Netsurion | EventTracker®

Integrate VMware Horizon7 with EventTracker

EventTracker v9.2 and above

Publication Date: September 9, 2020

Abstract

This guide will facilitate a VMware Horizon7 user to send logs to EventTracker.

Scope

The configuration details in this guide are consistent with EventTracker 9.2 or later and VMware Horizon7.

Audience

Administrators who want to monitor the VMware Horizon7 using EventTracker.

Table of Contents

1. Introduction

VMware Horizon7 provides virtual desktop and app capabilities to users utilizing **VMware's** virtualization technology.

VMware Horizon7 logs can be configured and forwarded to EventTracker by using syslog. It helps you to monitor the authentication failed for user accounts, and user passwords, user login success, user logout, security server logs, VCenter logs, folders management logs, administrative activities based on user authentication, username, and login activities.

EventTracker alerts you when any folder is removed, permission is removed, authentication fails, security server is removed, agent shutdown, etc.

EventTracker can also generate a schedule report for user login activities, agent activities, desktop task cancelation details, device management, security server activities happening in VMware Horizon7. It displays agent activities, user login success, authentication failed, removed VCenter server, unauthorized user, etc.

1.1 Pre-requisites

- Administrator privilege for VMware Horizon View Administrator.
- Port number 514 should open if any firewall exists between VMware Horizon7 and EventTracker.

1.2 Integration of VMware Horizon7 events to EventTracker

Before you configure the VMware Horizon View Administrator integration, you must have the IP Address of the EventTracker.

To configure VMware View Administrator to send log data to EventTracker

1. In the View Administrator, select View **Configuration > Event Configuration**.

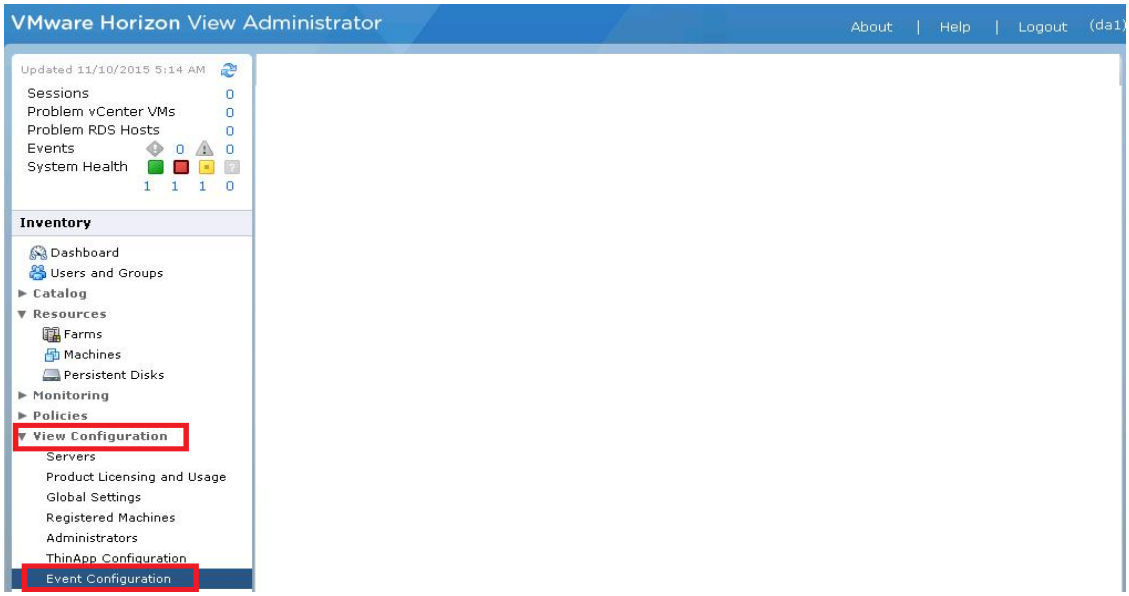

Figure 1

2. In the **Syslog area**, click **Add** (next to Send to Syslog servers), and specify the **EventTracker IP address** and the port number **514**. This step lets you configure the **View Connection Server** to send events to an EventTracker.

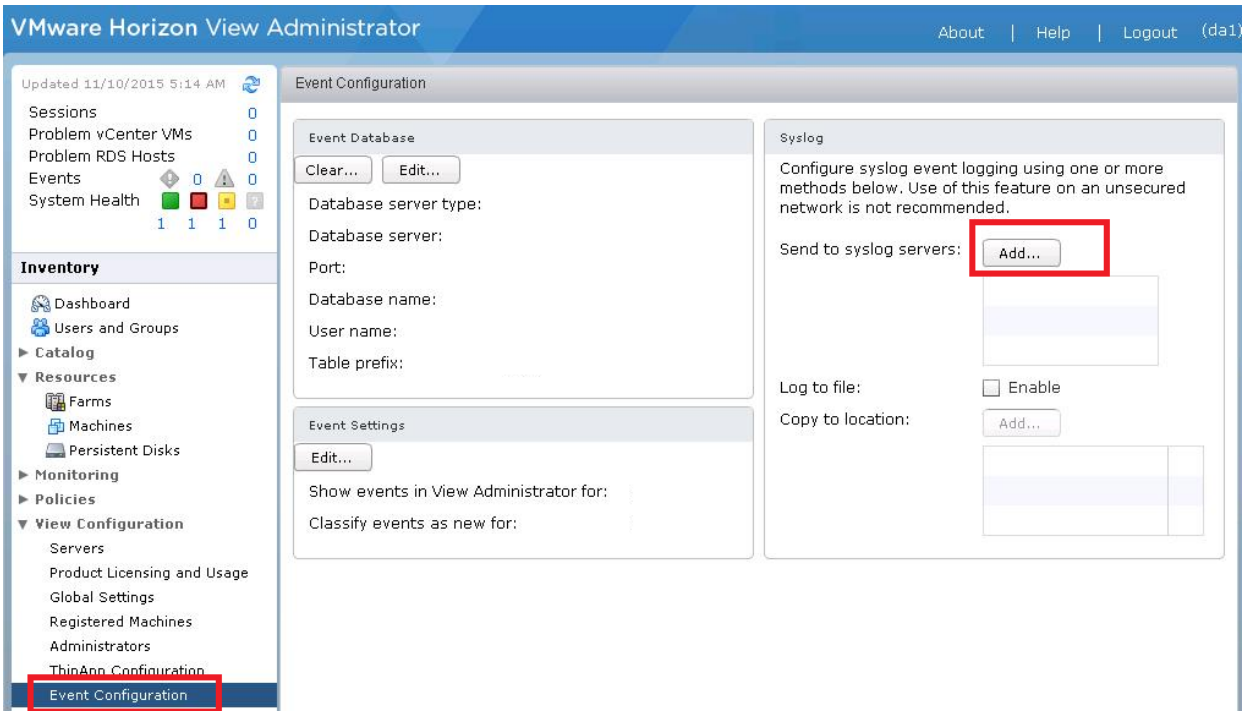

Figure 2

2. EventTracker Knowledge Pack

Once VMware Horizon7 events are received in EventTracker alerts, and reports can be configured in EventTracker.

The following knowledge packs are available in EventTracker to support VMware Horizon7 monitoring.

2.1 Categories

VMware Horizon7: Administrative activities – This category provides information related to admin activities like user-added, user removed, etc.

VMware Horizon7: Agent activities – This category provides information related to agent activities like agent started, agent stopped, agent offline, agent connected, agent disconnected, agent configured, agent pending, agent pending expired, and agent shutdown.

VMware Horizon7: Application activities – This category provides information related application activities like application added, application removed from desktop, application edited, etc.

VMware Horizon7: Authentication failed for password – This category provides information related to password expired, password incorrect, and pairing password not set, etc.

VMware Horizon7: Authentication failed for secure ID – This category provides information related to authentication failed for secure ID access denied, secure ID new pin rejected, secure ID wrong new pin entered, etc.

VMware Horizon7: Authentication failed for user account – This Category provides information related to authentication failed for user account disabled, the account is expired, account restriction, etc.

VMware Horizon7: Database activities – This category provides information related to database configuration added, deleted, and updated.

VMware Horizon7: Device management – This category provides information related to desktop assigned to the pool, desktop unassigned to the pool, etc.

VMware Horizon7: File management activities – This category provides information related to folder added, folder changed, folder updated, folder removed, etc.

VMware Horizon7: Policy management – This category provides information related to pool policy updated for desktops.

VMware Horizon7: Security server activities – This category provides information related to security server added, updated, and removed.

VMware Horizon7: User login success – This category provides information related to user login success for view administrator console.

