Inbound Autoscaling with Transit Gateway

Runbook

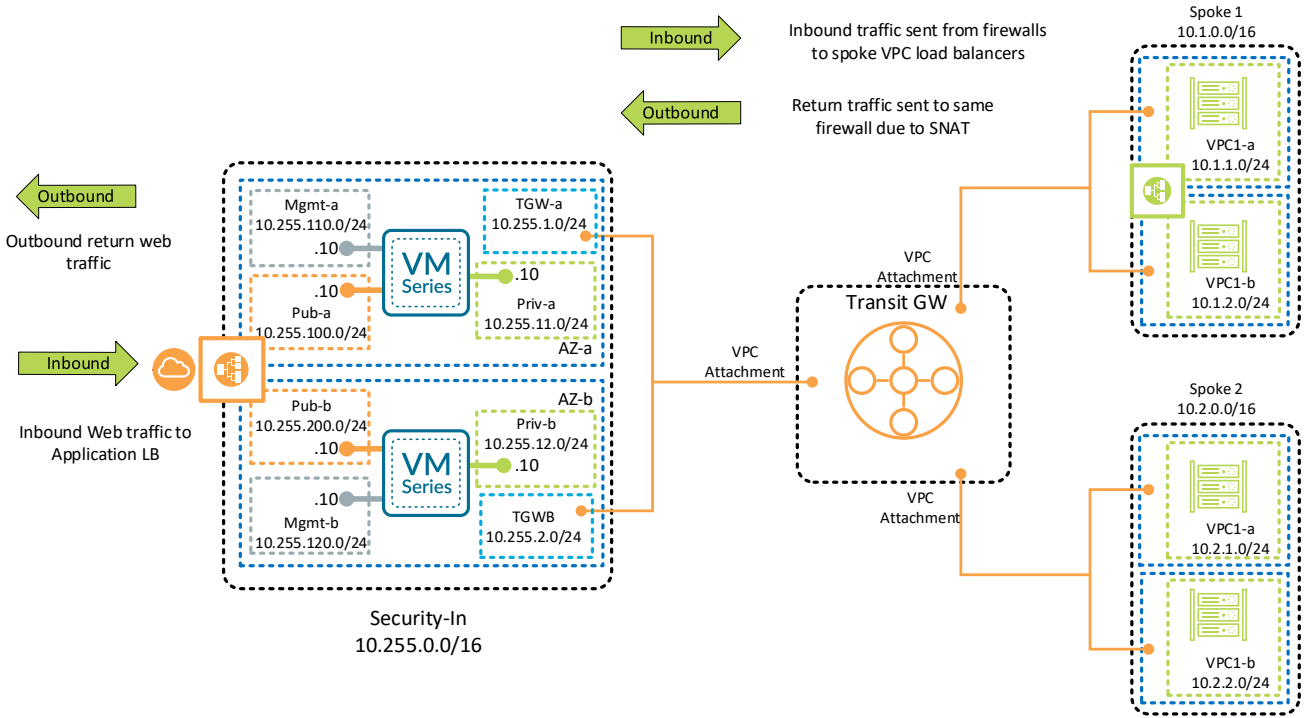
Matt McLimans
Public Cloud Consultant Engineer

SUPPORT POLICY

This is released under an as-is, best effort, support policy. These scripts should be seen as community supported and Palo Alto Networks will contribute our expertise as and when possible. We do not provide technical support or help in using or troubleshooting the components of the project through our normal support options such as Palo Alto Networks support teams, or ASC (Authorized Support Centers) partners and backline support options. The underlying product used (the VM-Series firewall) by the scripts or templates are still supported, but the support is only for the product functionality and not for help in deploying or using the template or script itself. Unless explicitly tagged, all projects or work posted in our GitHub repository (at https://github.com/PaloAltoNetworks) or sites other than our official Downloads page on https://support.paloaltonetworks.com are provided under the best effort policy.

