EventTracker

Actionable Security Intelligence

Integrate Azure Stack

EventTracker v8.x and above

Publication Date: December 10, 2018

Abstract

EventTracker allows you to effectively manage your systems and provides operational efficiencies – reducing IT costs and freeing resources for other duties that increase the business value of your organization. EventTracker's built-in knowledge base enables you to gather business intelligence providing increased security, performance, availability, and reliability of your systems.

Scope

The configurations detailed in this guide are consistent with EventTracker Enterprise version 8.x and later, and Azure Stack.

Audience

EventTracker users, who wish to monitor Azure Stack.



Table of Contents

Abstract	1
Scope	1
Audience	1
Introduction	3
Enable Syslog Forwarding on Azure Stack	3
EventTracker Knowledge Pack	
Flex Reports	3
Alerts	5
Import Azure Stack knowledge pack into EventTracker	6
Alerts	7
Token Templates	8
Flex Reports	9
Verify Azure Stack knowledge pack in EventTracker	11
Alerts	11
Token Templates	11
Flex Reports	12



Introduction

Azure Stack is a hybrid cloud computing software solution developed by Microsoft based on the company's Azure cloud platform. Azure Stack is designed to help organizations deliver Azure services from their own data center.

Azure Stack combines infrastructure-as-a-service (IaaS) and platform-as-a-service (PaaS) services in a software stack that spans on-premises datacenter environments as well as Microsoft's Azure cloud. Azure and Azure Stack share a standardized architecture, including the same portal, a unified application model and common DevOps tools.

Enable Syslog Forwarding on Azure Stack

To enable syslog forwarding on Azure stack, execute the following command in Azure Stack PowerShell.

Set-SyslogServer -ServerName <Eventtracker_IP> -ServerPort <Syslog_Port> -NoEncryption

Example:

Set-SyslogServer -ServerName 192.168.1.52 -ServerPort 512 -NoEncryption

EventTracker Knowledge Pack

Once logs are received by EventTracker manager, Knowledge Packs can be configured into EventTracker. The following Knowledge Packs are available in EventTracker Enterprise to support Azure Stack.

Flex Reports

• Azure Stack - User Logon Failed: This report provides information about the logon failures by users.

LogTime	Computer	System Name	Workstation Name	User Name	Account Domain	Source IP Address	Source Port Number	Reason For Failure	Logon ID
10/29/2018 04:59:56 PM	R1S5-VM30\AZURE01	AzS-Sql01.azurestack.local	WIN-R9H529RIO4Y	AzS-Was-RmSA\$	AZURESTACK	10.42.42.201	53176	Unknown user name or bad password.	0x119C822
10/29/2018 05:00:06 PM	R1S5-VM30VAZURE01	AzS-Sql01.azurestack.local	WIN-R9H529RIO4Y	John	AZURESTACK	10.42.42.201	\$3176	Unknown user name or bad password.	0x119C823

Figure 1

• Azure Stack - User Logon and Logoff: This report provides information about the user logon and logoff.



LogTime	Computer	System Name	User Name	Account Domain	Workstation Name	Source Network Address	Action	Logon Type	Logon ID
10/31/2018 04:02:34 PM	R1S5-VM30\AZUREEE	AzS-ERCS01.azurestack.local	0x4D39317	AZURESTACK.LOCAL	-		Logon	5	0x4D39317
							-		

Figure 2

• Azure Stack - User Account Locked Out: This report provides information about user account locked out.

LogTime	Computer	System Name	User Name	Account Domain	Caller Computer Name	Logon ID
10/31/2018 12:34:53 PM	R1S5-VM30\AZURE001	AzS-Sql01.azurestack.local	John	AZURESTACK	WIN-R9H529RIO4Y	0x119C822
10/31/2018 12:36:12 PM	R1S5-VM30\AZURE001	AzS-Sql01.azurestack.local	Jim	AZURESTACK	WIN-R9H529RIO4Y	0x119C823

Figure 3

• Azure Stack - Audit Logs Cleared: This report provides information about the audit logs cleared.

LogTime	Computer	System Name	User Name	Domain Name	Message	Logon ID
10/31/2018 12:34:53 PM	R1S5-VM30\AZURE001	AzS-Sql01.azurestack.local	Administrator	AZURESTACK	The audit log was cleared.	0x119C822
10/31/2018 12:36:12 PM	R1S5-VM30VAZURE001	AzS-Sql01.azurestack.local	ETAdmin	AZURESTACK	The audit log was cleared.	0x119C823

Figure 4

• Azure Stack - Administration Activities: This report provides information about the administrative activities.



