

Integration Guide

Integrating Azure Storage with EventTracker

Publication Date:

March 30, 2022

© Copyright Netsurion. All Rights Reserved.



Abstract

This guide provides instructions to retrieve the **Azure Storage** events via the Azure Event Hub and then configure the **Azure function app** to forward the logs to EventTracker. After EventTracker receives the logs from the Event Hub, the reports, dashboard, alerts, and saved searches can be configured.

Scope

The configuration details in this guide are consistent with EventTracker version 9.3 or above and **Azure Storage.**

Audience

The Administrators who are assigned the task to monitor the **Azure Storage** events using EventTracker.



Table of Contents

Та	Table of Contents							
1.	. Overview							
2.	. Prerequisites							
3.	Con	figuring Azure Storage to Forward Logs to EventTracker4						
	3.1	Forwarding Event Hub data to EventTracker4						
	3.2	Configuring Azure Storage to stream events to Event Hub4						
4.	Eve	ntTracker Knowledge Packs7						
	4.1	Alerts7						
	4.2	Categories7						
	4.3	Reports7						
	4.4	Dashboards8						
5.	Imp	orting Azure Storage Knowledge Packs into EventTracker9						
	5.1	Categories10						
	5.2	Alerts10						
	5.3	Knowledge Objects (KO)11						
	5.4	Reports						
	5.5	Dashboards14						
6.	Veri	ifying Azure Storage Knowledge Packs in EventTracker17						
	6.1	Categories17						
	6.2	Alerts						
	6.3	Knowledge Objects						
	6.4	Reports						
	6.5	Dashboards19						
	About	Netsurion						
	Conta	ct Us20						

1. Overview

Azure Storage platform is Microsoft's cloud storage solution for modern data storage scenarios. Azure Storage offers highly available, massively scalable, durable, and secure storage for a variety of data objects in the cloud.

EventTracker helps to monitor events from Azure Storage. Its dashboard and reports will help you track, user actions in Azure Storage, geo-location to modify and delete actions performed, and identity access to the storage with status code, which will help to identify manipulations, and malicious activities which may lead to potential data destruction.

2. Prerequisites

- An Azure Subscription and a user who is a global administrator.
- Azure Resource group.
- EventTracker Manager public IP address.

3. Configuring Azure Storage to Forward Logs to EventTracker

Azure Storage can be integrated with EventTracker by streaming the logs to the Azure Event Hub, and from Azure Event Hub to EventTracker.

3.1 Forwarding Event Hub data to EventTracker

Refer to the Configuration of the Azure function app to forward the logs to EventTracker.

3.2 Configuring Azure Storage to stream events to Event Hub

- Login to <u>portal.azure.com</u> using the Admin account and <u>create an event hub namespace</u>, if not created.
- 2. Search and select Storage from All services.



- 3. Open the storage account which is needed to be monitored.
- 4. From the left panel under Monitoring, select Diagnostics settings:



Мо	Monitoring							
Ŷ	Insights							
ų	Alerts							
ΰá	Metrics							
~	Workbooks							
45	Diagnostic settings							
P	Logs							

5. Click Blob.

• Select any of the resources to view diagnostic settings.						
Name	Resource type					
csg100320012a289dd4	Storage account					
blob	Storage account					
queue	Storage account					
table	Storage account					
🔲 file	Storage account					

6. Click Add diagnostics settings.

Diagnos	tic settings	
Na	me	Storage account
No	diagnostic settings d	efined
+ A	dd diagnostic setting]
Click 'Ac	ld Diagnostic setting'	above to configure th
• S • S • T	torageRead torageWrite torageDelete ransaction	

7. Provide the inputs.

Diagnostics settings name, such as **Storage**. Select **log** type, Storage Read, Storage Write, and Storage Delete In the **Destination details** section, select **stream to an Event Hub** and then choose the following options.

- **Subscription:** Select the desired Azure subscription.
- Event Hub namespace: Select the Event Hub namespace.
- **Event Hub name:** Select the Event Hub created under the Event Hub namespace.
- **Event Hub policy name:** Select the Event Hub policy.

