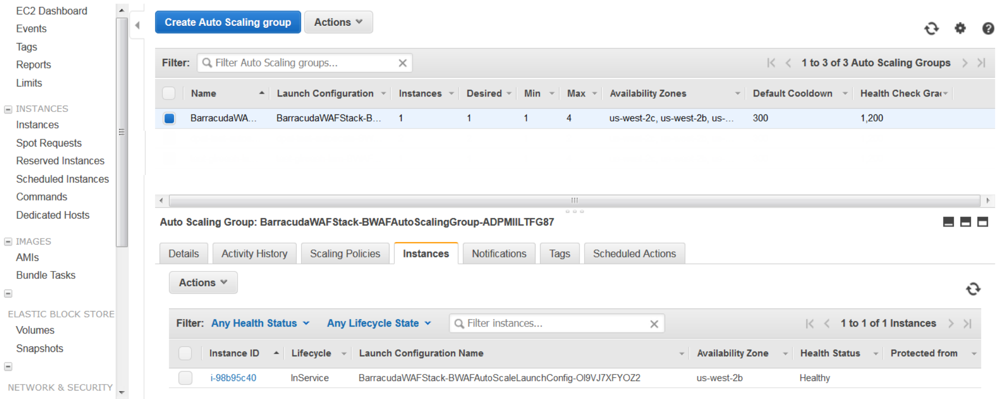
Verify the Instance in the Auto Scaling Group

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 Amazon EC2 Management Console.
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.

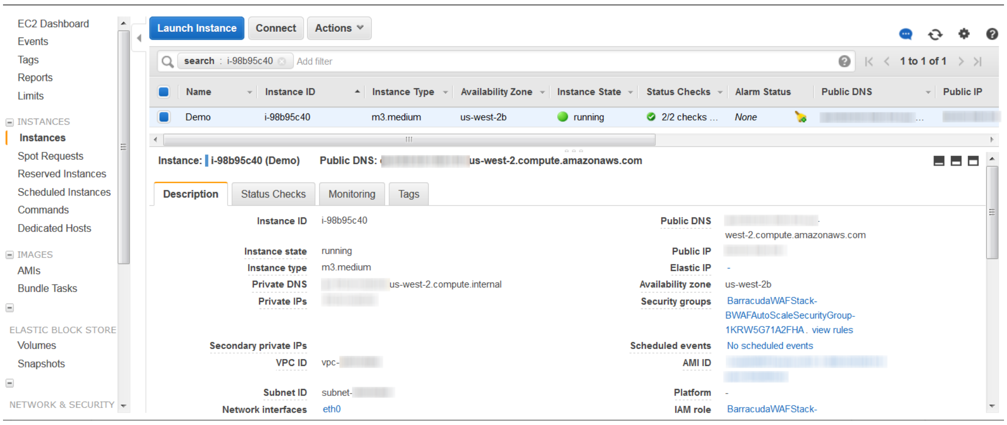


Name	Launch Configuration	Instances	Desired	Min	Max	Availability Zones	Default Cooldown	Health Check Gra
BarracudaWA...	BarracudaWAFStack-B...	1	1	1	4	us-west-2c, us-west-2b, us-...	300	1,200

Auto Scaling Group: BarracudaWAFStack-BWAFAutoScalingGroup-ADPMIILTFG87

Instance ID	Lifecycle	Launch Configuration Name	Availability Zone	Health Status	Protected from
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.



Name	Instance ID	Instance Type	Availability Zone	Instance State	Status Checks	Alarm Status	Public DNS	Public IP
Demo	i-98b95c40	m3.medium	us-west-2b	● running	✓ 2/2 checks ...	None	[redacted] ...	[redacted]

Instance: i-98b95c40 (Demo) Public DNS: [redacted]us-west-2.compute.amazonaws.com

Instance ID i-98b95c40
Instance state running
Instance type m3.medium
Private DNS [redacted]us-west-2.compute.internal
Private IPs [redacted]
Secondary private IPs
VPC ID vpc-[redacted]
Subnet ID subnet-[redacted]
Network interfaces eth0

