and Groups
○ RSS Feeds
● Reports
○ Behavior Rules
○ SCAP
○ Token Value

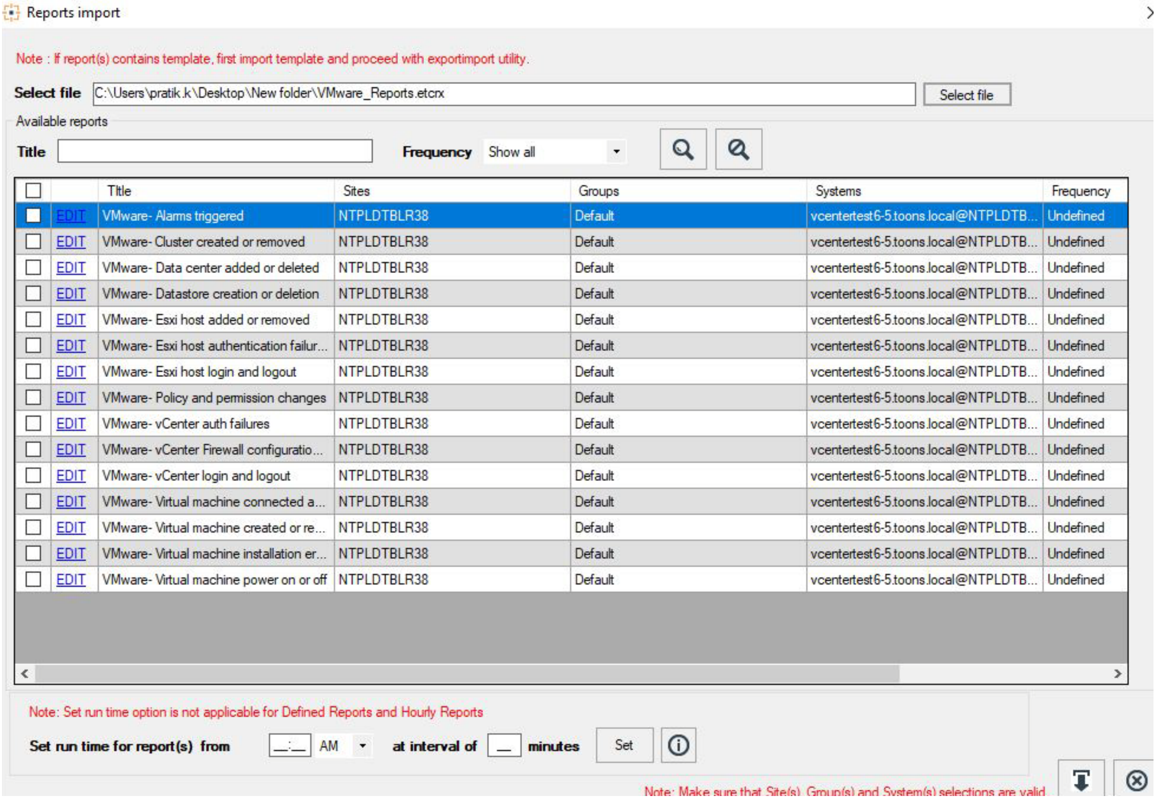
Location

○ Legacy (*.issch) ● New (*.etcrx)

Source : *.issch

Figure 44

2. Locate the file named **Reports_ VMware.etcrx**, and select all the check box.



Reports import

Note : If report(s) contains template, first import template and proceed with exportimport utility.

Select file C:\Users\pratik.k\Desktop\New folder\VMware_Reports.etcrx

Available reports

Title

Frequency Show all

□		TItle	Sites	Groups	Systems	Frequency
□	EDIT	VMware- Alarms triggered	NTPLDTBLR38	Default	vcentertest6-5.toons.local@NTPLDTB...	Undefined
□	EDIT	VMware- Cluster created or removed	NTPLDTBLR38	Default	vcentertest6-5.toons.local@NTPLDTB...	Undefined
□	EDIT	VMware- Data center added or deleted	NTPLDTBLR38	Default	vcentertest6-5.toons.local@NTPLDTB...	Undefined
□	EDIT	VMware- Datastore creation or deletion	NTPLDTBLR38	Default	vcentertest6-5.toons.local@NTPLDTB...	Undefined
□	EDIT	VMware- Esxi host added or removed	NTPLDTBLR38	Default	vcentertest6-5.toons.local@NTPLDTB...	Undefined
□	EDIT	VMware- Esxi host authentication failur...	NTPLDTBLR38	Default	vcentertest6-5.toons.local@NTPLDTB...	Undefined
□	EDIT	VMware- Esxi host login and logout	NTPLDTBLR38	Default	vcentertest6-5.toons.local@NTPLDTB...	Undefined
□	EDIT	VMware- Policy and permission changes	NTPLDTBLR38	Default	vcentertest6-5.toons.local@NTPLDTB...	Undefined
□	EDIT	VMware- vCenter auth failures	NTPLDTBLR38	Default	vcentertest6-5.toons.local@NTPLDTB...	Undefined
□	EDIT	VMware- vCenter Firewall configuratio...	NTPLDTBLR38	Default	vcentertest6-5.toons.local@NTPLDTB...	Undefined
□	EDIT	VMware- vCenter login and logout	NTPLDTBLR38	Default	vcentertest6-5.toons.local@NTPLDTB...	Undefined
□	EDIT	VMware- Virtual machine connected a...	NTPLDTBLR38	Default	vcentertest6-5.toons.local@NTPLDTB...	Undefined
□	EDIT	VMware- Virtual machine created or re...	NTPLDTBLR38	Default	vcentertest6-5.toons.local@NTPLDTB...	Undefined
□	EDIT	VMware- Virtual machine installation er...	NTPLDTBLR38	Default	vcentertest6-5.toons.local@NTPLDTB...	Undefined
□	EDIT	VMware- Virtual machine power on or off	NTPLDTBLR38	Default	vcentertest6-5.toons.local@NTPLDTB...	Undefined

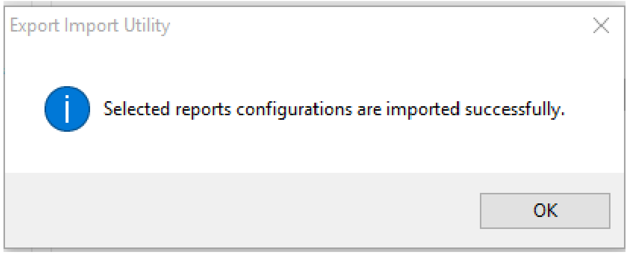
Note: Set run time option is not applicable for Defined Reports and Hourly Reports

Set run time for report(s) from __:__ AM at interval of __ minutes

Note: Make sure that Site(s), Group(s) and System(s) selections are valid

Figure 45

3. Click the **Import** button to import the reports. EventTracker displays success message.



Export Import Utility

Selected reports configurations are imported successfully.

