

Integration Guide

Integrate Azure Cache for Redis with EventTracker

Publication Date:

June 21, 2022

Abstract

This guide provides instructions to configure the Knowledge Packs in EventTracker to receive the logs from Azure Cache for Redis. The Knowledge Pack contains alerts, reports, dashboards, categories, and the knowledge objects.

Scope

The configuration details in this guide are consistent with EventTracker version 9.3 or above and Azure Cache for Redis.

Audience

This guide is for the administrators responsible for configuring the Knowledge Packs in EventTracker.



Table of Contents

1	Ove	rview	4
2	Prer	equisite	4
3	Ever	۰ ntTracker Knowledge Packs	4
	3.1	Category	4
	3.2	Reports	4
	3.3	Dashboard	5
4	Imp	orting Azure Cache for Redis Knowledge Packs into EventTracker	6
	4.1	Category	7
	4.2	Reports	8
	4.3	Knowledge Objects (KO)	9
	4.4	Dashboards	11
5	Veri	fying Azure Cache for Redis Knowledge Packs in EventTracker	.14
	5.1	Category	14
	5.2	Knowledge Objects	15
	5.3	Reports	14
	5.4	Dashboards	16

1 Overview

Azure Cache for Redis is a fully managed, in-memory cache service on Microsoft Azure that implements the open-source Redis. Redis enables high-performance and scalable architectures that bring a critical low-latency and high-throughput data storage solution to modern applications. It can process large volumes of application requests by retaining frequently accessed data in the server memory, which can be written to and read from quickly.

Netsurion facilitates monitoring events retrieved from the Azure Cache for Redis. The dashboard, category, alerts, and reports in Netsurion's threat protection platform, EventTracker, will benefit you in tracking users connected to the Cache and their connection count.

2 Prerequisite

- EventTracker version 9.3 or later must be installed and configured to receive logs.
- Configure Azure Cache for Redis to forward logs to EventTracker.

Note

Refer to the <u>How-To</u> guide to configure Azure Cache for Redis to forward logs to EventTracker.

3 EventTracker Knowledge Packs

Configure the Knowledge Packs into EventTracker once the logs are received by the EventTracker Manager.

The following Knowledge Packs (KPs) are available in EventTracker.

3.1 Category

Azure Cache for Redis – Cache activities: This category of the saved search allows you to parse events that are specific to the Cache activities on the Azure Cache for Redis.

3.2 Reports

Azure Cache for Redis – Connected clients list: This report provides a detailed summary of connected clients activities in Azure Cache for Redis. The report includes the source IP address, account name, resource ID, connection count, operation, and more.

Activity timestamp	Cache Name	Region	Source IP Address					
2022-05-12T07:12:16.37824002	Cacheapp	North Europe	10.36.56.4	25		/SUBSCRIPTIONS/5AB4A53E-DFF9- 40AC-B1CC- E6A5F26E177/RESOURCEGROUP S/AZ-CACHE- TEST/PROVIDERS/MICROSOFT.CA CHE/REDIS/CACHEAPP	6	5
2022-05-12T07:12:16.37824002	Ccaheapptrail	east us	10.2.5.6	5		/SUBSCRIPTIONS/5AB4A53E-DFF9- 40AC-B1CC- 66A5726E177/RESOURCEGROUP S/A2-CACHE- TEST/PROVIDERS/MICROSOFT.CA CHE/REDIS/CCAHEAPPTRAIL	5	2
2022-05-13T21:04:58.0466086Z	mycache	canadacentral	10.1.2.3	*86	10.1.1.4	/SUBSCRIPTIONS/E6761CE7-A7BC- 442E-BBAE- 950A121933B5/RESOURCEGROUP S/AZURE- CACHE/PROVIDERS/MICROSOFT.C ACHE/REDIS/MYCACHE	1	4

3.3 Dashboard

Azure Cache for Redis - Connection by geolocation: This dashlet displays the geolocation of the public IPs that are connected to the Cache.



Azure Cache for Redis – Connection via source IP: This dashlet displays the Cache and its connected source IP details.





4 Importing Azure Cache for Redis Knowledge Packs into EventTracker

Import the Knowledge Pack items in the following sequence.

- Category
- Reports
- Knowledge Objects
- Dashboards
- 1. Launch EventTracker Control Panel.
- 2. Double click Export-Import Utility and click the Import tab.





4.1 Category

1. In the **Import** tab, click **Category**, and then click the **Browse** button to locate the file.

3	Export Import Utility	-		x
Export Import Provide the path and file nan Collick the Import button. Options Category Filters Alerts Systems and Groups Token Value Reports Behavior Correlation	Export Import Utility	-1		×
	Import		Close	

- 2. In the Browse window, locate the Categories_Azure Cache for Redis.iscat file and click Open.
- **3.** To import the categories, click **Import**.
- 4. EventTracker displays a success message on successfully importing the selected file in **Category**.



