FORTINET®

FortiOS - AWS Cookbook

Version 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 22, 2020
FortiOS 6.2 AWS Cookbook
01-620-544190-20200922

TABLE OF CONTENTS

Deploying auto scaling on AWS

You can deploy FortiGate virtual machines (VMs) to support Auto Scaling on AWS. This is a manual deployment incorporating CloudFormation Templates (CFTs). Fortinet provides a FortiGate Autoscale for AWS deployment package to facilitate the deployment.

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 requires FortiOS 6.2.3 and supports any combination of On-Demand and Bring Your Own License (BYOL) instances.

Deploying auto scaling on AWS without Transit Gateway integration

FortiGate Autoscale for AWS without Transit Gateway integration is available with FortiOS 6.2.3 and supports any combination of On-Demand and BYOL instances.

Before you deploy FortiGate Autoscale for AWS without Transit Gateway integration, 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)
- An Amazon VPC configured with public 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 ASG 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

Planning

Deploying FortiGate Autoscale for AWS without Transit Gateway integration 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.

Following are descriptions of the templates included in the 2.0.x deployment package.

Template	Type	Description
autoscale-new-vpc.template	Entry template	Deploys the Auto Scaling solution to a new VPC.
autoscale-existing-vpc.template	Entry template	Deploys the Auto Scaling solution to an existing VPC.
autoscale-main.template	Dependency template	Does the majority of the work for deploying FortiGate Autoscale.
add-nic-attachment-service.template	Dependency template	Deploys a service to handle an additional network interface attachment / detachment to an EC2 instance in a given VPC.
copy-objects.template	Dependency template	Creates an S3 bucket in the same region where the stack is launched and copies deployment related objects to this S3 bucket.
create-autoscale-handler.template	Dependency template	Creates a FortiGate Autoscale Handler Lambda function and an API Gateway.
create-auto-scaling-group.template	Dependency template	Creates a FortiGate Auto Scaling group and related components.
create-db-table.template	Dependency template	Creates all necessary DynamoDB tables for the FortiGate Autoscale solution.
create-fortianalyzer.template	Dependency template	Deploys a single FortiAnalyzer instance for certain purposes such as storing logs from FortiGate-VMs.
create-fortigate.template	Dependency template	Deploys a FortiGate EC2 instance to a subnet using a given FortiGate AMI, security group, and instance profile.
create-hybrid-auto-scaling-group.template	Dependency template	Deploys the hybrid licensing FortiGate Auto Scaling groups.
create-load-balancer.template	Dependency template	Deploys network traffic Load Balancers and components for FortiGate Autoscale.
create-nat-fgt-master.template	Dependency template	Deploys FortiGate-VMs as NAT gateways.
create-new-vpc.template	Dependency template	Creates a new VPC in which to deploy the FortiGate Autoscale solution.

Prerequisites

Installing and configuring FortiGate Autoscale for AWS without Transit Gateway integration 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 without Transit Gateway integration 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.

   CFT deployment will fail if the AWS user deploying the template does not have sufficient AWS permissions to perform the required service actions on resources. At a minimum, the following are required:
   - *Service*: IAM; *Actions*:CreateRole; *Resource*: *.

2. Use the region selector in the navigation bar to choose the AWS region where you want to deploy FortiGate Autoscale for AWS without Transit Gateway integration.

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

   AWS Auto Scaling is not supported in every region. Please check the AWS Region Table prior to selecting a region. Region support may be added without prior notification.

3. Confirm that you have a valid subscription to the On-Demand and/or BYOL marketplace listings for FortiGate, as required for your deployment:
   - BYOL FortiGate listing
   - On-Demand FortiGate listing

   Without the valid subscriptions, the deployment will fail with errors.

4. Create a key pair in your selected region.
5. 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*.

Obtaining the deployment package

The FortiGate Autoscale for AWS without Transit Gateway integration deployment package is located in the Fortinet GitHub project.

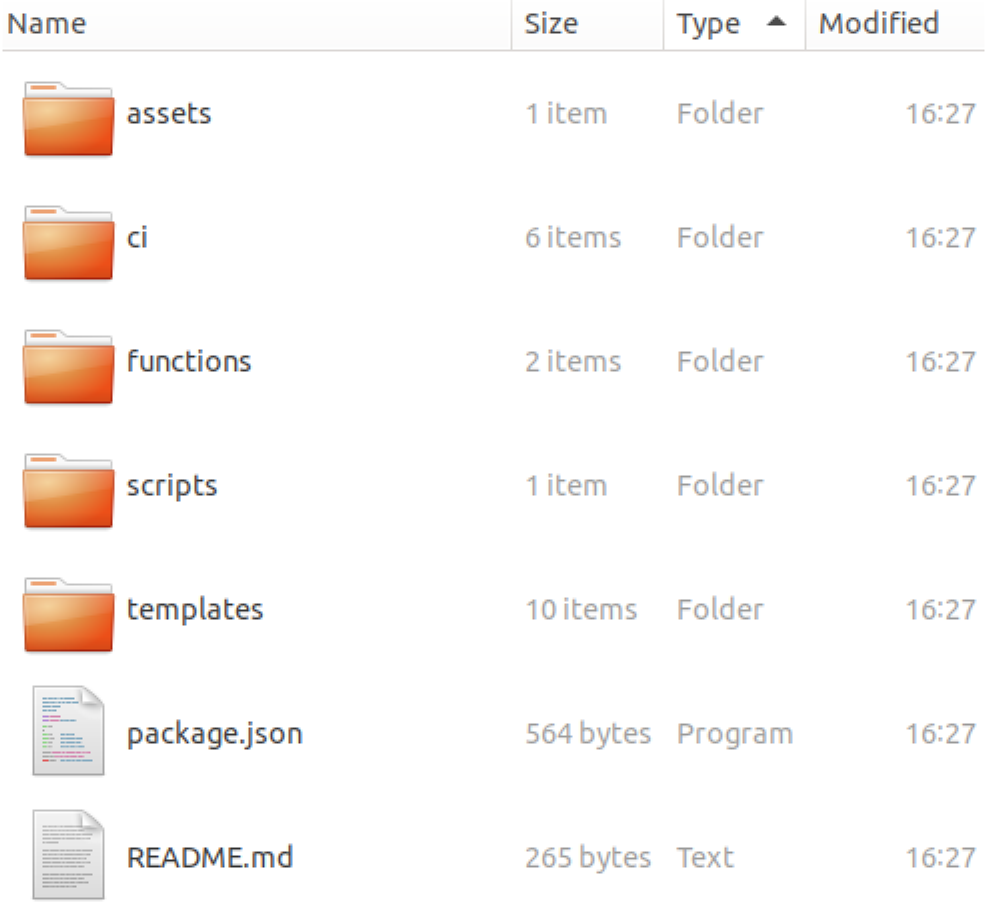
To obtain the package:

1. Visit the FortiGate Autoscale GitHub project release page and download the `fortigate-autoscale-aws-cloudformation.zip` for the version you want to use.

   This documentation is for the *Version 2.0.x* release which supports any combination of BYOL and On-Demand instances.

   Documentation for *Version 1.0.x* (which only supports On-Demand instances) is no longer maintained and is only available as a PDF in the 1.0.x GitHub repository.

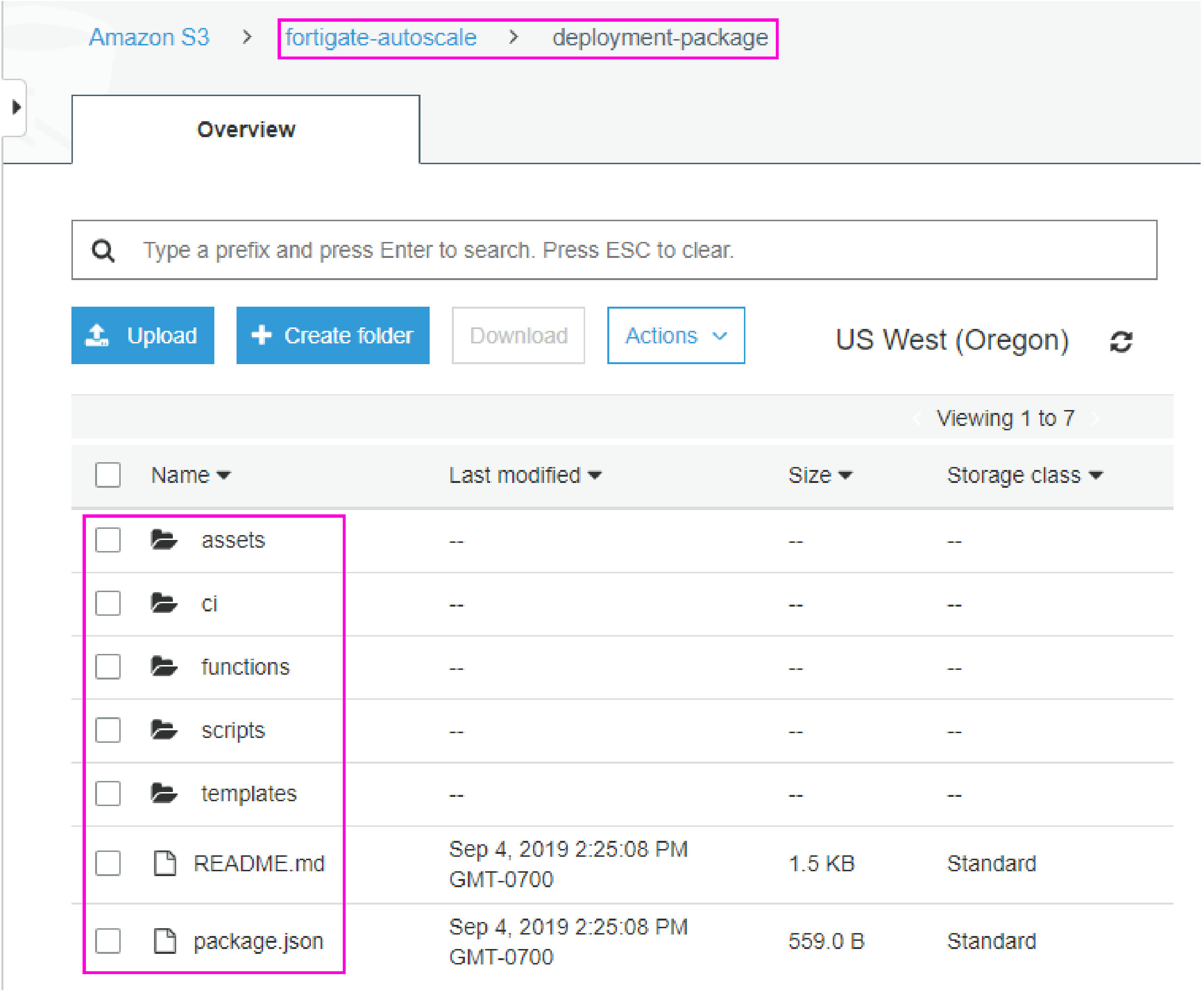
2. Unzip the file on your local PC. The following files and folders will be extracted:



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*.

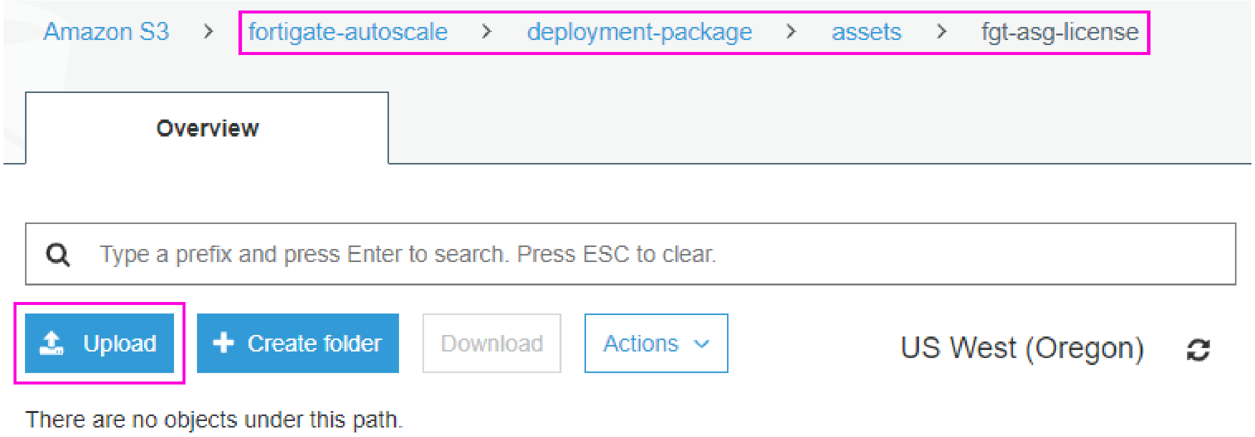
6. Navigate to this second folder and upload the files and folders you extracted in step 2 to this location. In the example below, we navigate to *Amazon S3 > fortigate-autoscale > deployment-package*.


Amazon S3 > fortigate-autoscale > deployment-package
Overview
Type a prefix and press Enter to search. Press ESC to clear.
Upload
Create folder
Download
Actions
US West (Oregon)
Viewing 1 to 7

□	Name	Last modified	Size	Storage class
□	assets	--	--	--
□	ci	--	--	--
□	functions	--	--	--
□	scripts	--	--	--
□	templates	--	--	--
□	README.md	Sep 4, 2019 2:25:08 PM GMT-0700	1.5 KB	Standard
□	package.json	Sep 4, 2019 2:25:08 PM GMT-0700	559.0 B	Standard

This *assets* folder contains configuration files that can be modified as needed to meet your network requirements. For details, refer to the Appendix > Major components on page 35 >*The "assets" folder in the S3 bucket*.

7. If you will be using BYOL instances, navigate to the *assets* folder, create a folder named *fgt-asg-license*, and upload your FortiGate license file(s) to this folder.


Amazon S3 > fortigate-autoscale > deployment-package > assets > fgt-asg-license
Overview
Type a prefix and press Enter to search. Press ESC to clear.
Upload
Create folder
Download
Actions
US West (Oregon)

There are no objects under this path.

Deploying the CloudFormation templates

The deployment will fail:

- if you do not have the required subscriptions for the On-Demand and/or BYOL marketplace listings for FortiGate.
- if the AWS user deploying the template does not have the AWS permissions to perform the required service actions on resources. At a minimum, the following are required:
  - *Service*: IAM; *Actions*:CreateRole; *Resource*: *.

FortiGate Autoscale for AWS without Transit Gateway integration provides separate CFTs for 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.

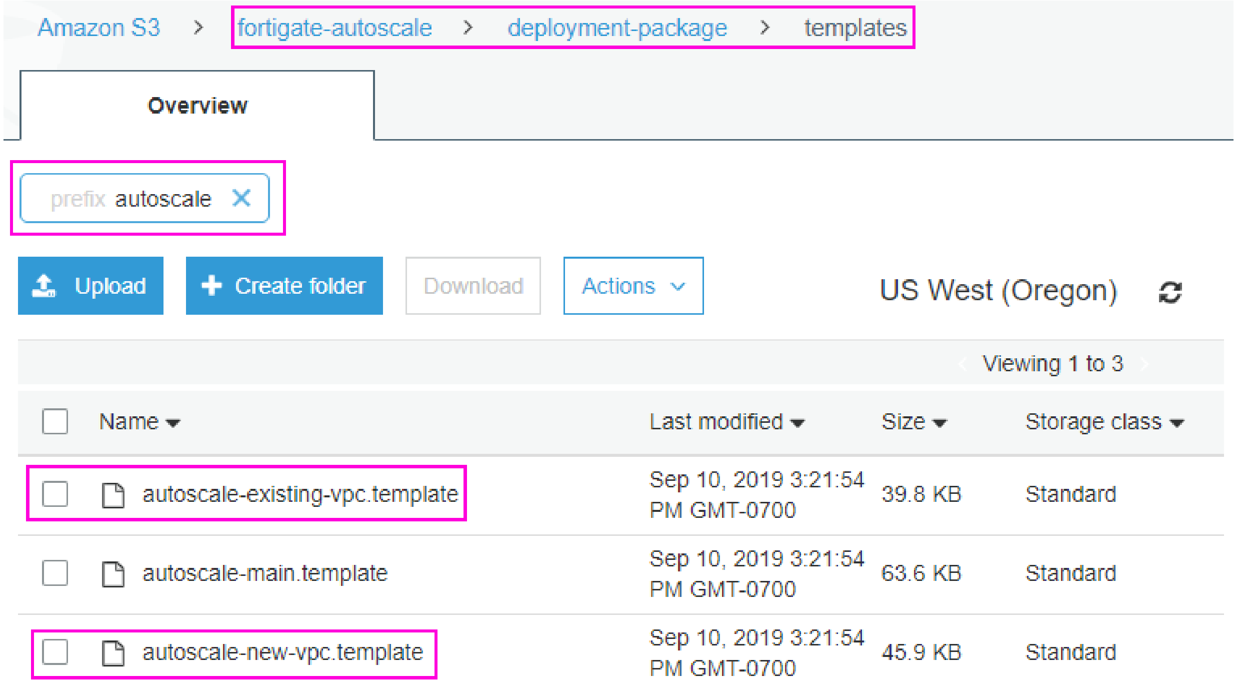
Incoming and outgoing requests

- 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.

