FortiOS - Deploying Auto Scaling on AWS

Version 6.0 and 6.2

FORTINET DOCUMENT LIBRARY
https://docs.fortinet.com

FORTINET VIDEO GUIDE
https://video.fortinet.com

FORTINET BLOG
https://blog.fortinet.com

CUSTOMER SERVICE & SUPPORT
https://support.fortinet.com

FORTINET TRAINING & CERTIFICATION PROGRAM
https://www.fortinet.com/support-and-training/training.html

NSE INSTITUTE
https://training.fortinet.com

FORTIGUARD CENTER
https://fortiguard.com/

END USER LICENSE AGREEMENT
https://www.fortinet.com/doc/legal/EULA.pdf

FEEDBACK
Email: techdoc@fortinet.com

September 25, 2019
FortiOS 6.0 and 6.2 Deploying Auto Scaling on AWS
01-620-544190-20190925

TABLE OF CONTENTS

Deploying auto scaling on AWS

You can deploy FortiGate-VM to support Auto Scaling on AWS. This requires a manual deployment incorporating CloudFormation Templates (CFTs).

Multiple FortiGate-VM instances form an Auto Scaling group (ASG) to provide highly efficient clustering at times of high workloads. FortiGate-VM instances can be scaled out automatically according to predefined workload levels. When a spike in traffic occurs, a Lambda script is invoked to scale out the ASG by automatically adding FortiGate-VM instances. Auto Scaling is achieved by using FortiGate-native High Availability (HA) features such as `config-sync`, which synchronizes operating system (OS) configurations across multiple FortiGate-VM instances at the time of scale-out events.

FortiGate Autoscale for AWS is available with FortiOS 6.0.6 and later versions as well as with FortiOS 6.2.1 and later versions and supports On-Demand (PAYG) instances.

Before you deploy FortiGate Autoscale for AWS, it is recommended that you become familiar with the following AWS services. If you are new to AWS, see Getting Started.

- Amazon Elastic Cloud Compute (Amazon EC2)
- Amazon EC2 Auto Scaling
- Amazon VPC
- AWS CloudFormation
- AWS Lambda
- Amazon DynamoDB
- Amazon API Gateway
- Amazon CloudWatch
- Amazon S3

FortiGate Autoscale for AWS uses AWS CFTs to deploy the following components:

- A highly available architecture that spans two Availability Zones (AZs)
- 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, FortiGate-VMs that act as NAT gateways, allowing outbound Internet access for resources in the private subnets
- In the public subnets, a FortiGate-VM host in an Auto Scaling group complements AWS security groups to provide intrusion protection, web filtering, and threat detection to protect your services from cyber-attacks. It also allows VPN access by authorized users.
- An external facing network load balancer is created as part of the deployment process. An internal facing network load balancer is optional.
- Amazon API Gateway, which acts as a front door by providing a callback URL for the FortiGate-VM ASG. FortiGate-VMs use an API Gateway to send API calls and to process FortiGate `config-sync` tasks to synchronize OS configuration across multiple FortiGate-VM instances at the time of the Auto Scaling scale-out event. This is currently only for internal use. 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

Acronyms

The following acronyms are used throughout this document.

Acronym	Expansion
ASG	Auto Scaling group
CFT	CloudFormation templates
CIDR	Classless Inter-Domain Routing
DMZ	Demilitarized Zone
ELB	Elastic Load Balancer
FGT	FortiGate
PAYG	Pay As You Go

Planning

Deploying FortiGate Autoscale for AWS requires the use of deployment templates. There are two types of templates:

- *Entry template*. This template could run as the entry point of a deployment.
- *Dependency template*. This template is automatically run by the deployment process as a Nested Stack. It cannot be run as an entry template. A dependency template is run based on user selected options.

Template	Type	Description
workload-master.template	Entry template	Deploys the Auto Scaling solution to a new VPC.
workload.template	Entry template	Deploys the Auto Scaling solution to an existing VPC.
nic-attachment.template	Dependency template	Deploys the secondary network interface controller attachment handler.
create-nat-fgt-master.template	Dependency template	Deploys FortiGate-VMs as NAT Gateways.
create-fortigate.template	Dependency template	Deploys a single FortiGate-VM instance for a certain purpose.
create-fortianalyzer.template	Dependency template	Deploys a single FortiAnalyzer instance for a certain purpose.
create-db-table.template	Dependency template	Deploys related DynamoDB tables.
copy-objects.template	Dependency template	Copies S3 objects to the deployment related S3 bucket.

All template files are included in the deployment package for FortiGate Autoscale for AWS.

Prerequisites

Installing and configuring FortiGate Autoscale for AWS requires knowledge of the following:

- Configuring a FortiGate using the CLI
- AWS CloudFormation templates
- AWS Lambda Function

It is expected that FortiGate Autoscale for AWS will be deployed by DevOps engineers or advanced system administrators who are familiar with the above.

Before starting the deployment, the following steps must be carried out:

1. Log into your AWS account. If you do not already have one, create one 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 FortiGate Autoscale for AWS.

The *c5.large* instance type is not compatible with the Asia Pacific (Sydney) Region (ap-southeast-2).

FortiGate Autoscale for AWS is also not compatible with Availability Zone B in the South America (São Paulo) region (sa-east-1).

3. Create a key pair in your preferred region.
4. If necessary, request a service limit increase. You may need to do this if you encounter an issue where you exceed the default limit with this deployment. The default instance type is *c5.large*.

Deployment options

FortiGate Autoscale for AWS provides two deployment options:

- *Deployment into a new VPC (end-to-end deployment)*. This option builds a new AWS environment consisting of the VPC, subnets, FortiGate-VMs, security groups, and other infrastructure components, and then deploys FortiGate Autoscale for AWS into this new VPC.
- *Deployment into an existing VPC*. This option provisions FortiGate Autoscale for AWS in your existing AWS infrastructure.

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-VM ASG 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-VM 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. FortiGate Autoscale for AWS automatically attaches a proper route to the route table, as described above.

FortiGate Autoscale for AWS provides separate CFTs for these options. It also allows you to configure CIDR blocks, instance types, and FortiGate settings.

Obtaining the deployment package

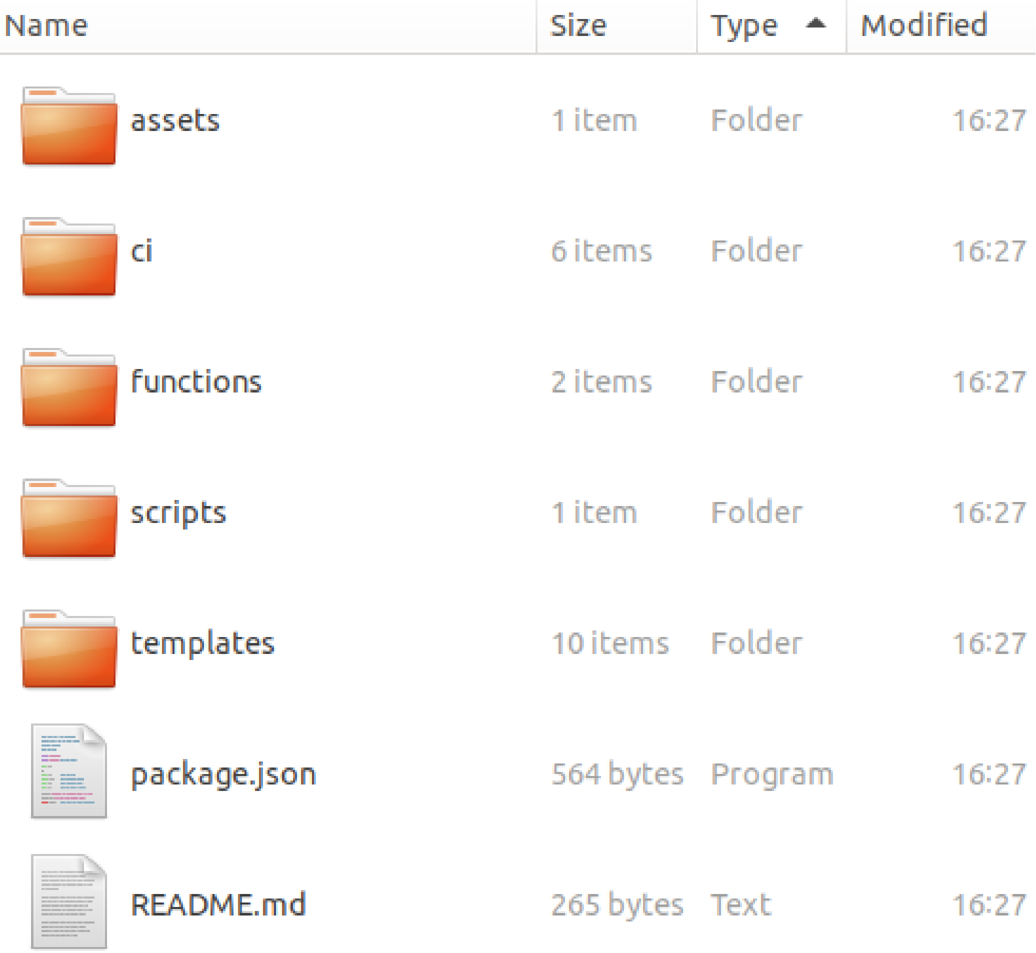
The FortiGate Autoscale for AWS deployment package is located in the Fortinet GitHub project.

To obtain the package:

1. Visit the FortiGate Autoscale GitHub project release page and download the `fortigate-autoscale-aws-cloudformation.zip` for the *1.0.x* version.

   This documentation is for *Version 1.0.x* which only supports PAYG instances.

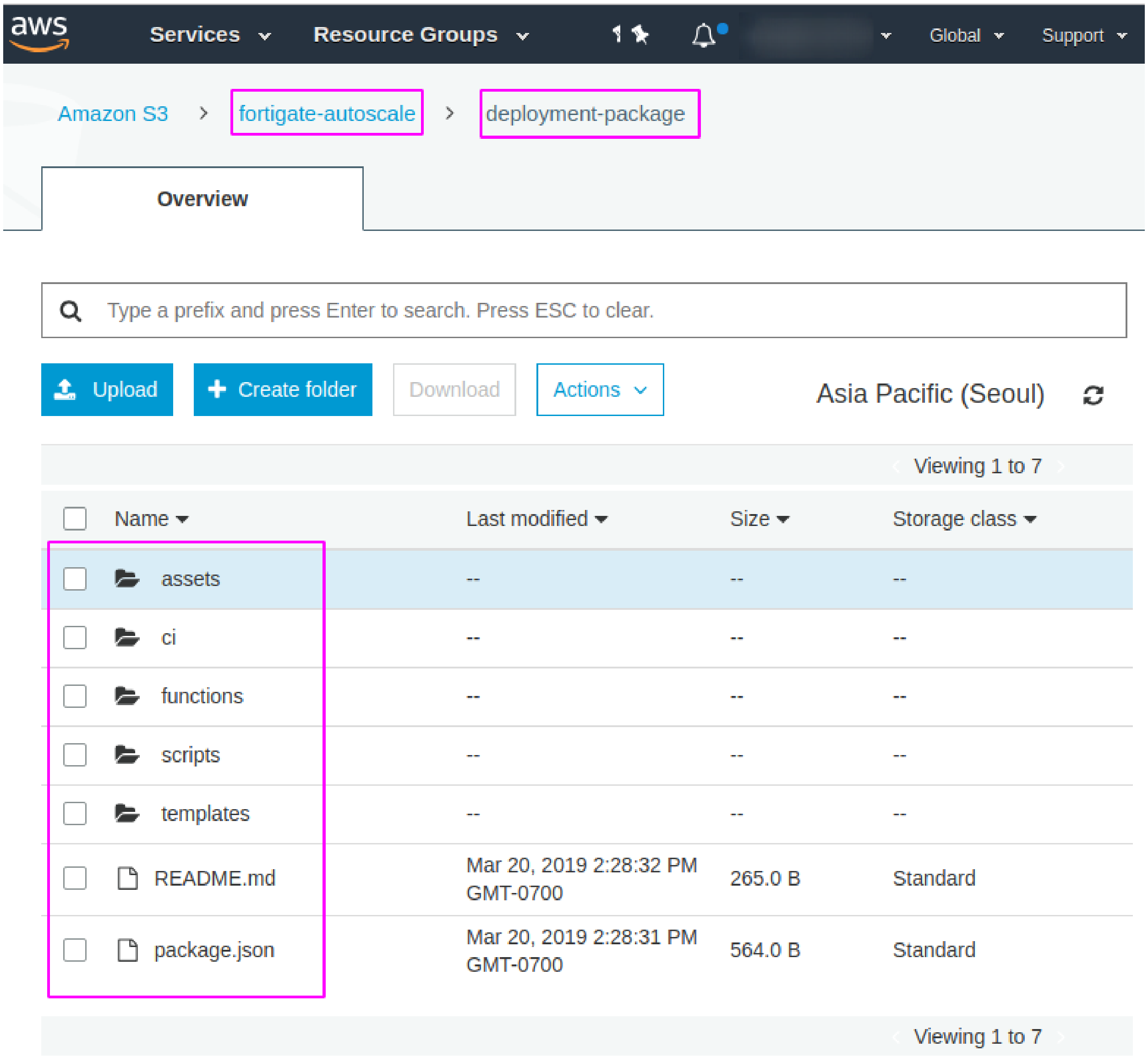
2. Unzip the file on your local PC. The following files and folders will be extracted:



Name	Size	Type ▲	Modified
assets	1 item	Folder	16:27
ci	6 items	Folder	16:27
functions	2 items	Folder	16:27
scripts	1 item	Folder	16:27
templates	10 items	Folder	16:27
package.json	564 bytes	Program	16:27
README.md	265 bytes	Text	16:27

3. Log into your AWS account.
4. In the Amazon S3 service, create an S3 bucket as the root folder for your deployment. In the example below, the folder is named *fortigate-autoscale*.

5. Inside this folder, create another folder to store the deployment resources. In the example below, this folder is named *deployment-package*.
6. Navigate to this second folder and upload the files and folders you extracted in step 2 to this location. In the example below, we navigate to *Amazon S3* > *fortigate-autoscale* > *deployment-package*.