DEPLOYMENT OVERVIEW

- The build creates VM-Series firewalls that can secure inbound traffic flows to Spoke VPCs connected to a TGW.
- VM-Series can horizontal scale based on performance demand.
- Spoke VPCs are deployed to automatically connect to TGW.
- Lambda automatically creates a NAT policy when an NLB is created within a Spoke VPC.



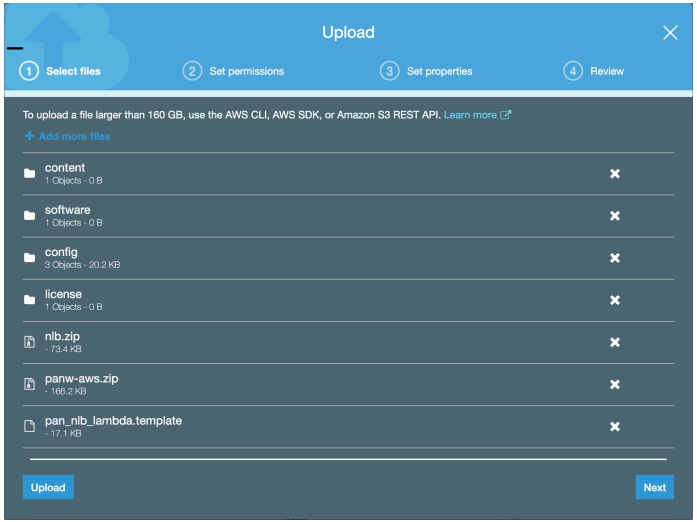
BUILD STEPS

1. Prepare Environment
    1. Create S3 Bucket for VM-Series bootstrap & Lambda packages
    2. Create Transit Gateway
    3. Create 2 empty TGW Route Tables
2. Launch VM-Series CFT
    - vmseries_asg_tgw.template
3. Launch the testapp.template
    - app_asg_tgw.template

Prepare Environment

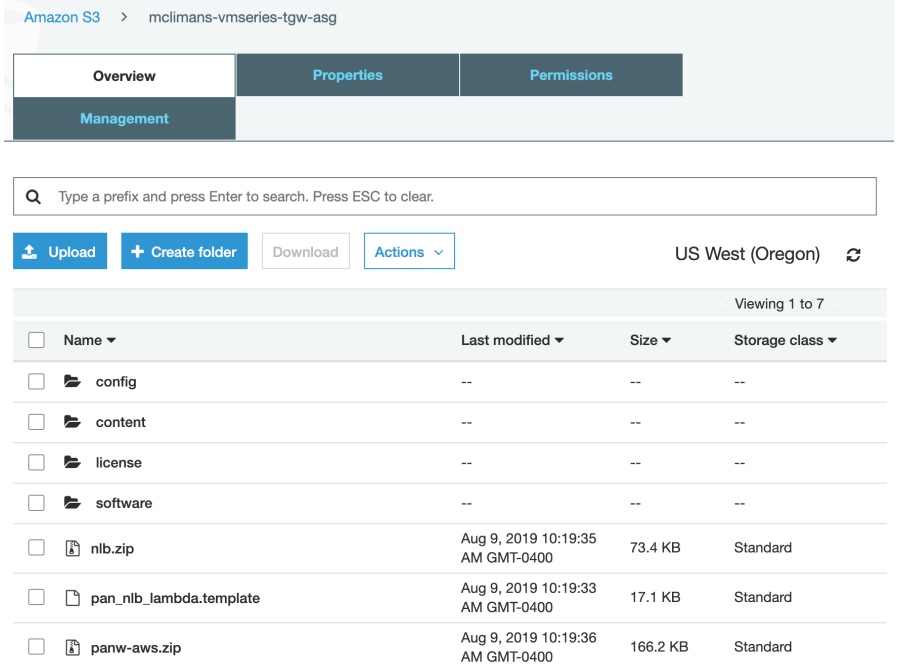
STEP 1. CREATE AN S3 BUCKET

1. Create an S3 bucket in your deployment region.
2. Drag-n-drop all files & folders in /bootstrap_files to the bucket.



Note: The nlb.zip and pan_nlb_lambda.template can be omitted if you are not using the application template.