8. Click Save.

🔚 Save 🗙 Discard 🗎 Dele	ete 🔗 Feedback					
A diagnostic setting specifies a list of destinations that you would stream categories and contents of those lo	of categories of platform logs and/or metrics that them to. Normal usage charges for the destinat gs	at you want to collect from a resource, and one or more tion will occur. Learn more about the different log				
Diagnostic setting name *	Storage	\checkmark				
Logs		Destination details				
Categories		Send to Log Analytics workspace				
StorageRead						
StorageWrite		Archive to a storage account				
		Stream to an event hub				
StorageDelete		For notantial nartner integrations, click to learn more about event bub integration				
Matrice		For potential paralel integrations, circle to team more about event hab integration.				
metrics		Subscription				
Transaction		PAYG-ET-AZURE-KP-DEV				
		Event hub namespace *				
		az-siemhub 🗸				
		Event hub name (optional) 🕕				
		collector 🗸				
		Event hub policy name				
		RootManageSharedAccessKey 🗸				

9. Click **Queue** and repeat steps 6, 7, and 8.

Select any of the resources to view diagnostic settings.						
Name	Resource type					
csg100320012a289dd4	Storage account					
blob	Storage account					
queue	Storage account					
table	Storage account					
ile 📕	Storage account					

10. Click Table and repeat steps 6, 7, and 8.

Select any of the resources to view diagnostic settings.						
Name	Resource type					
csg100320012a289dd4	Storage account					
blob	Storage account					
queue	Storage account					
table	Storage account					
📰 file	Storage account					



11. Click file and repeat steps 6, 7, and 8.



4. EventTracker Knowledge Packs

After the logs are received by the EventTracker Manager, then the Knowledge Packs can be configured into EventTracker.

The following Knowledge Packs (KPs) are available in EventTracker to support Azure Storage.

4.1 Alerts

• Azure Storage: Modify or delete action performed: This alert indicates that a modify or delete action is detected in Azure Storage.

4.2 Categories

 Azure Storage – Storage activities: This category of the saved search will allow users to parse events that are specific to the Storage activities in Azure Storage.

4.3 Reports

 Azure Storage – Storage activities: This report provides a detailed summary of Storage activities in Azure Storage. It contains a source IP address, account name, user agent, status code, port number, protocol, operation, and more.

		Account	Log			Source IP	Geo	Correlation					Identity		
LogTime	Computer	Name	Category	Operation	Http Code	and Port	Location		Object	Protocol	Status	User Agent	Туре	Туре	MD5
02-18-2022 04:49:44 AM	AZURESTO RAGE	csg1003200 12a9dd4	StorageRead	GetBlobProp erties	200	122.179.108. 12:53602	Central India	e49d8c4f- 501e-0015- 27ec- 2314520000 00	/csg1003200 12a289dd4/c ontainer/veb er/old/Analy sis on NSS server.docx	HTTPS	Success	AzCopy/10.1 3.0 Azure- Storage/0.14 (go1.16; Windows_N T)	SAS	blob	
02-18-2022 05:02:49 AM	AZURESTO RAGE	csg1003200 12a9dd4	StorageWrit e	PutBlob	201	122.179.108. 12:53604	Central India	43530028- 601e-003f- 1dec- 2361870000 00	/csg1003200 12a289dd4/c ontainer/cont oso/Analysis on internet access CA.docx	HTTPS	Success	AzCopy/10.1 3.0 Azure- Storage/0.14 (go1.16; Windows_N T)	SAS	blob	pPOAvfLKkd /rSgla0HMM Xw==



4.4 Dashboards

Azure Storage - Modify and delete action by Geo location



Azure Storage - Storage activities by Category





Azure Storage - Identity type by Http code



5. Importing Azure Storage Knowledge Packs into EventTracker

NOTE: Import the Knowledge Pack items in the following sequence:

- Categories
- Alerts
- Knowledge Objects
- Reports
- Dashboards
- 1. Launch the EventTracker Control Panel.
- 2. Double click the Export-Import Utility.





3. Click the **Import** tab.

5.1 Categories

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

9	Export Import Utility
Export Import Provide the path and file nam Click the Import button. Options Category Filters Alents Systems and Groups Token Value Reports Behavior Correlation	e of the Categories file. Use the '' button to browse and locate the import file. Location Source :
-	Import Close

- 2. Locate the Categories_Azure Storage.iscat file, and then click the Open button.
- 3. To import the categories, click the **Import** button.

EventTracker displays a success message.



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

5.2 Alerts

1. Click the **Alert** option, and then click the **Browse** button.



	Export Import Utility 📃 🗖					
xport Import						
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.						
Ontions	Location					
	✓ Import E-mail settings					
0 000030.7	Set Active					
○ Filters	 Only if notifications set This setting is applicable only for imports from Legacy (v6x) Alert files. For v7 the active status will be set based on 					
 Alerts 	By default "Active" key available in the configuration section.					
 Systems and Groups 	Watchlist Configuration					
	✓ Import Watchlist configuration					
	This setting is applicable only for alerts which have Advanced watchlist configured.					
○ Reports	on the console where the alerts are imported.					
Behavior Correlation						
	Source :					
	Isan					
	Import					

- 2. Locate the Alerts_Azure Storage.isalt file, and then click the Open button.
- 3. To import the alerts, click the **Import** button. EventTracker displays a success message.



