

FortiGate Python-Based Auto Scaling with Hybrid Licensing for AWS

Table of Contents

AWS Auto Scaling Overview	1
FortiGate Auto Scale Solution Overview	2
FortiGate Auto Scale Architecture	3
Auto Scale Service Interactions	5
BYUL License Management.....	7
Deploying the CloudFormation Templates	8

AWS Auto Scale Overview

It is typical for businesses to experience varying levels of demand on their digital infrastructure. The AWS public cloud platform provides several benefits through demand elasticity combined with cost optimization. Chief among these is Auto Scaling. Auto Scaling monitors compute resources and, based on utilization, will dynamically scale out the environment to support the additional demand.

Conversely, when peak utilization has passed, low-watermark thresholds trigger the environment to contract, or scale in. Typical reasons to deploy auto scaling include seasonal variation, failover or disaster recovery, and general cost optimization.

When considering if auto scaling is a fit for your needs, consider the variability in traffic patterns relative to a baseline. While auto scaling is great for business continuity and agility, right sizing the environment for the minimum amount of traffic will help to minimize the amount of scale-in and scale-out events to ensure the most stable environment.

A typical baseline starts with a traffic volume assessment. When deploying a security network virtual appliance (NVA), such as the FortiGate NGFW, it is important to consider processing requirements for the traffic volume being handled on a normal basis. Processing variance depends on the types of inspection being done. For example, stateful firewall and logging will consume far less resources than full threat protection and encryption functions (IPS and VPN).

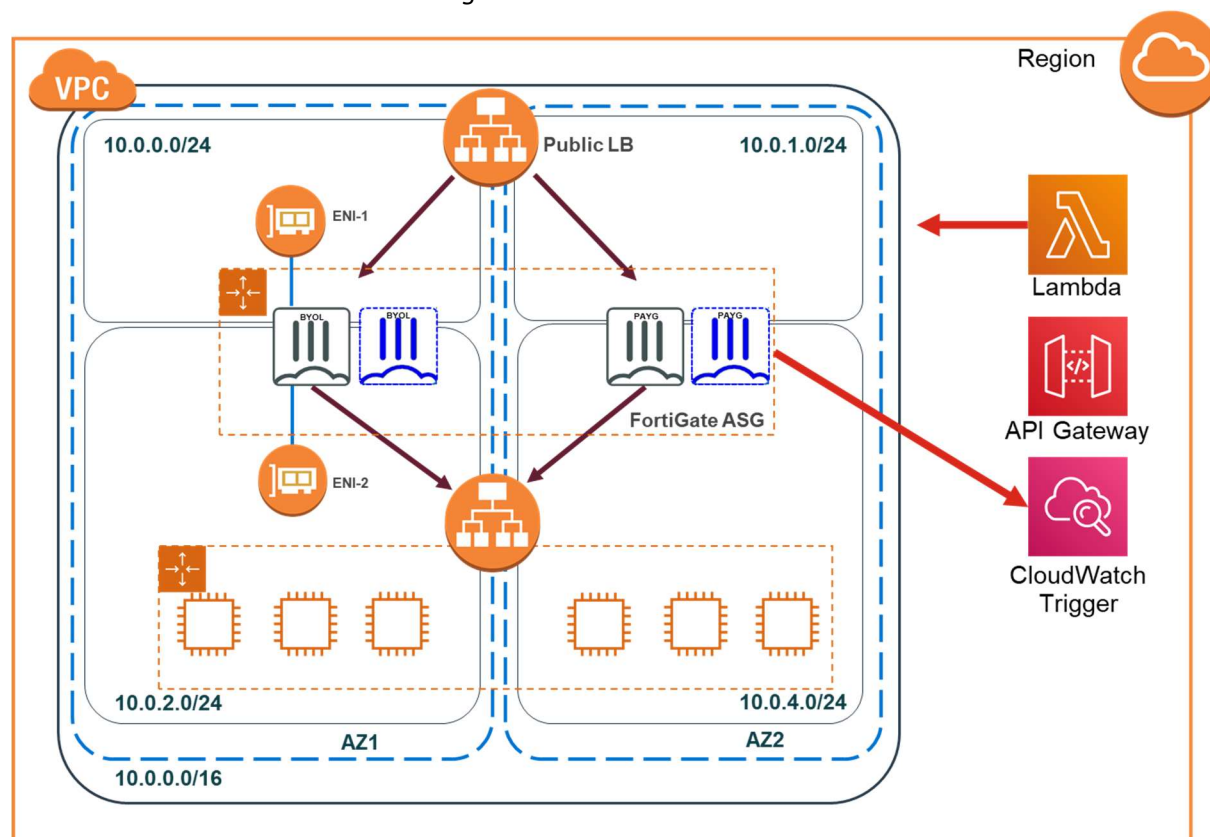
FortiGate Auto Scale Overview

Note that there are multiple versions of Fortinet's Auto Scale solution that are purposeful to different use cases and deployment scenarios. For example, Transit VPCs with ECMP VPNs. These different flavors of auto scale achieve the goal of scaling services though their frameworks are slightly different. For clarity, this document will refer to the template described for this particular deployment case and not make reference to any alternative auto scale solution.

Fortinet's auto scale solution provides many features that align with the intent of auto scaling. Hybrid licensing provides the best performance to cost by matching persistent bring-your-own-license (BYOL) instances with scale out pay-as-you-go (PAYG) instances. Both ingress and egress use cases are supported without the use of extra instances or NAT gateways.