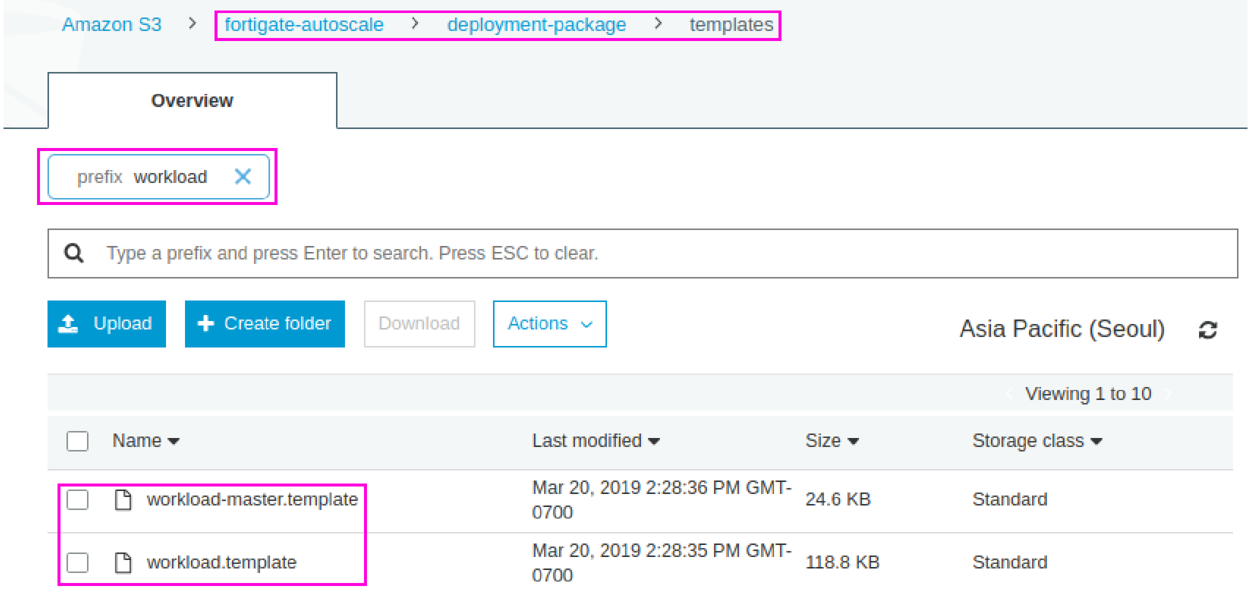


□	Name	Last modified	Size	Storage class
□	assets	--	--	--
□	ci	--	--	--
□	functions	--	--	--
□	scripts	--	--	--
□	templates	--	--	--
□	README.md	Mar 20, 2019 2:28:32 PM GMT-0700	265.0 B	Standard
□	package.json	Mar 20, 2019 2:28:31 PM GMT-0700	564.0 B	Standard

Deploying the CloudFormation templates

Use the following steps to deploy the CloudFormation templates:

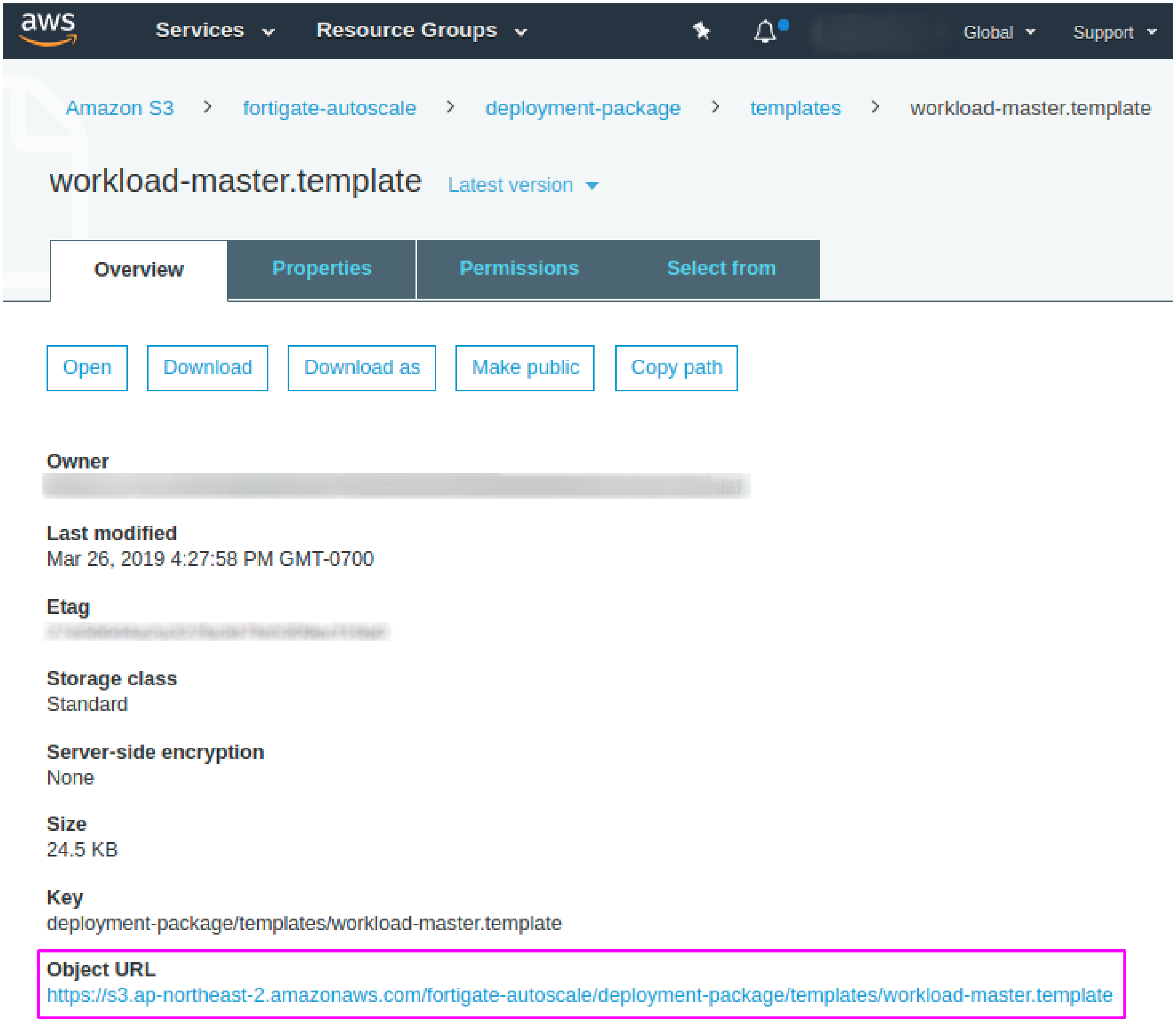
1. Navigate to the S3 folder you uploaded files to in the previous section. In the example below, we navigate to *Amazon S3 > fortigate-autoscale > deployment-package*.
2. Click *templates* and select the appropriate entry template to start the deployment:
   - To deploy into a new VPC, click `workload-master.template`.
   - To deploy into an existing VPC, click `workload.template`.



Amazon S3 > fortigate-autoscale > deployment-package > templates
Overview
prefix workload
Type a prefix and press Enter to search. Press ESC to clear.
Upload
Create folder
Download
Actions
Asia Pacific (Seoul)
Viewing 1 to 10

□	Name	Last modified	Size	Storage class
□	workload-master.template	Mar 20, 2019 2:28:36 PM GMT-0700	24.6 KB	Standard
□	workload.template	Mar 20, 2019 2:28:35 PM GMT-0700	118.8 KB	Standard

3. Copy the *Object URL* of the template you picked in the previous step. In our example, the template chosen is for deploying into a new VPC.



workload-master.template

Owner
[redacted]

Last modified
Mar 26, 2019 4:27:58 PM GMT-0700

Etag
[redacted]

Storage class
Standard

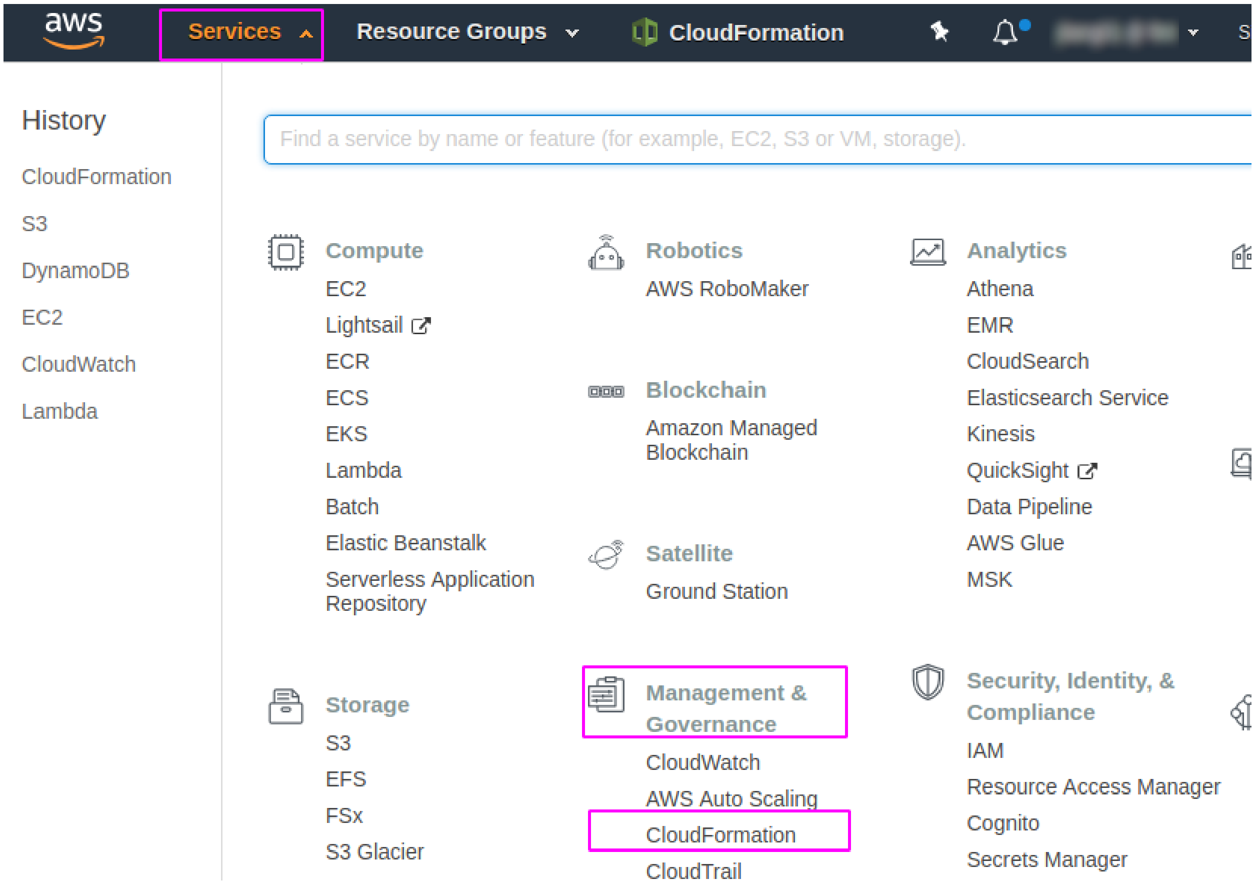
Server-side encryption
None

Size
24.5 KB

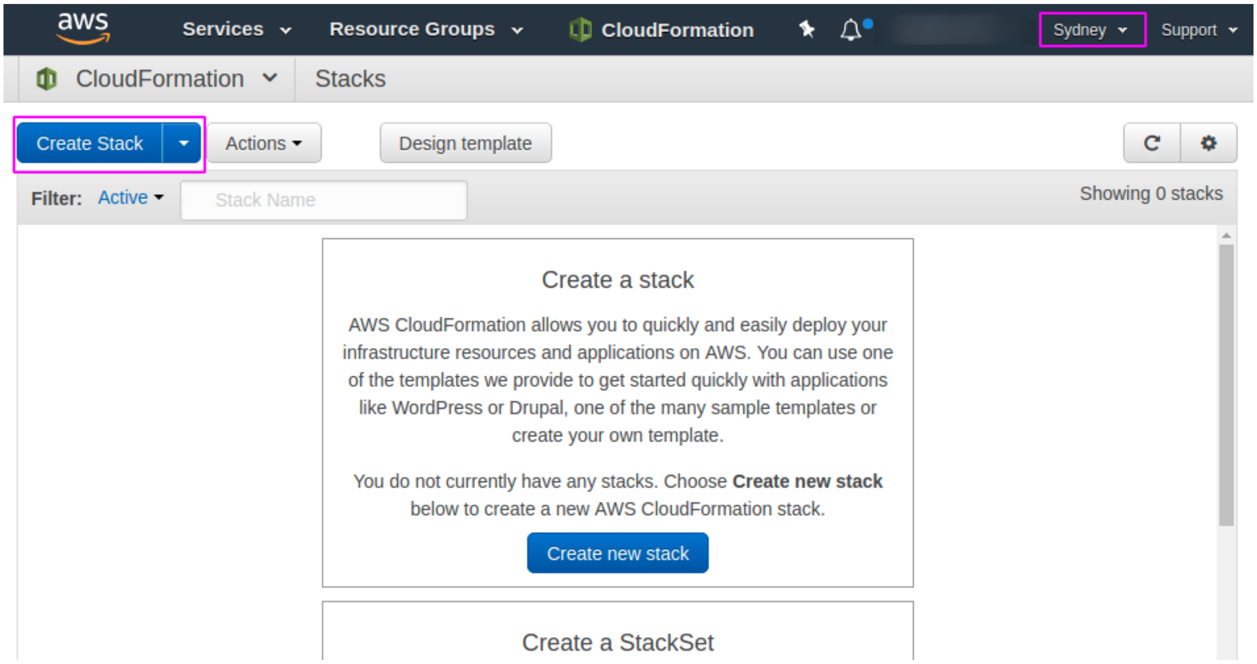
Key
deployment-package/templates/workload-master.template