Figure 46

Dashboards

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

1. Open **EventTracker Enterprise**.

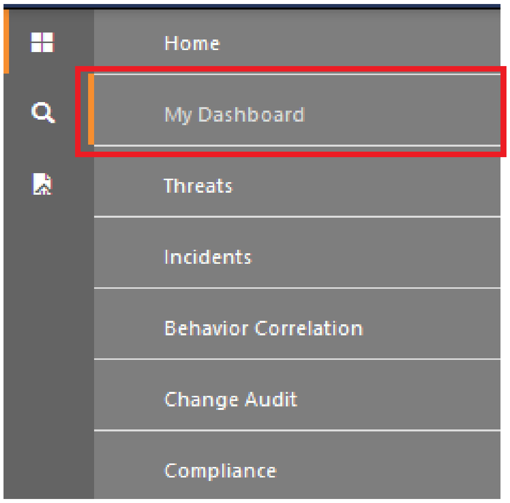
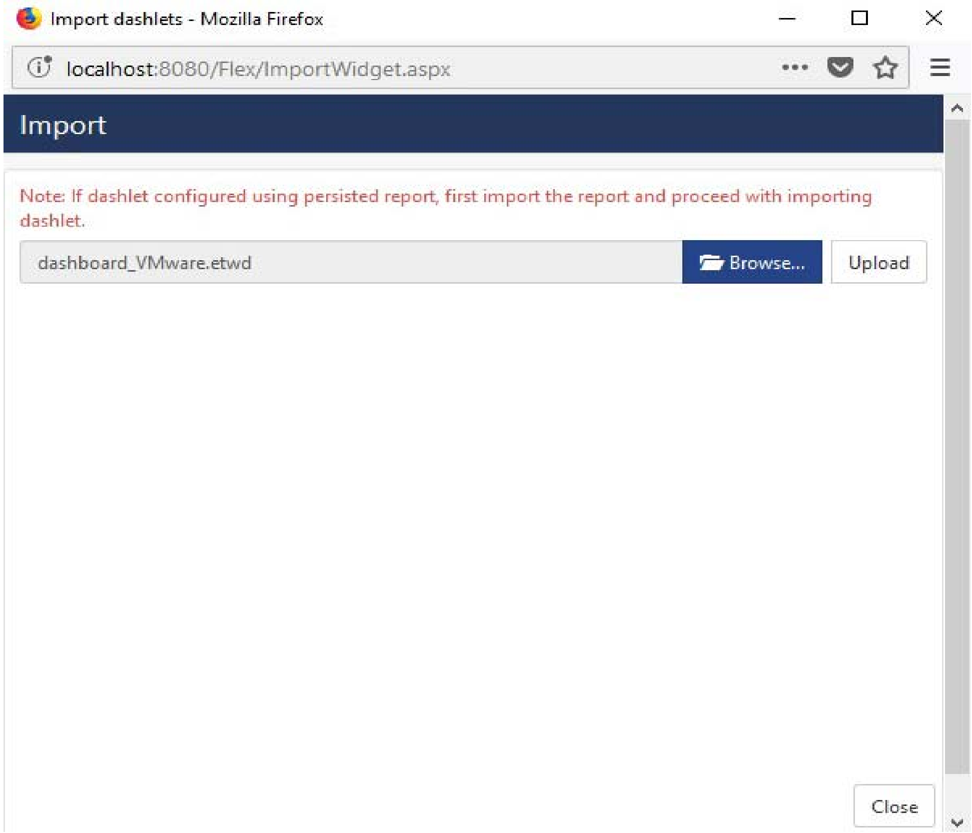


Figure 47

2. Navigate to **Dashboard>My Dashboard**.
   My Dashboard pane is shown.

3. Click the **'Import'** button to import the dashlets.

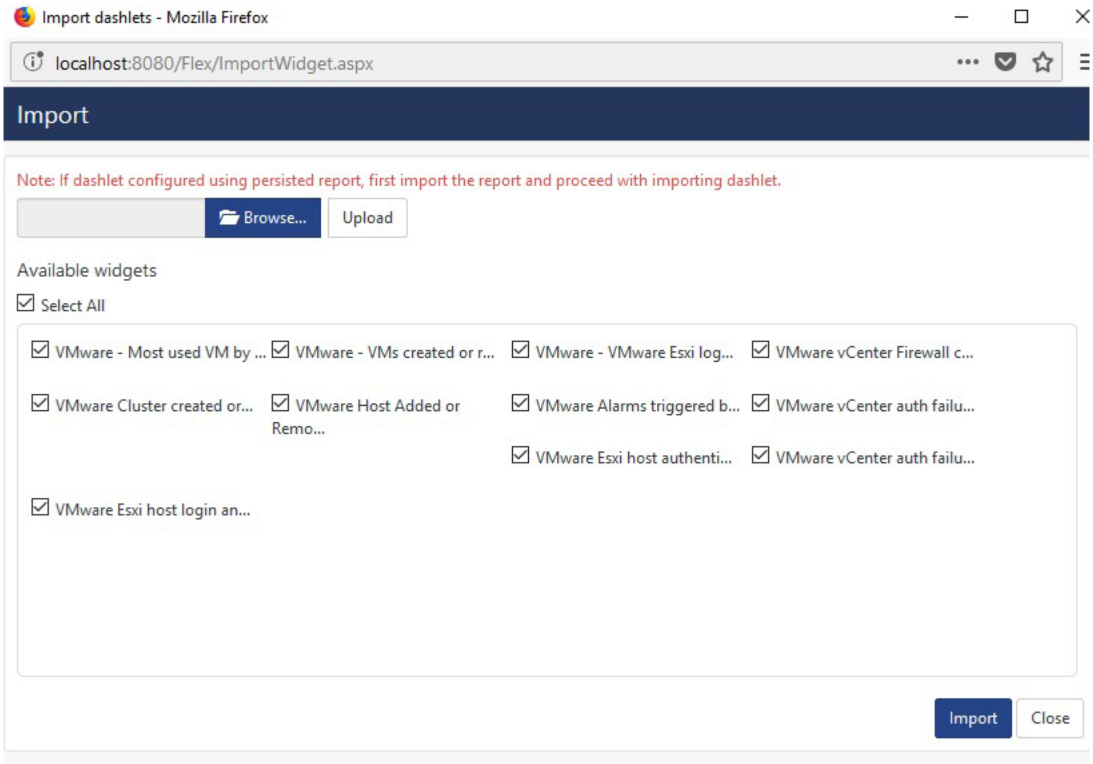

Import dashlets - Mozilla Firefox
localhost:8080/Flex/ImportWidget.aspx
Import
Browse...
Upload
Close

Note: If dashlet configured using persisted report, first import the report and proceed with importing dashlet.

dashboard_VMware.etwd

Figure 48

4. Locate the **Dashboard_Trend Micro CM.etwd** file.
5. Click the ‘**Upload’** option.



Import dashlets - Mozilla Firefox

localhost:8080/Flex/ImportWidget.aspx

Import

Note: If dashlet configured using persisted report, first import the report and proceed with importing dashlet.