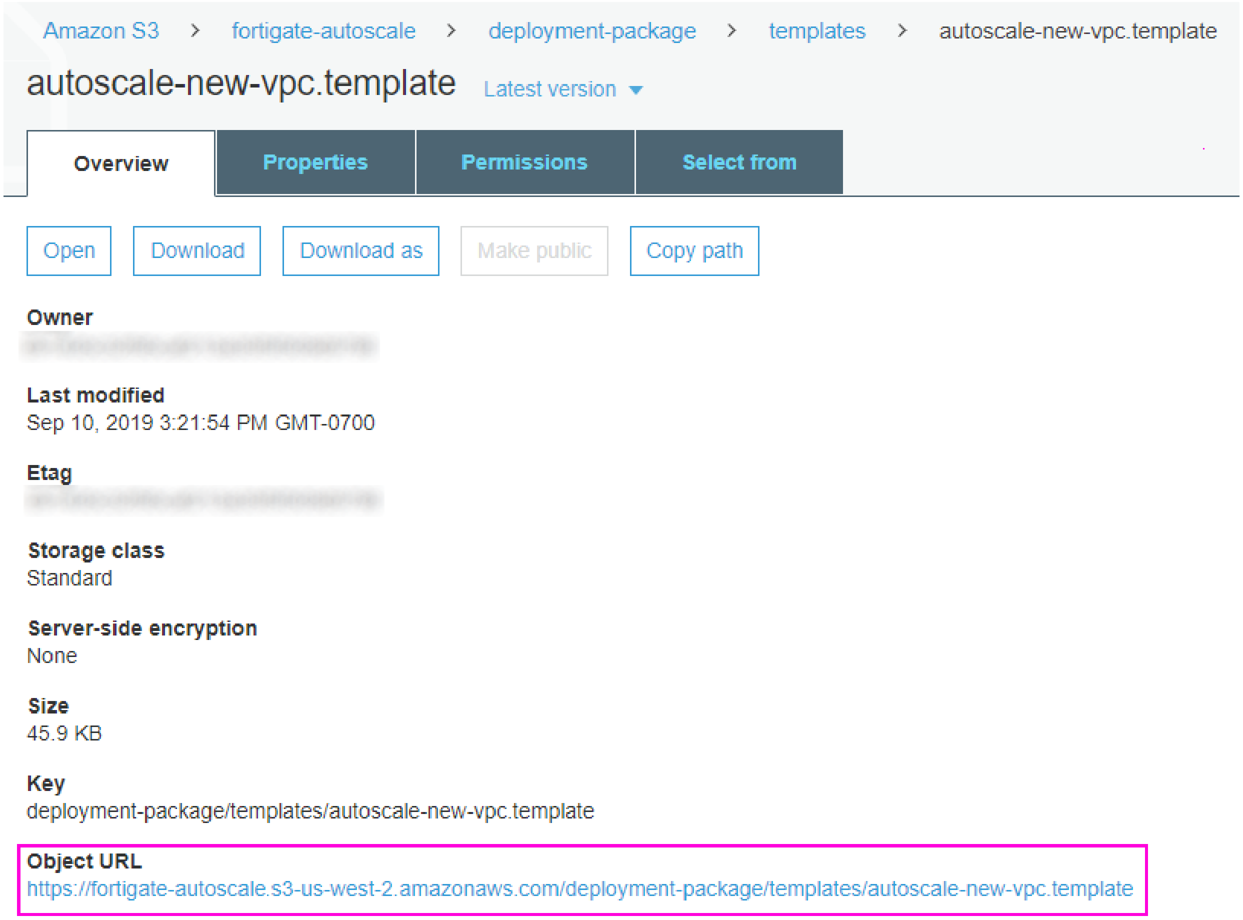
To deploy the CloudFormation templates:

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 `autoscale-new-vpc.template`.
   - To deploy into an existing VPC, click `autoscale-existing-vpc.template`.



	Name	Last modified	Size	Storage class
□	autoscale-existing-vpc.template	Sep 10, 2019 3:21:54 PM GMT-0700	39.8 KB	Standard
□	autoscale-main.template	Sep 10, 2019 3:21:54 PM GMT-0700	63.6 KB	Standard
□	autoscale-new-vpc.template	Sep 10, 2019 3:21:54 PM GMT-0700	45.9 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.


Amazon S3 > fortigate-autoscale > deployment-package > templates > autoscale-new-vpc.template
autoscale-new-vpc.template
Latest version
Overview
Properties
Permissions
Select from
Open
Download
Download as
Make public
Copy path

Owner
[redacted]

Last modified
Sep 10, 2019 3:21:54 PM GMT-0700

Etag
[redacted]

Storage class
Standard

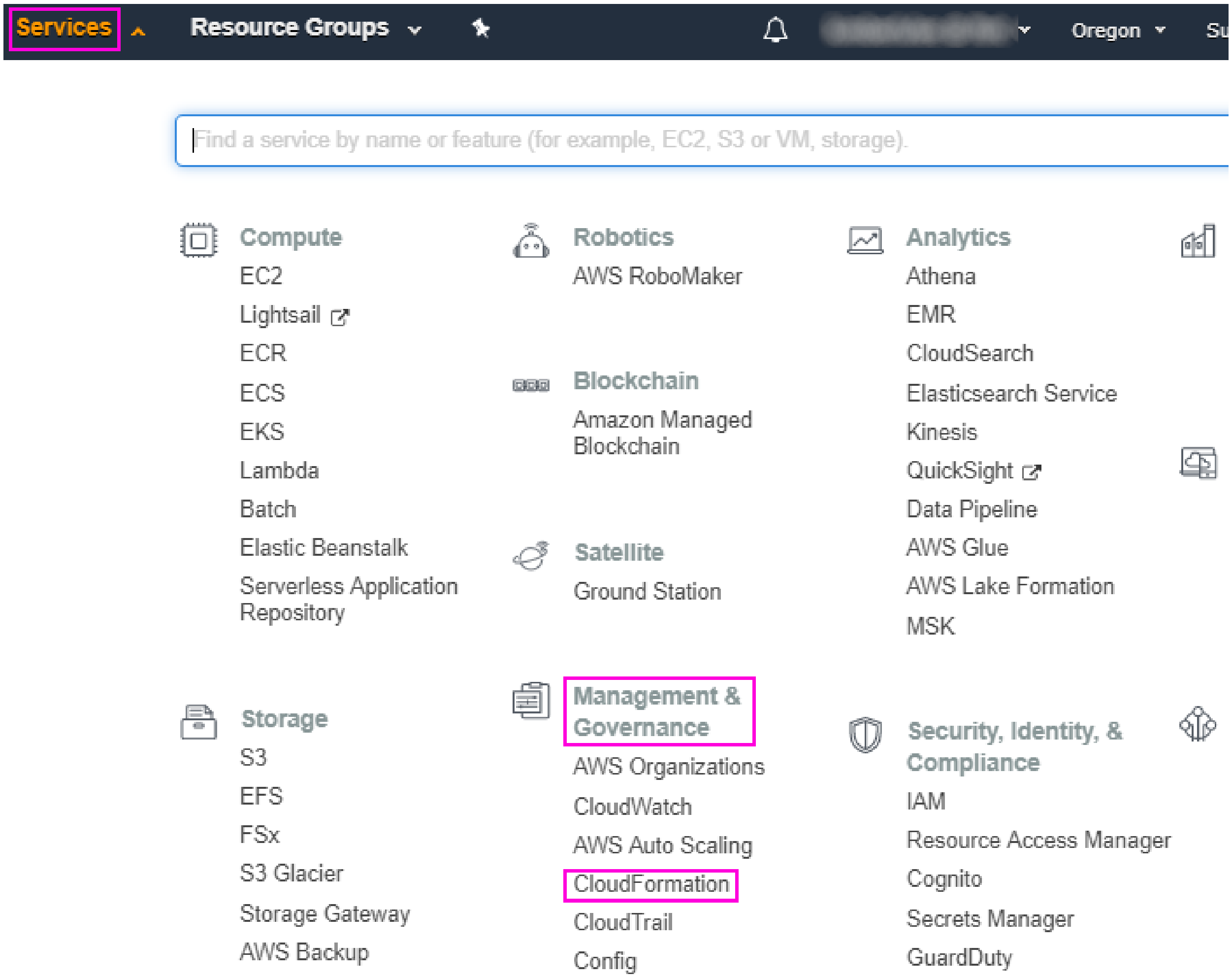
Server-side encryption
None

Size
45.9 KB

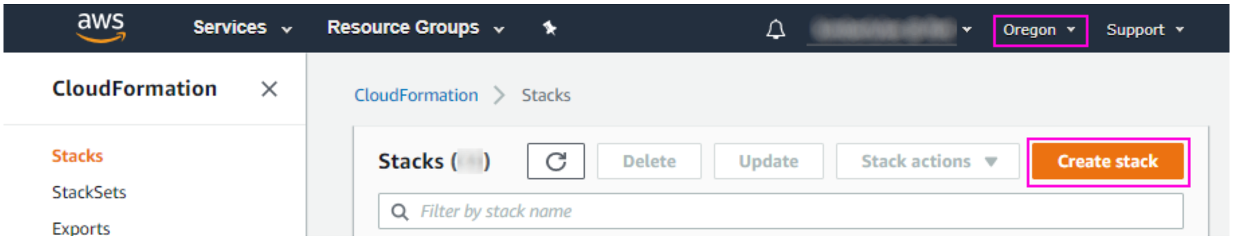
Key
deployment-package/templates/autoscale-new-vpc.template

Object URL
https://fortigate-autoscale.s3-us-west-2.amazonaws.com/deployment-package/templates/autoscale-new-vpc.template

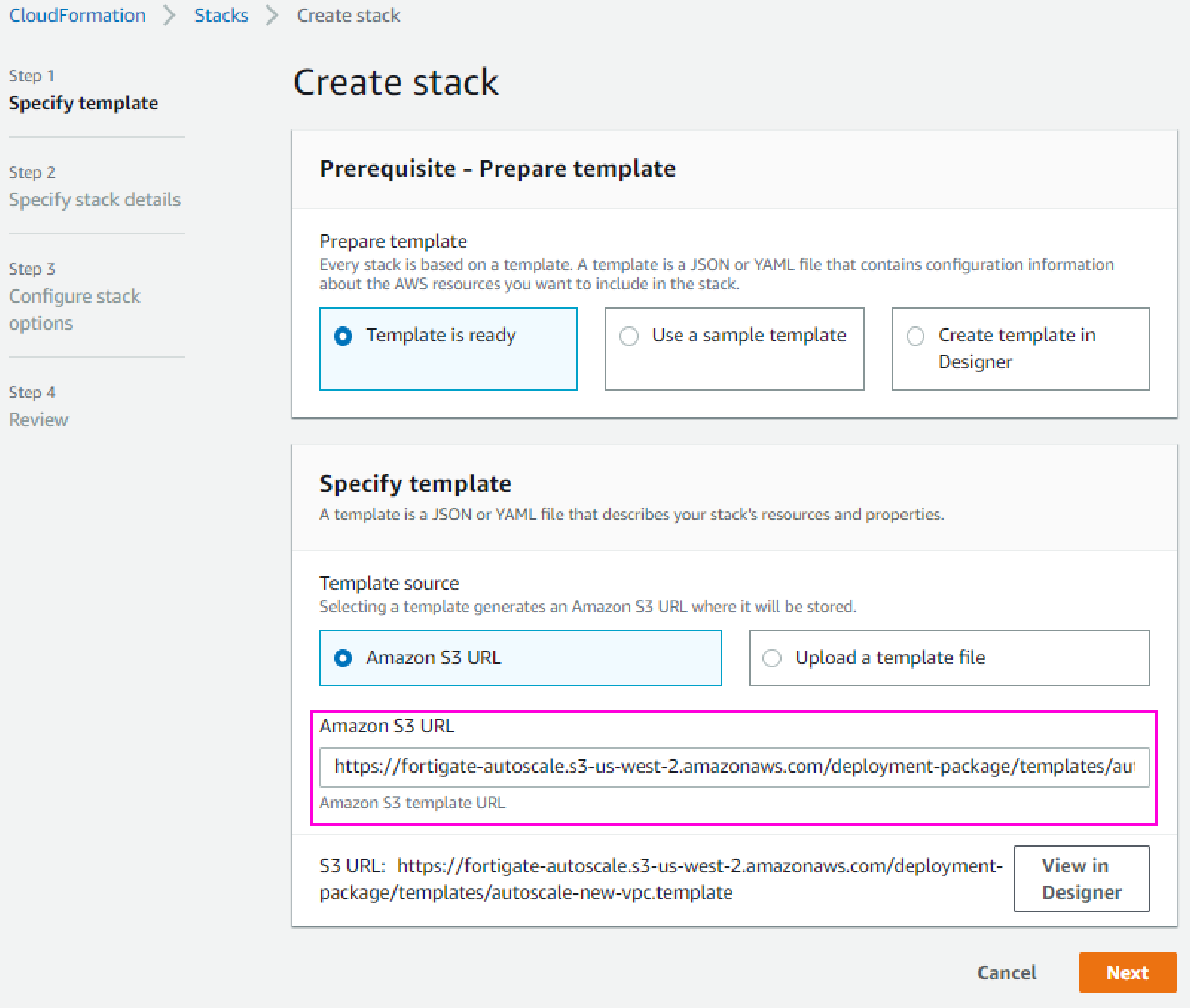
4. Click *Services*, and then *Management & Governance* > *CloudFormation*.



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



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



CloudFormation > Stacks > Create stack

Step 1
Specify template

Step 2
Specify stack details

Step 3
Configure stack options

Step 4
Review

Create stack

Prerequisite - Prepare template

Prepare template

Every stack is based on a template. A template is a JSON or YAML file that contains configuration information about the AWS resources you want to include in the stack.

● Template is ready ○ Use a sample template ○ Create template in Designer

Specify template

A template is a JSON or YAML file that describes your stack's resources and properties.

Template source

Selecting a template generates an Amazon S3 URL where it will be stored.

● Amazon S3 URL ○ Upload a template file

Amazon S3 URL

https://fortigate-autoscale.s3-us-west-2.amazonaws.com/deployment-package/templates/au

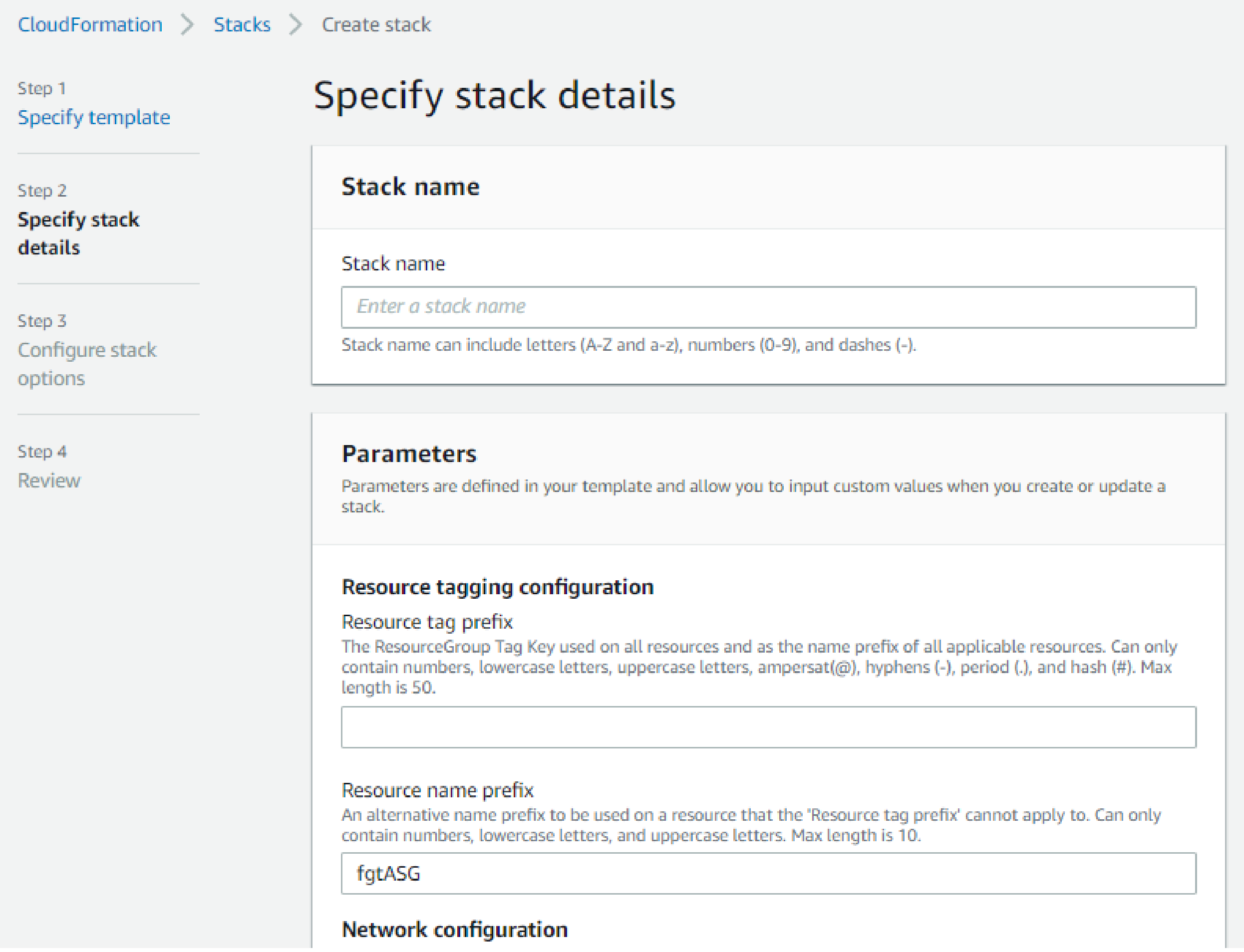
Amazon S3 template URL

S3 URL: https://fortigate-autoscale.s3-us-west-2.amazonaws.com/deployment-package/templates/autoscale-new-vpc.template

7. Click *Next*.

CFT parameters

In *Step 2 Specify stack details*, you enter the stack name and CFT parameters.



Specify stack details

Stack name

Stack name

Enter a stack name

Stack name can include letters (A-Z and a-z), numbers (0-9), and dashes (-).

Parameters

Parameters are defined in your template and allow you to input custom values when you create or update a stack.

