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. AWS Transit Gateway can be used to connect Amazon Virtual Private Clouds (Amazon VPCs) and their on-premises networks to a single gateway. This integration extends the FortiGate protection to all networks connected to the Transit Gateway. 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 with Transit Gateway integration requires FortiOS 6.2.1 and only supports On-Demand instances.

Deploying auto scaling on AWS with Transit Gateway integration

FortiGate Autoscale for AWS with Transit Gateway integration is available with FortiOS 6.2.1 and only supports On-Demand instances.

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

- AWS Transit Gateway
- 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 with Transit Gateway integration uses AWS CFTs to deploy the following components:

- A highly available architecture that spans two Availability Zones (AZs)
- An Amazon VPC configured with public and private subnets according to AWS best practices, to provide you with your own virtual network on AWS
- An Internet gateway to allow access to the Internet
- In the public subnets, FortiGate-VMs that act as NAT gateways, allowing outbound Internet access for resources in the private subnets
- In the public subnets, a FortiGate-VM host in an 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.
- 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
- Site-to-Site VPN connections

Planning

Deploying FortiGate Autoscale for AWS with 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 FortiGate Autoscale for AWS with Transit Gateway integration deployment package.

Template	Type	Description
workload-master.template	Entry template	Deploys the Auto Scaling solution to a new VPC by collecting information for deployment and then calling `workload.template`.
workload.template	Dependency template	Deploys the Auto Scaling solution to the target VPC.
create-transit-gateway.template	Dependency template	Creates a Transit Gateway for FortiGate Autoscale for AWS.
create-new-vpc.template	Dependency template	Creates a new VPC in which to deploy the FortiGate Autoscale solution.
create-autoscale-handler.template	Dependency template	Creates a FortiGate Autoscale Handler Lambda function and an API Gateway.
create-db-table.template	Dependency template	Creates all necessary DynamoDB tables for the FortiGate Autoscale solution.
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-tgw-vpn-handler.template	Dependency template	Creates a service for Transit Gateway VPN management.
create-auto-scaling-group.template	Dependency template	Creates a FortiGate Auto Scaling group and related components.

Prerequisites

Installing and configuring FortiGate Autoscale for AWS with Transit Gateway integration requires knowledge of the following:

- Configuring a FortiGate using the CLI
- AWS CloudFormation templates
- AWS Lambda Function
- Border Gateway Protocol (BGP)
- Equal-cost multi-path (ECMP)

It is expected that FortiGate Autoscale for AWS with 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 with Transit Gateway integration.

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

   AWS Auto Scaling and AWS Transit Gateway are not supported in every region. Please check the AWSRegion 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 FortiGate listing, as it is required for your deployment.

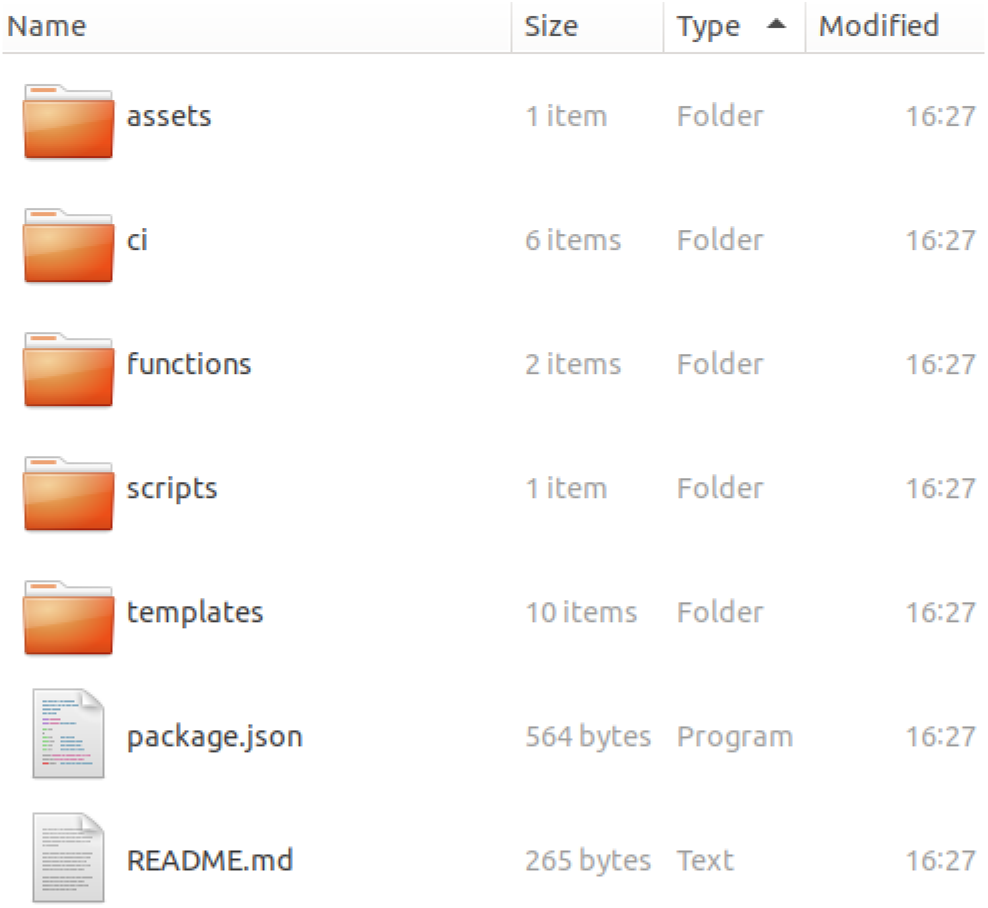
   Without a valid subscription, the deployment will fail with errors.

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 with Transit Gateway integration deployment package is located in the Fortinet GitHub project. To obtain the package:

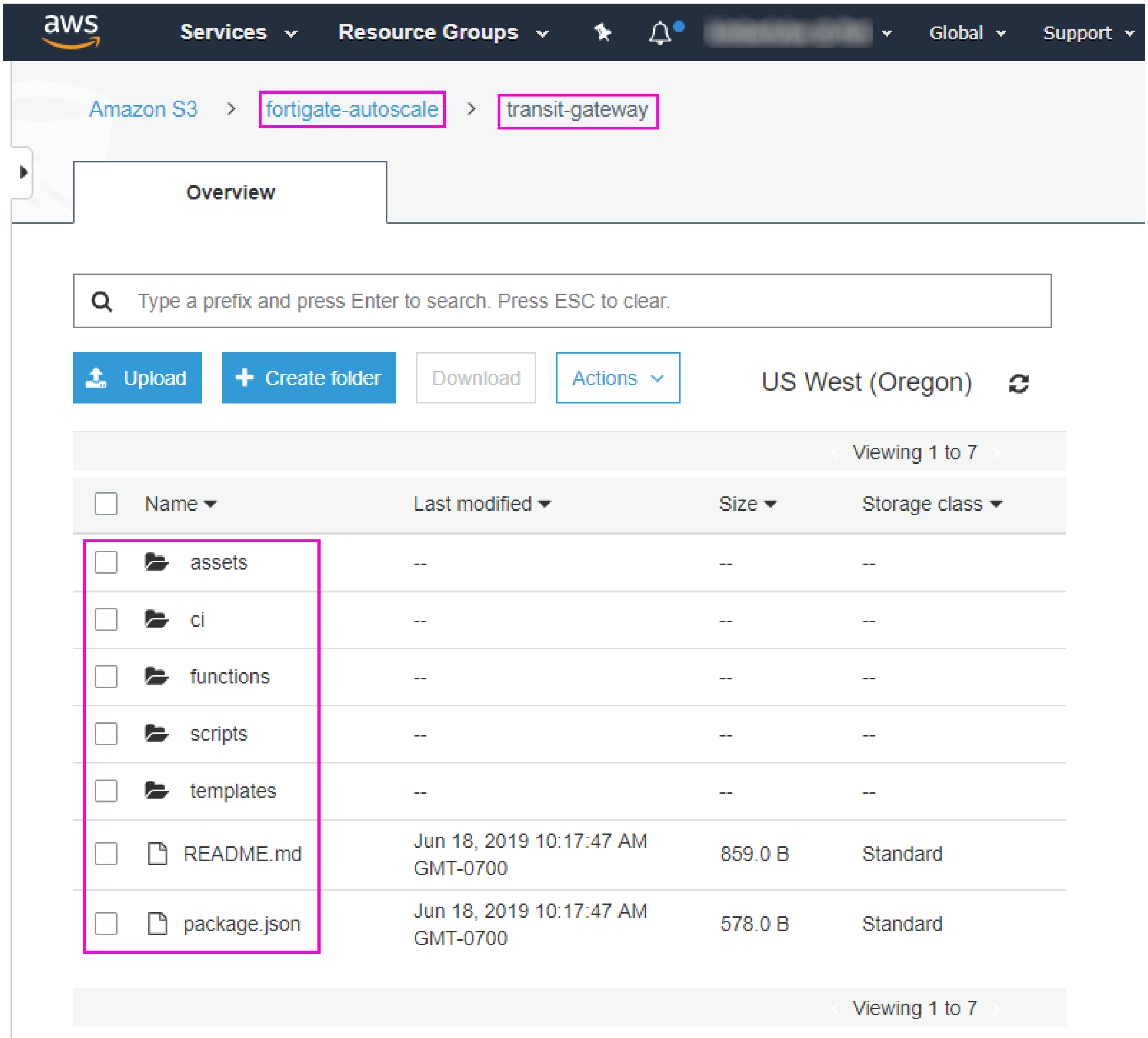
1. Visit the FortiGate Autoscale for AWS with Transit Gateway integration project release page and download the `fortigate-autoscale-aws-cloudformation.zip` for the version you want to use.
2. Unzip the file on your local PC. The following files and folders will be extracted:



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 the FortiGate Autoscale deployment package. In the example below, the folder is named *fortigate-autoscale*.
5. Inside this folder, create another folder to store the FortiGate Autoscale deployment resources. In the example below, this folder is named *transit-gateway*.
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 > transit-gateway*.



	Name	Last modified	Size	Storage class
□	assets	--	--	--
□	ci	--	--	--
□	functions	--	--	--
□	scripts	--	--	--
□	templates	--	--	--
□	README.md	Jun 18, 2019 10:17:47 AM GMT-0700	859.0 B	Standard
□	package.json	Jun 18, 2019 10:17:47 AM GMT-0700	578.0 B	Standard

Deploying the CloudFormation templates

The deployment will fail:

- if you do not have the required subscription for the On-Demand marketplace listing 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*: *.

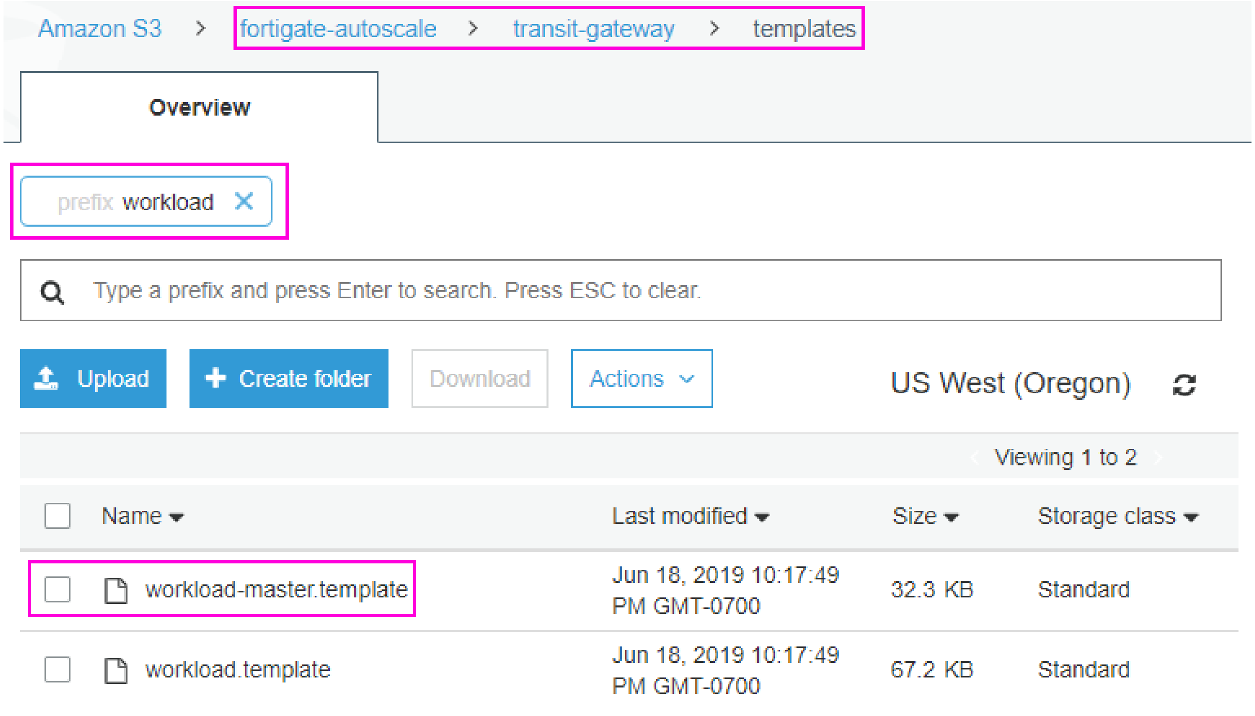
FortiGate Autoscale for AWS with Transit Gateway integration provides two deployment options:

- Deployment with a new Transit Gateway.
- Deployment with an existing Transit Gateway.

Both options will build a new AWS environment consisting of the VPC, subnets, FortiGate-VMs, security groups, and other infrastructure components. During configuration you can specify Classless Inter-Domain Routing (CIDR) blocks, instance types, and FortiGate settings. One inbound route domain and one outbound route domain will be created for the new or existing Transit Gateway. FortiGate Autoscale for AWS will then be deployed and attached to the Transit Gateway.

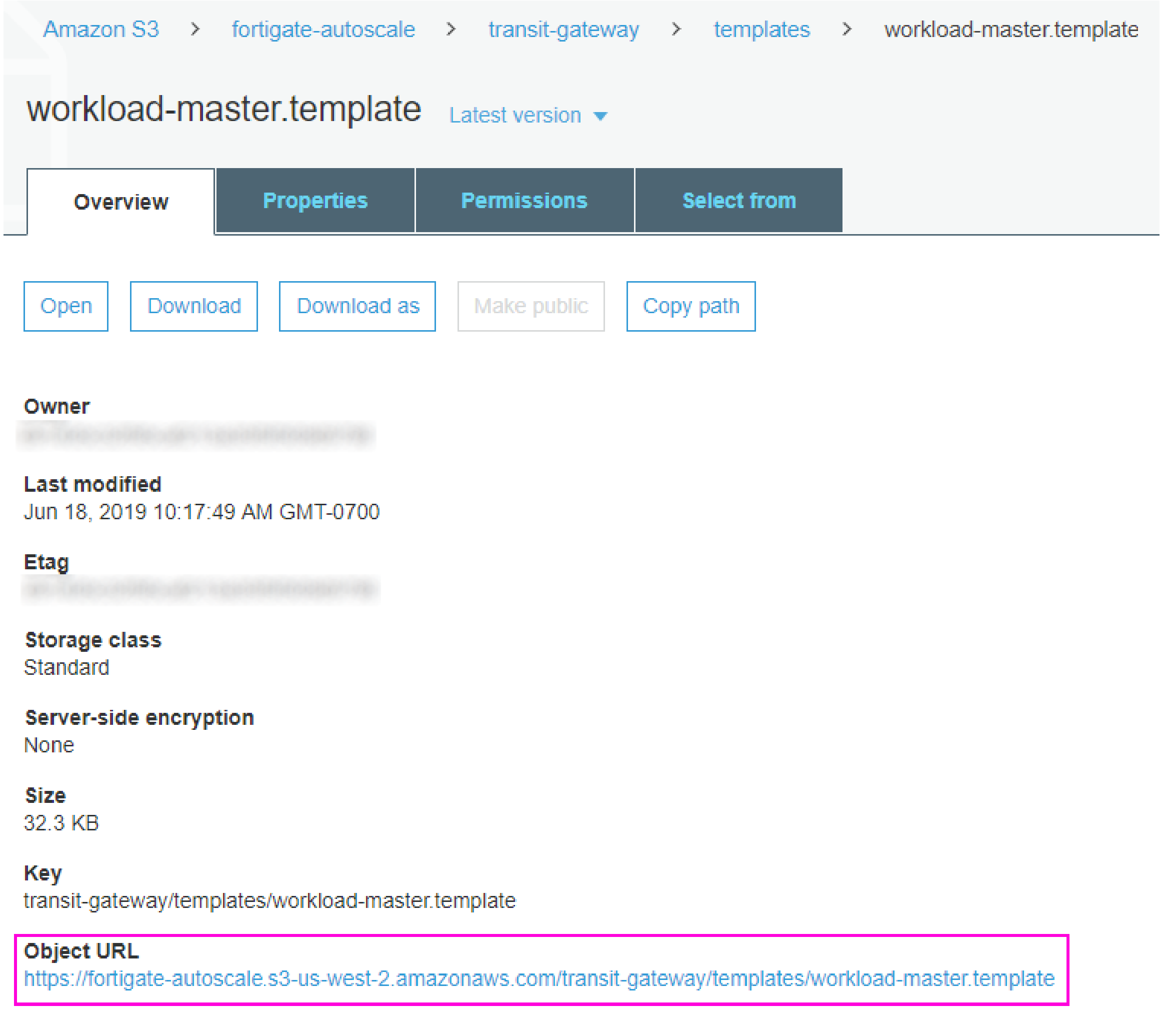
To deploy the CloudFormation templates:

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* > *transit-gateway*.
2. Click *templates* and select the entry template `workload-master.template`.


Amazon S3 > fortigate-autoscale > transit-gateway > templates
Overview
prefix workload ✕
Type a prefix and press Enter to search. Press ESC to clear.
Upload
Create folder
Download
Actions
US West (Oregon)
Viewing 1 to 2

□	Name	Last modified	Size	Storage class
□	workload-master.template	Jun 18, 2019 10:17:49 PM GMT-0700	32.3 KB	Standard
□	workload.template	Jun 18, 2019 10:17:49 PM GMT-0700	67.2 KB	Standard

3. Copy the *Object URL*.



Owner
[redacted]

Last modified
Jun 18, 2019 10:17:49 AM GMT-0700

Etag
[redacted]

Storage class
Standard

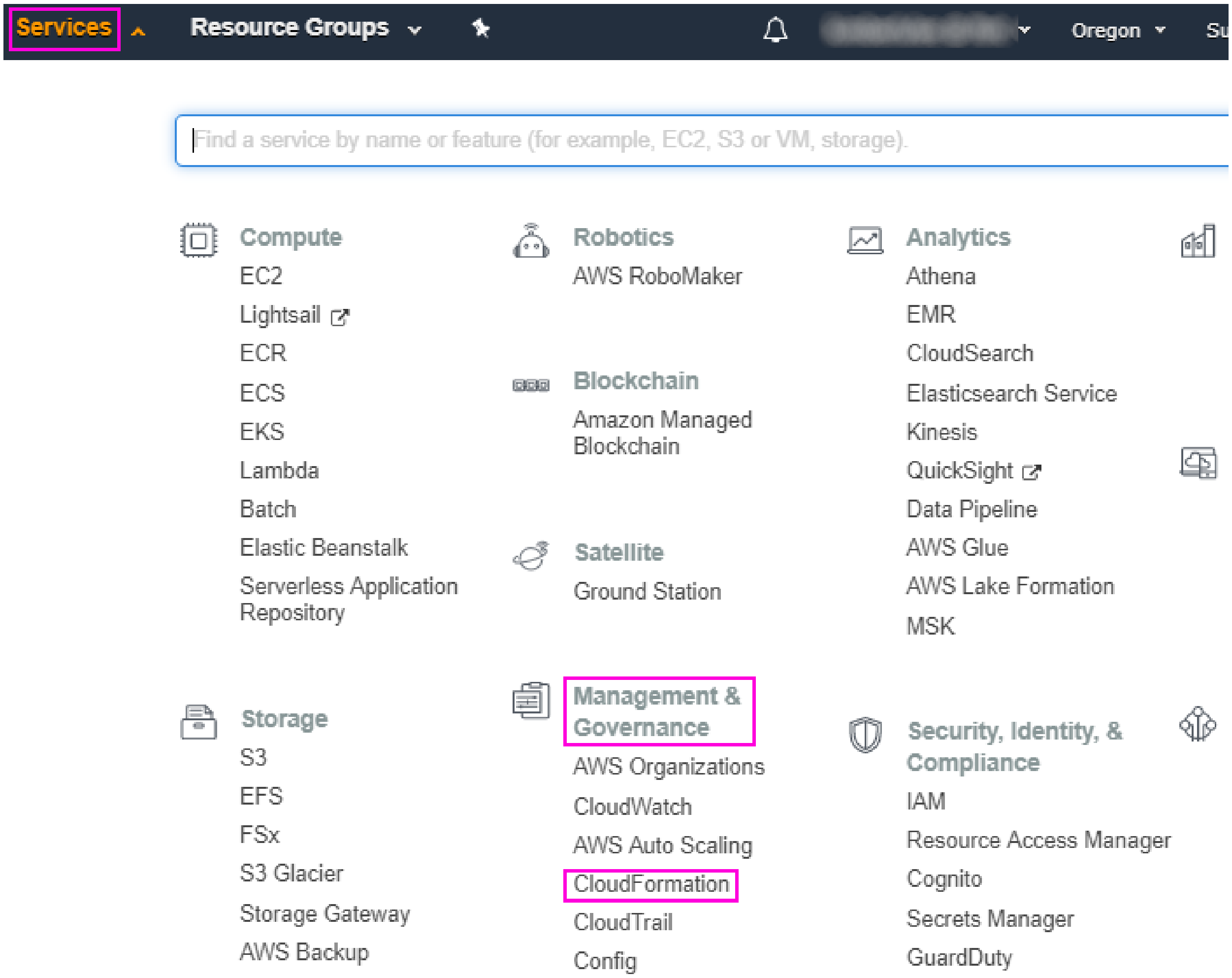
Server-side encryption
None

Size
32.3 KB

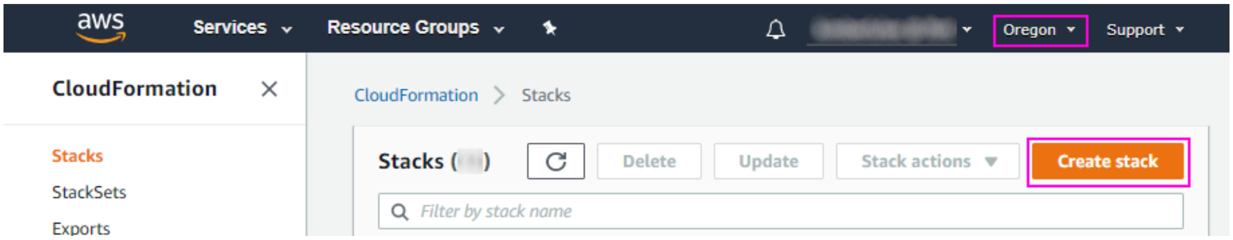
Key
transit-gateway/templates/workload-master.template

Object URL
https://fortigate-autoscale.s3-us-west-2.amazonaws.com/transit-gateway/templates/workload-master.template

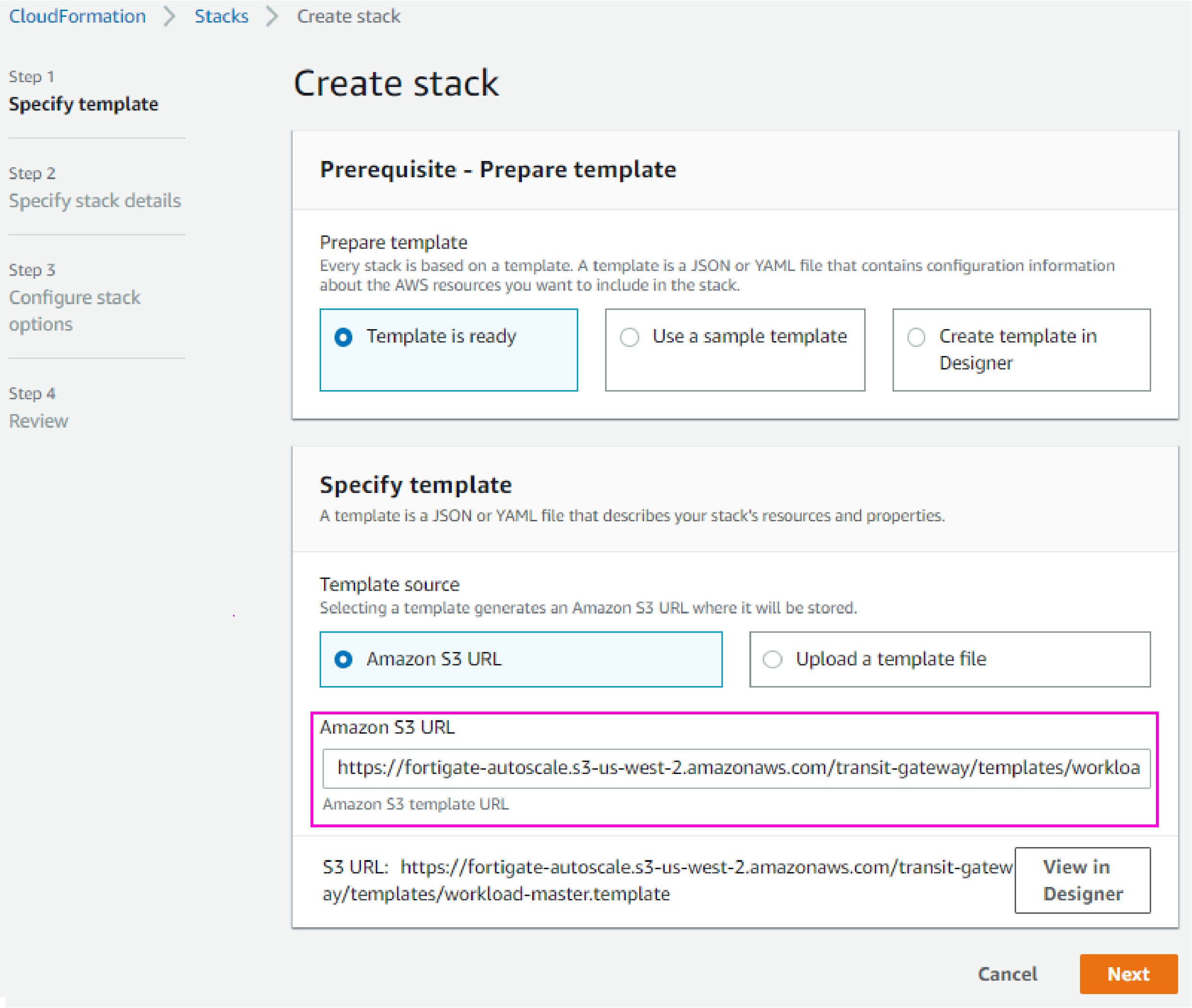
4. Click *Services*, and then *Management & Governance* > *CloudFormation*.



