Bring-Your-Own-License (BYOL) Auto Scaling

https://campus.barracuda.com/doc/68361421/

Refer to the article Pay-As-You-Go (PAYG)/Hourly Auto Scaling if you want to deploy the Hourly/PAYG Barracuda Web Application Firewall in the auto scaling model.

To deploy the **Bring-Your-Own-License** (**BYOL**) Barracuda Web Application Firewall in the auto-scaling model, follow the instructions in this article.

BYOL Auto Scaling CloudFormation Template (CFT)

Two types of auto-scaling deployments are supported for BYOL auto-scaling:

- Basic Bootstrapping
- Backup Bootstrapping

Basic Bootstrapping

In **Basic Bootstrapping**, the CFT deploys the Barracuda Web Application Firewall in the auto-scaling group and creates the service with the values provided while creating the stack. Use this mode of deployment if you are starting with your first deployment.The **Basic Bootstrapping CFT** is available on GitHub.

Backup Bootstrapping

In **Backup Bootstrapping** (deployment using the backup file), the service(s) and other configurations are restored from the specified backup file to the auto-scaling group. Use this deployment when you want to replicate the existing auto-scaling group for various reasons.

The **Backup Bootstrapping CFT** is available on GitHub.

Prerequisites

- Latest Barracuda Web Application Firewall CFT Template.
- Availability Zone(s), VPC ID, and subnet ID where you want to deploy the Barracuda Web

Application Firewall and protect your servers.
- Elastic Load Balancer to load balance the traffic between the deployed Barracuda Web Application Firewalls. For more information, see Elastic Load Balancing in the AWS documentation.
- S3 buckets:
  - **License S3 bucket**: The location where the license.json file needs to be created and saved. The license.json file contains the licenses that can be used. The file name should be “barracuda-byol-license-list.json”.
  - **Cluster S3 bucket**: The location where the clustering related information is stored.
  - **Backup S3 bucket** (Optional): This is required for backup-based bootstrapping. The configuration is restored from the selected backup.

    You can have a single bucket with sub-directories for each function, instead of three separate buckets for each function. It is also possible to use a single S3 bucket for all three functions. Any of these options can be chosen by providing the relevant inputs for each field when launching an instance.
- Create an IAM role to access the S3 buckets. See IAM Policy .

  The IAM role’s ARN should be used as the input value in the launch parameters .

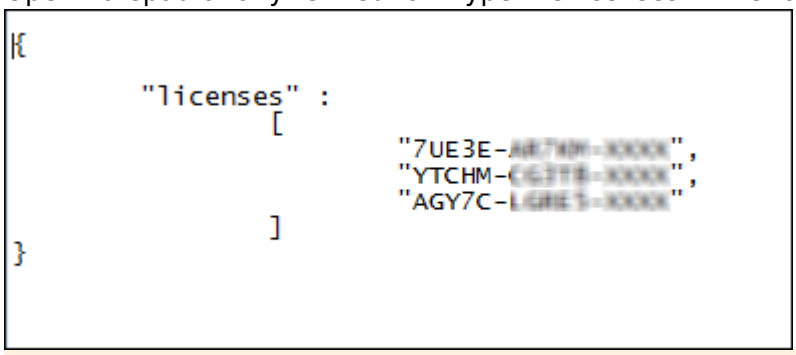
The BYOL Auto Scaling CloudFormation Template includes the following:

- **Stack Name**
  - **Stack name**: A name for the CloudFormation stack.
- **AWS Networking Configuration Details**
  - **VPC ID**: Select the VPC ID where the instance needs to be launched.
  - **Availability Zone(s):** Select the availability zone(s) of the VPC that needs to be used to launch the instance.
  - **Subnet ID(s)**: Select the subnet ID(s) that is assigned to the specified VPC.
  - **Elastic Load Balancer**: A preconfigured Elastic Load Balancer associated with the specified VPC and subnet.
- **AWS Auto scaling Configuration Details**
  - **Instance Type**: Instance type to be used in Amazon Web Services (AWS). Default: m3.medium
  - **Minimum instances**: The minimum number of Barracuda Web Application Firewall instances to be deployed initially to serve the web traffic. Default: 1
  - **Maximum Instances**: The maximum number of instances to be scaled up to handle the traffic whenever required. Default: 4
  - **Notification Email**: The email address to which the auto-scaling events need to be sent. Multiple email addresses can be specified with comma (,) as a delimiter without any space.
- **Barracuda Web Application Firewall BYOL License(s) Storage Details**
  - **License S3 Bucket**: This S3 bucket includes licensing-related information. Ensure this bucket is created before creating the stack for the auto-scaling group.
    - **licenses.json**: A license file contains the list of licenses that are used or uploaded by the administrator. This file should be created in the valid JSON format and should

be saved in the name " *barracuda-byol-license-list.json*.

Create a license file

1. Open notepad or any text editor. Type the licenses in the format illustrated below.



   It is recommended that you validate the JSON file using JSONLint or any other online validator before uploading the license file. The created WAF instances might fail during provisioning if the JSON file is not valid.
2. Save the license file. Note that you save the file with the name *barracuda-byol-license-list.json* as mentioned earlier.