VMware Horizon7: User logout – This category provides information related to user logout from view administrator console.

VMware Horizon7: VCenter management – This category provides information related to VCenter at address enabled, down, invalid credentials, etc.

2.2 Alerts

VMware Horizon7: Agent shutdown or offline – This alert is triggered when the agent is not responding and it's offline or shutdown.

VMware Horizon7: Authentication failed for user account – This alert is triggered when the user account disabled, the user account expired, and the user account restricted tries to authenticate but it fails.

VMware Horizon7: Authentication failed for user secure ID – This alert is triggered when the user secure ID expired, secure ID entered wrongly but it fails.

VMware Horizon7: Permission has been removed – This alert is triggered when the user's permission is removed.

VMware Horizon7: Role has been removed – This alert is triggered when the user role is removed.

VMware Horizon7: Security server has been removed – This alert is triggered when the security server is removed.

VMware Horizon7: User password authentication failed – This alert is triggered when the user password entered wrongly, and expired user password entered.

VMware Horizon7: VCenter Server removed – This alert is triggered when the VCenter server is removed.

VMware Horizon7: User is not authorized to perform operation – This alert is triggered when the user authenticated but not authorized to perform any operation.

VMware Horizon7: Endpoint deleted – This alert is triggered when the endpoint has been deleted.

2.3 Report

VMware Horizon7 - User login and logout – This report provides information related to user successfully login and logout. It provides details like username, user session ID, client IP address, forward client IP address, and message.

Log Considered

```
Aug 28 14:07:24 DC2A-HorznCon02 1 2020-08-28T14:07:23.025-04:00 DC2A-Horzn02.caa.domain.local View - 73
[View@6876 Severity="AUDIT_SUCCESS" Module="Broker" EventType="BROKER_USERLOGGEDIN" UserSID="S-1-5-21-
1498259142-3634561516-3640805228-1741" UserDisplayName="gary"
BrokerSessionId="50859822_8fc1_405b_a85f_a1d39fcbd3e7" ClientIpAddress="172.17.250.15"
ForwardedClientIpAddress="192.168.249.23, 172.17.250.15"] User gary has logged in
Aug 28 14:01:30 DC2A-HorznCon02 1 2020-08-28T14:01:29.045-04:00 DC2A-Hn02.can.domain.local View - 74
[View@6876 Severity="AUDIT_SUCCESS" Module="Broker" EventType="BROKER_USERLOGGEDOUT" UserSID="S-1-5-
21-1498259142-3634561516-3640805228-1741" UserDisplayName="maxx"
BrokerSessionId="19422dfa_8f95_42a2_8df3_271cc847a2d0"] User maxx has logged out
```

Sample_Report

LogTime	Computer	User Name	User SID	Broker Session ID	Client IP Address	Forwarded Client IP Address	Message
08/31/2020 04:08:52 PM	R1S5-VM30\VMWARE_HORIZON7-SYSLOG	kenneth	S-1-5-21-1016830772-765521188-868963166-2171	cd0e0d4c_29f0_4ef4_929e_b639b6fd9d82	172.16.250.38	192.168.250.8, 172.16.250.233, 172.16.250.38	User kenneth has logged in
08/31/2020 04:08:52 PM	R1S5-VM30\VMWARE_HORIZON7-SYSLOG	maya	S-1-5-21-4136356191-1247230178-2405973841-14612	5536c652_0917_4f8a_a9c8_d6d40688ac4d	172.16.250.38	192.168.250.8, 172.16.250.233, 172.16.250.38	User maya has logged in
08/31/2020 04:08:52 PM	R1S5-VM30\VMWARE_HORIZON7-SYSLOG	joeb	S-1-5-21-1016830772-765521188-868963166-4048	52ec8330_19bf_4fa0_96cd_5bc92b16315a			User joeb has logged out

Figure 3

VMware Horizon7 - Agent activities – This report provides information related to agent activities like agent connected, disconnected, offline, shutdown, etc. It provides details of machine name, username, session length, pool ID, and message.

Log Considered

```
Aug 28 14:05:43 DC1A-HorznCon01 1 2020-08-28T14:05:43.114-04:00 ap-vmr-x104.ew.domain.local View - 1008
[View@6876 Severity="INFO" Module="Agent" EventType="AGENT_ENDED" UserSID="S-1-5-21-4136356191-
1247230178-2405973841-1900" UserDisplayName="kenneth" DesktopId="NP-NMR-A" DesktopDisplayName="NP NMR
A" PoolId="np-nmr-a" MachineId="cac59f47-02e5-46c7-be25-e00ee4c694e2" MachineName="ap-vmr-x104"
MachineDnsName="ap-vmr-x104.ew.domain.local" CurrentSessionLength="3432" TotalLoginLength="-22530"
SessionType="DESKTOP"] User kenneth has logged off machine ap-vmr-x104
```

Sample_Report

LogTime	Computer	User Name	User SID	Name	Machine ID	Name	Session	Length	Display	Pool ID	Agent Status	Message
08/31/2020 04:08:52 PM	WKSTSVMH54\VMWARE_HORIZON7-SYSLOG	maxx	S-1-5-21-1498259142-3634561516-3640805228-8912	GNMO70033	304b9057-44ad-45c1-93f2-5208687b238d	canm70033.canada.domain.local			Canada-Main-Win7	canada-main-win7	AGENT_CONNECTED	User maxx has logged in to a new session on machine GNMO70033
08/31/2020 04:08:52 PM	WKSTSVMH54\VMWARE_HORIZON7-SYSLOG	david	S-1-5-21-1498259142-3634561516-3640805228-1682	GNMO70170	52a49ea7-a389-4d00-b1af-534577483 0f5	gnmo70170.canada.domain.local	-87214	-87214	Canada-Main-Win7	canada-main-win7	AGENT_ENDED	User david has logged in to a new session on machine GNMO70170

Figure 4

VMware Horizon7 - Desktop request detail – This report provides information related to user-requested for desktop, username, desktop name, and message.

Log Considered

```
Aug 28 14:08:40 DC1A-HorznCon02 1 2020-08-28T14:08:40.630-04:00 DC1A-HorznCon02.domain.local View - 81 [View@6876 Severity="INFO" Module="Broker" EventType="BROKER_DESKTOP_REQUEST" UserSID="S-1-5-21-1016830772-765521188-868963166-1916" UserDisplayName="maya" DesktopId="k-dys-x7-z" DesktopDisplayName="ECS Windows 7" SessionType="DESKTOP"] User maya requested Pool k-dys-x7-z
```

Sample_report

LogTime	Computer	User Name	User SID	Desktop Display Name	Message
08/31/2020 04:08:52 PM	WKSTSVMH67\VMWARE_HORIZON7-SYSLOG	kenneth	S-1-5-21-2586729455-2912892779-2859760340-50574	Remote Contractors A	User kenneth requested Pool remotecontractorsa
08/31/2020 04:08:52 PM	WKSTSVMH67\VMWARE_HORIZON7-SYSLOG	maya	S-1-5-21-1498259142-3634561516-3640805228-1767	WKS-Mini-Win7	User maya requested Pool canada-main-win7

Figure 5

VMware Horizon7 - Desktop management – This report provides information related to desktop allocated to the pool, desktop allocated to the user, username, pool name, desktop name, and message.

Log_Considered

```
Aug 28 14:11:30 DC2A-HorznCon02 1 2020-08-28T14:11:19.230-04:00 DC2A-HorznCon02.canada.domain.local View - 104 [View@6876 Severity="INFO" Module="Broker" EventType="BROKER_MACHINE_ALLOCATED" UserSID="S-1-5-21-1498259142-3634561516-3640805228-1741" UserDisplayName="kenneth" DesktopId="can-min-win7" DesktopDisplayName="Cda-Main-Win7" PoolId="cda-main-win7" MachineId="e3b50b64-ba49-4297-885d-fdf2648c3ca3" MachineName="CANM70130" MachineDnsName="ca0.can.domain.local" SessionType="DESKTOP" ProtocolId="[PCoIP\]"] User CANADA\vanessa.mccomb requested Pool ca-main-win7, allocated machine CNGM130
```

Sample_Report

LogTime	Computer	User Name	User SID	Type of Events	Machine Name	Machine ID	Machine Dns Name	Desktop Display Name
08/31/2020 04:59:38 PM	WKSTSVMH67\VMWARE_HORIZON7-SYSLOG	kenneth	S-1-5-21-4136356191-1247230178-2405973841-13248	BROKER_MACHINE_ALLOCATED	CP-CPR-V062	a442-2b35-461a-ab0b-21d3bc0	np2.ew.domain.local	NP NMR A
08/31/2020 04:59:38 PM	WKSTSVMH67\VMWARE_HORIZON7-SYSLOG	joeb	S-1-5-21-1498259142-3634561516-3640805228-8504	BROKER_MACHINE_OPERATION_DELETED	GNMO70190	467d9-7f87-45d7-9eab-3c90c2f	ca0.canada.domain.local	Canada-Main-Win7

Figure 6

VMware Horizon7 - User authentication failed – This report provides information related to user authentication failed, username, and message.

