Fortinet FortiGate Auto Scaling Baseline on the AWS Cloud

Quick Start Reference Deployment

December 2018

Jayden Liang, Daniel Chao, Jamie Pete, and Jun Kato, Fortinet, Inc.
Sameer Kumar Vasantapuram and Shivansh Singh, AWS

Contents
Quick Links ..................................................................................................................2
Overview .......................................................................................................................2
  Fortinet FortiGate Auto Scaling Baseline on AWS ......................................................3
  Costs and Licenses .....................................................................................................3
Architecture ..................................................................................................................4
Prerequisites ................................................................................................................6
  Specialized Knowledge ...............................................................................................6
Deployment Options ....................................................................................................6
Deployment Steps ........................................................................................................7
  Step 1. Prepare Your AWS Account ........................................................................7
  Step 2. Subscribe to the FortiGate AMI ...................................................................8
  Step 3. Launch the Quick Start ..............................................................................9
  Step 4. Test the Deployment ...................................................................................15
Fortinet FortiGate Auto Scaling Baseline Post-Deployment Steps on AWS ..................16
Troubleshooting .........................................................................................................20
GitHub Repository ......................................................................................................21
Additional Resources .................................................................................................21
This Quick Start was created by Fortinet in collaboration with Amazon Web Services (AWS).

Quick Starts are automated reference deployments that use AWS CloudFormation templates to deploy key technologies on AWS, following AWS best practices.

Quick Links

The links in this section are for your convenience. Before you launch the Quick Start, please review the architecture, security, and other considerations discussed in this guide.

- If you have an AWS account, and you’re already familiar with AWS services and Fortinet FortiGate Next-Generation Firewall technology, you can launch the Quick Start to build the architecture shown in Figure 1 in a new virtual private cloud (VPC). The deployment takes approximately 15 minutes. If you’re new to AWS or to FortiGate, please review the implementation details and follow the step-by-step instructions provided later in this guide.

- If you want to take a look under the covers, you can view the AWS CloudFormation templates that automate the deployment.

Overview

This Quick Start reference deployment guide provides step-by-step instructions for deploying Fortinet FortiGate Auto Scaling Baseline on the AWS Cloud.

This Quick Start is intended to be a baseline for users who are planning to implement or extend Fortinet’s Security Fabric workloads on the AWS Cloud, including IT infrastructure architects, administrators, and DevOps professionals.
Fortinet FortiGate Auto Scaling Baseline on AWS

FortiGate mid-range next-generation firewalls (NGFWs) provide high-performance, multi-layered advanced security, and better visibility to help protect against cyber attacks while reducing complexity. FortiGate firewalls are purpose-built with security processors to enable a high level of threat protection and performance for Secure Sockets Layer (SSL)-encrypted traffic.

By providing granular visibility of applications, users, and Internet of Things (IoT) devices, these firewalls are designed to identify issues quickly and intuitively. Fortinet security services from FortiGuard Labs provide continuous threat intelligence updates to help keep organizations protected from:

- Exploits and encrypted malware
- Malicious websites and botnets
- Ransomware and unknown attacks

FortiGate mid-range next-generation firewalls include:

- Top-rated security validated by NSS Labs, Virus Bulletin, and AV Comparatives
- Industry’s highest threat protection and SSL inspection performance
- Multi-layered security capabilities to reduce complexity
- Deep visibility and granular control of applications, users, and IoT devices
- Single-pane-of-glass view with centralized management and reporting
- An Auto Scaling group to provide highly efficient clustering at times of high workloads.

Multiple FortiGate instances can be scaled out automatically according to predefined workload levels. When a spike in traffic occurs, the Lambda script is invoked to scale out the group by automatically adding FortiGate instances. Auto Scaling is achieved by using FortiGate-native high availability features such as Config-Sync, which synchronizes operating system configurations across multiple FortiGate instances at the time of scale out events.

Costs and Licenses

You are responsible for the cost of the AWS services used while running this Quick Start reference deployment. There is no additional cost for using the Quick Start.