Resource tagging configuration

Resource tag prefix

The ResourceGroup Tag Key used on all resources and as the name prefix of all applicable resources. Can only contain numbers, lowercase letters, uppercase letters, ampersat(@), hyphens (-), period (.), and hash (#). Max length is 50.

Resource name prefix

An alternative name prefix to be used on a resource that the 'Resource tag prefix' cannot apply to. Can only contain numbers, lowercase letters, and uppercase letters. Max length is 10.

fgtASG

Network configuration

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

Resource tagging configuration

Parameter label (name)	Default	Description
Resource tag prefix (ResourceTagPrefix)	Requires input	The *ResourceGroup* Tag Key used on all resources and as the name prefix of all applicable resources. Can only contain uppercase letters, lowercase letters, and numbers, ampersat(@), hyphens (-), period (.), and hash (#). Maximum length is 50.
Resource name prefix (CustomIdentifier)	fgtASG	An alternative name prefix to be used on a resource that the *Resource tag prefix* cannot apply to. Can only contain uppercase letters, lowercase letters, and numbers. Maximum length is 10.

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)	192.168.0.0/16	The Classless Inter-Domain Routing (CIDR) block for the FortiGate Autoscale VPC.
Autoscale subnet 1 CIDR (PublicSubnet1CIDR)	192.168.0.0/24	The CIDR block for the subnet located in AZ 1 where the FortiGate Autoscale instances will be deployed to.
Autoscale subnet 2 CIDR (PublicSubnet2CIDR)	192.168.1.0/24	The CIDR block for the subnet located in AZ 2 where the FortiGate Autoscale instances will be deployed to.
Protected subnet 1 CIDR (PrivateSubnet1CIDR)	192.168.2.0/24	The CIDR block for the private subnet located in AZ 1 where it is protected by the FortiGates in the public subnet of the same AZ.
Protected subnet 2 CIDR (PrivateSubnet2CIDR)	192.168.3.0/24	The CIDR block for the private subnet located in AZ 2 where it is protected by the FortiGates in the public subnet of the same AZ.

Network configuration (Existing VPC)

Parameter label (name)	Default	Description
VPC ID (VpcId)	Requires input	The ID of the existing VPC where FortiGate Autoscale will be deployed. The VPC must have the option *DNS hostnames* enabled and each of the two AZs in the VPC must have at least 1 public subnet and at least 1 private subnet.
VPC CIDR (VPCCIDR)	Requires input	The CIDR block of the selected existing VPC. This can be found in parentheses in the VPC ID parameter selection.
FortiGate subnet 1 (PublicSubnet1)	Requires input	The ID of the public subnet 1 located in AZ 1 of the selected existing VPC.
FortiGate subnet 2 (PublicSubnet2)	Requires input	The ID of the public subnet 2 located in AZ 2 of the selected existing VPC.
Protected subnet 1 (PrivateSubnet1)	Requires input	The ID of the private subnet 1 located in AZ 1 of the selected existing VPC. This subnet will be protected by the FortiGates in the public subnet of the same AZ.
Protected subnet 2 (PrivateSubnet2)	Requires input	The ID of the private subnet 2 located in AZ 2 of the selected existing VPC. This subnet will be protected by the FortiGates in the public subnet of the same AZ.

Parameter label (name)	Default	Description
Route table ID (PrivateSubnetRouteTable)	Requires input	Route table ID associated with the two private subnets.

FortiGate-VM configuration

Parameter label (name)	Default	Description
Instance type (FortiGateInstanceType)	c5.large	Instance type to launch for the FortiGate-VMs in the Auto Scaling group. 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.
FortiOS version (FortiOSVersion)	6.2.3	FortiOS version supported by FortiGate Autoscale for AWS.
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 and may contain special characters. 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. Do not use the FortiGate reserved ports 443, 541, 514, or 703. Minimum is 1. Maximum is 65535.
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
Desired capacity (BYOL) (FgtAsgDesiredCapacityByol)	2	The number of FortiGate-VM instances the BYOL Auto Scaling group should have at any time. For High Availability in BYOL-only and Hybrid use cases, ensure at least 2 FortiGate-VMs are in the group.

Parameter label (name)	Default	Description
		For specific use cases, set to 0 for On-Demand-only, and >= 2 for BYOL-only or hybrid licensing.
Minimum group size (BYOL) (FgtAsgMinSizeByol)	2	Minimum number of FortiGate-VM instances in the BYOL Auto Scaling group. For specific use cases, set to 0 for On-Demand-only, and >= 2 for BYOL-only or hybrid licensing. For BYOL-only and hybrid licensing deployments, this parameter must be at least 2. If it is set to 1 and the instance fails to work, the current FortiGate-VM configuration will be lost.
Maximum group size (BYOL) (FgtAsgMaxSizeByol)	2	Maximum number of FortiGate-VM instances in the BYOL Auto Scaling group. For specific use cases, set to 0 for On-Demand-only, and >= 2 for BYOL-only or hybrid licensing. This number must be greater than or equal to the *Minimum group size (BYOL)*.
Desired capacity (On-Demand instances) (FgtAsgDesiredCapacityPayg)	0	The number of FortiGate-VM instances the On-Demand Auto Scaling group should have at any time. For High Availability in an On-Demand-only use case, ensure at least 2 FortiGate-VMs are in the group. For specific use cases, set to 0 for BYOL-only, >= 2 for On-Demand-only, and >= 0 for hybrid licensing.
Minimum group size (On-Demand instances) (FgtAsgMinSizePayg)	0	Minimum number of FortiGate-VM instances in the On-Demand Auto Scaling group. For specific use cases, set to 0 for BYOL-only, >= 2 for On-Demand-only, and >= 0 for hybrid licensing. For On-Demand-only deployments, this parameter must be at least 2. If it is set to 1 and the instance fails to work, the current FortiGate-VM configuration will be lost.
Maximum group size (On-Demand instances) (FgtAsgMaxSizePayg)	0	Maximum number of FortiGate-VM instances in the On-Demand Auto Scaling group. For specific use cases, set to 0 for BYOL-only, >= 2 for On-Demand-only, and >= 0 for hybrid licensing. This number must be greater than or equal to the *Minimum group size (On-Demand instances)*.
Scale-out threshold (FgtAsgScaleOutThreshold)	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 (FgtAsgScaleInThreshold)	25	The threshold (in percentage) for the FortiGate-VM Auto Scaling group to scale in (remove) 1 instance.

Parameter label (name)	Default	Description
		Minimum is 1. Maximum is 100.
Master election timeout (MasterElectionTimeout)	300	The maximum time (in seconds) to wait for a master election to complete. Minimum is 30. Maximum is 3600.
Get license grace period (GetLicenseGracePeriod)	600	The minimum time (in seconds) permitted before a distributed license can be revoked from a non-responsive FortiGate and re-distributed. Minimum is 300.
Health check grace period (FgtAsgHealthCheckGracePeriod)	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 (FgtAsgCooldown)	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.
Instance lifecycle timeout (LifecycleHookTimeout)	480	The amount of time (in seconds) that can elapse before the FortiGate Autoscale lifecycle hook times out. Minimum is 60. Maximum is 3600.

Load balancing configuration

Parameter label (name)	Default	Description
Traffic protocol (LoadBalancingTrafficProtocol)	HTTPS	Use this protocol to load balance traffic.
Traffic port (LoadBalancingTrafficPort)	443	Balance web service traffic over this port if the internal web-service load balancer is enabled. Minimum is 1. Maximum is 65535.
Health check threshold (LoadBalancingHealthCheckThreshold)	3	The number of consecutive health check failures required before considering a FortiGate instance unhealthy. Minimum 3.
Internal ELB options (InternalLoadBalancingOptions)	add a new internal load balancer	Add an optional predefined Elastic Load Balancer (ELB) to route traffic to web service in the private subnets. You can optionally use your own one or decide to not need one.
Health check path (InternalTargetGroupHealthCheckPath)	/	Optional. The destination path for health checks. This path must begin with a '/' character, and can be at most 1024 characters in length.

Parameter label (name)	Default	Description
Internal ELB DNS name (InternalLoadBalancerDnsName)	Requires input	Optional. Specify the DNS Name of an existing internal load balancer used to route traffic from a FortiGate to targets in a specified target group. Leave it blank if you don't use an existing load balancer.

Failover management configuration

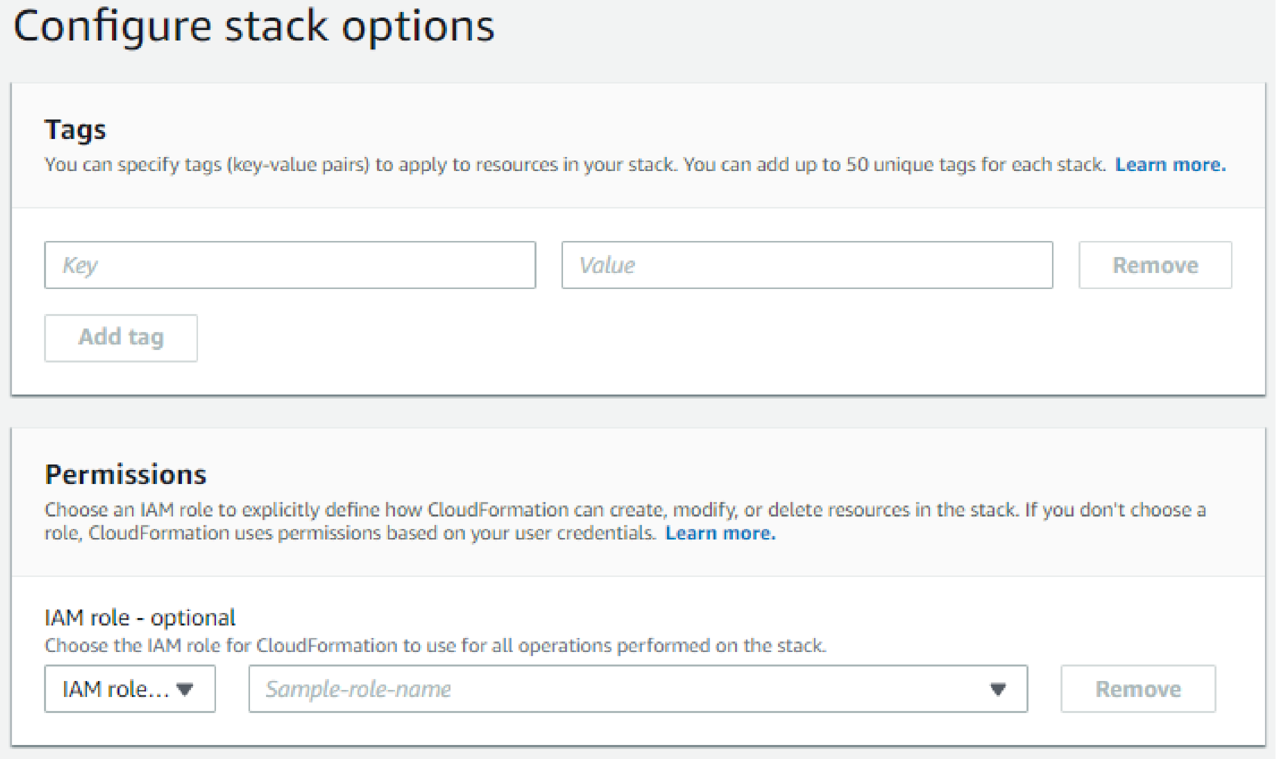
Parameter label (name)	Default	Description
Heart beat interval (HeartBeatInterval)	30	The length of time (in seconds) that a FortiGate-VM waits between sending heartbeat requests to the Autoscale handler. Minimum is 30. Maximum is 90.
Heart beat loss count (HeartBeatLossCount)	3	Number of consecutively lost heartbeats. When the Heartbeat loss count has been reached, the FortiGate-VM is deemed unhealthy and failover activities will commence.
Heart beat delay allowance (HeartBeatDelayAllowance)	2	The maximum amount of time (in seconds) allowed for network latency of the FortiGate-VM heartbeat arriving at the Autoscale handler. Minimum is 0.

Deployment resources configuration

Parameter label (name)	Default	Description
S3 bucket name (S3BucketName)	Requires input	Name of the S3 bucket (created in step 4 of Obtaining the deployment package on page 8) that contains the FortiGate Autoscale deployment package. Can only contain numbers, lowercase letters, uppercase letters, and hyphens (-). It cannot start or end with a hyphen (-).
S3 resource folder (S3KeyPrefix)	Requires input	Name of the S3 folder (created in step 5 of Obtaining the deployment package on page 8) that stores the FortiGate Autoscale deployment resources. Can only contain numbers, lowercase letters, uppercase letters, hyphens (-), and forward slashes (/). If provided, it must end with a forward slash (/).

Configuring optional settings

1. After entering required parameters and clicking *Next*, you are directed to the *Configure stack options* page:



Configure stack options

Tags

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

Permissions

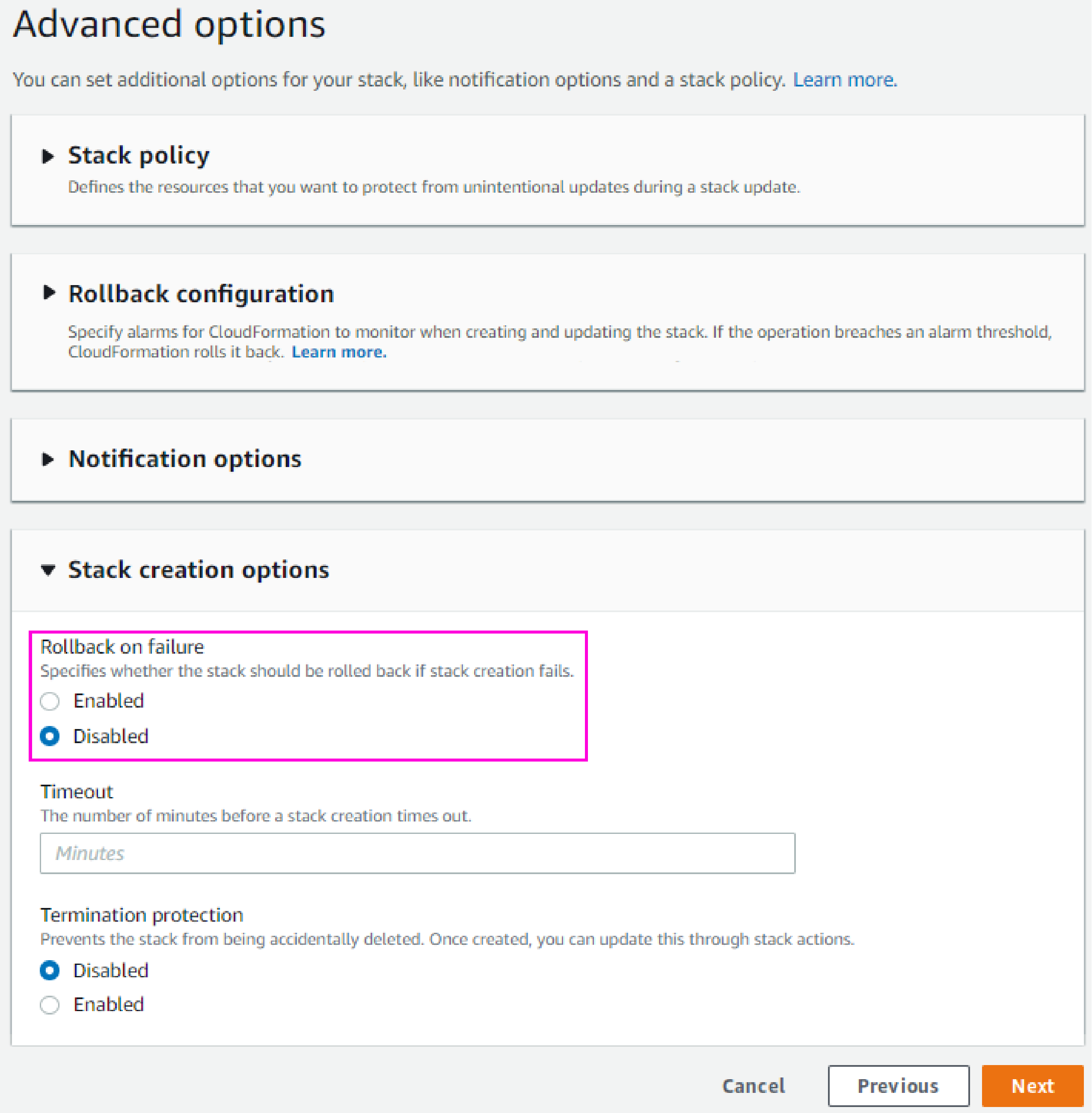
Choose an IAM role to explicitly define how CloudFormation can create, modify, or delete resources in the stack. If you don't choose a role, CloudFormation uses permissions based on your user credentials. Learn more.

IAM role - optional

Choose the IAM role for CloudFormation to use for all operations performed on the stack.

2. (Optional) Specify *Tags* and *Permissions* as desired:
   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.

3. *Advanced options* follow:



Advanced options

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

▶ **Stack policy**

Defines the resources that you want to protect from unintentional updates during a stack update.

▶ **Rollback configuration**

Specify alarms for CloudFormation to monitor when creating and updating the stack. If the operation breaches an alarm threshold, CloudFormation rolls it back. Learn more.

▶ **Notification options**

▼ **Stack creation options**

Rollback on failure

Specifies whether the stack should be rolled back if stack creation fails.

○ Enabled

● Disabled

Timeout

The number of minutes before a stack creation times out.

