

Verify the Instance in the Auto Scaling Group

https://campus.barracuda.com/doc/46897291/

After the CloudFormation template completes its operation and the stack is created, the **CREATE_COMPLETE** message is displayed in "Status". With this, the Barracuda Web Application Firewall instances will be deployed in the specified VPC and boot up with the default configuration. To verify the instance(s) created for auto scaling, perform the following steps:

- 1. Log into the <u>Amazon EC2 Management Console</u>.
- 2. From the EC2 Dashboard, select Auto Scaling Groups under AUTO SCALING.
- 3. Select the auto scaling group you created from the **Auto Scaling Group** list. This will display the details of the auto scaling group.
- 4. Select **Instances** under the **Auto Scaling Group** sub-tabs.

EC2 Dashboard	Create Auto Scaling group Actions 🔨 💠 😧
Reports	Fitter: Q. Filter Auto Scaling aroups × Is a constraint of the second s
Limits	Name A Launch Configuration V Instances V Desired Min V Max V Availability Zones V Default Cooldown V Health Check Grav
INSTANCES	RamacurdaWA RamacurdaWAFStack R 1 1 1 4 uswest-2c uswest
Instances Spot Requests	
Reserved Instances	
Scheduled Instances	
Commands	۲ III کې او کې
Dedicated Hosts	Auto Scaling Group: BarracudaWAFStack-BWAFAutoScalingGroup-ADPMIILTFG87
IMAGES	Detaile Article History Contra Detains Indexes Natifications Test
AMIs	Details Activity history Scaling Policies instances inouncations hats Scheduled Actions
Bundle Tasks	Actions *
ELASTIC BLOCK STORE Volumes	Filter: Any Health Status V Any Lifecycle State V Q. Filter instances X < < 1 to 1 of 1 instances > >
Snapshots	Instance ID 🔺 Lifecycle 👻 Launch Configuration Name 👻 Availability Zone 👻 Health Status 👻 Protected from 👻
NETWORK & SECURITY	i-98b95c40 InService BarracudaWAFStack-BWAFAutoScaleLaunchConfig-OI9VJ7XFYOZ2 us-west-2b Healthy

5. Click on an **Instance ID** and note it down. The instance details are displayed on the **Instances** page. Note: Ensure you note down the **Public IP** or **Public DNS** address.

22 Deekbaard					
vents	Launch Instance Connect	Actions *			😋 🕂 🌩
gs	Q search : i-98b95c40 🔿 Ad	l filter		ØK	1 to 1 of 1 > >
ports					
nits	Name - Instance i	Availability Zone 👻	Instance State - Status Checks	Alarm Status Public DNS	- Public II
STANCES	Demo i-98b95c40	m3.medium us-west-2b	running Ø 2/2 checks	None 🍃	
stances	- (
ot Requests	Instance: i-98b95c40 (Demo)	Public DNS: us-west-2.compu	ite.amazonaws.com		880
eserved Instances					
heduled Instances	Description Status Checks	Monitoring Tags			
ommands	lastras ID	i 09b0Ee.40	Dublic DNC		
edicated Hosts	Instance ID	1-56050040	Public DNS	west-2.compute.amazonaws.com	
AGES	Instance state	running	Public IP		
/Is	Instance type	m3.medium	Elastic IP	+	
indle Tasks	Private DNS	us-west-2.compute.internal	Availability zone	us-west-2b	
	Private IPs		Security groups	BarracudaWAFStack-	
STIC BLOCK STOPE				BWAFAutoScaleSecurityGroup- 1KRW5G7102EHA view rules	
lumes	Secondary private IPs		Scheduled events	No scheduled events	
apshots	VPC ID	vpc-	AMI ID		
	Subnet ID	subnet-	Platform	-	
WORK & SECURITY -	Network interfaces	eth0	IAM role	BarracudaWAFStack-	

 Open a web browser and enter the **Public IP** or **Public DNS** address noted in Step 5 followed by port 8000 (Example: <u>http://40.41.42.43:8000</u> or

http://ec2-40-41-42-43.us-west-2.compute.amazonaws.com:8000).

You might see the Barracuda loading page when accessing the web interface for the first time. This is because the Barracuda Web Application Firewall will be booting up with your configuration and takes a few minutes before presenting the login page.



7. Log into the Barracuda Web Application Firewall web interface using your login credentials: **Username** – *admin*

Password – <*Instance ID of the Barracuda Web Application Firewall noted in Step* 5 > 8. On the Barracuda Web Application Firewall web interface:

1. Go to the **BASIC** > **Services** page and check if the service is created with the values you specified when creating the stack.