The AWS CloudFormation template for this Quick Start includes configuration parameters that you can customize. Some of these settings, such as instance type, will affect the cost of
deployment. For cost estimates, see the pricing pages for each AWS service you will be using. Prices are subject to change.

**Tip** After you deploy the Quick Start, we recommend that you enable the [AWS Cost and Usage Report](https://aws.amazon.com/cost-management/usage-reports/) to track costs associated with the Quick Start. This report delivers billing metrics to an S3 bucket in your account. It provides cost estimates based on usage throughout each month, and finalizes the data at the end of the month. For more information about the report, see the [AWS documentation](https://aws.amazon.com/documentation/cost-management/usage-reports/about/).

This Quick Start will launch FortiGate On-Demand instances, for which you will pay an hourly fee based on the Amazon Elastic Compute Cloud (Amazon EC2) instance type.

**Architecture**

Deploying this Quick Start for a new or an existing virtual private cloud (VPC) with default parameters builds the following Fortinet FortiGate Auto Scaling Baseline environment in the AWS Cloud.
Figure 1: Quick Start architecture for Fortinet’s FortiGate Auto Scaling Baseline on AWS

The Quick Start uses AWS CloudFormation templates to set up the following:

- A highly available architecture that spans two Availability Zones.*
- A virtual private cloud (VPC) configured with public and private subnets according to AWS best practices, to provide you with your own virtual network on AWS.*
- An internet gateway to allow access to the internet.*
- In the public subnets, FortiGates that act as NAT gateways, allowing outbound internet access for resources in the private subnets.*
- In the public subnets, a FortiGate host in an Auto Scaling group complements AWS security groups to provide intrusion protection, web filtering, and threat detection to
help protect your services from cyber attacks. It also allows virtual private network (VPN) access by authorized users.

- An externally facing Network Load Balancer. An internally facing Network Load Balancer is optional.

- Amazon API Gateway, which acts as a front door by providing a callback URL for the FortiGate Auto Scaling group. FortiGates use API Gateway to send API calls and to process FortiGate Config-Sync tasks to synchronize operating system configuration across multiple FortiGate instances at the time of the Auto Scaling scale out event. This is currently only for internal use in the VPC. There is no public access available.

- AWS Lambda, which allows you to run certain scripts and code without provisioning servers. Fortinet provides Lambda scripts for running Auto Scaling. Lambda functions are used to handle Auto Scaling, failover management, AWS CloudFormation deployment, and configuration for other related components.

- An Amazon DynamoDB database that uses Fortinet-provided scripts to store information about Auto Scaling condition states.

**Prerequisites**

**Specialized Knowledge**

Before you deploy this Quick Start, we recommend that you become familiar with the following AWS services. (If you are new to AWS, see [Getting Started with AWS](#).)

- **Amazon Elastic Cloud Compute (Amazon EC2)**
- **Amazon EC2 Auto Scaling**
- **Amazon VPC**
- **AWS CloudFormation**
- **AWS Lambda**
- **Amazon DynamoDB**
- **Amazon API Gateway**

**Deployment Options**

This Quick Start provides two deployment options:

- Deploy Fortinet FortiGate Auto Scaling Baseline into a new VPC (end-to-end deployment). This option builds a new AWS environment consisting of the VPC,
subnets, FortiGates, security groups, and other infrastructure components, and then deploys Fortinet FortiGate Auto Scaling Baseline into this new VPC.

- Deploy Fortinet FortiGate Auto Scaling Baseline into an existing VPC. This option provisions Fortinet FortiGate Auto Scaling Baseline in your existing AWS infrastructure.

  **Note**  
  Incoming requests to the web servers in the private subnets present in your existing VPC will go through a connection that flows through the internet gateway, Network Load Balancer, and the FortiGate Auto Scaling group before reaching the web server. The web server returns the response using the same connection.

  Outgoing requests from the web servers go through the individual FortiGate NAT gateway and the internet gateway to the external network. The external network returns the response using the same path.

  Ensure that you remove any existing NAT device routes from existing route tables associated with the private subnets. The Quick Start will automatically attach a proper route (as described above) to the route table.