FortiGate Auto Scale Architecture

Figure 1. Auto Scale Architecture

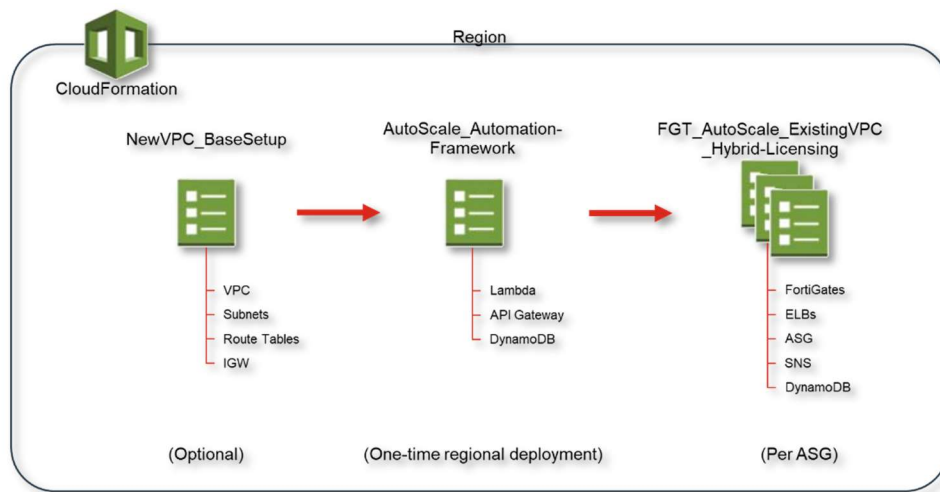


There are three templates used during the phases of auto scale deployment, supporting both new and existing VPCs.

- **NewVPC_BaseSetup** – This template is for the convenience of setting up any new VPC. Output of this stack is the VPC, Subnets, and route tables required to support the Auto Scale deployment. This is an optional stack which is not necessary for existing VPC deployments.
- **AutoScale_Automation-Framework** – Deploys the Lambda service and supporting API gateway and DynamoDB table that will track all ASG groups deployed in the region.
- **FGT_AutoScale_ExistingVPC_Hybrid-Licensing** – Deploys the Auto Scale Group (ASG) and supporting AWS services such as the ELBs, target groups, instances, and SNS.

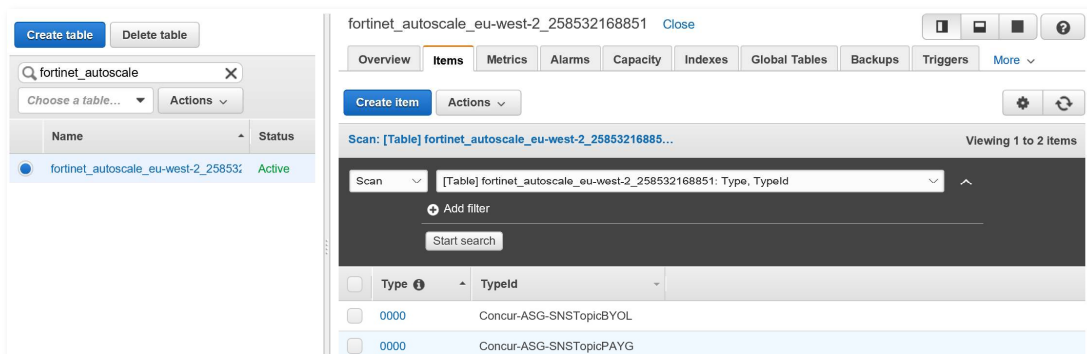
Figure 1 shows the relationship between the templates. Use the **NewVPC_BaseSetup** only when a new VPC is required. The outputs of this VPC can be fed into the **AutoScale_Automation-Framework** CFT. The AutoScale_Automation-Framework CFT will install the region's Lambda function which will manage all ASGs in the region.

Figure 2. Relationship between CloudFormation Templates for Auto Scale



The Lambda function provides a registration framework by creating DynamoDB table entry for each ASG deployed in the region. In this way, the AutoScale_Automation-Framework template only needs to be deployed once per region.

Figure 3: DynamoDB table tracking ASG deployments in region



FGT_AutoScale_ExistingVPC_Hybrid-Licensing is the core ASG CFT that will deploy each ASG instance. Outputs from NewVPC_BaseSetup and AutoScale_Automation-Framework are used as inputs for the ASG.

Service Interactions

Figure 4. provides an overview of the different services deployed and how they interact. For the CloudFormation-based mode of deployment, the services created from the previously described CFTs interact primarily through the Simple Notification Service (SNS) and the API Gateway. Auto Scaling is deployed as two ASGs – one for BYOL and a second for PAYG. These ASGs make up an Auto Scale Deployment (ASD). Each of these ASGs within the ASD can be configured independently to provide flexibility in the CAPEX or OPEX interests of the business. For example, if the business requires a very small baseline of a single FortiGate with no high availability (HA), a single BYOL instance can be instantiated with a minimum ASG size of 1. The PAYG ASG can be set with a minimum of 0 and a maximum desired of 5, as an example. Such a case may also be preferable in the scoping phase of the implementation where a solid baseline has not yet been set. As the needs of the business change, the ASG minimum and maximum values for both BYOL and PAYG can be adjusted.