5. Click **OK** or the **Close** button to complete the process.

4.2 Reports

1. In the Import tab, click Reports, and then click New (*.etcrx).

1. Provide the path and file na 2. Click the Import button Note : If report(s) contains ten	ame of Schedule Report file. Use the '' button to browse and locate the import file. nplate, first import template and proceed with exportimport utility.
Options Category Filters Alerts Systems and Groups Token Value Reports Behavior Correlation	Location O Legacy (*issch) Source : *issch

2. In the **Reports Import** window, click **Select file** to locate the **Reports_ Azure Cache for Redis.etcrx** file.

* Reports Import				×
Note : If report(s) contains template, first import template	e and proceed with report import process.			
Select file C:\Users\Chithra\Desktop\Azure Cache	for Redis\Reports_Azure Cache for Redis_fit	nal.etcrx	Select file	
Available reports				
	Frequency Show all	- Q Q		
Title	Sites	Groups	Systems	Frequency
EDIT Azure Cache for Redis - Connected cli.				Undefined
4				
Note: Set run time option is not applicable for Define	d Reports and Hourly Reports			
Set run time for report(s) from	AM • at interval of minute	is Sec		
Replace to	Repla	ace Assign systems		
		Note: Make sure that Site(s)	, Group(s) and System(s) selections are	valid.



- 3. Select the check box of all the files and click the **Import** \mathbb{T} button to import the selected files.
- 4. EventTracker displays a success message on successful importing of the selected files in **Reports**.



5. Click **OK** or the **Close** button to complete the process.

4.3 Knowledge Objects (KO)

1. In the EventTracker Manager console, hover over the Admin menu and click Knowledge Objects.

≡	Event Tracker ⊕					🐥 🛛 Admin-	Tools -
	Home		Active Watch Lists	Collection Master	🔄 Group Management	Systems	🕈 / Dashb
٩		Alerts	Correlation	🔍 IP Lookup Configuration	🛱 Users		
	0	1	Behavior Correlation Rules	Diagnostics	· Knowledge Objects	r Weights	
~			🇞 Behavior Correlation Settings	🐨 Event Filters	Manager	Windows Agent Config	
	Potential Cyber Breaches Unsafe connections or processes, new TCP entry point	Indicators of Cc USB activities, New sen	Casebook Configuration	Eventvault	😥 Parsing Rules		
			elos Category	FAQ Configuration	Report Settings		
	Attacker		- News				

2. In the Knowledge Objects interface, click the Import \blacksquare button to import the KO files.

	Knowledge Ob	jects		🕈 / Admin / Knowledge Objects
Q	Search objects	Q	Q Activate Now	Objects 🕀 耳 🏦 🌣
Ex.				
	Groups	🕀 🖉 🗓		Î
	E Cylance			
	EventTracker			



3. In the Import window, click Browse and locate the KO_ Azure Cache for Redis.etko file.



4. Select the check box next to the browsed file, and then click the \blacksquare Import button.

Impor	t		
Sele	:t file		Growse Upload
	Object name	Applies to	Group name
~	Azure Cache for Redis	Azure Cache for Redis	Microsoft Azure
			Import Close

5. EventTracker displays a success message on successfully importing the selected file in **Knowledge Objects**.



4.4 Dashboards

1. Log in to the **EventTracker** web interface and go to **Dashboard** > **My Dashboard**.

11	Home			
۹	My Dashboard			
R	Threats		1	
	Incidents	ntry point	Indicators of Compromise USB activities, New services or software install	
	Behavior Correlation			
	Change Audit			-
	Compliance		California	

2. In the My Dashboard interface, click the Import I button to import the files.



3. In the Import window, click Browse to locate the Dashboards_Azure Cache for Redis Redis.etwd file and then click Upload.



4. Select the **Select All** checkbox to select all the dashlet files and click **Import** to import the selected dashlet files.

nport			
Note: If dashlet configured using dashlet.	persisted report, first import the r	report and proceed with im	nporting
		🗁 Browse	Upload
Available widgets			
Select All			

5. The EventTracker displays a success message on successful import of the dashlet files.



6. Then, in the My Dashboard interface, click the Add \oplus button to add the dashboard.

My Dashboard	ł		👚 / Dashboard / My Dashboar
CheckPoint	Trend Micr	Microsoft	⊕∥⊘ @ ‡ 1 ⊽ ⊚



7. In the Edit Dashboard interface, specify the Title and Description and click Save.

Edit Dashboard	
Title	
Azure Cache for Redis	
Description	
Azure Cache for Redis	
	Save Delete Cancel

From the newly created dashboard interface (for example, Azure Cache for Redis), click the Configuration Sutton to add the Azure Cache for Redis dashlets.