The Quick Start provides separate templates for these options. It also lets you configure CIDR blocks, instance types, and FortiGate settings, as discussed later in this guide.

**Deployment Steps**

**Step 1. Prepare Your AWS Account**

1. If you don’t already have an AWS account, create one at [https://aws.amazon.com](https://aws.amazon.com) by following the on-screen instructions.

2. Use the region selector in the navigation bar to choose the AWS Region where you want to deploy Fortinet FortiGate Auto Scaling Baseline on AWS.

   **Note**  
   The c5.large instance type is not compatible with the Asia Pacific (Sydney) Region (ap-southeast-2). The Fortinet FortiGate Auto Scaling Baseline solution is also not compatible with Availability Zone B in the South America (São Paolo) Region (sa-east-1).

3. Create a [key pair](https://aws.amazon.com) in your preferred region.

4. If necessary, [request a service limit increase](https://aws.amazon.com). You might need to do this if you encounter an issue where you exceed the [default limit](https://aws.amazon.com) with this deployment. The default instance type is c5.large.
Step 2. Subscribe to the FortiGate AMI

This Quick Start uses AWS Marketplace software from Fortinet and requires that you accept the terms within the AWS account where the Quick Start will be deployed.

2. Open the page for the Fortinet FortiGate Next-Generation Firewall AMI.
3. Choose **Continue to Subscribe**.

![Figure 2: Continue to subscribe in AWS Marketplace](image)

4. Choose **Accept Terms** for subscribing to the software. For detailed subscription instructions, see the AWS Marketplace documentation.

![Figure 3: Accepting terms in AWS Marketplace](image)
5. When the subscription process is complete, exit out of AWS Marketplace without further action. **Do not** provision the software from AWS Marketplace—the Quick Start will deploy the AMI for you.

**Step 3. Launch the Quick Start**

**Note**  You are responsible for the cost of the AWS services used while running this Quick Start reference deployment. The FortiGate Auto Scaling Baseline Quick Start deployment will launch On-Demand EC2 instances. There is no additional cost for using this Quick Start. For full details, see the pricing pages for each AWS service you will be using in this Quick Start. Prices are subject to change.

1. Choose one of the following options to launch the AWS CloudFormation template into your AWS account.

<table>
<thead>
<tr>
<th>Option 1</th>
<th>Option 2</th>
</tr>
</thead>
<tbody>
<tr>
<td>Deploy Fortinet FortiGate Auto Scaling Baseline into a new VPC on AWS</td>
<td>Deploy Fortinet FortiGate Auto Scaling Baseline into an existing VPC on AWS</td>
</tr>
</tbody>
</table>

   Each deployment takes about 15 minutes to complete.

2. Check the region that's displayed in the upper-right corner of the navigation bar, and change it if necessary. This is where the network infrastructure for Fortinet FortiGate Auto Scaling Baseline will be built. The template is launched in the US East (Ohio) Region by default.

3. On the **Select Template** page, keep the default setting for the template URL, and then on the lower left choose **Next**.

4. On the **Specify Details** page, change the stack name if needed. Review the parameters for the template. Provide values for the parameters that require input. For all other parameters, review the default settings and customize them as necessary. When you finish reviewing and customizing the parameters, choose **Next**.

In the following tables, parameters are listed by category and described separately for the two deployment options:

- Parameters for deploying Fortinet FortiGate Auto Scaling Baseline into a new VPC
- Parameters for deploying Fortinet FortiGate Auto Scaling Baseline into an existing VPC
### Option 1: Parameters for deploying Fortinet FortiGate Auto Scaling Baseline into a new VPC