Object URL
https://s3.ap-northeast-2.amazonaws.com/fortigate-autoscale/deployment-package/templates/workload-master.template

4. Click *Services*, and then *Management & Governance* > *CloudFormation*.



5. Confirm the region you are in and then click *Create Stack*.



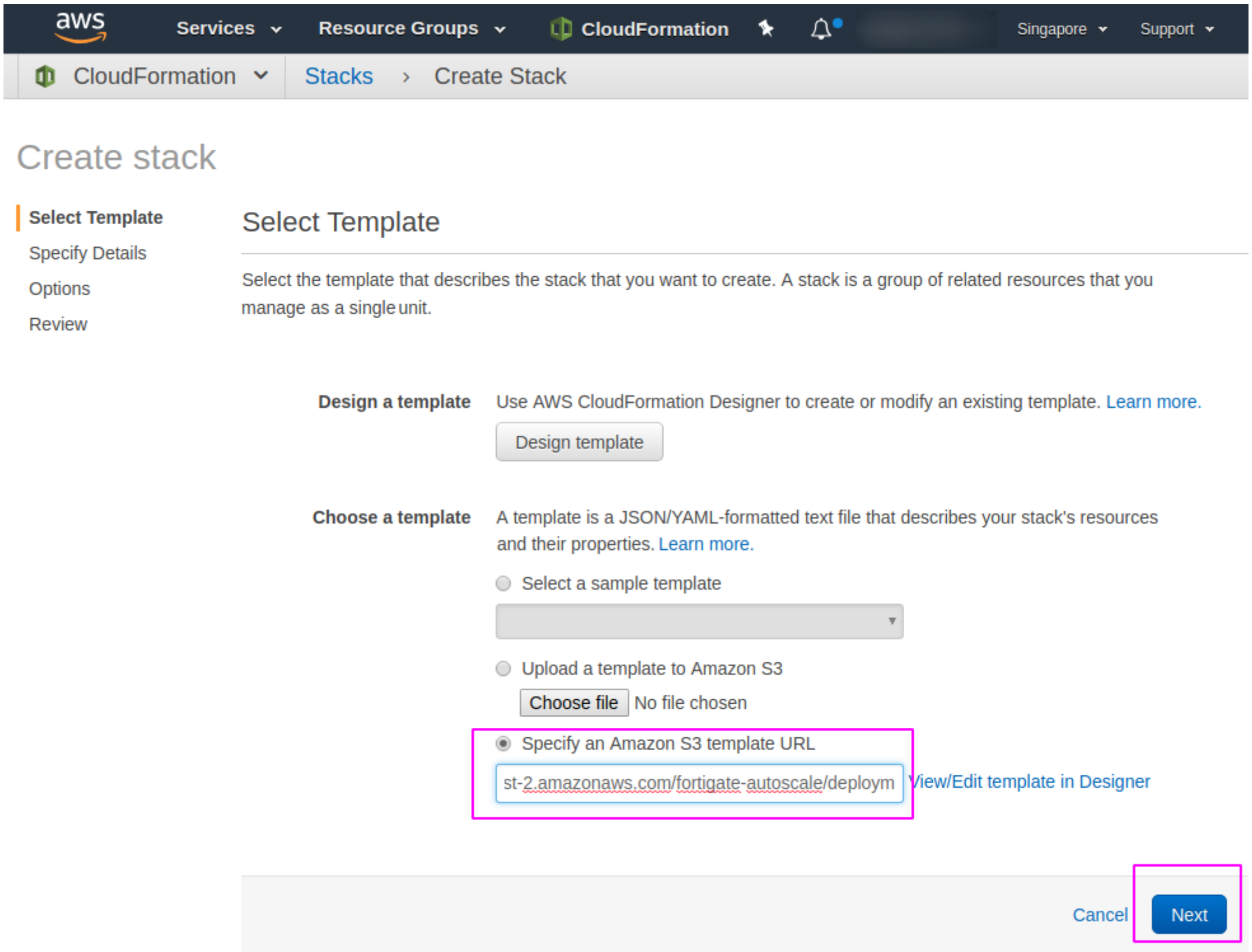
Create a stack

AWS CloudFormation allows you to quickly and easily deploy your infrastructure resources and applications on AWS. You can use one of the templates we provide to get started quickly with applications like WordPress or Drupal, one of the many sample templates or create your own template.

You do not currently have any stacks. Choose **Create new stack** below to create a new AWS CloudFormation stack.

Create a StackSet

6. Paste the *Object URL* from step 3 into the *Specify an Amazon S3 template URL* field as shown below.



Create stack

- Select Template
- Specify Details
- Options
- Review

Select Template

Select the template that describes the stack that you want to create. A stack is a group of related resources that you manage as a single unit.

Design a template Use AWS CloudFormation Designer to create or modify an existing template. Learn more.

Design template

Choose a template A template is a JSON/YAML-formatted text file that describes your stack's resources and their properties. Learn more.

○ Select a sample template

○ Upload a template to Amazon S3

Choose file No file chosen

● Specify an Amazon S3 template URL

st-2.amazonaws.com/fortigate-autoscale/deploym

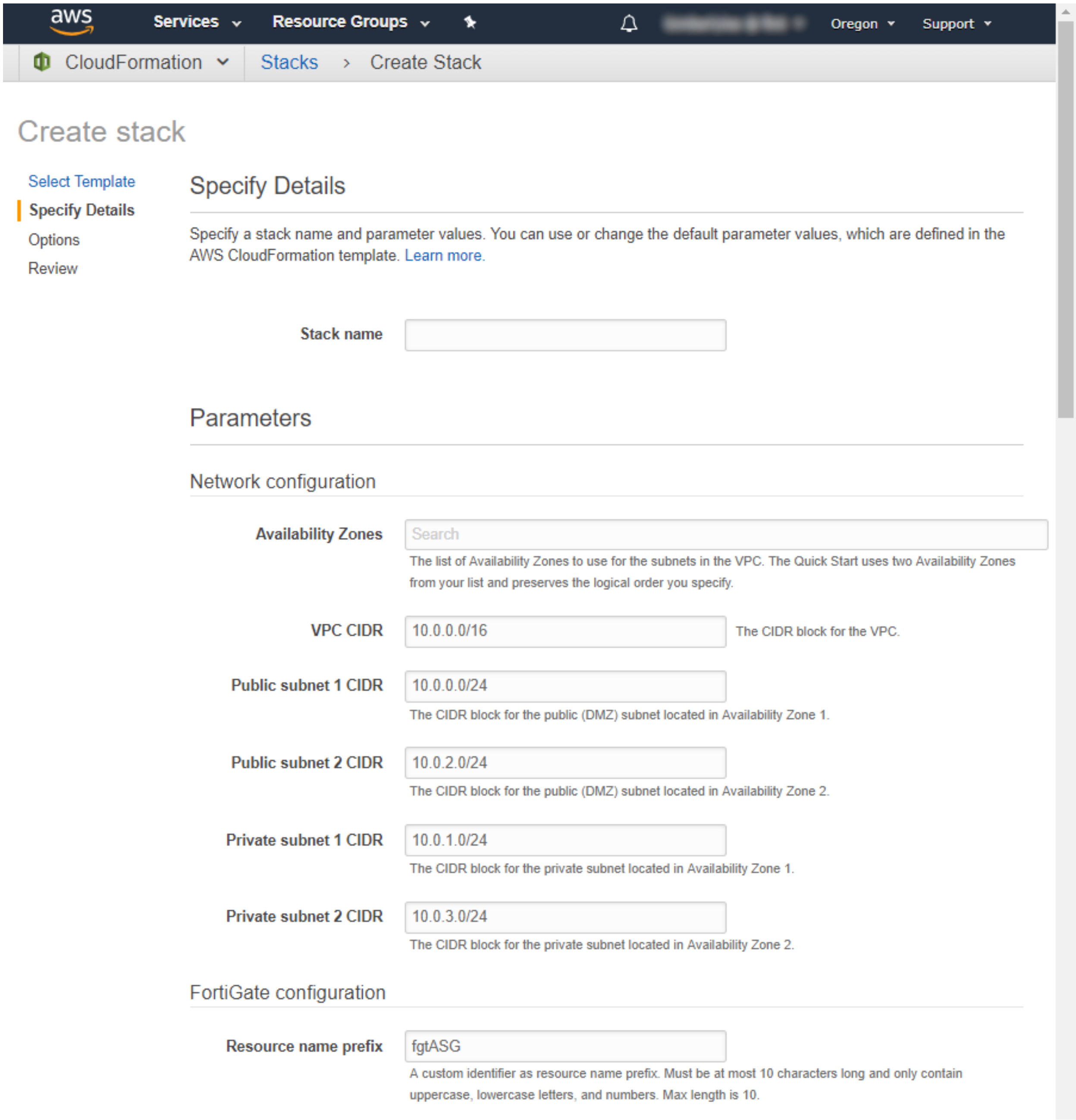
View/Edit template in Designer

Cancel Next

7. Click *Next*.

CFT parameters

The *Specify Details* page is where you enter the stack name and CFT parameters.



Create stack

- Select Template
- **Specify Details**
- Options
- Review

Specify Details

Specify a stack name and parameter values. You can use or change the default parameter values, which are defined in the AWS CloudFormation template. Learn more.

Stack name

Parameters

Network configuration

Availability Zones Search
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.

VPC CIDR 10.0.0.0/16 The CIDR block for the VPC.

Public subnet 1 CIDR 10.0.0.0/24
The CIDR block for the public (DMZ) subnet located in Availability Zone 1.

Public subnet 2 CIDR 10.0.2.0/24
The CIDR block for the public (DMZ) subnet located in Availability Zone 2.

Private subnet 1 CIDR 10.0.1.0/24
The CIDR block for the private subnet located in Availability Zone 1.

Private subnet 2 CIDR 10.0.3.0/24
The CIDR block for the private subnet located in Availability Zone 2.

FortiGate configuration

Resource name prefix fgtASG
A custom identifier as resource name prefix. Must be at most 10 characters long and only contain uppercase, lowercase letters, and numbers. Max length is 10.

The following sections provide descriptions of the available parameters. After entering all required parameters, click *Next*.

Network configuration (New VPC)

Parameter label (name)	Default	Description
Availability Zones (AvailabilityZones)	Requires input	The list of AZs to use for the subnets in the VPC. The FortiGate Autoscale solution uses two AZs from your list and preserves the logical order you specify.
VPC CIDR (VPCCIDR)	10.0.0.0/16	The CIDR block for the FortiGate Autoscale VPC.
Public subnet 1 CIDR (PublicSubnet1CIDR)	10.0.0.0/24	The CIDR block for the public (DMZ) subnet located in AZ 1.
Public subnet 2 CIDR (PublicSubnet2CIDR)	10.0.2.0/24	The CIDR block for the public (DMZ) subnet located in AZ 2.
Private subnet 1 CIDR (PrivateSubnet1CIDR)	10.0.1.0/24	The CIDR block for the private subnet located in AZ 1.
Private subnet 2 CIDR (PrivateSubnet2CIDR)	10.0.3.0/24	The CIDR block for the private subnet located in AZ 2.

Network configuration (Existing VPC)

Parameter label (name)	Default	Description
VPC ID (VpcId)	Requires input	The existing VPC ID where you deploy the Auto Scaling group and related resources. The VPC must have the option *DNS hostnames* enabled.
VPC CIDR (VPCCIDR)	Requires input	The CIDR block for the selected VPC.
FortiGate subnet 1 (PublicSubnet1)	Requires input	Public (DMZ) subnet 1, which is located in AZ 1.
FortiGate subnet 2 (PublicSubnet2)	Requires input	Public (DMZ) subnet 1, which is located in AZ 2.
Protected subnet 1 (PrivateSubnet1)	Requires input	Private subnet, which is located in AZ 1.
Protected subnet 2 (PrivateSubnet2)	Requires input	Private subnet, which is located in AZ 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-VM configuration

Parameter label (name)	Default	Description
Resource name prefix (CustomIdentifier)	fgtASG	A custom identifier as a resource name prefix. Must contain uppercase letters, lowercase letters, and numbers. Maximum length is 10.
Instance type (FortiGateInstanceType)	c5.large	Instance type to launch as FortiGate-VM 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 Instance Types.
FortiGate PSK secret (FortiGatePskSecret)	Requires input	A secret key for the FortiGate-VM instances to securely communicate with each other. Must contain numbers and letters. Maximum length is 128. 💡 Changes to the PSK secret after FortiGate Autoscale for AWS has been deployed are not reflected here. For new instances to be spawned with the changed PSK secret, this environment variable will need to be manually updated.
Admin port (FortiGateAdminPort)	8443	A port number for FortiGate-VM administration. Minimum is 1. Maximum is 65535. Do not use the FortiGate reserved ports 443, 541, 514, or 703.
Admin CIDR block (FortiGateAdminCidr)	Requires input	CIDR block for external admin management access. ⚠ 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.
Key pair name (KeyPairName)	Requires input	Amazon EC2 Key Pair for admin access.

FortiGate-VM Auto Scaling group configuration

Parameter label (name)	Default	Description
Instance lifecycle expiry (ExpireLifecycleEntry)	400	FortiGate-VM instance lifecycle expiry entry (in seconds). This is the time between the FortiGate-VM instance launching and when it starts to send the first request to the callback endpoint. Minimum is 60. Maximum is 3600.
Desired capacity (FortiGateAsgDesiredCapacity)	2	The number of FortiGate-VM instances the Auto Scaling group should have at any time. For High Availability, ensure at least 2 FortiGate-VMs are in the group. Minimum is 2.