Log Considered

```
Aug 28 10:53:10 DC1A-HorznCon02 1 2020-08-28T10:53:10.328-04:00 DC1A-HorznCon02.domain.local View - 156 [View@6876 Severity="AUDIT_FAIL" Module="Broker"
```

EventType="BROKER_USER_AUTHFAILED_RADIUS_ACCESS_DENIED" UserDisplayName="kenneth"] RADIUS access denied for user kenneth

Sample_report

LogTime	Computer	User Name	Message
08/31/2020 06:08:43 PM	WKSTSVMH56\VMWARE_HORIZON7-SYSLOG	joeb	RADIUS access denied for user joeb
08/31/2020 06:08:43 PM	WKSTSVMH56\VMWARE_HORIZON7-SYSLOG	kenneth	RADIUS access denied for user kenneth
08/31/2020 06:08:43 PM	WKSTSVMH56\VMWARE_HORIZON7-SYSLOG	gary	RADIUS access denied for user gary

Figure 7

VMware Horizon7 - Endpoint task cancelation detail – This report provides information related to endpoint tasks canceled by the user. It gives details like username, desktop name, and task canceled by reason, etc.

VMware Horizon7 - Unassigned users – This report provides information related to a user not assigned for any pool. It gives details like username, desktop name, and message.

VMware Horizon7 - VCenter activities – This report provides information related to VCenter added, removed, updated, username, VCenter name, and message.