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

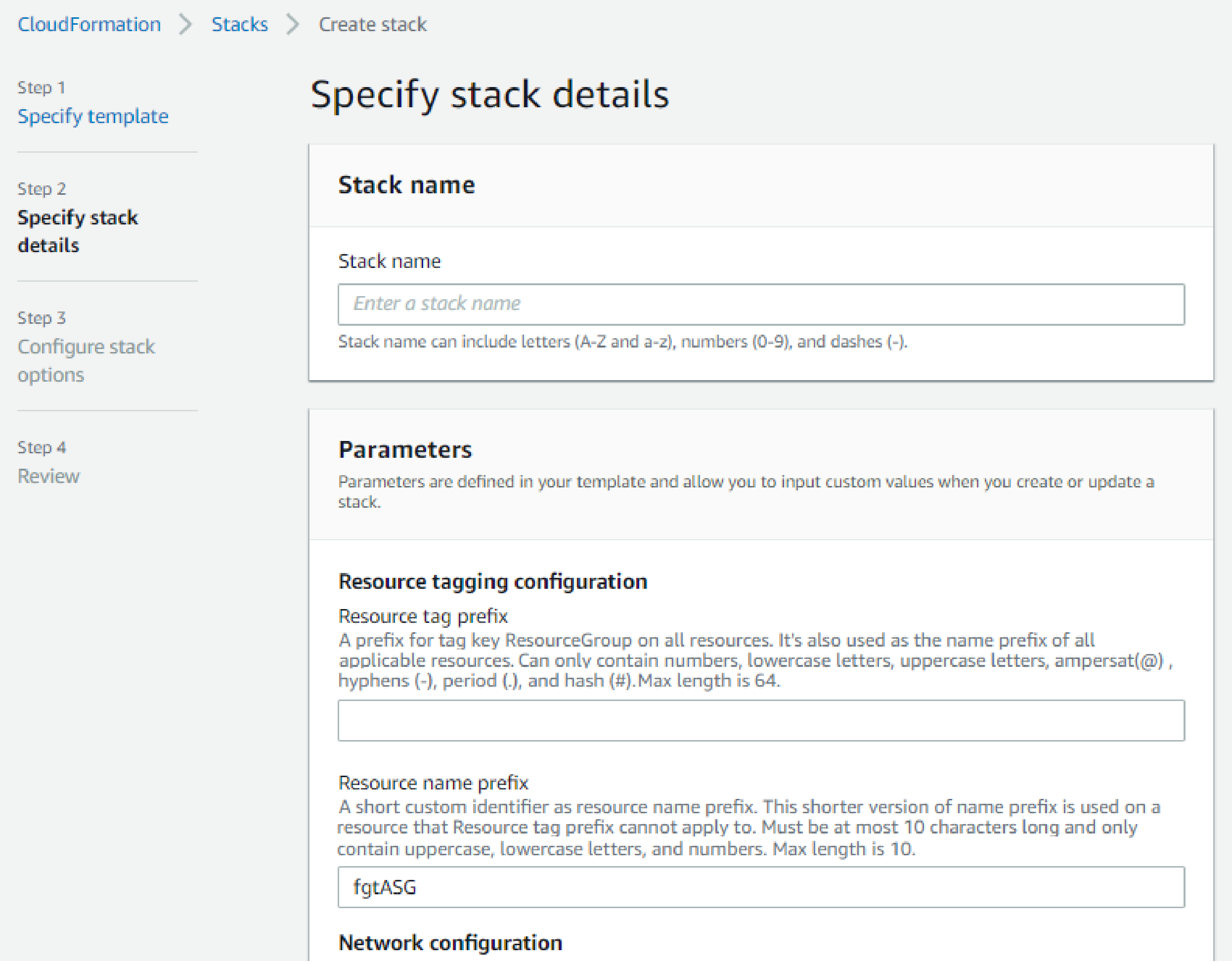
Amazon S3 URL
https://fortigate-autoscale.s3-us-west-2.amazonaws.com/transit-gateway/templates/workloa
Amazon S3 template URL

S3 URL: https://fortigate-autoscale.s3-us-west-2.amazonaws.com/transit-gateway/templates/workload-master.template

7. Click *Next*.

CFT parameters

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



CloudFormation > Stacks > Create stack

Step 1
Specify template

Step 2
Specify stack details

Step 3
Configure stack options

Step 4
Review

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

A prefix for tag key ResourceGroup on all resources. It's also used as the name prefix of all applicable resources. Can only contain numbers, lowercase letters, uppercase letters, ampersat(@) , hyphens (-), period (.), and hash (#).Max length is 64.

Resource name prefix

A short custom identifier as resource name prefix. This shorter version of name prefix is used on a resource that Resource tag prefix cannot apply to. Must be at most 10 characters long and only contain uppercase, lowercase letters, and numbers. 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

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 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.

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)	6.2.1	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.

Parameter label (name)	Default	Description
Key pair name (KeyPairName)	Requires input	Amazon EC2 Key Pair for admin access.
BGP ASN (BgpAsn)	65000	The Border Gateway Protocol (BGP) Autonomous System Number (ASN) of the Customer Gateway of each FortiGate-VM instance in the Auto Scaling group. This value ranges from 64512 to 65534.

FortiGate-VM Auto Scaling group configuration

Parameter label (name)	Default	Description
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.
Desired capacity (FgtAsgDesiredCapacity)	2	The number of FortiGate-VM instances the Auto Scaling group should have at any time. For High Availability, ensure at least 2 FortiGate-VMs are in the group. Minimum is 2.
Minimum group size (FgtAsgMinSize)	2	The number of FortiGate-VM instances the Auto Scaling group should have at any time. Minimum is 2.
Maximum group size (FgtAsgMaxSize)	4	Maximum number of FortiGate-VM instances in the Auto Scaling group. Minimum is 2.
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 (FgtCooldown)	300	The Auto Scaling group waits for the cool down period (in seconds) to complete before resuming scaling activities. Minimum is 60. Maximum is 3600.
Scale-out threshold (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. Minimum is 1. Maximum is 100.

Transit Gateway configuration

Parameter label (name)	Default	Description
Transit Gateway support (TransitGatewaySupportOptions)	Create one	Create a Transit Gateway for the FortiGate Autoscale VPC to attach to, or specify to use an existing one.
Transit Gateway ID (TransitGatewayId)	Conditionally requires input	Required when *Transit Gateway support* is set to "use an existing one". It is the ID of the Transit Gateway that the FortiGate Autoscale VPC will be attached to.

Failover configuration

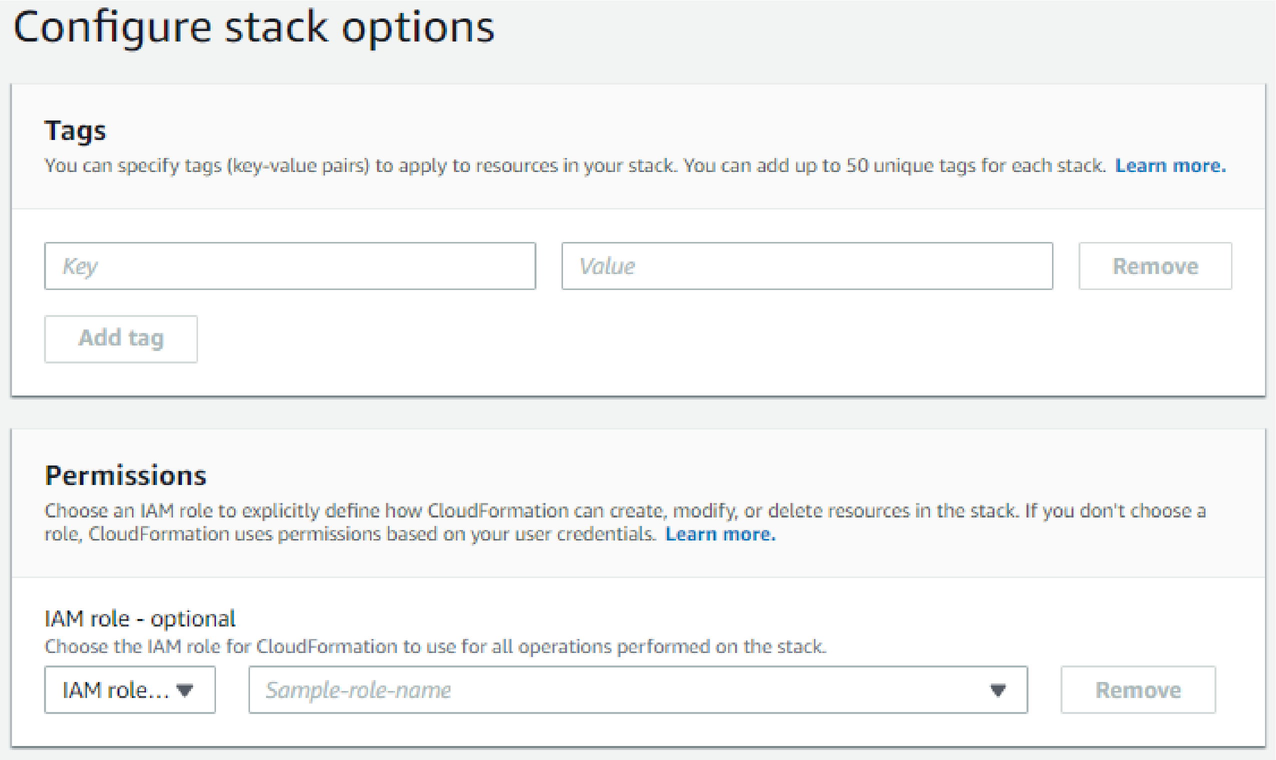
Parameter label (name)	Default	Description
Heart beat loss count (HeartBeatLossCount)	3	Number of consecutively lost heartbeats. When the Heartbeat loss count has been reached, the FortiGate-VM is deemed unhealthy and failover activities will commence.
Heart beat interval (HeartBeatInterval)	30	The length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

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

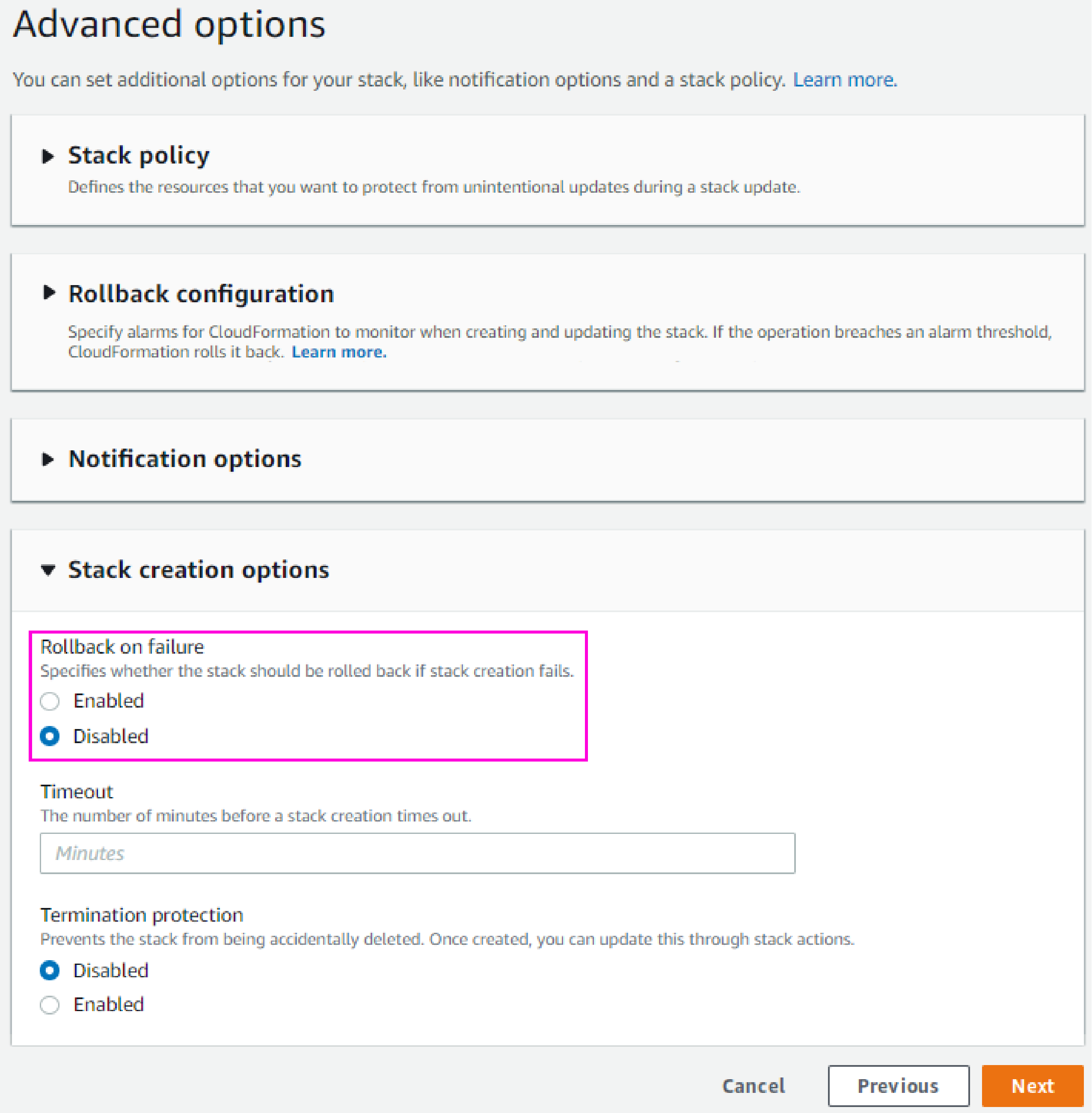
Choose an IAM role to explicitly define how CloudFormation can create, modify, or delete resources in the stack. If you don't choose a role, CloudFormation uses permissions based on your user credentials. **Learn more.**

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**

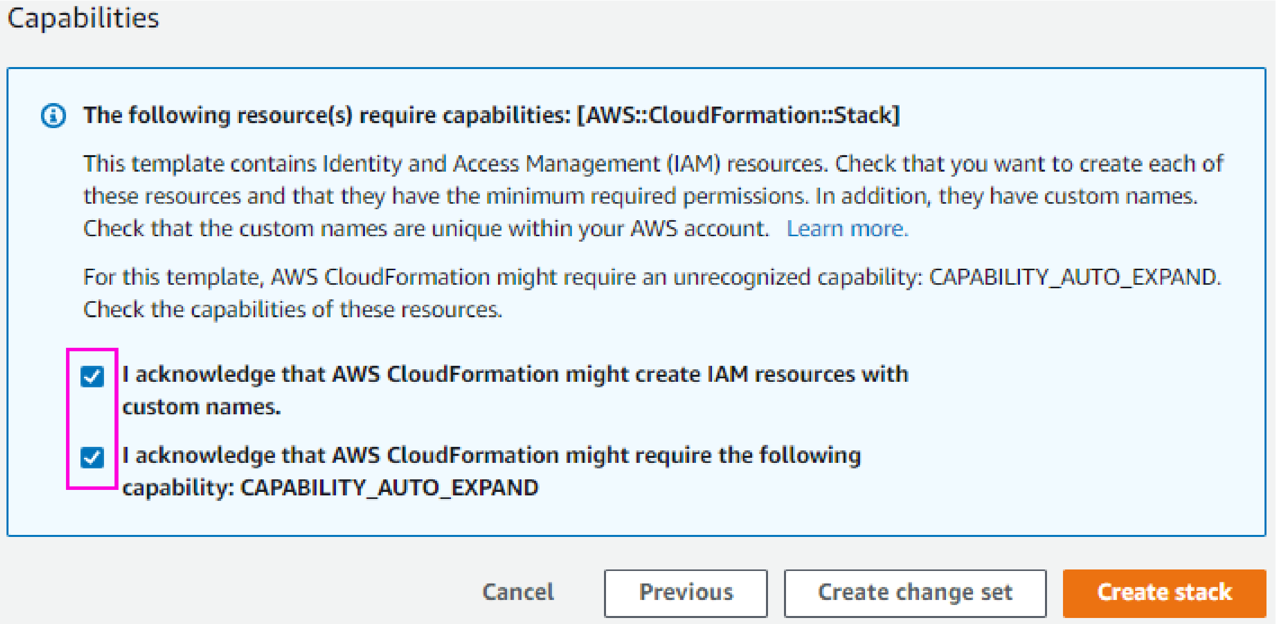
▼ **Stack creation options**

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]

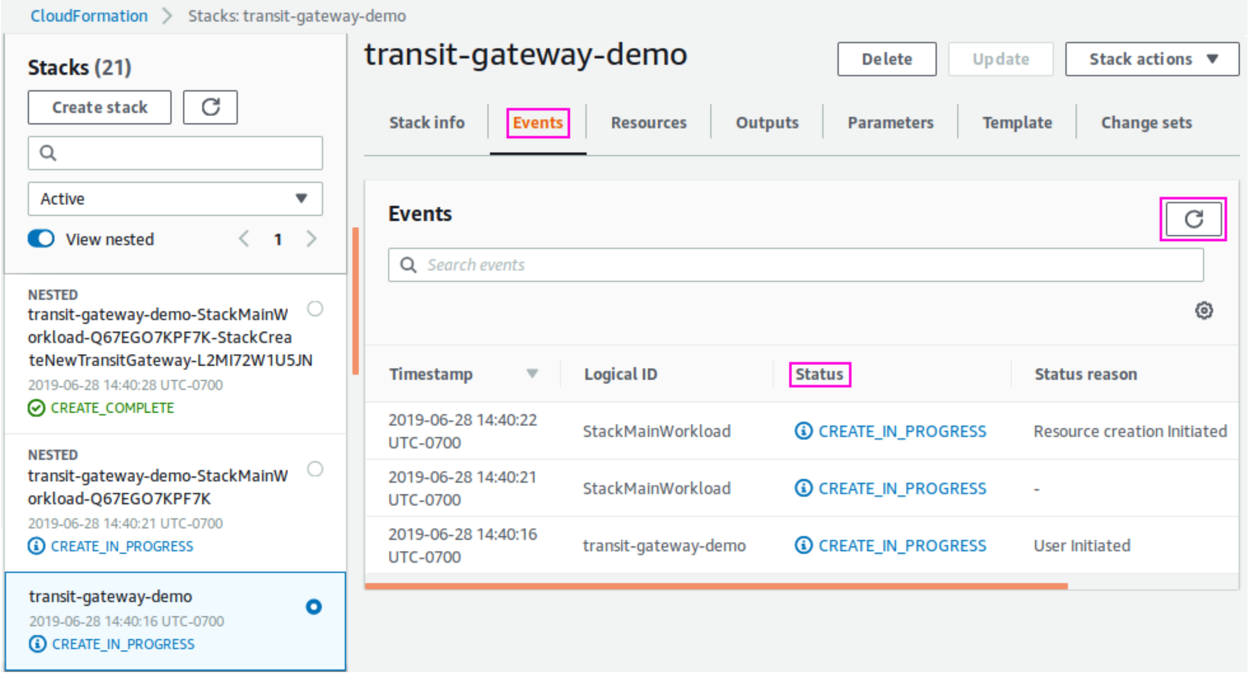
This template contains Identity and Access Management (IAM) resources. Check that you want to create each of these resources and that they have the minimum required permissions. In addition, they have custom names. Check that the custom names are unique within your AWS account. Learn more.

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.



transit-gateway-demo

NESTED
transit-gateway-demo-StackMainWorkload-Q67EGO7KPF7K-StackCreateNewTransitGateway-L2MI72W1U5JN
2019-06-28 14:40:28 UTC-0700
CREATE_COMPLETE

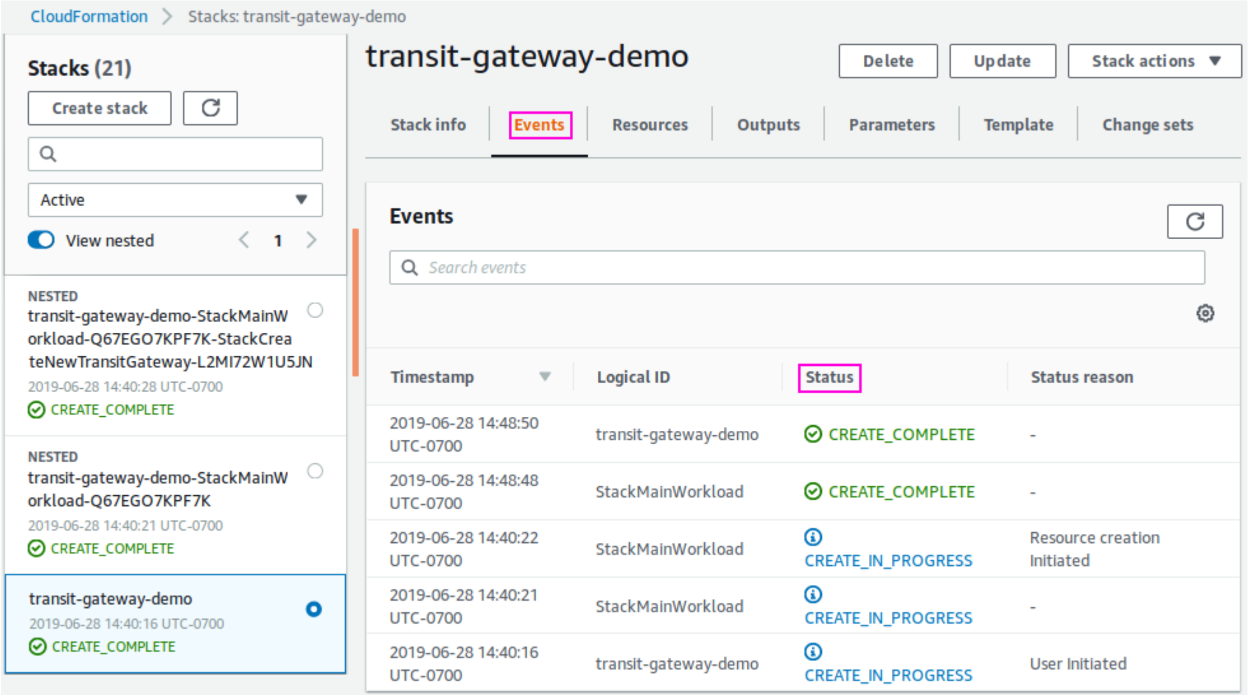
NESTED
transit-gateway-demo-StackMainWorkload-Q67EGO7KPF7K
2019-06-28 14:40:21 UTC-0700
CREATE_IN_PROGRESS

transit-gateway-demo
2019-06-28 14:40:16 UTC-0700
CREATE_IN_PROGRESS

Events

Timestamp	Logical ID	Status	Status reason
2019-06-28 14:40:22 UTC-0700	StackMainWorkload	CREATE_IN_PROGRESS	Resource creation Initiated
2019-06-28 14:40:21 UTC-0700	StackMainWorkload	CREATE_IN_PROGRESS	-
2019-06-28 14:40:16 UTC-0700	transit-gateway-demo	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
transit-gateway-demo-StackMainWorkload-Q67EGO7KPF7K-StackCreateNewTransitGateway-L2MI72W1U5JN
2019-06-28 14:40:28 UTC-0700
CREATE_COMPLETE

NESTED
transit-gateway-demo-StackMainWorkload-Q67EGO7KPF7K
2019-06-28 14:40:21 UTC-0700
CREATE_COMPLETE

transit-gateway-demo
2019-06-28 14:40:16 UTC-0700
CREATE_COMPLETE

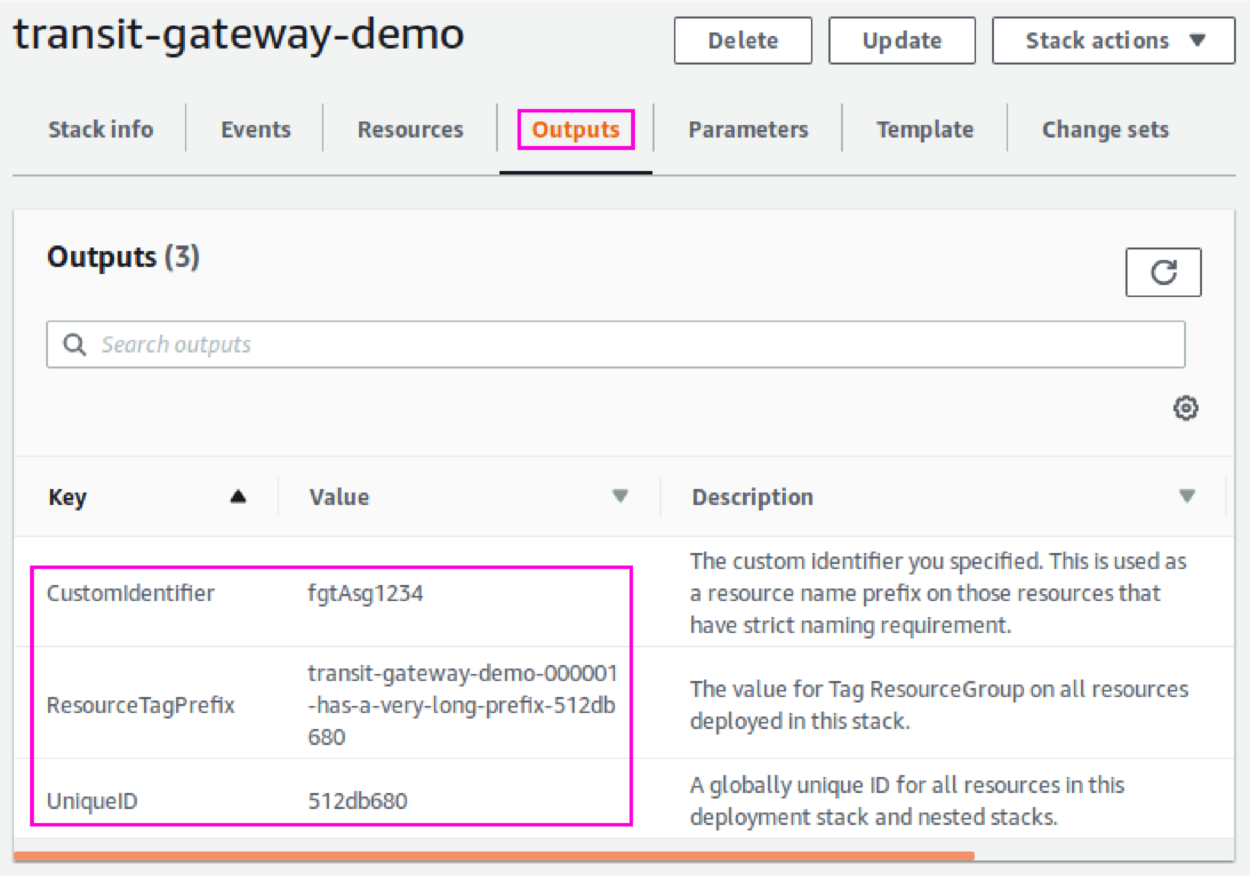
transit-gateway-demo

Events

Timestamp	Logical ID	Status	Status reason
2019-06-28 14:48:50 UTC-0700	transit-gateway-demo	CREATE_COMPLETE	-
2019-06-28 14:48:48 UTC-0700	StackMainWorkload	CREATE_COMPLETE	-
2019-06-28 14:40:22 UTC-0700	StackMainWorkload	CREATE_IN_PROGRESS	Resource creation Initiated
2019-06-28 14:40:21 UTC-0700	StackMainWorkload	CREATE_IN_PROGRESS	-
2019-06-28 14:40:16 UTC-0700	transit-gateway-demo	CREATE_IN_PROGRESS	User Initiated

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*.

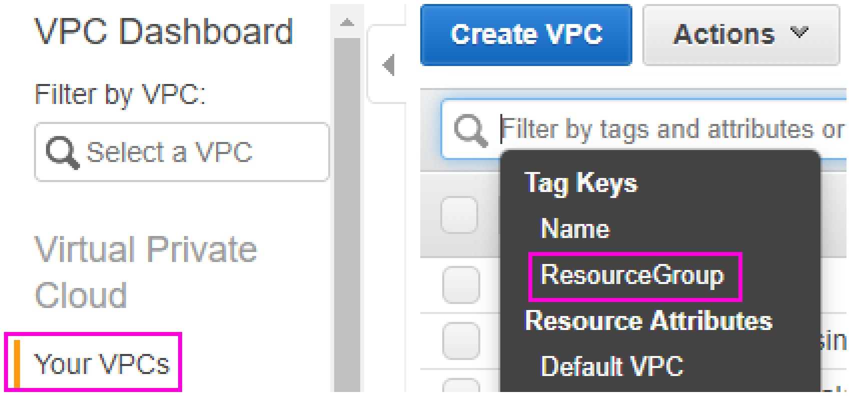


Key	Value	Description
CustomIdentifier	fgtAsg1234	The custom identifier you specified. This is used as a resource name prefix on those resources that have strict naming requirement.
ResourceTagPrefix	transit-gateway-demo-000001-has-a-very-long-prefix-512db680	The value for Tag ResourceGroup on all resources deployed in this stack.
UniqueID	512db680	A globally unique ID for all resources in this deployment stack and nested stacks.