Parameter label (name)	Default	Description
Minimum group size (FortiGateAsgMinSize)	2	Minimum number of FortiGate-VM instances in the Auto Scaling group. Minimum is 2.
Maximum group size (FortiGateAsgMaxSize)	4	Maximum number of FortiGate-VM instances in the Auto Scaling group. Minimum is 2.
Health check grace period (FortiGateAsgHealthCheckGracePeriod)	300	The length of time (in seconds) that Auto Scaling waits before checking an instance's health status. Minimum is 60.
Scaling cool down period (FortiGateAsgCooldown)	300	The Auto Scaling group waits for the cool down period (in seconds) to complete before resuming scaling activities. Minimum is 60. Maximum is 3600.
Scale-out threshold (FortiGateAsgScaleOutThreshold)	80	The threshold (in percentage) for the FortiGate-VM Auto Scaling group to scale out (add) 1 instance. Minimum is 1. Maximum is 100.
Scale-in threshold (FortiGateAsgScaleInThreshold)	25	The threshold (in percentage) for the FortiGate-VM Auto Scaling group to scale in (remove) 1 instance. Minimum is 1. Maximum is 100.
Healthy threshold (FortiGateElbTgHealthyThreshold)	3	The number of consecutive health check failures required before considering a FortiGate-VM instance unhealthy. Minimum is 3.

Failover configuration

Parameter label (name)	Default	Description
Heart beat loss count (HeartBeatLossCount)	3	Number of consecutively lost heartbeats. When the Heartbeat loss count has been reached, the FortiGate-VM is deemed unhealthy and failover activities will commence.

Load balancing configuration

Parameter label (name)	Default	Description
Internal ELB options (InternalLoadBalancingOptions)	add a new internal load balancer	(Optional) Add a predefined load balancer to route traffic to web service in the private subnets.

Parameter label (name)	Default	Description
Internal ELB DNS name (InternalLoadBalancerDnsName)	Conditionally requires input	Required when *Internal ELB options* is set to "use an existing load balancer". It is the DNS Name of the Elastic Load Balancer to be used in the private subnets.
Web service traffic port (BalanceWebTrafficOverPort)	443	If an internal ELB is selected, specify the port over which web service traffic is balanced. Minimum is 1. Maximum is 65535.

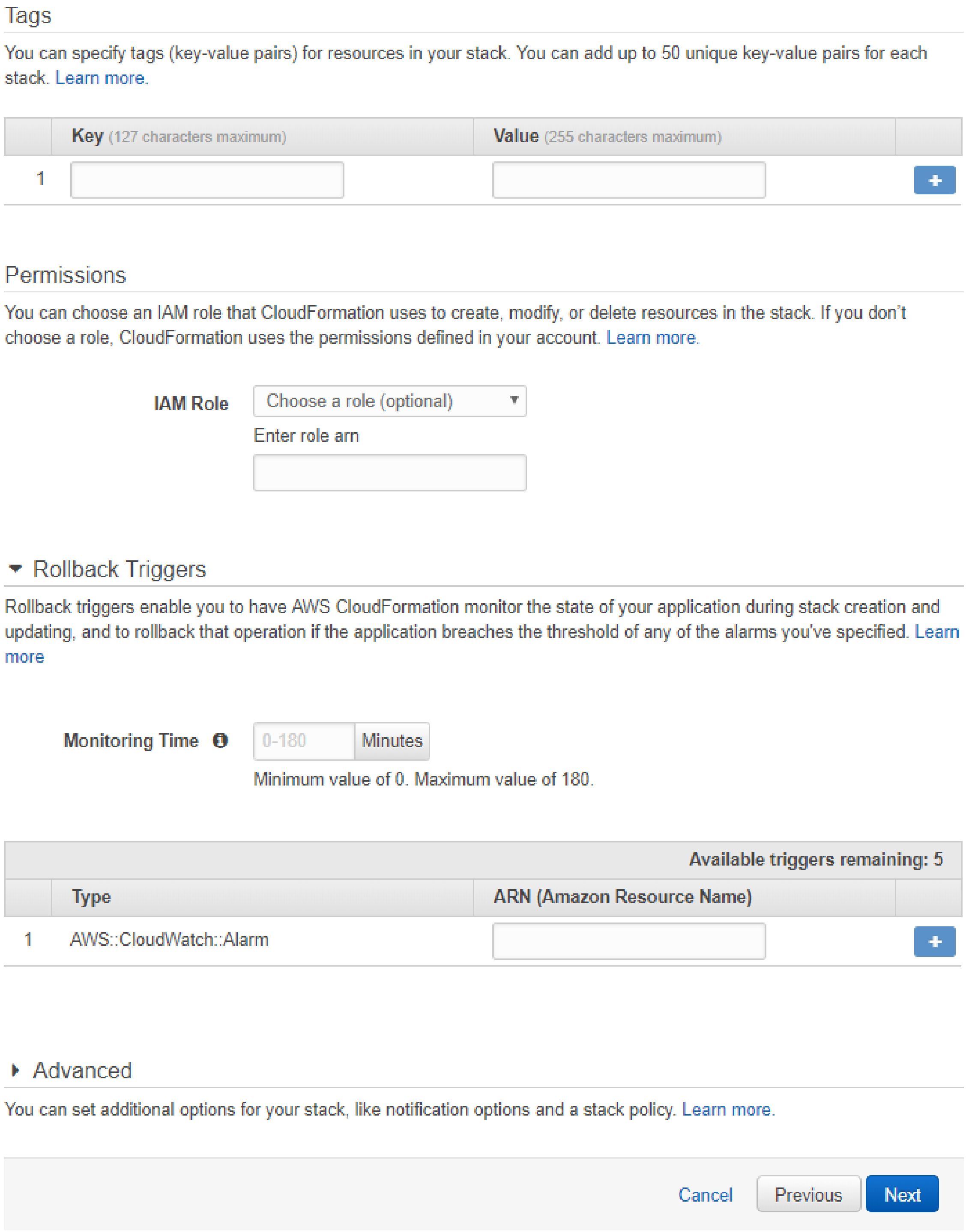
AWS Quick Start configuration

Parameter label (name)	Default	Description
Quick Start S3 bucket name (QSS3BucketName)	Requires input	S3 bucket name for the Quick Start assets. Can include numbers, lowercase letters, uppercase letters, and hyphens (-). It cannot start or end with a hyphen (-).
Quick Start S3 key prefix (QSS3KeyPrefix)	Requires input	S3 key prefix for the Quick Start assets. Can include numbers, lowercase letters, uppercase letters, hyphens (-), and forward slashes (/). It must end with a trailing slash (/).

The “Quick Start S3 bucket name” (QSS3BucketName) refers to the S3 bucket you created (*fortigate-autoscale* in the example above) and the “Quick Start S3 key prefix (QSS3KeyPrefix)” refers to the subfolder you created (*deployment-package* in the example above) in the S3 bucket.

Configuring optional settings

1. After entering required parameters and clicking *Next*, you are directed to the *Options* page as shown below:



Tags

You can specify tags (key-value pairs) for resources in your stack. You can add up to 50 unique key-value pairs for each stack. Learn more.

	Key (127 characters maximum)	Value (255 characters maximum)	
1			+

Permissions

You can choose an IAM role that CloudFormation uses to create, modify, or delete resources in the stack. If you don't choose a role, CloudFormation uses the permissions defined in your account. Learn more.

IAM Role: Choose a role (optional) ▾

Enter role arn

Rollback Triggers

Rollback triggers enable you to have AWS CloudFormation monitor the state of your application during stack creation and updating, and to rollback that operation if the application breaches the threshold of any of the alarms you've specified. Learn more

Monitoring Time: 0-180 Minutes

Minimum value of 0. Maximum value of 180.

Available triggers remaining: 5

	Type	ARN (Amazon Resource Name)	
1	AWS::CloudWatch::Alarm		+

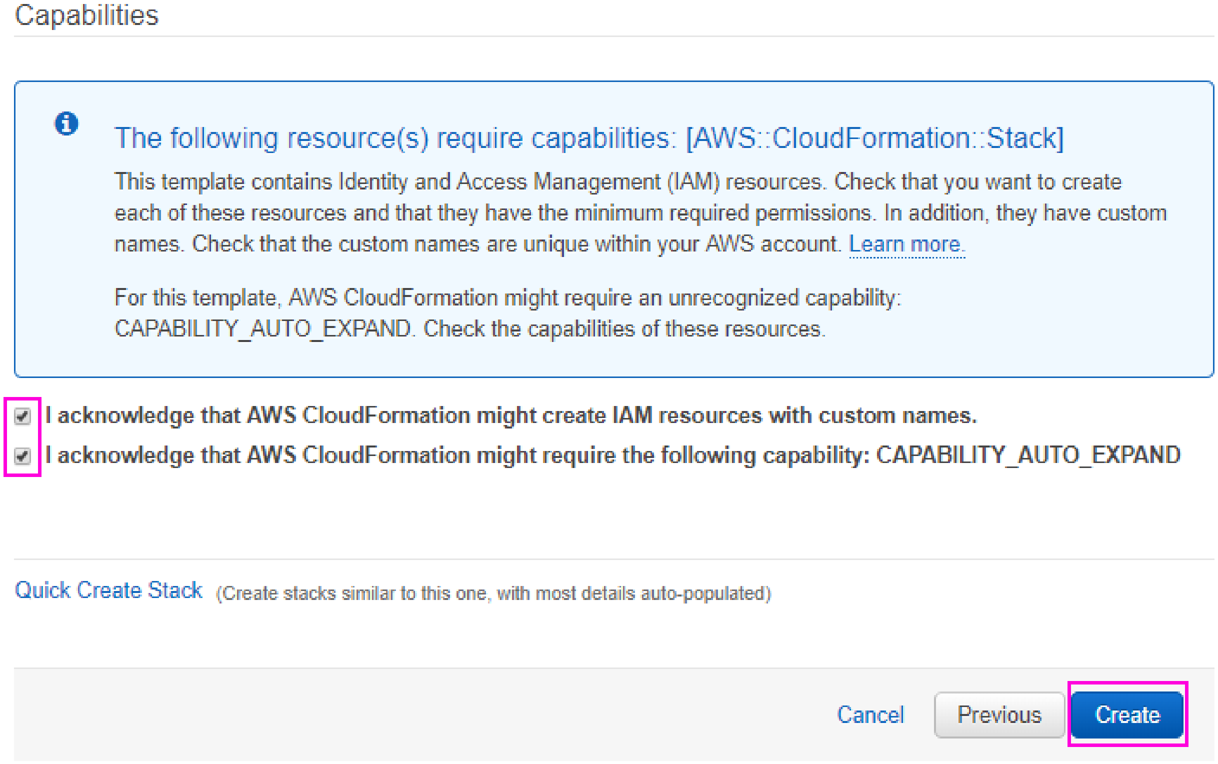
Advanced

You can set additional options for your stack, like notification options and a stack policy. Learn more.

2. Specify the following where needed:
   a. Tags: Key-Value pairs for resources in your stack.
   b. Permissions: An IAM role that AWS CloudFormation uses to create, modify, or delete resources in your stack.

c. Rollback triggers that enable AWS CloudFormation to monitor the state of your application during stack creation.
d. Advanced options.

3. Click *Next.*
4. On the *Review* page, review and confirm the template settings. Under *Capabilities*, select both check boxes.



Capabilities

The following resource(s) require capabilities: [AWS::CloudFormation::Stack]

This template contains Identity and Access Management (IAM) resources. Check that you want to create each of these resources and that they have the minimum required permissions. In addition, they have custom names. Check that the custom names are unique within your AWS account. Learn more.

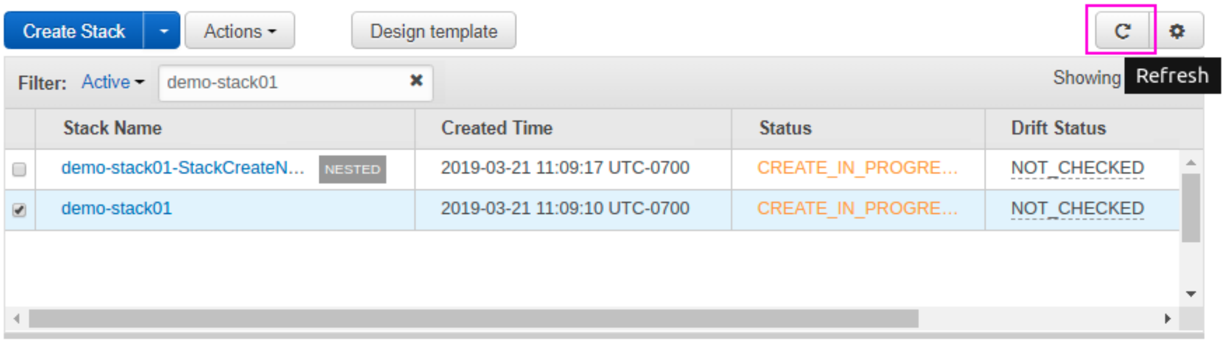
For this template, AWS CloudFormation might require an unrecognized capability: CAPABILITY_AUTO_EXPAND. Check the capabilities of these resources.

☑ I acknowledge that AWS CloudFormation might create IAM resources with custom names.

