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.

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

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

Netsurion 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 Netsurion, 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.

© 2020 Netsurion. All rights reserved. The names of actual companies and products mentioned herein may be the trademarks of their respective owners.



Table of Contents

1.	Intr	oduction	3
	1.1	Pre-requisites	3
	1.2	Integration of VMware Horizon7 events to EventTracker	3
2.	Eve	ntTracker Knowledge Pack	5
	2.1	Categories	5
	2.2	Alerts	6
	2.3	Report	6
	2.4	Dashboards	9
3.	Imp	oorting knowledge pack into EventTracker	14
	3.1	Categories	15
	3.2	Alerts	16
	3.3	Flex Reports	17
	3.4	Knowledge Objects	19
	3.5	Dashboards	20
4.	Ver	ifying knowledge pack in EventTracker	21
	4.1	Categories	21
	4.2	Alerts	22
	4.3	Flex Reports	23
	4.4	Knowledge Objects	24
	4.5	Dashboards	24



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**.



VMware Horizon View A	dministrator		Abou	t	Help	Lo	gout	(da1
Updated 11/10/2015 5;14 AM Sessions 0 Problem vCenter VMs 0 Problem RDS Hosts 0 Events 0 A 0 System Health 0 1 1 0								
Inventory								
Catalog Users and Groups Catalog Cata								
ThinApp Configuration								
Event Configuration								



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.

VMware Horizon View A	dministrator	About Help	Logout (da1
VMware Horizon View A Updated 11/10/2015 5:14 AM Sessions 0 Problem vCenter VMs 0 Problem RDS Hosts 0 Events 0 Events 0 System Health 0 1 1 1 0 Inventory Sababoard Users and Groups Catalog Resources Farms Machines Persistent Disks Monitoring Policies View Configuration Servers Product Licensing and Usage Global Settings Registered Machines Administrators	Event Configuration Event Configuration Event Database Clear Database server type: Database server: Port: Database name: User name: Table prefix: Event Settings Edit Show events in View Administrator for: Classify events as new for:	About Help Syslog Configure syslog event logging using on methods below. Use of this feature on a network is not recommended. Send to syslog servers: Add Log to file: Enable Copy to location: Add	e or more n unsecured
ThinAnn Configuration Event Configuration			





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-	kenneth	S-1-5-21-1016830772-765521188-	cd0e0d4c_29f0_4ef4_929e_b639	172.16.250.38	192.168.250.8, 172.16.250.233,	User kenneth has logged in
	VM30\VMWARE_HORIZON7-		868963166-2171	b6fd9d82		172.16.250.38	
	SYSLOG						
08/31/2020 04:08:52 PM	R1S5-	maya	S-1-5-21-4136356191-	5536c652_0917_4f8a_a9c8_d6d4	172.16.250.38	192.168.250.8, 172.16.250.233,	User maya has logged in
	VM30\VMWARE_HORIZON7-		1247230178-2405973841-14612	0688ac4d		172.16.250.38	
	SYSLOG						
08/31/2020 04:08:52 PM	R1S5-	joeb	S-1-5-21-1016830772-765521188-	52ec8330_19bf_4fa0_96cd_5bc9			User joeb has logged out
	VM30\VMWARE_HORIZON7-		868963166-4048	2b16315a			
	SYSLOG						

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

1			1	1								1
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	WKSTSVMH5	maxx	S-1-5-21-	GNMO70033	304b9057-	canm70033.ca			Canada-Main-	canada-main-	AGENT_CONNECTED	User maxx
	4\VMWARE_H		1498259142-		44ad-45c1-	nada.domain.l			Win7	win7		has logged in
	ORIZON7-		3634561516-		93f2-	ocal						to a new
	SYSLOG		3640805228-		5208687b238							session on
			8912		d							machine
												GNM070033
08/31/2020 04:08:52 PM	WKSTSVMH5	david	S-1-5-21-	GNM070170	52a49ea7-	gnmo70170.ca	-87214	-87214	Canada-Main-	canada-main-	AGENT_ENDED	User david
	4\VMWARE_H		1498259142-		a389-4d00-	nada.domain.l			Win7	win7		has logged in
	ORIZON7-		3634561516-		b1af-	ocal						to a new
	SYSLOG		3640805228-		5345774830f5							session on
			1682									machine
												GNM070170