Upload the license file

1. Upload the license file *barracuda-byol-license-list.json* to the **License S3 Bucket** you created.
   - **licenses.dat**: Contains all the available (unused) and used licenses. This file is generated by Barracuda when the stack is created. You should not edit or delete this file. Note that editing or deleting this file may affect your auto-scaling setup.
   - **license usage history file**: A log file that contains license usage activity by different instances whenever the instances are scaled up/down because of auto-scaling.
   - **License Sub Directory**: Folder in the S3 bucket from where the license can be read. Leave it blank if you do not have a folder.
- **Barracuda Web Application Firewall Bootstrapping Configuration Storage Details**
  - **Clustering S3 Bucket**: Provides details of instances that are in a cluster. A file is created for each instance with the serial number and primary IP address (i.e., WAN IP address) of the instance that is in a cluster.
  - **Bootstrapping S3 Bucket**: Contains the backup file(s) restored by the administrator.
  - **Bootstrapping Sub Directory**: Folder in the S3 bucket from where the bootstrapping configuration file can be read. Leave it blank if you do not have a folder.
- **Barracuda Web Application Firewall Bootstrapping Configuration**
  - **Default Domain**: Domain name that is used in the licensing. Use this format: example.com.
  - **Backup File Name**: The Barracuda Web Application Firewall configuration backup that needs to be restored on WAF for bootstrapping.
  - **Time Zone**: Select the time zone for the Barracuda Web Application Firewall.

- **NTP Servers**: NTP server IP or hostname. Multiple IPs/hostnames can be specified with comma (,) as a delimiter without any space.

  When launching a stack with backup-based bootstrapping CFT, you can either configure the NTP server from the CFT or use a backup that has the necessary NTP configured for bootstrapping. If you configure NTP in the CFT, and if the backup also has NTP configured, then the backup takes precedence over CFT. The bootstrapped instances are launched with the NTP configuration from the backup and not from the CFT.
  You can provide the NTP configuration as part of the user data in the CFT while launching the stack. Use the following syntax to add the NTP server configuration: ***--ntp "ip/Hostname,ip/hostname" (example --ntp test1.bc.com,test2.bc.com)***

- **Barracuda Web Application Firewall Proxy Server Configuration**
  - **Proxy Server IP**: The IP address or host name of the proxy server.
  - **Proxy Server Port**: The port (usually 8080) used for proxy client authentication.
  - **Proxy Server Username**: The proxy username (if any) assigned to the Barracuda Web Application Firewall.
  - **Proxy Server Password**: The proxy password (if any) assigned to the Barracuda Web Application Firewall.
- **AWS Identity & Access Management (IAM) Details**
  - **IAM Role Name**: IAM role name that has the permission to read/write the S3 bucket used for licensing, clustering, and bootstrapping.

To back up system configuration to Amazon S3 bucket, see the "Backing Up the Barracuda Web Application Firewall Instance(s) System Configuration in Amazon Web Services" section in the Backing Up and Restoring Your System Configuration article.

Default Values of the Barracuda Web Application Firewall BYOL CloudFormation Template

The following are the default values of the Barracuda Web Application Firewall BYOL CloudFormation Template (CFT). You can modify the values as needed.

- **Minimum Instances** - The minimum number of Barracuda Web Application Firewall instances to be deployed initially to serve the web traffic. Default: 1
- **Maximum Instances** - The maximum number of instances to be scaled up to handle the traffic whenever required. Default: 4
- **Instance Type** - Instance type to be used in Amazon Web Services (AWS). Default: m3.medium
- **Security Group** with the following ports opened:

Port	Protocol	Description
8000	TCP	Provides HTTP access to the Barracuda Web Application Firewall web interface.

8443	TCP	Provides HTTPS access to the Barracuda Web Application Firewall web interface.
8002	TCP	Required for clustering the instances and to auto scale the instances up/down.
32575	TCP	Required for clustering the instances and to auto scale the instances up/down.
32576	UDP	Required for clustering the instances and to auto scale the instances up/down.

- **Default Cool Down time** for scaling the instances up/down is set to 300 seconds.
- **Alarms** for CPU and Bandwidth. Note: These alarms are designed in such a way as to ensure that auto-scaling does not lead to instability. The alarms will scale up quickly and scale down slowly to ensure traffic to the site is not disrupted.

Alarm Type	Threshold Value (Average)	Action	Evaluation Periods
Network-In High Alarm	70% of max throughput for 5 minutes	Bring up one instance	5 minutes
Network-In Low Alarm	< 50% of max throughput for 1 hour 15 minutes	Bring down one instance	1 hour 15 minutes
Network-Out High Alarm	70% of max throughput for 5 minutes	Bring up one instance	5 minutes
Network-Out Low Alarm	< 50% of max throughput for 1 hour 15 minutes	Bring down one instance	1 hour 15 minutes
CPU High Alarm	> 85% for 5 minutes	Bring up one instance	5 minutes
CPU Normal Alarm	< 60% for 1 hour 15 minutes	Bring up one instance	1 hour 15 minutes

Figures

1. JsonLicenseFile.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.