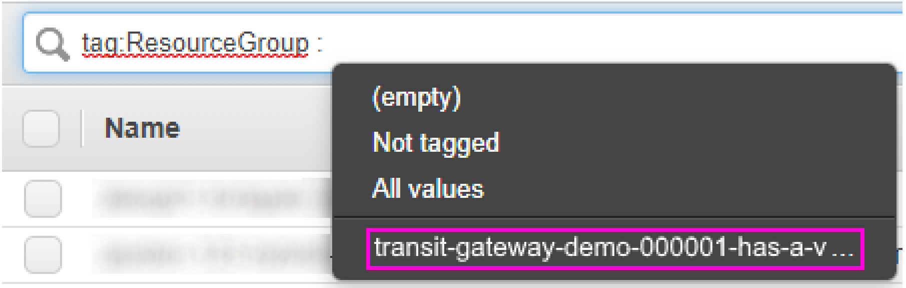
To look up the newly deployed VPC using the Tag Key:

1. In the AWS console, select *Services* > *Network & Content Delivery* > *VPC*.
2. In the left navigation tree, click *Your VPCs*.

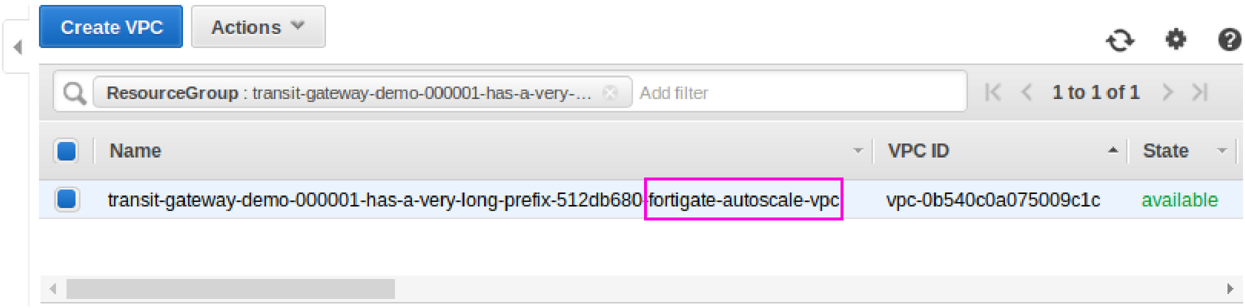
3. Click the filter box and select *Tag Keys* > *ResourceGroup*.



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*.

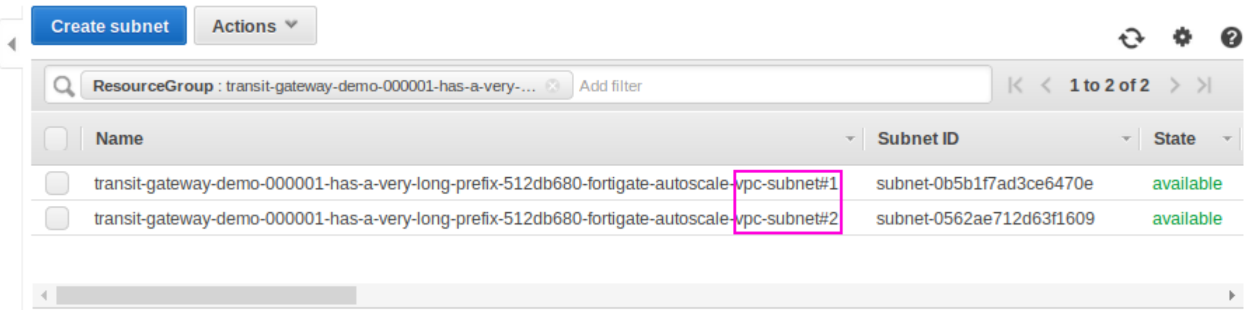


Name	VPC ID	State
transit-gateway-demo-000001-has-a-very-long-prefix-512db680-fortigate-autoscale-vpc	vpc-0b540c0a075009c1c	available

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

1. In the left navigation tree, click *Your VPCs*.
2. Click the filter box and select *Tag Keys* > *ResourceGroup*.
3. Select your *ResourceTagPrefix* from the list of Tag Keys.

Your VPC subnets will be displayed. The *Name* of each subnets will be of the format *<ResourceTagPrefix>-fortigate-autoscale-vpc-subnet#<#>*.

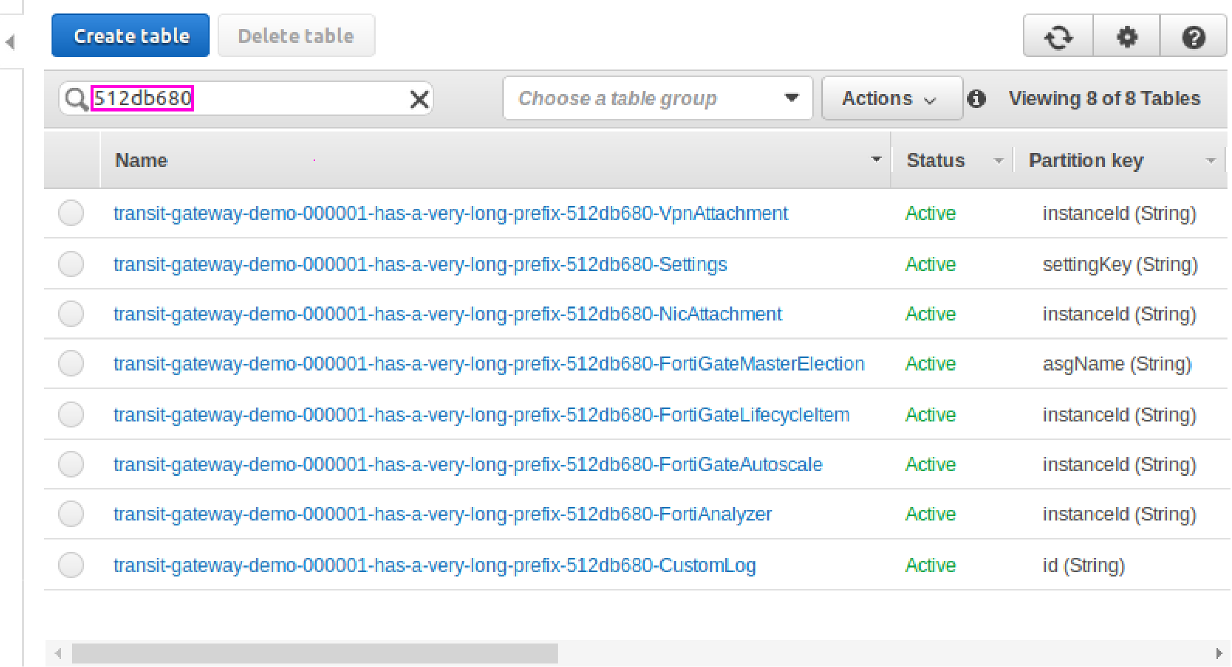


Name	Subnet ID	State
transit-gateway-demo-000001-has-a-very-long-prefix-512db680-fortigate-autoscale-vpc-subnet#1	subnet-0b5b1f7ad3ce6470e	available
transit-gateway-demo-000001-has-a-very-long-prefix-512db680-fortigate-autoscale-vpc-subnet#2	subnet-0562ae712d63f1609	available

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>*.

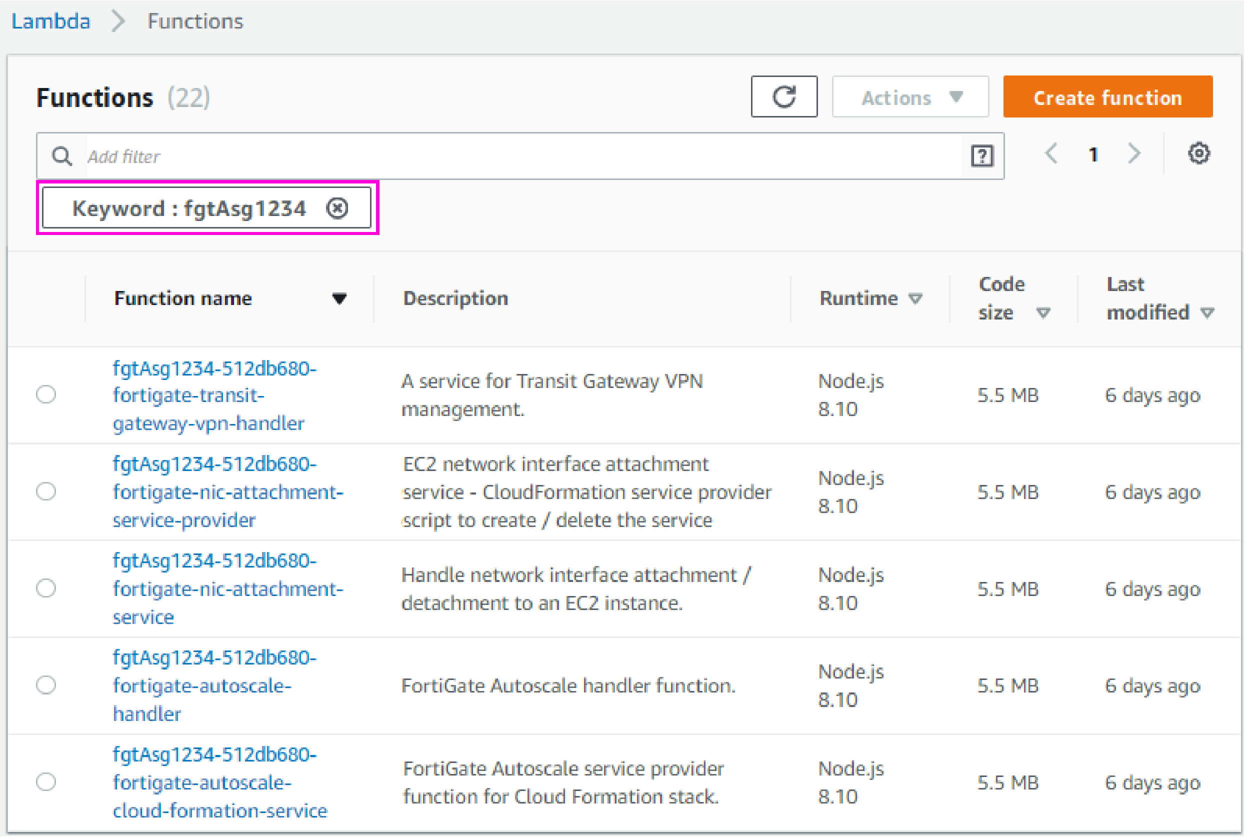


Name	Status	Partition key
transit-gateway-demo-000001-has-a-very-long-prefix-512db680-VpnAttachment	Active	instanceId (String)
transit-gateway-demo-000001-has-a-very-long-prefix-512db680-Settings	Active	settingKey (String)
transit-gateway-demo-000001-has-a-very-long-prefix-512db680-NicAttachment	Active	instanceId (String)
transit-gateway-demo-000001-has-a-very-long-prefix-512db680-FortiGateMasterElection	Active	asgName (String)
transit-gateway-demo-000001-has-a-very-long-prefix-512db680-FortiGateLifecycleItem	Active	instanceId (String)
transit-gateway-demo-000001-has-a-very-long-prefix-512db680-FortiGateAutoscale	Active	instanceId (String)
transit-gateway-demo-000001-has-a-very-long-prefix-512db680-FortiAnalyzer	Active	instanceId (String)
transit-gateway-demo-000001-has-a-very-long-prefix-512db680-CustomLog	Active	id (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*.



	Function name ▼	Description	Runtime ▽	Code size ▽	Last modified ▽
○	fgtAsg1234-512db680-fortigate-transit-gateway-vpn-handler	A service for Transit Gateway VPN management.	Node.js 8.10	5.5 MB	6 days ago
○	fgtAsg1234-512db680-fortigate-nic-attachment-service-provider	EC2 network interface attachment service - CloudFormation service provider script to create / delete the service	Node.js 8.10	5.5 MB	6 days ago
○	fgtAsg1234-512db680-fortigate-nic-attachment-service	Handle network interface attachment / detachment to an EC2 instance.	Node.js 8.10	5.5 MB	6 days ago
○	fgtAsg1234-512db680-fortigate-autoscale-handler	FortiGate Autoscale handler function.	Node.js 8.10	5.5 MB	6 days ago
○	fgtAsg1234-512db680-fortigate-autoscale-cloud-formation-service	FortiGate Autoscale service provider function for Cloud Formation stack.	Node.js 8.10	5.5 MB	6 days ago

Click the *Function name* to go directly to the function.

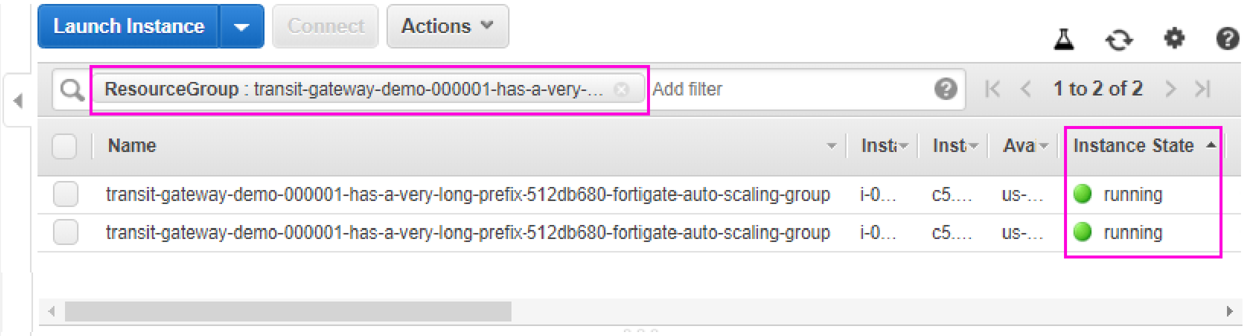
Verifying the deployment

FortiGate Autoscale for AWS with Transit Gateway integration creates an Auto Scaling group with lifecycle events attached to the group. This VPC is attached to a Transit Gateway. Verify the following components:

- the Auto Scaling group
- the master election
- the Transit Gateway

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*.

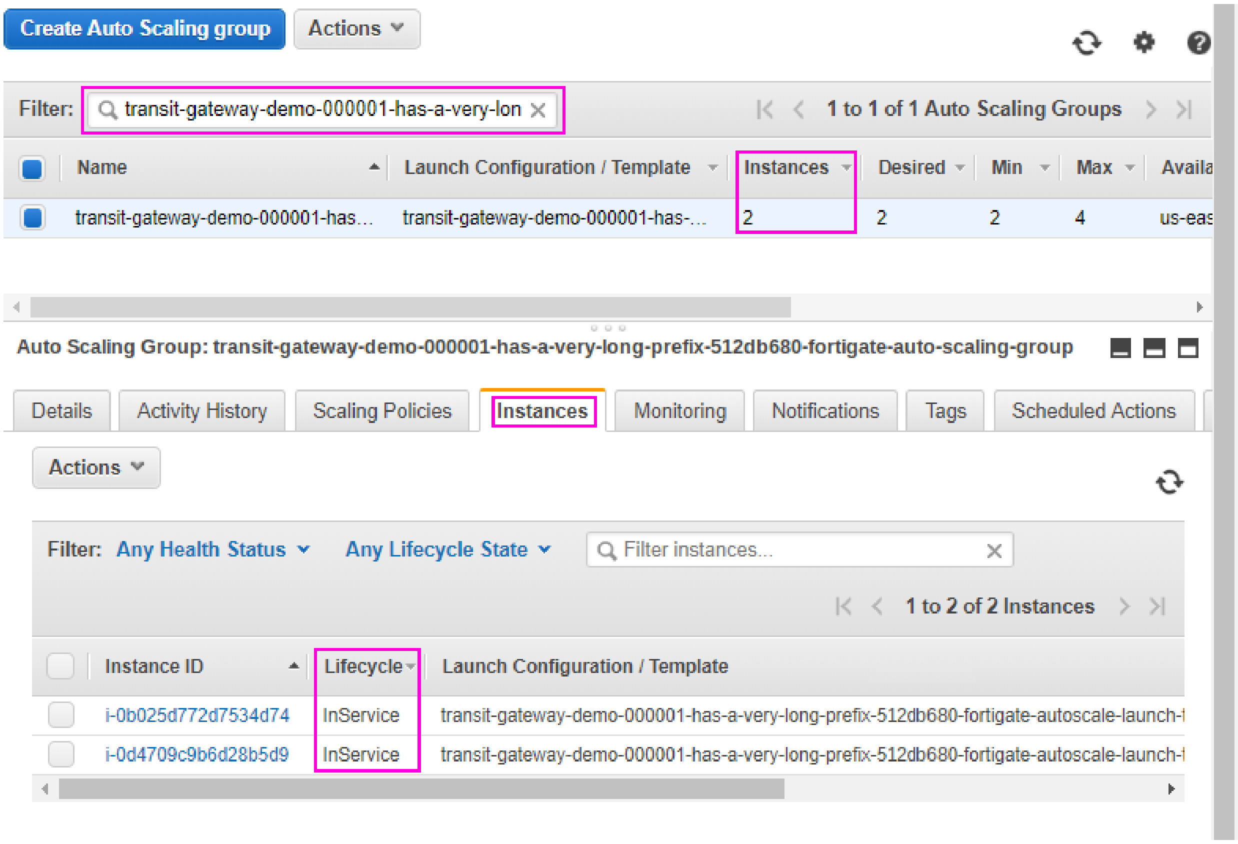


ResourceGroup : transit-gateway-demo-000001-has-a-very-...

□	Name	Inst	Inst	Ava	Instance State
□	transit-gateway-demo-000001-has-a-very-long-prefix-512db680-fortigate-auto-scaling-group	i-0...	c5....	us-...	● running
□	transit-gateway-demo-000001-has-a-very-long-prefix-512db680-fortigate-auto-scaling-group	i-0...	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*.



Filter: transit-gateway-demo-000001-has-a-very-lon

1 to 1 of 1 Auto Scaling Groups

Name	Launch Configuration / Template	Instances	Desired	Min	Max	Availa
transit-gateway-demo-000001-has…	transit-gateway-demo-000001-has-…	2	2	2	4	us-eas

Auto Scaling Group: transit-gateway-demo-000001-has-a-very-long-prefix-512db680-fortigate-auto-scaling-group

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

1 to 2 of 2 Instances

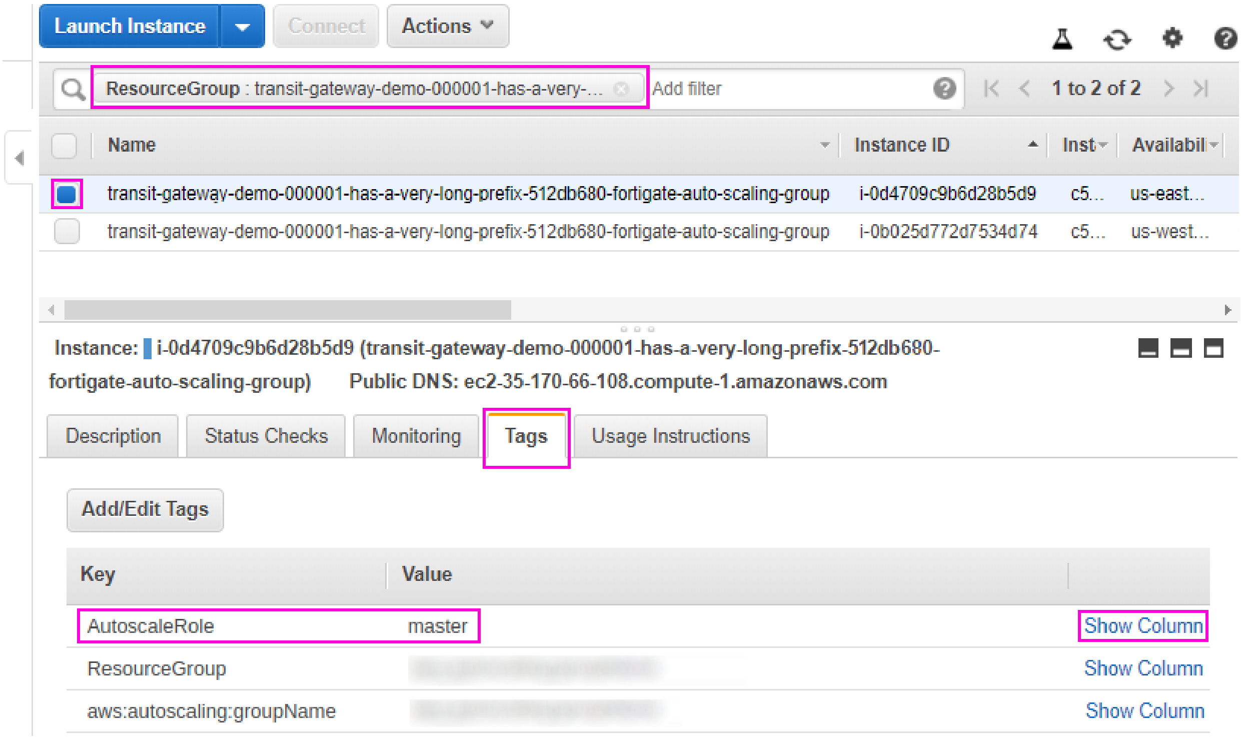
Instance ID	Lifecycle	Launch Configuration / Template
i-0b025d772d7534d74	InService	transit-gateway-demo-000001-has-a-very-long-prefix-512db680-fortigate-autoscale-launch-
i-0d4709c9b6d28b5d9	InService	transit-gateway-demo-000001-has-a-very-long-prefix-512db680-fortigate-autoscale-launch-

8. The Auto Scaling group will be listed. Confirm that the number in the *Instances* column is equal to or greater than the *Desired Capacity* you specified.
9. In the lower pane, click on the *Instances* tab and confirm that the *Lifecycle* of each instance is *InService*.

To verify the master election:

1. Locate the instances as described in steps 1 - 4 of the section To verify the Auto Scaling group: on page 26.
2. Select one of the instances.
3. In the lower pane, click the *Tags* tab and look for the Key *AutoScaleRole*. This tag only appears on the master FortiGate-VM instance. If you find it, it should be set to *master*. If it is not present, try another instance until you

find it.



Name	Instance ID	Inst	Availabil
transit-gateway-demo-000001-has-a-very-long-prefix-512db680-fortigate-auto-scaling-group	i-0d4709c9b6d28b5d9	c5...	us-east...
transit-gateway-demo-000001-has-a-very-long-prefix-512db680-fortigate-auto-scaling-group	i-0b025d772d7534d74	c5...	us-west...

Instance: i-0d4709c9b6d28b5d9 (transit-gateway-demo-000001-has-a-very-long-prefix-512db680-fortigate-auto-scaling-group) Public DNS: ec2-35-170-66-108.compute-1.amazonaws.com

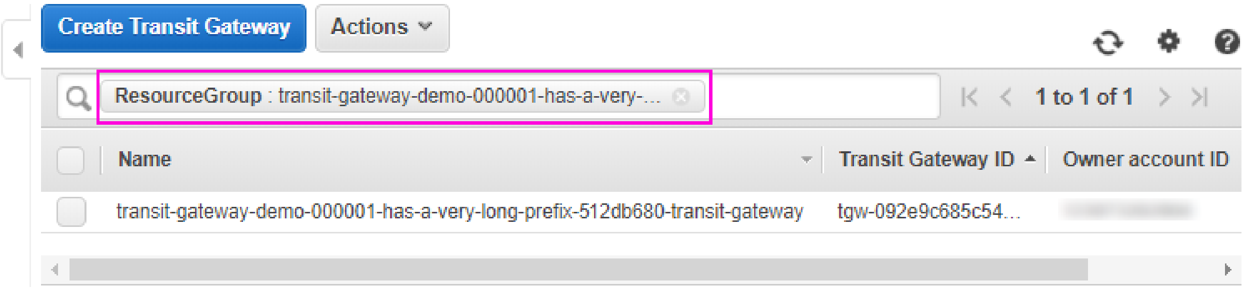
Key	Value	
AutoscaleRole	master	Show Column
ResourceGroup	[redacted]	Show Column
aws:autoscaling:groupName	[redacted]	Show Column

To display the *AutoScaleRole* column in the upper section, click *Show Column*.

Make note of the *instanceID* of the master instance, as you will need it to connect to the FortiGate-VM in the section Connecting to the master FortiGate-VM instance on page 31.

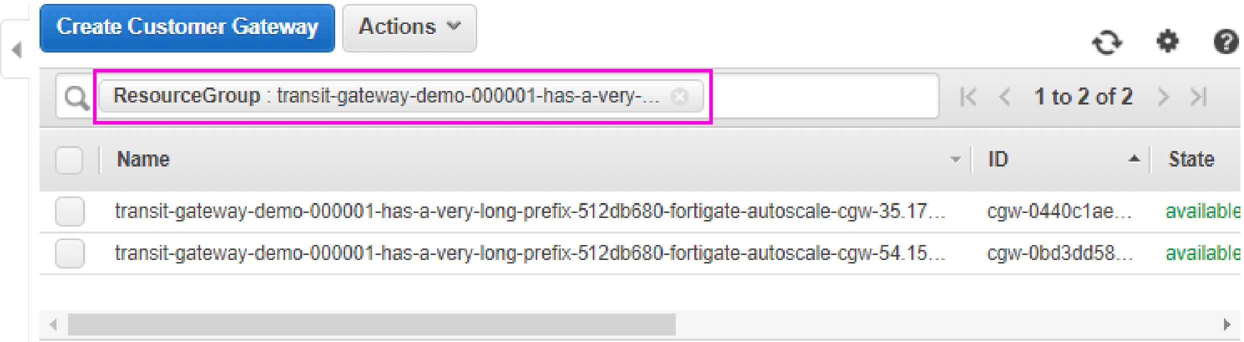
To verify the Transit Gateway:

1. In the AWS console, select the *Services* > *Network & Content Delivery* > *VPC*.
2. In the left navigation tree, click *Transit Gateways* > *Transit Gateways*.
3. Filter by the Tag Key *ResourceGroup*. There should be one result.



Name	Transit Gateway ID	Owner account ID
transit-gateway-demo-000001-has-a-very-long-prefix-512db680-transit-gateway	tgw-092e9c685c54...	[redacted]

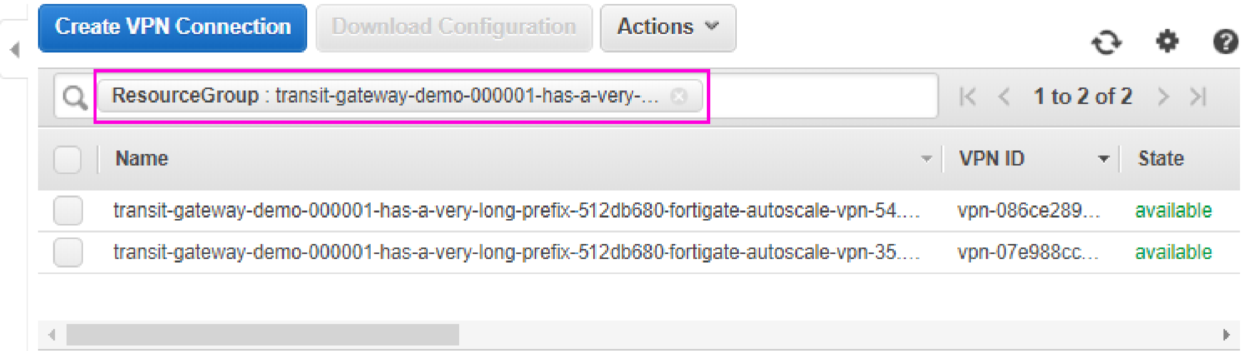
4. In the left navigation tree, click *Virtual Private Network (VPN)* > *Customer Gateways*.
5. Filter by the Tag Key *ResourceGroup*. There should be one customer gateway per running FortiGate-VM instance (2 at the start).