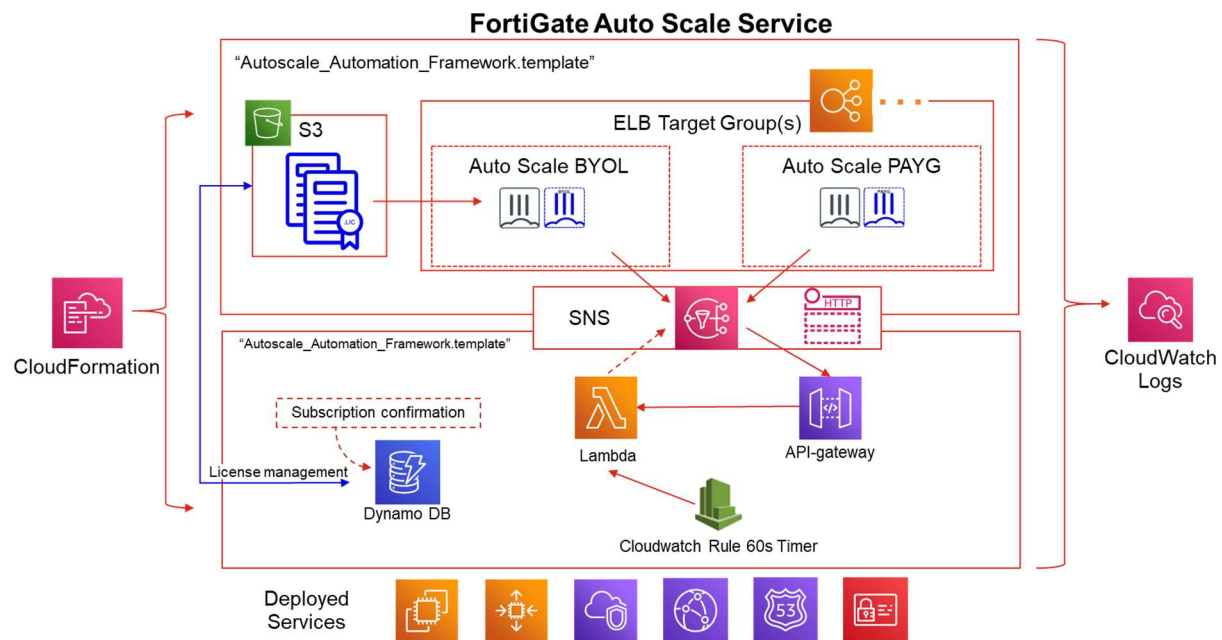
When a new ASD is deployed, auto scale events are posted to SNS which then notifies the Lambda function via the API gateway of scaling events and EC2 instance service statuses. SNS uses HTTPS for protected communication. Further reading on this topic can be found at the following URLs.

Auto Scaling Lifecycle:

<https://docs.aws.amazon.com/autoscaling/ec2/userguide/lifecycle-hooks.html>

<https://docs.aws.amazon.com/autoscaling/ec2/userguide/AutoScalingGroupLifecycle.html>

Figure 4: Auto Scale Service Interactions



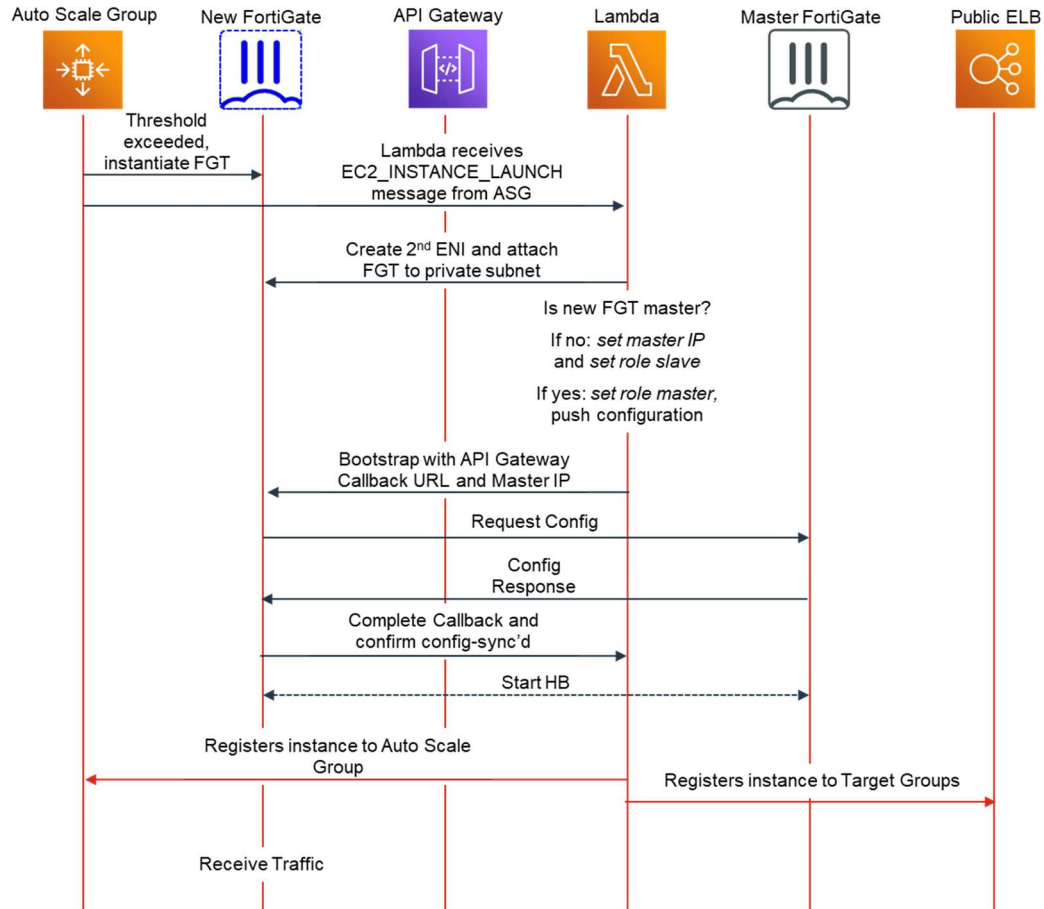
On instance instantiation, the newly launched FortiGate will transition through the “Pending:Wait”, “Pending:Proceed”, and finally to “InService”. When an auto-scaled FortiGate comes to InService status, it will bootstrap with a basic configuration which includes a basic auto scale configuration for it to communicate with the API Gateway.