Browse... Upload

Available widgets

☑ Select All

☑ VMware - Most used VM by ... ☑ VMware - VMs created or r... ☑ VMware - VMware Esxi log... ☑ VMware vCenter Firewall c...

☑ VMware Cluster created or... ☑ VMware Host Added or Remo... ☑ VMware Alarms triggered b... ☑ VMware vCenter auth failu...

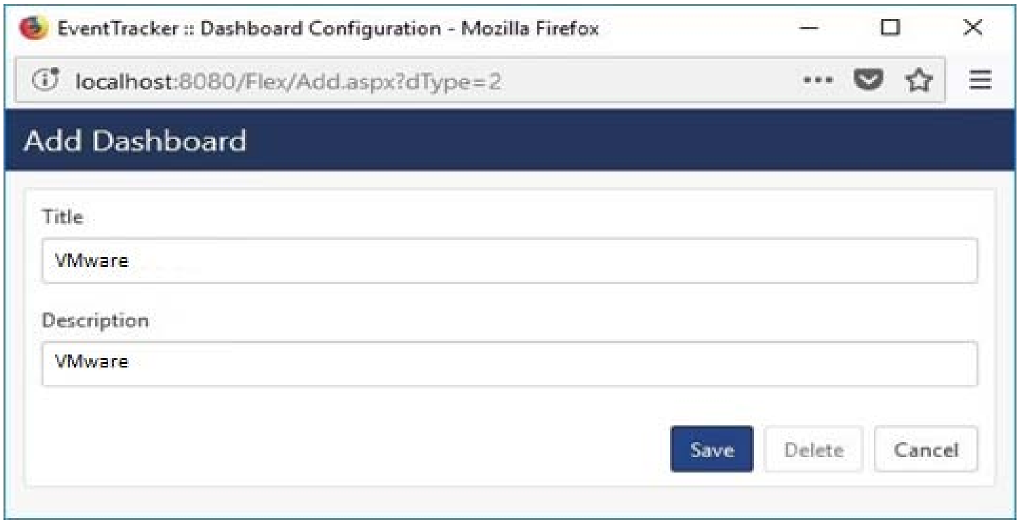
☑ VMware Esxi host authenti... ☑ VMware vCenter auth failu...

☑ VMware Esxi host login an...

Import Close

Figure 49

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.



EventTracker :: Dashboard Configuration - Mozilla Firefox

localhost:8080/Flex/Add.aspx?dType=2

Add Dashboard

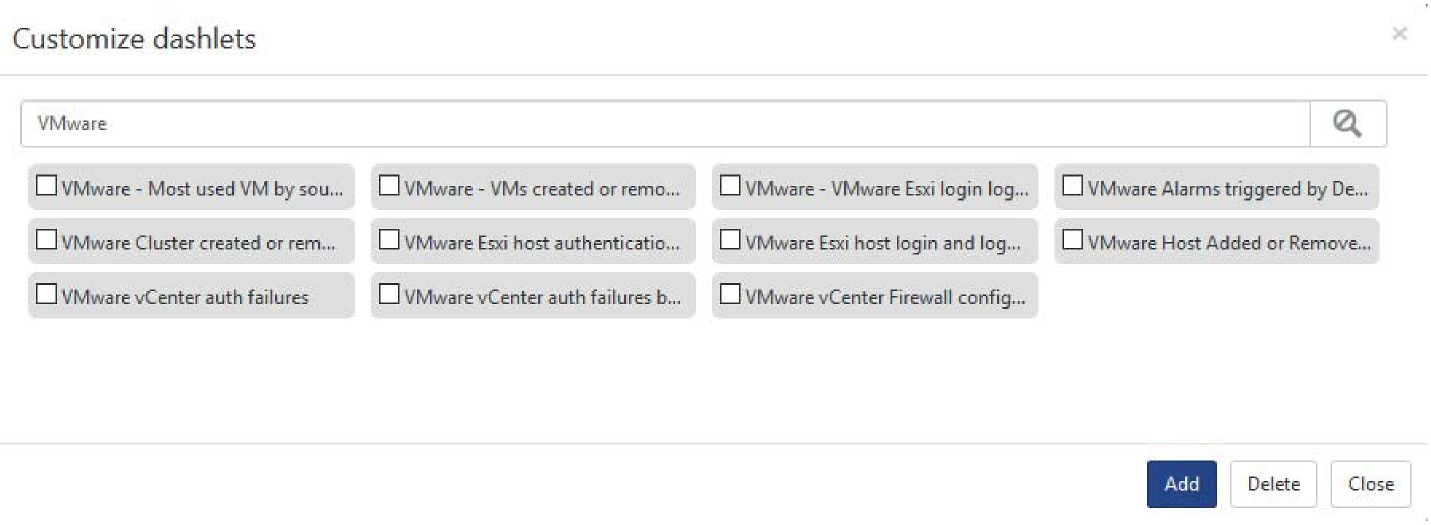
Title: VMware

Description: VMware

Save Delete Cancel

Figure 50

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.



Customize dashlets

VMware

□ VMware - Most used VM by sou...
□ VMware - VMs created or remo...
□ VMware - VMware Esxi login log...
□ VMware Alarms triggered by De...
□ VMware Cluster created or rem...
□ VMware Esxi host authenticatio...
□ VMware Esxi host login and log...
□ VMware Host Added or Remove...
□ VMware vCenter auth failures
□ VMware vCenter auth failures b...
□ VMware vCenter Firewall config...

