

Barracuda Web Application Firewall with Microsoft Azure Log Analytics

https://campus.barracuda.com/doc/73696952/

You can use Barracuda Web Application Firewall Azure Resource Manager (ARM) template to create and configure a Log Analytics workspace. The Barracuda Web Application Firewall sends the following types of logs to Log Analytics:

- **barracuda_CL** This category contains all types of logs generated on the Barracuda Web Application Firewall, i.e., Web Firewall Logs, Access Logs, Audit Logs, Network Firewall Logs, and System Logs. These logs are sent by the Barracuda Web Application Firewall to Log Analytics using the Microsoft Azure Log Analytics-specific format. To view specific types of logs on Log Analytics Workbook, you can perform a query using 'LogType_s' field in the barracuda_CL logs. The valid values for LogType_s are:
- TR Access logs
- AUDIT Audit logs
- SYS System logs
- WF Web firewall logs
- NF Network firewall logs

You can enable/disable these logs in the Barracuda Web Application Firewall web interface either when you are adding the Log Analytics server or by editing it. By default, all logs are enabled, and this is the recommended configuration for maximum visibility.

Disabling Access Logs and Audit Logs will disable Barracuda Application Performance Dashboard and Barracuda WAF Audit Logs Dashboard provided by the Barracuda Web Application Firewall on Microsoft Azure Log Analytics.

- **Performance** These are the performance logs of the Barracuda Web Application Firewall virtual machine(s) that are collected by Log Analytics.
- **Hearbeat** These are the heartbeat logs sent by the Log Analytics agent installed on the Barracuda Web Application Firewall.

The logs (barracuda_CL, Performance and Heartbeat) sent by the Barracuda Web Application Firewall are displayed as the following solutions in Log Analytics:

- Barracuda Application Attack Statistics Dashboard Displays the graphs and charts based on the analysis of Web Firewall Logs that are sent as "CommonSecurityEvents" by the Barracuda Web Application Firewall. The graphs include:
 - Attack Action Statistics
 - Attack Severity Distribution
 - Application Attack Statistics
 - Aggregated Attack Types
 - Per Instance Attack Types
 - Per Application Attack Types
 - Top Attacking Clients



• Top Attacking User Agents

Diverview		ack Statistics Dasl	hboard												
		ATTACKACTION STATIST	ns	ATTACK SDURITY DIST	BUTION	APPLICATION ATTACK STATISTICS		APPLICATION ATTACK STATE	10	APPLICATION ATTACK STATISTICS		TOP ATTACIPUS CLEMIS		TOP ATTACKING USERAGEN	
		Action Taken Count		Count of different S	invertity Laweix a Littlean analysis Executed Apple Test.	Apprepared Attack types		Per Instance Attack Type		Per Application Attack Types		Top Attacking Clients b	y Source®	Top Attacking Client Us	rAgeras
	Web Application Firewall ™		14.8x old 3.7x		18.5x	30 30	400 AN 1210 PM	100 MM 1210 AM	/	8 8 8 8 8 8 8 8 8 8 8 8 8 8 8 8 8 8 8	600'AN 1230'AN		18.5x		Vienes profile 18.5K
-	ation Attack Statistics	ACTION	count	59/9879	00697	710	00.91	THE UNITAMES	00497	798	09,97	CONTRACTO	COVAT	ISBN 60-F	00
Darhboard	AND NOR ADDRES	DENV	3486		18.56	INVACE,UR, DICCOING	378.	CR025,578, Q47157	746	954630730. CR055,578,5.		994571.1	33X	"Ibnee perid 33"	355 -
CONTENTS		106	130			CROSS_STL_SCRPTING_N_PA.	7.4K	SQUINECTL QATEST	226	96.06.207.20 CROSS_STR_S					
	1					PRAMULANSTH, EXCELOED	2.7%	ANNALIN. QUITER	124	MAG20720 INVADJURL,-	-				
	iction Statistics investo Nationalism					IQURETER/DURING	3.7%	NAME AND ADDRESS OF AD	114	MAG20720- NAMAD_MA					
3. Application Attack Statistics 1. Appropriate Datach Types 2. Per Sectorize Attack Types										SHORES AND					
										REGISTED. PARAMULTING.					
4. Top Atta	Per Application Attack Types ecking Clients									96.06.207.20., SQL_NIGCTO.,					

- Barracuda Application Performance Dashboard Displays the graphs and charts based on the analysis of Access Logs that are sent as "barracuda_CL" by the Barracuda Web Application Firewall. The graphs include:
 - HTTP and HTTPS Stats
 - HTTP Version Distribution
 - HTTP Status Code Distribution
 - Requests Over Time Statistics
 - Inbound Bandwidth Stats
 - Outbound Bandwidth Stats
 - Application Response Summary