Example 1: config sys auto-scale

```
FGVM04TM19000016 (auto-scale) # show
config system auto-scale
  set status enable
  set sync-interface "port3"
  set callback-url "https://someurl.apigateway.aws.com"
end
```

The FortiGates support auto scaling natively in the FortiOS (FOS) starting with version 6.0. In this way, the slave FortiGates can source their configuration from a master FortiGate. As each ASD member comes online, Lambda will configure the FortiGate’s initial, base configuration based on it’s designated role as master or slave. Lambda’s actions here are triggered by lifecycle hook message EC2_INSTANCE_LAUNCH. The FortiGates in the ASD will exchange a heartbeat message that will ensure that each device is still available and that it has the latest configuration. Should the master configuration change, the slave FortiGates will be updated immediately. Consequently, the user will only ever need to set the configuration on the master. The following summarizes the configuration steps.

Figure 5. New FortiGate configuration



BYOL License Management

The ASD supports hybrid, or mixed-mode, licensing options. When using bring-your-own-licensing (BYOL) instances, the FortiGate license files must be provided supplied to a user-defined S3 bucket. This parameter is defined when launching the “FGT_AutoScale_ExistingVPC_Hybrid-Licensing” template. Note that the licenses should be supplied prior deploying this CFT if the minimum instance count is set to >0. When the FortiGate turns up and reaches out to the Lambda service for configuration instructions, Lambda will recognize the instance as BYOL and will push a license to the new FortiGate. These licenses are then updated in a DynamoDB table for tracking the license service status and the FortiGate to which the license belongs. Should an instance be terminated, Lambda will remove the license record from the database and will make that license available in the license pool for subsequent FortiGates.

Master FortiGate Selection

Within the Auto Scale Deployment (ASD), which may be comprised of multiple ASGs, there is one master from which all other slave FortiGates source their configuration. Configurations need only occur on the master which then sync’s to all other FortiGates in the ASD. Configuration can be provided by using cloud-init, a configuration file upload, via API, CLI, web GUI, or FortiManager. The configuration of the master FortiGate is backed up to S3 by Lambda. Note that no FortiGate is bootstrapped with a status of master; Lambda sets this status based on its selection process. The status of all FortiGates are tracked in DynamoDB.

Master FortiGate High Availability

Master FortiGate failover is managed by Lambda. Should the master FortiGate fail (not respond to a health check), Lambda will elect a new master determined to be the FortiGate with the longest uptime. There is currently no manual intervention to deterministically set the master. To change the master assignment, reboot the member FortiGates who’s uptime is greater than the desired master. The status of the master FortiGate is tracked in DynamoDB as shown in *Figure 6*.

Figure 6. DynamoDB entry with master role assignment

Uptime.

Deploying an Auto Scale Group

Note: This assumes that the **AutoScale_Automation-Framework** has been deployed in the region.

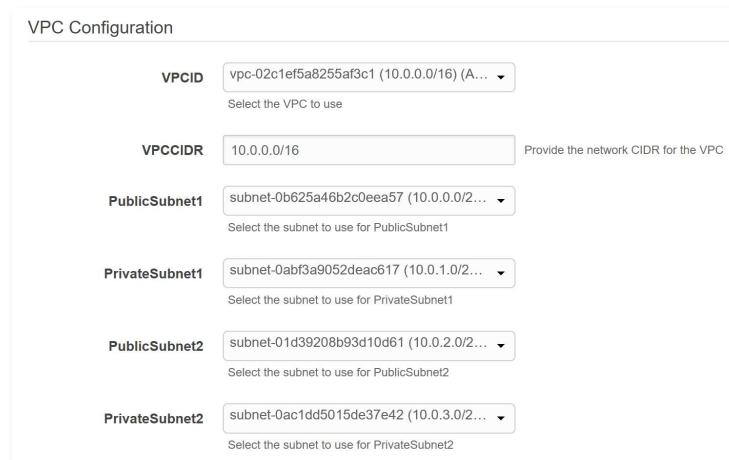
Note: The template locations and instructions may change with iterative versions of the solution. Please check the Readme file at https://github.com/aidanwalden/FortiGate_ASG_CFT_Lambda_ExistingVPC for updates.