Figure 51

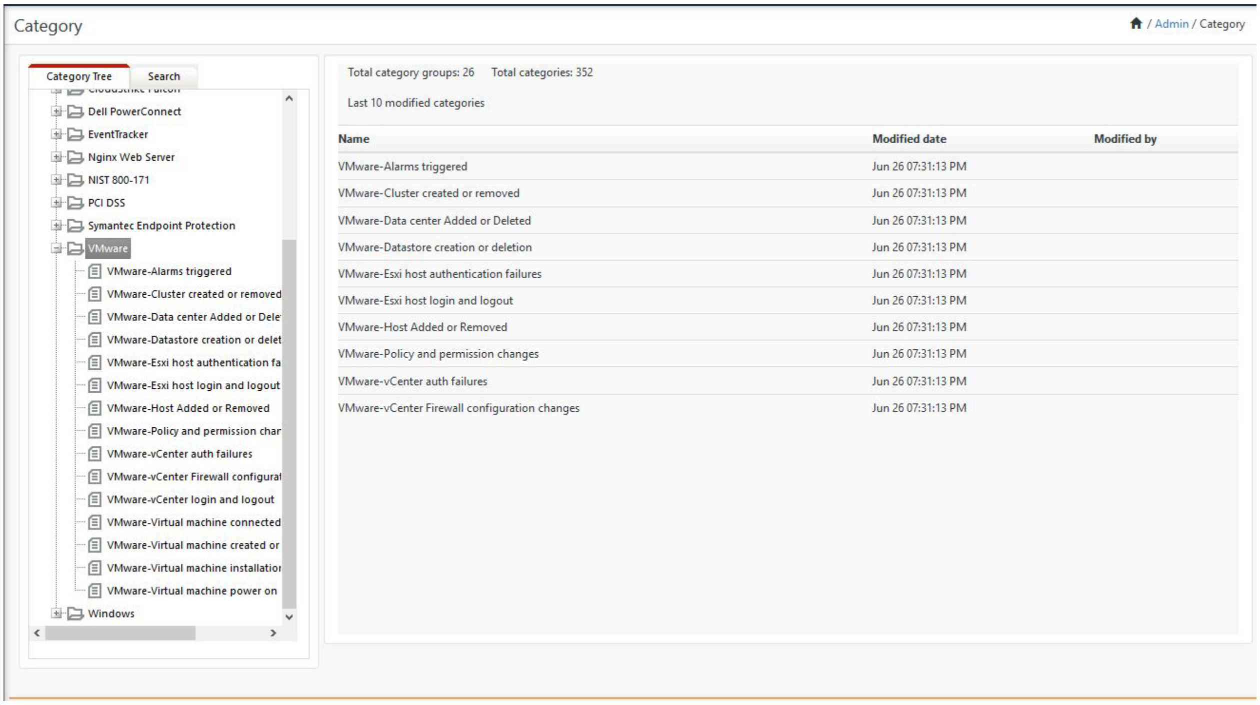
10. Click '**Add'** dashlet to create dashboard.

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.



Category

/ Admin / Category

- Dell PowerConnect
- EventTracker
- Nginx Web Server
- NIST 800-171
- PCI DSS
- Symantec Endpoint Protection
- VMware
  - VMware-Alarms triggered
  - VMware-Cluster created or removed
  - VMware-Data center Added or Dele
  - VMware-Datastore creation or delet
  - VMware-Esxi host authentication fa
  - VMware-Esxi host login and logout
  - VMware-Host Added or Removed
  - VMware-Policy and permission char
  - VMware-vCenter auth failures
  - VMware-vCenter Firewall configurat
  - VMware-vCenter login and logout
  - VMware-Virtual machine connected
  - VMware-Virtual machine created or
  - VMware-Virtual machine installatior
  - VMware-Virtual machine power on
- Windows

Total category groups: 26 Total categories: 352

Last 10 modified categories

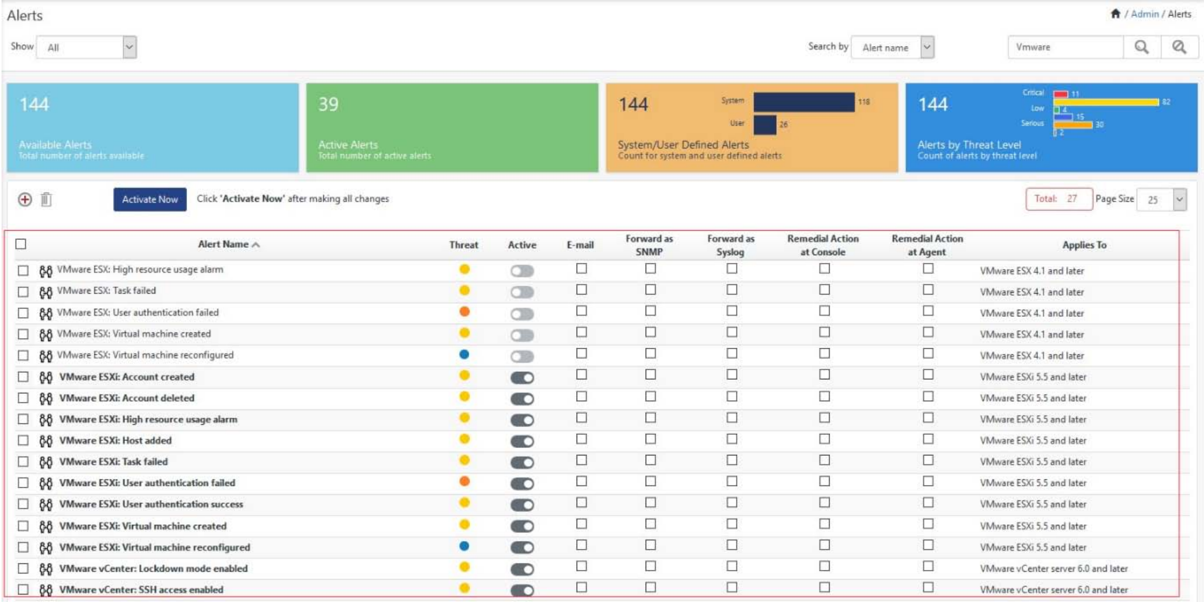
Name	Modified date	Modified by
VMware-Alarms triggered	Jun 26 07:31:13 PM	
VMware-Cluster created or removed	Jun 26 07:31:13 PM	
VMware-Data center Added or Deleted	Jun 26 07:31:13 PM	
VMware-Datastore creation or deletion	Jun 26 07:31:13 PM	
VMware-Esxi host authentication failures	Jun 26 07:31:13 PM	
VMware-Esxi host login and logout	Jun 26 07:31:13 PM	
VMware-Host Added or Removed	Jun 26 07:31:13 PM	
VMware-Policy and permission changes	Jun 26 07:31:13 PM	
VMware-vCenter auth failures	Jun 26 07:31:13 PM	
VMware-vCenter Firewall configuration changes	Jun 26 07:31:13 PM	