LogTime	Computer	- System Name	Action	Object Changes	Permissions Change	Process Information	Subject Information
10/31/2018 12:46:49 PM	R1SS-VM30\AZURE001	AzS-ADFS01.azurestack.local	Permissions on an object were changed.	Object Server:Security\nObject Type:File\nObject Name: C:\Users\4dministratorestfolder\Ne w Text Document.txt\nHandle ID::0x3E7	Original Security Descriptor:0x8c0\nProcess Name:C:\Windows\explorer.e xeMasEventID=4670	Process ID:D:PAI(A;;FA;;;LA)(A;;FA;;;S Y) (A;;FA;;;BA)InNew Security Descriptor:D:PARAI(A;;FA;;;S Y)(A;;FA;;;BA)	Security ID:S-1-5- 18\nAccount Name:AZS- ADFS01\$\nAccount Name AZURESTACK\nLogon ID:0x3E7

Figure 5

• Azure Stack - Registry Changed: This report provides information about the registry changes.

LogTime	Computer	System Name	User Name	Account Domain	Operation Type	Object Name	Object Value Name	Old Value Type Old Value	New Value Type	New Value	Process Name
10/31/2018 01:06:37 PM	R1S5- VM30\AZURE001	AzS- ADFS01.azurestack.local	AZS-ADFS01\$	AZURESTACK	New registry value created	\REGISTRYMACHINE\ SOFTWARE\MTG	C:WindowsISystem32WindowsPowerShelfv 1.0powershell.exe		-	-	C:\Windows egedit.exe

Figure 6

Alerts

- Azure stack *Security: User account unlocked This alert will be generated when a user account is unlocked.
- Azure stack Active Directory: Group policy changed This alert will be generated when a group policy is changed.
- Azure stack Admin Interactive/Remote Interactive login failure This alert will be generated when admin Interactive/Remote Interactive login failure occurs.
- Azure stack Admin Interactive/Remote Interactive login success This alert will be generated when admin Interactive/Remote Interactive login is successful.
- Azure stack Administrative logon failure This alert will be generated when an administrative logon failure occurs.
- Azure stack Administrative logon success This alert will be generated when administrative logon is successful.
- Azure stack Audit event records discarded This alert will be generated when audit event records are discarded.
- Azure stack Audit log cleared This alert will be generated when audit logs are cleared.
- Azure stack Directory permission change- This alert will be generated when directory permissions are changed.
- Azure stack Domain policy changes This alert will be generated when domain policies are changed.
- Azure stack Excessive access failures by a user This alert will be generated when failure for excessive access occurs by a user.
- Azure stack Excessive access failures in your organization This alert will be generated when failure for excessive access occurs in your organization.
- Azure stack Excessive access failures on a specific computer This alert will be generated when failure for excessive access occurs on a specific computer.



- Azure stack Excessive file deletes on a computer This alert will be generated when excessive file is deleted on a computer.
- Azure stack Excessive logon attempts from a IP address This alert will be generated when excessive login attempts from a IP address.
- Azure stack Excessive logon failures due to bad password/username This alert will be generated when an excessive logon failure occurs due to bad password.
- Azure stack Excessive logon failures in your enterprise This alert will be generated when excessive logon failures occurs in your enterprise.
- Azure stack Excessive logon failures in your enterprise due to user account locked This alert will be generated when excessive logon failures occurs in your enterprise due to user account locked.
- Azure stack Excessive user lockout in your enterprise This alert will be generated when excessive user lockout occurs in your enterprise.
- Azure stack File replication service staging area full This alert will be generated when the file replication service staging area is full.
- Azure stack Group policy processing error- This alert will be generated when an error occurs while processing a group policy.
- Azure stack Possible malware lateral movement This alert will be generated when a possible malware lateral movement is suspected.
- Azure stack Security: User account locked out This alert will be generated when a user account is locked out.
- Azure stack Security: Users added to Domain Admin or local Admin group This alert will be generated when user is added to domain admin or local admin group.
- Azure stack Security: Users password set to never expire This alert will be generated when user password is set to never expire.
- Azure stack System shutdown This alert will be generated when the system is shutdown.

Import Azure Stack knowledge pack into EventTracker

NOTE: Import knowledge pack items in the following sequence:

- Alerts
- Token Templates
- Flex Reports
- 1. Launch EventTracker Control Panel.
- 2. Double click Export Import Utility.





Figure 7

....

3. Click the Import tab.

Alerts

1. Click **Alert** option, and then click the browse

button.



 Provide the path and file has Click the Import button. 	ame of the Alerts file. Use the button to browse and locate the import file.	
Options	Location	
	✓ Import E-mail settings	
<u>-</u> ,	Set Active	
O Filters	Only if notifications set This setting is applicable only for imports from Legacy (v6x) Aleft files. For v7 the active status will be set based on	
Alerts	O By default "Active" key available in the configuration section.	
Systems and Groups	Watchlist Configuration	
O Takan Valua	✓ Import Watchlist configuration	
	This setting is applicable only for alerts which have Advanced watchlist configured.	
O Reports	on the console where the alerts are imported.	
Behavior Correlation		
	Source :	
	C:\Users\Desktop\Azure Stack.isalt	

Figure 8

- 2. Locate Alert_Azure Stack. isalt file, and then click the Open button.
- 3. To import alerts, click the **Import** button.