Step 1: If not already downloaded, download the FGT_AutoScale_ExistingVPC_Hybrid-Licensing.template.json from Github at https://github.com/aidanwalden/FortiGate_ASG_CFT_Lambda_ExistingVPC

Step 2: Create the Stack

- In the AWS console, navigate to the CloudFormation Dashboard and select “Create Stack”
- Select to upload the FGT_AutoScale_ExistingVPC_Hybrid-Licensing template from either S3 or a local store
- Enter the CFT parameters the VPC into which the ASG will be deployed. Public and Private subnet details are required for each Availability Zone used.

Figure 3: Existing VPC details for ASG



The screenshot shows the 'VPC Configuration' section of an AWS CloudFormation stack creation form. It contains several dropdown menus for selecting existing VPC and subnet resources. The fields are: VPCID (selected: vpc-02c1ef5a8255af3c1 (10.0.0.0/16) (A...)), VPCCIDR (10.0.0.0/16), PublicSubnet1 (selected: subnet-0b625a46b2c0eea57 (10.0.0.0/2...)), PrivateSubnet1 (selected: subnet-0abf3a9052deac617 (10.0.1.0/2...)), PublicSubnet2 (selected: subnet-01d39208b93d10d61 (10.0.2.0/2...)), and PrivateSubnet2 (selected: subnet-0ac1dd5015de37e42 (10.0.3.0/2...)). Each dropdown has a small instruction below it: 'Select the VPC to use' for VPCID, and 'Select the subnet to use for [SubnetName]' for the others.

Parameter	Value	Instruction
VPCID	vpc-02c1ef5a8255af3c1 (10.0.0.0/16) (A...	Select the VPC to use
VPCCIDR	10.0.0.0/16	Provide the network CIDR for the VPC
PublicSubnet1	subnet-0b625a46b2c0eea57 (10.0.0.0/2...	Select the subnet to use for PublicSubnet1
PrivateSubnet1	subnet-0abf3a9052deac617 (10.0.1.0/2...	Select the subnet to use for PrivateSubnet1
PublicSubnet2	subnet-01d39208b93d10d61 (10.0.2.0/2...	Select the subnet to use for PublicSubnet2
PrivateSubnet2	subnet-0ac1dd5015de37e42 (10.0.3.0/2...	Select the subnet to use for PrivateSubnet2

- d. Locate the `APIGatewayURL` which can be found from the output of the `AutoScale_Automation-Framework`

Figure 4: APIGatewayURL from AutoScale_Automation-Framework

The screenshot shows the AWS CloudFormation console. At the top, there are buttons for 'Create Stack', 'Actions', and 'Design template'. Below these is a filter section with 'Filter: Active' and a search box 'By Stack Name'. A table lists three stacks:

Stack Name	Created Time	Status	Drift Status	Description
<input checked="" type="checkbox"/> ASG-Lambda-Deployment	2019-05-29 21:53:51 UTC-0600	CREATE_COMPLETE	NOT_CHECKED	(v1.0) AWS CloudFormation Template to deploy an API Gatew...
<input type="checkbox"/> ASG-VPC	2019-05-28 22:35:10 UTC-0600	CREATE_COMPLETE	NOT_CHECKED	(1.0) AWS CloudFormation Template to launch a VPC with 2 pu...
<input type="checkbox"/> GuardDuty-MainEvent	2018-05-03 00:05:44 UTC-0600	CREATE_COMPLETE	⚠️ DRIFTED	Deploys a Lambda function that receives GuardDuty finding ev...

Below the stack list, there are tabs for 'Overview', 'Outputs', 'Resources', 'Events', 'Template', 'Parameters', 'Tags', 'Stack Policy', 'Change Sets', and 'Rollback Triggers'. The 'Outputs' tab is selected, showing a table with the following data:

Key	Value	Description	Export Name
AutoScaleAPIURL	https://gn61jipiv5.execute-api.eu-west-2.amazonaws.com/dev/sns	AWS API Gateway URL	

- e. Enter the FortiGate Instance Configuration parameters. This includes keypair, S3 bucket for license management, etc.

Figure 5: Sample inputs for FortiGate Instance Configuration

The screenshot shows the 'FortiGate Instance Configuration' form with the following fields and values:

- CIDRForInstanceAccess**: 0.0.0.0/0 (Provide a network CIDR from which the FortiGate instances will be accessed)
- KeyPair**: Londonkey (Select a keypair to associate with the FortiGates)
- Password**: ***** (Provide a password for the admin account of the FortiGates)
- InitS3Bucket**: n.com/s3/buckets/asg-ajw/?region=eu-west-2 (Provide the Init S3 Bucket name where your license files exists)
- ListenerPort**: 80 (Provide the listener port for the external ELB)
- APIGatewayURL**: https://gn61jipiv5.execute-api.eu-west-2.amaz (Provide an API Gateway URL to receive notifications for AutoScaling events)
- EnvironmentTag**: test (Select an environment tag)

- f. Enter the AutoScale parameter details.
 - i. For production environments, the **BYOLInstanceType** should be sized based on the proper baseline requirements as estimated
 - ii. The **ASGBYOLMinSize** is the minimum number of BYOL instances that will be in service at any time. Ensure that the minimum number of licenses allocated are available in the InitS3Bucket designated

Figure 6: Auto Scaling Configuration Parameters

The screenshot shows the 'Auto Scaling Configuration' form with the following parameters and values:

Parameter	Value	Description
ScaleUpThreshold	70	Provide the value at which a scale up event would take place (CPU Usage)
ScaleDownThreshold	20	Provide the value at which a scale down event would take place (CPU Usage)
BYOLInstanceType	c5.large	Select the instance type for the BYOL FortiGates
ASGBYOLMinSize	2	Minimum number of FortiGate instances in the BYOL Auto-Scaling Group.
ASGBYOLMaxSize	2	Maximum number of FortiGate instances in the BYOL Auto-Scaling Group.
PAYGInstanceType	c5.large	Select the instance type for the PAYG FortiGates
ASGPAYGMinSize	0	Maximum number of FortiGate instances in the PAYG Auto-Scaling Group.
ASGPAYGMaxSize	5	Maximum number of FortiGate instances in the PAYG Auto-Scaling Group.

- g. Apply Tags as needed to identify this stack
- h. If an existing IAM role is to be used, it can be chosen. Otherwise, an IAM role will be created.

Figure 7: Tags and IAM roles

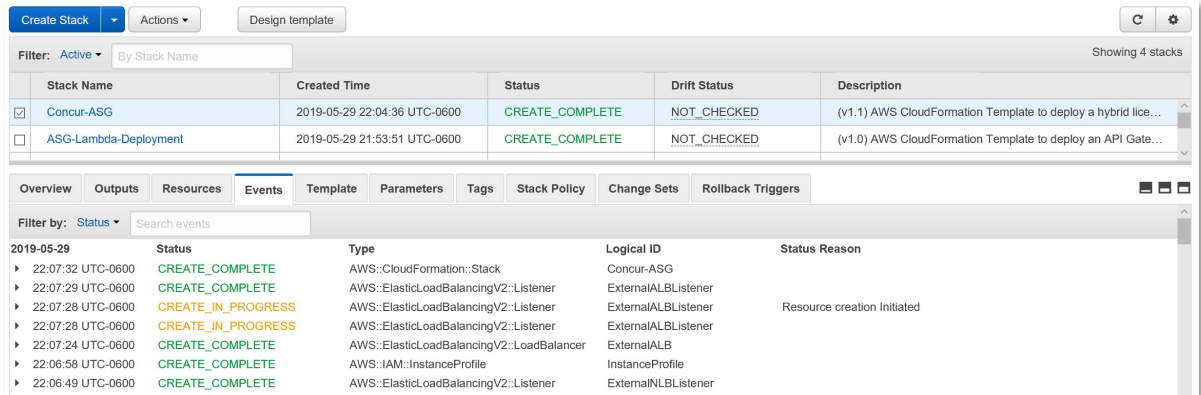
The screenshot shows the 'Options' section of the console, which includes two sub-sections:

- Tags:** A section where you can specify tags (key-value pairs) for resources in your stack. It includes a table with columns for 'Key' (127 characters maximum) and 'Value' (255 characters maximum). There is one row with a blue '+' button to add more tags.
- Permissions:** A section where you can choose an IAM role that CloudFormation uses to create, modify, or delete resources in the stack. It includes a dropdown menu labeled 'IAM Role' with the text 'Choose a role (optional)'.

- i. Select your rollback behavior and click Next to Review
- j. If the parameter details are correctly entered, click "Launch Stack"

Step 3: Validate FGT_AutoScale_ExistingVPC_Hybrid-Licensing Stack Deployment

- a. In the CloudFormation dashboard, validate that the ASG has a status of “CREATE_COMPLETE”

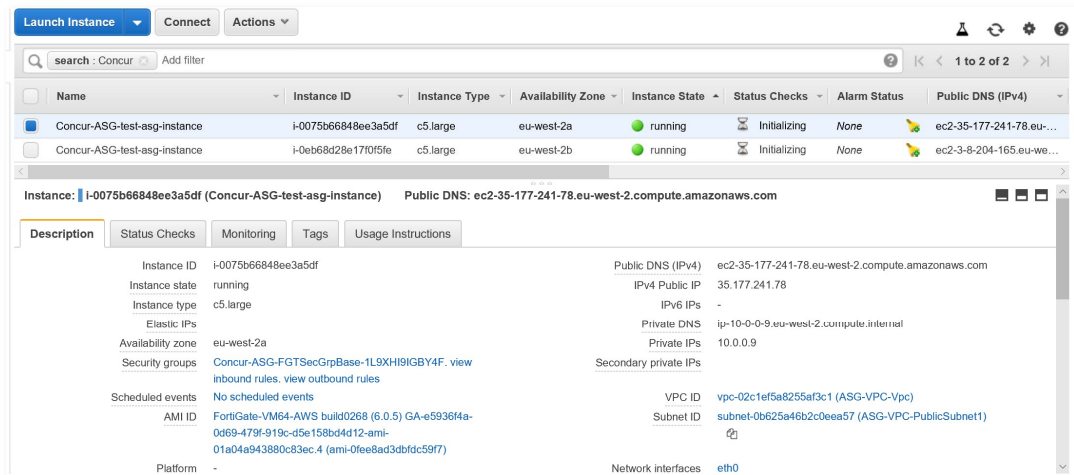


Stack Name	Created Time	Status	Drift Status	Description
Concur-ASG	2019-05-29 22:04:36 UTC-0600	CREATE_COMPLETE	NOT_CHECKED	(v1.1) AWS CloudFormation Template to deploy a hybrid lice...
ASG-Lambda-Deployment	2019-05-29 21:53:51 UTC-0600	CREATE_COMPLETE	NOT_CHECKED	(v1.0) AWS CloudFormation Template to deploy an API Gate...