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

5.3 Knowledge Objects (KO)

1. Click Knowledge Objects under the Admin option on the EventTracker Manager page.

Netsurion®

I	Event Tracker ⊕					.▲ Admin•	Tools -
	Home	Active Watch Lists	Collection Master	Group Management	Systems	🕈 / Dashb	
٩		_	Alerts	Correlation	🔍 IP Lookup Configuration	Q Users	
	0	1	Behavior Correlation Rules	Diagnostics		🕀 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. Click the **Import** \mathbb{T} button as highlighted in the below image.

	I Knowledge Objects						
٩	Search objetts Q Q Attivate Now	Objects 🕀 Ҭ 🏦 🌣					
~							
	Groups 🕀 🔗 🗊	Ĺ					
	D _{Cylance}						
	© EventTacker						

3. Click Browse.

Import		×
Select file	🗁 Browse Upload	
		Close

- 4. Locate the file named **KO_Azure Storage.etko**.
- 5. Select the check box and then click the \mathbb{T} Import option.



Import			>
Select	file		🖆 Browse Upload
	Object name	Applies to	Group name
	Azure Storage	Azure Storage	Microsoft Azure
			Import

6. The Knowledge Objects (KO) are now imported successfully.

File imported s	successfully.
	ОК

5.4 Reports

1. Click the **Reports** option and select the **New (*.etcrx)** option.

4	Export Import Utility		
Export Import			
1. Provide the path and file nar 2. Click the Import button Note : If report(s) contains temp	me of Schedule Report file. Use the '' button to browse and locate the import file.		
Options	Location		
 Category 			
⊖ Filters			
 Alerts 	O Legacy (*.issch)		
 Systems and Groups 	Source : *issch		
O Token Value			
Reports			
O Behavior Correlation			
	Import Close		

2. Locate the file named **Reports_Azure Storage.etcrx** and select all the check boxes.



Reports Import	:					>
Note : If report(s) co	ntains template, first import template and	proceed with report import process.				
Select file U:\Us	ers \E l'Admin \Desktop \Hansh \Azure Sto	orage \Reports_Azure Storage.etcrx		Select file		
Title		Frequency Show all	- Q Q			
	Title	Sites	Groups	Systems	Freque	ncy
EDIT Azur	e Storage - Storage activities				Undefined	
c						>
Note: Set run time Set run time fo	e option is not applicable for Defined Rep r report (s) from	• at interval of minute	ns Set (j)			
Destaur						
Replace	to	Repl	ace Assign systems			
			Note: Make sure that Site(s)	Group(s) and System(s) selections are	e valid,	X

3. Click the **Import** I button to import the report. EventTracker displays a success message.

Export Import Utility	×
Selected reports configurations are imported successfully	
ОК	

5.5 Dashboards

NOTE: Below steps given are specific to EventTracker 9 and later.

1. Open EventTracker in a browser and log on.

-	Home		
۹	My Dashboard		
R	Threats	1	
	Incidents	ntry point USE	dicators of Compromise activities, New services or software install
	Behavior Correlation		
	Change Audit		-
	Compliance		Carteria



- 2. Navigate to the **My Dashboard** option.
- 3. Click the **Import** \blacksquare button as shown below.



- 4. Import the dashboard file Dashboards_ Azure Storage.etwd and select the Select All checkbox.
- 5. Click **Import** as shown below.

lote: If dashlet configured using lashlet.	persisted report, first	import the report ar	id proceed with im	porting
			🗁 Browse	Upload
Available widgets				
Select All				
Azure Storage - Storage a	Azure Storage	- Modify an		
Azure Storage - Identity				

6. Import is now completed successfully.

Selected dashlets impo	orted successfully.
	ОК

7. In the **My Dashboard** page select ⊕ to add dashboard.



My Dashboard		🕈 / Dashboard / My Dashboar
CheckPoint Trend Micr	Missoroft	+ C (1) + C
Thend Mich	MICrosoft	

8. Choose the appropriate name for the **Title** and **Description**. Click **Save**.

Add Dashboard	
Title	
Azure Storage	
Description	
Azure Storage	
	Save Delete Cancel

9. On the **My Dashboard** page select (a) to add dashlets.

My Dashboard
Azure Stor

10. Select the imported dashlets and click **Add**.

Customize dashlets					×
Azure Storage					Q,
Azure Storage - Identity type by	Azure Storage - Modify and del	Azure Storage - Storage activiti			
			Add	Delete	Close



6. Verifying Azure Storage Knowledge Packs in EventTracker

6.1 Categories

- 1. Logon to **EventTracker**.
- 2. Click the Admin dropdown, and then click Category.