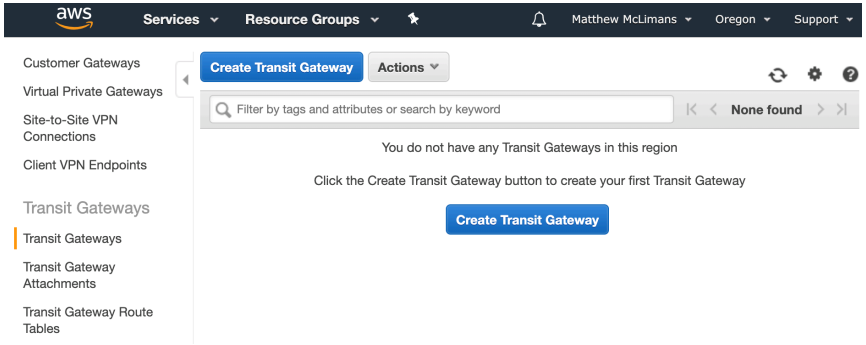
Your S3 bucket should look like this before continuing

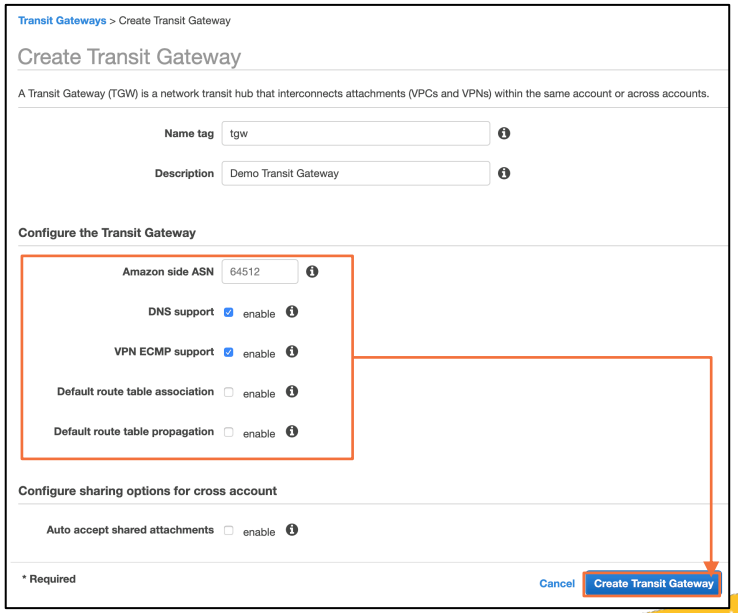


Note: If you are using BYOL for the VM-Series, paste your auth codes inside the /license/authcodes file. The authcodes must be registered to your PANW support account prior to deployment.

STEP 2. CREATE TRANSIT GATEWAY

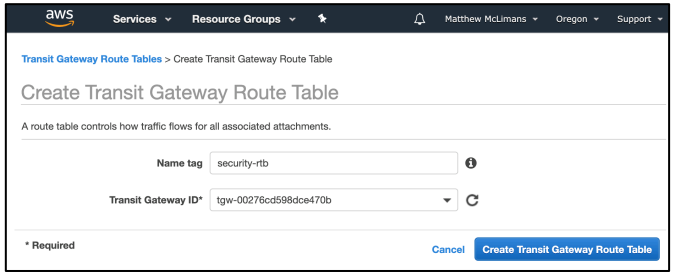
1. Go to **VPC → Transit Gateways → Create Transit Gateway**
2. **Uncheck** *Default Route Table Association* and *Default Route Table Propagation*.