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.**



Alerts

/ Admin / Alerts

Show All

Search by Alert name

Vmware

144 Available Alerts Total number of alerts available

39 Active Alerts Total number of active alerts

144 System/User Defined Alerts Count for system and user defined alerts

144 Alerts by Threat Level Count of alerts by threat level

Click **'Activate Now'** after making all changes

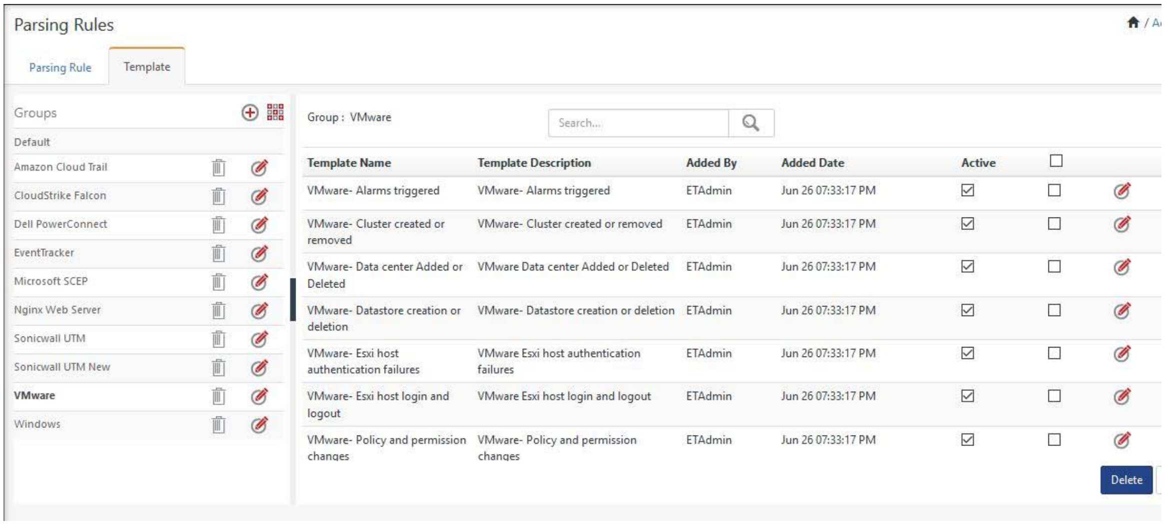
Total: 27 Page Size 25

□ Alert Name	Threat	Active	E-mail	Forward as SNMP	Forward as Syslog	Remedial Action at Console	Remedial Action at Agent	Applies To
□ VMware ESX: High resource usage alarm	●	○	□	□	□	□	□	VMware ESX 4.1 and later
□ VMware ESX: Task failed	●	○	□	□	□	□	□	VMware ESX 4.1 and later
□ VMware ESX: User authentication failed	●	○	□	□	□	□	□	VMware ESX 4.1 and later
□ VMware ESX: Virtual machine created	●	○	□	□	□	□	□	VMware ESX 4.1 and later
□ VMware ESX: Virtual machine reconfigured	●	○	□	□	□	□	□	VMware ESX 4.1 and later
□ **VMware ESXi: Account created**	●	●	□	□	□	□	□	VMware ESXi 5.5 and later
□ **VMware ESXi: Account deleted**	●	●	□	□	□	□	□	VMware ESXi 5.5 and later
□ **VMware ESXi: High resource usage alarm**	●	●	□	□	□	□	□	VMware ESXi 5.5 and later
□ **VMware ESXi: Host added**	●	●	□	□	□	□	□	VMware ESXi 5.5 and later
□ **VMware ESXi: Task failed**	●	●	□	□	□	□	□	VMware ESXi 5.5 and later
□ **VMware ESXi: User authentication failed**	●	●	□	□	□	□	□	VMware ESXi 5.5 and later
□ **VMware ESXi: User authentication success**	●	●	□	□	□	□	□	VMware ESXi 5.5 and later
□ **VMware ESXi: Virtual machine created**	●	●	□	□	□	□	□	VMware ESXi 5.5 and later
□ **VMware ESXi: Virtual machine reconfigured**	●	●	□	□	□	□	□	VMware ESXi 5.5 and later
□ **VMware vCenter: Lockdown mode enabled**	●	●	□	□	□	□	□	VMware vCenter server 6.0 and later
□ **VMware vCenter: SSH access enabled**	●	●	□	□	□	□	□	VMware vCenter server 6.0 and later

Figure 53

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.



Group : VMware

Template Name	Template Description	Added By	Added Date	Active	□
VMware- Alarms triggered	VMware- Alarms triggered	ETAdmin	Jun 26 07:33:17 PM	☑	□
VMware- Cluster created or removed	VMware- Cluster created or removed	ETAdmin	Jun 26 07:33:17 PM	☑	□
VMware- Data center Added or Deleted	VMware Data center Added or Deleted	ETAdmin	Jun 26 07:33:17 PM	☑	□
VMware- Datastore creation or deletion	VMware- Datastore creation or deletion	ETAdmin	Jun 26 07:33:17 PM	☑	□
VMware- Esxi host authentication failures	VMware Esxi host authentication failures	ETAdmin	Jun 26 07:33:17 PM	☑	□
VMware- Esxi host login and logout	VMware Esxi host login and logout	ETAdmin	Jun 26 07:33:17 PM	☑	□
VMware- Policy and permission changes	VMware- Policy and permission changes	ETAdmin	Jun 26 07:33:17 PM	☑	□

Figure 54

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.