☑ I acknowledge that AWS CloudFormation might require the following capability: CAPABILITY_AUTO_EXPAND

Quick Create Stack (Create stacks similar to this one, with most details auto-populated)

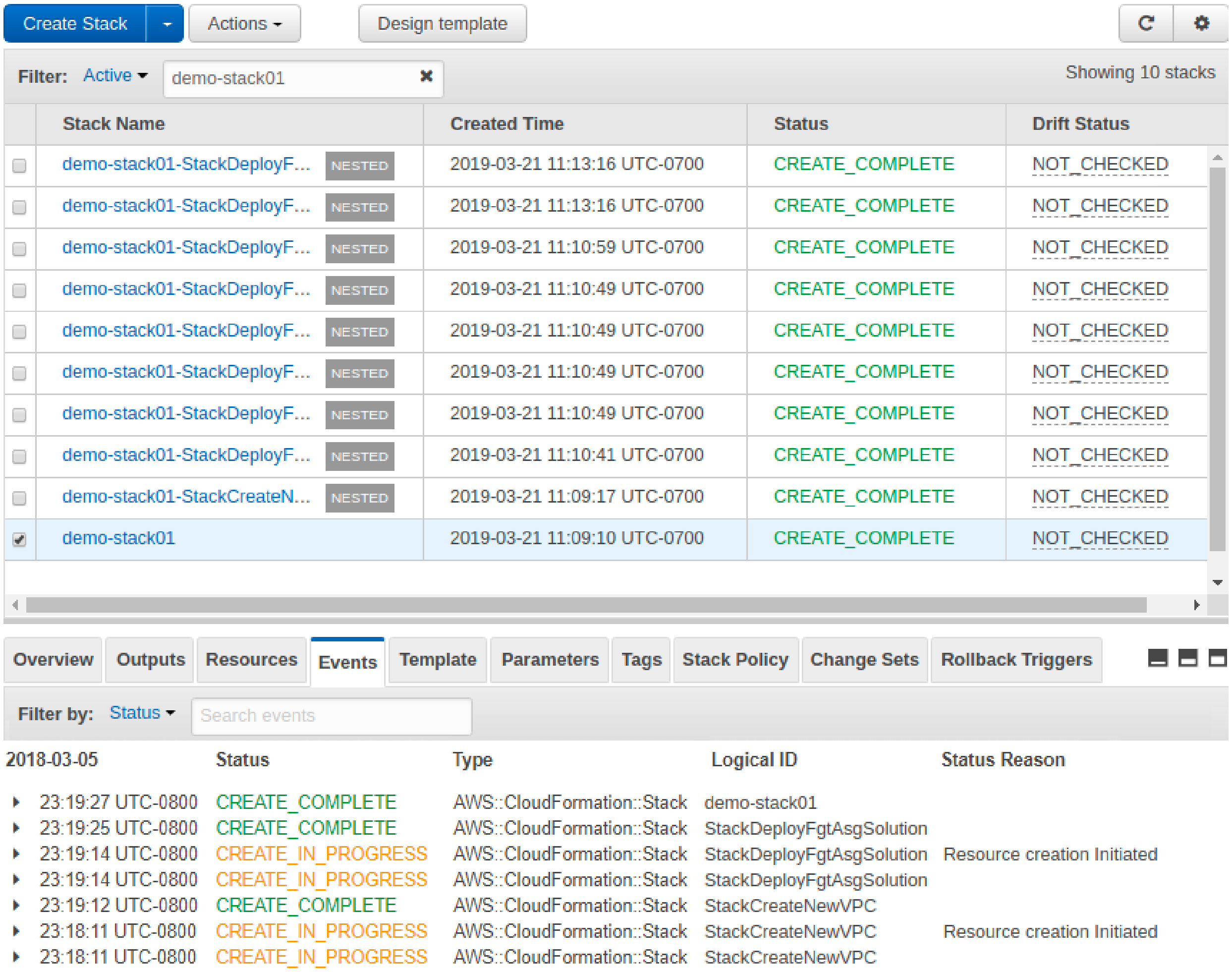
5. Click *Create Stack* to deploy the stack. Creation status is shown in the *Status* column. To see the latest status, refresh the view. It takes about ten minutes to complete the stack creation.



Filter: Active demo-stack01

	Stack Name	Created Time	Status	Drift Status
□	demo-stack01-StackCreateN... NESTED	2019-03-21 11:09:17 UTC-0700	CREATE_IN_PROGRE...	NOT_CHECKED
☑	demo-stack01	2019-03-21 11:09:10 UTC-0700	CREATE_IN_PROGRE...	NOT_CHECKED

6. Deployment has completed when each stack (including the main stack and all nested stacks) has a status of *CREATE_COMPLETE*.



	Stack Name		Created Time	Status	Drift Status
□	demo-stack01-StackDeployF...	NESTED	2019-03-21 11:13:16 UTC-0700	CREATE_COMPLETE	NOT_CHECKED
□	demo-stack01-StackDeployF...	NESTED	2019-03-21 11:13:16 UTC-0700	CREATE_COMPLETE	NOT_CHECKED
□	demo-stack01-StackDeployF...	NESTED	2019-03-21 11:10:59 UTC-0700	CREATE_COMPLETE	NOT_CHECKED
□	demo-stack01-StackDeployF...	NESTED	2019-03-21 11:10:49 UTC-0700	CREATE_COMPLETE	NOT_CHECKED
□	demo-stack01-StackDeployF...	NESTED	2019-03-21 11:10:49 UTC-0700	CREATE_COMPLETE	NOT_CHECKED
□	demo-stack01-StackDeployF...	NESTED	2019-03-21 11:10:49 UTC-0700	CREATE_COMPLETE	NOT_CHECKED
□	demo-stack01-StackDeployF...	NESTED	2019-03-21 11:10:49 UTC-0700	CREATE_COMPLETE	NOT_CHECKED
□	demo-stack01-StackDeployF...	NESTED	2019-03-21 11:10:41 UTC-0700	CREATE_COMPLETE	NOT_CHECKED
□	demo-stack01-StackCreateN...	NESTED	2019-03-21 11:09:17 UTC-0700	CREATE_COMPLETE	NOT_CHECKED
☑	demo-stack01		2019-03-21 11:09:10 UTC-0700	CREATE_COMPLETE	NOT_CHECKED

2018-03-05	Status	Type	Logical ID	Status Reason
▸ 23:19:27 UTC-0800	CREATE_COMPLETE	AWS::CloudFormation::Stack	demo-stack01	
▸ 23:19:25 UTC-0800	CREATE_COMPLETE	AWS::CloudFormation::Stack	StackDeployFgtAsgSolution	
▸ 23:19:14 UTC-0800	CREATE_IN_PROGRESS	AWS::CloudFormation::Stack	StackDeployFgtAsgSolution	Resource creation Initiated
▸ 23:19:14 UTC-0800	CREATE_IN_PROGRESS	AWS::CloudFormation::Stack	StackDeployFgtAsgSolution	
▸ 23:19:12 UTC-0800	CREATE_COMPLETE	AWS::CloudFormation::Stack	StackCreateNewVPC	
▸ 23:18:11 UTC-0800	CREATE_IN_PROGRESS	AWS::CloudFormation::Stack	StackCreateNewVPC	Resource creation Initiated
▸ 23:18:11 UTC-0800	CREATE_IN_PROGRESS	AWS::CloudFormation::Stack	StackCreateNewVPC	

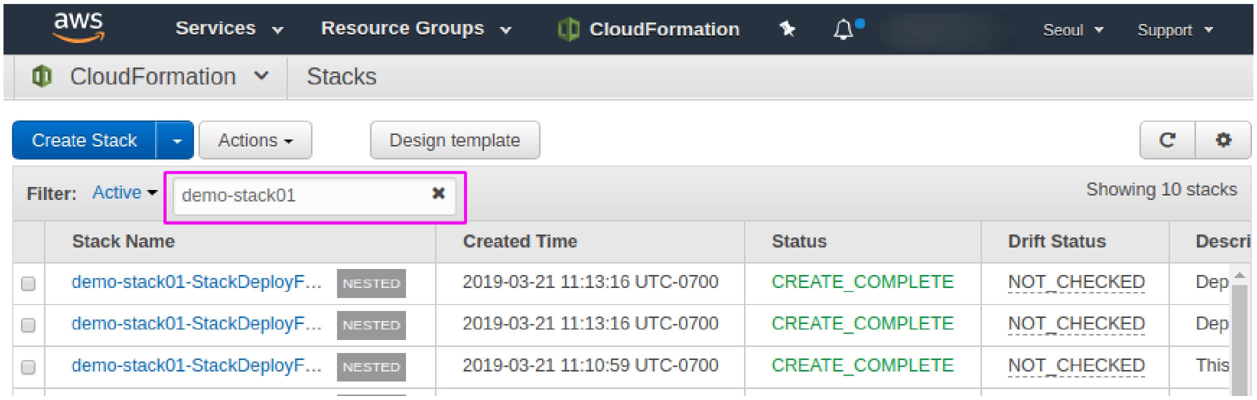
Verifying the deployment

FortiGate Autoscale for AWS creates an Auto Scaling group with lifecycle events attached to the group. Verify the following components:

- the Auto Scaling group
- the master election

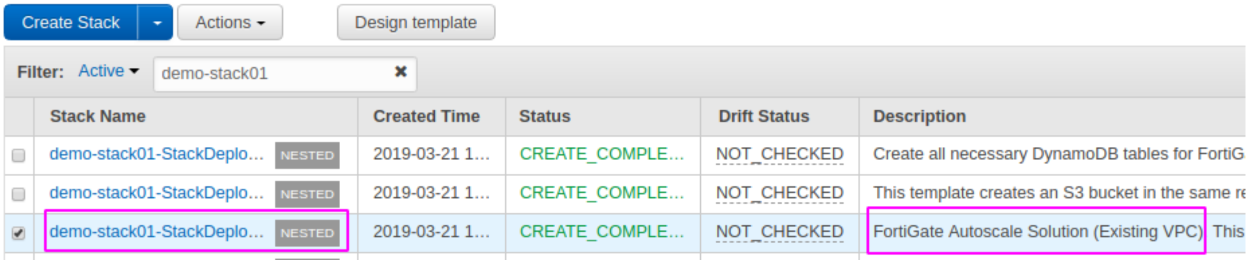
To verify the Auto Scaling group:

1. In the AWS console, select the *Services* > *Management & Governance* > *CloudFormation*.
2. On the top right, choose the AWS region where you deployed the template.
3. In the *Filter* box, enter the *Stack name* you entered on the *Specify Details* page of the section CFT parameters on page 13.



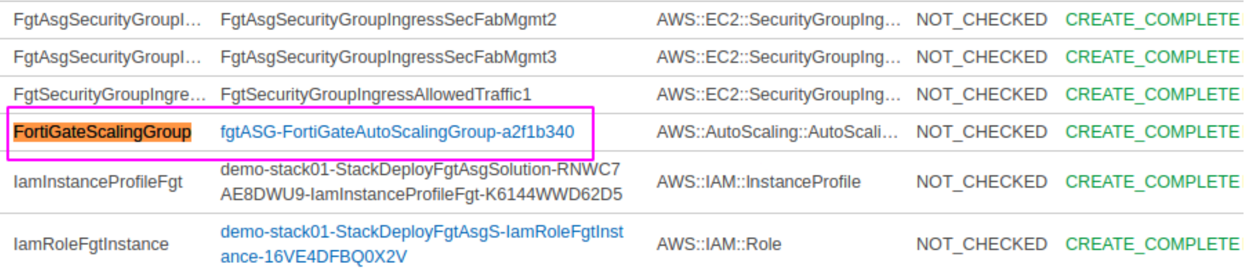
	Stack Name	Created Time	Status	Drift Status	Descri
□	demo-stack01-StackDeployF… NESTED	2019-03-21 11:13:16 UTC-0700	CREATE_COMPLETE	NOT_CHECKED	Dep
□	demo-stack01-StackDeployF… NESTED	2019-03-21 11:13:16 UTC-0700	CREATE_COMPLETE	NOT_CHECKED	Dep
□	demo-stack01-StackDeployF… NESTED	2019-03-21 11:10:59 UTC-0700	CREATE_COMPLETE	NOT_CHECKED	This

4. Look for the stack which has a *Description* starting with "FortiGate Autoscale Solution (Existing VPC)". Click the *Stack Name* for that stack.



	Stack Name	Created Time	Status	Drift Status	Description
□	demo-stack01-StackDeplo… NESTED	2019-03-21 1…	CREATE_COMPLE…	NOT_CHECKED	Create all necessary DynamoDB tables for FortiG
□	demo-stack01-StackDeplo… NESTED	2019-03-21 1…	CREATE_COMPLE…	NOT_CHECKED	This template creates an S3 bucket in the same re
☑	demo-stack01-StackDeplo… NESTED	2019-03-21 1…	CREATE_COMPLE…	NOT_CHECKED	FortiGate Autoscale Solution (Existing VPC) This

5. Under *Resources*, search for the resource with a *Logical ID* of "FortiGateScalingGroup". The *Physical ID* for this resource is a link to the Auto Scaling group. You will need this link to connect to the FortiGate in the section Connecting to the master FortiGate-VM instance on page 25.

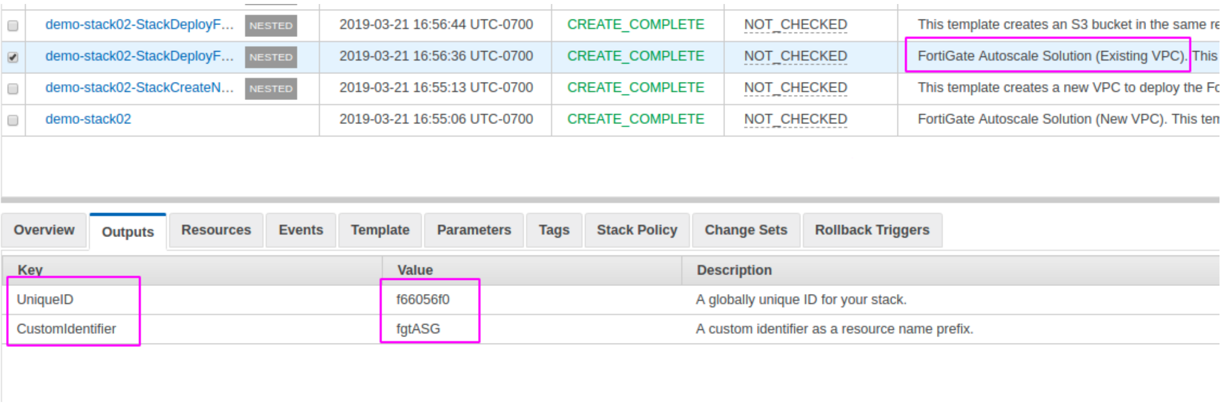


FgtAsgSecurityGroupI…	FgtAsgSecurityGroupIngressSecFabMgmt2	AWS::EC2::SecurityGroupIng…	NOT_CHECKED	CREATE_COMPLETE
FgtAsgSecurityGroupI…	FgtAsgSecurityGroupIngressSecFabMgmt3	AWS::EC2::SecurityGroupIng…	NOT_CHECKED	CREATE_COMPLETE
FgtSecurityGroupIngre…	FgtSecurityGroupIngressAllowedTraffic1	AWS::EC2::SecurityGroupIng…	NOT_CHECKED	CREATE_COMPLETE
FortiGateScalingGroup	fgtASG-FortiGateAutoScalingGroup-a2f1b340	AWS::AutoScaling::AutoScali…	NOT_CHECKED	CREATE_COMPLETE
IamInstanceProfileFgt	demo-stack01-StackDeployFgtAsgSolution-RNWC7AE8DWU9-IamInstanceProfileFgt-K6144WWD62D5	AWS::IAM::InstanceProfile	NOT_CHECKED	CREATE_COMPLETE
IamRoleFgtInstance	demo-stack01-StackDeployFgtAsgS-IamRoleFgtInstance-16VE4DFBQ0X2V	AWS::IAM::Role	NOT_CHECKED	CREATE_COMPLETE

6. Click on that link.
7. Check that the number in the *Instances* column is equal to or greater than the *Desired Capacity* you specified.
8. In the lower pane, click on the *Instances* tab and check that the *Lifecycle* of each instance is “InService”.