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

1	LogTime	Computer	User Name	User SID	Desktop Display Name	Message
1	08/31/2020 04:08:52 PM	WKSTSVMH67\VMWARE_HO	kenneth	S-1-5-21-2586729455-	Remote Contractors A	User kenneth requested Pool
l		RIZON7-SYSLOG		2912892779-2859760340-50574		remotecontractorsa
	08/31/2020 04:08:52 PM	WKSTSVMH67\VMWARE_HO	maya	S-1-5-21-1498259142-	WKS-Mini-Win7	User maya requested Pool canada-
		RIZON7-SYSLOG		3634561516-3640805228-1767		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-ba49-4297-885dfdf2648c3ca3" 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_HO	kenneth	S-1-5-21-4136356191-	BROKER_MACHINE_ALLOCATED	CP-CPR-V062	a442-2b35-461a-ab0b-	np2.ew.domain.local	NP NMR A
	RIZON7-SYSLOG		1247230178-2405973841-13248			21d3bc0		
08/31/2020 04:59:38 PM	WKSTSVMH67\VMWARE_H0	joeb	S-1-5-21-1498259142-	BROKER_MACHINE_OPERATION_	GNMO70190	467d9-7f87-45d7-9eab-	ca0.canada.domain.local	Canada-Main-Win7
	RIZON7-SYSLOG		3634561516-3640805228-8504	DELETED		3c90c2f		

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_HORIZO	joeb	RADIUS access denied for user
	N7-SYSLOG		joeb
08/31/2020 06:08:43 PM	WKSTSVMH56\VMWARE_HORIZO	kenneth	RADIUS access denied for user
	N7-SYSLOG		kenneth
08/31/2020 06:08:43 PM	WKSTSVMH56\VMWARE_HORIZO		RADIUS access denied for user
	N7-SYSLOG	gary	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



- VMware Horizon7 Login success by tr... 🖾 – 🗙 1,000 800 600 400 <0 200 0 08/30 09102 08128 08/29 08131 09101 09103 09104 Aug 28 11:32 AM - Sep 04 11:33 AM
- VMware Horizon7 Login success by count







• VMware Horizon7 - Endpoint management by event type



• 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



• VMware Horizon7 - User not assigned for any pool









• 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

🌯 Expo	💺 Export Import Utility								
Export	Import								
1. Pro 2. Cli	ovide the p ck the Imp	oath and file nam ort button.	ne of the Categories file. Use the '' button to l						
Opt	ions		Location						
•	Category								



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.



Export Import Utility		—		×
Export Import				
1. Provide the path and fi 2. Click the Import button.	le name of the Categories file. Use the '' button to browse and locate the import file.			
Options Category Filters Alerts Systems and Groups Token Value Reports Behavior Correlation	Location Source : *.iscat			
	Impor	rt	Clos	se



EventTracker displays a success message:





3.2 Alerts

- 1. Once you have opened "Export-Import Utility" via "EventTracker Control Panel", click Alert option, and then click the browse _____ button.
- 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.



Ontions	Location	
 Category 	Import E-mail settings	
 Filters Alerts 	Set Active Only if notifications set Dy 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.
 Systems and Groups 	Watchlist Configuration	
O Token Value	Import Watchlist configurat This setting is applicable only f Note: If this action is applied to the setting is applied to the setting is applied to the setting is applied to the setting is applied	ion or alerts which have Advanced watchlist configured.
○ Reports	on the console where the alert	s are imported.
Behavior Correlation		
	Source :	
Benavior Correlation	Source : *.isalt	



EventTracker displays a success message.





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)".

🐁 Export Import Utility	-		\times
Export Import			
1. Provide the path and file name 2. Click the Import button Note : If report(s) contains templa	of Schedule Report file. Use the '' button to browse and locate the import file. ite, first import template and proceed with exportimport utility.		
Options	Location		
Category			
◯ Filters			
 Alerts 	 Legacy (* issch) New (*.etcrx) 		
 Systems and Groups 	Source : *.issch		
O Token Value			
Reports			
Behavior Correlation			
	Import	Clo	se

Figure 24

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".