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

Token Templates

- 1. Click Parsing rules under Admin option in the EventTracker manager page.
- 2. Move to **Template** and click on import configuration \mathbb{F} icon on the top right corner.
- 3. In the popup window browse the file named Token Template_ Azure Stack.ettd.



~	Template name	Separator	Template description	Added date	Added by	Group Name	
7	Azure Stack - Account Locked Out	١n	"Aug 20 05:55:02 ass-bgpnat01 Aug 20 12:45:20 AZS-SQL01 CEF.0.0[Micr osoft]Microsoft Azure Stack[10]Microsoft-Windows-Security-Auditing: 47 40]Logoff[0]MiscThannel Security MasComputersAsS-5q0[12:aucrestack]o cal MasEventDescription=A user account was locked out.hu/Nsübject/n S ecurity ID: SYSTEM/n Account Name: A2S-Was-RmSA\$n Account Domai m: AZURESTACK/n Logon ID: 0x119C822(hu/Account That Was Locked Ou thn Security ID: S-15-21-3001455328-1185715961-2121332241-1299/n Account Name: John/n/nAdditional Information: \n Caller Computer Nam e: WIN-RM5258IO4*/n"	Oct 29 05:53:16 PM	pratik.k	Azure Stack	
1	Azure Stack - Account Logon and Logooff	١n	*Aug 20 05:55:02 azs-bgpnat01 Aug 20 12:45:20 AZS-SQL01 CEF.0.0]Micr osoft[Microsoft Azure Stack]10]Microsoft-Windows-Security-Auditing:46 34[Logoff]0]Maschannel=Security MascComputer-AzS-Sql01 azurestacklo cal MasEventDescription=An account was logged off:\n\nsblecth Secur ity ID: 5-1-5-21-3081455328-1185715961-2121332241-1299\n Account N mere: AzS-Was-RnSA9h Account Domain: AZURESTACK Logon ID: 0x1 19C822\n\nLogon Type: 3\n\nThis event is generated with a logon event using t he Logon ID value. Logon ID are only unique between reboots on the sa me computer. MasEventID=4634 MasEvecutionProcessID=668 MasEvecut ionTirreadID=1584 MasKeywords=0:M020000000000 MasKeywordMi me=;Audit Success MasLevel-00 MasOpcode=0 MasOpcodeName=Info MasProvideName=Microsoft-Windows-Security-Auditing MasTask=1254 5 MasTasKCategory-Logoff MasVersion=0 MasEventUat=5-1-3-21-3081	Oct 29 03:17:23 PM	pratikk	Azure Stack	2

Figure 10

4. Now select all the check box and then click on \mathbb{T} Import option.

Flex Reports

On EventTracker Control Panel,

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

💺 Export Import Utility		_		\times
Export Import				
1. Provide the path and file nan 2. Click the Import button Note : If report(s) contains temp	ne of Schedule Report file. Use the '' button to browse and locate the import file. late, first import template and proceed with exportimport utility.			
	Location			
◯ Alerts	O Legacy (*.issch)			
O Systems and Groups	Source :			
O RSS Feeds	-issch			
Reports				
O Behavior Rules				
⊖ SCAP				
O Token Value				
	Impo	ort	Clos	e





2. Locate the **Reports_Azure Stack.etcrx** file and select all the check box.

lect	t file	\\NTPLDTBLR49\Sample_Logs\Azure St	ack Reports etcrx		Select file	0
alat	ble repo	ds		0.0		
le			Frequency Show all			
		Title	Sites	Groups	Systems	Frequency
	EDII	Azure Stack - Administration Activities	R155-VM30			Undefined
ļ	EDIT	Azure Stack - Audit Logs Cleared	R1S5-VM30	Default	Azure001	Undefined
1	EDIT	Azure Stack - Registry Changed	R1S5-VM30			Undefined
	EDIT	Azure Stack - User Account Locked Out	R1S5-VM30			Undefined
1	EDIT	Azure Stack - User Logon and Logoff	R1S5-VM30	Default	Azure, Azure01, Azure2	Undefined
	EDIT	Azure Stack - User Logon Failed	R155-VM30			Undefined
	EDII	Azure Stack - User Logon Failed	R155-VM30			Undefined
	EDII	Azure Stack - User Logon Failed	R155-VM30			Undefined

Figure 12

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



Figure 13

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



Verify Azure Stack knowledge pack in EventTracker

Alerts

- 1. In the EventTracker Enterprise web interface, click the Admin dropdown, and then click Alerts.
- 2. In search box, enter **Azure Stack** and then click the **Search** button. EventTracker displays alert of **Azure Stack**.