My Dashboard
Azure Cac

9. Search and select the newly imported dashlets and click Add.

Customize dashlets						×
azure cache					Q	
Azure Cache for Redis - Connec	e for Redis - Connec					
			Add	Delete	Close	,



5 Verifying Azure Cache for Redis Knowledge Packs in EventTracker

5.1 Category

1. In the EventTracker web interface, hover over the Admin menu and click Category.

≡	Event Tracker ⊕					🐥 Admin-	Tools -
	Home		Active Watch Lists	Collection Master	🖙 Group Management	Systems	🕈 / Dashb
a			Alerts	Correlation	🔍 IP Lookup Configuration	였 Users	
	0	1	Behavior Correlation Rules	Diagnostics	· Knowledge Objects	A Weights	
<u>~</u>			🗞 Behavior Correlation Settings	⊽ Event Filters	Manager	Windows Agent Config	
	Potential Cyber Breaches Unsafe connections or processes, new TCP entry point	USB activities, New sen	Casebook Configuration	Eventvault	Parsing Rules		
			କଳ୍ପି Category	FAQ Configuration	Report Settings		
	Attacker			 News 			

2. In the **Category** interface, under the **Category Tree** tab, click the **Microsoft Azure** group folder to expand and see the imported categories.



5.2 Reports

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

≡	Event Tracker ⊕			
	Home			
م ا	Report Configuration		1	
	Report Dashboard	l ntry point	Indicators of Compromise USB activities, New services or software install	
	Explorer Attacker			-

- 2. In the **Reports Configuration** interface, click **Defined**.
- **3.** In the search field, type **Microsoft Azure** and click **Search** to search for the Azure Cache for Redis files.

4. EventTracker displays the reports for Azure Cache for Redis.

Reports configuration: Azure Cache for Redis					
⊕ [⊥] _ℓ ,					
Title					
0 🔅	Azure Cache for Redis - Connected clients list				

5.3 Knowledge Objects (KO)

1. In the EventTracker web interface, hover over the Admin menu and click Knowledge Objects.

≡	Event Tracker ⊕					.▲ Admin•	Tools 🕶
	Home		Active Watch Lists	Collection Master	Group Management	Systems	🕈 / Dashb
٩		_	Alerts	Correlation	🔍 IP Lookup Configuration	🛱 Users	
	0	1	Behavior Correlation Rules	Diagnostics	💮 Knowledge Objects	r Weights	
~		🇞 Behavior Correlation Settings	Event Filters	Manager	Windows Agent Config		
	Potential Cyber Breaches Unsafe connections or processes, new TCP entry point	Indicators of Cc USB activities, New sen	Casebook Configuration	Seventvault	😥 Parsing Rules		
			eterory €	FAQ Configuration	Report Settings		
	Attacker		- News				

2. In the **Knowledge Object** interface, under **Groups** tree, click the **Microsoft Azure** group to expand and view the imported Knowledge objects.



3. Click Activate Now to apply the imported Knowledge Objects.

5.4 Dashboards

1. In the **EventTracker** web interface, go to **Home** > **My Dashboard**.

	EventTracker							
-	Home							
Q. 	Report Configuration		1					
	Report Dashboard	ntry point	Indicators of Compromise USB activities, New services or software install					
	Explorer Attacker			-				

2. The My Dashboard interface displays all the dashlets related to Azure Cache for Redis.

C	ustomize dashlets					\times
	azure cache				Q]
	Azure Cache for Redis - Connec	Azure Cache for Redis - Connec				
			Add	Delete	Clos	e



About Netsurion

Netsurion[®] delivers an adaptive managed security solution that integrates our XDR platform with your existing security investments and technology stack, easily scaling to fit your business needs. Netsurion's managed offering includes our 24x7 SOC that operates as your trusted cybersecurity partner, working closely with your IT team to strengthen your cybersecurity posture. Our solution delivers Managed Threat Protection so you can confidently focus on your core business.

Headquartered in Ft. Lauderdale, FL with a global team of security analysts and engineers, Netsurion is a leader in Managed Detection and Response (MDR) and a Top 25 Global MSSP. Learn more at <u>www.netsurion.com</u>.

Contact Us Corporate Headquarters

Netsurion Trade Centre South 100 W. Cypress Creek Rd Suite 530 Fort Lauderdale, FL 33309

Contact Numbers

EventTracker Enterprise SOC: 877-333-1433 (Option 2) EventTracker Enterprise for MSPs SOC: 877-333-1433 (Option 3) EventTracker Essentials SOC: 877-333-1433 (Option 4) EventTracker Software Support: 877-333-1433 (Option 5) https://www.netsurion.com/eventtracker-support