유 Reports Import	
Note : If report(s) contains template, first import template and proceed with report import process.	
Select file *.etcrx	Select file
Available reports	
Title Frequency Show all Image: Constraint of the state of the sta	L
Title Sites Groups Systems Frequency	Runtime Type

Figure 25

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

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	Set 🛈		
Replace	to Replace	Assign systems		
		Note: Make sure that Site(s), Group(s) and System(s) selections are valid.	9	

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.

		🔎 🛛 Admin 🗸	Tools 🗸 🌔
Active Watch Lists	Event Filters	🧭 Parsing Rules	† / D
Alerts	Eventvault	Report Settings	_
Behavior Correlation Rules	FAQ Tile Configuration	Systems	
🗞 Behavior Correlation Setting	s Group Management	QQ Users	
mi r sc 🚺 Casebook Configuration	Q IP Lookup Configuration	T Weights	since the last 24 ho
କଟ୍ଟି Category	·☆ Knowledge Objects	Windows Agent Config	
Diagnostics	Manager		



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



Figure 29



 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.

Import	
KO_ <product name="">.etko</product>	🗁 Browse Upload

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.





3.5 Dashboards

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











- 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.

Import
Note: If dashlet configured using persisted report, first import the report and proceed with importing dashlet.
🗁 Browse Upload
Available widgets Select All
Figure 34
Import Close



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.



Category Tree Search					
VMWARe Horizon	^				
Category					
✓ VMware Horizon7: Administrative activities					
✓VMware Horizon7: Agent activities					
✓ VMware Horizon7: Application activities					
✓VMware Horizon7: Authentication failed for password					
✓VMware Horizon7: Authentication failed for secure ID					
VMware Horizon7: Authentication failed for user account					
VMware Horizon7: Connection server activities					

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.



Alerts										🔒 / Admin / Alerts
Show All							Search by	Alert name 🗸	horizor	0, 0,
Netsurion EventTracker								🔎 Admin	+ Tools +	💽 Pavan Kumar Tirupathi 👻
174 Available Alerts Total number of alerts available	44 Active Alerts Total number of active alerts				174 System/User Count for system ar	User User Defined Alerts id user defined alerts	127	174 Alerts by 7 Count of alerts	Low Serious Threat Level by threat level	5 5 5 6 4 26
Activate Now Click 'Activate Now	' after making all changes								Total:	11 Page Size 25 🗸
Alert Name 🔨	т	'hreat	Active	Email	Forward as SNMP	Forward as Syslog	Remedial Action at Console	Remedial Action at Agent		Applies To
ββ VMware Horizon7 - Agent offline		•							v7.0 and later	
ြ ဖို့စို VMware Horizon7 - Agent shutdown		•							v7.0 and later	
ြ နိုစို VMware Horizon7 - Authentication failed for use	r account	•							v7.0 and later	
ြ နိုစို VMware Horizon7 - Authentication failed for use	r secure ID	•							v7.0 and later	
ြ ဖို့စို VMware Horizon7 - Folder deleted		•							v7.0 and later	
ြ ဖိုစို VMware Horizon7 - Permission removed		•							v7.0 and later	
ြ ဖို့စို VMware Horizon7 - Role removed		•							v7.0 and later	
ြ နိုစို VMware Horizon7 - Security server removed		•							v7.0 and later	
ြ ဖိုစို VMware Horizon7 - User pasword authentication	failed	•							v7.0 and later	
ြ ဖို့ပို VMware Horizon7 - VCenter Server removed		•							v7.0 and later	
βδ VMware Horizon7: User not authorized		•							v7.0 and later	

Figure 37

4.3 Flex Reports

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





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

Report Configuration					
Scheduled Queued Defined					
Report Groups		÷			
VMware Horizon7	1	0			

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.

Knowledge Objects		
VMWARe Horizon	Q	Q
Groups 🕀 🖉 🖡	Ì	
VMware Horizon7		

Figure 40

4.5 Dashboards

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





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

Available dashlets			×
VMWAre			Q
VMware Horizon7 - Agent ac	VMware Horizon7 - Agent sh	VMware Horizon7 - Authenti	VMware Horizon7 - Authenti
VMware Horizon7 - Login su	VMware Horizon7 - Login su	VMware Horizon7 - Not auth	VMware Horizon7 - Task canc
VMware Horizon7 - User not	VMware Horizon7 - VCenter	VMware Horizon7 - VLSI End	VMware Horizon7 - VLSI End
			Export