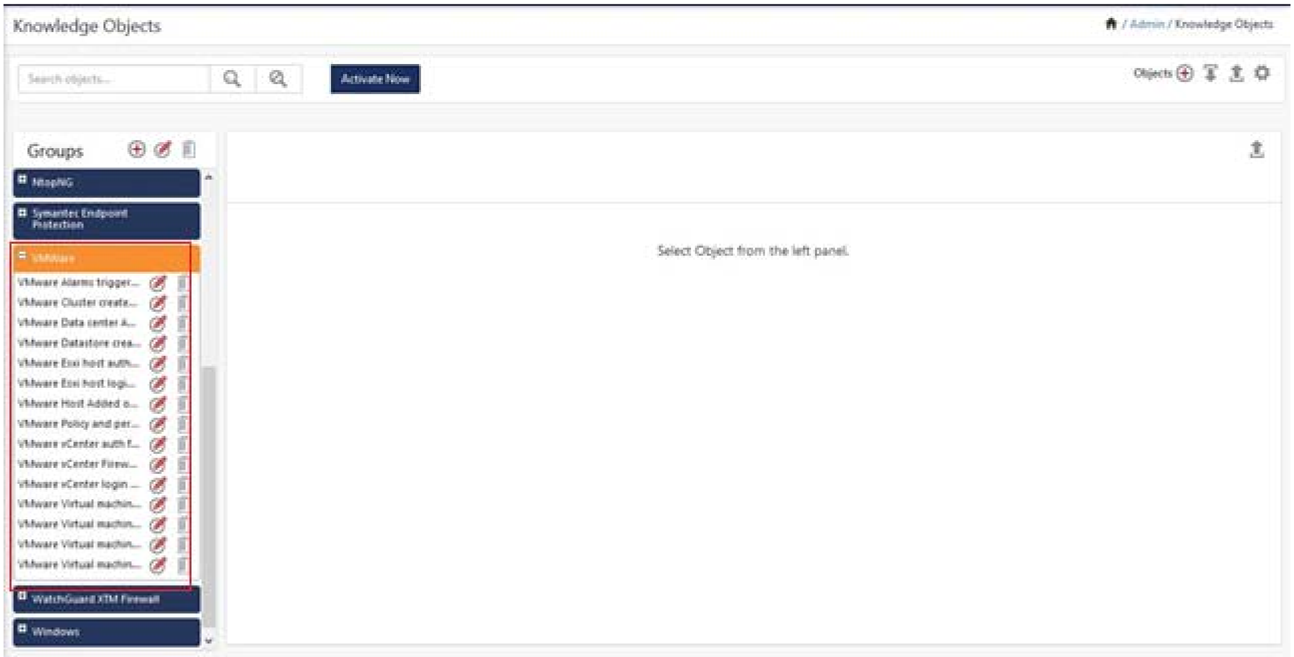
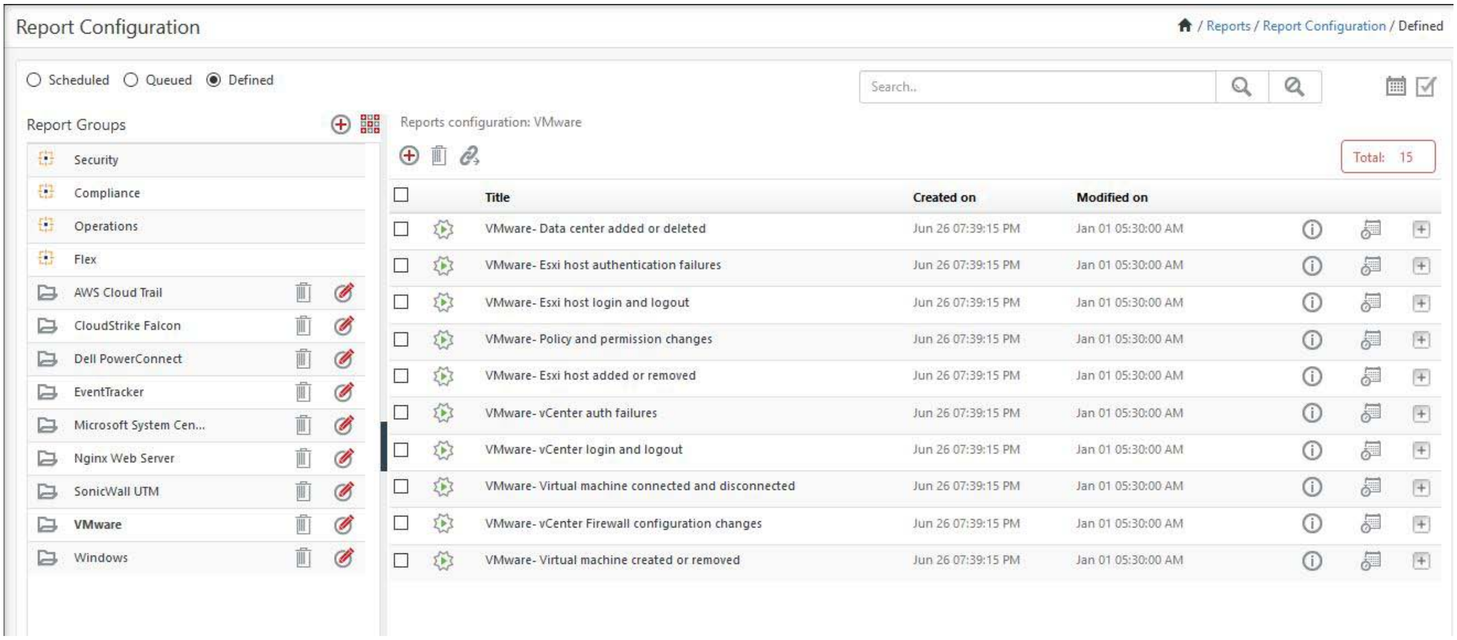


Figure 55

Reports

1. Logon to **EventTracker Enterprise**.
2. Click the **Reports** menu, and then **Configuration**.
3. Select **Defined** in report type.
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.



Report Configuration

/ Reports / Report Configuration / Defined

○ Scheduled ○ Queued ● Defined

Search..

Report Groups

- Security
- Compliance
- Operations
- Flex
- AWS Cloud Trail
- CloudStrike Falcon
- Dell PowerConnect
- EventTracker
- Microsoft System Cen...
- Nginx Web Server
- SonicWall UTM
- VMware
- Windows

Reports configuration: VMware

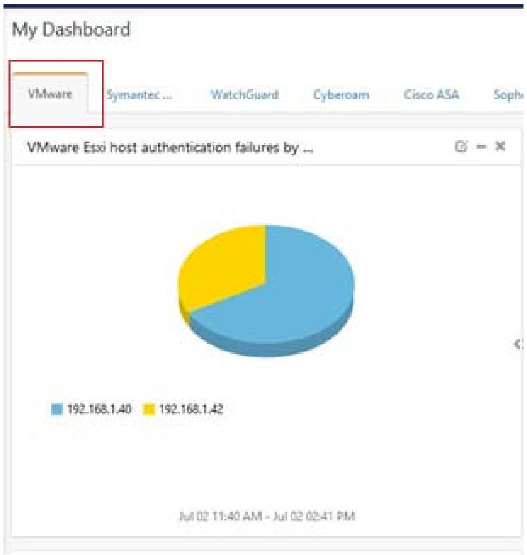
Total: 15

□	Title	Created on	Modified on
□	VMware- Data center added or deleted	Jun 26 07:39:15 PM	Jan 01 05:30:00 AM
□	VMware- Esxi host authentication failures	Jun 26 07:39:15 PM	Jan 01 05:30:00 AM
□	VMware- Esxi host login and logout	Jun 26 07:39:15 PM	Jan 01 05:30:00 AM
□	VMware- Policy and permission changes	Jun 26 07:39:15 PM	Jan 01 05:30:00 AM
□	VMware- Esxi host added or removed	Jun 26 07:39:15 PM	Jan 01 05:30:00 AM
□	VMware- vCenter auth failures	Jun 26 07:39:15 PM	Jan 01 05:30:00 AM
□	VMware- vCenter login and logout	Jun 26 07:39:15 PM	Jan 01 05:30:00 AM
□	VMware- Virtual machine connected and disconnected	Jun 26 07:39:15 PM	Jan 01 05:30:00 AM
□	VMware- vCenter Firewall configuration changes	Jun 26 07:39:15 PM	Jan 01 05:30:00 AM
□	VMware- Virtual machine created or removed	Jun 26 07:39:15 PM	Jan 01 05:30:00 AM

Figure 56

Dashboards

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



My Dashboard

VMware | Symantec ... | WatchGuard | Cyberoam | Cisco ASA | Soph

VMware Esxi host authentication failures by ...