**View template**

**Network configuration:**

<table>
<thead>
<tr>
<th>Parameter label (name)</th>
<th>Default</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Availability Zones (AvailabilityZones)</td>
<td>Requires input</td>
<td>The list of Availability Zones to use for the subnets in the VPC. The Quick Start uses two Availability Zones from your list and preserves the logical order you specify.</td>
</tr>
<tr>
<td>VPC CIDR (VPCCIDR)</td>
<td>10.0.0.0/16</td>
<td>The CIDR block for the VPC.</td>
</tr>
<tr>
<td>Public subnet 1 CIDR (PublicSubnet1CIDR)</td>
<td>10.0.0.0/24</td>
<td>The CIDR block for the public (DMZ) subnet located in Availability Zone 1.</td>
</tr>
<tr>
<td>Public subnet 2 CIDR (PublicSubnet2CIDR)</td>
<td>10.0.2.0/24</td>
<td>The CIDR block for the public (DMZ) subnet located in Availability Zone 2.</td>
</tr>
<tr>
<td>Private subnet 1 CIDR (PrivateSubnet1CIDR)</td>
<td>10.0.1.0/24</td>
<td>The CIDR block for the private subnet located in Availability Zone 1.</td>
</tr>
<tr>
<td>Private subnet 2 CIDR (PrivateSubnet2CIDR)</td>
<td>10.0.3.0/24</td>
<td>The CIDR block for the private subnet located in Availability Zone 2.</td>
</tr>
</tbody>
</table>

**FortiGate configuration:**

<table>
<thead>
<tr>
<th>Parameter label (name)</th>
<th>Default</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Resource name prefix (CustomIdentifier)</td>
<td>fgtASG</td>
<td>A custom identifier as resource name prefix. Must be at most 10 characters long and only contain uppercase, lowercase letters, and numbers. Maximum length is 10.</td>
</tr>
<tr>
<td>Instance type (FortiGateInstanceType)</td>
<td>c5.large</td>
<td>Instance type to launch as FortiGate On-Demand instances. There are t2.small and compute-optimized instances such as c4 and c5 available with different vCPU sizes and bandwidths. For more information about instance types, see [<a href="https://aws.amazon.com/ec2(instance-types/">https://aws.amazon.com/ec2(instance-types/</a>](<a href="https://aws.amazon.com/ec2(instance-types/)">https://aws.amazon.com/ec2(instance-types/)</a>.</td>
</tr>
<tr>
<td>FortiGate PSK secret (FortiGatePskSecret)</td>
<td>Requires input</td>
<td>A secret key for the FortiGate instances to securely communicate with each other. It can be of your choice of a string, such as numbers or letters or the combination of them. Maximum length is 128.</td>
</tr>
<tr>
<td>Admin port (FortiGateAdminPort)</td>
<td>8443</td>
<td>A port number for FortiGate administration. Minimum is 1. Maximum is 65535. Do not use: 443, 541, 514, or 703 because these are FortiGate reserved ports.</td>
</tr>
<tr>
<td>Admin CIDR block (FortiGateAdminCidr)</td>
<td>Requires input</td>
<td>CIDR block for external admin management access. <strong>Warning:</strong> 0.0.0.0/0 accepts connections from any IP address. We recommend that</td>
</tr>
</tbody>
</table>
you use a constrained CIDR range to reduce the potential of inbound attacks from unknown IP addresses.