2.4 Dashboards

- **VMware Horizon7 - Agent shutdown by device name**

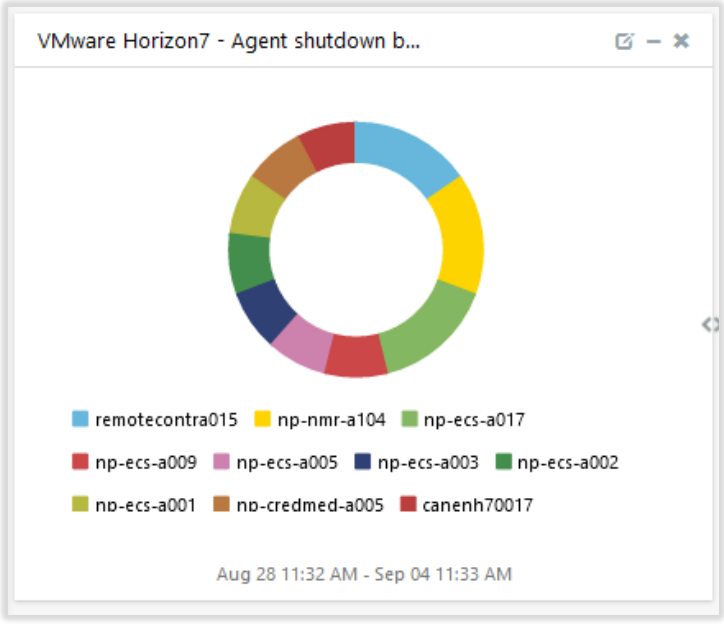

Figure 8

- **VMware Horizon7 - Login success by username**

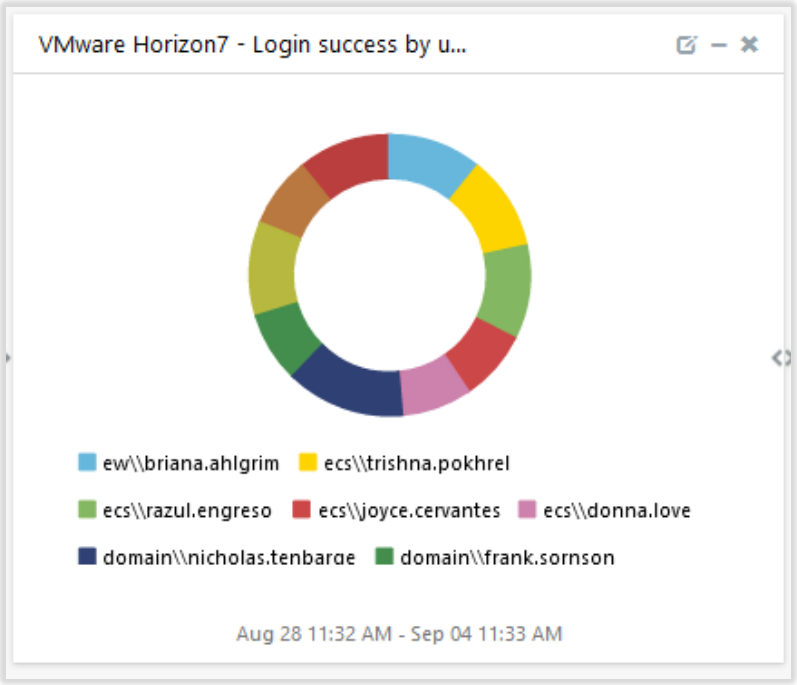

Figure 9

- **VMware Horizon7 - Login success by count**

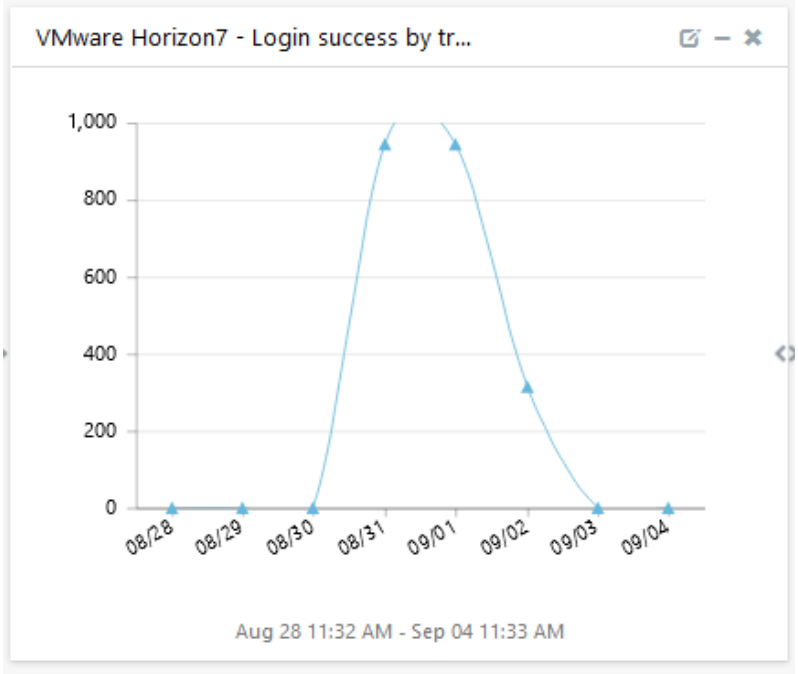

Figure 10

- **VMware Horizon7 - Endpoint management by event type**

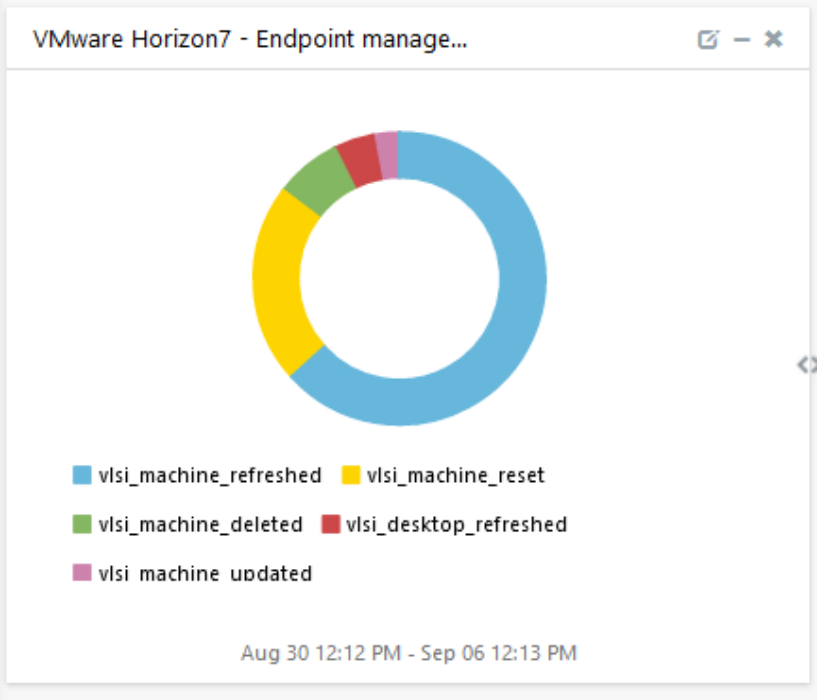

Figure 11

- **VMware Horizon7 - Endpoint deleted by device name**

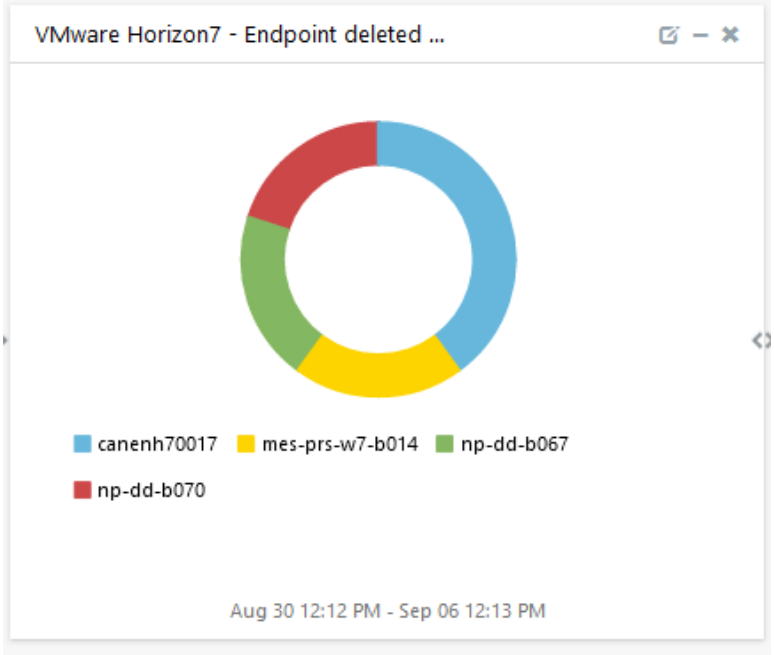

Figure 12

- **VMware Horizon7 - Agent activities by event type**

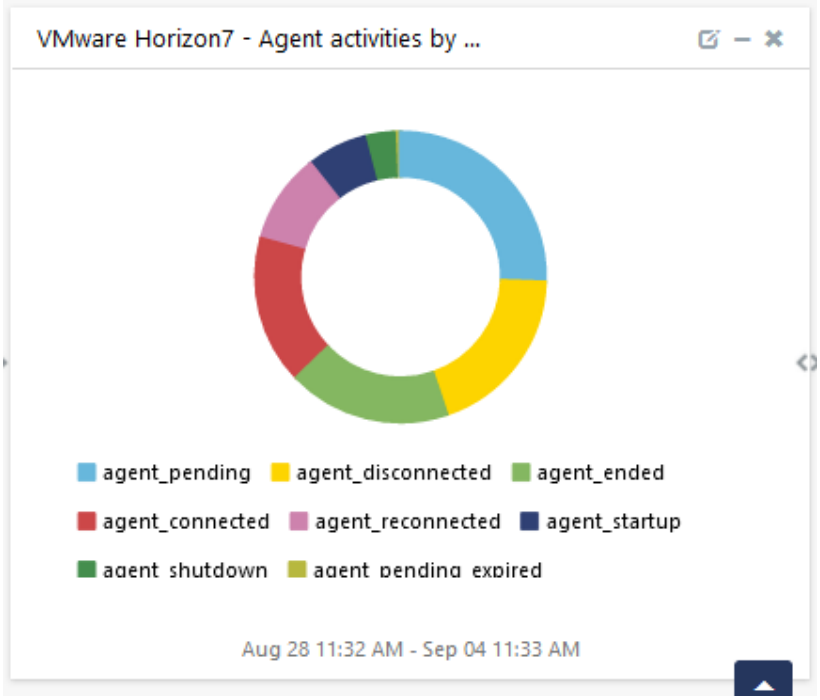

Figure 13

- **VMware Horizon7 - Authentication failed by username**

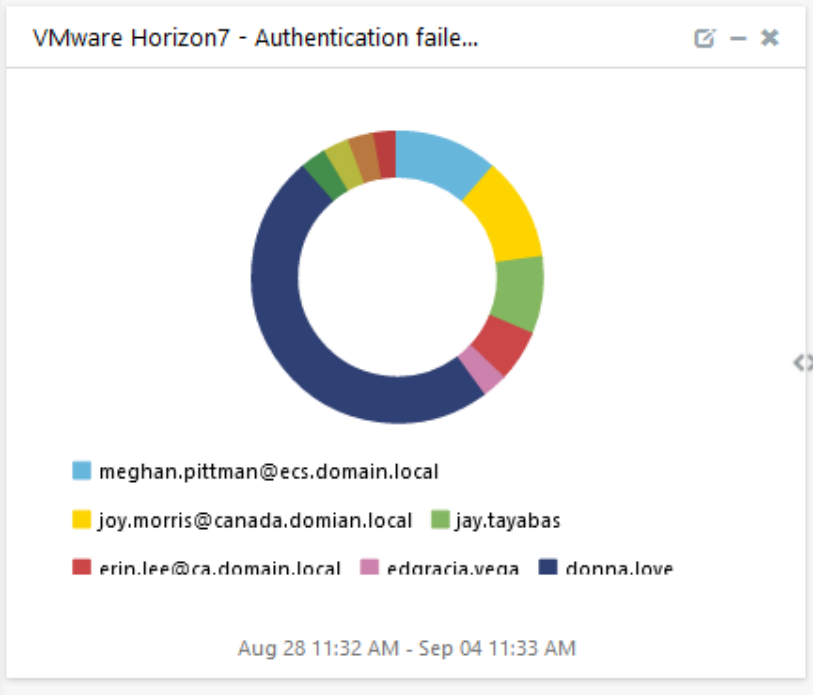

Figure 14

- **VMware Horizon7 - Authentication failure by count**

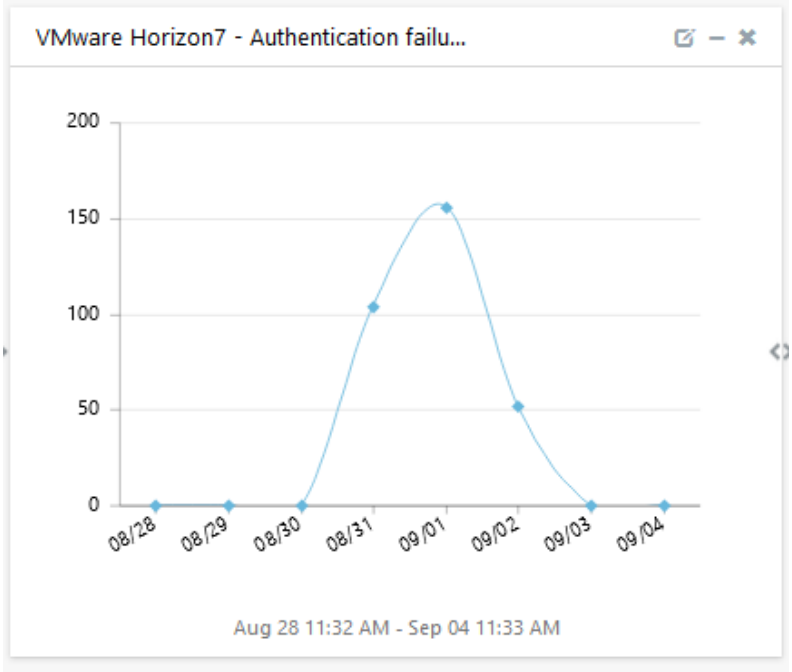

Figure 15

- **VMware Horizon7 - User not assigned for any pool**

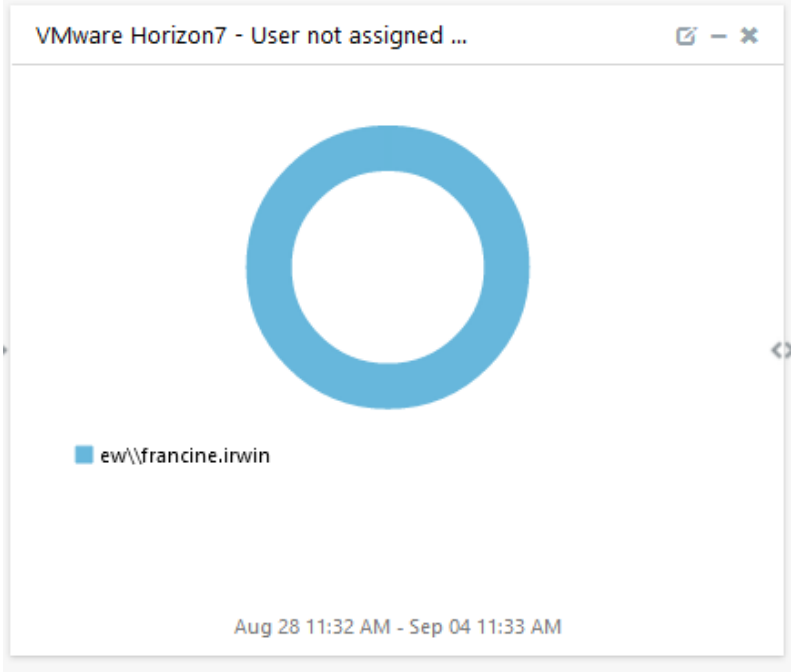