Minutes

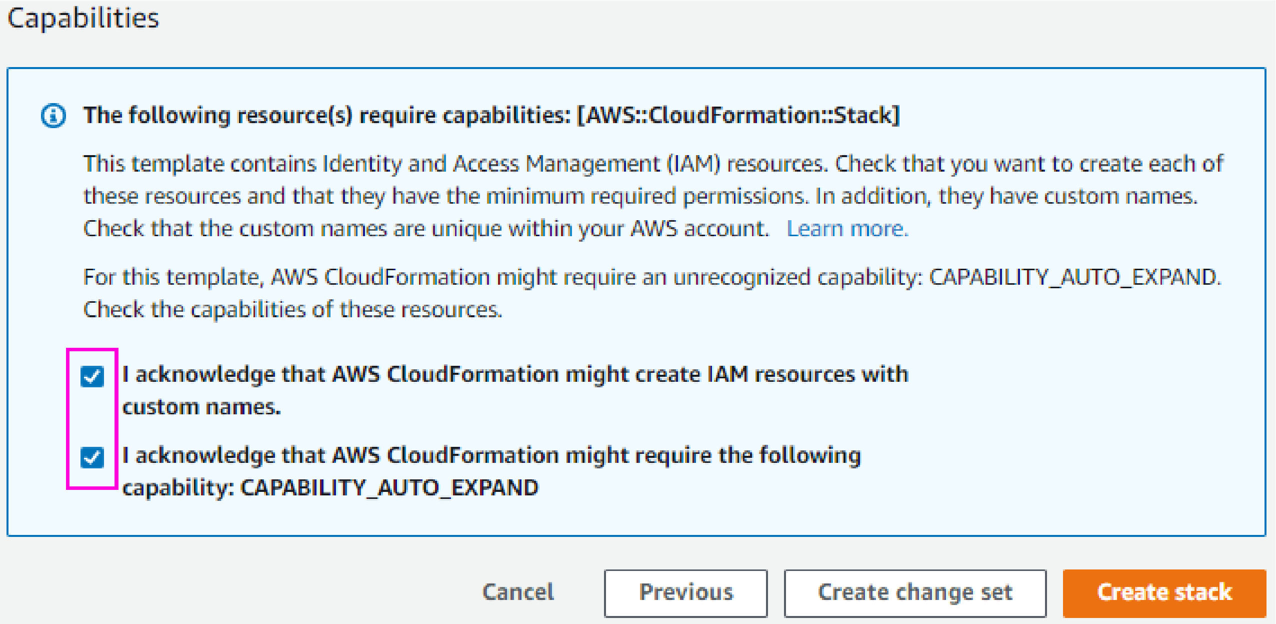
Termination protection

Prevents the stack from being accidentally deleted. Once created, you can update this through stack actions.

● Disabled

○ Enabled

4. It is recommended that you disable the Stack creation option *Rollback on failure*. This will allow for a better troubleshooting experience. Other advanced options can be specified as desired.
5. Click *Next*.
6. On the *Review* page, review and confirm the template, the stack details, and the stack options. Under *Capabilities*, select both check boxes.



Capabilities

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

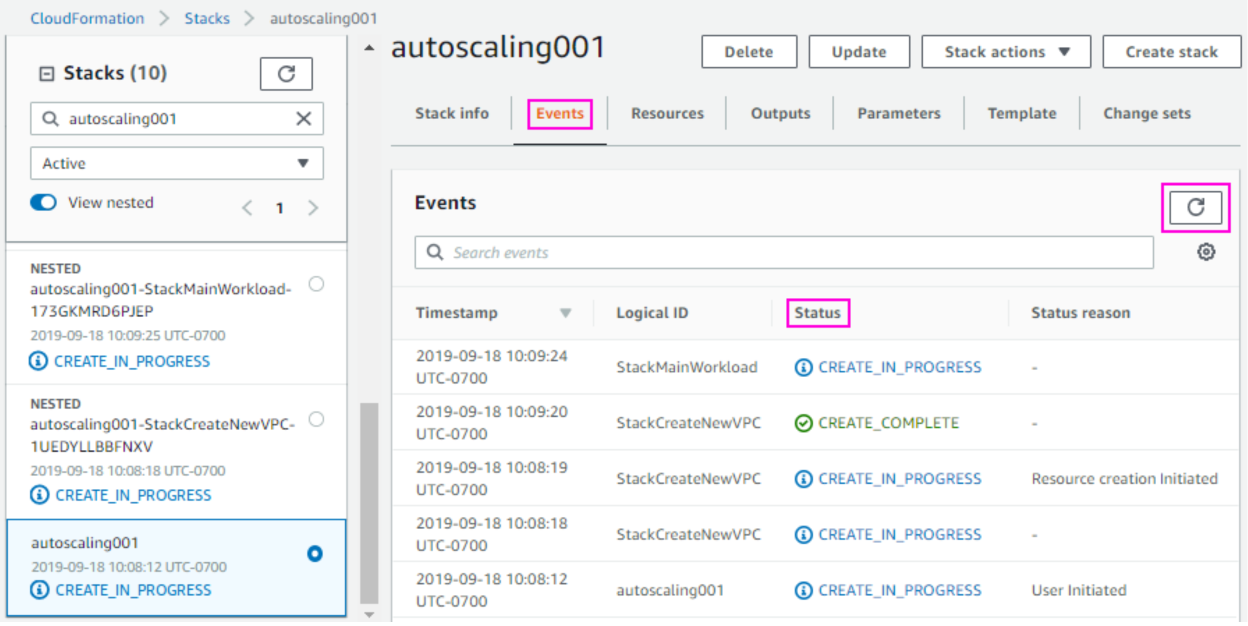
This template contains Identity and Access Management (IAM) resources. Check that you want to create each of these resources and that they have the minimum required permissions. In addition, they have custom names. Check that the custom names are unique within your AWS account. Learn more.

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**

7. 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 10 minutes to create the stack.



NESTED
autoscaling001-StackMainWorkload-173GKMRD6PJEP
2019-09-18 10:09:25 UTC-0700
ⓘ CREATE_IN_PROGRESS

NESTED
autoscaling001-StackCreateNewVPC-1UEDYLLBBFNXV
2019-09-18 10:08:18 UTC-0700
ⓘ CREATE_IN_PROGRESS

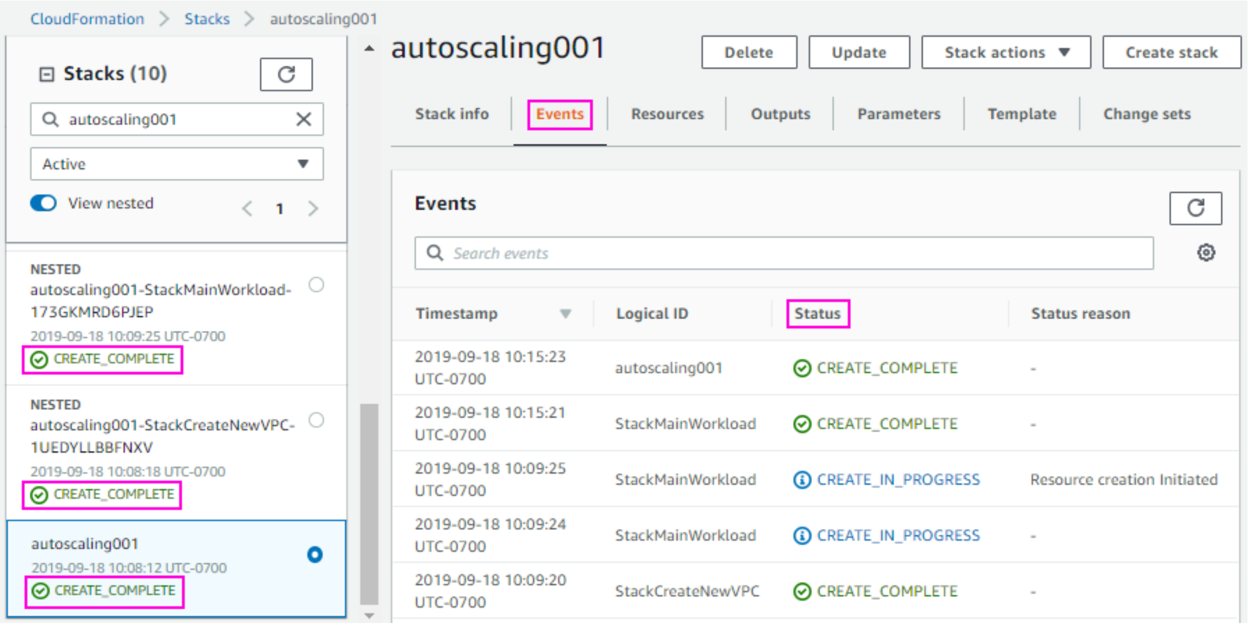
autoscaling001
2019-09-18 10:08:12 UTC-0700
ⓘ CREATE_IN_PROGRESS

autoscaling001

Events

Timestamp	Logical ID	Status	Status reason
2019-09-18 10:09:24 UTC-0700	StackMainWorkload	ⓘ CREATE_IN_PROGRESS	-
2019-09-18 10:09:20 UTC-0700	StackCreateNewVPC	✓ CREATE_COMPLETE	-
2019-09-18 10:08:19 UTC-0700	StackCreateNewVPC	ⓘ CREATE_IN_PROGRESS	Resource creation Initiated
2019-09-18 10:08:18 UTC-0700	StackCreateNewVPC	ⓘ CREATE_IN_PROGRESS	-
2019-09-18 10:08:12 UTC-0700	autoscaling001	ⓘ CREATE_IN_PROGRESS	User Initiated

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



NESTED
autoscaling001-StackMainWorkload-173GKMRD6PJEP
2019-09-18 10:09:25 UTC-0700
CREATE_COMPLETE

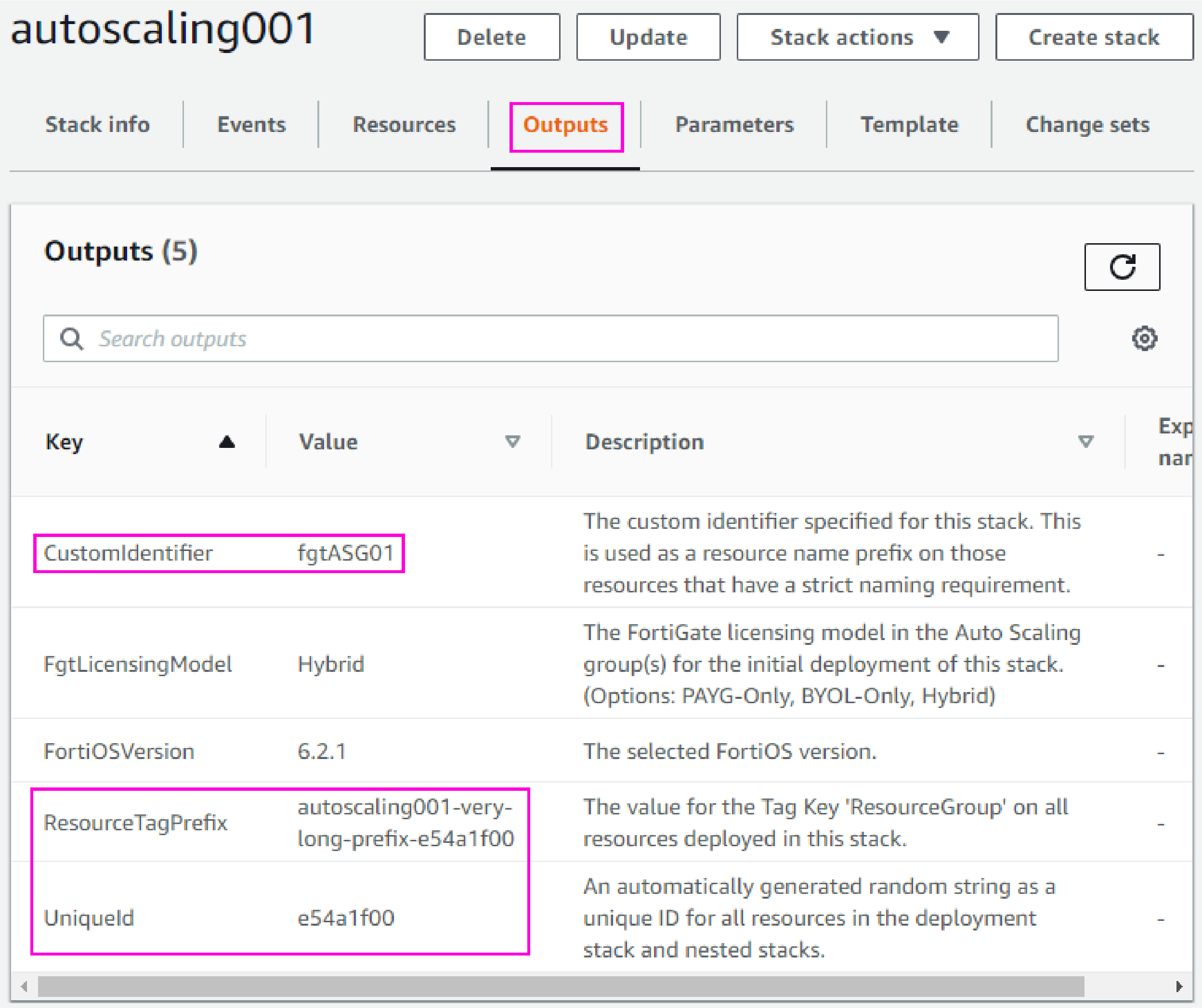
NESTED
autoscaling001-StackCreateNewVPC-1UEDYLLBBFNXV
2019-09-18 10:08:18 UTC-0700
CREATE_COMPLETE

autoscaling001
2019-09-18 10:08:12 UTC-0700
CREATE_COMPLETE

Timestamp	Logical ID	Status	Status reason
2019-09-18 10:15:23 UTC-0700	autoscaling001	CREATE_COMPLETE	-
2019-09-18 10:15:21 UTC-0700	StackMainWorkload	CREATE_COMPLETE	-
2019-09-18 10:09:25 UTC-0700	StackMainWorkload	CREATE_IN_PROGRESS	Resource creation Initiated
2019-09-18 10:09:24 UTC-0700	StackMainWorkload	CREATE_IN_PROGRESS	-
2019-09-18 10:09:20 UTC-0700	StackCreateNewVPC	CREATE_COMPLETE	-

Locating deployed resources

To locate a newly deployed resource, it is recommended to search for it using the *ResourceTagPrefix*, also referred to as the *ResourceGroup Tag Key*. Alternatively, the *UniqueID* can be used. For items that need a shorter prefix, the *CustomIdentifier* can be used. These keys are found on the *Outputs* tab as shown below. Note that the *UniqueID* is at the end of the *ResourceTagPrefix*.

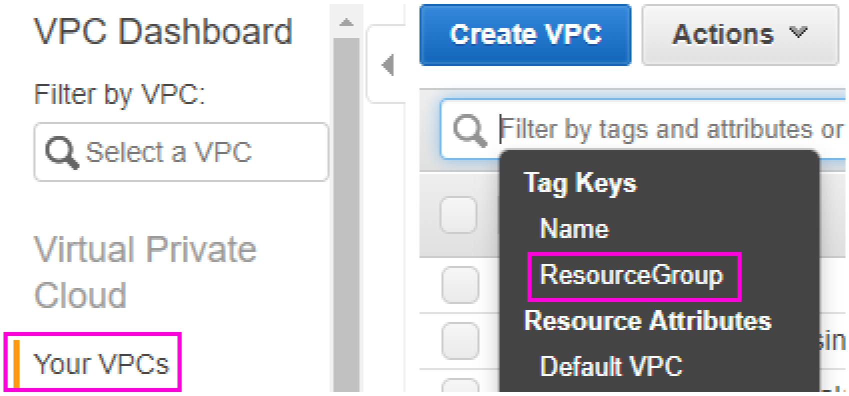


Outputs (5)

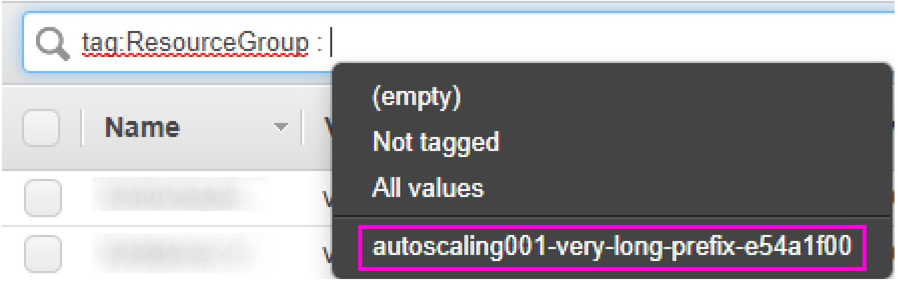
Key ▲	Value	Description	Exp nar
CustomIdentifier	fgtASG01	The custom identifier specified for this stack. This is used as a resource name prefix on those resources that have a strict naming requirement.	-
FgtLicensingModel	Hybrid	The FortiGate licensing model in the Auto Scaling group(s) for the initial deployment of this stack. (Options: PAYG-Only, BYOL-Only, Hybrid)	-
FortiOSVersion	6.2.1	The selected FortiOS version.	-
ResourceTagPrefix	autoscaling001-very-long-prefix-e54a1f00	The value for the Tag Key 'ResourceGroup' on all resources deployed in this stack.	-
UniqueId	e54a1f00	An automatically generated random string as a unique ID for all resources in the deployment stack and nested stacks.	-

To look up the newly deployed VPC using the Tag Key:

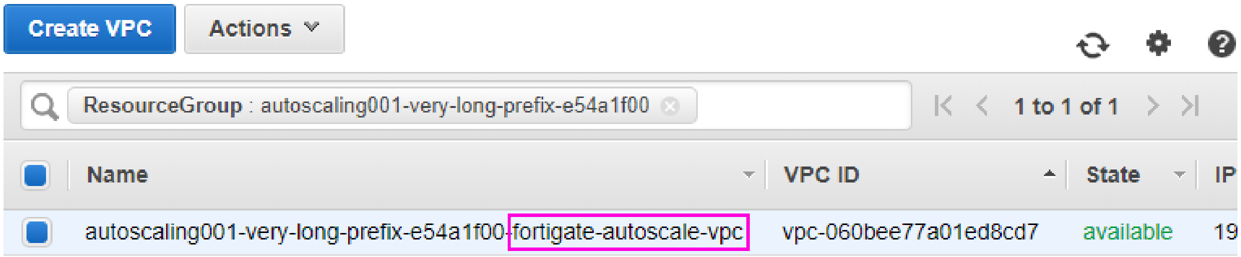
1. In the AWS console, select *Services* > *Network & Content Delivery* > *VPC*.
2. In the left navigation tree, click *Your VPCs*.
3. Click the filter box and select *Tag Keys* > *ResourceGroup*.