**Key pair name** *(KeyPairName)*  
*Requires input*  
Amazon EC2 Key Pair for admin access.

---

**FortiGate Auto Scaling group configuration:**

<table>
<thead>
<tr>
<th>Parameter label (name)</th>
<th>Default</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Instance lifecycle expiry</strong> <em>(ExpireLifecycleEntry)</em></td>
<td>300</td>
<td>FortiGate instance lifecycle expiry entry (in seconds). Minimum is 60. Maximum is 3600.</td>
</tr>
<tr>
<td><strong>Desired capacity</strong> <em>(FortiGateAsgDesiredCapacity)</em></td>
<td>2</td>
<td>The number of FortiGate instances the group should have at any time, also called desired capacity. Must keep at least 2 FortiGates in the group for High Availability. Minimum is 2.</td>
</tr>
<tr>
<td><strong>Minimum group size</strong> <em>(FortiGateAsgMinSize)</em></td>
<td>2</td>
<td>Minimum number of FortiGate instances in the Auto-Scaling Group. Minimum is 2.</td>
</tr>
<tr>
<td><strong>Maximum group size</strong> <em>(FortiGateAsgMaxSize)</em></td>
<td>4</td>
<td>Maximum number of FortiGate instances in the Auto-Scaling Group. Minimum is 2.</td>
</tr>
<tr>
<td><strong>Health check grace period</strong> <em>(FortiGateAsgHealthCheckGracePeriod)</em></td>
<td>300</td>
<td>The length of time (in seconds) that Auto-Scaling waits before checking an instance’s health status. Minimum is 60.</td>
</tr>
<tr>
<td><strong>Scaling cooldown period</strong> <em>(FortiGateAsgCooldown)</em></td>
<td>300</td>
<td>Auto-Scaling group waits for the cooldown period (in seconds) to complete before resuming scaling activities. Minimum is 60. Maximum is 3600.</td>
</tr>
<tr>
<td><strong>Scale-out threshold</strong> <em>(FortiGateAsgScaleOutThreshold)</em></td>
<td>80</td>
<td>The threshold (in percentage) for the FortiGate Auto-Scaling group to scale out (add) 1 instance. Minimum is 1. Maximum is 100.</td>
</tr>
<tr>
<td><strong>Scale-in threshold</strong> <em>(FortiGateAsgScaleInThreshold)</em></td>
<td>25</td>
<td>The threshold (in percentage) for the FortiGate Auto-Scaling group to scale in (remove) 1 instance. Minimum is 1. Maximum is 100.</td>
</tr>
<tr>
<td><strong>Healthy threshold</strong> <em>(FortiGateElbTgHealthyThreshold)</em></td>
<td>3</td>
<td>The number of consecutive health check failures required before considering a FortiGate instance unhealthy. Minimum is 3.</td>
</tr>
</tbody>
</table>
Load balancing configuration:

<table>
<thead>
<tr>
<th>Parameter label (name)</th>
<th>Default</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Internal ELB options</strong></td>
<td>add a new internal load</td>
<td>Options for add an optional pre-defined load balancer to route traffic to web service in the private subnets. You can optionally use your own one or decide to not need one.</td>
</tr>
<tr>
<td>(InternalLoadBalancingOptions)</td>
<td>balancer</td>
<td></td>
</tr>
<tr>
<td><strong>Internal ELB DNS name</strong></td>
<td>Requires input</td>
<td>(Optional) DNS Name of the Elastic Load Balancer which is used in the private subnets. Specify if only you use your own one.</td>
</tr>
<tr>
<td>(InternalLoadBalancerDnsName)</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Web service traffic port</strong></td>
<td>443</td>
<td>Balance web service traffic over this port if the internal web-service load balancer is enabled. Minimum is 1. Maximum is 65535.</td>
</tr>
<tr>
<td>(BalanceWebTrafficOverPort)</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

AWS Quick Start configuration:

<table>
<thead>
<tr>
<th>Parameter label (name)</th>
<th>Default</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Quick Start S3 bucket name</strong></td>
<td>aws-quickstart</td>
<td>The S3 bucket you have created for your copy of Quick Start assets, if you decide to customize or extend the Quick Start for your own use. The bucket name can include numbers, lowercase letters, uppercase letters, and hyphens, but should not start or end with a hyphen.</td>
</tr>
<tr>
<td>(QSS3BucketName)</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Quick Start S3 key prefix</strong></td>
<td>quickstart-fortinet-</td>
<td>The S3 key name prefix used to simulate a folder for your copy of Quick Start assets, if you decide to customize or extend the Quick Start for your own use. This prefix can include numbers, lowercase letters, uppercase letters, hyphens, and forward slashes.</td>
</tr>
<tr>
<td>(QSS3KeyPrefix)</td>
<td>fortigate/</td>
<td></td>
</tr>
</tbody>
</table>

- **Option 2: Parameters for deploying Fortinet FortiGate Auto Scaling Baseline into an existing VPC**

  View template

Network configuration:

<table>
<thead>
<tr>
<th>Parameter label (name)</th>
<th>Default</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>VPC ID</strong></td>
<td>Requires input</td>
<td>The existing VPC IDs where you deploy the Auto-Scaling group and related resources. The VPC must have the option DNS hostnames enabled.</td>
</tr>
<tr>
<td>(VpcId)</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>VPC CIDR</strong></td>
<td>Requires input</td>
<td>The CIDR block for the selected VPC.</td>
</tr>
<tr>
<td>(VPCCIDR)</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>FortiGate subnet 1</strong></td>
<td>Requires input</td>
<td>Public (DMZ) subnet 1, which is located in Availability Zone 1.</td>
</tr>
<tr>
<td>(PublicSubnet1)</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>FortiGate subnet 2</strong></td>
<td>Requires input</td>
<td>Public (DMZ) subnet 2, which is located in Availability Zone 2.</td>
</tr>
<tr>
<td>(PublicSubnet2)</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Protected subnet 1</strong></td>
<td>Requires input</td>
<td>Private subnet, which is located in Availability Zone 1.</td>
</tr>
<tr>
<td>(PrivateSubnet1)</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Protected subnet 2 (PrivateSubnet2)  
**Requires input**  
Private subnet, which is located in Availability Zone 2.

Route table 1 ID (PrivateSubnet1RouteTable)  
**Requires input**  
Route table ID associated with the private subnet 1.

Route table 2 ID (PrivateSubnet2RouteTable)  
**Requires input**  
Route table ID associated with the private subnet 2.

**FortiGate configuration:**

<table>
<thead>
<tr>
<th>Parameter label (name)</th>
<th>Default</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Resource name prefix (CustomIdentifier)</td>
<td>fgtASG</td>
<td>A custom identifier as resource name prefix. Must be at most 10 characters long and only contain uppercase, lowercase letters, and numbers. Maximum length is 10.</td>
</tr>
<tr>
<td>Instance type (FortiGateInstanceType)</td>
<td>c5.large</td>
<td>Instance type to launch as FortiGate On-Demand instances. There are t2, small and compute-optimized instances such as c4 and c5 available with different vCPU sizes and bandwidths. For more information about instance types, see <a href="https://aws.amazon.com/ec2/instance-types/">https://aws.amazon.com/ec2/instance-types/</a>.</td>
</tr>
<tr>
<td>FortiGate PSK secret (FortiGatePskSecret)</td>
<td>Requires input</td>
<td>A secret key for the FortiGate instances to securely communicate with each other. It can be of your choice of a string, such as numbers or letters or the combination of them. Maximum length is 128.</td>
</tr>
<tr>
<td>Admin port (FortiGateAdminPort)</td>
<td>8443</td>
<td>A port number for FortiGate administration. Minimum is 1. Maximum is 65535. Do not use: 443, 541, 514, 703 because these are FortiGate reserved ports.</td>
</tr>
<tr>
<td>Admin CIDR block (FortiGateAdminCidr)</td>
<td>Requires input</td>
<td>CIDR block for external admin management access. <strong>Warning:</strong> 0.0.0.0/0 accepts connections from any IP address. We recommend that you use a constrained CIDR range to reduce the potential of inbound attacks from unknown IP addresses.</td>
</tr>
<tr>
<td>Key pair name (KeyPairName)</td>
<td>Requires input</td>
<td>Amazon EC2 Key Pair for admin access.</td>
</tr>
</tbody>
</table>