Filter by: Status	Search events
2019-05-29	
22:07:32 UTC-0600	CREATE_COMPLETE
22:07:29 UTC-0600	CREATE_COMPLETE
22:07:28 UTC-0600	CREATE_IN_PROGRESS
22:07:28 UTC-0600	CREATE_IN_PROGRESS
22:07:24 UTC-0600	CREATE_COMPLETE
22:06:58 UTC-0600	CREATE_COMPLETE
22:06:49 UTC-0600	CREATE_COMPLETE

Status	Type	Logical ID	Status Reason
CREATE_COMPLETE	AWS::CloudFormation::Stack	Concur-ASG	
CREATE_COMPLETE	AWS::ElasticLoadBalancingV2::Listener	ExternalALBListener	
CREATE_IN_PROGRESS	AWS::ElasticLoadBalancingV2::Listener	ExternalALBListener	Resource creation initiated
CREATE_IN_PROGRESS	AWS::ElasticLoadBalancingV2::Listener	ExternalALBListener	
CREATE_COMPLETE	AWS::ElasticLoadBalancingV2::LoadBalancer	ExternalALB	
CREATE_COMPLETE	AWS::IAM::InstanceProfile	InstanceProfile	
CREATE_COMPLETE	AWS::ElasticLoadBalancingV2::Listener	ExternalNLBListener	

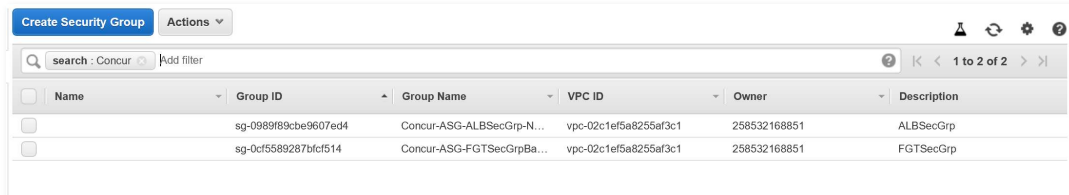
- b. Navigate to the EC2 dashboard and verify that the minimum number of instances of BYOL, and if selected, PAYG instances are instantiated. Validate that the FortiGates have 2 ENIs attached and that they are attached to the proper subnets.



Name	Instance ID	Instance Type	Availability Zone	Instance State	Status Checks	Alarm Status	Public DNS (IPv4)
Concur-ASG-test-asg-instance	i-0075b66848ee3a5df	c5.large	eu-west-2a	running	Initializing	None	ec2-35-177-241-78.eu-...
Concur-ASG-test-asg-instance	i-0eb68d28e17f0f5fe	c5.large	eu-west-2b	running	Initializing	None	ec2-3-8-204-165.eu-we...

Description	Status Checks	Monitoring	Tags	Usage Instructions
Instance ID: i-0075b66848ee3a5df	Instance state: running	Public DNS (IPv4): ec2-35-177-241-78.eu-west-2.compute.amazonaws.com		
Instance type: c5.large	IPV4 Public IP: 35.177.241.78	IPV6 IPs: -		
Elastic IPs: -	Private DNS: ip-10-0-0-8.eu-west-2.compute.internal	Private IPs: 10.0.0.9		
Availability zone: eu-west-2a	Secondary private IPs: -	VPC ID: vpc-02c1ef5a8255af3c1 (ASG-VPC-Vpc)		
Security groups: Concur-ASG-FGTSecGrpBase-1L9XH9IGBY4F. view inbound rules. view outbound rules		Subnet ID: subnet-0b625a46b2c0eea57 (ASG-VPC-PublicSubnet1)		
Scheduled events: No scheduled events		Network interfaces: eth0		
AMI ID: FortiGate-VM64-AWS build0268 (6.0.5) GA-e5936f4a-0d69-479f-919c-d5e158bd4d12-ami-01a04a943880c83ec.4 (ami-0fee8ad3dbfcd59f7)				
Platform: -				

- c. Validate that the Security Groups are created for the FortiGates and the ELBs



Name	Group ID	Group Name	VPC ID	Owner	Description
sg-0989f89cbe9607ed4	sg-0989f89cbe9607ed4	Concur-ASG-ALBSecGrp-N...	vpc-02c1ef5a8255af3c1	258532168851	ALBSecGrp
sg-0cf5589287bfcf514	sg-0cf5589287bfcf514	Concur-ASG-FGTSecGrpBa...	vpc-02c1ef5a8255af3c1	258532168851	FGTSecGrp

- d. Validate that the ENIs are created and attached to the FortiGates and the ELBs