Alerts									A /4	Idmin / Alerts
Show All						Search by Alert	name 💙	Abirt	1	9
269 Analable Aprts Second and an annum	79 Active Alerta Total handward within early			269 System/User D Court for system of	terre and the series	a a	269 Alerts by T Court of and	Conce Line Series Fernat Level a try transf level	19 14 ₁₈ 1	-
Achiere Now Cick 'Achiere Now'	after making all changes							Total	26 Page Size	3.4
Alert Name -	Threat	Active	E-mail	Forward as SNMP	Forward as Syslog	Remedial Action at Console	Remedial Action at Agent		Applies To	1
Acure stack - "Security: User account unlocked	•	00					Ó	Azure stack		
0 Anure stack - Active Directory: Group policy changed	•	0						Azure stack		
0 Acute stack - Admin Interactive/Remote Interactive logi	n failure 😐							Abure stack		
0 66 Acure stack - Admin Interactive/Remote Interactive logi	n success	C						Azure stack		
08 Azure stack - Administrative logon failure		CID				0		Azure stack		
60 Azure stack - Administrative logon success	•	00						Azure stack		
Acure stack - Audit event records discarded	•	0						Azure stack		
08 Azure stack - Audit log cleared	•	0						Azure stack		
60 Azure stack - Directory permission change	•	0						Azure stack		
00 Acure stack - Domain policy changes	•							Azure stack		
00 Azure stack - Excessive access failures by a user	•	0						Azure stack		
Acure stack - Excessive access failures in your origination	•	CID						Azure stack		
D & Azure stack - Excessive access failures on a specific com	puter 😐						Activate	Azure Halk		N
□ δδ Azure stack - Excessive file deletes on a computer	•	0					Co Dovin	Azure stack	to activity why	
60 Acure stack - Excessive logon attempts from a particular	IP address 😐	0						Azure stack		



Token Templates

- 1. In the EventTracker Enterprise web interface, click the Admin dropdown, and then click Parsing Rules.
- 2. On Template tab, click on the Azure Stack group folder to view the imported Token Values.



Parsing Rules									
Parsing Rule	Template								
Groups		⊕ ⊠			Group : Azure Stack		Search_	Q	
Default				~					
AirWatch MDM		創	1		Template Name	Template Des	cription	Added By	Added Date
Aruba AirWave		Û	0		Azure Stack - Account Locked Out	Azure Stack		pratik.k	Oct 29 05:53:16 PM
ArubaO5		Û	0		Azure Stack - Account Logon and Az Logooff	Azure Stack		pratik.k	Oct 29 03:17:23 PM
A5400		10	Ø			A			0-100453-33 04
Avaya Selfich		圓	0		Azure Stack - Account Logon Pared	Azure Stack		praciele	Oct 29 04:53:52 PM
Azure Stack		Û	0		Azure Stack - Administration Activities	Azure Stack		pratik.k	Oct 30 06:10:32 PM
Berracude NG firewal		徝	0		Azure Stack - Audit Log Cleared	Azure Stack		pratik.k	Oct 29 05:29:32 PM
Berracuda SSL VPN		1	0		Azure Stack - Registry Changed	Azure Stack		pratik.k	Oct 30 06:25:22 PM
Blue Coat Proxy SG		創	1						
CheckPoint(syslog)		創	1						
Cisco ASA		前	0						
Cisco ASA VPN		Ð	Ø	~					

Figure 15

Flex Reports

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





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

Scheduled Queued Defi	ned	Search.					
Report Groups							
9 Security				⊕ II ∂.			
Compliance	ince				Title	Created on	Modified on
(Operations	rations				Azure Stack - Registry Changed	Oct 30 06:27:47 PM	Oct 31 05:05:09 P
😟 : Rex				۲	Azure Stack - Administration Activities	Oct 30 06/14/56 PM	Oct 31 05:10:59 P
Malwarebytes				(3)	Azure Stack - Audit Logs Cleared	Oct 30 11:2640 AM	Oct 31 05/14:57 P
ArWatch MOM	自	1		151	Azure Stack - User Account Locked Out	Oct 29 05:57:11 PM	Oct 31 05/18/33 P
All Compliance Repor	0	0		25	An an March - Marcal Anna Balant	0.0 10 0.0 The last	0.000000000
🕞 A5400	10	1	-	2	Azure stack - user Logon Palled	OG 20 OKG721 PM	Oct 31 052 CT2 P
🔁 Avaya Switch	Ð	0	10	0	Azure Stack - User Logon and Logoff	Oct 29 02:37:19 PM	Oct 31 05/26/23 F
C3 AWS Cloud Trail	6	a					



