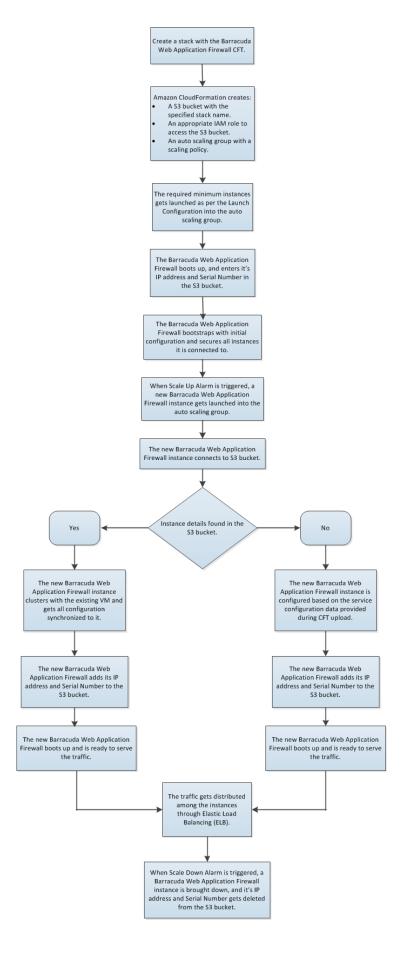# How Barracuda CloudFormation Template Works in PAYG/Hourly Instance

https://campus.barracuda.com/doc/46897285/

The following flowchart explains how the Barracuda CloudFormation Template works:

Barracuda Web Application Firewall

Create a stack with the Barracuda Web Application Firewall CFT.

Amazon CloudFormation creates:
- A S3 bucket with the specified stack name.
- An appropriate IAM role to access the S3 bucket.
- An auto scaling group with a scaling policy.

The required minimum instances gets launched as per the Launch Configuration into the auto scaling group.

The Barracuda Web Application Firewall boots up, and enters it's IP address and Serial Number in the S3 bucket.

The Barracuda Web Application Firewall bootstraps with initial configuration and secures all instances it is connected to.

When Scale Up Alarm is triggered, a new Barracuda Web Application Firewall instance gets launched into the auto scaling group.

The new Barracuda Web Application Firewall instance connects to S3 bucket.

Instance details found in the S3 bucket.

Yes

No

The new Barracuda Web Application Firewall instance clusters with the existing VM and gets all configuration synchronized to it.

The new Barracuda Web Application Firewall instance is configured based on the service configuration data provided during CFT upload.

The new Barracuda Web Application Firewall adds its IP address and Serial Number to the S3 bucket.

The new Barracuda Web Application Firewall adds its IP address and Serial Number to the S3 bucket.

The new Barracuda Web Application Firewall boots up and is ready to serve the traffic.

The new Barracuda Web Application Firewall boots up and is ready to serve the traffic.

The traffic gets distributed among the instances through Elastic Load Balancing (ELB).

When Scale Down Alarm is triggered, a Barracuda Web Application Firewall instance is brought down, and it's IP address and Serial Number gets deleted from the S3 bucket.

With regard to the flowchart, the following steps describe how a Barracuda CloudFormation Template works:

1. A CloudFormation Template (CFT) is uploaded and a stack is created on Amazon Web Services. With this:
    1. An Amazon S3 bucket gets created with the specified stack name and unique ID.
    2. An appropriate IAM role to access the S3 bucket is added.
2. The Barracuda Web Application Firewall VM(s) will be deployed and provisioned in the Virtual Private Cloud (VPC) specified while creating the stack.
3. After the Barracuda Web Application Firewall VM(s) is/are up and ready to serve the traffic:
    1. It checks the S3 bucket created in step **1 (a)** for any other existing VM(s) in this Auto Scaling group.
        1. If there is no VM data available in the S3 bucket, the VM is configured based on the service configuration data provided during CFT upload.
        2. If there is any VM information available in the S3 bucket, the VM clusters with the existing VM and gets all configuration synchronized to it.
    2. Adds its information to the S3 bucket created in **step 1 (a)**. Typically, an S3 bucket stores the instance data such as serial number and primary IP address (i.e., WAN IP address) of the deployed Barracuda Web Application Firewall VM(s).
4. The Barracuda Web Application Firewall is now ready to serve the traffic to the configured services.
5. If the instance encounters high traffic flow and triggers any of the created alarms, such as high bandwidth utilization, CPU usage, etc., then:
    1. A new Barracuda Web Application Firewall for AWS instance gets initiated automatically.
    2. Looks at the S3 bucket created in **step 1 (a)** and clusters with it.
    3. Adds its information to the S3 bucket, and is ready to serve the traffic.
    4. Traffic gets distributed among the instances through ELB.

Next Step

Continue with the [Importing the Barracuda Web Application Firewall PAYG CFT and Deploying the Instance](#) article to import the CFT and deploy the instance.

Barracuda Web Application Firewall

5 / 5

Figures

1. Auto scaling flow chart1.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.

How Barracuda CloudFormation Template Works in PAYG/Hourly Instance

5 / 5