**FortiGate Auto Scaling group configuration:**

<table>
<thead>
<tr>
<th>Parameter label (name)</th>
<th>Default</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Instance lifecycle expiry (ExpireLifecycleEntry)</td>
<td>300</td>
<td>FortiGate instance lifecycle expiry entry (in seconds). Minimum is 60. Maximum is 3600.</td>
</tr>
<tr>
<td>Desired capacity (FortiGateAsgDesiredCapacity)</td>
<td>2</td>
<td>The number of FortiGate instances the group should have at any time, also called desired capacity. Must keep at least 2 FortiGates in the group for High Availability. Minimum is 2.</td>
</tr>
<tr>
<td>Minimum group size (FortiGateAsgMinSize)</td>
<td>2</td>
<td>Minimum number of FortiGate instances in the Auto-Scaling Group. Minimum is 2.</td>
</tr>
<tr>
<td>Maximum group size (FortiGateAsgMaxSize)</td>
<td>4</td>
<td>Maximum number of FortiGate instances in the Auto-Scaling Group. Minimum is 2.</td>
</tr>
</tbody>
</table>
5. On the Options page, you can specify the following:
   - **Tags** (key-value pairs) for resources in your stack
- An **IAM role** that AWS CloudFormation uses to create, modify, or delete resources in your stack
- **Rollback triggers** that enable AWS CloudFormation to monitor the state of your application during stack creation
- **Advanced options**

When you’re done, choose **Next**.

6. On the **Review** page, review and confirm the template settings. Under **Capabilities**, select the check box to acknowledge that the template will create IAM resources.

7. Choose **Create** at the lower right to deploy the stack.

8. Monitor the status of the stack. When the status is **CREATE_COMPLETE**, the deployment is complete.

9. Use the URLs displayed in the **Outputs** tab for the stack to view the resources that were created.

**Step 4. Test the Deployment**

Fortinet FortiGate Auto Scaling Baseline creates an Auto Scaling group with lifecycle events attached to the group.

To test the deployment, follow these steps:

1. Check that an Auto Scaling group (the name starting with `fgtASG` by default or the prefix you specified in **Resource name prefix**) was created after completion of the CloudFormation stack.

   ![Figure 4: Auto Scaling group in AWS management console](image)

2. Navigate to the **Scaling Policies** tab of the Auto Scaling group, and execute a scale out action.
Figure 5: Execute a scale out action in AWS management console

The scale out action should trigger a lifecycle event for instantiating a FortiGate instance.

Figure 6: A scale out action added one FortiGate instance

3. Follow step 1 for a similar scale in action. Note that you must wait 300 seconds, as specified in the Scaling Cooldown period, between scale out and scale in actions.

Fortinet FortiGate Auto Scaling Baseline Post-Deployment Steps on AWS

Connect to FortiGate-VM:

1. To connect to the FortiGate-VM, you need the primary FortiGate-VM’s public DNS address. First, determine which instance is the primary FortiGate. Go to DynamoDB. In the region where you deployed the stack, go to Tables and search for the custom identifier that you provided when deploying the template in CloudFormation. In Figure 7, the custom identifier is fgtASG.

2. Click the table with FortiGateMasterElection in its name. On the Items tab, find the primary FortiGate’s instance ID and IP address.
Figure 7: Primary FortiGate instance ID and IP address

3. In the EC2 Management Console, select **Instances** and look at the **Public DNS (IPv4)** field in the lower pane for the primary FortiGate.

Figure 8: FortiGate public DNS on EC2 Management Console

**Note** If you do not see the DNS address, you may need to enable DNS host management on your VPC. In this case, go to the VPC Management Console and select the desired VPC from **Your VPCs**. From the **Action** dropdown menu, select **Edit DNS Hostnames**. Select **Yes**, and then **Save**.

4. Open an HTTPS session using the public DNS address of the FortiGate-VM in your browser (https://<public DNS>: 8443).
You will see a certificate error message from your browser, which is normal because the default FortiGate certificate is self-signed and isn’t recognized by browsers. Proceed past this error. At a later time, you can upload a publicly signed certificate to avoid this error.

5. Log in to the FortiGate-VM with the default user name `admin` and the default password `<InstanceID>`.

![FortiGate initial login screen](image)

**Figure 9: FortiGate initial login screen**

You will be prompted to change the default password at the first-time login.

![FortiGate default password change](image)

**Figure 10: FortiGate default password change**

**Note** When you change the primary FortiGate’s password, the new password is synced to all FortiGates in the Auto Scaling group. Any attempt to change the password on a secondary FortiGate is overwritten with the primary FortiGate’s password.
6. You will now see the FortiGate-VM dashboard. Depending on your license type, the information in the license widget on the dashboard may vary.