- **Barracuda WAF Monitoring Dashboard** Displays the analysis of the Barracuda Web Application Firewall based on the performance logs that are sent as "Perf" by the Log Analytics agent. The graphs include:
 - Average CPU Utilization
 - Average Memory Usage
 - Average Disk Usage
 - Average Network Utilization
 - CPU Utilization
 - Memory Utilization
 - Disk Utilization
 - Network Utilization

6	Cherver + Baraouda WW Monitorin) Dishboard							
+ p	<u>e</u> .								
٥		ABAR OVVERNIN	ATTEND MEROFF ZIND	Advantation parts	ACARD CONTRACTOR OF A CONTRACTOR OFONO OFONO OFONO OFONO OFONO	CONTRACTOR .	MROF-VED-SIN	INCOMPANY .	MINOR LEADON
â	Web Application Firewall Income 9	$\begin{array}{c} \operatorname{decay} \operatorname{Distribution metrics} \\ 19.2 \\ y \\ $	Annuel Henry Supran for France.	derays Dis Days now line 19 cm line 39.4 b b b b b b b b b b b b b	Array fold foir fournel based	AmproV Distance) to and MV	Interpr Merrory Gaspelli) for and SM I and Tomase I and Tomase I and Tomase I and Tomase I and Tomase I and Tomase I and Tomase	Amp Dal Specificapiti for and MM	Shickiya Bashadi walawali waki Kili
	Neuroscie IVM Headoning Cubboard CONTINES - except PCHILDEN - except	Information Inc.	Internet and sense Valahilariy 94		Annya Yani Ajun Bannari B Maria Maria (Balan anjara (Balan Annya Yani Ban) kudurat	Remon DV United (N or and RM DVV United (N or and RM of the general sector of the general of the general sector of the general Remons CAL Information of the general Remonstration of the general sector of the general sector of the general Remonstration of the general sector	Image Menay Mugdall, for said Mill Image Menay Mugdall, for said Mill Image Menay Mugdall, for said Mill Image Menay Mugdall, for said Mill Image Menay Mugdall, for said Mill Image Menay Mugdall, for said Mill		Total Apart Analast for and VMA Terror & Second Se
	1. Smoot Orlanter				The function of the function o	C. /	- I per jacon	an Alexandra A	and a second sec

- Barracuda WAF Audit Logs Dashboard Displays the graphs and charts based on the analysis of Audit Logs that are sent as "barracuda_CL" by the Barracuda Web Application Firewall. The graphs include:
 - WAF Configuration Events
 - Aggregated WAF Configuration Events
 - Configuration Events Per WAF
 - Configuration Events Per Username



🔅 🖺 Edit Clane							
	WAF CONFIGURATION EVEN	пs	WAF CONFIGURATION EVENTS		WAF CONFIGURATION EVENTS		
Web Application Firewall	Aggregated WAF Confi	guration Events 202 UNSUCESSFULLOGIN 4 LOGIN 2	Configuration Events per W/	600 AM 1200 PM	Configuration Events per Us 150 100 50 600 PM 1200 AM	600 AM 2200 F	
Barracuda WAF Audit Logs Analysis	EVENT NAME	COUNT	EVENT NAME HOST_S	COUNT	EVENTNAME ADMINNAME_S	COUNT	
	CONFIG	202	CONFIG QATEST	202	CONFIG admin	202	
CONTENTS	UNSUCCESSFUL_LOGIN	4	UNSUCCESSF QATEST	4	UNSUCCESSF admin	3	
1. WAF Configuration Events	E LOGIN	2	LOGIN QATEST	2	LOGIN admin	2	
 Aggregated WAF Configuration Events Configuration Events per WAF Configuration Events Per UserName 	LOGOUT	1 \	LOGOUT QATEST	1 \	LOGOUT admin	1	
Important Information					UNSUCCESSF admind	1	

Next Step

Continue with Creating a Workspace Using the ARM Template.

Barracuda Web Application Firewall



Figures

- 1. WAF_Attack_Stats.png
- 2. App_Performance_Dashboard.png
- 3. Monitoring_Dashboard.png
- 4. Audit_Logs_Dashboard.png

© Barracuda Networks Inc., 2024 The information contained within this document is confidential and proprietary to Barracuda Networks Inc. No portion of this document may be copied, distributed, publicized or used for other than internal documentary purposes without the written consent of an official representative of Barracuda Networks Inc. All specifications are subject to change without notice. Barracuda Networks Inc. assumes no responsibility for any inaccuracies in this document. Barracuda Networks Inc. reserves the right to change, modify, transfer, or otherwise revise this publication without notice.