ResourceGroup : transit-gateway-demo-000001-has-a-very-...

Name	ID	State
transit-gateway-demo-000001-has-a-very-long-prefix-512db680-fortigate-autoscale-cgw-35.17...	cgw-0440c1ae...	available
transit-gateway-demo-000001-has-a-very-long-prefix-512db680-fortigate-autoscale-cgw-54.15...	cgw-0bd3dd58...	available

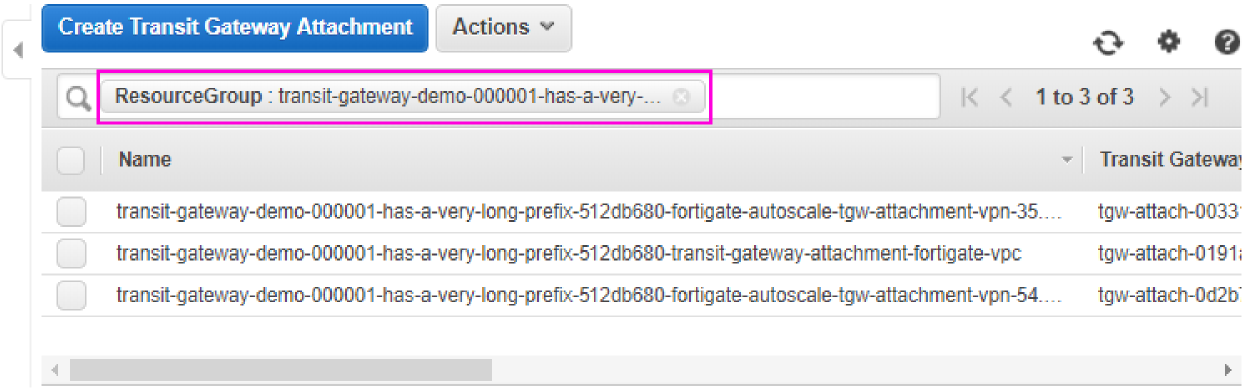
6. In the left navigation tree, click *Virtual Private Network (VPN) > Site-to-Site VPN Connections*.
7. Filter by the Tag Key *ResourceGroup*. There should be two items, 1 per FortiGate-VM instance, each with a corresponding Transit Gateway attachment.



ResourceGroup : transit-gateway-demo-000001-has-a-very-...

Name	VPN ID	State
transit-gateway-demo-000001-has-a-very-long-prefix-512db680-fortigate-autoscale-vpn-54....	vpn-086ce289...	available
transit-gateway-demo-000001-has-a-very-long-prefix-512db680-fortigate-autoscale-vpn-35....	vpn-07e988cc...	available

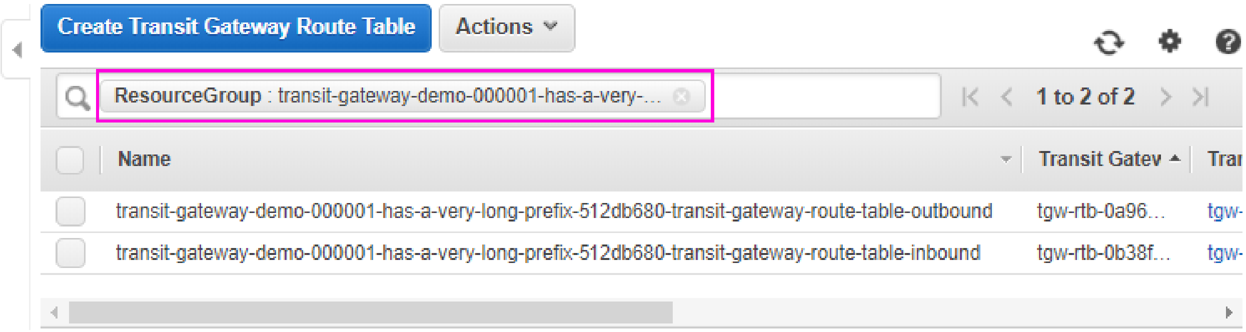
8. In the left navigation tree, click *Transit Gateways > Transit Gateway Attachments*.
9. Filter by the Tag Key *ResourceGroup*. There should be one VPC, and one VPN per running FortiGate-VM instance in the Auto Scaling group. (2 at the start, one master and one slave). The VPN name will contain the public IP address of the VPN.



ResourceGroup : transit-gateway-demo-000001-has-a-very-...

Name	Transit Gateway
transit-gateway-demo-000001-has-a-very-long-prefix-512db680-fortigate-autoscale-tgw-attachment-vpn-35....	tgw-attach-0033
transit-gateway-demo-000001-has-a-very-long-prefix-512db680-transit-gateway-attachment-fortigate-vpc	tgw-attach-0191
transit-gateway-demo-000001-has-a-very-long-prefix-512db680-fortigate-autoscale-tgw-attachment-vpn-54....	tgw-attach-0d2b

10. In the left navigation tree, click *Transit Gateway > Transit Gateway Route Tables*.
11. Filter by the Tag Key *ResourceGroup*. There should be two items, one for inbound and one for outbound. For diagrams, refer to the Appendix on page 44.



ResourceGroup : transit-gateway-demo-000001-has-a-very-…

□	Name	Transit Gatev	Trar
□	transit-gateway-demo-000001-has-a-very-long-prefix-512db680-transit-gateway-route-table-outbound	tgw-rtb-0a96…	tgw-
□	transit-gateway-demo-000001-has-a-very-long-prefix-512db680-transit-gateway-route-table-inbound	tgw-rtb-0b38f…	tgw-

Connecting to the master FortiGate-VM instance

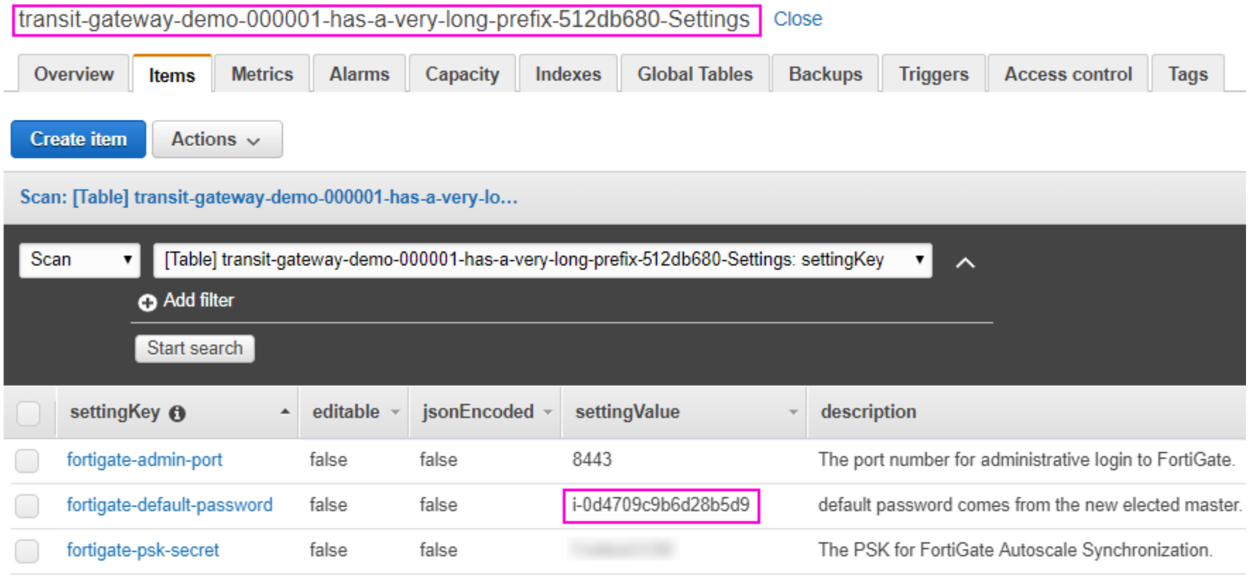
To connect to the master FortiGate-VM instance, you will need:

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

To obtain the password:

The initial password for all FortiGate-VM instances is the *instanceID* of the master FortiGate-VM. This is the *instanceID* you noted in the section To verify the master election: on page 27. It is also stored in the DynamoDB table *<ResourceTagPrefix>-Settings*.

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



transit-gateway-demo-000001-has-a-very-long-prefix-512db680-Settings

Scan: [Table] transit-gateway-demo-000001-has-a-very-lo...

Scan | [Table] transit-gateway-demo-000001-has-a-very-long-prefix-512db680-Settings: settingKey

settingKey	editable	jsonEncoded	settingValue	description
fortigate-admin-port	false	false	8443	The port number for administrative login to FortiGate.
fortigate-default-password	false	false	i-0d4709c9b6d28b5d9	default password comes from the new elected master.
fortigate-psk-secret	false	false	[redacted]	The PSK for FortiGate Autoscale Synchronization.

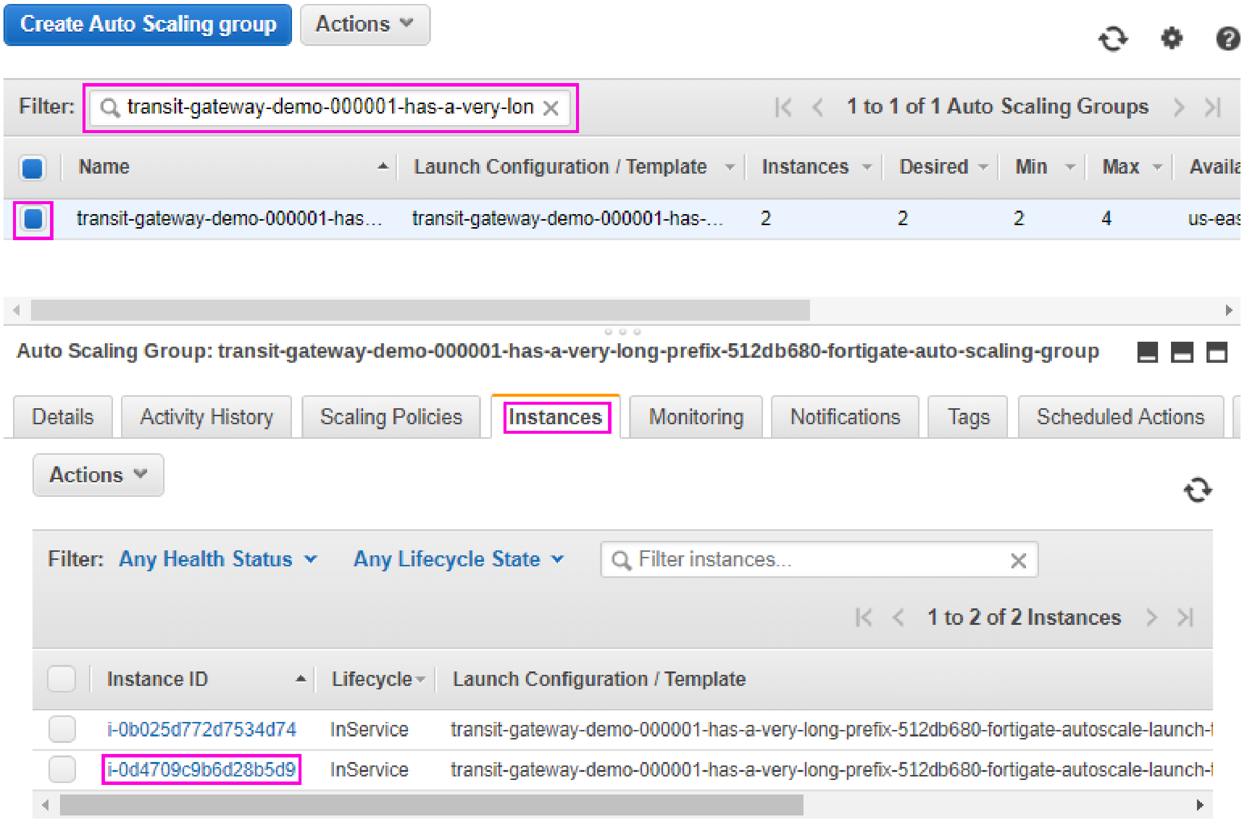
As the master FortiGate-VM propagates the password to all secondary FortiGate-VM instances, this is the initial password for all FortiGate-VM instances.

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 and 7 of the ASG portion of the section Verifying the deployment on page 26.

2. Select the Auto Scaling group.



Filter: transit-gateway-demo-000001-has-a-very-lon

1 to 1 of 1 Auto Scaling Groups

	Name	Launch Configuration / Template	Instances	Desired	Min	Max	Availa
■	transit-gateway-demo-000001-has…	transit-gateway-demo-000001-has-…	2	2	2	4	us-eas

Auto Scaling Group: transit-gateway-demo-000001-has-a-very-long-prefix-512db680-fortigate-auto-scaling-group

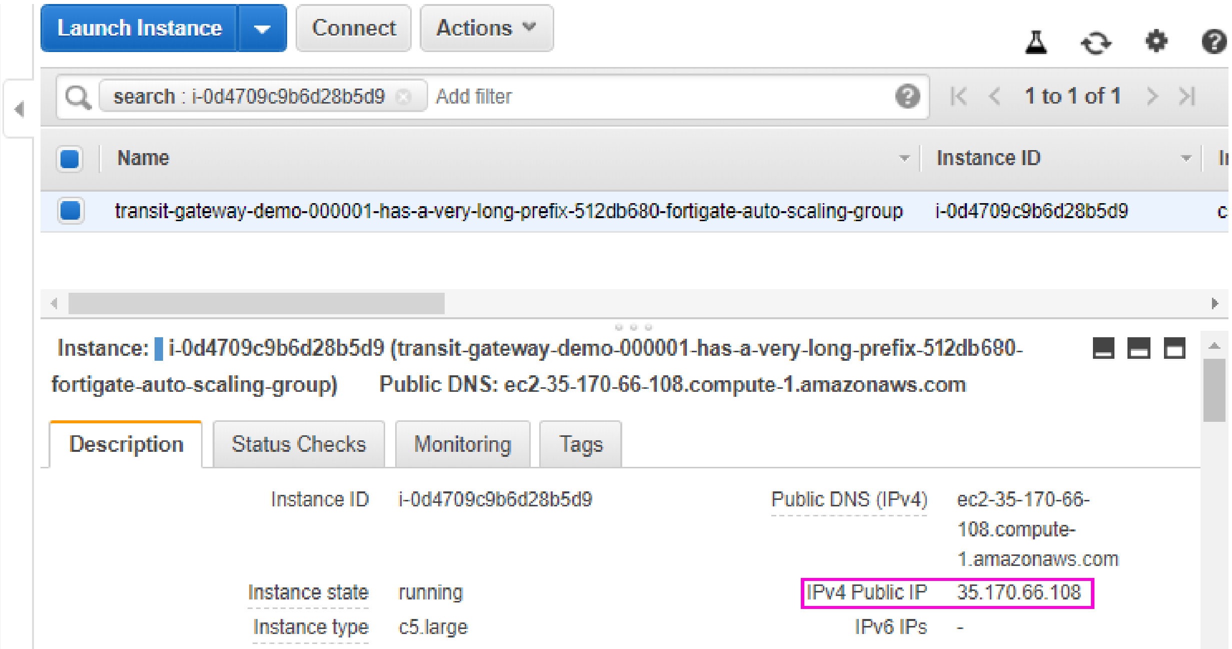
Filter: Any Health Status Any Lifecycle State Filter instances...

1 to 2 of 2 Instances

□	Instance ID	Lifecycle	Launch Configuration / Template
□	i-0b025d772d7534d74	InService	transit-gateway-demo-000001-has-a-very-long-prefix-512db680-fortigate-autoscale-launch-t
□	i-0d4709c9b6d28b5d9	InService	transit-gateway-demo-000001-has-a-very-long-prefix-512db680-fortigate-autoscale-launch-t

3. In the lower pane, select the *Instances* tab and then click the master instance. This is the instance with the *instanceID* you noted in the section To verify the master election: on page 27 or retrieved from the DynamoDB table *<ResourceTagPrefix>-Settings* in the section To obtain the password: on page 31.

4. Make note of the *IPv4 Public IP* in the lower pane.



Name	Instance ID
transit-gateway-demo-000001-has-a-very-long-prefix-512db680-fortigate-auto-scaling-group	i-0d4709c9b6d28b5d9

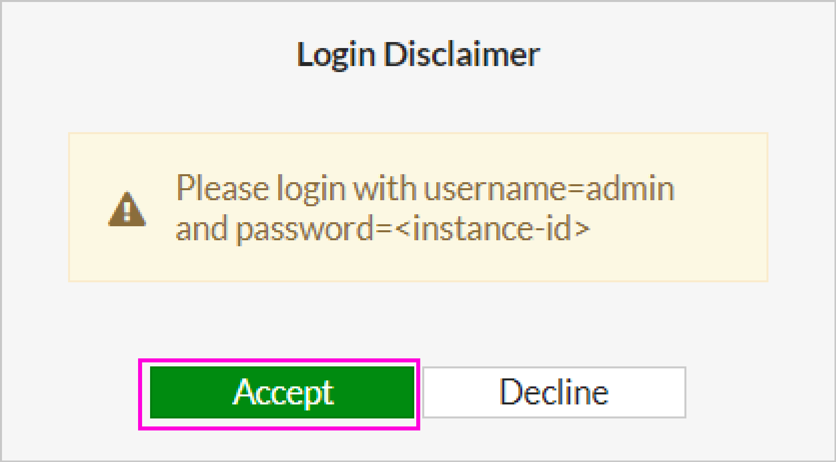
Instance: i-0d4709c9b6d28b5d9 (transit-gateway-demo-000001-has-a-very-long-prefix-512db680-fortigate-auto-scaling-group) Public DNS: ec2-35-170-66-108.compute-1.amazonaws.com

Instance ID	i-0d4709c9b6d28b5d9	Public DNS (IPv4)	ec2-35-170-66-108.compute-1.amazonaws.com
Instance state	running	IPv4 Public IP	35.170.66.108
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 15.

To connect to the master FortiGate-VM instance:

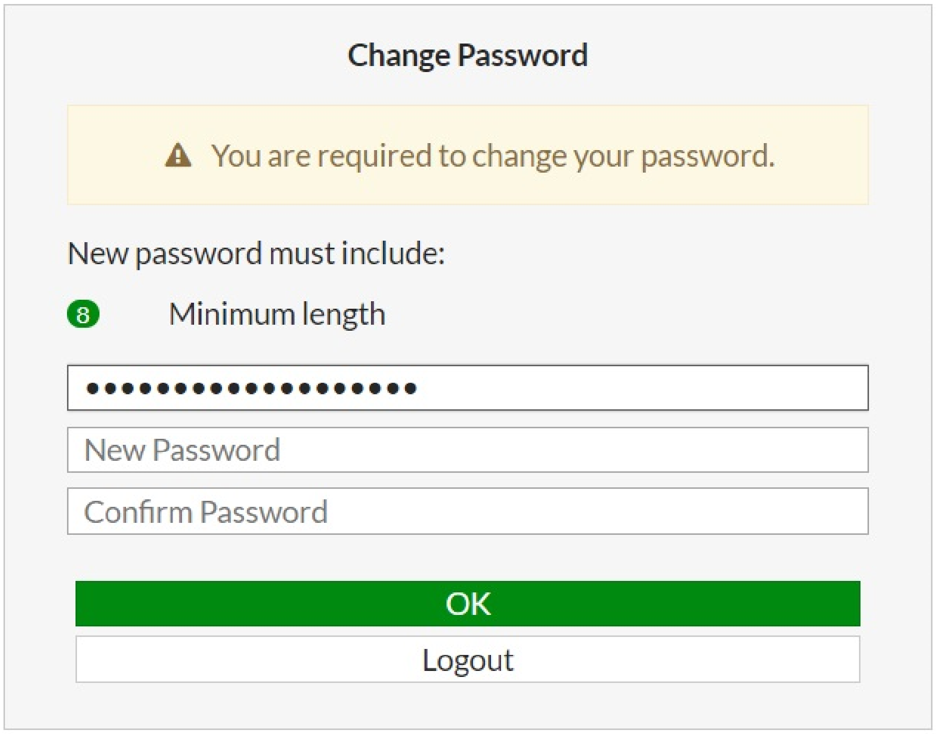
1. Open an HTTPS session in your browser and go to the login URL.
   - Your browser will display a certificate error message. This is normal because the default FortiGate certificate is self-signed and not recognized by browsers. Proceed past this error. At a later time, you can upload a publicly signed 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 noted in the section To verify the master election: on page 27 or retrieved from the DynamoDB table <*ResourceTagPrefix*>*-Settings* in the section To obtain the password: on page 31.
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

●●●●●●●●●●●●●●●●●●●

New Password

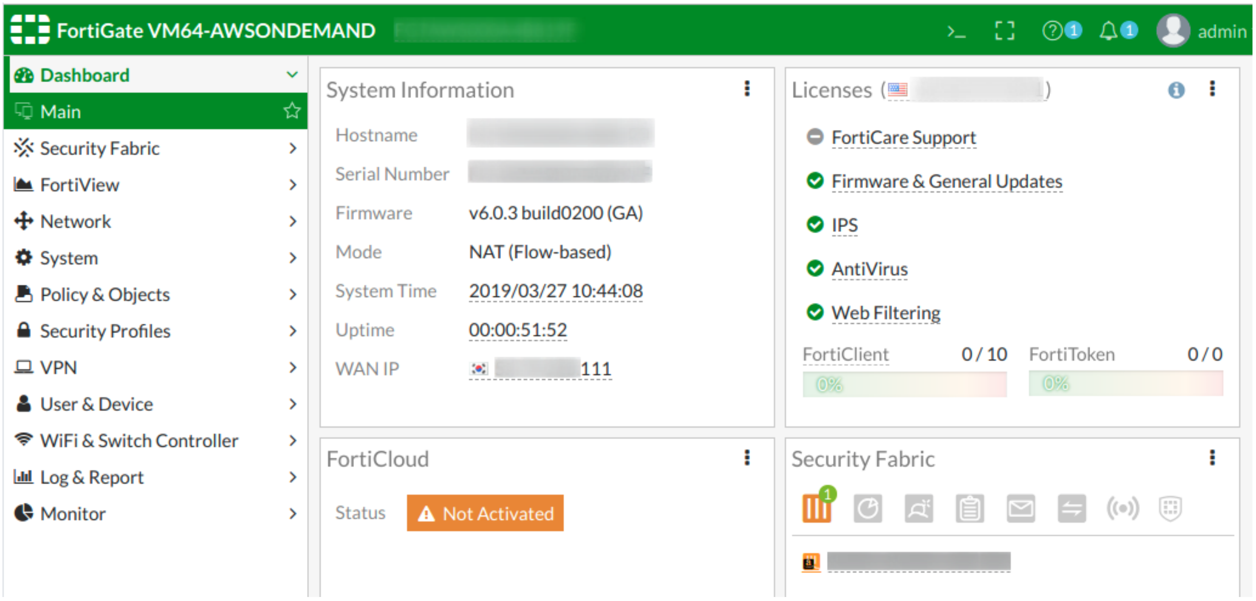
Confirm Password

OK

Logout

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

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



FortiGate VM64-AWSONDEMAND [redacted]

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	FortiToken	0 / 0
0%		0%	

FortiCloud

Status ⚠ Not Activated

Security Fabric

[redacted]

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

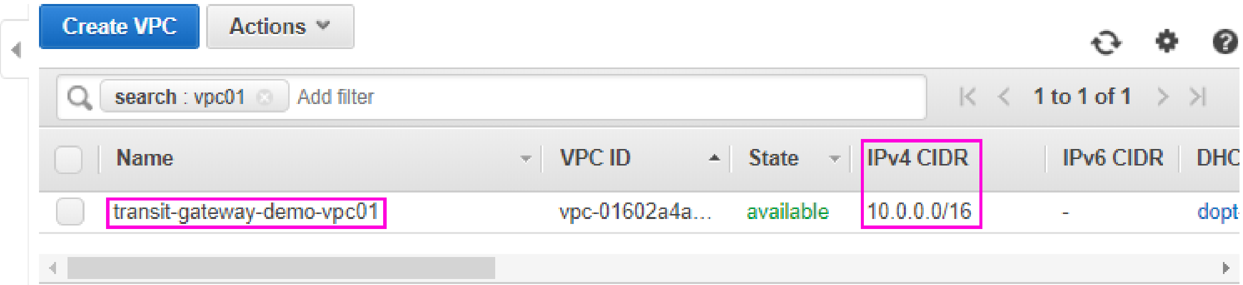
Attaching a VPC to the Transit Gateway

You can attach an existing VPC to the FortiGate Autoscale with Transit Gateway environment by manually creating a Transit Gateway attachment and adding the necessary routes, propagations, and associations:

1. Create a Transit Gateway attachment.
2. Create a route to the Transit Gateway.
3. Create a propagation in the inbound route table.
4. Create an association in the outbound route table.

The CIDR block for the VPC you are attaching must differ from that of the FortiGate Autoscale VPC.

In the instructions that follow, the VPC *transit-gateway-demo-vpc01* with CIDR *10.0.0.0/16* will be attached to the FortiGate Autoscale with Transit Gateway environment.



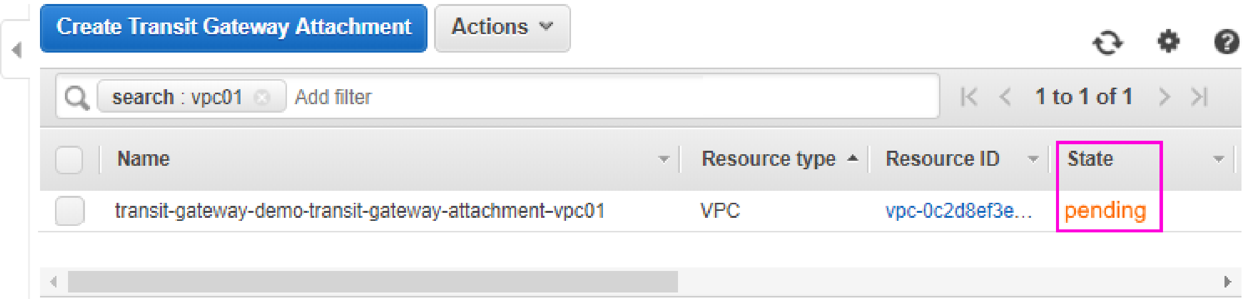
Name	VPC ID	State	IPv4 CIDR	IPv6 CIDR	DHC
transit-gateway-demo-vpc01	vpc-01602a4a...	available	10.0.0.0/16	-	dopt

To create a Transit Gateway attachment:

1. In the left navigation tree, click *Transit Gateways* > *Transit Gateway Attachment*.
2. Click *Create Transit Gateway Attachment*.
3. Specify information as follows:
   a. *Transit Gateway ID*: Select from the dropdown menu
   b. *Attachment type*: VPC
   c. *Attachment name tag:* Enter a tag of your choice
   d. *VPC ID*: Select from the dropdown menu
   e. *Subnet IDs*: This option appears once the *VPC ID* has been selected. Check the AZ check box(es) and choose 1 subnet per AZ.