4. Select your *ResourceTagPrefix* from the list of Tag Keys.



Your VPC will be displayed. The *Name* of VPC is of the format *<ResourceTagPrefix>-fortigate-autoscale-vpc*.

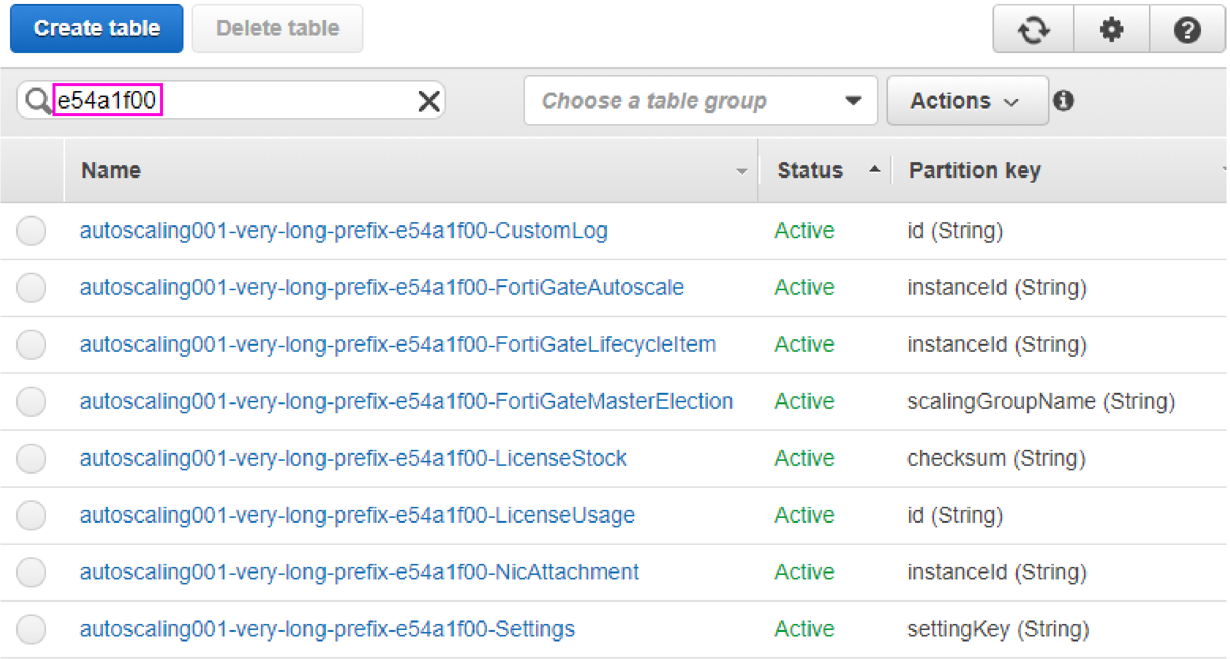


Name	VPC ID	State	IP
autoscaling001-very-long-prefix-e54a1f00-fortigate-autoscale-vpc	vpc-060bee77a01ed8cd7	available	19

To look up the newly deployed DynamoDB tables using the UniqueID:

1. In the AWS console, select *Services* > *Database* > *DynamoDB*.
2. In the left navigation tree, click *Tables*.
3. Click the filter box and enter the *UniqueID*.

The DynamoDB tables will be displayed. The *Name* of each DynamoDB table will be of the format *<ResourceTagPrefix>-<table-name>*.

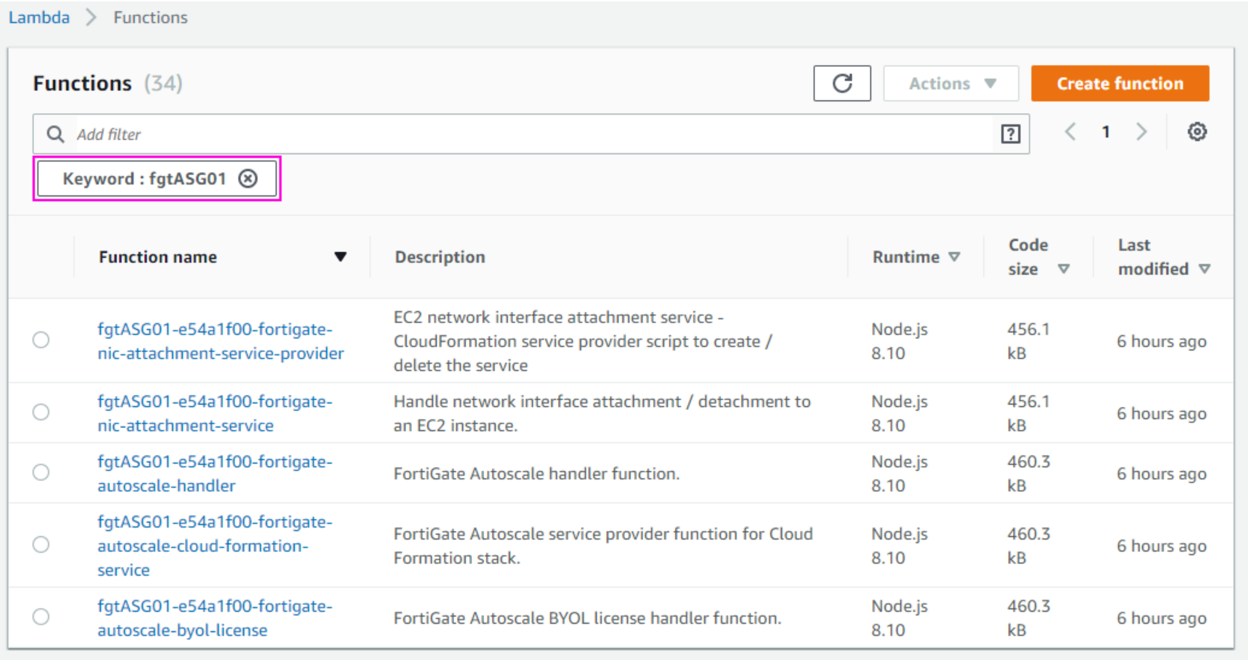


Name	Status	Partition key
autoscaling001-very-long-prefix-e54a1f00-CustomLog	Active	id (String)
autoscaling001-very-long-prefix-e54a1f00-FortiGateAutoscale	Active	instanceId (String)
autoscaling001-very-long-prefix-e54a1f00-FortiGateLifecycleItem	Active	instanceId (String)
autoscaling001-very-long-prefix-e54a1f00-FortiGateMasterElection	Active	scalingGroupName (String)
autoscaling001-very-long-prefix-e54a1f00-LicenseStock	Active	checksum (String)
autoscaling001-very-long-prefix-e54a1f00-LicenseUsage	Active	id (String)
autoscaling001-very-long-prefix-e54a1f00-NicAttachment	Active	instanceId (String)
autoscaling001-very-long-prefix-e54a1f00-Settings	Active	settingKey (String)

To look up the newly deployed Lambda Functions using the CustomIdentifier:

1. In the AWS console, select *Services* > *Compute* > *Lambda*.
2. In the left navigation tree, click *Functions*.
3. Click the filter box and enter the *CustomIdentifier*.

The Lambda Functions will be displayed. Each *Function name* will be of the format *<CustomIdentifier>-<UniqueID>-LambdaFunctionName*. Click the *Function name* to go directly to the function.



Function name	Description	Runtime	Code size	Last modified
fgtASG01-e54a1f00-fortigate-nic-attachment-service-provider	EC2 network interface attachment service - CloudFormation service provider script to create / delete the service	Node.js 8.10	456.1 kB	6 hours ago
fgtASG01-e54a1f00-fortigate-nic-attachment-service	Handle network interface attachment / detachment to an EC2 instance.	Node.js 8.10	456.1 kB	6 hours ago
fgtASG01-e54a1f00-fortigate-autoscale-handler	FortiGate Autoscale handler function.	Node.js 8.10	460.3 kB	6 hours ago
fgtASG01-e54a1f00-fortigate-autoscale-cloud-formation-service	FortiGate Autoscale service provider function for Cloud Formation stack.	Node.js 8.10	460.3 kB	6 hours ago
fgtASG01-e54a1f00-fortigate-autoscale-byol-license	FortiGate Autoscale BYOL license handler function.	Node.js 8.10	460.3 kB	6 hours ago

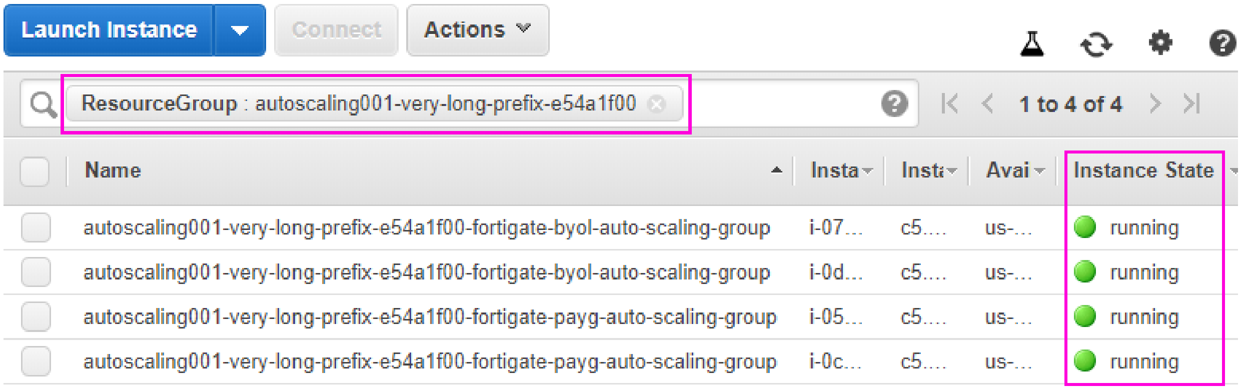
Verifying the deployment

FortiGate Autoscale for AWS without Transit Gateway integration creates an Auto Scaling group with lifecycle events attached to the group. Verify the following components:

- the Auto Scaling group
- the master election

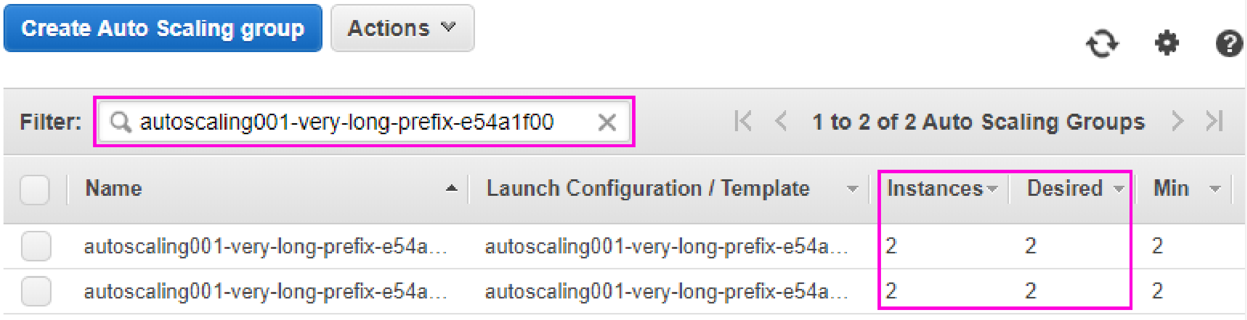
To verify the Auto Scaling group:

1. In the AWS console, select the *Services* > *Compute* > *EC2*.
2. In the left navigation tree, click *INSTANCES* > *Instances*.
3. Click the filter box and select *Tag Keys* > *ResourceGroup*.
4. Select your *ResourceTagPrefix* from the list of *Tag Keys*.
5. Instances will be listed along with a status. Confirm that the *Instance Status* for each instance is *running*.



Name	Insta	Insta	Avai	Instance State
autoscaling001-very-long-prefix-e54a1f00-fortigate-byol-auto-scaling-group	i-07...	c5....	us-...	● running
autoscaling001-very-long-prefix-e54a1f00-fortigate-byol-auto-scaling-group	i-0d...	c5....	us-...	● running
autoscaling001-very-long-prefix-e54a1f00-fortigate-payg-auto-scaling-group	i-05...	c5....	us-...	● running
autoscaling001-very-long-prefix-e54a1f00-fortigate-payg-auto-scaling-group	i-0c...	c5....	us-...	● running

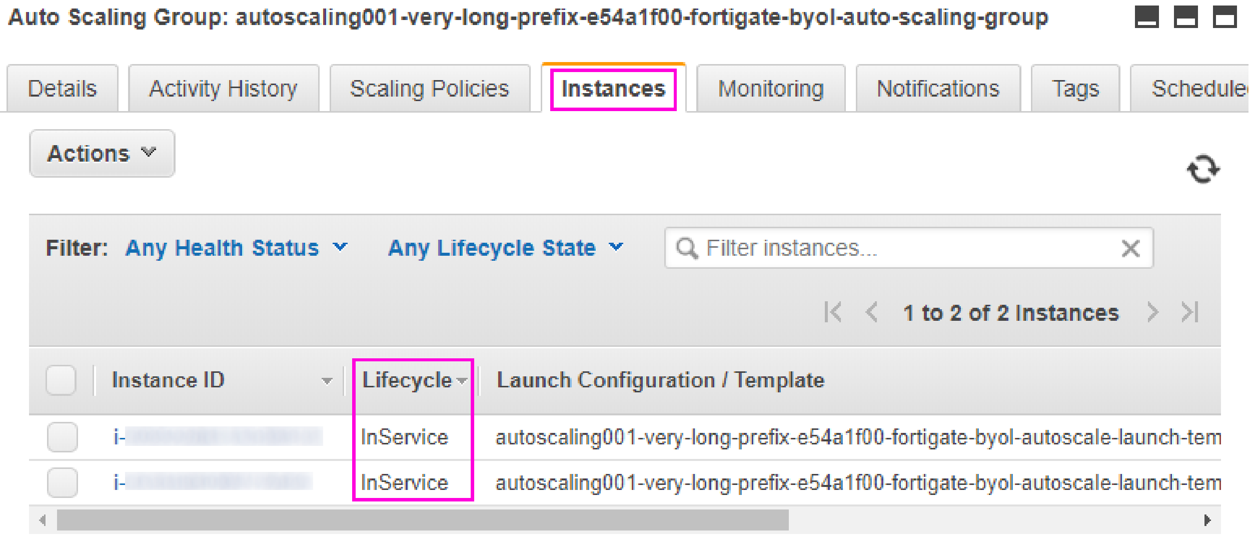
6. In the left navigation tree, click *AUTO SCALING* > *Auto Scaling Groups*.
7. Click the filter box and look up the Auto Scaling group using the *ResourceTagPrefix*.
8. The number of Auto Scaling groups listed is based on your implementation. The image below shows two Auto Scaling groups, one for BYOL instances, and one for On-Demand instances. Confirm that the number in the *Instances* column is equal to or greater than the *Desired Capacity* you specified.


Create Auto Scaling group
Actions
Filter:
autoscaling001-very-long-prefix-e54a1f00
1 to 2 of 2 Auto Scaling Groups

Name	Launch Configuration / Template	Instances	Desired	Min
autoscaling001-very-long-prefix-e54a...	autoscaling001-very-long-prefix-e54a...	2	2	2
autoscaling001-very-long-prefix-e54a...	autoscaling001-very-long-prefix-e54a...	2	2	2

9. For each Auto Scaling group, select the check box to left of the *Name*, and then click the *Instances* tab in the lower

pane and confirm that the *Lifecycle* of each instance is *InService*.