Figure 16

- **VMware Horizon7 - Task canceled by username**

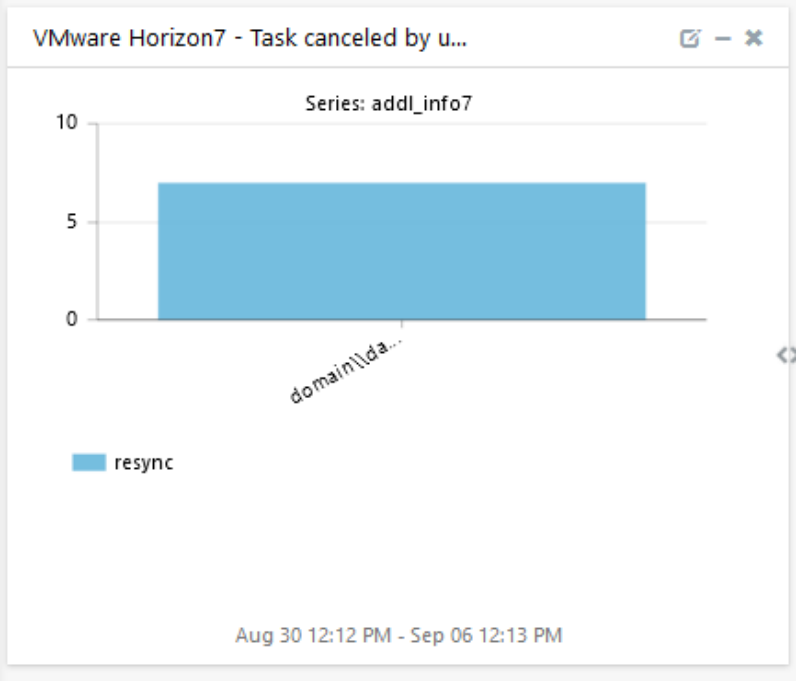

Figure 17

3. Importing knowledge pack into EventTracker

NOTE: Import knowledge pack items in the following sequence:

- Categories
- Alerts
- Flex Reports
- Knowledge Objects
- Dashboards

1. Launch the **EventTracker Control Panel**.
2. Double click **Export-Import Utility**.

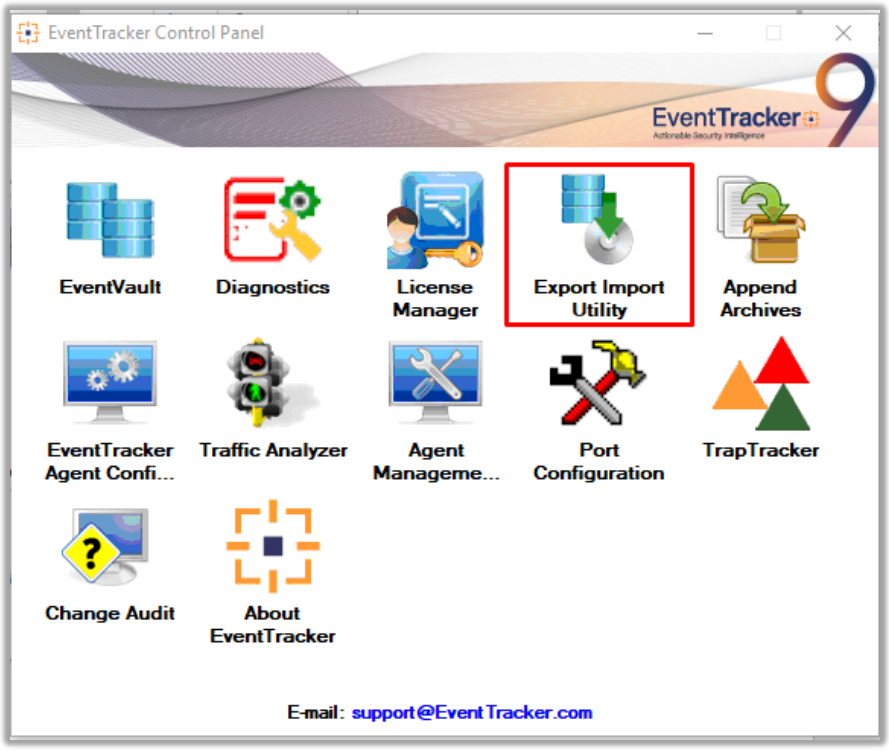

Figure 18

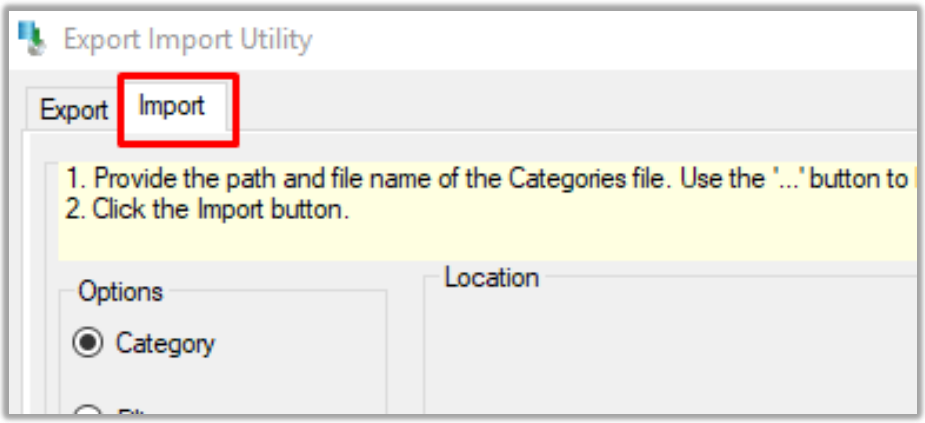

Figure 19

3. Click the **Import** tab.

3.1 Categories

1. Once you have opened "**Export-Import Utility**" via "**EventTracker Control Panel**", click the **Category** option, and then click the browse ... button.
2. Navigate to the knowledge pack folder and select the file with the extension **".iscat", like "Categories_VMware Horizon7. iscat"** and then click on the "**Import**" button.

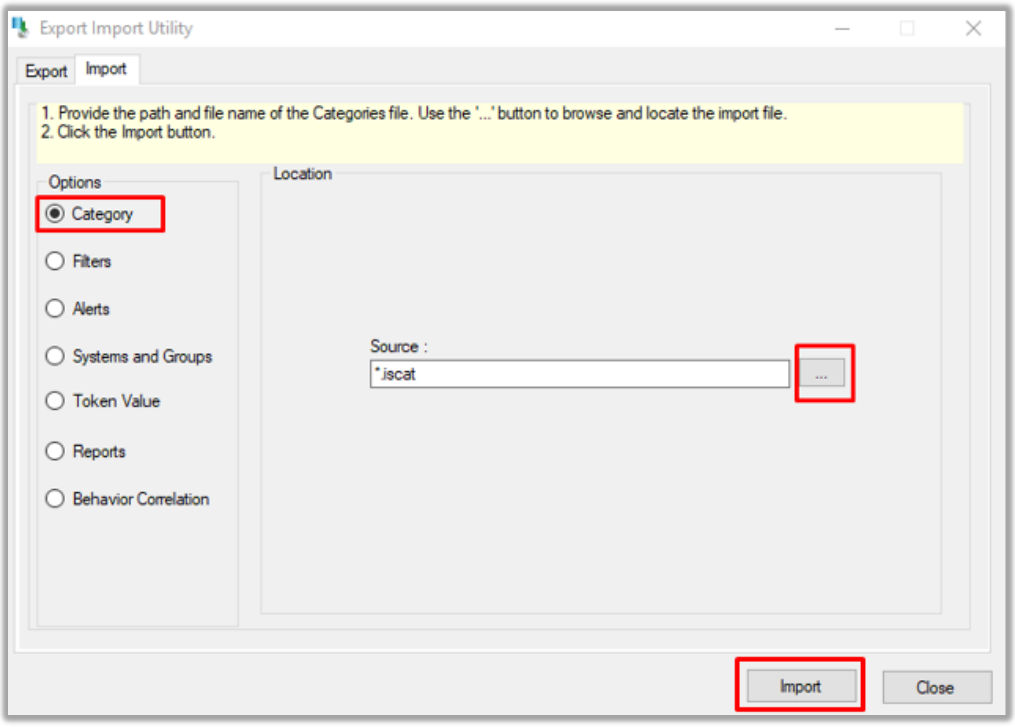

Figure 20

EventTracker displays a success message:

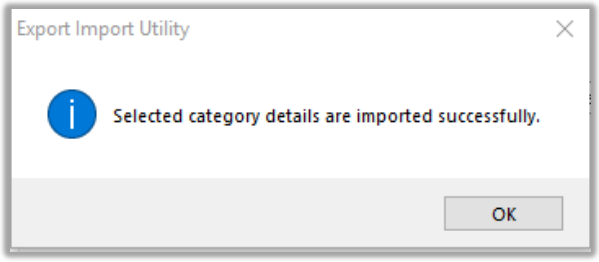

Figure 21

3.2 Alerts

1. Once you have opened "**Export-Import Utility**" via "**EventTracker Control Panel**", click **Alert** option, and then click the browse ... button.
2. Navigate to the knowledge pack folder and select the file with the extension **".isalt"**, **e.g**. "**Alerts_ VMware Horizon7.isalt**" and then click on the "**Import**" button.

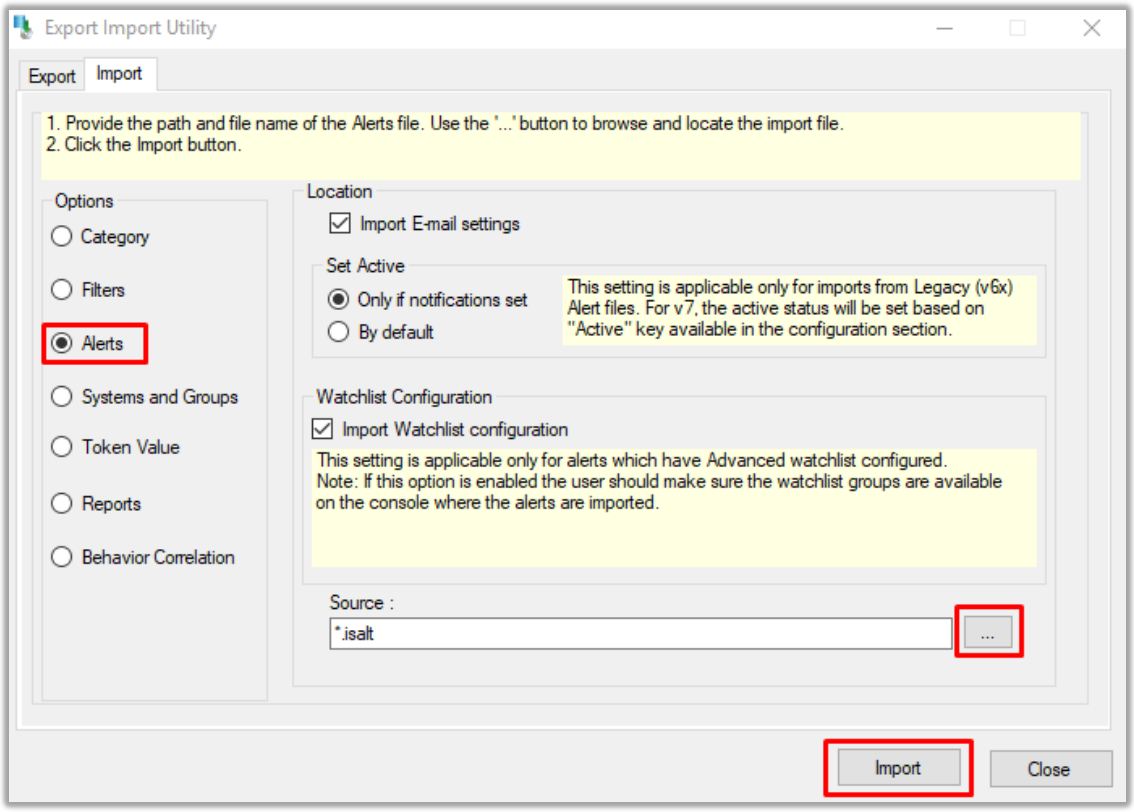

Figure 22

EventTracker displays a success message.

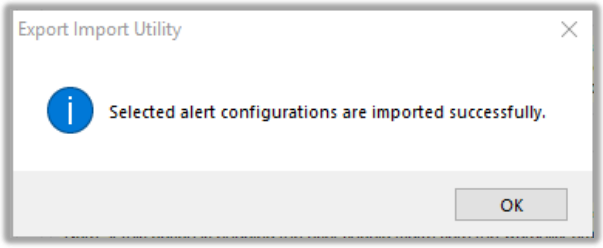

Figure 23

3.3 Flex Reports

1. In the EventTracker control panel, select "**Export/ Import utility**" and select the "**Import tab**". Then, click the **Reports** option, and choose "**New (*.etcrx)**".

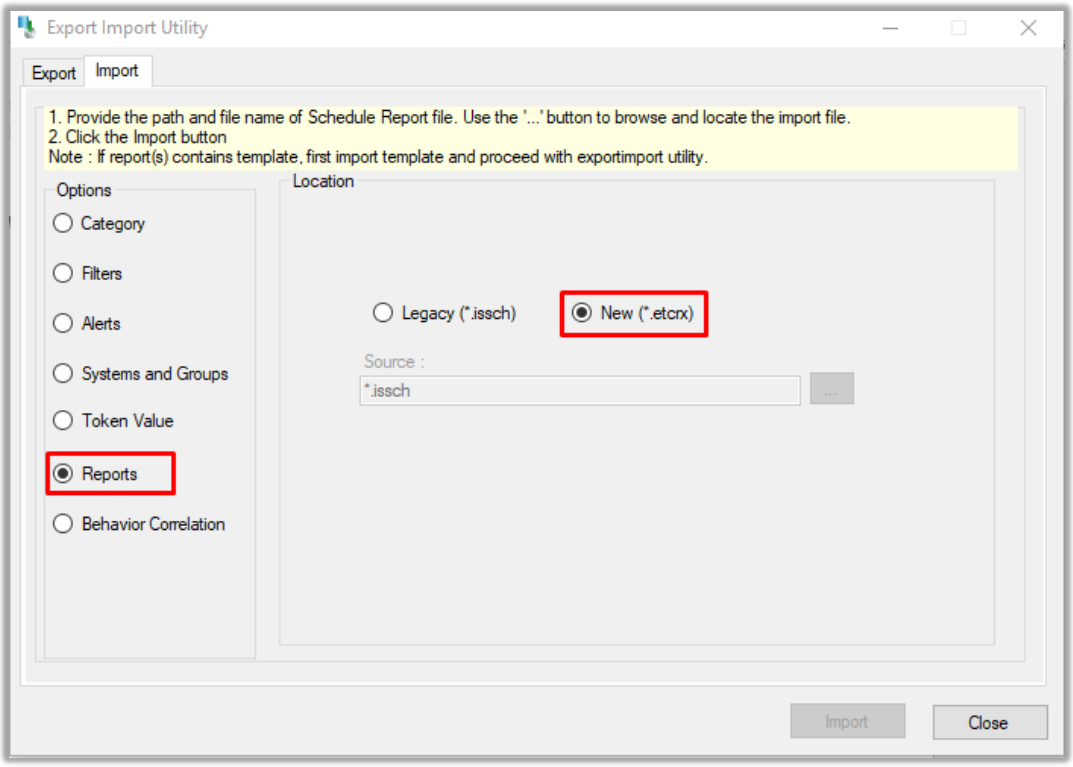

Figure 24

2. Once you have selected "**New (*.etcrx)**", a new pop-up window will appear. Click the "**Select File**" button and navigate to the knowledge pack folder and select file with the extension **".etcrx", e.g. "Reports_VMware Horizon7.etcrx".**