Jul 02 11:40 AM - Jul 02 02:41 PM

Figure 57

Sample Flex Dashboards

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

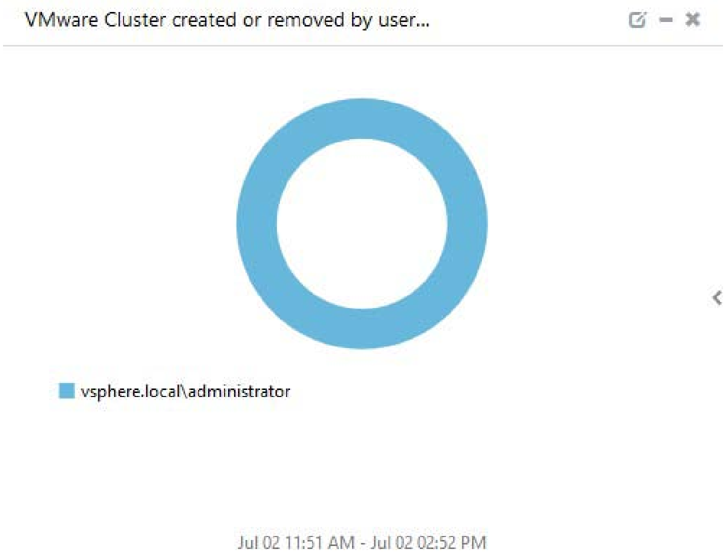

VMware Cluster created or removed by user...
vsphere.local\administrator
Jul 02 11:51 AM - Jul 02 02:52 PM

Figure 58

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

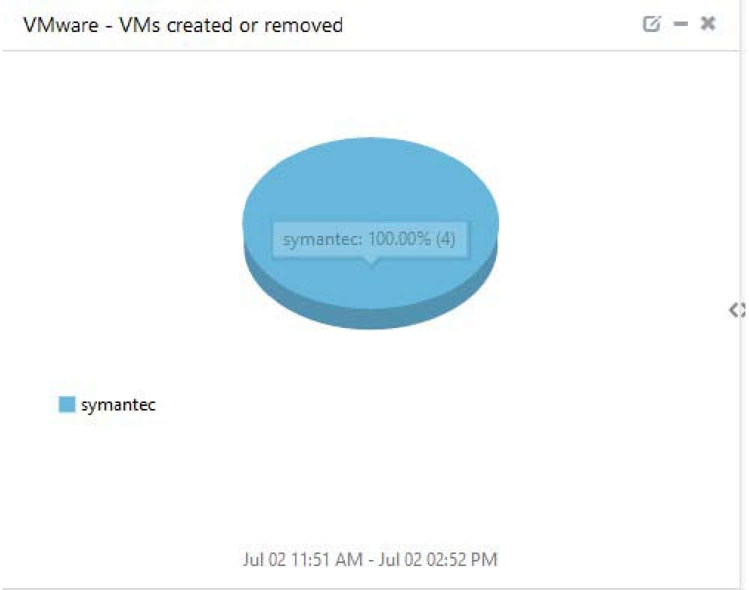

VMware - VMs created or removed
symantec: 100.00% (4)
symantec
Jul 02 11:51 AM - Jul 02 02:52 PM

Figure 59

VMware - VMware ESXi login logout details by source IP address: This dashboard provides information related to ESXi login logout details.

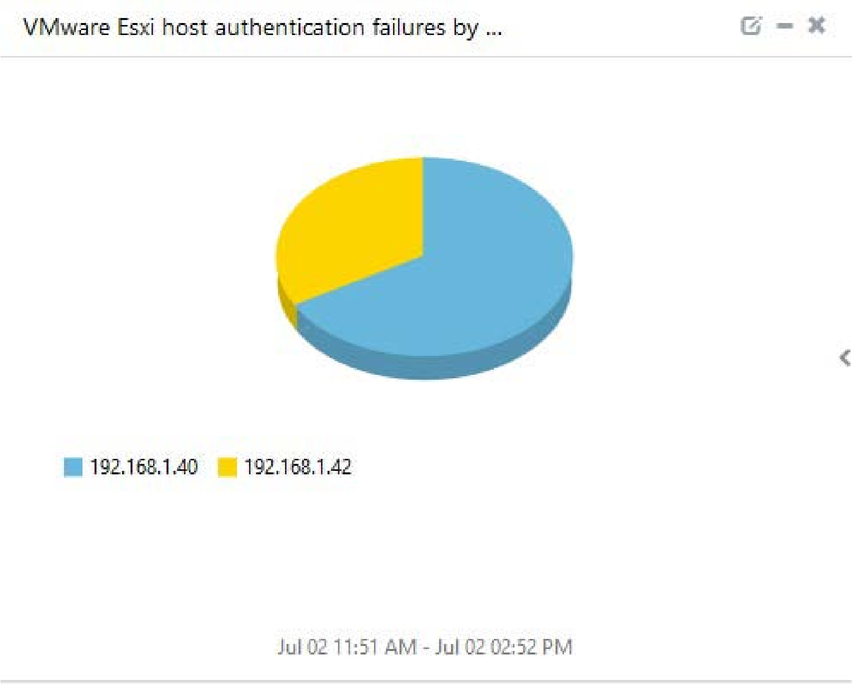

VMware Esxi host authentication failures by ...
🟦 192.168.1.40
🟨 192.168.1.42
Jul 02 11:51 AM - Jul 02 02:52 PM