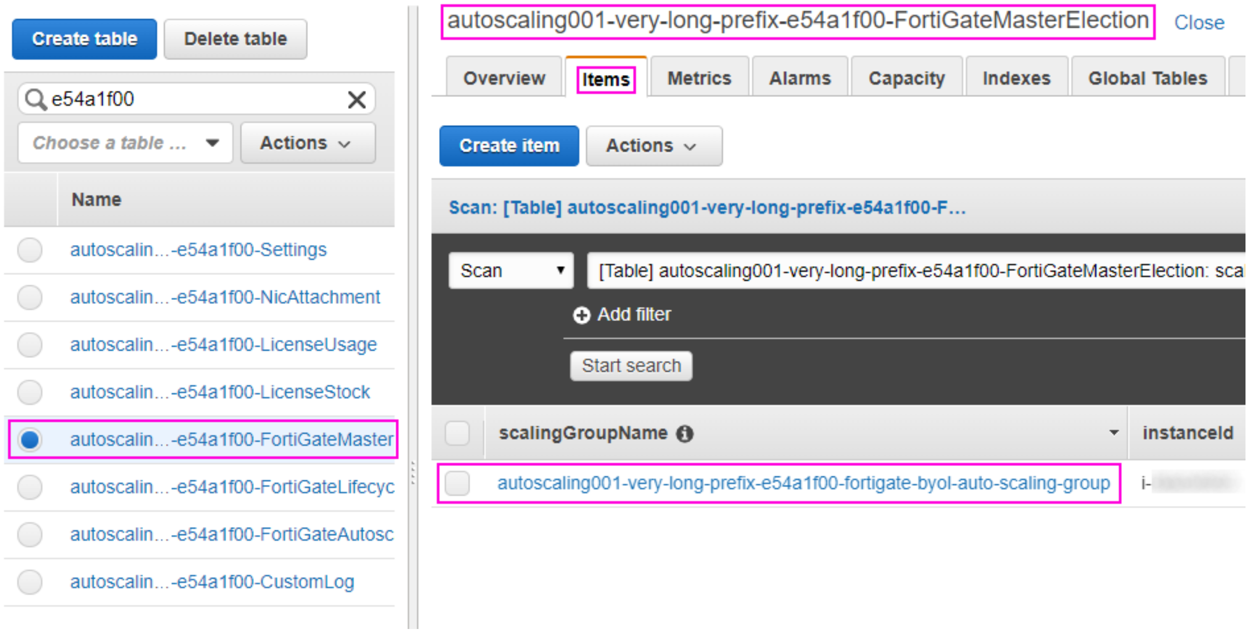


Auto Scaling Group: autoscaling001-very-long-prefix-e54a1f00-fortigate-byol-auto-scaling-group

Instance ID	Lifecycle	Launch Configuration / Template
i-[redacted]	InService	autoscaling001-very-long-prefix-e54a1f00-fortigate-byol-autoscale-launch-tem
i-[redacted]	InService	autoscaling001-very-long-prefix-e54a1f00-fortigate-byol-autoscale-launch-tem

To verify the master election:

1. Look up the DynamoDB table <*ResourceTagPrefix*>*-FortiGateMasterElection* as described in the section Locating deployed resources on page 24.
2. Select the <*ResourceTagPrefix*>*-FortiGateMasterElection* table.
3. In the right hand pane, select the *Items* tab.
4. The master record will be the only item listed. Click the master record.



Create table
Delete table
e54a1f00
Choose a table ...
Actions
autoscaling001-very-long-prefix-e54a1f00-FortiGateMasterElection
Close
Overview
Items
Metrics
Alarms
Capacity
Indexes
Global Tables
Create item
Actions
Scan: [Table] autoscaling001-very-long-prefix-e54a1f00-F...
Scan
[Table] autoscaling001-very-long-prefix-e54a1f00-FortiGateMasterElection: sca
Add filter
Start search

Name
autoscalin...-e54a1f00-Settings
autoscalin...-e54a1f00-NicAttachment
autoscalin...-e54a1f00-LicenseUsage
autoscalin...-e54a1f00-LicenseStock
autoscalin...-e54a1f00-FortiGateMaster
autoscalin...-e54a1f00-FortiGateLifecyc
autoscalin...-e54a1f00-FortiGateAutosc
autoscalin...-e54a1f00-CustomLog

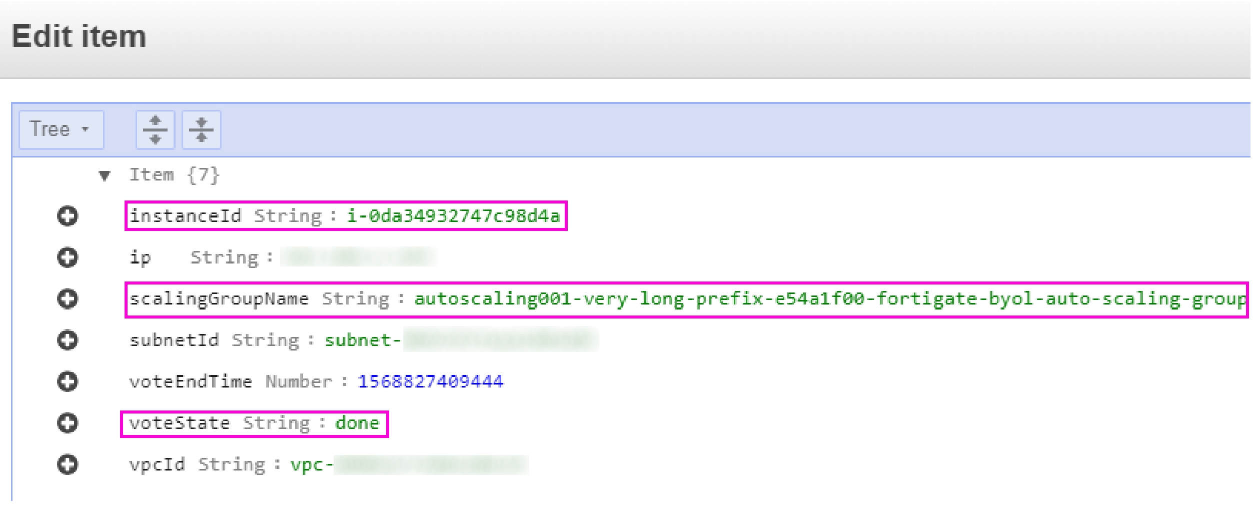
scalingGroupName	instanceId
autoscaling001-very-long-prefix-e54a1f00-fortigate-byol-auto-scaling-group	i-[redacted]

In the master record,

- *instanceId* is the instance ID of the master instance.
- *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 record will look as follows:



Edit item

```
▼ Item {7}
  instanceId String : i-0da34932747c98d4a
  ip  String : [redacted]
  scalingGroupName String : autoscaling001-very-long-prefix-e54a1f00-fortigate-byol-auto-scaling-group
  subnetId String : subnet-[redacted]
  voteEndTime Number : 1568827409444
  voteState String : done
  vpcId String : vpc-[redacted]
```

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

Make note of the *instanceID*, as you will need it to connect to the FortiGate-VM in the section Connecting to the master FortiGate-VM instance on page 30.

If you have both BYOL and On-Demand instances, you will also need the *scalingGroupName* to locate the master instance.

Connecting to the master FortiGate-VM instance

To connect to the master FortiGate-VM instance, you will need:

- a login URL
- a username (*admin*)
- a password (the *InstanceID* of the master FortiGate-VM instance)

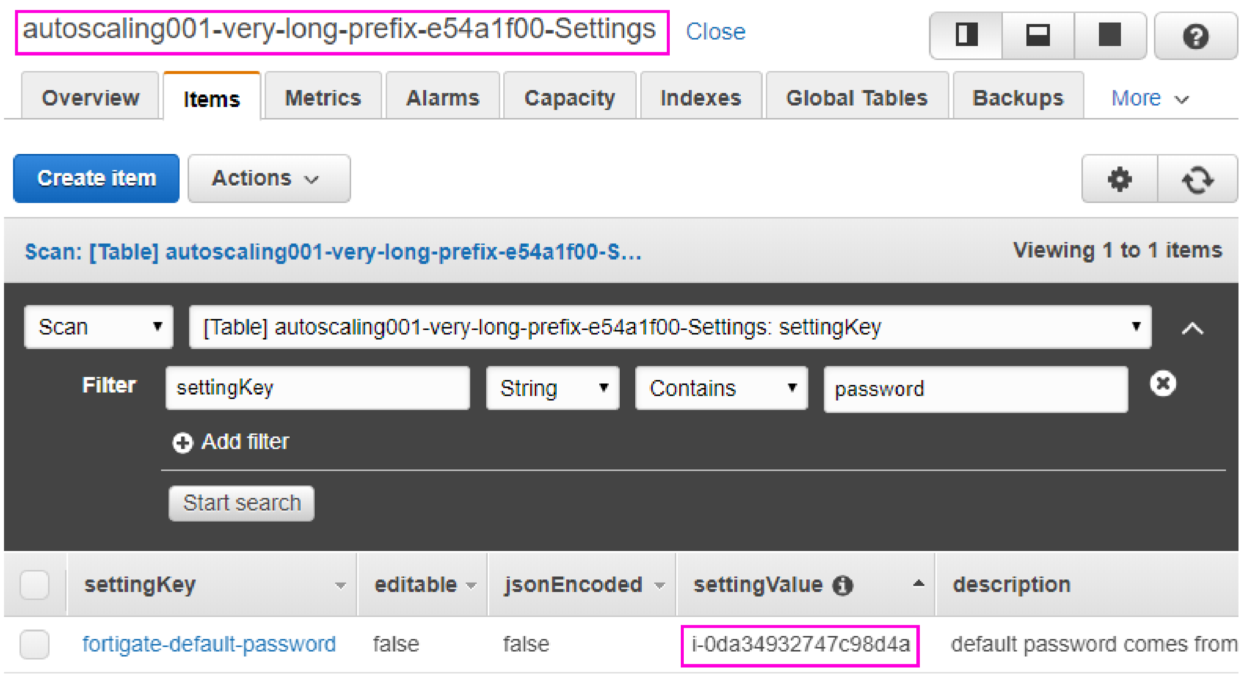
Deployments with both BYOL and On-Demand instances, also need the *scalingGroupName* of the master FortiGate-VM. This name is listed in the master record. For details on how to locate the master record, refer to the end of the section Verifying the deployment on page 28.

To obtain the password:

The initial password for all FortiGate-VM instances is the *instanceID* of the master FortiGate-VM. This *instanceID* is stored in the master record and in the DynamoDB table *<ResourceTagPrefix>-Settings*.

For details on how to locate the master record, refer to the end of the section Verifying the deployment on page 28.

For details on locating the DynamoDB table *<ResourceTagPrefix>-Settings*, refer to the section Locating deployed resources on page 24.



Scan: [Table] autoscaling001-very-long-prefix-e54a1f00-S...

Viewing 1 to 1 items

Scan: [Table] autoscaling001-very-long-prefix-e54a1f00-Settings: settingKey

Filter: settingKey | String | Contains | password

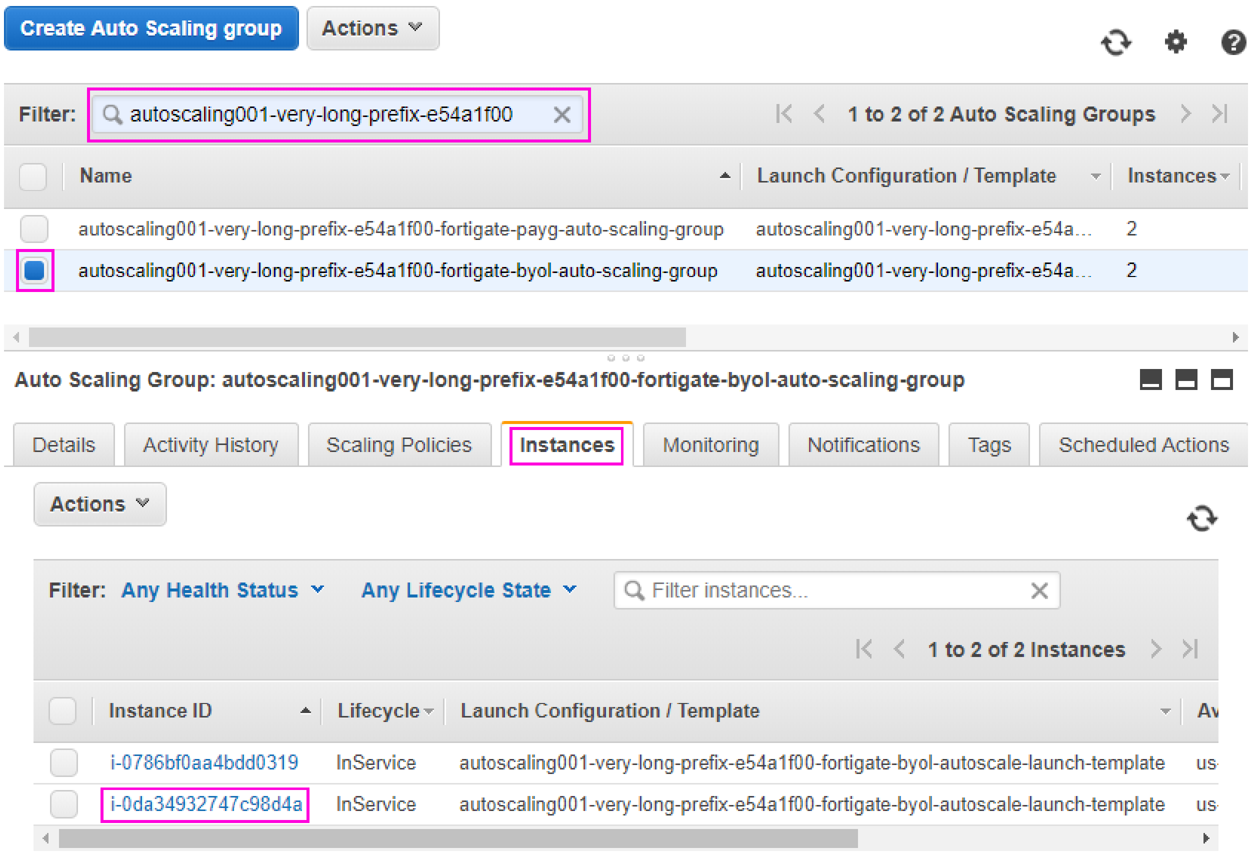
	settingKey	editable	jsonEncoded	settingValue	description
□	fortigate-default-password	false	false	i-0da34932747c98d4a	default password comes from

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.

To construct the login URL of the master FortiGate-VM instance:

1. Look up the Auto Scaling group(s) as described in steps 6-8 of the ASG portion of the section Verifying the deployment on page 28.
2. Select the Auto Scaling group that contains the master instance. If you have more than one instance type, two groups will be listed. The group containing the master instance is the group with the *scalingGroupName* listed in the master record.



Filter: autoscaling001-very-long-prefix-e54a1f00

1 to 2 of 2 Auto Scaling Groups

	Name	Launch Configuration / Template	Instances
□	autoscaling001-very-long-prefix-e54a1f00-fortigate-payg-auto-scaling-group	autoscaling001-very-long-prefix-e54a...	2
■	autoscaling001-very-long-prefix-e54a1f00-fortigate-byol-auto-scaling-group	autoscaling001-very-long-prefix-e54a...	2

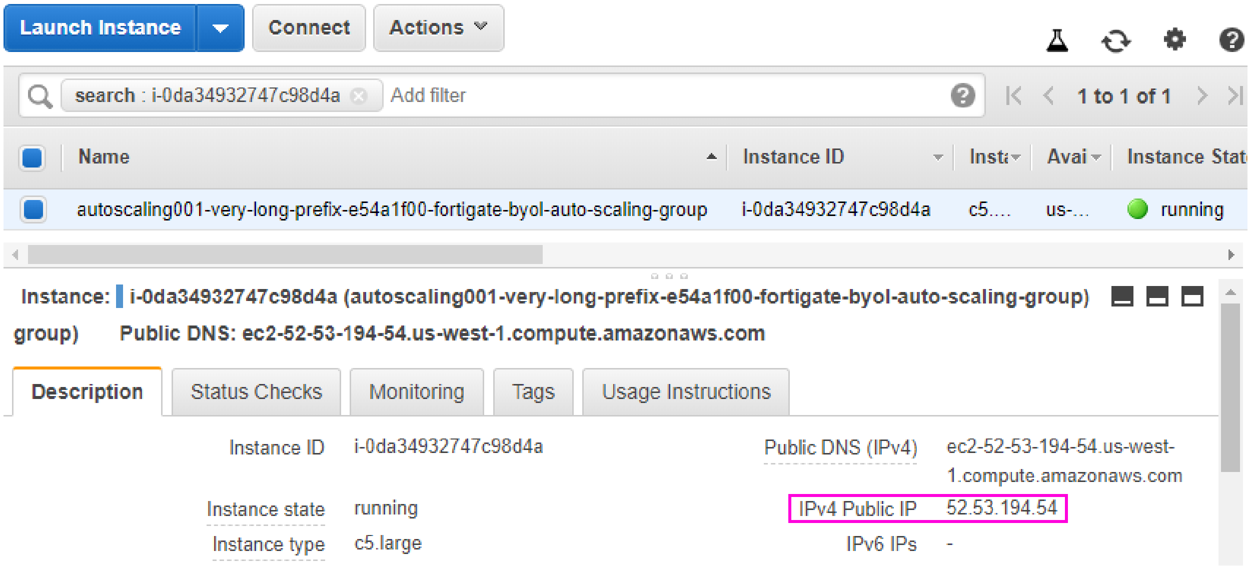
Auto Scaling Group: autoscaling001-very-long-prefix-e54a1f00-fortigate-byol-auto-scaling-group

Filter: Any Health Status Any Lifecycle State Filter instances...

1 to 2 of 2 Instances

	Instance ID	Lifecycle	Launch Configuration / Template	Av
□	i-0786bf0aa4bdd0319	InService	autoscaling001-very-long-prefix-e54a1f00-fortigate-byol-autoscale-launch-template	us
□	i-0da34932747c98d4a	InService	autoscaling001-very-long-prefix-e54a1f00-fortigate-byol-autoscale-launch-template	us

3. In the lower pane, select the *Instances* tab and then click the master instance. This is the instance with the *instanceID* you obtained in the section To obtain the password: on page 30.
4. Make note of the *IPv4 Public IP* in the lower pane.



search : i-0da34932747c98d4a Add filter

1 to 1 of 1

	Name	Instance ID	Insta	Avai	Instance Stat
■	autoscaling001-very-long-prefix-e54a1f00-fortigate-byol-auto-scaling-group	i-0da34932747c98d4a	c5....	us-...	● running

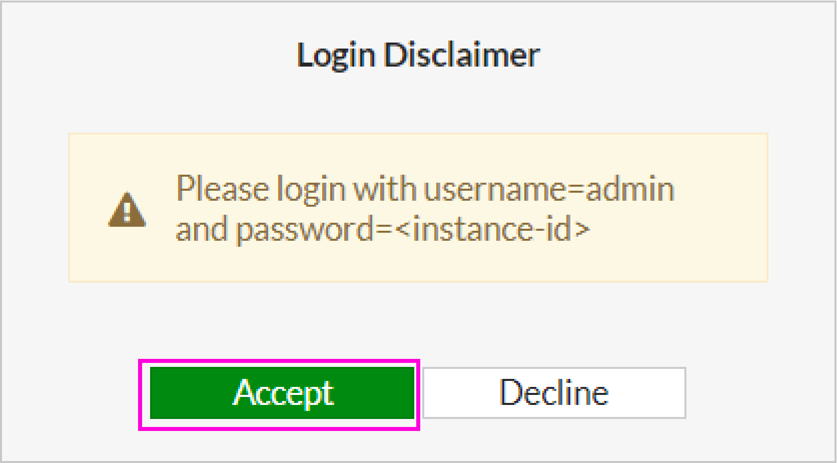
Instance: i-0da34932747c98d4a (autoscaling001-very-long-prefix-e54a1f00-fortigate-byol-auto-scaling-group) group) Public DNS: ec2-52-53-194-54.us-west-1.compute.amazonaws.com

Instance ID	i-0da34932747c98d4a	Public DNS (IPv4)	ec2-52-53-194-54.us-west-1.compute.amazonaws.com
Instance state	running	IPv4 Public IP	52.53.194.54
Instance type	c5.large	IPv6 IPs	-

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 on page 17.

