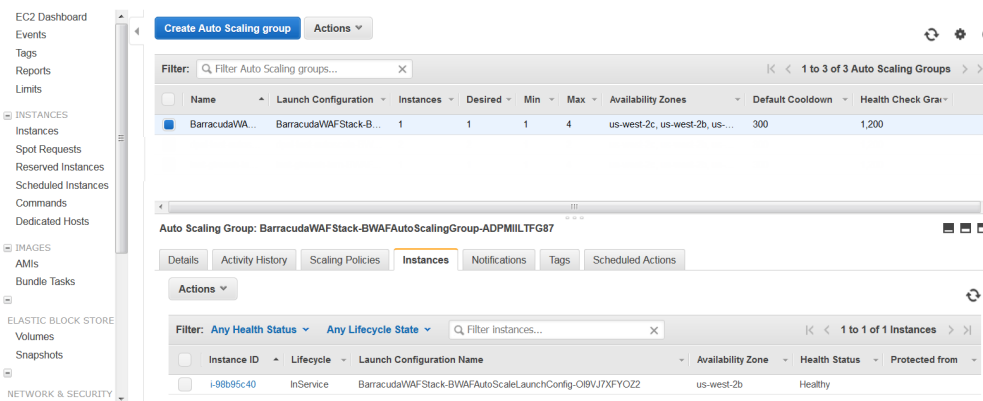


## Verify the Instance in the Auto Scaling Group

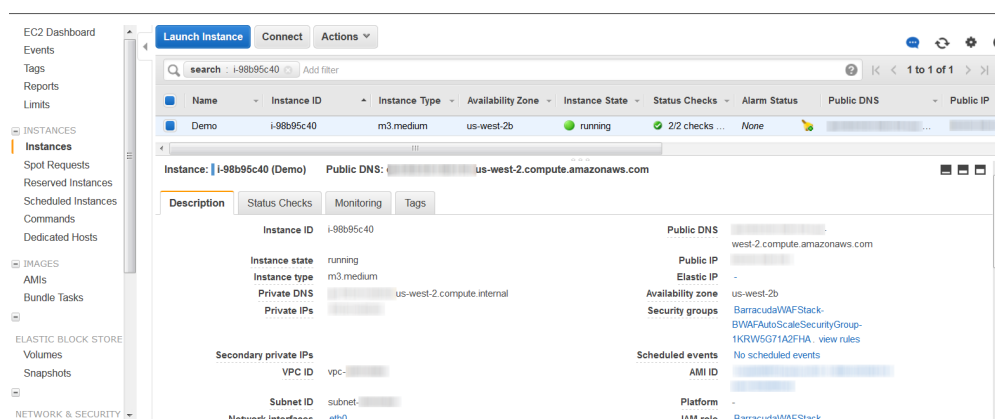
<https://campus.barracuda.com/doc/46897291/>

After the CloudFormation template completes its operation and the stack is created, the **CREATE\_COMPLETE** message is displayed in "Status". With this, the Barracuda CloudGen WAF 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 Auto Scaling Group sub-tabs.



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



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>).

Sometimes 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 CloudGen WAF web interface using your login credentials:

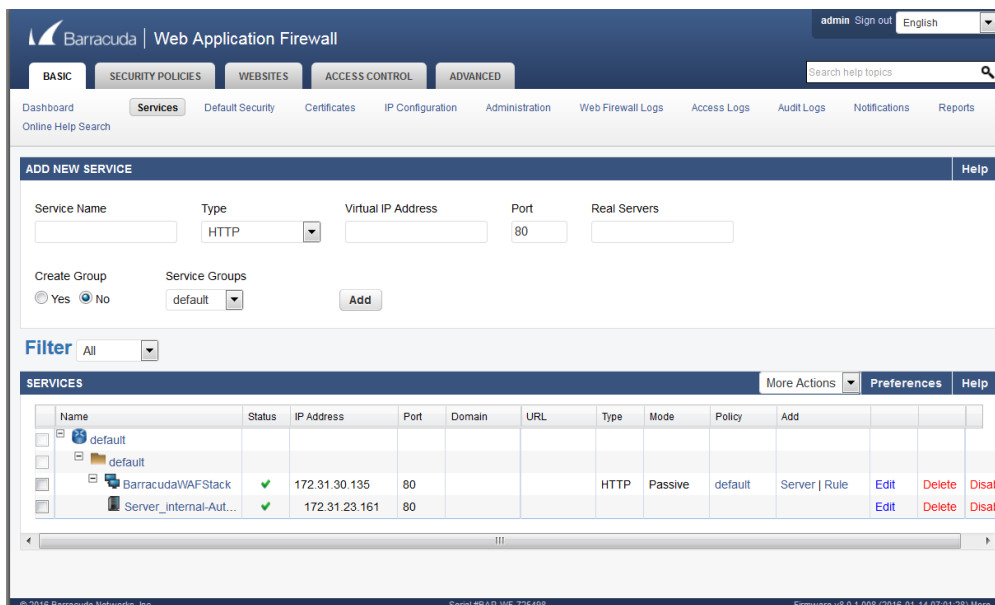
**Username** - *admin*

**Password** - *<Instance ID of the Barracuda CloudGen WAF 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.

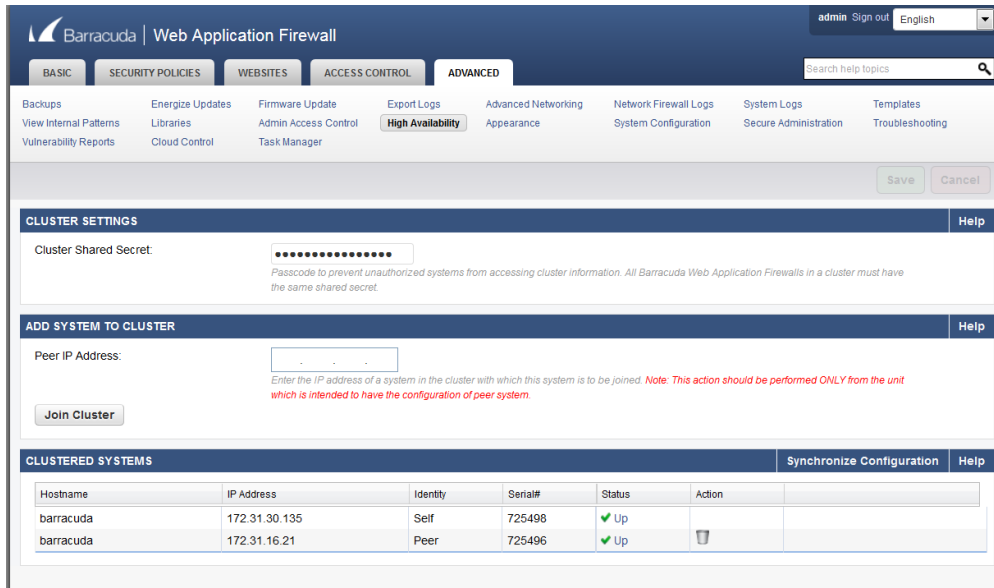
If you had specified the Fully Qualified Domain Name (FQDN) of a downstream ELB, the service will display multiple servers associated with it. Each of these servers will have an IP address that was returned by resolving the FQDN. The Barracuda CloudGen WAF will automatically resolve the FQDN at specific 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.



The screenshot shows the Barracuda Web Application Firewall interface. The top navigation bar includes 'BASIC', 'SECURITY POLICIES', 'WEBSITES', 'ACCESS CONTROL', and 'ADVANCED'. The 'Services' page is active, showing a form to 'ADD NEW SERVICE' and a table of existing services. The table has columns for Name, Status, IP Address, Port, Domain, URL, Type, Mode, Policy, and Add. Two services are listed:

Name	Status	IP Address	Port	Domain	URL	Type	Mode	Policy	Add
default									
default									
BarracudaWAFStack	OK	172.31.30.135	80			HTTP	Passive	default	Server   Rule
Server_internal-Aut...	OK	172.31.23.161	80						

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.



The screenshot shows the Barracuda Web Application Firewall configuration interface. The top navigation bar includes tabs for BASIC, SECURITY POLICIES, WEBSITES, ACCESS CONTROL, and ADVANCED. The ADVANCED tab is selected, and the 'High Availability' sub-tab is active. The main content area is divided into three sections:

- CLUSTER SETTINGS:** Contains a 'Cluster Shared Secret' field with a masked password and a 'Help' link. A note below states: "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:** Contains a 'Peer IP Address' field and a 'Join Cluster' button. A note below states: "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:** Contains a table with columns for Hostname, IP Address, Identity, Serial#, Status, and Action. The table shows two systems: 'barracuda' (Self, Serial# 725498, Status Up) and 'barracuda' (Peer, Serial# 725496, Status Up). A 'Synchronize Configuration' button and a 'Help' link are also present.

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 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. Refer to step **6** to know 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

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

© Barracuda Networks Inc., 2020 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.