Create Network Interface

Attach

Detach

Delete

Actions

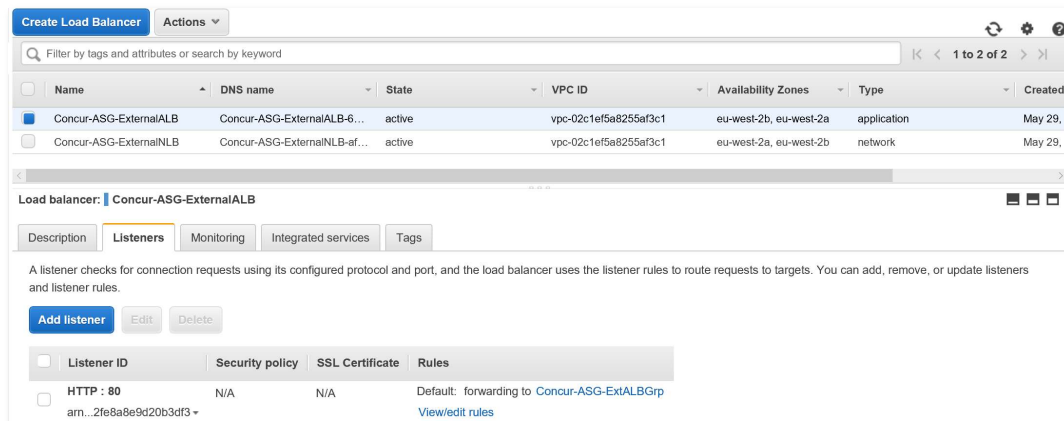
search : concur

Add filter

1 to 6 of 6

<input type="checkbox"/>	Name	Network interface	Subnet ID	VPC ID	Zone	Security group	Description	Instance ID
<input type="checkbox"/>	eni-030aa100d...	subnet-0b625a...	vpc-02c1ef5a8...	eu-west-2a	Concur-AS...	ELB app/Concur-ASG-ExternalALB/042399520a28994c		
<input type="checkbox"/>	eni-0b38f12c9...	subnet-0b625a...	vpc-02c1ef5a8...	eu-west-2a		ELB net/Concur-ASG-ExternalNLB/af90792770c00f92		
<input type="checkbox"/>	eni-0e36af66e...	subnet-0b625a...	vpc-02c1ef5a8...	eu-west-2a	Concur-AS...			i-0075b66848ee3a5df
<input type="checkbox"/>	eni-065bc2036...	subnet-01d392...	vpc-02c1ef5a8...	eu-west-2b	Concur-AS...	ELB app/Concur-ASG-ExternalALB/042399520a28994c		
<input type="checkbox"/>	eni-091a9fbb3...	subnet-01d392...	vpc-02c1ef5a8...	eu-west-2b		ELB net/Concur-ASG-ExternalNLB/af90792770c00f92		
<input type="checkbox"/>	eni-0c22d59dc...	subnet-01d392...	vpc-02c1ef5a8...	eu-west-2b	Concur-AS...			i-0eb68d28e17f0f5fe

- e. Validate LBs are deployed with the appropriate listeners (FortiGate policy will have to allow the ports configured on the ELBs)



Name	DNS name	State	VPC ID	Availability Zones	Type	Created
Concur-ASG-ExternalALB	Concur-ASG-ExternalALB-6...	active	vpc-02c1ef5a8255af3c1	eu-west-2b, eu-west-2a	application	May 29, 2019
Concur-ASG-ExternalNLB	Concur-ASG-ExternalNLB-af...	active	vpc-02c1ef5a8255af3c1	eu-west-2a, eu-west-2b	network	May 29, 2019

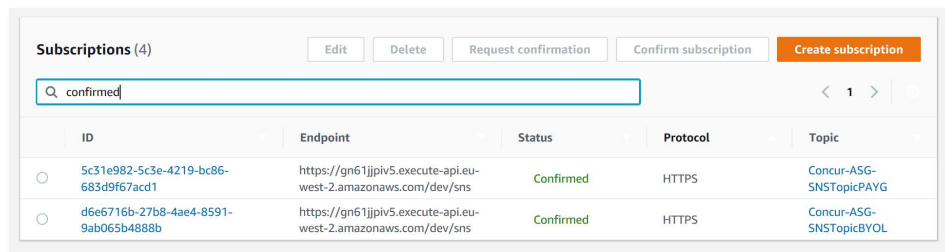
Listener ID	Security policy	SSL Certificate	Rules
arn:aws:elasticloadbalancing:eu-west-2:123456789012:listener/application/Concur-ASG-ExtALBGrp	N/A	N/A	Default: forwarding to Concur-ASG-ExtALBGrp

- f. Validate that the ASG has deployed with 2 ASGs – one each for BYOL and PAYG



Name	Launch Configuration / Template	Instances	Desired	Min	Max	Availability Zones	Default Cooldown	Health Check
Concur-ASG-A...	Concur-ASG-LaunchConfigBYOL-RCTBI33SVLVN	2	2	2	2	eu-west-2a, eu-west-2b	300	0
Concur-ASG-B...	Concur-ASG-LaunchConfigPAYG-PU1T4FL6MH5Q	0	0	0	5	eu-west-2a, eu-west-2b	300	0

- g. Validate that the SNS topics has valid subscriptions that are in a “Confirmed” Status



ID	Endpoint	Status	Protocol	Topic
5c31e982-5c3e-4219-bc86-683d9f67acd1	https://gn61jipiv5.execute-api.eu-west-2.amazonaws.com/dev/sns	Confirmed	HTTPS	Concur-ASG-SNSTopicPAYG
d6e6716b-27b8-4ae4-8591-9ab063b4888b	https://gn61jipiv5.execute-api.eu-west-2.amazonaws.com/dev/sns	Confirmed	HTTPS	Concur-ASG-SNSTopicBYOL

API Callback and SNS subscription

Modifying the Auto Scale Deployment

1. Adding load balancers
2. Dependencies