To connect to the master FortiGate-VM instance:

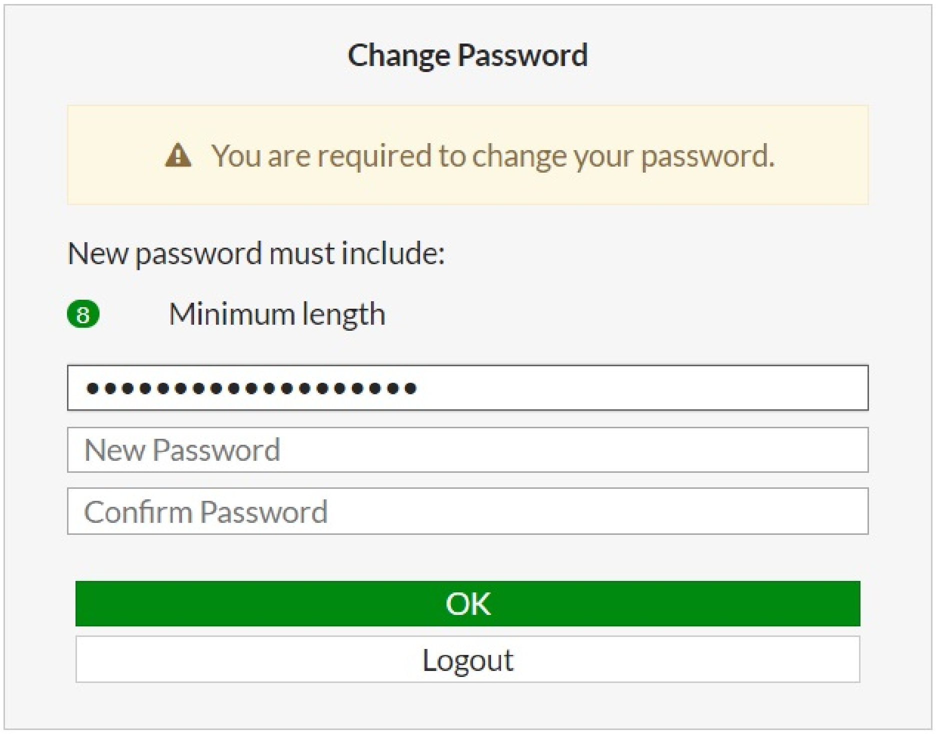
1. Open an HTTPS session in your browser and go to the login URL.
   - Your browser will display a certificate error message. This is normal because the default FortiGate certificate is self-signed and not recognized by browsers. Proceed past this error. At a later time, you can upload a publicly signed certificate to avoid this error.



Login Disclaimer

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

2. Log into the master FortiGate-VM instance with the username *admin* and the *instanceID* you obtained in the section To obtain the password: on page 30.
3. 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

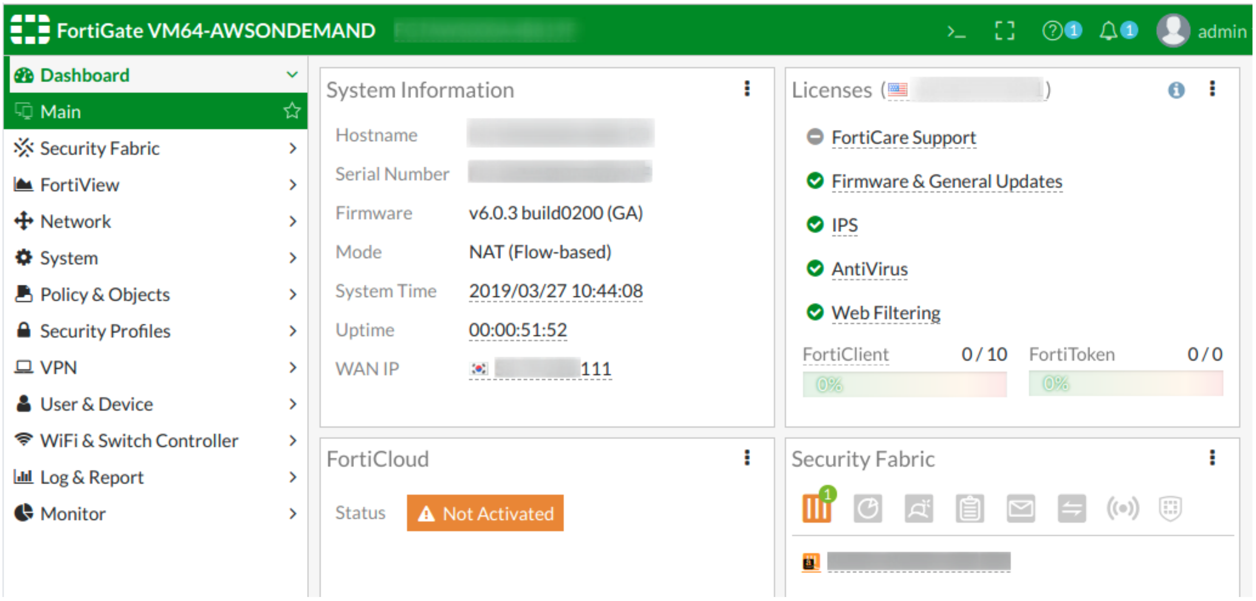
You are required to change your password.

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 slave FortiGate-VMs. Any attempt to change the password on a slave FortiGate-VM is overwritten with the master FortiGate-VM's password.

4. 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(s) 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 *<ResourceTagPrefix>-FortiGateMasterElection*. 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 *<ResourceTagPrefix>-FortiGateMasterElection*, refer to the master election portion of the section Verifying the deployment on page 28.

Appendix

FortiGate Autoscale for AWS features

Major components

- *The BYOL Auto Scaling group*. This Auto Scaling group contains 0 to many FortiGate-VMs of the BYOL licensing model and will dynamically scale-out or scale-in based on the scaling metrics specified by the parameters Scale-out threshold and Scale-in threshold. For each instance you must provide a valid license purchased from FortiCare.

  For BYOL-only and hybrid licensing deployments, the Minimum group size (FgtAsgMinSizeByol) must be at least 2. These FortiGate-VMs are the main instances and are fixed and running 7x24. If it is set to 1 and the instance fails to work, the current FortiGate-VM configuration will be lost.

- *The On-Demand Auto Scaling group*. This Auto Scaling group contains 0 to many FortiGate-VMs of the On-Demand licensing model and will dynamically scale-out or scale-in based on the scaling metrics specified by the parameters Scale-out threshold and Scale-in threshold.

  For On-Demand-only deployments, the Minimum group size (FgtAsgMinSizePayg) must be at least 2. These FortiGate-VMs are the main instances and are fixed and running 7x24. If it is set to 1 and the instance fails to work, the current FortiGate-VM configuration will be lost.

- *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 on page 36 table below
    - *httproutingpolicy* and *httpsroutingpolicy* are provided as part of the base configset - for a common use case - and specify the FortiGate firewall policy for VIPs for *http* routing and *https* routing respectively. This common use case includes a VIP on port 80 and a VIP on port 443 with a policy that points to an internal load balancer. The port numbers are configurable and can be changed during CFT deployment. Additional VIPs can be added here as needed.

      In FortiOS 6.2.3, any VIPs created on the master will not sync to the slave units. Any VIP you wish to add must be added as part of the base configuration.

      If you set the *Internal ELB options* parameter to `do not need one`, then you must include your VIP configuration in the base configuration.

  - The *fgt-asg-license* container contains BYOL license files.
- *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.
- *Networking Components* These are the network load balancers, the target group, and the VPC and subnets. You are expected to create your own client and server instances that you want protected by the FortiGate-VM.

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.
{HEART_BEAT_ INTERVAL}	Number	The time interval (in seconds) that the FortiGate-VM waits between sending heartbeat requests to the Autoscale handler function.

Auto Scaling Handler environment variables

Variable name	Description
UNIQUE_ID	Reserved, empty string.
CUSTOM_ID	Reserved, empty string.
RESOURCE_TAG_ PREFIX	The value of the CFT parameter *Resource tag prefix* which is described in the section Resource tagging configuration on page 15.

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

```
FGVM4VTM19000025 # diagnose 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>.amazonaws.com/prod/fgt-
     asg-handler
>> AWS download config script successfully
>> Run config script
>> Finish running script
>> FGVM4VTM19000025 $ config sys interface
>> FGVM4VTM19000025 (interface) $ edit "port2"
>> FGVM4VTM19000025 (port2) $ set mode dhcp
>> FGVM4VTM19000025 (port2) $ set defaultgw disable
>> FGVM4VTM19000025 (port2) $ set allowaccess ping https ssh http fgfm
>> FGVM4VTM19000025 (port2) $ # work around for FortiOS 6.0.4 #0543036 mtu values from DNS
     interfere with HA checksum.
>> FGVM4VTM19000025 (port2) $ set mtu-override enable
>> FGVM4VTM19000025 (port2) $ set mtu 9001
>> FGVM4VTM19000025 (port2) $ next
>> FGVM4VTM19000025 (interface) $ end
>> FGVM4VTM19000025 $ config system dns
>> FGVM4VTM19000025 (dns) $ unset primary
>> FGVM4VTM19000025 (dns) $ unset secondary
>> FGVM4VTM19000025 (dns) $ end
>> FGVM4VTM19000025 $ config system global
>> FGVM4VTM19000025 (global) $ set admin-sport 8443
>> FGVM4VTM19000025 (global) $ end
>> FGVM4VTM19000025 $ config system auto-scale
>> FGVM4VTM19000025 (auto-scale) $ set status enable
>> FGVM4VTM19000025 (auto-scale) $ set sync-interface "port1"
>> FGVM4VTM19000025 (auto-scale) $ set hb-interval 30
>> FGVM4VTM19000025 (auto-scale) $ set role master
>> FGVM4VTM19000025 (auto-scale) $ set callback-url https://<the_masked_api_
     id>.amazonaws.com/prod/fgt-asg-handler
>> FGVM4VTM19000025 (auto-scale) $ set psksecret <the_masked_psksecret>
>> FGVM4VTM19000025 (auto-scale) $ end
>> FGVM4VTM19000025 $
>> FGVM4VTM19000025 $ config firewall address
>> FGVM4VTM19000025 (address) $ edit internal-elb-web
>> FGVM4VTM19000025 (internal-elb-web) $ set type fqdn
>> FGVM4VTM19000025 (internal-elb-web) $ set fqdn "<the_masked_elb_dns>"
>> FGVM4VTM19000025 (internal-elb-web) $ set associated-interface "port1"
>> FGVM4VTM19000025 (internal-elb-web) $ next
>> FGVM4VTM19000025 (address) $ end
>> FGVM4VTM19000025 $
>> FGVM4VTM19000025 $ config firewall vip
>> FGVM4VTM19000025 (vip) $ edit internal-web
>> FGVM4VTM19000025 (internal-web) $ set type fqdn
>> FGVM4VTM19000025 (internal-web) $ set mapped-addr internal-elb-web
>> FGVM4VTM19000025 (internal-web) $ set portforward enable
>> FGVM4VTM19000025 (internal-web) $ set extintf port1
>> FGVM4VTM19000025 (internal-web) $ set extport 443
>> FGVM4VTM19000025 (internal-web) $ set mappedport 443
>> FGVM4VTM19000025 (internal-web) $ next
>> FGVM4VTM19000025 (vip) $ end
>> FGVM4VTM19000025 $
>> FGVM4VTM19000025 $ config firewall policy
>> FGVM4VTM19000025 (policy) $ edit 2
>> FGVM4VTM19000025 (2) $ set name "internal-web-https"
>> FGVM4VTM19000025 (2) $ set srcintf "port1"
>> FGVM4VTM19000025 (2) $ set dstintf "port2"
>> FGVM4VTM19000025 (2) $ set srcaddr "all"
>> FGVM4VTM19000025 (2) $ set dstaddr "internal-web"
>> FGVM4VTM19000025 (2) $ set action accept
>> FGVM4VTM19000025 (2) $ set schedule "always"
>> FGVM4VTM19000025 (2) $ set service "HTTPS"
>> FGVM4VTM19000025 (2) $ set fsso disable
>> FGVM4VTM19000025 (2) $ set nat enable
>> FGVM4VTM19000025 (2) $ next
>> FGVM4VTM19000025 (policy) $ end
```

Slave FortiGate-VM cloudinit output

```
FortiGate-VM64-AWSON~AND # diagnose 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>.amazonaws.com/prod/fgt-
     asg-handler
>> AWS download config script successfully
>> Run config script
>> Finish running script
>> FGVM4VTM19000027 $ config sys interface
>> FGVM4VTM19000027 (interface) $ edit "port2"
>> FGVM4VTM19000027 (port2) $ set mode dhcp
>> FGVM4VTM19000027 (port2) $ set defaultgw disable
>> FGVM4VTM19000027 (port2) $ set allowaccess ping https ssh http fgfm
>> FGVM4VTM19000027 (port2) $ # work around for FortiOS 6.0.4 #0543036 mtu values from DNS
     interfere with HA checksum.
>> FGVM4VTM19000027 (port2) $ set mtu-override enable
>> FGVM4VTM19000027 (port2) $ set mtu 9001
>> FGVM4VTM19000027 (port2) $ next
>> FGVM4VTM19000027 (interface) $ end
>> FGVM4VTM19000027 $ config system dns
>> FGVM4VTM19000027 (dns) $ unset primary
>> FGVM4VTM19000027 (dns) $ unset secondary
>> FGVM4VTM19000027 (dns) $ end
>> FGVM4VTM19000027 $ config system global
>> FGVM4VTM19000027 (global) $ set admin-sport 8443
>> FGVM4VTM19000027 (global) $ end
>> FGVM4VTM19000027 $ config system auto-scale
>> FGVM4VTM19000027 (auto-scale) $ set status enable
>> FGVM4VTM19000027 (auto-scale) $ set sync-interface "port1"
>> FGVM4VTM19000027 (auto-scale) $ set hb-interval 30
>> FGVM4VTM19000027 (auto-scale) $ set role slave
>> FGVM4VTM19000027 (auto-scale) $ set callback-url https://<the_masked_api_
     id>.amazonaws.com/prod/fgt-asg-handler
>> FGVM4VTM19000027 (auto-scale) $ set psksecret <the_masked_psksecret>
>> FGVM4VTM19000027 (auto-scale) $ end
>> FGVM4VTM19000027 $
>> FGVM4VTM19000027 $ config firewall address
>> FGVM4VTM19000027 (address) $ edit internal-elb-web
>> FGVM4VTM19000027 (internal-elb-web) $ set type fqdn
>> FGVM4VTM19000027 (internal-elb-web) $ set fqdn "<the_masked_elb_dns>"
>> FGVM4VTM19000027 (internal-elb-web) $ set associated-interface "port1"
>> FGVM4VTM19000027 (internal-elb-web) $ next
>> FGVM4VTM19000027 (address) $ end
>> FGVM4VTM19000027 $
>> FGVM4VTM19000027 $ config firewall vip
>> FGVM4VTM19000027 (vip) $ edit internal-web
>> FGVM4VTM19000027 (internal-web) $ set type fqdn
>> FGVM4VTM19000027 (internal-web) $ set mapped-addr internal-elb-web
>> FGVM4VTM19000027 (internal-web) $ set portforward enable
>> FGVM4VTM19000027 (internal-web) $ set extintf port1
>> FGVM4VTM19000027 (internal-web) $ set extport 443
>> FGVM4VTM19000027 (internal-web) $ set mappedport 443
>> FGVM4VTM19000027 (internal-web) $ next
>> FGVM4VTM19000027 (vip) $ end
>> FGVM4VTM19000027 $
>> FGVM4VTM19000027 $ config firewall policy
>> FGVM4VTM19000027 (policy) $ edit 2
>> FGVM4VTM19000027 (2) $ set name "internal-web-https"
>> FGVM4VTM19000027 (2) $ set srcintf "port1"
>> FGVM4VTM19000027 (2) $ set dstintf "port2"
>> FGVM4VTM19000027 (2) $ set srcaddr "all"
>> FGVM4VTM19000027 (2) $ set dstaddr "internal-web"
>> FGVM4VTM19000027 (2) $ set action accept
>> FGVM4VTM19000027 (2) $ set schedule "always"
>> FGVM4VTM19000027 (2) $ set service "HTTPS"
>> FGVM4VTM19000027 (2) $ set fsso disable
>> FGVM4VTM19000027 (2) $ set nat enable
>> FGVM4VTM19000027 (2) $ next
>> FGVM4VTM19000027 (policy) $ end
```