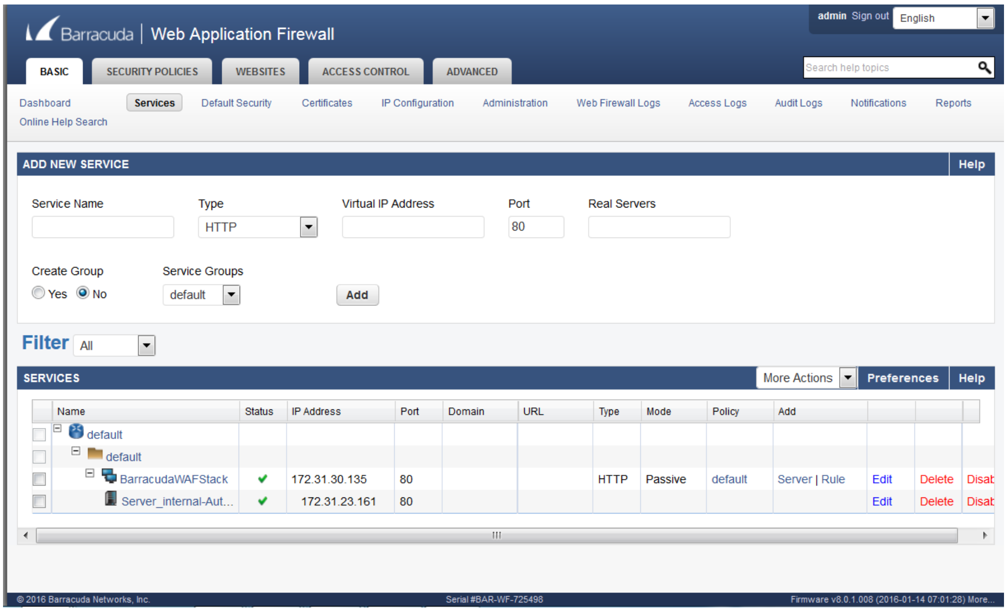
Public DNS [redacted]-west-2.compute.amazonaws.com
Public IP [redacted]
Elastic IP -
Availability zone us-west-2b
Security groups BarracudaWAFStack-BWAFAutoScaleSecurityGroup-1KRW5G71A2FHA . view rules
Scheduled events No scheduled events
AMI ID [redacted]
Platform -
IAM role BarracudaWAFStack-

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



Service Name
Type: HTTP
Virtual IP Address
Port: 80
Real Servers
Create Group: ○ Yes ● No
Service Groups: default

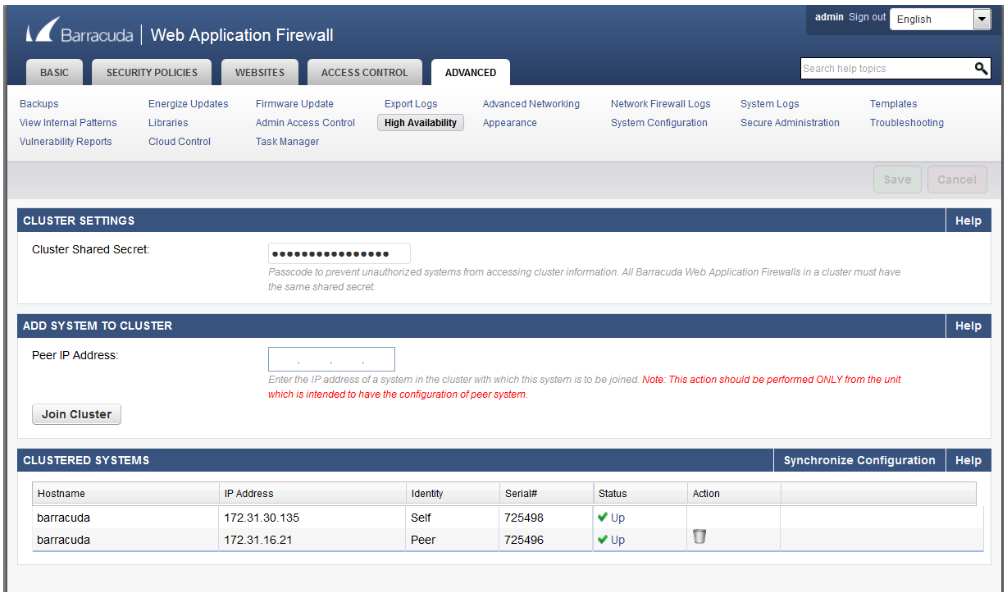
Filter: All

SERVICES

	Name	Status	IP Address	Port	Domain	URL	Type	Mode	Policy	Add			
□	⊟ default												
□	⊟ default												
□	⊟ BarracudaWAFStack	✓	172.31.30.135	80			HTTP	Passive	default	Server | Rule	Edit	Delete	Disab
□	Server_internal-Aut...	✓	172.31.23.161	80							Edit	Delete	Disab

© 2016 Barracuda Networks, Inc. Serial #BAR-WF-725498 Firmware v8.0.1.008 (2016-01-14 07:01:28) More...

   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.



CLUSTER SETTINGS

Cluster Shared Secret: ••••••••••••••••

Passcode to prevent unauthorized systems from accessing cluster information. All Barracuda Web Application Firewalls in a cluster must have the same shared secret.

ADD SYSTEM TO CLUSTER

Peer IP Address: . . .

Enter the IP address of a system in the cluster with which this system is to be joined. Note: This action should be performed ONLY from the unit which is intended to have the configuration of peer system.

CLUSTERED SYSTEMS

Hostname	IP Address	Identity	Serial#	Status	Action
barracuda	172.31.30.135	Self	725498	✓ Up	
barracuda	172.31.16.21	Peer	725496	✓ Up	🗑

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 Amazon Management Console 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.

Figures

© 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.