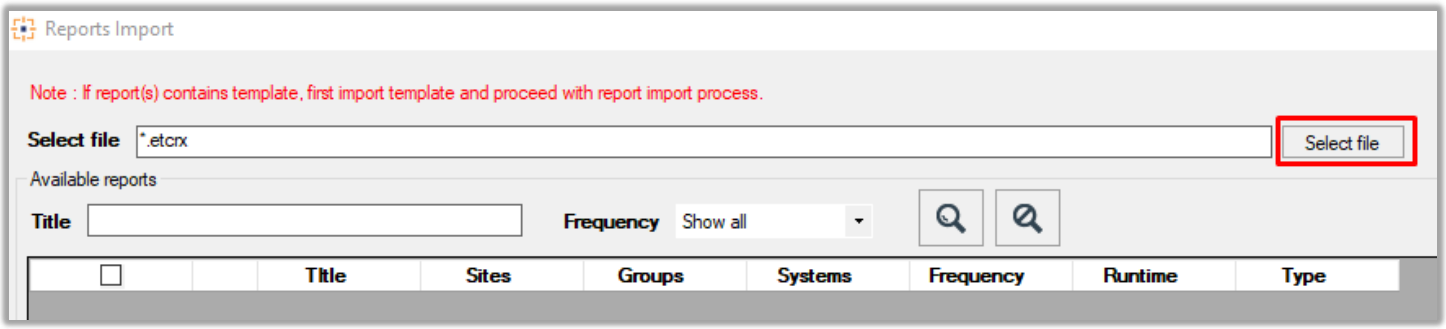

Figure 25

3. Wait while reports are being populated in the below tables. Now, select all the relevant reports and then click the **Import** button.

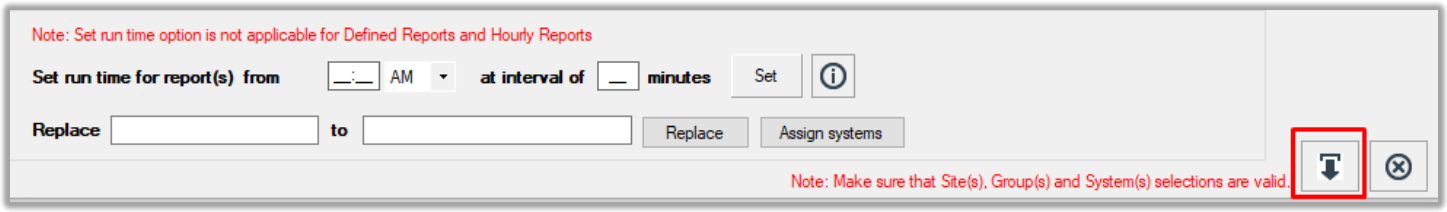

Figure 26

EventTracker displays a success message.

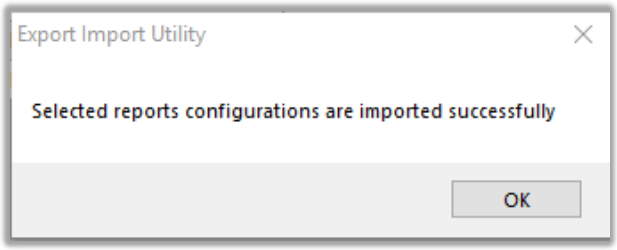

Figure 27

3.4 Knowledge Objects

1. Click **Knowledge objects** under the **Admin** option in the EventTracker web interface.

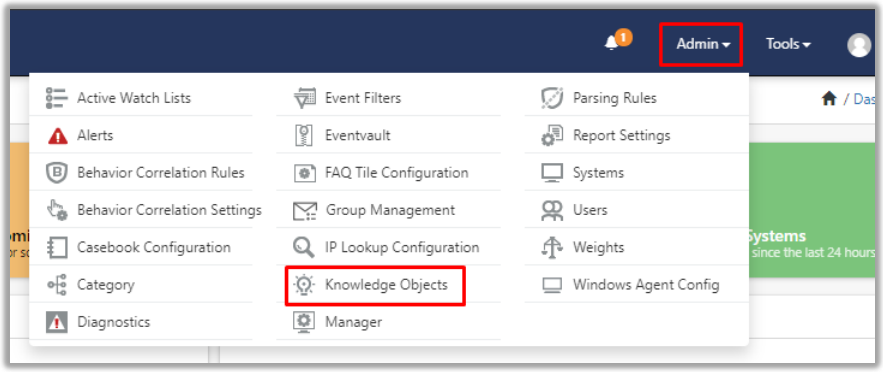

Figure 28

2. Next, click the **"import object"** icon.

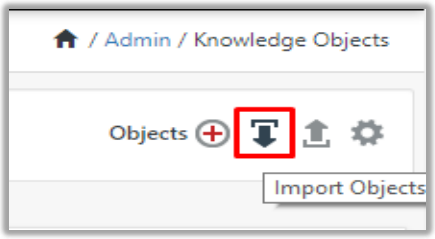

Figure 29

3. A pop-up box will appear, click "**Browse**" in that and navigate to the knowledge packs folder (type "**C:\Program Files (x86)\Prism Microsystems\EventTracker\Knowledge Packs**" in the navigation bar) with the extension **".etko", e.g. "KO_VMware Horizon7.etko"** and then click the "**Upload**" button.

Figure 30

4. Wait while EventTracker populates all the relevant knowledge objects. Once the objects are displayed, select the required ones and click on the "**Import**" button.

Figure 31

3.5 Dashboards

1. Login to the **EventTracker web interface**.
2. Navigate to **Dashboard → My Dashboard**.
3. In "My Dashboard", Click **Import Button**.

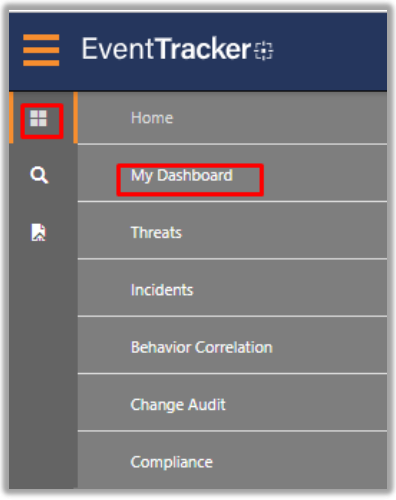

Figure 32

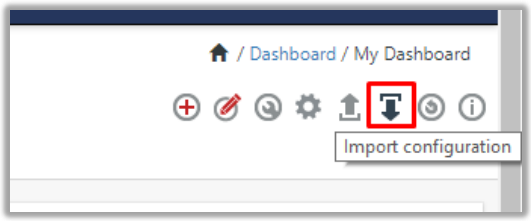

Figure 33

4. Select the **Browse** button and navigate to the knowledge pack folder (type **"C:\Program Files (x86)\Prism Microsystems\EventTracker\Knowledge Packs"** in the navigation bar) where "**.etwd**", **e.g.** "**Dashboard_VMware Horizon7.etwd**" is saved and click on "**Upload**" button.

5. Wait while EventTracker populates all the available dashboards. Now, choose "**Select All**" and click on **"Import"** Button.

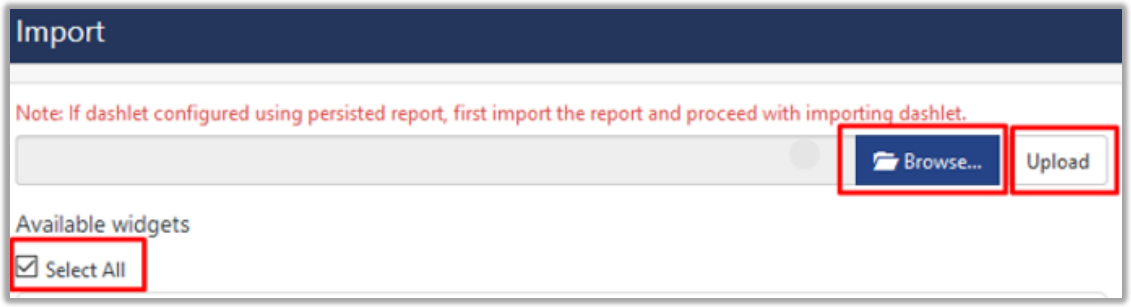

Figure 34

Figure 34

4. Verifying knowledge pack in EventTracker

4.1 Categories

1. Login to the **EventTracker web interface**.
2. Click **Admin** dropdown, and then click **Categories**.
3. In **Category Tree** to view imported categories, please click on "**Search**" and search with the **"VMware Horizon7".** You will see the below results.