Ш	Event Tracker ⊕					🐥 🛛 Admin 🕶	Tools -
	Home		🚰 Active Watch Lists	Collection Master	Group Management	Systems	🕈 / Dashb
a		_	Alerts	C Correlation	Q IP Lookup Configuration	QQ Users	
	0	1	Behavior Correlation Rules	A Diagnostics	· Knowledge Objects	1 Weights	
<u>~</u>			🗞 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	P Eventvault	🧭 Parsing Rules		
			oloo⊂ Category	FAQ Configuration	Report Settings		
	Attacker			- News			

3. In the **Category Tree**, scroll down and expand the **Microsoft Azure** group folder to view the imported category.



6.2 Alerts

- 1. Logon to EventTracker.
- 2. Click the Admin menu, and then click Alerts.

	Event Tracker ⊕					🔎 🛛 Admin-	Tools -
	Home		Active Watch Lists	Collection Master	Group Management	Systems	🕈 / Dasht
a			Alerts	Correlation	🔍 IP Lookup Configuration	Q Users	
	0	2	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		
			• Category	FAQ Configuration	Report Settings		
	Attacker			- News			

3. In the **Search** box, type **Azure Storage**, and then click the **Go** button. The Alert Management page will display the imported alert.

⊕ [‡]	Activate Now	Click 'Activate Now' after making all changes					
	Alert Name A						
🗌 දිංචී Azure Storage: Modify or delete action performed							

4. To activate the imported alert, toggle the **Active** switch.

EventTracker displays a message box.

Successfully saved cor	nfiguration. ng additional dialogs
	ОК

5. Click **OK**, and then click the **Activate Now** button.

NOTE: Specify the appropriate **system** in **alert configuration** for better performance.

6.3 Knowledge Objects

1. In the EventTracker web interface, click the Admin dropdown, and then select Knowledge Objects.

≡	Event Tracker ⊕					🐥 🛛 Admin-	Tools -
	Home		Active Watch Lists	Collection Master	Group Management	Systems	🕈 / Dashb
a			Alerts	Correlation	🔍 IP Lookup Configuration	QQ Users	
	0	1	Behavior Correlation Rules	A Diagnostics	· Knowledge Objects	T 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	C Eventvault	Parsing Rules		
			o-∰ Category	FAQ Configuration	Report Settings		
	Attacker			- News			

2. In the Knowledge Object tree, expand the **Microsoft Azure group** folder to view the imported Knowledge Objects.



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



6.4 Reports

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

	EventTracker⊕						
**	Home						
٩							
R	Report Configuration		1				
	Report Dashboard	ntry point	Indicators of Compromise USB activities, New services or software install				
	Explorer Attacker			-			

- 2. In the **Reports Configuration** pane, select the **Defined** option.
- 3. Click the Microsoft Azure group folder to view the imported reports.

Rep	Reports configuration: Microsoft Azure					
Ð	Ü 🕗					
		Title				
	£\$\$	Azure Storage - Storage activities				

6.5 Dashboards

1. In the EventTracker web interface, click the Home Button and select My Dashboard.



2. Click **Search** (Search) for the **Azure Storage**. You will see the following screen.

Customize dashlets				×
Azure Storage				Q
Azure Storage - Identity type by	Azure Storage - Modify and del	Azure Storage - Storage activiti		
			Add	Delete Close



About Netsurion

Flexibility and security within the IT environment are two of the most important factors driving business today. Netsurion's managed cybersecurity platforms enable companies to deliver on both. Netsurion <u>Managed Threat Protection</u> combines our ISO-certified security operations center (SOC) with our own award-winning cybersecurity platform to better predict, prevent, detect, and respond to threats against your business. Netsurion <u>Secure Edge Networking</u> delivers our purpose-built edge networking platform with flexible managed services to multi-location businesses that need optimized network security, agility, resilience, and compliance for all branch locations. Whether you need technology with a guiding hand or a complete outsourcing solution, Netsurion has the model to help drive your business forward. To learn more visit <u>netsurion.com</u> or follow us on <u>Twitter</u> or <u>LinkedIn</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