   For everything else, use the default settings.
4. Click *Create attachment*.

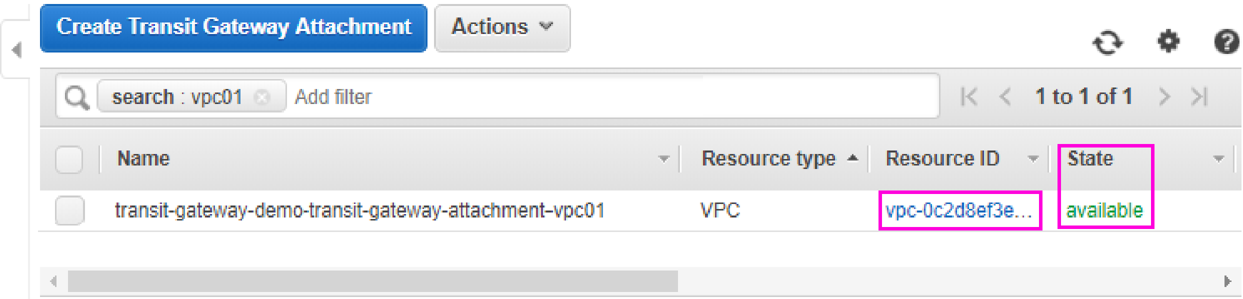
5. Wait for the *State* to change from *pending* to *available*.



Name	Resource type	Resource ID	State
transit-gateway-demo-transit-gateway-attachment-vpc01	VPC	vpc-0c2d8ef3e...	pending

The *Name* is what you specified for the *Attachment name tag*.

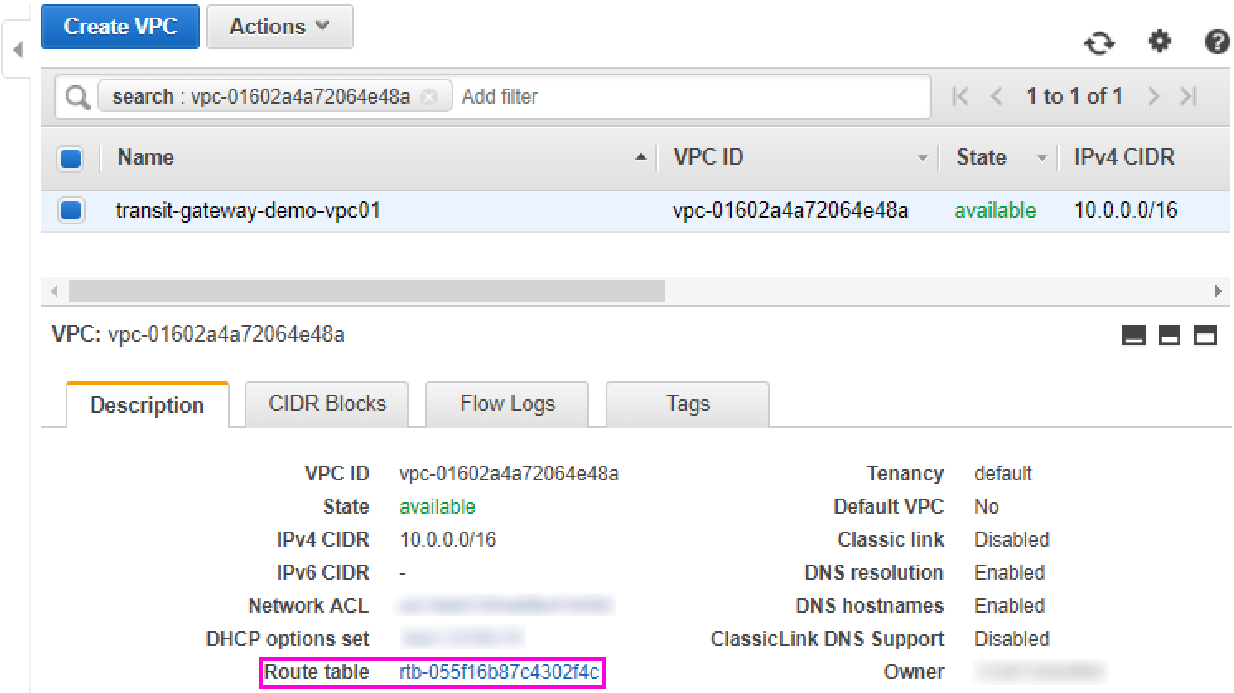
6. When the *State* is *available*, click on the *Resource ID* to go to the VPC.



Name	Resource type	Resource ID	State
transit-gateway-demo-transit-gateway-attachment-vpc01	VPC	vpc-0c2d8ef3e...	available

To create a route to the Transit Gateway:

1. In the VPC, click on the *Route table*.

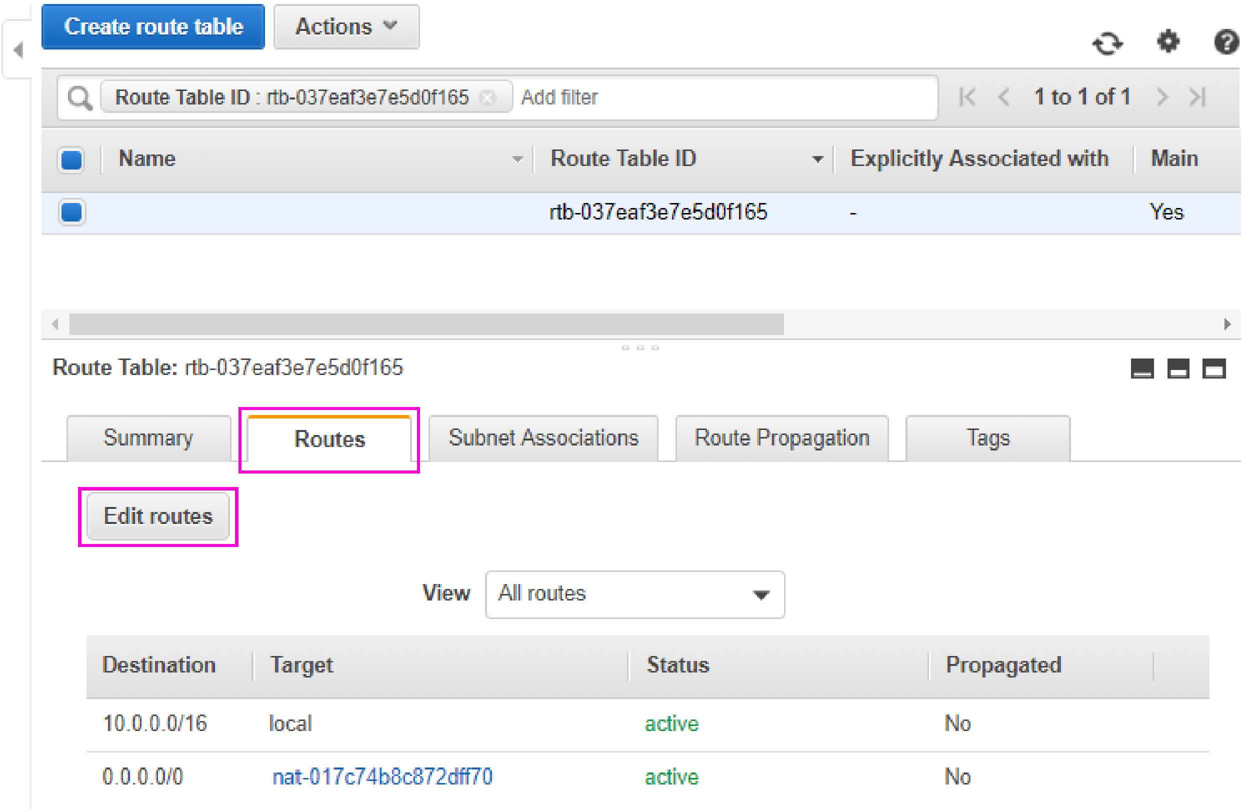


Name	VPC ID	State	IPv4 CIDR
transit-gateway-demo-vpc01	vpc-01602a4a72064e48a	available	10.0.0.0/16

VPC: vpc-01602a4a72064e48a

VPC ID	vpc-01602a4a72064e48a	Tenancy	default
State	available	Default VPC	No
IPv4 CIDR	10.0.0.0/16	Classic link	Disabled
IPv6 CIDR	-	DNS resolution	Enabled
Network ACL	[redacted]	DNS hostnames	Enabled
DHCP options set	[redacted]	ClassicLink DNS Support	Disabled
Route table	rtb-055f16b87c4302f4c	Owner	[redacted]

2. Click the *Routes* tab and then click *Edit routes*.



Create route table | Actions

Route Table ID : rtb-037eaf3e7e5d0f165 | Add filter | 1 to 1 of 1

☐	Name	Route Table ID	Explicitly Associated with	Main
☐		rtb-037eaf3e7e5d0f165	-	Yes

Route Table: rtb-037eaf3e7e5d0f165

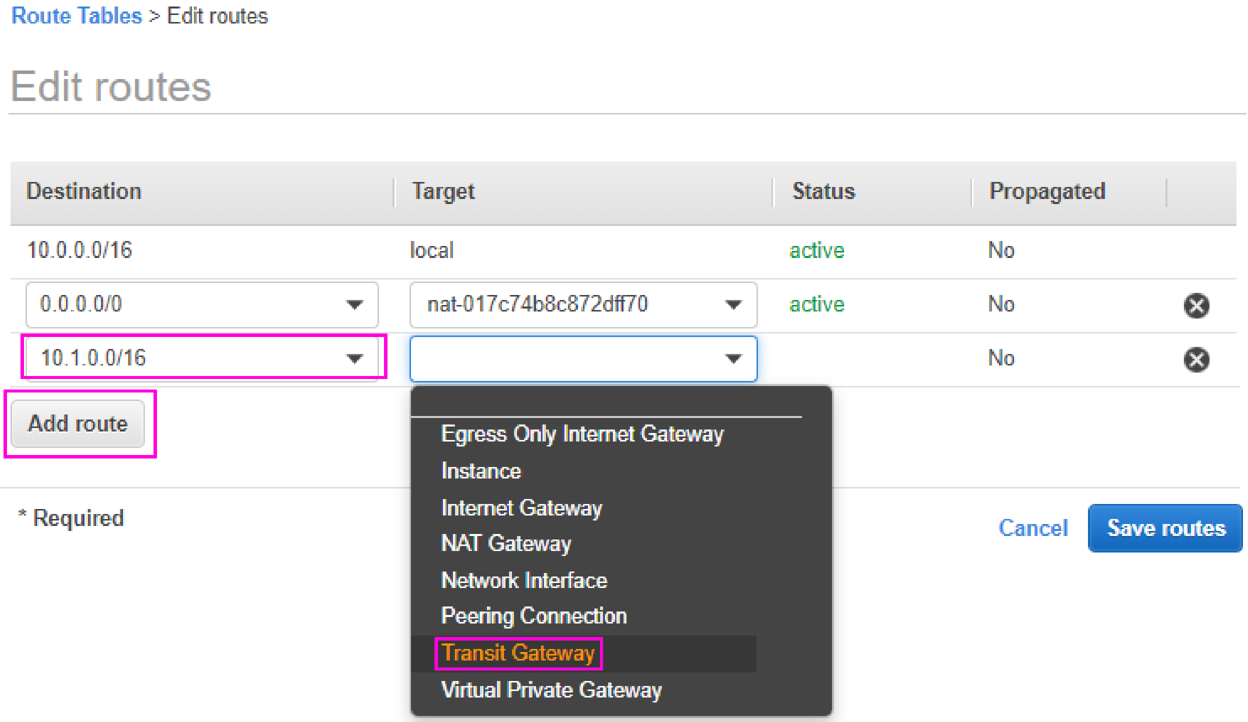
Summary | Routes | Subnet Associations | Route Propagation | Tags

Edit routes

View: All routes

Destination	Target	Status	Propagated
10.0.0.0/16	local	active	No
0.0.0.0/0	nat-017c74b8c872dff70	active	No

3. Click *Add route*and specify the *Destination*, for example, 10.1.0.0/16. Under *Target*, select *Transit Gateway*.



Route Tables > Edit routes

Edit routes

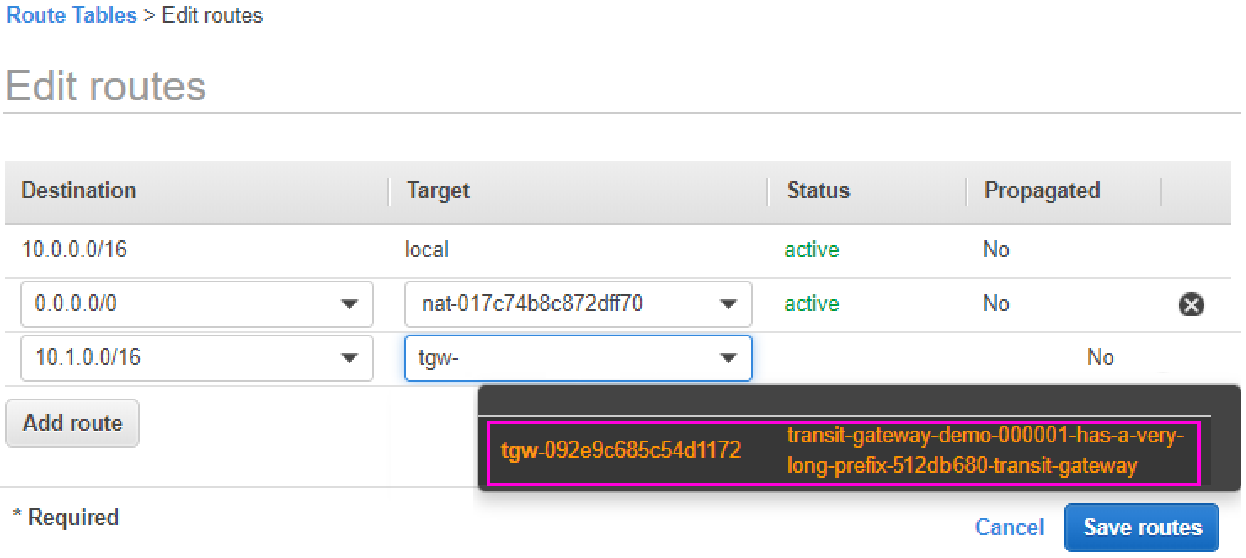
Destination	Target	Status	Propagated
10.0.0.0/16	local	active	No
0.0.0.0/0	nat-017c74b8c872dff70	active	No
10.1.0.0/16			No

Add route

* Required

Cancel | Save routes

4. Then dropdown will change to display available Transit Gateways. Select the one created by the deployment stack and then click *Save routes*.



Route Tables > Edit routes

Edit routes

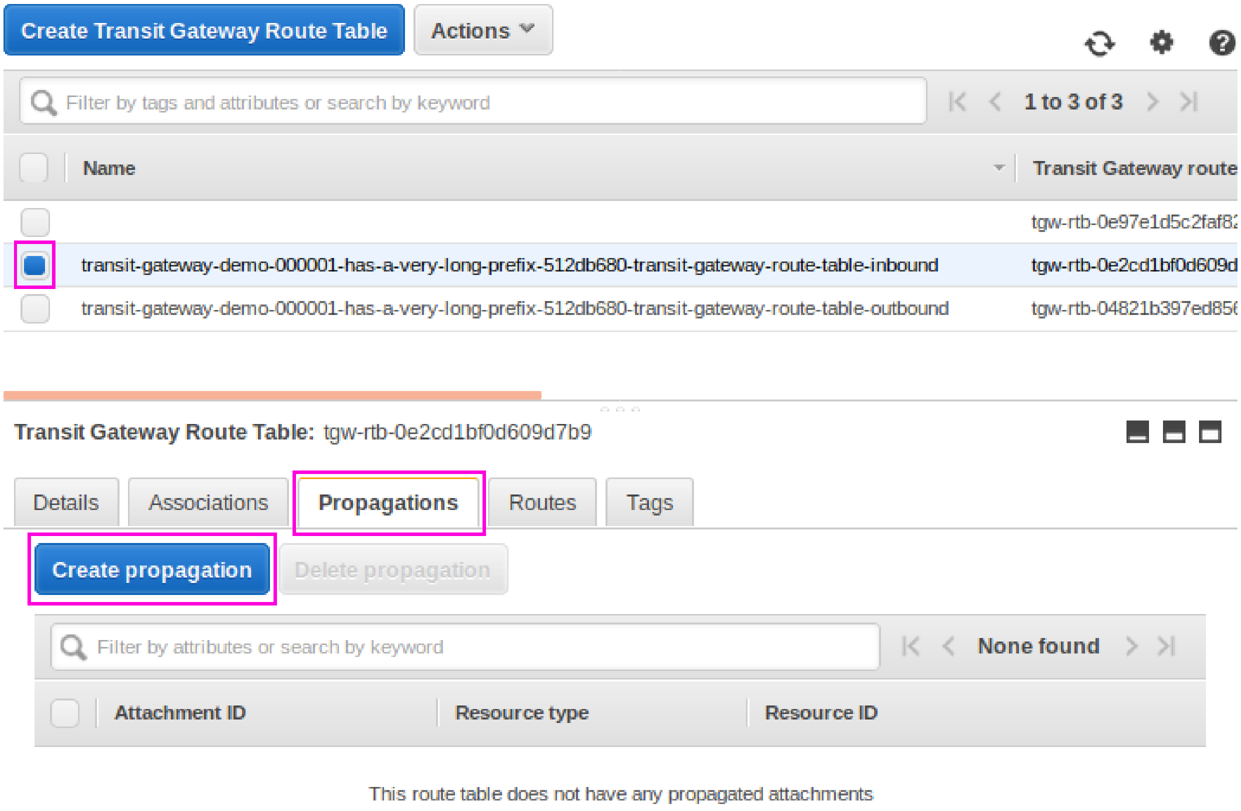
Destination	Target	Status	Propagated
10.0.0.0/16	local	active	No
0.0.0.0/0	nat-017c74b8c872dff70	active	No
10.1.0.0/16	tgw-		No

tgw-092e9c685c54d1172 transit-gateway-demo-000001-has-a-very-long-prefix-512db680-transit-gateway

If you want to route all traffic to the Transit Gateway, you should add a new route for destination 0.0.0.0/0. If this route already exists, simply remove the route and add a new one for the same destination with the target set to the Transit Gateway created by the deployment stack.

To create a propagation in the inbound route table:

1. In the left navigation tree, click *Transit Gateways* > *Transit Gateway Route Tables*.
2. Select the *<ResourceTagPrefix>-transit-gateway-route-table-inbound* route table.



Create Transit Gateway Route Table
Actions
Filter by tags and attributes or search by keyword
1 to 3 of 3
Details
Associations
Propagations
Routes
Tags
Create propagation
Delete propagation
Filter by attributes or search by keyword
None found

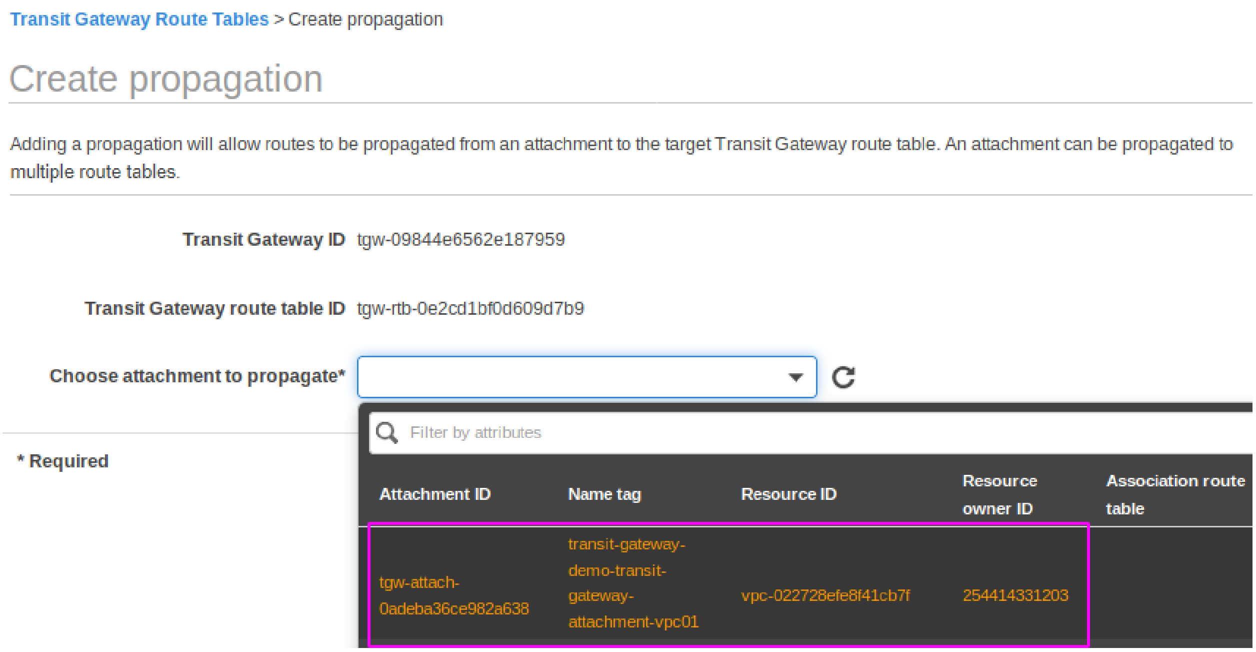
	Name	Transit Gateway route
□		tgw-rtb-0e97e1d5c2faf82
☑	transit-gateway-demo-000001-has-a-very-long-prefix-512db680-transit-gateway-route-table-inbound	tgw-rtb-0e2cd1bf0d609d
□	transit-gateway-demo-000001-has-a-very-long-prefix-512db680-transit-gateway-route-table-outbound	tgw-rtb-04821b397ed85

Transit Gateway Route Table: tgw-rtb-0e2cd1bf0d609d7b9

□	Attachment ID	Resource type	Resource ID

This route table does not have any propagated attachments

3. Click the *Propagations* tab and then click *Create propagation*.
4. From *Choose attachment to propagate*, select the attachment created in the section To create a Transit Gateway attachment: on page 35.



Transit Gateway Route Tables > Create propagation

Create propagation

Adding a propagation will allow routes to be propagated from an attachment to the target Transit Gateway route table. An attachment can be propagated to multiple route tables.

Transit Gateway ID tgw-09844e6562e187959

Transit Gateway route table ID tgw-rtb-0e2cd1bf0d609d7b9

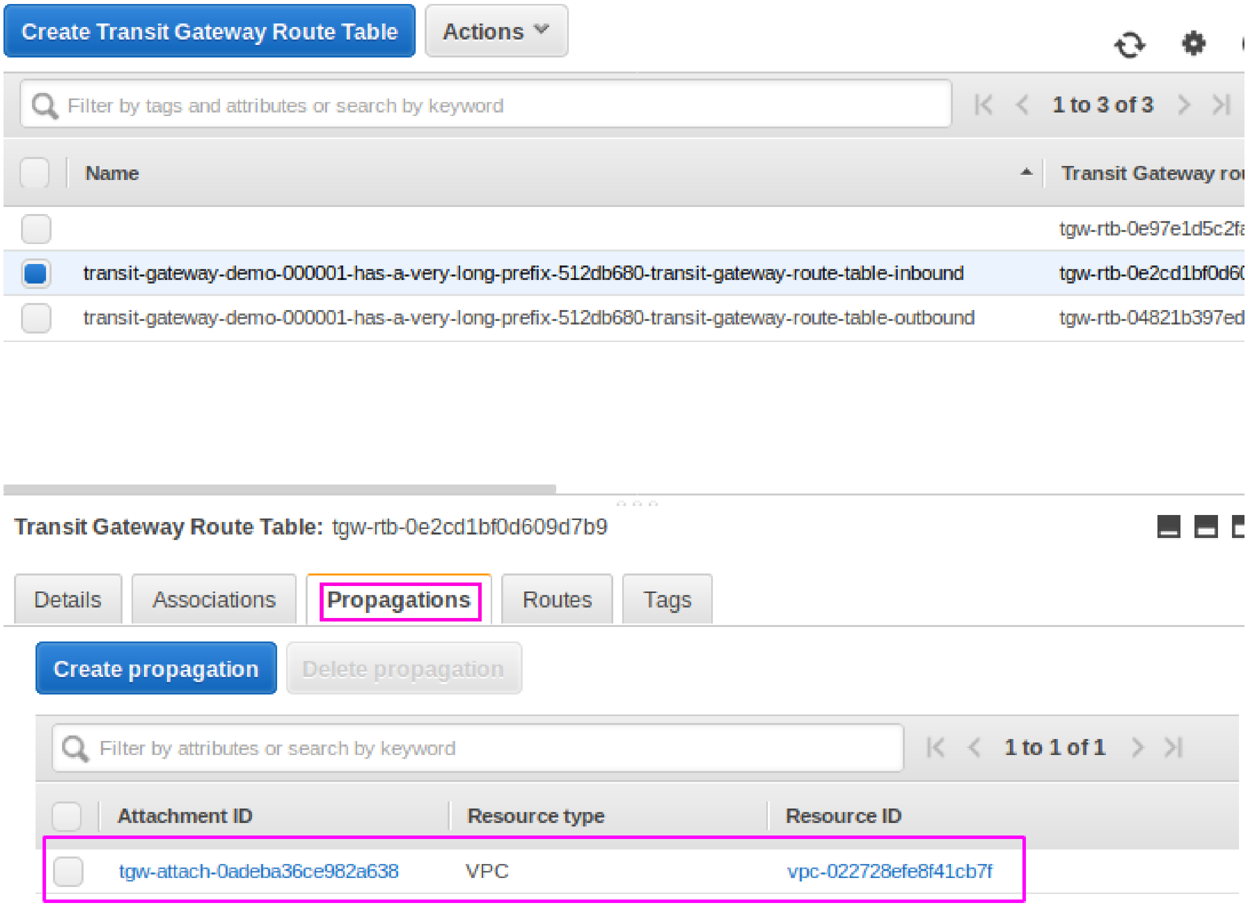
Choose attachment to propagate*

Filter by attributes

Attachment ID	Name tag	Resource ID	Resource owner ID	Association route table
tgw-attach-0adeba36ce982a638	transit-gateway-demo-transit-gateway-attachment-vpc01	vpc-022728efe8f41cb7f	254414331203	

* Required

5. Click *Create propagation* and then click *Close*.
6. The new propagation with *Resource type* VPC is now listed on the *Propagations* tab.