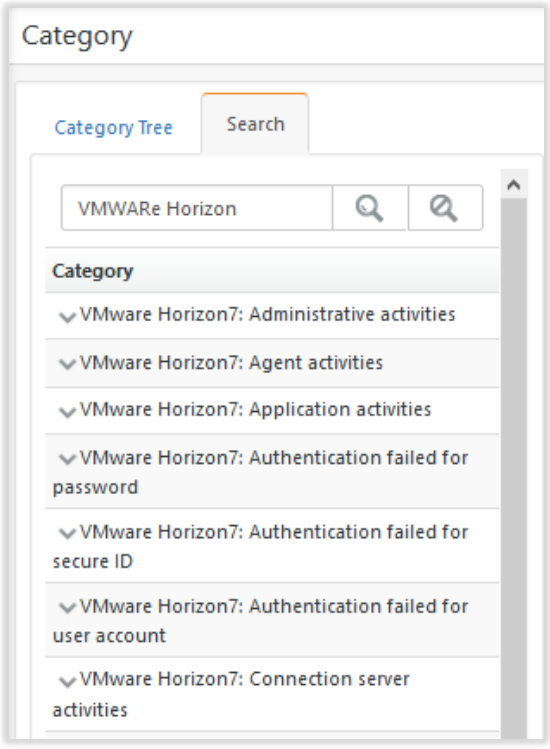

Figure 36

4.2 Alerts

1. In the **EventTracker** web interface, click the **Admin** dropdown, and then click **Alerts.**
2. In search box enter **"VMware Horizon7"** and then click the **Search** button.
   EventTracker displays an alert related to VMware Horizon7.

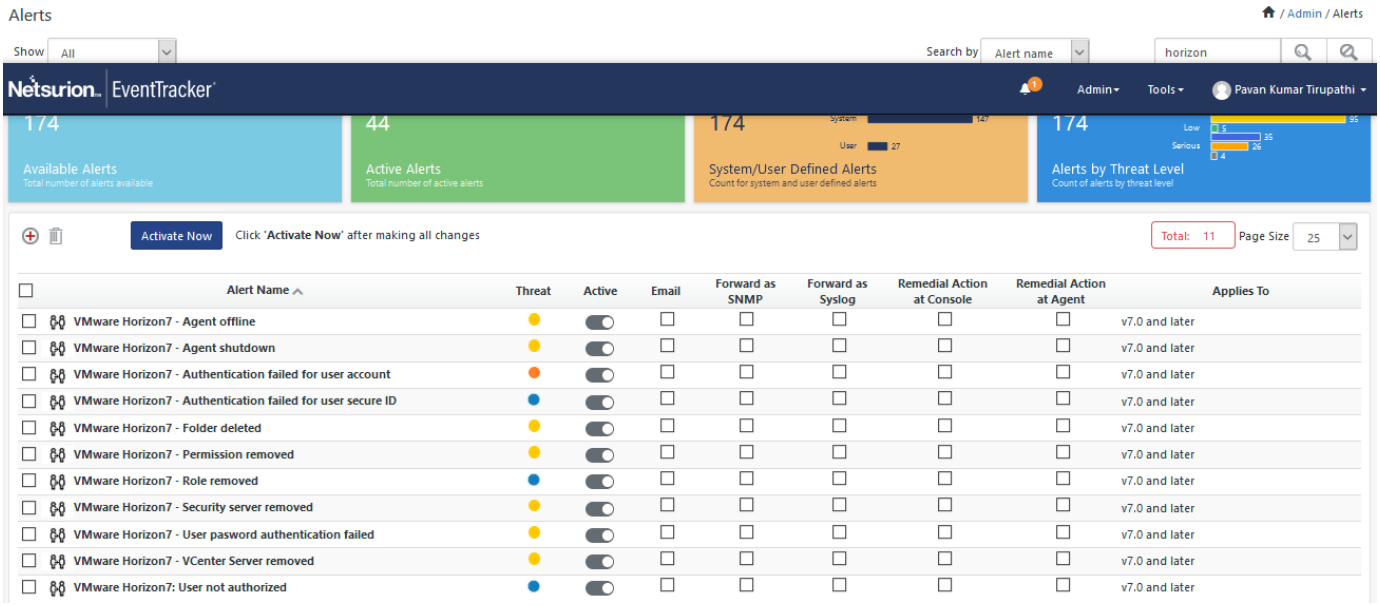

Figure 37

4.3 Flex Reports

1. In the **EventTracker** web interface, click the **Reports** menu, and then select the **Report Configuration**.

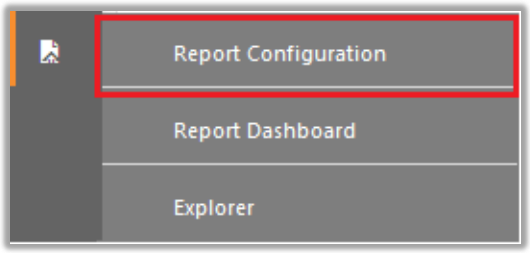

Figure 38

2. In **Reports Configuration** pane, select the **Defined** option.
3. Click on the **"VMware Horizon7"** group folder to view the imported reports.

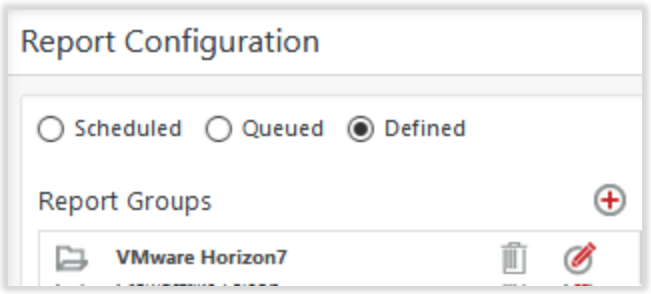

Figure 39

4.4 Knowledge Objects

1. In the **EventTracker** web interface, click the **Admin** dropdown, and then click **Knowledge Objects.**
2. In the **Knowledge Object** tree, expand the **"VMware Horizon7"** group folder to view the imported Knowledge objects.

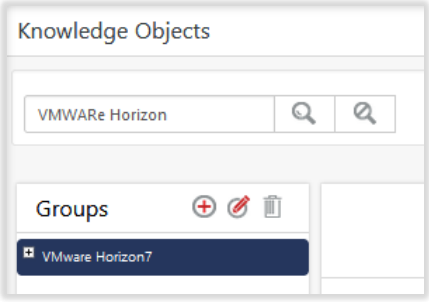

Figure 40

4.5 Dashboards

1. In the EventTracker web interface, Click on Home Button and select "**My Dashboard**".

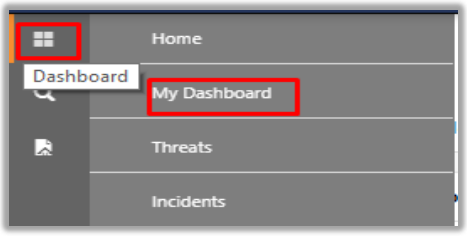

Figure 41

2. In the "**VMware Horizon7"** dashboard you should be now able to see something like this.

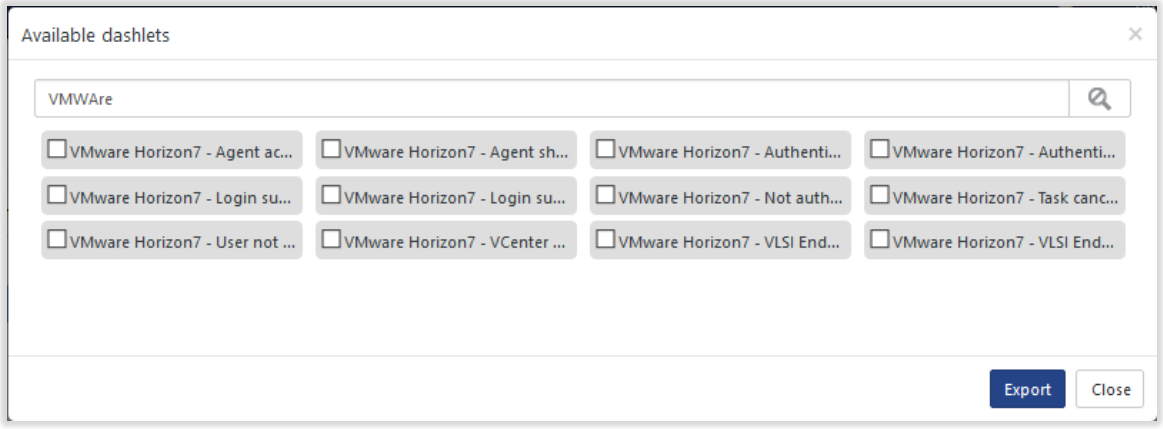

Figure 42