To verify the master election:

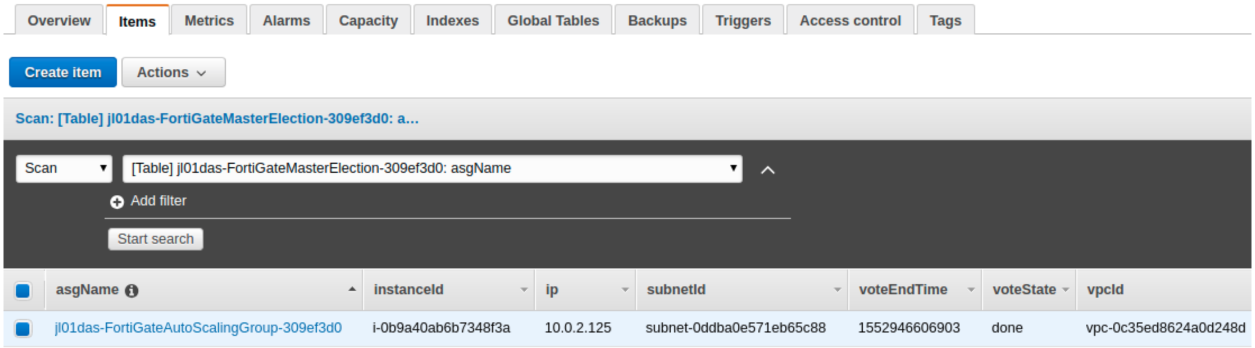
1. Look up the DynamoDB table *CustomIdentifier*-FortiGateMasterElection-*UniqueID*.
   - *CustomIdentifier* refers to the template parameter *Resource name prefix* you specified when filling out the CFT parameters.
   - *UniqueID* refers to a random string automatically generated during the deployment.
   - Both are found on the *Outputs* tab of the stack you located in step 4 when verifying the Auto Scaling group .



□	demo-stack02-StackDeployF…	NESTED	2019-03-21 16:56:44 UTC-0700	CREATE_COMPLETE	NOT_CHECKED	This template creates an S3 bucket in the same re
☑	demo-stack02-StackDeployF…	NESTED	2019-03-21 16:56:36 UTC-0700	CREATE_COMPLETE	NOT_CHECKED	FortiGate Autoscale Solution (Existing VPC). This
□	demo-stack02-StackCreateN…	NESTED	2019-03-21 16:55:13 UTC-0700	CREATE_COMPLETE	NOT_CHECKED	This template creates a new VPC to deploy the Fo
□	demo-stack02		2019-03-21 16:55:06 UTC-0700	CREATE_COMPLETE	NOT_CHECKED	FortiGate Autoscale Solution (New VPC). This ten

Key	Value	Description
UniqueID	f66056f0	A globally unique ID for your stack.
CustomIdentifier	fgtASG	A custom identifier as a resource name prefix.

2. Click the *Items* tab and double-click the master record.



	asgName	instanceId	ip	subnetId	voteEndTime	voteState	vpcId
■	jl01das-FortiGateAutoScalingGroup-309ef3d0	i-0b9a40ab6b7348f3a	10.0.2.125	subnet-0ddba0e571eb65c88	1552946606903	done	vpc-0c35ed8624a0d248d

In the master record,

- *instanceId* is the instance ID of the master instance of the Auto Scaling group. You will need the instance ID to connect to the FortiGate-VM in the section Connecting to the master FortiGate-VM instance on page 25.
- *ip* refers to its primary private IP address.

- *subnetId* is the ID of the subnet in which the master FortiGate-VM is located.
- *voteState* is the state of the voting process.
    - *pending*: election of the master instance is still in progress.
    - *done*: the master election process is done.
- *vpcId* is the ID of the VPC in which the master FortiGate-VM instance is located.

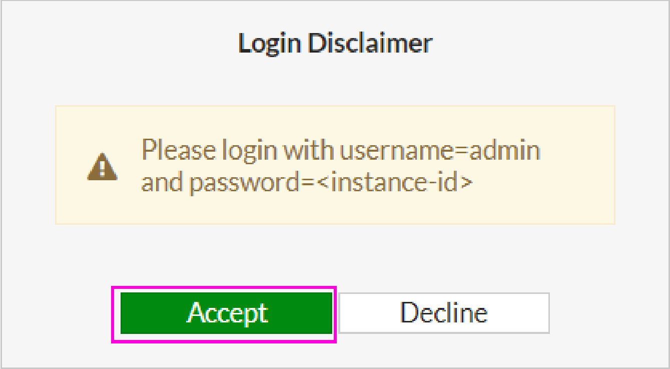
The master election has been completed when the *voteState* is *done*.

Connecting to the master FortiGate-VM instance

The initial password for all FortiGate-VM instances is the *instanceID* of the master FortiGate-VM. For details on how to obtain the master FortiGate-VM *instanceID*, refer to the section Verifying the deployment on page 22.

To connect to the master FortiGate-VM instance:

1. Look up the Auto Scaling group. For details on how to do this, refer to the section Verifying the deployment on page 22.
2. Click the *Instances* tab.
3. Click the master FortiGate-VM instance.
4. Make note of the *IPv4 Public IP* in the lower pane as you will use it to construct a login URL.
5. Construct a login URL in this way: https://*<IPAddress>:<Port>*/, where:
   - *IPAddress* refers to the IPv4 Public IP of the FortiGate-VM.
   - *Port* refers to the *Admin port* specified in the section “FortiGate-VM configuration”.
6. Open an HTTPS session in your browser and go to the URL you just constructed.
   - Your browser will display a certificate error message. This is normal because the default FortiGate-VM certificate is self-signed and not recognized by browsers. Proceed past this error. At a later time, you can upload a publicly signed certificate to avoid this error.

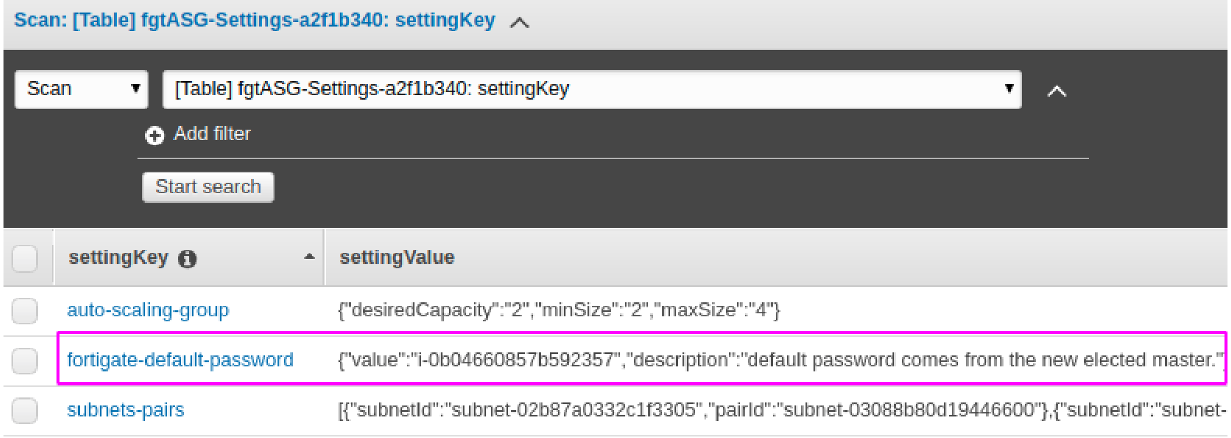


Login Disclaimer

⚠ Please login with username=admin and password=<instance-id>

7. Log into the master FortiGate-VM instance with the user name *admin* and the *<InstanceID>* of the master FortiGate-VM instance as the initial password.

- The initial password is stored in the <*CustomIdentifier*>-Settings-<*UniqueID*> table:

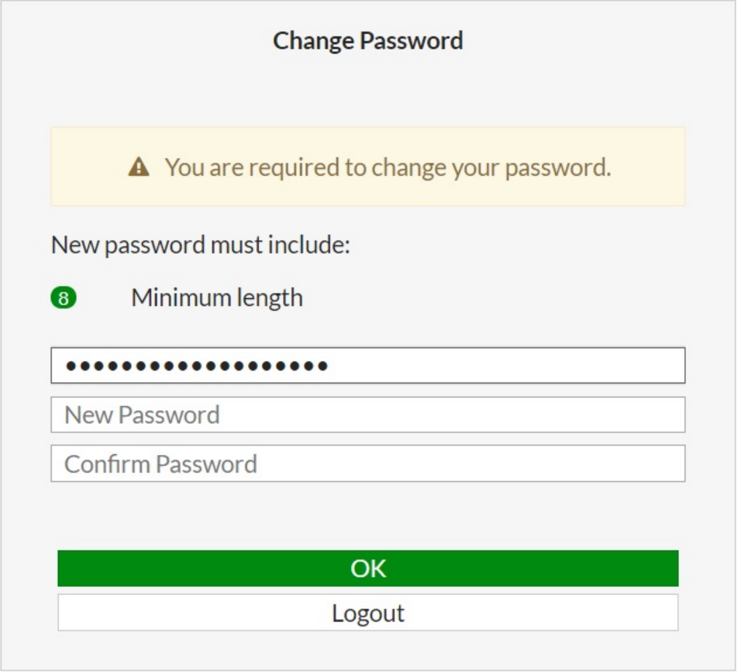


Scan: [Table] fgtASG-Settings-a2f1b340: settingKey

	settingKey	settingValue
□	auto-scaling-group	{"desiredCapacity":"2","minSize":"2","maxSize":"4"}
□	fortigate-default-password	{"value":"i-0b04660857b592357","description":"default password comes from the new elected master."
□	subnets-pairs	[{"subnetId":"subnet-02b87a0332c1f3305","pairId":"subnet-03088b80d19446600"},{"subnetId":"subnet-

- As the master FortiGate-VM propagates the password to all secondary FortiGate-VM instances, this is the initial password for all FortiGate-VM instances.
- You will need this initial password if failover occurs prior to the password being changed, as the newly elected master FortiGate-VM will still have the initial password of the previous master.

8. You are prompted to change the default password at the first-time login. It is recommended that you do so at this time.



Change Password

⚠ You are required to change your password.

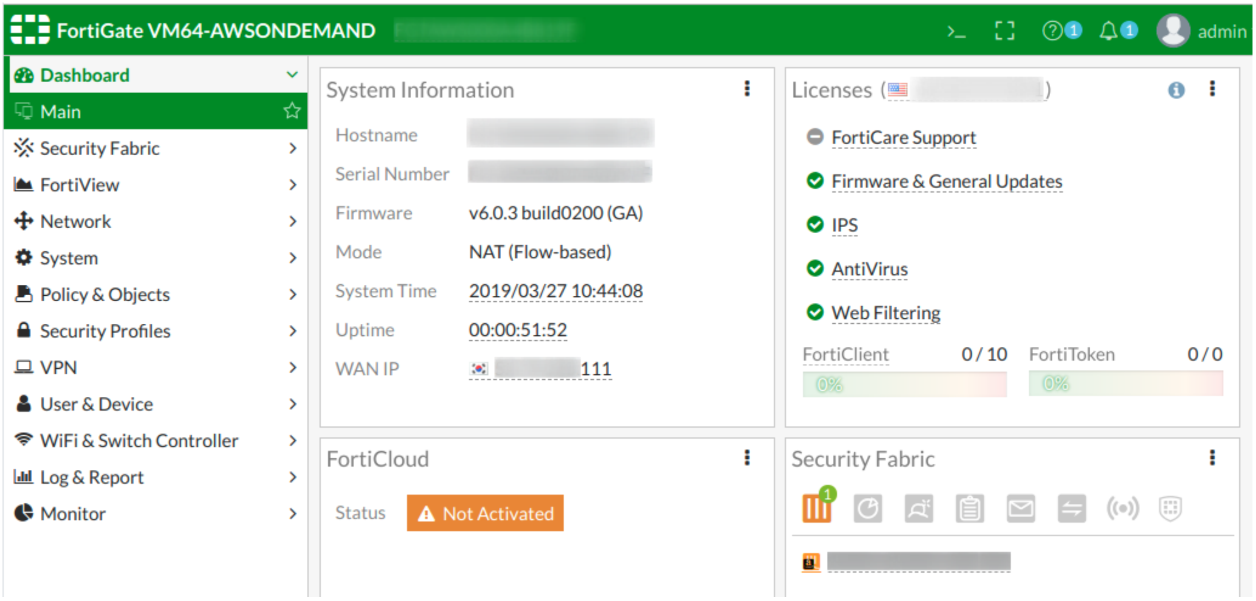
New password must include:

8 Minimum length

••••••••••••••••••

You should only change the password on the master FortiGate-VM instance. The master FortiGate-VM instance will propagate the password to all FortiGate-VMs in the Auto Scaling group. Any attempt to change the password on a secondary FortiGate-VM is overwritten with the primary FortiGate-VM's password.

9. You will now see the FortiGate-VM dashboard. The information displayed in the license widget of the dashboard depends on your license type:



System Information

Hostname	[redacted]
Serial Number	[redacted]
Firmware	v6.0.3 build0200 (GA)
Mode	NAT (Flow-based)
System Time	2019/03/27 10:44:08
Uptime	00:00:51:52
WAN IP	[redacted]111

Licenses ([redacted])

- FortiCare Support
- ✓ Firmware & General Updates
- ✓ IPS
- ✓ AntiVirus
- ✓ Web Filtering

FortiClient 0 / 10 0%

FortiToken 0 / 0 0%

FortiCloud

Status ⚠ Not Activated

Security Fabric

[redacted]

Follow the same steps to log into any other FortiGate-VM in the Auto Scaling group as needed.