Filter by tags and attributes or search by keyword

1 to 3 of 3

	Name	Transit Gateway ro
□		tgw-rtb-0e97e1d5c2fa
■	transit-gateway-demo-000001-has-a-very-long-prefix-512db680-transit-gateway-route-table-inbound	tgw-rtb-0e2cd1bf0d60
□	transit-gateway-demo-000001-has-a-very-long-prefix-512db680-transit-gateway-route-table-outbound	tgw-rtb-04821b397ed

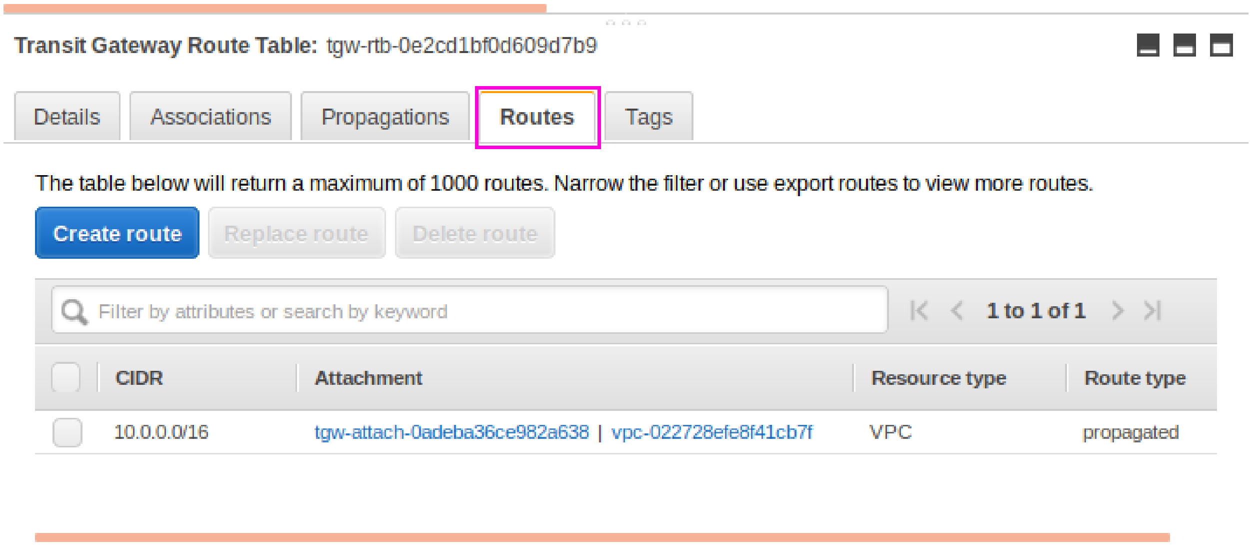
Transit Gateway Route Table: tgw-rtb-0e2cd1bf0d609d7b9

Filter by attributes or search by keyword

1 to 1 of 1

	Attachment ID	Resource type	Resource ID
□	tgw-attach-0adeba36ce982a638	VPC	vpc-022728efe8f41cb7f

7. Click on the *Routes* tab to see that the route for your VPC has been automatically propagated.



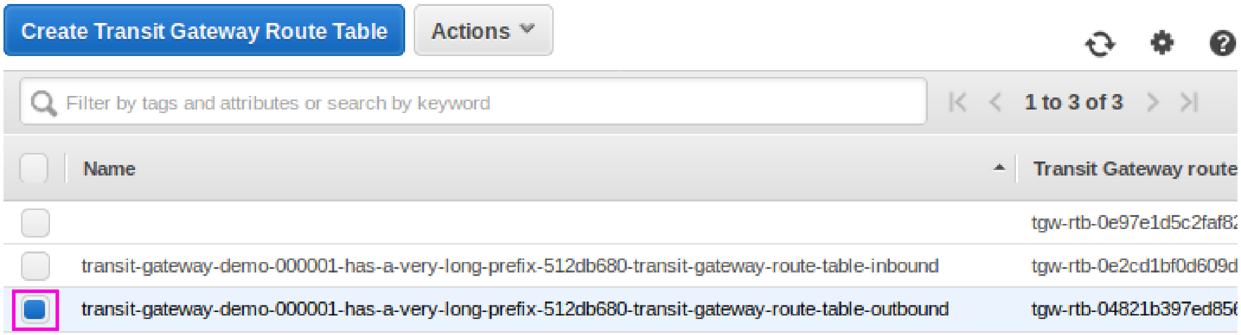
Transit Gateway Route Table: tgw-rtb-0e2cd1bf0d609d7b9

The table below will return a maximum of 1000 routes. Narrow the filter or use export routes to view more routes.

□	CIDR	Attachment	Resource type	Route type
□	10.0.0.0/16	tgw-attach-0adeba36ce982a638 | vpc-022728efe8f41cb7f	VPC	propagated

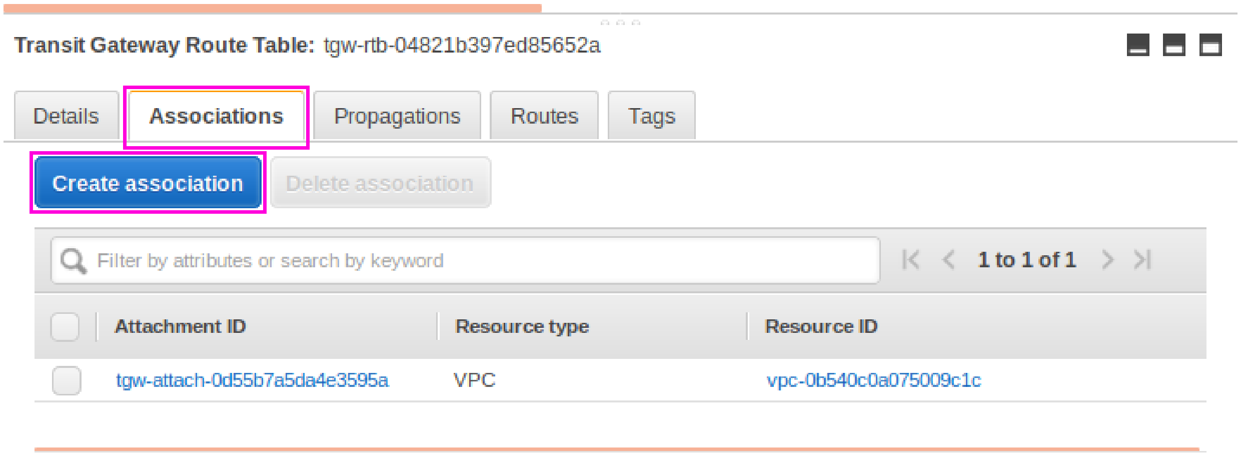
To create an association in the outbound route table:

1. In the left navigation tree, click *Transit Gateways > Transit Gateway Route Tables*.
2. Select the *<ResourceTagPrefix>-transit-gateway-route-table-outbound* route table.



Create Transit Gateway Route Table
Actions
Filter by tags and attributes or search by keyword
1 to 3 of 3

□	Name	Transit Gateway route
□		tgw-rtb-0e97e1d5c2faf82
□	transit-gateway-demo-000001-has-a-very-long-prefix-512db680-transit-gateway-route-table-inbound	tgw-rtb-0e2cd1bf0d609d
☑	transit-gateway-demo-000001-has-a-very-long-prefix-512db680-transit-gateway-route-table-outbound	tgw-rtb-04821b397ed85(

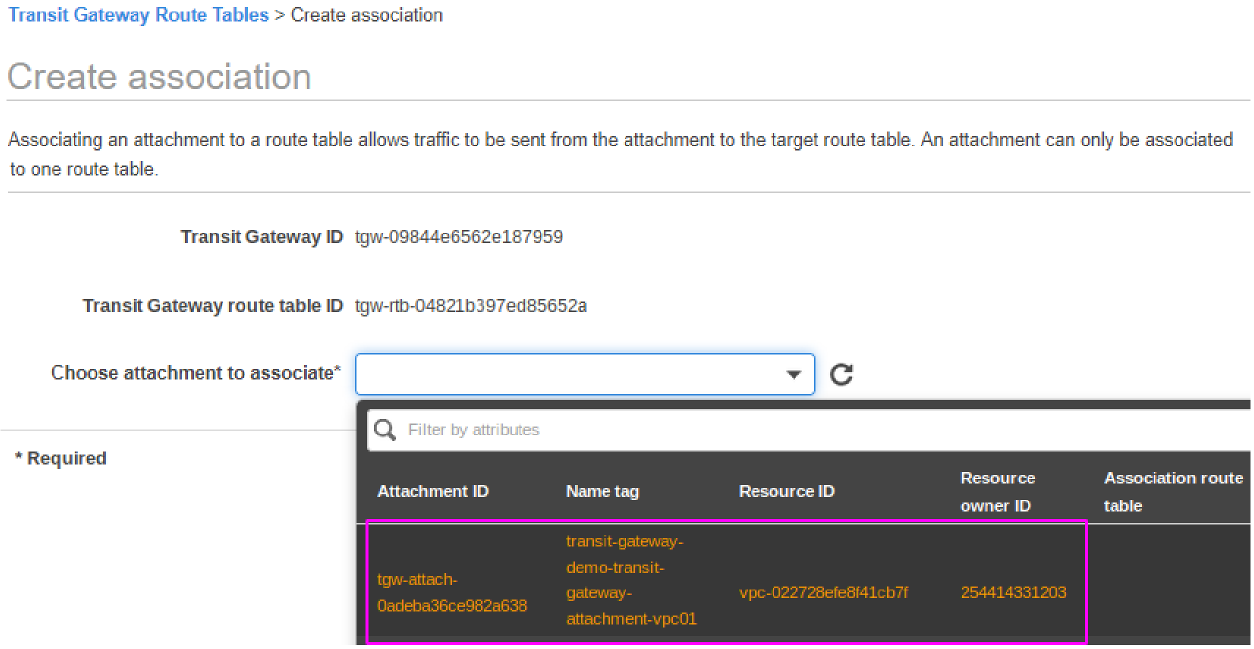


Transit Gateway Route Table: tgw-rtb-04821b397ed85652a

□	Attachment ID	Resource type	Resource ID
□	tgw-attach-0d55b7a5da4e3595a	VPC	vpc-0b540c0a075009c1c

3. Click the *Associations* tab and then click *Create association*.

4. From *Choose attachment to associate*, select the attachment created in the section To create a Transit Gateway attachment: on page 35.



Create association

Associating an attachment to a route table allows traffic to be sent from the attachment to the target route table. An attachment can only be associated to one route table.

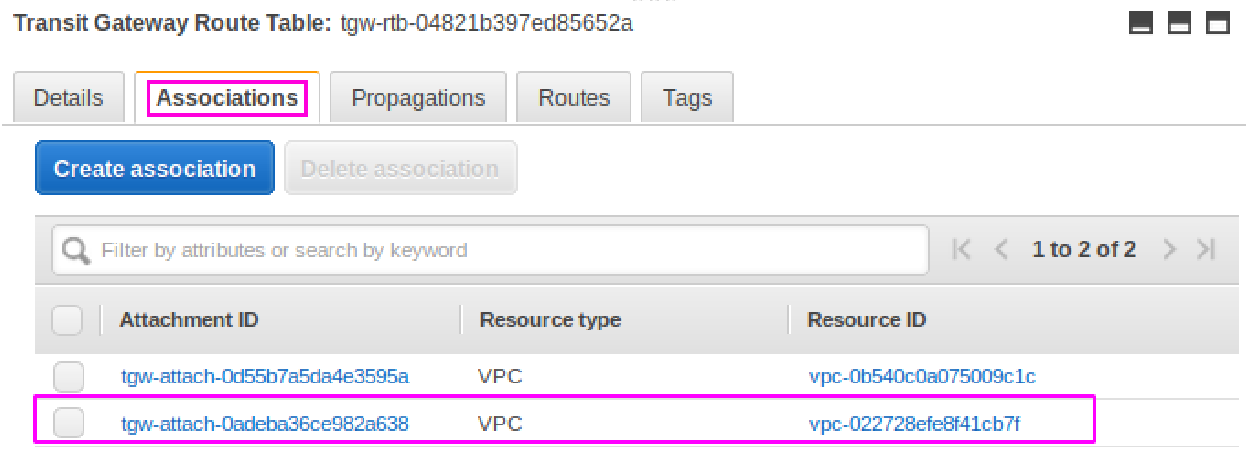
Transit Gateway ID tgw-09844e6562e187959

Transit Gateway route table ID tgw-rtb-04821b397ed85652a

Choose attachment to associate*

Attachment ID	Name tag	Resource ID	Resource owner ID	Association route table
tgw-attach-0adeba36ce982a638	transit-gateway-demo-transit-gateway-attachment-vpc01	vpc-022728efe8f41cb7f	254414331203	

5. Click *Create association* and then click *Close*.
6. The new association with *Resource type* VPC is now listed on the *Associations* tab.



Transit Gateway Route Table: tgw-rtb-04821b397ed85652a

	Attachment ID	Resource type	Resource ID
□	tgw-attach-0d55b7a5da4e3595a	VPC	vpc-0b540c0a075009c1c
□	tgw-attach-0adeba36ce982a638	VPC	vpc-022728efe8f41cb7f

The VPC is now connected to the FortiGate Autoscale Transit Gateway. For a technical view of attaching VPCs to the FortiGate Autoscale Transit Gateway, please refer to the architectural diagram Route propagation on page 60.

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 only item in the table.

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

For details on locating the master record, refer to the master election portion of the section Verifying the deployment on page 26.

Appendix

FortiGate Autoscale for AWS features

Major components

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

Auto Scaling Handler environment variables

Variable name	Description
RESOURCE_TAG_PREFIX	Descriptions of these variables are identical to those of the related parameters which are described in the section Resource tagging configuration on page 14. • RESOURCE_TAG_PREFIX: *Resource tag prefix* • CUSTOM_ID: *Resource name prefix*
CUSTOM_ID	
AUTO_SCALING_GROUP_NAME	The Auto Scaling group name.
API_GATEWAY_NAME	The API Gateway name generated during the deployment.
API_GATEWAY_STAGE_NAME	The API Gateway stage. It is always set to *prod*.
API_GATEWAY_RESOURCE_NAME	The API Gateway resource. It is always set to *complete*.
UNIQUE_ID	This is a deprecated variable. It should remain as an empty string.
EXPIRE_LIFECYCLE_ENTRY	The value of the CFT parameter *Instance lifecycle timeout* which is described in the section FortiGate-VM Auto Scaling group configuration on page 16.
FORTIGATE_PSKSECRET	Descriptions of these variables are identical to those of the related parameters which are described in the section FortiGate-VM configuration on page 15. • FORTIGATE_PSKSECRET: *FortiGate PSK secret* • FORTIGATE_ADMIN_PORT: *Admin port*
FORTIGATE_ADMIN_PORT	
FORTIGATE_INTERNAL_ELB_DNS	This is a deprecated variable. It should remain as an empty string.
FORTIGATE_TRAFFIC_PORT	This is reserved for other features. It should remain empty.
HEART_BEAT_INTERVAL	Descriptions of these variables are identical to those of the related parameters which are described in the section Failover configuration on page 17. • HEART_BEAT_INTERVAL: *Heart beat interval* • HEART_BEAT_LOSS_COUNT: *Heart beat loss count*
HEART_BEAT_LOSS_COUNT	
STACK_ASSETS_S3_BUCKET_NAME	Descriptions of these variables are identical to those of the related parameters which are described in the section Deployment resources configuration on page 17. • STACK_ASSETS_S3_BUCKET_NAME: *S3 bucket name* • STACK_ASSETS_S3_KEY_PREFIX: *S3 key prefix*
STACK_ASSETS_S3_KEY_PREFIX	
VPC_ID	The VPC ID of the FortiGate Autoscale VPC created in this CFT deployment stack.
REQUIRED_CONFIG_SET	This is a comma delimited string for additional configsets to load. (Reserved for future use.)

Variable name	Description
FORTIGATE_SYNC_INTERFACE	The FortiGate-VM sync interface. This should always be set to *port1*.
SCALING_GROUP_NAME_PAYG	This is reserved for other features. Do not modify its value.
SCALING_GROUP_NAME_BYOL	This is reserved for other features. Do not modify its value.
MASTER_SCALING_GROUP_NAME	This is reserved for other features. Do not modify its value.
ENABLE_SECOND_NIC	This is reserved for other features. Do not modify its value.
ENABLE_TGW_VPN	This is the Transit Gateway feature toggle. It should always be set to *true*.
TGW_ID	The ID of the Transit Gateway used in this deployment.

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

```
FortiGate-VM64-AWSON~AND # diag debug cloudinit show
 >> Checking metadata source aws
 >> AWS curl header: Fos-instance-id: <masked_instance_id>
 >> AWS trying to get config script from https://<masked_api_id>/prod/fgt-asg-handler
 >> AWS download config script successfully
 >> Run config script
 >> Finish running script
 >> FortiGate-VM64-AWSON~AND $ config system dns
 >> FortiGate-VM64-AWSON~AND (dns) $ unset primary
 >> FortiGate-VM64-AWSON~AND (dns) $ unset secondary
 >> FortiGate-VM64-AWSON~AND (dns) $ end
 >> FortiGate-VM64-AWSON~AND $ config system global
 >> FortiGate-VM64-AWSON~AND (global) $ set admin-sport 8443
 >> FortiGate-VM64-AWSON~AND (global) $ end
 >> FortiGate-VM64-AWSON~AND $ config system auto-scale
 >> FortiGate-VM64-AWSON~AND (auto-scale) $ set status enable
 >> FortiGate-VM64-AWSON~AND (auto-scale) $ set sync-interface "port1"
 >> FortiGate-VM64-AWSON~AND (auto-scale) $ set hb-interval 30
 >> FortiGate-VM64-AWSON~AND (auto-scale) $ set role master
 >> FortiGate-VM64-AWSON~AND (auto-scale) $ set callback-url https://<masked_api_id>/prod/fgt-
      asg-handler
 >> FortiGate-VM64-AWSON~AND (auto-scale) $ set psksecret <masked_psksecret>
 >> FortiGate-VM64-AWSON~AND (auto-scale) $ end
 >> FortiGate-VM64-AWSON~AND $ config system vdom-exception
 >> FortiGate-VM64-AWSON~AND (vdom-exception) $ edit 0
 >> FortiGate-VM64-AWSON~AND (0) $ set object vpn.ipsec.phase1-interface
 >> FortiGate-VM64-AWSON~AND (0) $ next
 >> FortiGate-VM64-AWSON~AND (vdom-exception) $ edit 0
 >> FortiGate-VM64-AWSON~AND (0) $ set object vpn.ipsec.phase2-interface
 >> FortiGate-VM64-AWSON~AND (0) $ next
 >> FortiGate-VM64-AWSON~AND (vdom-exception) $ edit 0
 >> FortiGate-VM64-AWSON~AND (0) $ set object router.bgp
 >> FortiGate-VM64-AWSON~AND (0) $ next
 >> FortiGate-VM64-AWSON~AND (vdom-exception) $ edit 0
 >> FortiGate-VM64-AWSON~AND (0) $ set object router.route-map
 >> FortiGate-VM64-AWSON~AND (0) $ next
 >> FortiGate-VM64-AWSON~AND (vdom-exception) $ edit 0
 >> FortiGate-VM64-AWSON~AND (0) $ set object router.prefix-list
 >> FortiGate-VM64-AWSON~AND (0) $ next
 >> FortiGate-VM64-AWSON~AND (vdom-exception) $ edit 0
 >> FortiGate-VM64-AWSON~AND (0) $ set object firewall.ippool
 >> FortiGate-VM64-AWSON~AND (0) $ next
 >> FortiGate-VM64-AWSON~AND (vdom-exception) $ end
 >> FortiGate-VM64-AWSON~AND $
 >> FortiGate-VM64-AWSON~AND $ config router prefix-list
 >> FortiGate-VM64-AWSON~AND (prefix-list) $ edit "pflist-default-route"
 >> FortiGate-VM64-AWSON~AND (pflist-default-route) $ config rule
 >> FortiGate-VM64-AWSON~AND (rule) $ edit 1
 >> FortiGate-VM64-AWSON~AND (1) $ set prefix 0.0.0.0 0.0.0.0
 >> FortiGate-VM64-AWSON~AND (1) $ unset ge
 >> FortiGate-VM64-AWSON~AND (1) $ unset le
 >> FortiGate-VM64-AWSON~AND (1) $ next
 >> FortiGate-VM64-AWSON~AND (rule) $ end
 >> FortiGate-VM64-AWSON~AND (pflist-default-route) $ next
 >> FortiGate-VM64-AWSON~AND (prefix-list) $ edit "pflist-port1"
 >> FortiGate-VM64-AWSON~AND (pflist-port1) $ config rule
 >> FortiGate-VM64-AWSON~AND (rule) $ edit 1
 >> FortiGate-VM64-AWSON~AND (1) $ set prefix 192.168.2.150 255.255.255.255
 >> FortiGate-VM64-AWSON~AND (1) $ unset ge
 >> FortiGate-VM64-AWSON~AND (1) $ unset le
 >> FortiGate-VM64-AWSON~AND (1) $ next
 >> FortiGate-VM64-AWSON~AND (rule) $ end
 >> FortiGate-VM64-AWSON~AND (pflist-port1) $ next
 >> FortiGate-VM64-AWSON~AND (prefix-list) $ end
 >> FortiGate-VM64-AWSON~AND $
 >> FortiGate-VM64-AWSON~AND $ config router route-map
 >> FortiGate-VM64-AWSON~AND (route-map) $ edit "rmap-outbound"
 >> FortiGate-VM64-AWSON~AND (rmap-outbound) $ config rule
 >> FortiGate-VM64-AWSON~AND (rule) $ edit 1
 >> FortiGate-VM64-AWSON~AND (1) $ set match-ip-address "pflist-default-route"
 >> FortiGate-VM64-AWSON~AND (1) $ next
 >> FortiGate-VM64-AWSON~AND (rule) $ edit 2
 >> FortiGate-VM64-AWSON~AND (2) $ set match-ip-address "pflist-port1"
 >> FortiGate-VM64-AWSON~AND (2) $ next
 >> FortiGate-VM64-AWSON~AND (rule) $ end
 >> FortiGate-VM64-AWSON~AND (rmap-outbound) $ next
 >> FortiGate-VM64-AWSON~AND (route-map) $ end
 >> FortiGate-VM64-AWSON~AND $
 >> FortiGate-VM64-AWSON~AND $ config vpn ipsec phase1-interface
 >> FortiGate-VM64-AWSON~AND (phase1-interface) $ edit "tgw-vpn-1"
 >> FortiGate-VM64-AWSON~AND (tgw-vpn-1) $ set interface "port1"
 >> FortiGate-VM64-AWSON~AND (tgw-vpn-1) $ set local-gw 192.168.2.150
 >> FortiGate-VM64-AWSON~AND (tgw-vpn-1) $ set dhgrp 2
 >> FortiGate-VM64-AWSON~AND (tgw-vpn-1) $ set proposal aes128-sha1
 >> FortiGate-VM64-AWSON~AND (tgw-vpn-1) $ set keylife 28800
 >> FortiGate-VM64-AWSON~AND (tgw-vpn-1) $ set net-device enable
 >> FortiGate-VM64-AWSON~AND (tgw-vpn-1) $ set remote-gw 3.219.71.235
 >> FortiGate-VM64-AWSON~AND (tgw-vpn-1) $ set psksecret <masked_psksecret>
 >> FortiGate-VM64-AWSON~AND (tgw-vpn-1) $ set dpd-retryinterval 10
 >> FortiGate-VM64-AWSON~AND (tgw-vpn-1) $ next
 >> FortiGate-VM64-AWSON~AND (phase1-interface) $ end
 >> FortiGate-VM64-AWSON~AND $
 >> FortiGate-VM64-AWSON~AND $ config vpn ipsec phase2-interface
 >> FortiGate-VM64-AWSON~AND (phase2-interface) $ edit "tgw-vpn-1"
 >> FortiGate-VM64-AWSON~AND (tgw-vpn-1) $ set phase1name "tgw-vpn-1"
 >> FortiGate-VM64-AWSON~AND (tgw-vpn-1) $ set proposal aes128-sha1
 >> FortiGate-VM64-AWSON~AND (tgw-vpn-1) $ set dhgrp 2
 >> FortiGate-VM64-AWSON~AND (tgw-vpn-1) $ set keylifeseconds 3600
 >> FortiGate-VM64-AWSON~AND (tgw-vpn-1) $ next
 >> FortiGate-VM64-AWSON~AND (phase2-interface) $ end
 >> FortiGate-VM64-AWSON~AND $
 >> FortiGate-VM64-AWSON~AND $ config system interface
 >> FortiGate-VM64-AWSON~AND (interface) $ edit "tgw-vpn-1"
 >> FortiGate-VM64-AWSON~AND (tgw-vpn-1) $ set interface "port1"
 >> FortiGate-VM64-AWSON~AND (tgw-vpn-1) $ set ip 169.254.47.226 255.255.255.255
 >> FortiGate-VM64-AWSON~AND (tgw-vpn-1) $ set allowaccess ping
 >> FortiGate-VM64-AWSON~AND (tgw-vpn-1) $ set type tunnel
 >> FortiGate-VM64-AWSON~AND (tgw-vpn-1) $ set tcp-mss 1379
 >> FortiGate-VM64-AWSON~AND (tgw-vpn-1) $ set remote-ip 169.254.47.225 255.255.255.252
 >> FortiGate-VM64-AWSON~AND (tgw-vpn-1) $ next
 >> FortiGate-VM64-AWSON~AND (interface) $ end
 >> FortiGate-VM64-AWSON~AND $
 >> FortiGate-VM64-AWSON~AND $ config router bgp
 >> FortiGate-VM64-AWSON~AND (bgp) $ set as 65000
 >> FortiGate-VM64-AWSON~AND (bgp) $ set router-id 192.168.2.150
 >> FortiGate-VM64-AWSON~AND (bgp) $ set ebgp-multipath enable
 >> FortiGate-VM64-AWSON~AND (bgp) $ set network-import-check disable
 >> FortiGate-VM64-AWSON~AND (bgp) $ config neighbor
 >> FortiGate-VM64-AWSON~AND (neighbor) $ edit 169.254.47.225
 >> FortiGate-VM64-AWSON~AND (169.254.47.225) $ set capability-default-originate enable
 >> FortiGate-VM64-AWSON~AND (169.254.47.225) $ set link-down-failover enable
 >> FortiGate-VM64-AWSON~AND (169.254.47.225) $ set description "vpn-02b56c99935bfcbea-1"
 >> FortiGate-VM64-AWSON~AND (169.254.47.225) $ set remote-as 64512
 >> FortiGate-VM64-AWSON~AND (169.254.47.225) $ set route-map-out "rmap-outbound"
 >> FortiGate-VM64-AWSON~AND (169.254.47.225) $ next
 >> FortiGate-VM64-AWSON~AND (neighbor) $ end
 >> FortiGate-VM64-AWSON~AND (bgp) $ config network
 >> FortiGate-VM64-AWSON~AND (network) $ edit 1
 >> FortiGate-VM64-AWSON~AND (1) $ set prefix 192.168.2.150 255.255.255.255
 >> FortiGate-VM64-AWSON~AND (1) $ next
 >> FortiGate-VM64-AWSON~AND (network) $ end
 >> FortiGate-VM64-AWSON~AND (bgp) $ end
 >> FortiGate-VM64-AWSON~AND $
 >> FortiGate-VM64-AWSON~AND $ config vpn ipsec phase1-interface
 >> FortiGate-VM64-AWSON~AND (phase1-interface) $ edit "tgw-vpn-2"
 >> FortiGate-VM64-AWSON~AND (tgw-vpn-2) $ set interface "port1"
 >> FortiGate-VM64-AWSON~AND (tgw-vpn-2) $ set local-gw 192.168.2.150
 >> FortiGate-VM64-AWSON~AND (tgw-vpn-2) $ set dhgrp 2
 >> FortiGate-VM64-AWSON~AND (tgw-vpn-2) $ set proposal aes128-sha1
 >> FortiGate-VM64-AWSON~AND (tgw-vpn-2) $ set keylife 28800
 >> FortiGate-VM64-AWSON~AND (tgw-vpn-2) $ set net-device enable
 >> FortiGate-VM64-AWSON~AND (tgw-vpn-2) $ set remote-gw 34.197.152.22
 >> FortiGate-VM64-AWSON~AND (tgw-vpn-2) $ set psksecret <masked_psksecret>
 >> FortiGate-VM64-AWSON~AND (tgw-vpn-2) $ set dpd-retryinterval 10
 >> FortiGate-VM64-AWSON~AND (tgw-vpn-2) $ next
 >> FortiGate-VM64-AWSON~AND (phase1-interface) $ end
 >> FortiGate-VM64-AWSON~AND $
 >> FortiGate-VM64-AWSON~AND $ config vpn ipsec phase2-interface
 >> FortiGate-VM64-AWSON~AND (phase2-interface) $ edit "tgw-vpn-2"
 >> FortiGate-VM64-AWSON~AND (tgw-vpn-2) $ set phase1name "tgw-vpn-2"
 >> FortiGate-VM64-AWSON~AND (tgw-vpn-2) $ set proposal aes128-sha1
 >> FortiGate-VM64-AWSON~AND (tgw-vpn-2) $ set dhgrp 2
 >> FortiGate-VM64-AWSON~AND (tgw-vpn-2) $ set keylifeseconds 3600
 >> FortiGate-VM64-AWSON~AND (tgw-vpn-2) $ next
 >> FortiGate-VM64-AWSON~AND (phase2-interface) $ end
 >> FortiGate-VM64-AWSON~AND $
 >> FortiGate-VM64-AWSON~AND $ config system interface
 >> FortiGate-VM64-AWSON~AND (interface) $ edit "tgw-vpn-2"
 >> FortiGate-VM64-AWSON~AND (tgw-vpn-2) $ set interface "port1"
 >> FortiGate-VM64-AWSON~AND (tgw-vpn-2) $ set ip 169.254.45.90 255.255.255.255
 >> FortiGate-VM64-AWSON~AND (tgw-vpn-2) $ set allowaccess ping
 >> FortiGate-VM64-AWSON~AND (tgw-vpn-2) $ set type tunnel
 >> FortiGate-VM64-AWSON~AND (tgw-vpn-2) $ set tcp-mss 1379
 >> FortiGate-VM64-AWSON~AND (tgw-vpn-2) $ set remote-ip 169.254.45.89 255.255.255.252
 >> FortiGate-VM64-AWSON~AND (tgw-vpn-2) $ next
 >> FortiGate-VM64-AWSON~AND (interface) $ end
 >> FortiGate-VM64-AWSON~AND $
 >> FortiGate-VM64-AWSON~AND $ config router bgp
 >> FortiGate-VM64-AWSON~AND (bgp) $ set as 65000
 >> FortiGate-VM64-AWSON~AND (bgp) $ set router-id 192.168.2.150
 >> FortiGate-VM64-AWSON~AND (bgp) $ set ebgp-multipath enable
 >> FortiGate-VM64-AWSON~AND (bgp) $ set network-import-check disable
 >> FortiGate-VM64-AWSON~AND (bgp) $ config neighbor
 >> FortiGate-VM64-AWSON~AND (neighbor) $ edit 169.254.45.89
 >> FortiGate-VM64-AWSON~AND (169.254.45.89) $ set capability-default-originate enable
 >> FortiGate-VM64-AWSON~AND (169.254.45.89) $ set link-down-failover enable
 >> FortiGate-VM64-AWSON~AND (169.254.45.89) $ set description "vpn-02b56c99935bfcbea-2"
 >> FortiGate-VM64-AWSON~AND (169.254.45.89) $ set remote-as 64512
 >> FortiGate-VM64-AWSON~AND (169.254.45.89) $ set route-map-out "rmap-outbound"
 >> FortiGate-VM64-AWSON~AND (169.254.45.89) $ next
 >> FortiGate-VM64-AWSON~AND (neighbor) $ end
 >> FortiGate-VM64-AWSON~AND (bgp) $ config network
 >> FortiGate-VM64-AWSON~AND (network) $ edit 1
 >> FortiGate-VM64-AWSON~AND (1) $ set prefix 192.168.2.150 255.255.255.255
 >> FortiGate-VM64-AWSON~AND (1) $ next
 >> FortiGate-VM64-AWSON~AND (network) $ end
 >> FortiGate-VM64-AWSON~AND (bgp) $ end
 >> FortiGate-VM64-AWSON~AND $
 >> FortiGate-VM64-AWSON~AND $
 >> FortiGate-VM64-AWSON~AND $ config firewall ippool
 >> FortiGate-VM64-AWSON~AND (ippool) $ edit "ippool"
 >> FortiGate-VM64-AWSON~AND (ippool) $ set startip 192.168.2.150
 >> FortiGate-VM64-AWSON~AND (ippool) $ set endip 192.168.2.150
 >> FortiGate-VM64-AWSON~AND (ippool) $ next
 >> FortiGate-VM64-AWSON~AND (ippool) $ end
```

```
 >> FortiGate-VM64-AWSON~AND $
 >> FortiGate-VM64-AWSON~AND $ config system zone
 >> FortiGate-VM64-AWSON~AND (zone) $ edit "sys-zone-tgw-vpn"
 >> FortiGate-VM64-AWSON~AND (sys-zone-tgw-vpn) $ set interface "tgw-vpn-1" "tgw-vpn-2"
 >> FortiGate-VM64-AWSON~AND (sys-zone-tgw-vpn) $ next
 >> FortiGate-VM64-AWSON~AND (zone) $ end
 >> FortiGate-VM64-AWSON~AND $
 >> FortiGate-VM64-AWSON~AND $ config firewall policy
 >> FortiGate-VM64-AWSON~AND (policy) $ edit 1
 >> FortiGate-VM64-AWSON~AND (1) $ set name "vpc-vpc_access"
 >> FortiGate-VM64-AWSON~AND (1) $ set srcintf "sys-zone-tgw-vpn"
 >> FortiGate-VM64-AWSON~AND (1) $ set dstintf "sys-zone-tgw-vpn"
 >> FortiGate-VM64-AWSON~AND (1) $ set srcaddr "all"
 >> FortiGate-VM64-AWSON~AND (1) $ set dstaddr "all"
 >> FortiGate-VM64-AWSON~AND (1) $ set action accept
 >> FortiGate-VM64-AWSON~AND (1) $ set schedule "always"
 >> FortiGate-VM64-AWSON~AND (1) $ set service "ALL"
 >> FortiGate-VM64-AWSON~AND (1) $ set fsso disable
 >> FortiGate-VM64-AWSON~AND (1) $ set nat enable
 >> FortiGate-VM64-AWSON~AND (1) $ set ippool enable
 >> FortiGate-VM64-AWSON~AND (1) $ set poolname "ippool"
 >> FortiGate-VM64-AWSON~AND (1) $ next
 >> FortiGate-VM64-AWSON~AND (policy) $ edit 2
 >> FortiGate-VM64-AWSON~AND (2) $ set name "vpc-internet_access"
 >> FortiGate-VM64-AWSON~AND (2) $ set srcintf "sys-zone-tgw-vpn"
 >> FortiGate-VM64-AWSON~AND (2) $ set dstintf "port1"
 >> FortiGate-VM64-AWSON~AND (2) $ set srcaddr "all"
 >> FortiGate-VM64-AWSON~AND (2) $ set dstaddr "all"
 >> FortiGate-VM64-AWSON~AND (2) $ set action accept
 >> FortiGate-VM64-AWSON~AND (2) $ set schedule "always"
 >> FortiGate-VM64-AWSON~AND (2) $ set service "ALL"
 >> FortiGate-VM64-AWSON~AND (2) $ set fsso disable
 >> FortiGate-VM64-AWSON~AND (2) $ set nat enable
 >> FortiGate-VM64-AWSON~AND (2) $ next
 >> FortiGate-VM64-AWSON~AND (policy) $ end
```