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

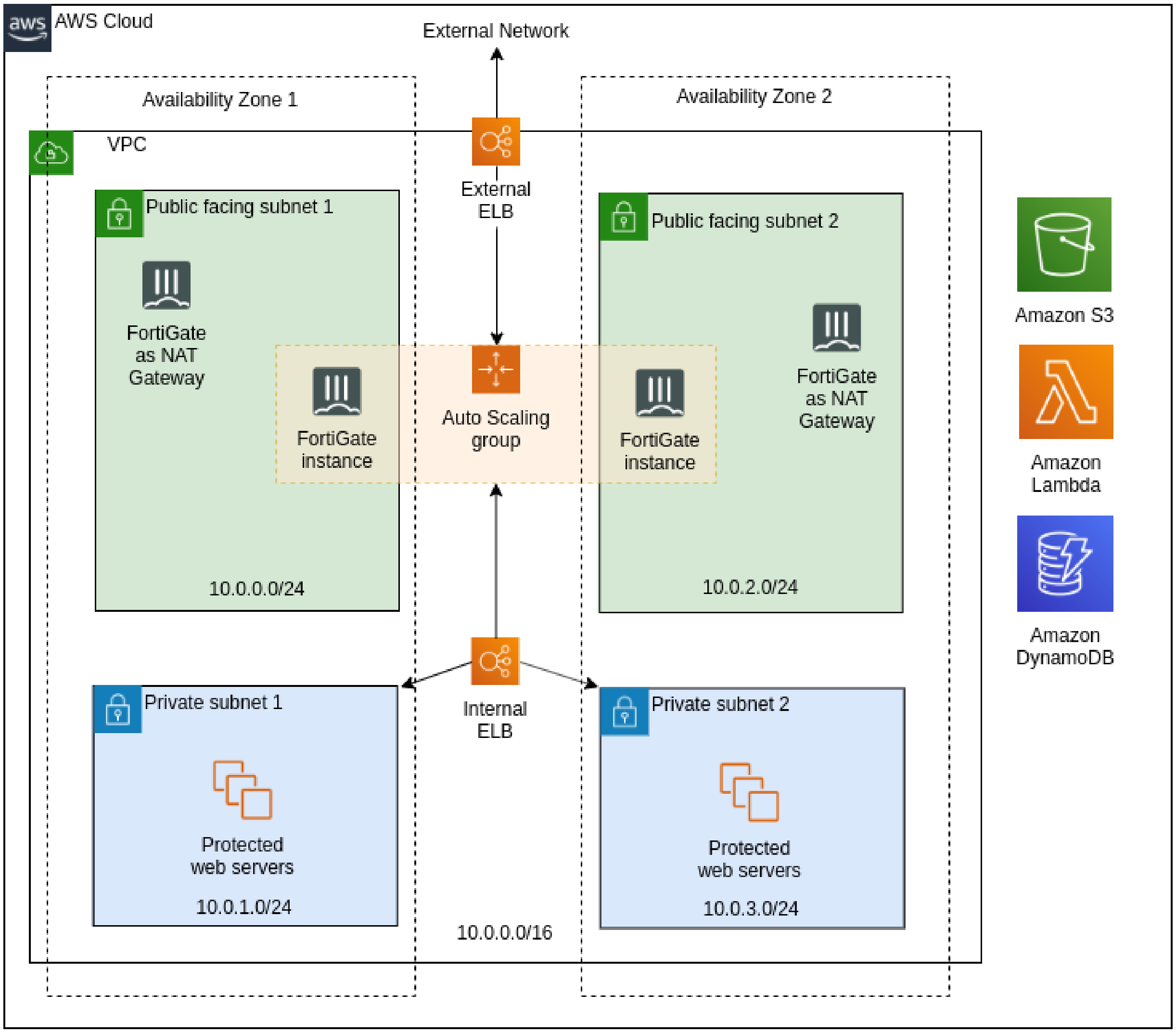
VPN output

```
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
```

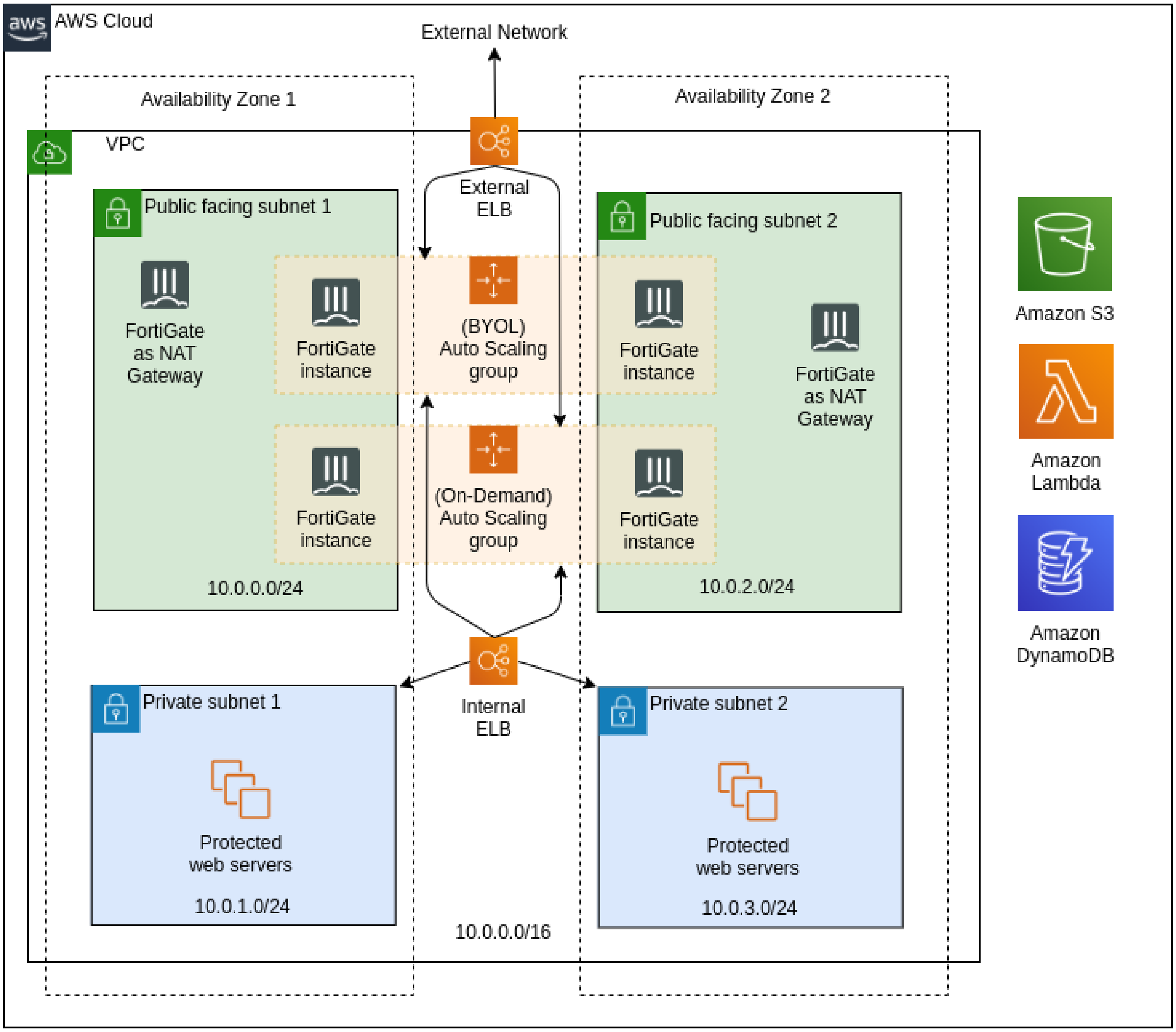
Architectural diagrams

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

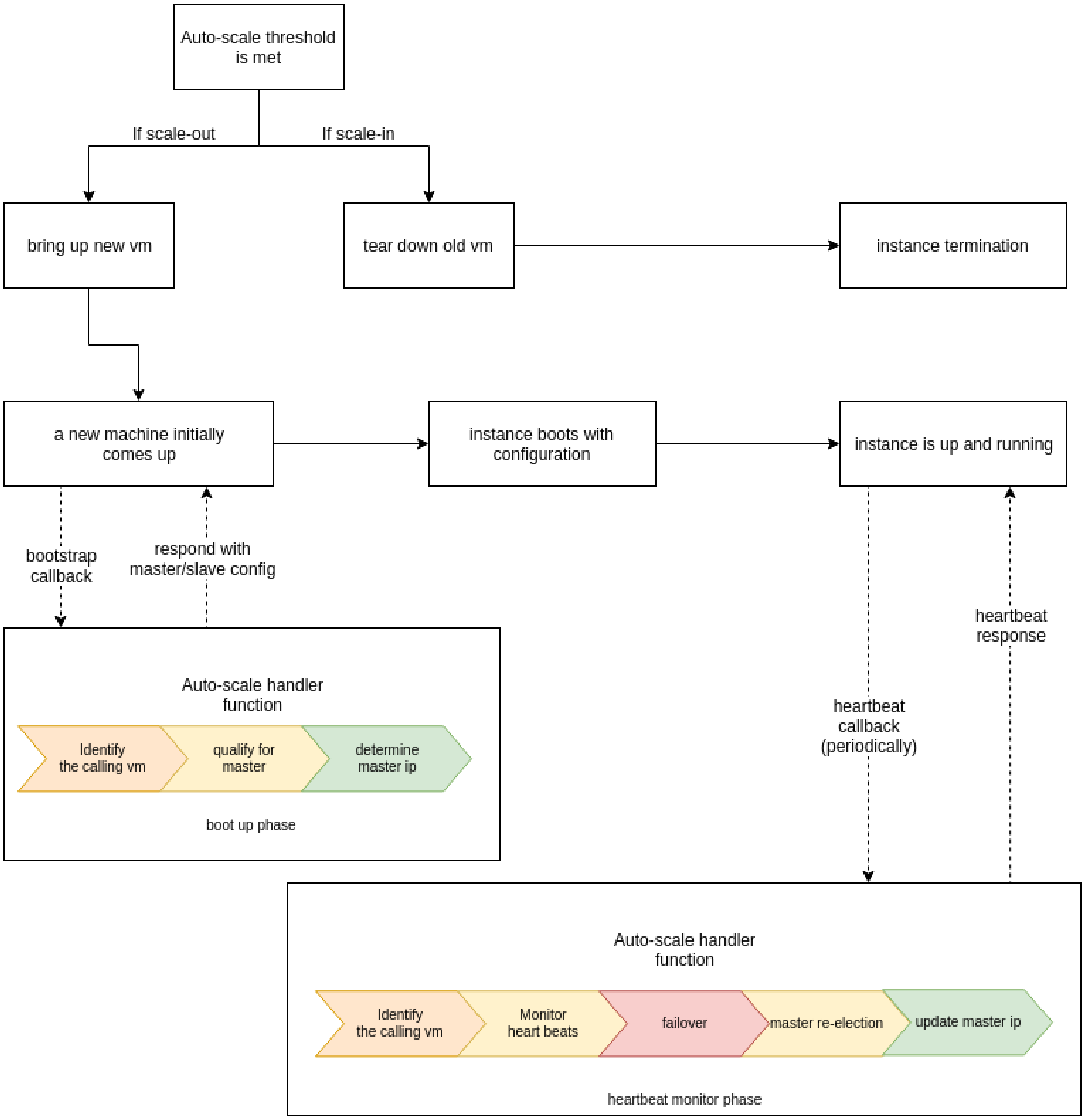
FortiGate Autoscale VPC (one instance type)



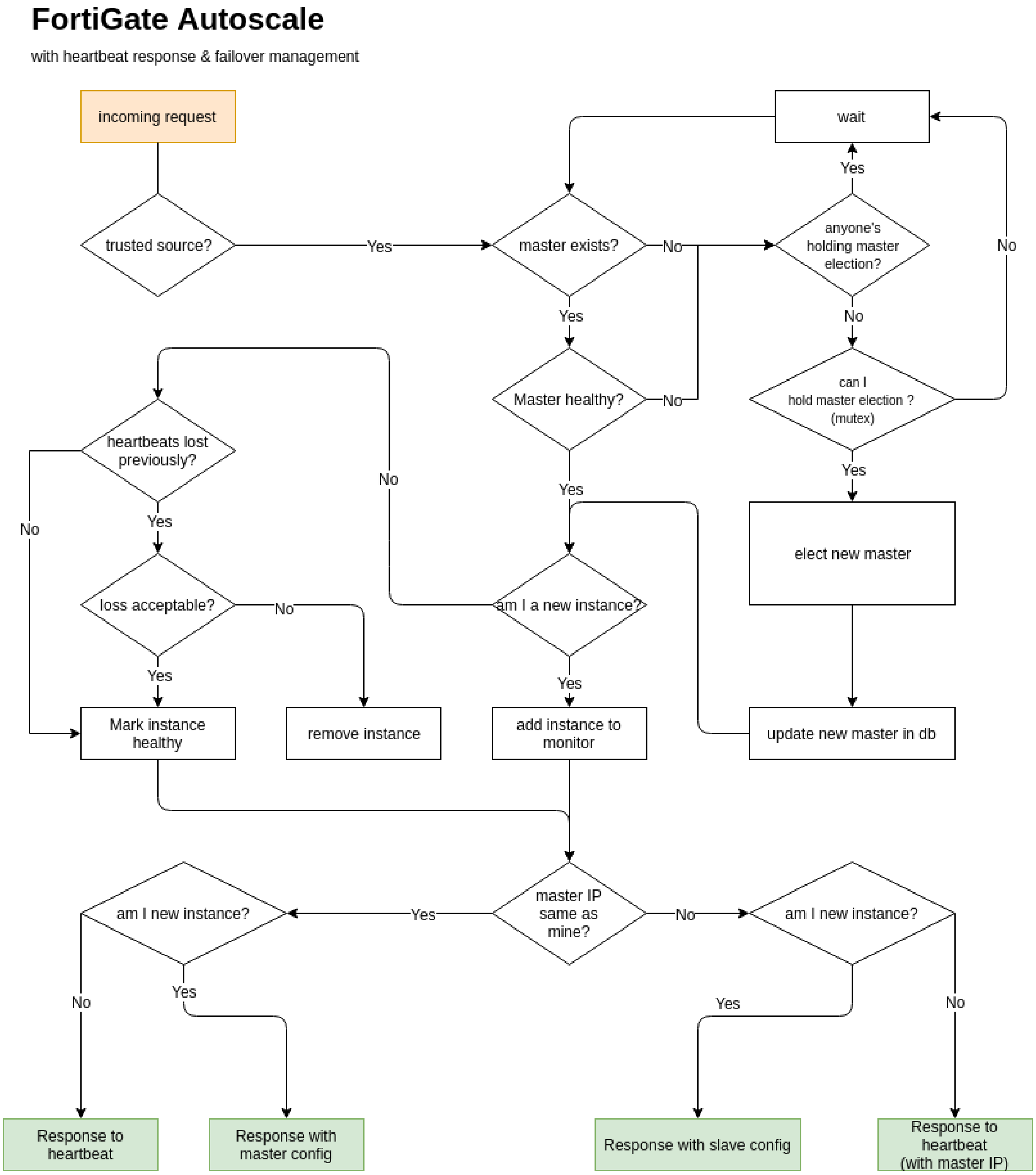
FortiGate Autoscale VPC (hybrid licensing)



Autoscale handler flowchart



Master election



Change log

Date	Change Description
2019-03-28	Initial release.
2019-07-01	Updated Deploying auto scaling on AWS without Transit Gateway integration on page 5.
2019-08-07	Reorganized Deploying auto scaling on AWS without Transit Gateway integration on page 5 to match 6.0.
2019-08-23	Updated the section Obtaining the deployment package on page 8 from the guide for Deploying auto scaling on AWS without Transit Gateway integration.
2019-09-20	Updated the Region support note the Prerequisites sections of Deploying auto scaling on AWS on page 4.
2019-10-07	Updated the section Deploying auto scaling on AWS without Transit Gateway integration on page 5 to add support for BYOL instances.
2019-10-30	Updated the *Prerequisites* for Deploying auto scaling on AWS on page 4.
2019-11-15	Updated the Introduction as well as both of the *Prerequisites* and *Deploying the CloudFormation templates* sections in Deploying auto scaling on AWS on page 4.
2019-01-02	The *S3KeyPrefix* label has been renamed to *S3 resource folder* in Deploying auto scaling on AWS on page 4.
2020-02-07	Updated the Appendix for Deploying auto scaling on AWS without Transit Gateway integration on page 5 to add FortiOS 6.2.3 specific information.
2020-02-25	Minor updates to Deploying auto scaling on AWS on page 4.
2020-09-22	Created the final version of Deploying auto scaling on AWS on page 4

Copyright© 2020 Fortinet, Inc. All rights reserved. Fortinet®, FortiGate®, FortiCare® and FortiGuard®, and certain other marks are registered trademarks of Fortinet, Inc., in the U.S. and other jurisdictions, and other Fortinet names herein may also be registered and/or common law trademarks of Fortinet. All other product or company names may be trademarks of their respective owners. Performance and other metrics contained herein were attained in internal lab tests under ideal conditions, and actual performance and other results may vary. Network variables, different network environments and other conditions may affect performance results. Nothing herein represents any binding commitment by Fortinet, and Fortinet disclaims all warranties, whether express or implied, except to the extent Fortinet enters a binding written contract, signed by Fortinet's General Counsel, with a purchaser that expressly warrants that the identified product will perform according to certain expressly-identified performance metrics and, in such event, only the specific performance metrics expressly identified in such binding written contract shall be binding on Fortinet. For absolute clarity, any such warranty will be limited to performance in the same ideal conditions as in Fortinet's internal lab tests. In no event does Fortinet make any commitment related to future deliverables, features or development, and circumstances may change such that any forward-looking statements herein are not accurate. Fortinet disclaims in full any covenants, representations, and guarantees pursuant hereto, whether express or implied. Fortinet reserves the right to change, modify, transfer, or otherwise revise this publication without notice, and the most current version of the publication shall be applicable.