Troubleshooting

CREATE_FAILED error in CloudFormation stack

If you encounter a CREATE_FAILED error when you launch the Quick Start, it is recommended 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 is retained and the instance is left running, so you can troubleshoot the issue.

When you set *Rollback on failure* to *No*, you continue to incur AWS charges for this stack. Ensure to delete the stack when you finish troubleshooting.

FortiGate-VM master election was not successful

If the FortiGate-VM master election is not successful, reset the master election. If the reset does not solve the problem, please contact support.

How to reset the master election

To reset the master election, navigate to the DynamoDB table *CustomIdentifier*-FortiGateMasterElection-*UniqueID*. Click the *Items* tab and delete the master record (the only item listed).

A new master FortiGate-VM will be elected and a new record will be created as a result.

For details on locating the DynamoDB table *CustomIdentifier*-FortiGateMasterElection-*UniqueID*, refer to the section To verify the master election: on page 23.

Appendix

FortiGate Autoscale for AWS features

Major components

- *The Auto Scaling group*. The Auto Scaling group contains 2 to many FortiGate-VMs (PAYG licensing model). This Auto Scaling group will dynamically scale-out or scale-in based on the scaling metrics specified by the parameters Scale-out threshold and Scale-in threshold. By design, there are a minimum of two instances in this group.
- *The "assets" folder in the S3 Bucket*. The *configset* folder contains files that are loaded as the initial configuration for a new FortiGate-VM instance.
  - *baseconfig* is the base configuration. This file can be modified as needed to meet your network requirements. Placeholders such as {SYNC_INTERFACE} are explained in the Configset placeholders table below.
- *Tables in DynamoDB*. These tables are required to store information such as health check monitoring, master election, state transitions, etc. These records should not be modified unless required for troubleshooting purposes.

Configset placeholders

When the FortiGate-VM requests the configuration from the Auto Scaling Handler function, the placeholders in the table below will be replaced with actual values about the Auto Scaling group.

Placeholder	Type	Description
{SYNC_INTERFACE}	Text	The interface for FortiGate-VMs to synchronize information. Specify as port1, port2, port3, etc. All characters must be lowercase.
{CALLBACK_URL}	URL	The endpoint URL to interact with the auto scaling handler script. Automatically generated during CloudFormation deployment.
{PSK_SECRET}	Text	The Pre-Shared Key used in FortiOS. Specified during CloudFormation deployment.
{ADMIN_PORT}	Number	A port number specified for admin login. A positive integer such as 443 etc. Specified during CloudFormation deployment.

Auto Scaling Handler environment variables

Variable name	Description
AUTO_SCALING_GROUP_NAME	The Auto Scaling group name.

Variable name	Description
API_GATEWAY_NAME	The API Gateway name generated during the deployment.
API_GATEWAY_STAGE_NAME	The API Gateway stage. It is always set to *prod*.
API_GATEWAY_RESOURCE_NAME	The API Gateway resource. It is always set to *complete*.
UNIQUE_ID	The value of the random string automatically generated during the deployment.
EXPIRE_LIFECYCLE_ENTRY	The value of the CFT parameter *Instance lifecycle expiry* which is described in the section “FortiGate-VM Auto Scaling group configuration”.
CUSTOM_ID	Descriptions of these variables are identical to those of the related parameters which are described in the section “FortiGate-VM configuration”. • CUSTOM_ID: *Resource name prefix* • FORTIGATE_PSKSECRET: *FortiGate PSK secret* • FORTIGATE_ADMIN_PORT: *Admin port*
FORTIGATE_PSKSECRET	
FORTIGATE_ADMIN_PORT	
FORTIGATE_INTERNAL_ELB_DNS	Descriptions of these variables are identical to those of the related parameters which are described in the section “Load Balancing configuration”. • FORTIGATE_INTERNAL_ELB_DNS: *Internal ELB options* • FORTIGATE_TRAFFIC_PORT: *Web service traffic port*
FORTIGATE_TRAFFIC_PORT	
HEART_BEAT_LOSS_COUNT	The value of the CFT parameter *Heart beat loss count* which is described in the section “Failover Configuration”.
STACK_ASSETS_S3_BUCKET_NAME	Descriptions of these variables are identical to those of the related parameters which are described in the section “AWS Quick Start configuration”. • STACK_ASSETS_S3_BUCKET_NAME: *Quick Start S3 bucket name* • STACK_ASSETS_S3_KEY_PREFIX: *Quick Start S3 key prefix*
STACK_ASSETS_S3_KEY_PREFIX	
VPC_ID	The value of the CFT parameter *VPC ID* which is described in the section "Network configuration".
REQUIRED_CONFIG_SET	This is a comma delimited string for additional configsets to load. (Reserved for future use.)
FORTIGATE_SYNC_INTERFACE	The FortiGate-VM sync interface. This should always be set to *port1*.
SCALING_GROUP_NAME_PAYG	This should always be the same as AUTO_SCALING_GROUP_NAME.
SCALING_GROUP_NAME_BYOL	This should always be the same as AUTO_SCALING_GROUP_NAME.
MASTER_SCALING_GROUP_NAME	This should always be the same as AUTO_SCALING_GROUP_NAME.

Cloud-init

In Auto Scaling, a FortiGate-VM uses the `cloud-init` feature to pre-configure the instances when they first come up. During template deployment, an internal API Gateway endpoint will be created.

A FortiGate-VM sends requests to the endpoint to retrieve necessary configurations after initialization. Following are examples from the Master and Slave FortiGate-VMs.

Master FortiGate-VM cloudinit output

```
FGTAWS00084FEF38 # diag debug cloudinit show
>> Checking metadata source aws
>> AWS curl header: Fos-instance-id: <the_masked_instance_id>
>> AWS trying to get config script from https://<the_masked_api_id> .execute-api.us-west-
     1.amazonaws.com/prod/get-config
>> AWS download config script successfully
>> Run config script
>> Finish running script
>> FGTAWS00084FEF38 $ config sys interface
>> FGTAWS00084FEF38 (interface) $ edit "port2"
>> FGTAWS00084FEF38 (port2) $ set mode dhcp
>> FGTAWS00084FEF38 (port2) $ set defaultgw disable
>> FGTAWS00084FEF38 (port2) $ set allowaccess ping https ssh http fgfm
>> FGTAWS00084FEF38 (port2) $ # work around for FortiOS 6.0.4 #0543036 mtu values from DNS
     interfere with HA checksum.
>> FGTAWS00084FEF38 (port2) $ set mtu-override enable
>> FGTAWS00084FEF38 (port2) $ set mtu 9001
>> FGTAWS00084FEF38 (port2) $ next
>> FGTAWS00084FEF38 (interface) $ end
>> FGTAWS00084FEF38 $ config system dns
>> FGTAWS00084FEF38 (dns) $ unset primary
>> FGTAWS00084FEF38 (dns) $ unset secondary
>> FGTAWS00084FEF38 (dns) $ end
>> FGTAWS00084FEF38 $ config system global
>> FGTAWS00084FEF38 (global) $ set admin-sport 8443
>> FGTAWS00084FEF38 (global) $ end
>> FGTAWS00084FEF38 $ config system auto-scale
>> FGTAWS00084FEF38 (auto-scale) $ set status enable
>> FGTAWS00084FEF38 (auto-scale) $ set sync-interface "port1"
>> FGTAWS00084FEF38 (auto-scale) $ set role master
>> FGTAWS00084FEF38 (auto-scale) $ set callback-url https://<the_masked_api_id>.execute-
     api.us-west-1.amazonaws.com/prod/complete
>> FGTAWS00084FEF38 (auto-scale) $ set psksecret <the_masked_psksecret>
>> FGTAWS00084FEF38 (auto-scale) $ end
>> FGTAWS00084FEF38 $
>> FGTAWS00084FEF38 $ config firewall address
>> FGTAWS00084FEF38 (address) $ edit internal-elb-web
>> FGTAWS00084FEF38 (internal-elb-web) $ set type fqdn
>> FGTAWS00084FEF38 (internal-elb-web) $ set fqdn "<the_masked_elb_id>.elb.us-west-
     1.amazonaws.com"
>> FGTAWS00084FEF38 (internal-elb-web) $ set associated-interface "port1"
>> FGTAWS00084FEF38 (internal-elb-web) $ next
>> FGTAWS00084FEF38 (address) $ end
>> FGTAWS00084FEF38 $
>> FGTAWS00084FEF38 $ config firewall vip
>> FGTAWS00084FEF38 (vip) $ edit internal-web
>> FGTAWS00084FEF38 (internal-web) $ set type fqdn
>> FGTAWS00084FEF38 (internal-web) $ set mapped-addr internal-elb-web
>> FGTAWS00084FEF38 (internal-web) $ set portforward enable
>> FGTAWS00084FEF38 (internal-web) $ set extintf port1
>> FGTAWS00084FEF38 (internal-web) $ set extport 443
>> FGTAWS00084FEF38 (internal-web) $ set mappedport 443
>> FGTAWS00084FEF38 (internal-web) $ next
>> FGTAWS00084FEF38 (vip) $ end
>> FGTAWS00084FEF38 $
>> FGTAWS00084FEF38 $ config firewall policy
>> FGTAWS00084FEF38 (policy) $ edit 2
>> FGTAWS00084FEF38 (2) $ set name "internal-web-https"
>> FGTAWS00084FEF38 (2) $ set srcintf "port1"
>> FGTAWS00084FEF38 (2) $ set dstintf "port2"
>> FGTAWS00084FEF38 (2) $ set srcaddr "all"
>> FGTAWS00084FEF38 (2) $ set dstaddr "internal-web"
>> FGTAWS00084FEF38 (2) $ set action accept
>> FGTAWS00084FEF38 (2) $ set schedule "always"
>> FGTAWS00084FEF38 (2) $ set service "HTTPS"
>> FGTAWS00084FEF38 (2) $ set fsso disable
>> FGTAWS00084FEF38 (2) $ set nat enable
>> FGTAWS00084FEF38 (2) $ next
>> FGTAWS00084FEF38 (policy) $ end
```

Slave FortiGate-VM cloudinit output

```
>> Checking metadata source aws [14/99]
>> AWS curl header: Fos-instance-id: <the_masked_instance_id>
>> AWS trying to get config script from https://<the_masked_api_id>.execute-api.us-west-
     1.amazonaws.com/prod/get-config
>> AWS download config script successfully
>> Run config script
>> Finish running script
>> FGTAWS00091BFEAB $ config sys interface
>> FGTAWS00091BFEAB (interface) $ edit "port2"
>> FGTAWS00091BFEAB (port2) $ set mode dhcp
>> FGTAWS00091BFEAB (port2) $ set defaultgw disable
>> FGTAWS00091BFEAB (port2) $ set allowaccess ping https ssh http fgfm
>> FGTAWS00091BFEAB (port2) $ # work around for FortiOS 6.0.4 #0543036 mtu values from DNS
     interfere with HA checksum.
>> FGTAWS00091BFEAB (port2) $ set mtu-override enable
>> FGTAWS00091BFEAB (port2) $ set mtu 9001
>> FGTAWS00091BFEAB (port2) $ next
>> FGTAWS00091BFEAB (interface) $ end
>> FGTAWS00091BFEAB $ config system dns
>> FGTAWS00091BFEAB (dns) $ unset primary
>> FGTAWS00091BFEAB (dns) $ unset secondary
>> FGTAWS00091BFEAB (dns) $ end
>> FGTAWS00091BFEAB $ config system global
>> FGTAWS00091BFEAB (global) $ set admin-sport 8443
>> FGTAWS00091BFEAB (global) $ end
>> FGTAWS00091BFEAB $ config system auto-scale
>> FGTAWS00091BFEAB (auto-scale) $ set status enable
>> FGTAWS00091BFEAB (auto-scale) $ set sync-interface "port1"
>> FGTAWS00091BFEAB (auto-scale) $ set role slave
>> FGTAWS00091BFEAB (auto-scale) $ set master-ip 10.0.0.177
>> FGTAWS00091BFEAB (auto-scale) $ set callback-url https://<the_masked_api_id>.execute-
      api.us-west-1.amazonaws.com/prod/complete
>> FGTAWS00091BFEAB (auto-scale) $ set psksecret <the_masked_psksecret>
>> FGTAWS00091BFEAB (auto-scale) $ end
>> FGTAWS00091BFEAB $
>> FGTAWS00091BFEAB $ config firewall address
>> FGTAWS00091BFEAB (address) $ edit internal-elb-web
>> FGTAWS00091BFEAB (internal-elb-web) $ set type fqdn
>> FGTAWS00091BFEAB (internal-elb-web) $ set fqdn "<the_masked_elb_id>.elb.us-west-
      1.amazonaws.com"
>> FGTAWS00091BFEAB (internal-elb-web) $ set associated-interface "port1"
>> FGTAWS00091BFEAB (internal-elb-web) $ next
>> FGTAWS00091BFEAB (address) $ end
>> FGTAWS00091BFEAB $
>> FGTAWS00091BFEAB $ config firewall vip
>> FGTAWS00091BFEAB (vip) $ edit internal-web
>> FGTAWS00091BFEAB (internal-web) $ set type fqdn
>> FGTAWS00091BFEAB (internal-web) $ set mapped-addr internal-elb-web
>> FGTAWS00091BFEAB (internal-web) $ set portforward enable
>> FGTAWS00091BFEAB (internal-web) $ set extintf port1
>> FGTAWS00091BFEAB (internal-web) $ set extport 443
>> FGTAWS00091BFEAB (internal-web) $ set mappedport 443
>> FGTAWS00091BFEAB (internal-web) $ next
>> FGTAWS00091BFEAB (vip) $ end
>> FGTAWS00091BFEAB $
>> FGTAWS00091BFEAB $ config firewall policy
>> FGTAWS00091BFEAB (policy) $ edit 2
>> FGTAWS00091BFEAB (2) $ set name "internal-web-https"
>> FGTAWS00091BFEAB (2) $ set srcintf "port1"
>> FGTAWS00091BFEAB (2) $ set dstintf "port2"
>> FGTAWS00091BFEAB (2) $ set srcaddr "all"
>> FGTAWS00091BFEAB (2) $ set dstaddr "internal-web"
>> FGTAWS00091BFEAB (2) $ set action accept
>> FGTAWS00091BFEAB (2) $ set schedule "always"
>> FGTAWS00091BFEAB (2) $ set service "HTTPS"
>> FGTAWS00091BFEAB (2) $ set fsso disable
>> FGTAWS00091BFEAB (2) $ set nat enable
>> FGTAWS00091BFEAB (2) $ next
>> FGTAWS00091BFEAB (policy) $ end
```

Wait for a bit for Auto Scaling to bring up and sync the configuration between the instances.