Slave FortiGate-VM cloudinit output

```
FortiGate-VM64-AWSON~AND # diag debug cloudinit show
 >> Checking metadata source aws
 >> AWS curl header: Fos-instance-id: <masked_instance_id>
 >> AWS trying to get config script from https://<masked_api_id>/prod/fgt-asg-handler
 >> AWS download config script successfully
 >> Run config script
 >> Finish running script
 >> FortiGate-VM64-AWSON~AND $ config system dns
 >> FortiGate-VM64-AWSON~AND (dns) $ unset primary
 >> FortiGate-VM64-AWSON~AND (dns) $ unset secondary
 >> FortiGate-VM64-AWSON~AND (dns) $ end
 >> FortiGate-VM64-AWSON~AND $ config system global
 >> FortiGate-VM64-AWSON~AND (global) $ set admin-sport 8443
 >> FortiGate-VM64-AWSON~AND (global) $ end
 >> FortiGate-VM64-AWSON~AND $ config system auto-scale
 >> FortiGate-VM64-AWSON~AND (auto-scale) $ set status enable
 >> FortiGate-VM64-AWSON~AND (auto-scale) $ set sync-interface "port1"
 >> FortiGate-VM64-AWSON~AND (auto-scale) $ set hb-interval 30
 >> FortiGate-VM64-AWSON~AND (auto-scale) $ set role slave
 >> FortiGate-VM64-AWSON~AND (auto-scale) $ set master-ip 192.168.2.150
 >> FortiGate-VM64-AWSON~AND (auto-scale) $ set callback-url https://<masked_api_id>/prod/fgt-
    asg-handler
 >> FortiGate-VM64-AWSON~AND (auto-scale) $ set psksecret <masked_psksecret>
 >> FortiGate-VM64-AWSON~AND (auto-scale) $ end
 >> FortiGate-VM64-AWSON~AND $ config system vdom-exception
 >> FortiGate-VM64-AWSON~AND (vdom-exception) $ edit 0
 >> FortiGate-VM64-AWSON~AND (0) $ set object vpn.ipsec.phase1-interface
 >> FortiGate-VM64-AWSON~AND (0) $ next
 >> FortiGate-VM64-AWSON~AND (vdom-exception) $ edit 0
 >> FortiGate-VM64-AWSON~AND (0) $ set object vpn.ipsec.phase2-interface
 >> FortiGate-VM64-AWSON~AND (0) $ next
 >> FortiGate-VM64-AWSON~AND (vdom-exception) $ edit 0
 >> FortiGate-VM64-AWSON~AND (0) $ set object router.bgp
 >> FortiGate-VM64-AWSON~AND (0) $ next
 >> FortiGate-VM64-AWSON~AND (vdom-exception) $ edit 0
 >> FortiGate-VM64-AWSON~AND (0) $ set object router.route-map
 >> FortiGate-VM64-AWSON~AND (0) $ next
 >> FortiGate-VM64-AWSON~AND (vdom-exception) $ edit 0
 >> FortiGate-VM64-AWSON~AND (0) $ set object router.prefix-list
 >> FortiGate-VM64-AWSON~AND (0) $ next
 >> FortiGate-VM64-AWSON~AND (vdom-exception) $ edit 0
 >> FortiGate-VM64-AWSON~AND (0) $ set object firewall.ippool
 >> FortiGate-VM64-AWSON~AND (0) $ next
 >> FortiGate-VM64-AWSON~AND (vdom-exception) $ end
 >> FortiGate-VM64-AWSON~AND $
 >> FortiGate-VM64-AWSON~AND $ config router prefix-list
 >> FortiGate-VM64-AWSON~AND (prefix-list) $ edit "pflist-default-route"
 >> FortiGate-VM64-AWSON~AND (pflist-default-route) $ config rule
 >> FortiGate-VM64-AWSON~AND (rule) $ edit 1
 >> FortiGate-VM64-AWSON~AND (1) $ set prefix 0.0.0.0 0.0.0.0
 >> FortiGate-VM64-AWSON~AND (1) $ unset ge
 >> FortiGate-VM64-AWSON~AND (1) $ unset le
 >> FortiGate-VM64-AWSON~AND (1) $ next
 >> FortiGate-VM64-AWSON~AND (rule) $ end
 >> FortiGate-VM64-AWSON~AND (pflist-default-route) $ next
 >> FortiGate-VM64-AWSON~AND (prefix-list) $ edit "pflist-port1"
 >> FortiGate-VM64-AWSON~AND (pflist-port1) $ config rule
 >> FortiGate-VM64-AWSON~AND (rule) $ edit 1
 >> FortiGate-VM64-AWSON~AND (1) $ set prefix 192.168.1.143 255.255.255.255
 >> FortiGate-VM64-AWSON~AND (1) $ unset ge
 >> FortiGate-VM64-AWSON~AND (1) $ unset le
 >> FortiGate-VM64-AWSON~AND (1) $ next
 >> FortiGate-VM64-AWSON~AND (rule) $ end
 >> FortiGate-VM64-AWSON~AND (pflist-port1) $ next
 >> FortiGate-VM64-AWSON~AND (prefix-list) $ end
 >> FortiGate-VM64-AWSON~AND $
 >> FortiGate-VM64-AWSON~AND $ config router route-map
 >> FortiGate-VM64-AWSON~AND (route-map) $ edit "rmap-outbound"
 >> FortiGate-VM64-AWSON~AND (rmap-outbound) $ config rule
 >> FortiGate-VM64-AWSON~AND (rule) $ edit 1
 >> FortiGate-VM64-AWSON~AND (1) $ set match-ip-address "pflist-default-route"
 >> FortiGate-VM64-AWSON~AND (1) $ next
 >> FortiGate-VM64-AWSON~AND (rule) $ edit 2
 >> FortiGate-VM64-AWSON~AND (2) $ set match-ip-address "pflist-port1"
 >> FortiGate-VM64-AWSON~AND (2) $ next
 >> FortiGate-VM64-AWSON~AND (rule) $ end
 >> FortiGate-VM64-AWSON~AND (rmap-outbound) $ next
 >> FortiGate-VM64-AWSON~AND (route-map) $ end
 >> FortiGate-VM64-AWSON~AND $
 >> FortiGate-VM64-AWSON~AND $ config vpn ipsec phase1-interface
 >> FortiGate-VM64-AWSON~AND (phase1-interface) $ edit "tgw-vpn-1"
 >> FortiGate-VM64-AWSON~AND (tgw-vpn-1) $ set interface "port1"
 >> FortiGate-VM64-AWSON~AND (tgw-vpn-1) $ set local-gw 192.168.1.143
 >> FortiGate-VM64-AWSON~AND (tgw-vpn-1) $ set dhgrp 2
 >> FortiGate-VM64-AWSON~AND (tgw-vpn-1) $ set proposal aes128-sha1
 >> FortiGate-VM64-AWSON~AND (tgw-vpn-1) $ set keylife 28800
 >> FortiGate-VM64-AWSON~AND (tgw-vpn-1) $ set net-device enable
 >> FortiGate-VM64-AWSON~AND (tgw-vpn-1) $ set remote-gw 3.220.220.108
 >> FortiGate-VM64-AWSON~AND (tgw-vpn-1) $ set psksecret <masked_psksecret>
 >> FortiGate-VM64-AWSON~AND (tgw-vpn-1) $ set dpd-retryinterval 10
 >> FortiGate-VM64-AWSON~AND (tgw-vpn-1) $ next
 >> FortiGate-VM64-AWSON~AND (phase1-interface) $ end
 >> FortiGate-VM64-AWSON~AND $
 >> FortiGate-VM64-AWSON~AND $ config vpn ipsec phase2-interface
 >> FortiGate-VM64-AWSON~AND (phase2-interface) $ edit "tgw-vpn-1"
 >> FortiGate-VM64-AWSON~AND (tgw-vpn-1) $ set phase1name "tgw-vpn-1"
 >> FortiGate-VM64-AWSON~AND (tgw-vpn-1) $ set proposal aes128-sha1
 >> FortiGate-VM64-AWSON~AND (tgw-vpn-1) $ set dhgrp 2
 >> FortiGate-VM64-AWSON~AND (tgw-vpn-1) $ set keylifeseconds 3600
 >> FortiGate-VM64-AWSON~AND (tgw-vpn-1) $ next
 >> FortiGate-VM64-AWSON~AND (phase2-interface) $ end
 >> FortiGate-VM64-AWSON~AND $
 >> FortiGate-VM64-AWSON~AND $ config system interface
 >> FortiGate-VM64-AWSON~AND (interface) $ edit "tgw-vpn-1"
 >> FortiGate-VM64-AWSON~AND (tgw-vpn-1) $ set interface "port1"
 >> FortiGate-VM64-AWSON~AND (tgw-vpn-1) $ set ip 169.254.44.14 255.255.255.255
 >> FortiGate-VM64-AWSON~AND (tgw-vpn-1) $ set allowaccess ping
 >> FortiGate-VM64-AWSON~AND (tgw-vpn-1) $ set type tunnel
 >> FortiGate-VM64-AWSON~AND (tgw-vpn-1) $ set tcp-mss 1379
 >> FortiGate-VM64-AWSON~AND (tgw-vpn-1) $ set remote-ip 169.254.44.13 255.255.255.252
 >> FortiGate-VM64-AWSON~AND (tgw-vpn-1) $ next
 >> FortiGate-VM64-AWSON~AND (interface) $ end
 >> FortiGate-VM64-AWSON~AND $
 >> FortiGate-VM64-AWSON~AND $ config router bgp
 >> FortiGate-VM64-AWSON~AND (bgp) $ set as 65000
 >> FortiGate-VM64-AWSON~AND (bgp) $ set router-id 192.168.1.143
 >> FortiGate-VM64-AWSON~AND (bgp) $ set ebgp-multipath enable
 >> FortiGate-VM64-AWSON~AND (bgp) $ set network-import-check disable
 >> FortiGate-VM64-AWSON~AND (bgp) $ config neighbor
 >> FortiGate-VM64-AWSON~AND (neighbor) $ edit 169.254.44.13
 >> FortiGate-VM64-AWSON~AND (169.254.44.13) $ set capability-default-originate enable
 >> FortiGate-VM64-AWSON~AND (169.254.44.13) $ set link-down-failover enable
 >> FortiGate-VM64-AWSON~AND (169.254.44.13) $ set description "vpn-023854714704ae854-1"
 >> FortiGate-VM64-AWSON~AND (169.254.44.13) $ set remote-as 64512
 >> FortiGate-VM64-AWSON~AND (169.254.44.13) $ set route-map-out "rmap-outbound"
 >> FortiGate-VM64-AWSON~AND (169.254.44.13) $ next
 >> FortiGate-VM64-AWSON~AND (neighbor) $ end
 >> FortiGate-VM64-AWSON~AND (bgp) $ config network
 >> FortiGate-VM64-AWSON~AND (network) $ edit 1
 >> FortiGate-VM64-AWSON~AND (1) $ set prefix 192.168.1.143 255.255.255.255
 >> FortiGate-VM64-AWSON~AND (1) $ next
 >> FortiGate-VM64-AWSON~AND (network) $ end
 >> FortiGate-VM64-AWSON~AND (bgp) $ end
 >> FortiGate-VM64-AWSON~AND $
 >> FortiGate-VM64-AWSON~AND $ config vpn ipsec phase1-interface
 >> FortiGate-VM64-AWSON~AND (phase1-interface) $ edit "tgw-vpn-2"
 >> FortiGate-VM64-AWSON~AND (tgw-vpn-2) $ set interface "port1"
 >> FortiGate-VM64-AWSON~AND (tgw-vpn-2) $ set local-gw 192.168.1.143
 >> FortiGate-VM64-AWSON~AND (tgw-vpn-2) $ set dhgrp 2
 >> FortiGate-VM64-AWSON~AND (tgw-vpn-2) $ set proposal aes128-sha1
 >> FortiGate-VM64-AWSON~AND (tgw-vpn-2) $ set keylife 28800
 >> FortiGate-VM64-AWSON~AND (tgw-vpn-2) $ set net-device enable
 >> FortiGate-VM64-AWSON~AND (tgw-vpn-2) $ set remote-gw 54.82.184.6
 >> FortiGate-VM64-AWSON~AND (tgw-vpn-2) $ set psksecret <masked_psksecret>
 >> FortiGate-VM64-AWSON~AND (tgw-vpn-2) $ set dpd-retryinterval 10
 >> FortiGate-VM64-AWSON~AND (tgw-vpn-2) $ next
 >> FortiGate-VM64-AWSON~AND (phase1-interface) $ end
 >> FortiGate-VM64-AWSON~AND $
 >> FortiGate-VM64-AWSON~AND $ config vpn ipsec phase2-interface
 >> FortiGate-VM64-AWSON~AND (phase2-interface) $ edit "tgw-vpn-2"
 >> FortiGate-VM64-AWSON~AND (tgw-vpn-2) $ set phase1name "tgw-vpn-2"
 >> FortiGate-VM64-AWSON~AND (tgw-vpn-2) $ set proposal aes128-sha1
 >> FortiGate-VM64-AWSON~AND (tgw-vpn-2) $ set dhgrp 2
 >> FortiGate-VM64-AWSON~AND (tgw-vpn-2) $ set keylifeseconds 3600
 >> FortiGate-VM64-AWSON~AND (tgw-vpn-2) $ next
 >> FortiGate-VM64-AWSON~AND (phase2-interface) $ end
 >> FortiGate-VM64-AWSON~AND $
 >> FortiGate-VM64-AWSON~AND $ config system interface
 >> FortiGate-VM64-AWSON~AND (interface) $ edit "tgw-vpn-2"
 >> FortiGate-VM64-AWSON~AND (tgw-vpn-2) $ set interface "port1"
 >> FortiGate-VM64-AWSON~AND (tgw-vpn-2) $ set ip 169.254.46.194 255.255.255.255
 >> FortiGate-VM64-AWSON~AND (tgw-vpn-2) $ set allowaccess ping
 >> FortiGate-VM64-AWSON~AND (tgw-vpn-2) $ set type tunnel
 >> FortiGate-VM64-AWSON~AND (tgw-vpn-2) $ set tcp-mss 1379
 >> FortiGate-VM64-AWSON~AND (tgw-vpn-2) $ set remote-ip 169.254.46.193 255.255.255.252
 >> FortiGate-VM64-AWSON~AND (tgw-vpn-2) $ next
 >> FortiGate-VM64-AWSON~AND (interface) $ end
 >> FortiGate-VM64-AWSON~AND $
 >> FortiGate-VM64-AWSON~AND $ config router bgp
 >> FortiGate-VM64-AWSON~AND (bgp) $ set as 65000
 >> FortiGate-VM64-AWSON~AND (bgp) $ set router-id 192.168.1.143
 >> FortiGate-VM64-AWSON~AND (bgp) $ set ebgp-multipath enable
 >> FortiGate-VM64-AWSON~AND (bgp) $ set network-import-check disable
 >> FortiGate-VM64-AWSON~AND (bgp) $ config neighbor
 >> FortiGate-VM64-AWSON~AND (neighbor) $ edit 169.254.46.193
 >> FortiGate-VM64-AWSON~AND (169.254.46.193) $ set capability-default-originate enable
 >> FortiGate-VM64-AWSON~AND (169.254.46.193) $ set link-down-failover enable
 >> FortiGate-VM64-AWSON~AND (169.254.46.193) $ set description "vpn-023854714704ae854-2"
 >> FortiGate-VM64-AWSON~AND (169.254.46.193) $ set remote-as 64512
 >> FortiGate-VM64-AWSON~AND (169.254.46.193) $ set route-map-out "rmap-outbound"
 >> FortiGate-VM64-AWSON~AND (169.254.46.193) $ next
 >> FortiGate-VM64-AWSON~AND (neighbor) $ end
 >> FortiGate-VM64-AWSON~AND (bgp) $ config network
 >> FortiGate-VM64-AWSON~AND (network) $ edit 1
 >> FortiGate-VM64-AWSON~AND (1) $ set prefix 192.168.1.143 255.255.255.255
 >> FortiGate-VM64-AWSON~AND (1) $ next
 >> FortiGate-VM64-AWSON~AND (network) $ end
 >> FortiGate-VM64-AWSON~AND (bgp) $ end
 >> FortiGate-VM64-AWSON~AND $
 >> FortiGate-VM64-AWSON~AND $
 >> FortiGate-VM64-AWSON~AND $ config firewall ippool
 >> FortiGate-VM64-AWSON~AND (ippool) $ edit "ippool"
 >> FortiGate-VM64-AWSON~AND (ippool) $ set startip 192.168.1.143
 >> FortiGate-VM64-AWSON~AND (ippool) $ set endip 192.168.1.143
 >> FortiGate-VM64-AWSON~AND (ippool) $ next
 >> FortiGate-VM64-AWSON~AND (ippool) $ end
 >> FortiGate-VM64-AWSON~AND $
 >> FortiGate-VM64-AWSON~AND $ config system zone
 >> FortiGate-VM64-AWSON~AND (zone) $ edit "sys-zone-tgw-vpn"
 >> FortiGate-VM64-AWSON~AND (sys-zone-tgw-vpn) $ set interface "tgw-vpn-1" "tgw-vpn-2"
 >> FortiGate-VM64-AWSON~AND (sys-zone-tgw-vpn) $ next
 >> FortiGate-VM64-AWSON~AND (zone) $ end
 >> FortiGate-VM64-AWSON~AND $
 >> FortiGate-VM64-AWSON~AND $ config firewall policy
 >> FortiGate-VM64-AWSON~AND (policy) $ edit 1
 >> FortiGate-VM64-AWSON~AND (1) $ set name "vpc-vpc_access"
 >> FortiGate-VM64-AWSON~AND (1) $ set srcintf "sys-zone-tgw-vpn"
 >> FortiGate-VM64-AWSON~AND (1) $ set dstintf "sys-zone-tgw-vpn"
 >> FortiGate-VM64-AWSON~AND (1) $ set srcaddr "all"
 >> FortiGate-VM64-AWSON~AND (1) $ set dstaddr "all"
 >> FortiGate-VM64-AWSON~AND (1) $ set action accept
 >> FortiGate-VM64-AWSON~AND (1) $ set schedule "always"
 >> FortiGate-VM64-AWSON~AND (1) $ set service "ALL"
 >> FortiGate-VM64-AWSON~AND (1) $ set fsso disable
 >> FortiGate-VM64-AWSON~AND (1) $ set nat enable
 >> FortiGate-VM64-AWSON~AND (1) $ set ippool enable
 >> FortiGate-VM64-AWSON~AND (1) $ set poolname "ippool"
 >> FortiGate-VM64-AWSON~AND (1) $ next
 >> FortiGate-VM64-AWSON~AND (policy) $ edit 2
 >> FortiGate-VM64-AWSON~AND (2) $ set name "vpc-internet_access"
 >> FortiGate-VM64-AWSON~AND (2) $ set srcintf "sys-zone-tgw-vpn"
 >> FortiGate-VM64-AWSON~AND (2) $ set dstintf "port1"
 >> FortiGate-VM64-AWSON~AND (2) $ set srcaddr "all"
 >> FortiGate-VM64-AWSON~AND (2) $ set dstaddr "all"
 >> FortiGate-VM64-AWSON~AND (2) $ set action accept
 >> FortiGate-VM64-AWSON~AND (2) $ set schedule "always"
 >> FortiGate-VM64-AWSON~AND (2) $ set service "ALL"
 >> FortiGate-VM64-AWSON~AND (2) $ set fsso disable
 >> FortiGate-VM64-AWSON~AND (2) $ set nat enable
 >> FortiGate-VM64-AWSON~AND (2) $ next
 >> FortiGate-VM64-AWSON~AND (policy) $ end
```