If you specified the Fully Qualified Domain Name (FQDN) of a downstream ELB, the service will display multiple servers associated with it. Each of these servers will have an IP address that was returned by resolving the FQDN. The Barracuda Web Application Firewall will automatically resolve the FQDN at specific intervals and update the IP addresses in case of changes. The intervals are equal to the Time To Live (TTL) value returned during DNS resolution.

🔟 Barracuda Web Applic	ation F	irewall							admin S	Sign out E	nglish	-
BASIC SECURITY POLICIES	WEBSITES	ACCESS CONT	ROL	ADVANCED					Search help	o topics		٩
ishboard Services Default line Help Search	Security	Certificates IF	P Configur	ation Adr	ninistration	Web Firewall	Logs Ad	ccess Logs	Audit Logs N	lotifications	Repo	rts
DD NEW SERVICE												Help
Service Name Type	þ	Virtual IP	Address	;	Port 80	Real Serv	vers					
Create Group Service Group Ves No default	os ·	Add										
									More Actions 💌	Prefere	nces	Help
ERVICES	Status	IP Address	Port	Domain	URL	Туре	Mode	Policy	More Actions 💌	Prefere	nces	Help
Ilter All ERVICES Name Be default Gefault	Status	IP Address	Port	Domain	URL	Туре	Mode	Policy	More Actions 💌	Prefere	nces	Help
Ilter All ERVICES Name B & default B & default B & BarracudaWAFStack	Status	IP Address 172.31.30.135	Port 80	Domain	URL	Type	Mode	Policy	More Actions Add Server Rule	Prefere	nces Delete	Help
Ilter All ERVICES Name Gefault Gefaul	Status	IP Address 172.31.30.135 172.31.23.161	Port 80 80	Domain	URL	Type	Mode Passive	Policy	Add Server Rule	Prefere Edit Edit	nces Delete Delete	Help Disa Disa

2. Go to the **ADVANCED** > **High Availability** page and check the cluster status. Ensure the cluster page displays all the instances deployed in this auto scaling group.



🖌 Barracuda	a Web Applic	ation Firewall					admin	English
BASIC SECU	JRITY POLICIES	WEBSITES ACCESS C	ONTROL ADVAN	CED			Search hel	o topics
ckups w Internal Patterns nerability Reports	Energize Updates Libraries Cloud Control	Firmware Update Admin Access Control Task Manager	Export Logs High Availability	Advanced Networking Appearance	Network Firew System Config	all Logs Sys uration Se	stem Logs cure Administration	Templates Troubleshooting
								Save
LUSTER SETTING	S							ŀ
DD SYSTEM TO C	LUSTER	the same shared secre	rauuronzeu systems iron it.	n accessing Cluster Inic	rmauon, All Ballacut	а тыл мррисано.	n rnewans in a clusier	HUSE HAVE
Poor ID Address:		Enter the IP address of	f a system in the cluster w	ith which this system is	to be joined. Note: 7	his action should i	be performed ONLY fr	
reel in Address.		Line nen dureo o				no dobon onobia i	00 pononiou on 21 in	in the unit
Join Cluster		which is intended to ha	ve the configuration of pe	eer system.				nn me unit
Join Cluster	MS	which is intended to ha	ve the configuration of pe	eer system.			Synchronize	Configuration H
Join Cluster	MS	which is intended to ha	ve the configuration of pe	ser system.	Status	Action	Synchronize	Configuration F
Join Cluster LUSTERED SYSTE Hostname barracuda	IP. 17	Address 2.31.30.135	ldentity Self	Serial# 725498	Status ✔ Up	Action	Synchronize	Configuration F

- 9. Repeat the Steps 5 to 8 for all other instances in this auto scaling group. Note: In an auto scaling group, each instance has a unique public DNS (which includes the public IP address in it), and is associated with same security group. When a new instance is added to the auto scaling group, you can use the public DNS or public IP address of that instance to access it. See Step 6 to learn how to access the instance using the public DNS or public IP address.
- 10. Log into the <u>Amazon Management Console</u> and select **S3** under **Storage and Content Delivery**.

11. In the S3 Management Console:

1. An S3 bucket is automatically created with the stack name as part of the unique identifier. Example: "barracudawafstackone-s3bucket-1pcf5nbtp8uh5". You can verify that the bucket includes the data of the deployed Barracuda Web Application Firewall instances.

Barracuda Web Application Firewall



Figures

- 1. Auto Scaling Group.png
- 2. Instance.png
- 3. Services.png
- 4. Cluster.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.