![FortiGate dashboard](image)

**Figure 11: FortiGate dashboard**

7. Choose **Network**, choose **Interfaces**, and edit the interfaces depending on your requirements. If the IP address or subnet mask is missing for **port1** or **port2**, configure these values.

![FortiGate Network Interfaces page](image)

**Figure 12: FortiGate Network Interfaces page**
Troubleshooting

If you encountered a CREATE_FAILED error when you launch the Quick Start, we recommend that you relaunch the template with Rollback on failure set to No. (This setting is under Advanced in the AWS CloudFormation console, Options page.) With this setting, the stack’s state will be retained and the instance will be left running, so you can troubleshoot the issue.
Important  When you set **Rollback on failure** to **No**, you will continue to incur AWS charges for this stack. Please make sure to delete the stack when you finish troubleshooting.

For additional information, see [Troubleshooting AWS CloudFormation](https://aws.amazon.com/documentation/cloudformation/) on the AWS website or contact us on the AWS Quick Start Discussion Forum.

**GitHub Repository**

You can visit our [GitHub repository](https://github.com/aws-quick-start) to download the templates and scripts for this Quick Start, to post your comments, and to share your customizations with others.

**Additional Resources**

**AWS services**

- Amazon EBS
- Amazon EC2
  [https://aws.amazon.com/documentation/ec2/](https://aws.amazon.com/documentation/ec2/)
- Amazon VPC
  [https://aws.amazon.com/documentation/vpc/](https://aws.amazon.com/documentation/vpc/)
- AWS CloudFormation
  [https://aws.amazon.com/documentation/cloudformation/](https://aws.amazon.com/documentation/cloudformation/)

**Fortinet FortiGate documentation**

- FortiGate FortiOS handbook
  [https://docs.fortinet.com/d/fortigate-pdf-handbook-60](https://docs.fortinet.com/d/fortigate-pdf-handbook-60)
- FortiGate quick deployment
  [https://docs2.fortinet.com/vm/aws/fortigate/6.0/about-fortigate-for-aws/](https://docs2.fortinet.com/vm/aws/fortigate/6.0/about-fortigate-for-aws/)
- FortiGate-VM datasheets
  [https://www.fortinet.com/content/dam/fortinet/assets/data-sheets/FortiGate_VM.pdf](https://www.fortinet.com/content/dam/fortinet/assets/data-sheets/FortiGate_VM.pdf)

**Quick Start reference deployments**

- AWS Quick Start home page
  [https://aws.amazon.com/quickstart/](https://aws.amazon.com/quickstart/)
Document Revisions

<table>
<thead>
<tr>
<th>Date</th>
<th>Change</th>
<th>In sections</th>
</tr>
</thead>
<tbody>
<tr>
<td>December 2018</td>
<td>Initial draft</td>
<td>—</td>
</tr>
</tbody>
</table>

© 2018, Amazon Web Services, Inc. or its affiliates, and Fortinet, Inc. All rights reserved.

Notices

This document is provided for informational purposes only. It represents AWS’s current product offerings and practices as of the date of issue of this document, which are subject to change without notice. Customers are responsible for making their own independent assessment of the information in this document and any use of AWS’s products or services, each of which is provided “as is” without warranty of any kind, whether express or implied. This document does not create any warranties, representations, contractual commitments, conditions or assurances from AWS, its affiliates, suppliers or licensors. The responsibilities and liabilities of AWS to its customers are controlled by AWS agreements, and this document is not part of, nor does it modify, any agreement between AWS and its customers.

The software included with this paper is licensed under the Apache License, Version 2.0 (the "License"). You may not use this file except in compliance with the License. A copy of the License is located at http://aws.amazon.com/apache2.0/ or in the "license" file accompanying this file. This code is distributed on an "AS IS" BASIS, WITHOUT WARRANTIES OR CONDITIONS OF ANY KIND, either express or implied. See the License for the specific language governing permissions and limitations under the License.