Master FortiGate-VM VPN output

```
FortiGate-VM64-AWSON~AND # diag vpn tun list
list all ipsec tunnel in vd 0
------------------------------------------------------
name=tgw-vpn-1 ver=1 serial=1 192.168.2.150:4500->3.219.71.235:4500 dst_mtu=9001
bound_if=3 lgwy=static/1 tun=intf/0 mode=auto/1 encap=none/528 options[0210]=create_dev frag-
      rfc accept_traffic=1

proxyid_num=1 child_num=0 refcnt=15 ilast=0 olast=0 ad=/0
stat: rxp=248 txp=250 rxb=33648 txb=15612
dpd: mode=on-demand on=1 idle=10000ms retry=3 count=0 seqno=0
natt: mode=keepalive draft=32 interval=10 remote_port=4500
proxyid=tgw-vpn-1 proto=0 sa=1 ref=2 serial=1
   src: 0:0.0.0.0/0.0.0.0:0
   dst: 0:0.0.0.0/0.0.0.0:0
   SA:  ref=3 options=10202 type=00 soft=0 mtu=8926 expire=2159/0B replaywin=2048
         seqno=fb esn=0 replaywin_lastseq=000000f8 itn=0 qat=0
   life: type=01 bytes=0/0 timeout=3301/3600
   dec: spi=d49814e0 esp=aes key=16 <masked_key>
         ah=sha1 key=20 <masked_key>
   enc: spi=f65cea35 esp=aes key=16 <masked_key>
         ah=sha1 key=20 <masked_key>
   dec:pkts/bytes=248/15161, enc:pkts/bytes=250/34224
------------------------------------------------------
name=tgw-vpn-2 ver=1 serial=2 192.168.2.150:4500->34.197.152.22:4500 dst_mtu=9001
bound_if=3 lgwy=static/1 tun=intf/0 mode=auto/1 encap=none/528 options[0210]=create_dev frag-
      rfc accept_traffic=1

proxyid_num=1 child_num=0 refcnt=15 ilast=1 olast=1 ad=/0
stat: rxp=248 txp=250 rxb=33648 txb=15612
dpd: mode=on-demand on=1 idle=10000ms retry=3 count=0 seqno=0
natt: mode=keepalive draft=32 interval=10 remote_port=4500
proxyid=tgw-vpn-2 proto=0 sa=1 ref=2 serial=1
   src: 0:0.0.0.0/0.0.0.0:0
   dst: 0:0.0.0.0/0.0.0.0:0
   SA:  ref=3 options=10202 type=00 soft=0 mtu=8926 expire=2157/0B replaywin=2048
         seqno=fb esn=0 replaywin_lastseq=000000f8 itn=0 qat=0
   life: type=01 bytes=0/0 timeout=3300/3600
   dec: spi=d49814df esp=aes key=16 <masked_key>
         ah=sha1 key=20 <masked_key>
   enc: spi=b867a1a8 esp=aes key=16 <masked_key>
         ah=sha1 key=20 <masked_key>
   dec:pkts/bytes=248/15161, enc:pkts/bytes=250/34224
------------------------------------------------------
name=__autoscale_m_p1 ver=1 serial=3 192.168.2.150:0->0.0.0.0:0 dst_mtu=0
bound_if=3 lgwy=static/1 tun=tunnel/1 mode=dialup/2 encap=none/0 accept_traffic=1

proxyid_num=0 child_num=1 refcnt=5 ilast=1142 olast=1142 ad=/0
stat: rxp=0 txp=0 rxb=0 txb=0
dpd: mode=on-idle on=0 idle=60000ms retry=3 count=0 seqno=0
natt: mode=none draft=0 interval=0 remote_port=0
run_tally=0
------------------------------------------------------
name=__autoscale_m_p1_0 ver=1 serial=5 192.168.2.150:0->192.168.1.143:0 dst_mtu=9001
bound_if=3 lgwy=static/1 tun=tunnel/1 mode=dial_inst/3 encap=none/128 options[0080]=rgwy-chg
      run_state=0 accept_traffic=1

parent=__autoscale_m_p1 index=0
proxyid_num=1 child_num=0 refcnt=5 ilast=8 olast=8 ad=/0
stat: rxp=76 txp=75 rxb=18768 txb=8548
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: 0:192.168.1.143-192.168.1.143:0
   SA:  ref=3 options=202 type=00 soft=0 mtu=8942 expire=42745/0B replaywin=2048
         seqno=4c esn=0 replaywin_lastseq=0000004d itn=0 qat=0
   life: type=01 bytes=0/0 timeout=43187/43200
   dec: spi=d49814e2 esp=aes key=16 <masked_key>
         ah=sha1 key=20 <masked_key>
   enc: spi=dff389cc esp=aes key=16 <masked_key>
```

```
         ah=sha1 key=20 <masked_key>
   dec:pkts/bytes=76/13847, enc:pkts/bytes=75/13480
```

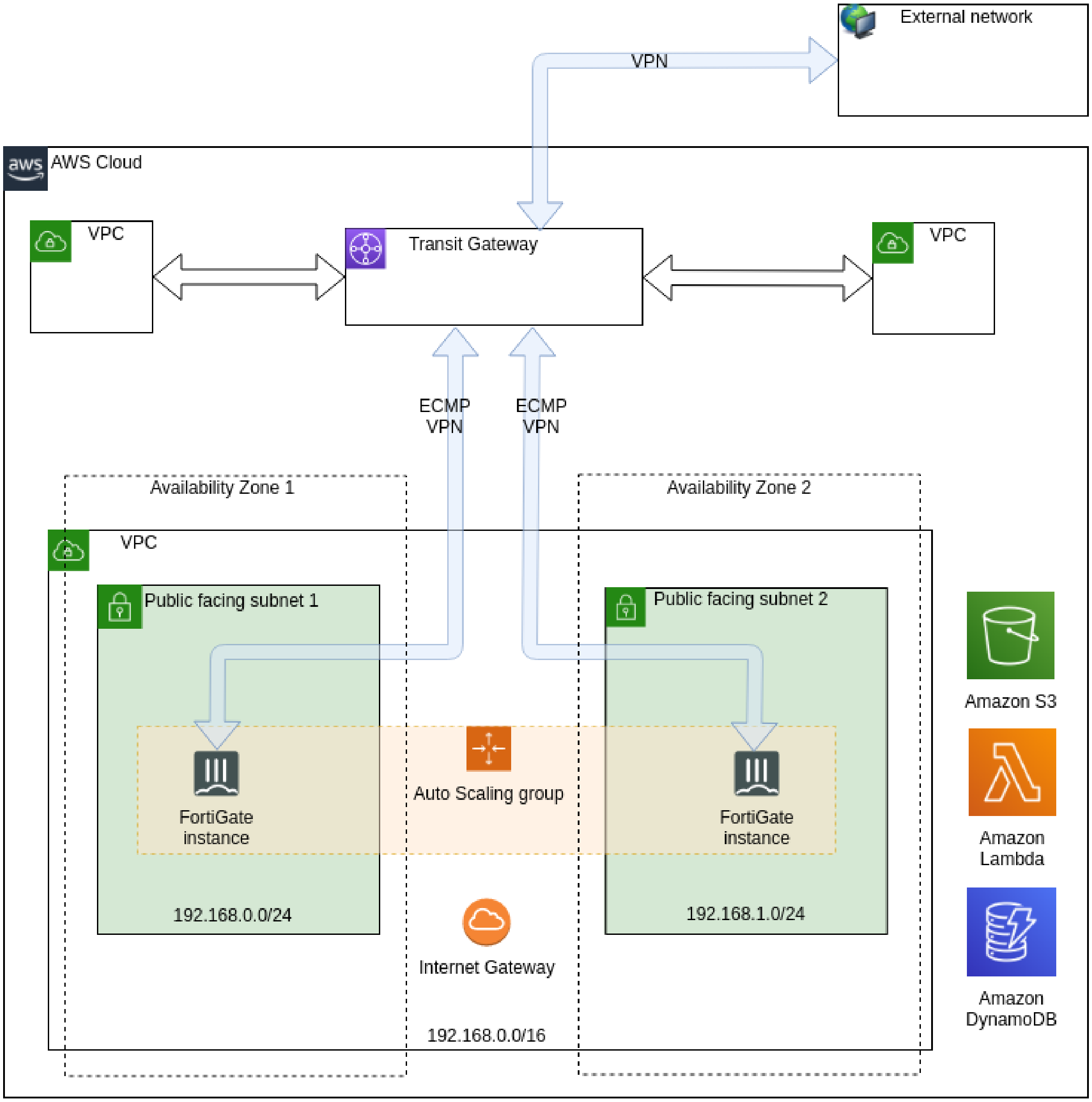
Slave FortiGate-VM VPN output

```
FortiGate-VM64-AWSON~AND # diag vpn tun list
list all ipsec tunnel in vd 0
------------------------------------------------------
name=tgw-vpn-1 ver=1 serial=1 192.168.1.143:4500->3.220.220.108:4500 dst_mtu=9001
bound_if=3 lgwy=static/1 tun=intf/0 mode=auto/1 encap=none/528 options[0210]=create_dev frag-
     rfc accept_traffic=1

proxyid_num=1 child_num=0 refcnt=15 ilast=0 olast=0 ad=/0
stat: rxp=122 txp=124 rxb=16576 txb=7787
dpd: mode=on-demand on=1 idle=10000ms retry=3 count=0 seqno=0
natt: mode=keepalive draft=32 interval=10 remote_port=4500
proxyid=tgw-vpn-1 proto=0 sa=1 ref=2 serial=1
   src: 0:0.0.0.0/0.0.0.0:0
   dst: 0:0.0.0.0/0.0.0.0:0
   SA:  ref=3 options=10202 type=00 soft=0 mtu=8926 expire=2749/0B replaywin=2048
         seqno=7d esn=0 replaywin_lastseq=0000007a itn=0 qat=0
   life: type=01 bytes=0/0 timeout=3301/3600
   dec: spi=dff389ca esp=aes key=16 <masked_key>
         ah=sha1 key=20 <masked_key>
   enc: spi=fb2e8342 esp=aes key=16 <masked_key>
         ah=sha1 key=20 <masked_key>
   dec:pkts/bytes=122/7488, enc:pkts/bytes=124/17024
------------------------------------------------------
name=tgw-vpn-2 ver=1 serial=2 192.168.1.143:4500->54.82.184.6:4500 dst_mtu=9001
bound_if=3 lgwy=static/1 tun=intf/0 mode=auto/1 encap=none/528 options[0210]=create_dev frag-
     rfc accept_traffic=1

proxyid_num=1 child_num=0 refcnt=15 ilast=1 olast=1 ad=/0
stat: rxp=122 txp=124 rxb=16576 txb=7787
dpd: mode=on-demand on=1 idle=10000ms retry=3 count=0 seqno=0
natt: mode=keepalive draft=32 interval=10 remote_port=4500
proxyid=tgw-vpn-2 proto=0 sa=1 ref=2 serial=1
   src: 0:0.0.0.0/0.0.0.0:0
   dst: 0:0.0.0.0/0.0.0.0:0
   SA:  ref=3 options=10202 type=00 soft=0 mtu=8926 expire=2750/0B replaywin=2048
         seqno=7d esn=0 replaywin_lastseq=0000007a itn=0 qat=0
   life: type=01 bytes=0/0 timeout=3303/3600
   dec: spi=dff389c9 esp=aes key=16 <masked_key>
         ah=sha1 key=20 <masked_key>
   enc: spi=c2db9a6d esp=aes key=16 <masked_key>
         ah=sha1 key=20 <masked_key>
   dec:pkts/bytes=122/7488, enc:pkts/bytes=124/17024
------------------------------------------------------
name=__autoscale_s_p1 ver=1 serial=5 192.168.1.143:0->192.168.2.150:0 dst_mtu=9001
bound_if=3 lgwy=dyn/0 tun=tunnel/1 mode=auto/1 encap=none/0 run_state=0 accept_traffic=1

proxyid_num=1 child_num=0 refcnt=6 ilast=12 olast=12 ad=/0
stat: rxp=80 txp=81 rxb=14224 txb=14155
dpd: mode=on-demand on=1 idle=20000ms retry=3 count=0 seqno=0
natt: mode=none draft=0 interval=0 remote_port=0
proxyid=__autoscale_s_p2 proto=0 sa=1 ref=2 serial=1 auto-negotiate
   src: 0:192.168.1.143/255.255.255.255:0
   dst: 0:0.0.0.0/0.0.0.0:0
   SA:  ref=3 options=18203 type=00 soft=0 mtu=8942 expire=42442/0B replaywin=2048
          seqno=52 esn=0 replaywin_lastseq=00000051 itn=0 qat=0
   life: type=01 bytes=0/0 timeout=42903/43200
   dec: spi=dff389cc esp=aes key=16 <masked_key>
          ah=sha1 key=20 <masked_key>
   enc: spi=d49814e2 esp=aes key=16 <masked_key>
          ah=sha1 key=20 <masked_key>
   dec:pkts/bytes=80/8964, enc:pkts/bytes=81/19400
run_tally=0
```

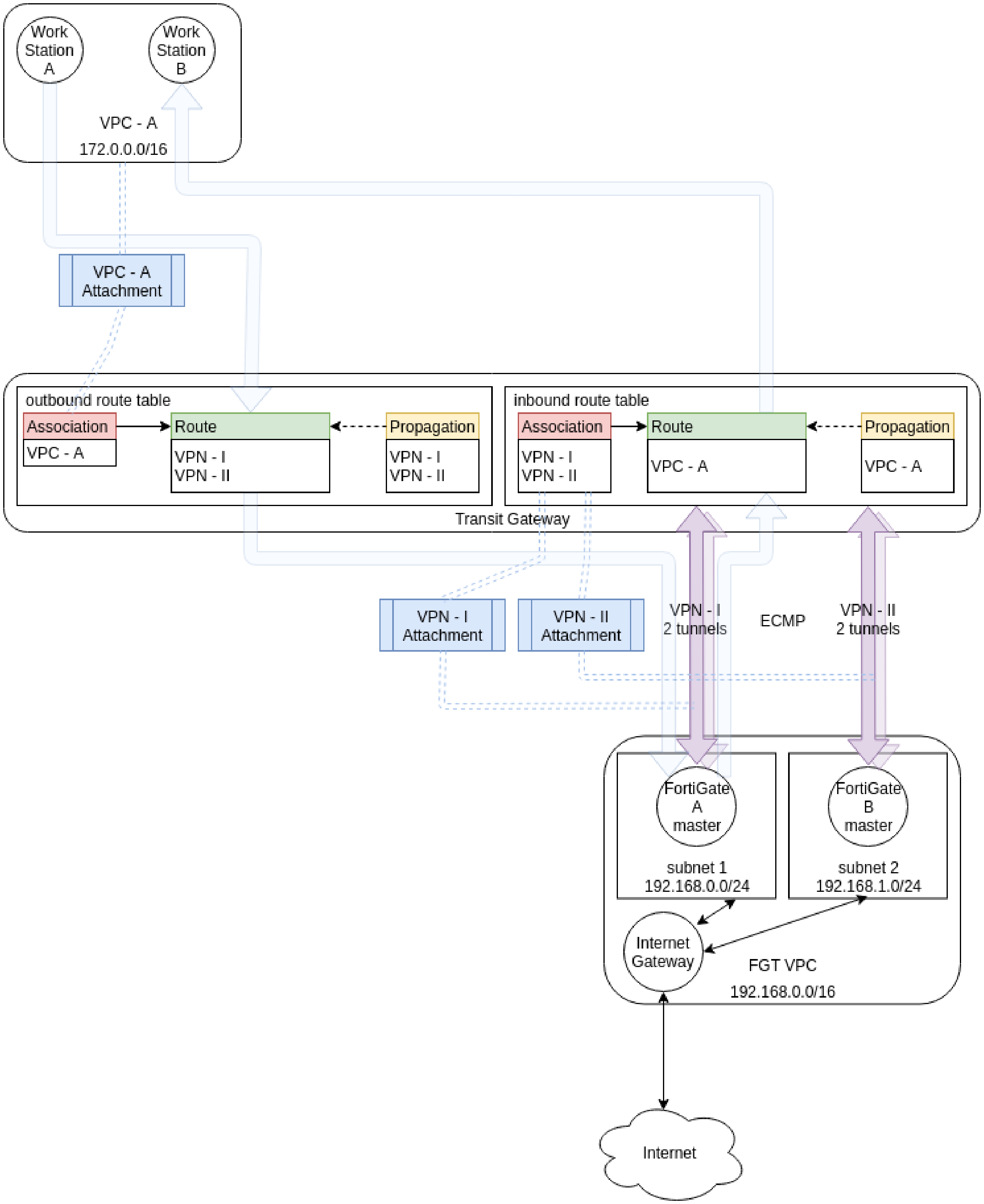
Architectural diagrams

The following diagrams illustrate the different aspects of the architecture of FortiGate Autoscale for AWS with Transit Gateway integration.

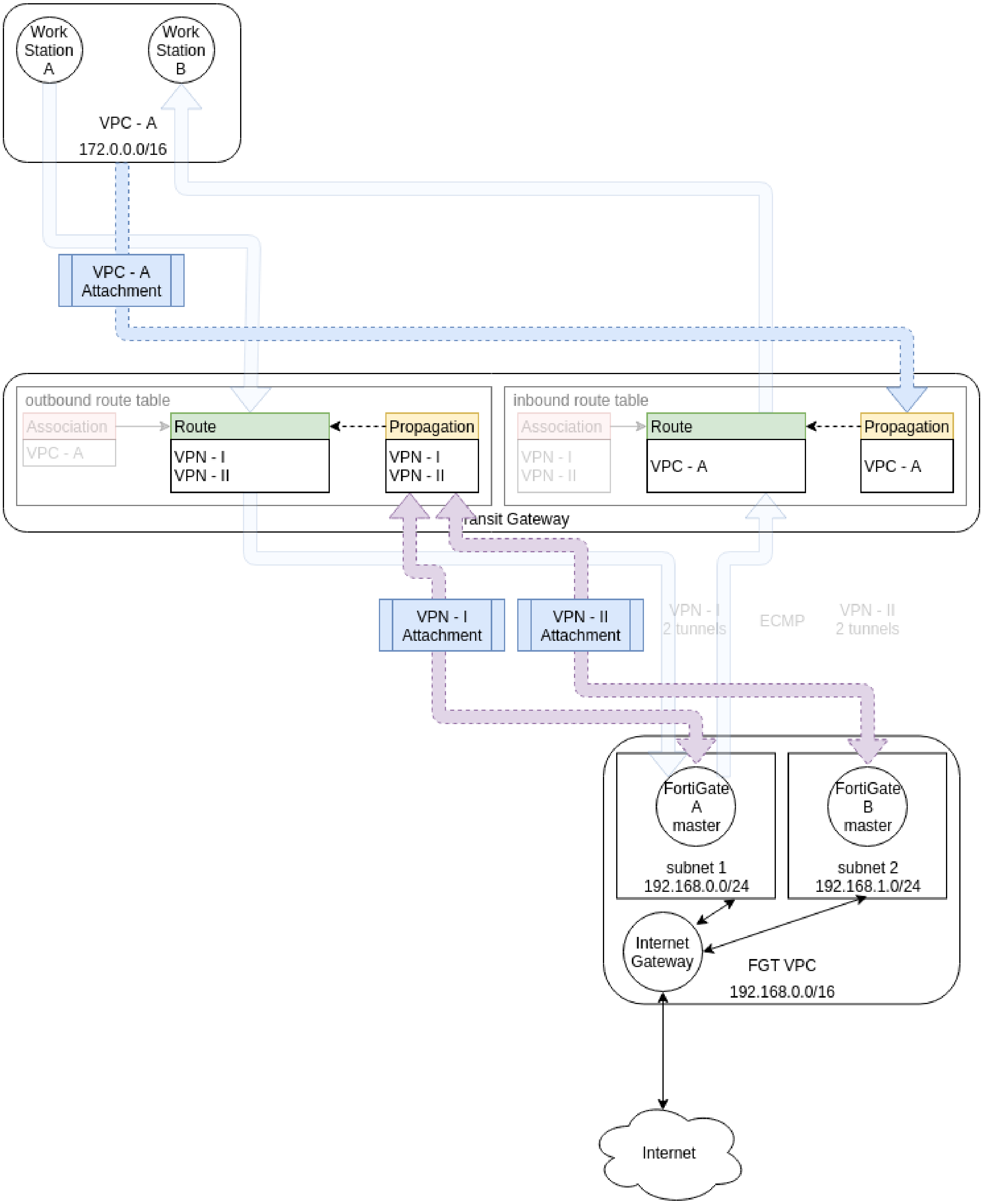
FortiGate-VM Autoscale VPC attached to a Transit Gateway



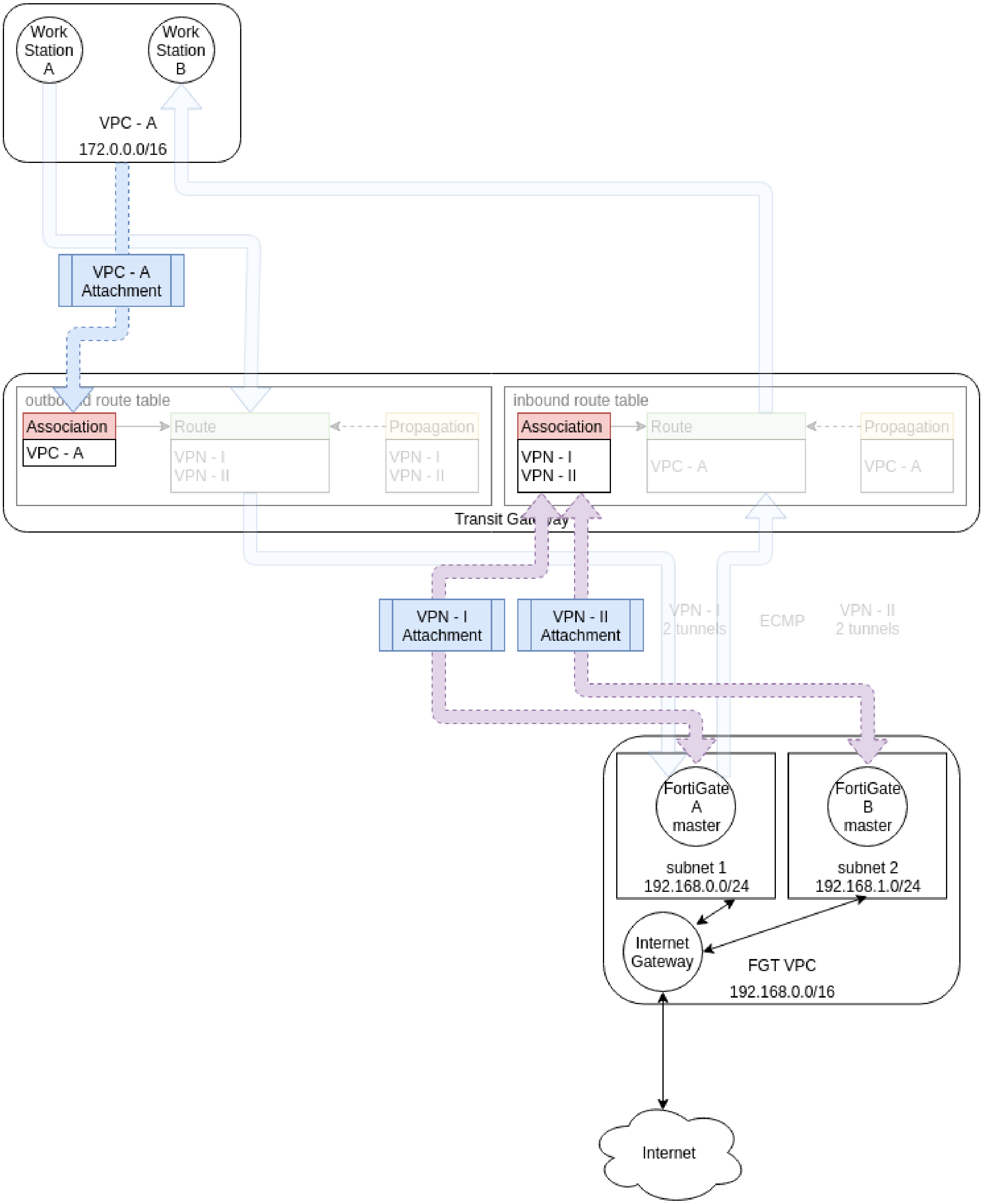
FortiGate Autoscale VPC integration with Transit Gateway



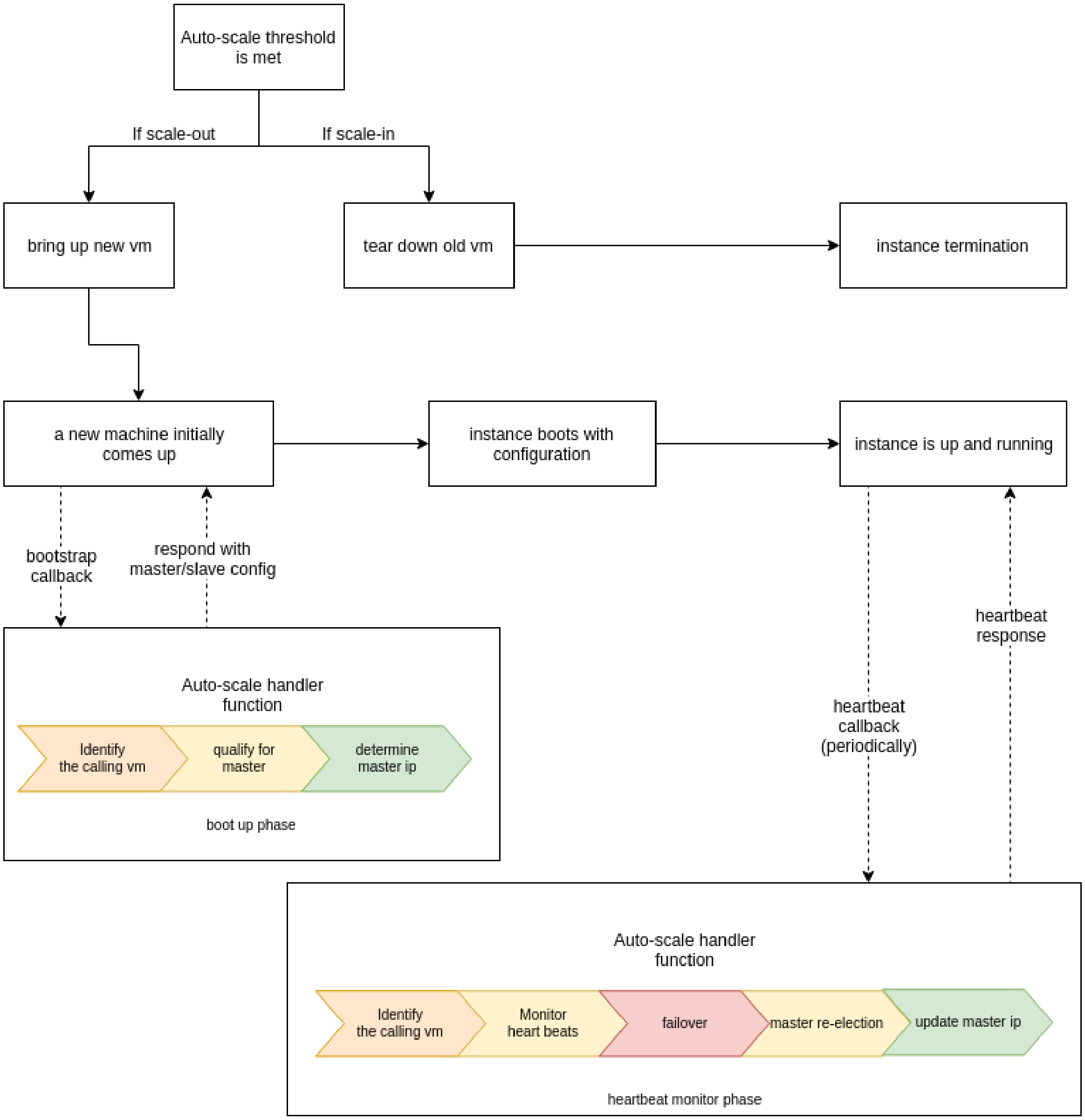
Route propagation



Route associations



Autoscale handler flowchart



Change log

Date	Change Description
2019-03-28	Initial release.
2019-07-01	Updated Deploying auto scaling on AWS on page 4.
2019-08-07	Added Deploying auto scaling on AWS with Transit Gateway integration on page 5.
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 with Transit Gateway integration on page 5.
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.
2020-01-21	Updated Deploying auto scaling on AWS with Transit Gateway integration on page 5.
2020-02-25	Minor updates to Deploying auto scaling on AWS on page 4.
2020-04-23	Add video link to Deploying auto scaling on AWS with Transit Gateway integration on page 5.
2020-09-22	Created the final version of Deploying auto scaling on AWS on page 4