Figure 60

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

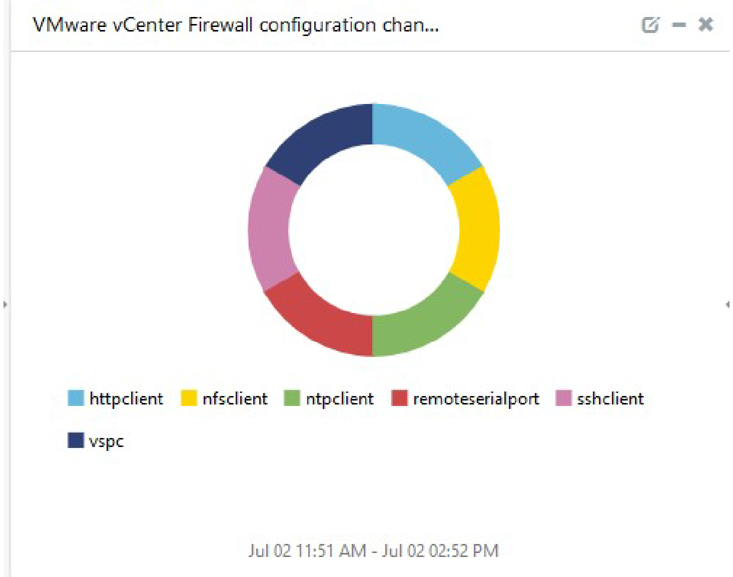
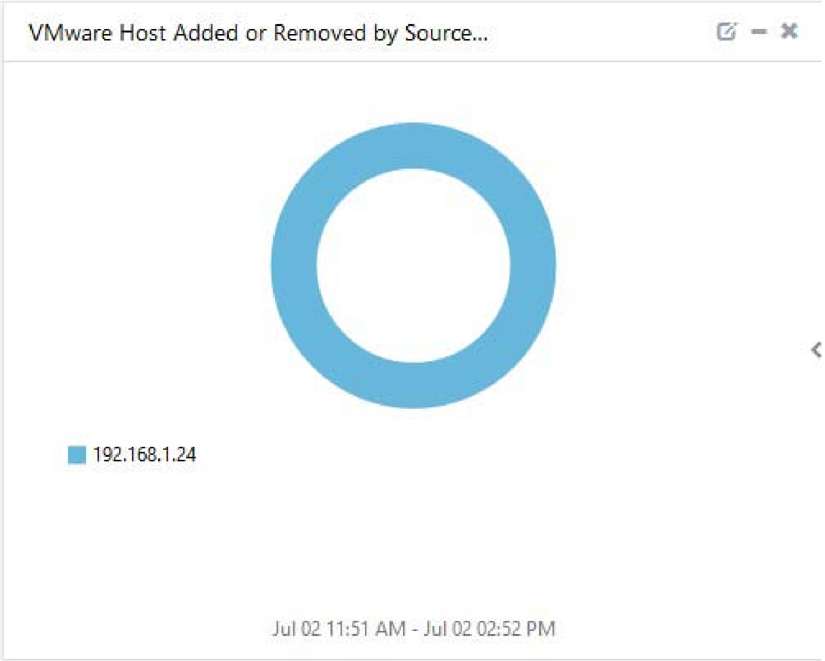

VMware vCenter Firewall configuration chan...
🟦 httpclient
🟨 nfsclient
🟩 ntpclient
🟥 remoteserialport
🟪 sshclient
🟦 vspc
Jul 02 11:51 AM - Jul 02 02:52 PM

Figure 61

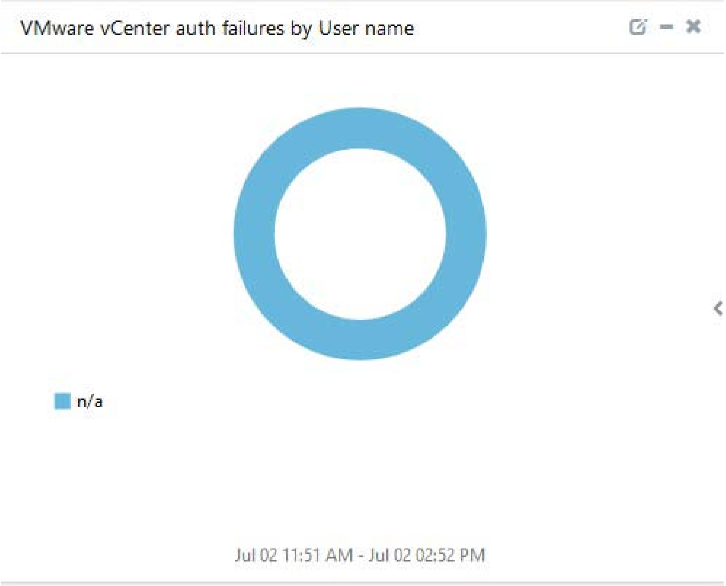
VMware - Host Added or Removed by source IP address: This dashboard provides information related hosts added o removed.



VMware Host Added or Removed by Source...

Figure 62

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



VMware vCenter auth failures by User name

Figure 63

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

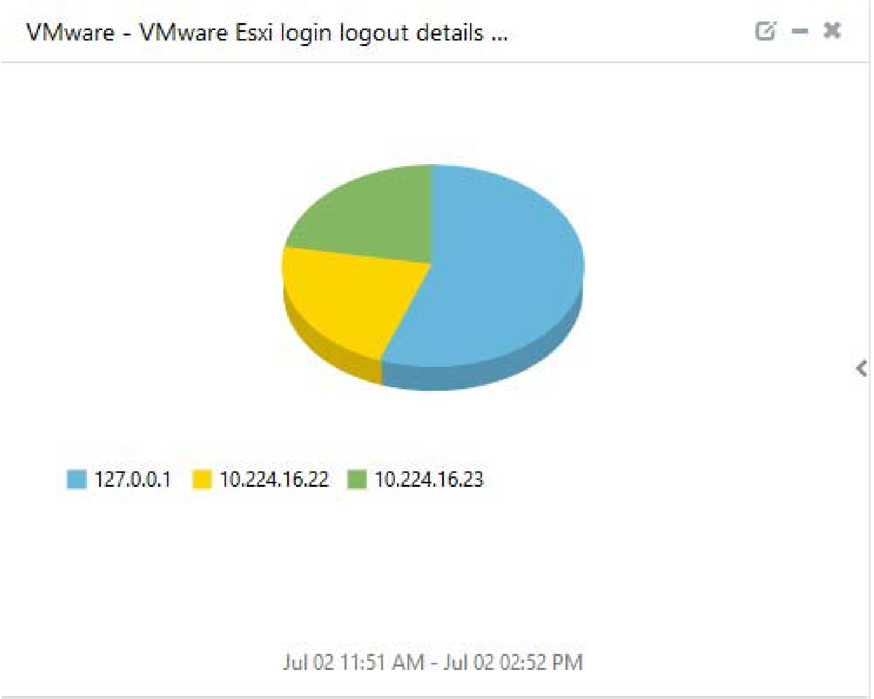

VMware - VMware Esxi login logout details ...
🟦 127.0.0.1
🟨 10.224.16.22
🟩 10.224.16.23
Jul 02 11:51 AM - Jul 02 02:52 PM

Figure 64