VPN output

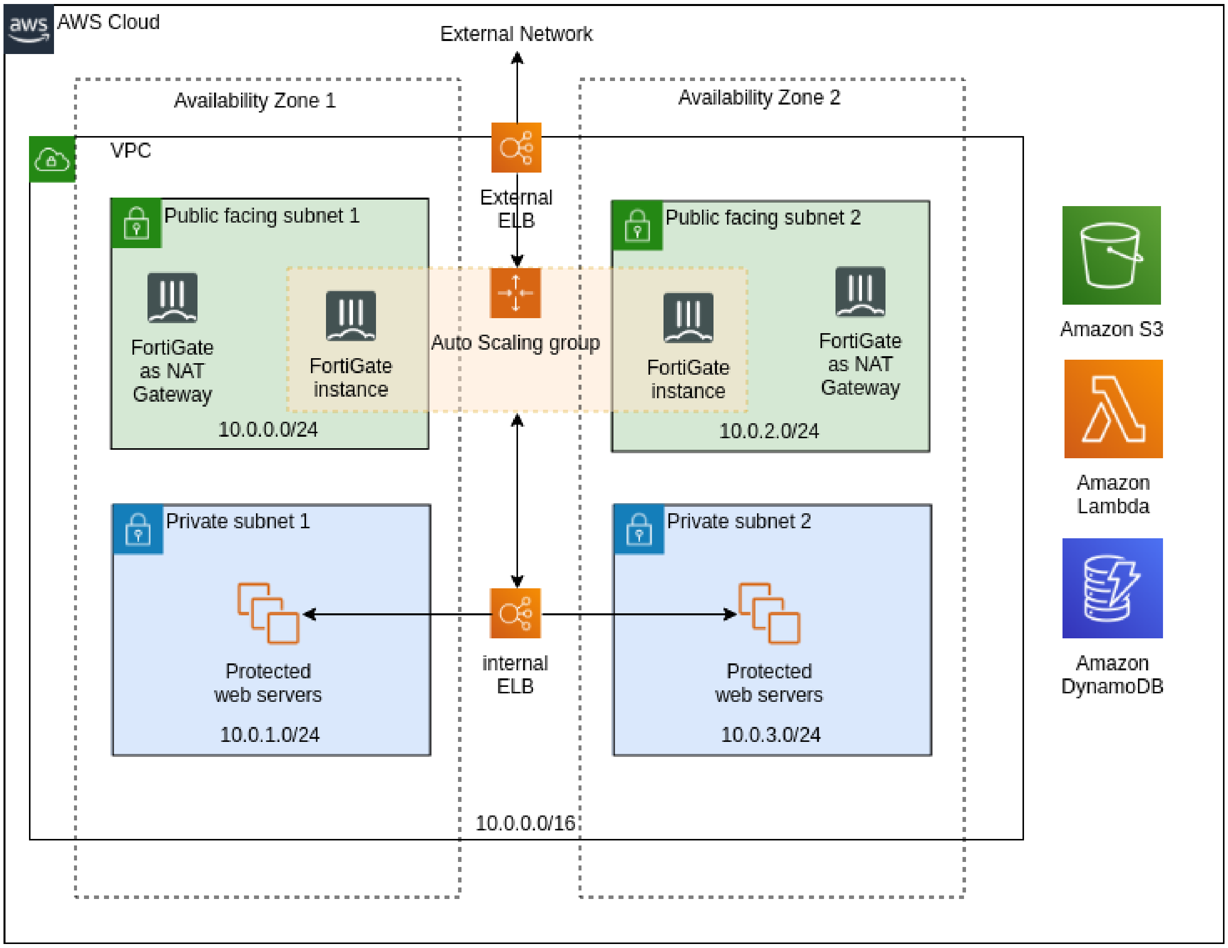
```
name=__autoscale_m_p1_0 ver=1 serial=3 10.0.0.177:0->10.0.2.235:0
bound_if=3 lgwy=static/1 tun=tunnel/1 mode=dial_inst/3 encap=none/128 options[0080]=rgwy-chg
   parent=__autoscale_m_p1 index=0
proxyid_num=1 child_num=0 refcnt=5 ilast=30 olast=30 ad=/0
stat: rxp=47 txp=39 rxb=5896 txb=2892
dpd: mode=on-idle on=1 idle=60000ms retry=3 count=0 seqno=0
natt: mode=none draft=0 interval=0 remote_port=0
proxyid=__autoscale_m_p2 proto=0 sa=1 ref=2 serial=1
   src: 0:0.0.0.0-255.255.255.255:0
   dst: 0:10.0.2.235-10.0.2.235:0
   SA: ref=3 options=226 type=00 soft=0 mtu=8942 expire=42771/0B replaywin=2048
      seqno=28 esn=0 replaywin_lastseq=00000030 itn=0
   life: type=01 bytes=0/0 timeout=43186/43200
```

```
dec: spi=28b967de esp=aes key=16 <masked_key>
   ah=sha1 key=20 7<masked_key>
enc: spi=97a7fc49 esp=aes key=16 <masked_key>
   ah=sha1 key=20 <masked_key>
dec:pkts/bytes=47/2828, enc:pkts/bytes=39/5448
```

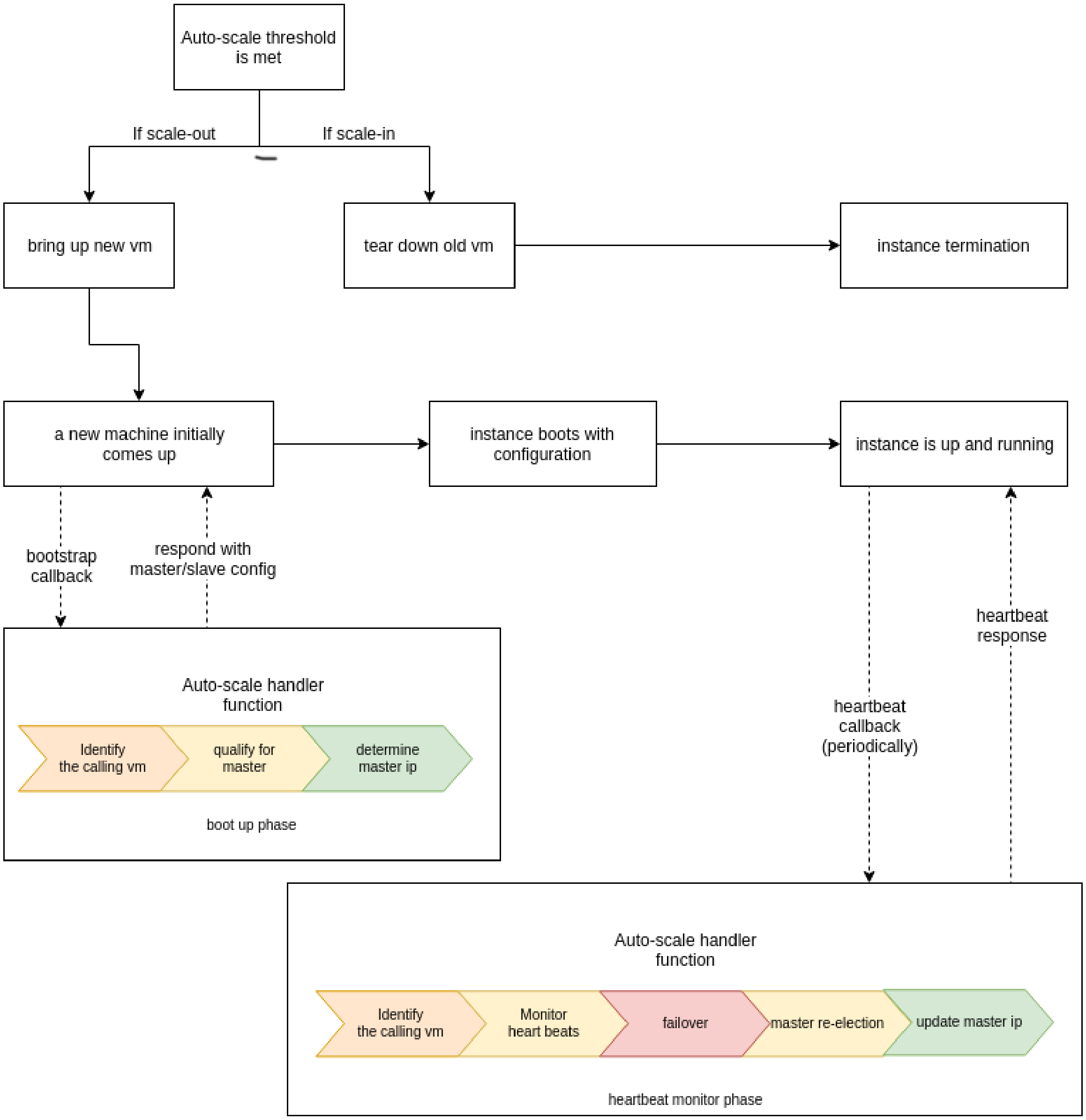
Architectural diagrams

The following diagrams illustrate the different aspects of the architecture of FortiGate Autoscale for AWS.

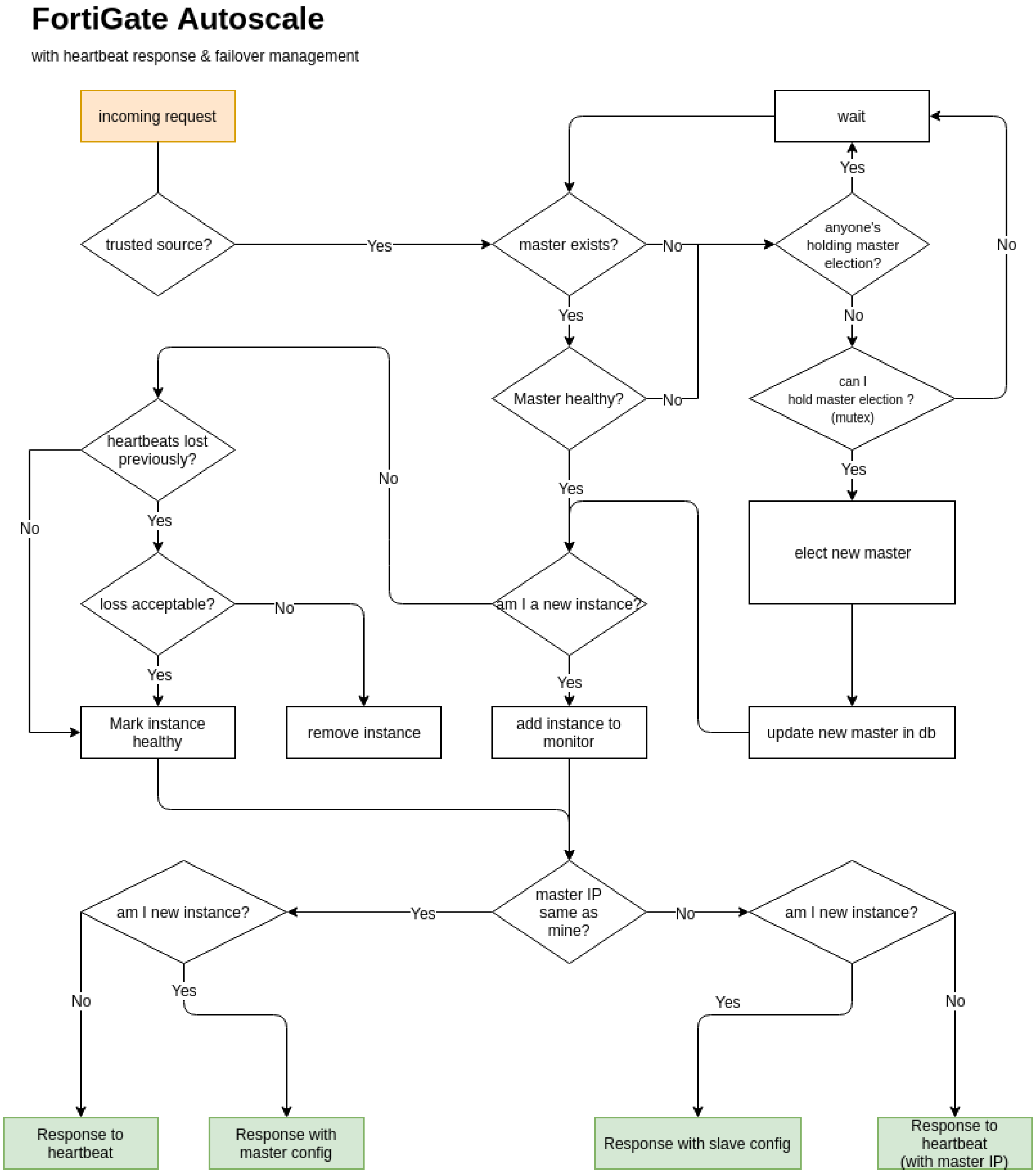
FortiGate Autoscale VPC



Autoscale handler flowchart



Master election


FortiGate Autoscale
with heartbeat response & failover management
incoming request
trusted source?
Yes
master exists?
No
Yes
wait
Yes
anyone's holding master election?
No
No
can I hold master election ? (mutex)
Yes
elect new master
update new master in db
Master healthy?
No
Yes
heartbeats lost previously?
No
Yes
loss acceptable?
No
Yes
No
am I a new instance?
Yes
Mark instance healthy
remove instance
add instance to monitor
master IP same as mine?
Yes
No
am I new instance?
No
Yes
am I new instance?
Yes
No
Response to heartbeat
Response with master config
Response with slave config
Response to heartbeat (with master IP)