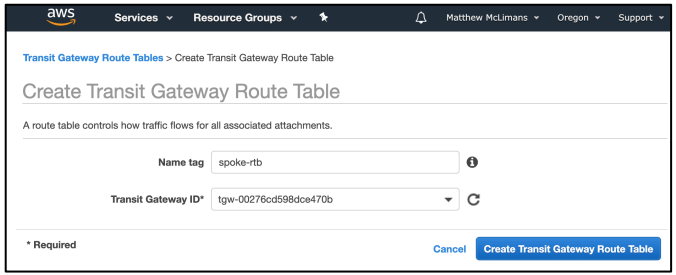




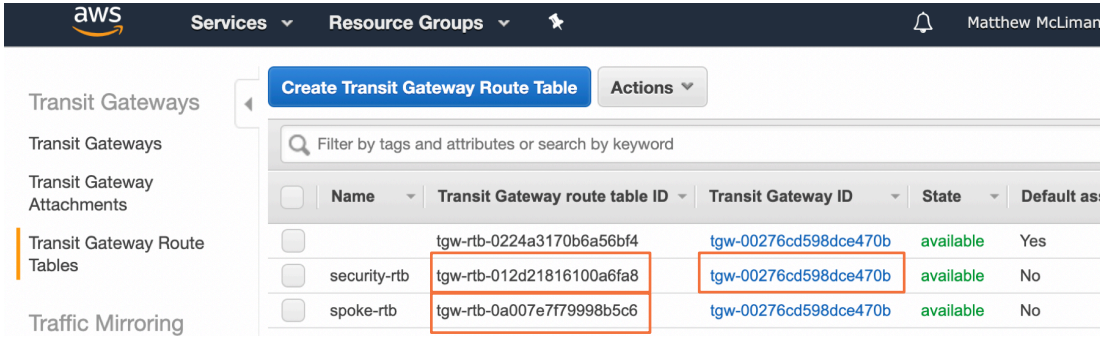
STEP 3. CREATE TRANSIT GATEWAY ROUTE TABLES

1. Go to **VPC → Transit Gateway Route Tables**
2. Create two Route Tables (1 for spoke attachments, 1 for security attachment)





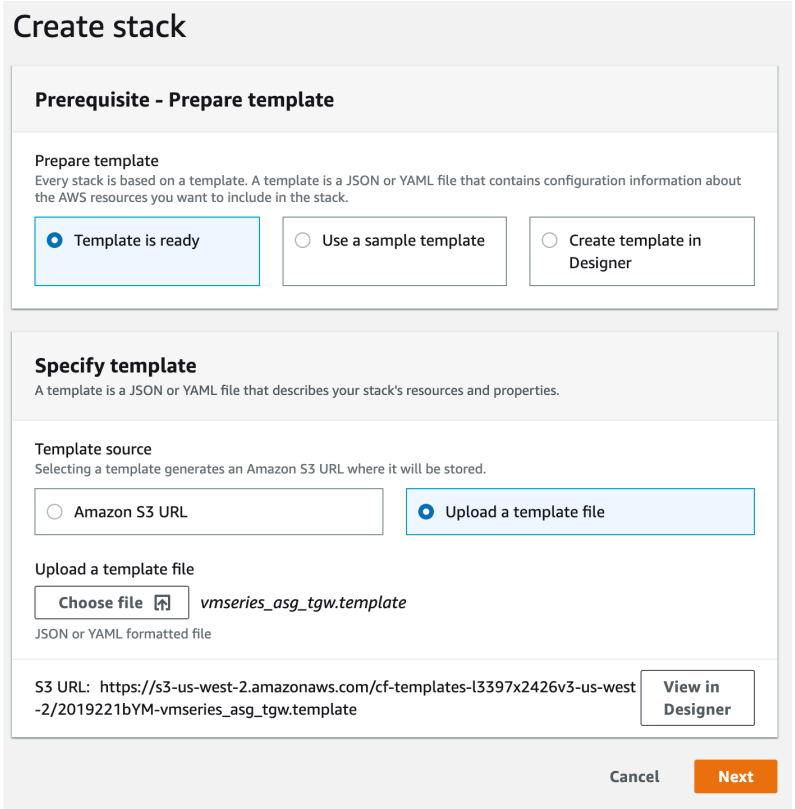
Record your TGW ID & TGW Route Table IDs



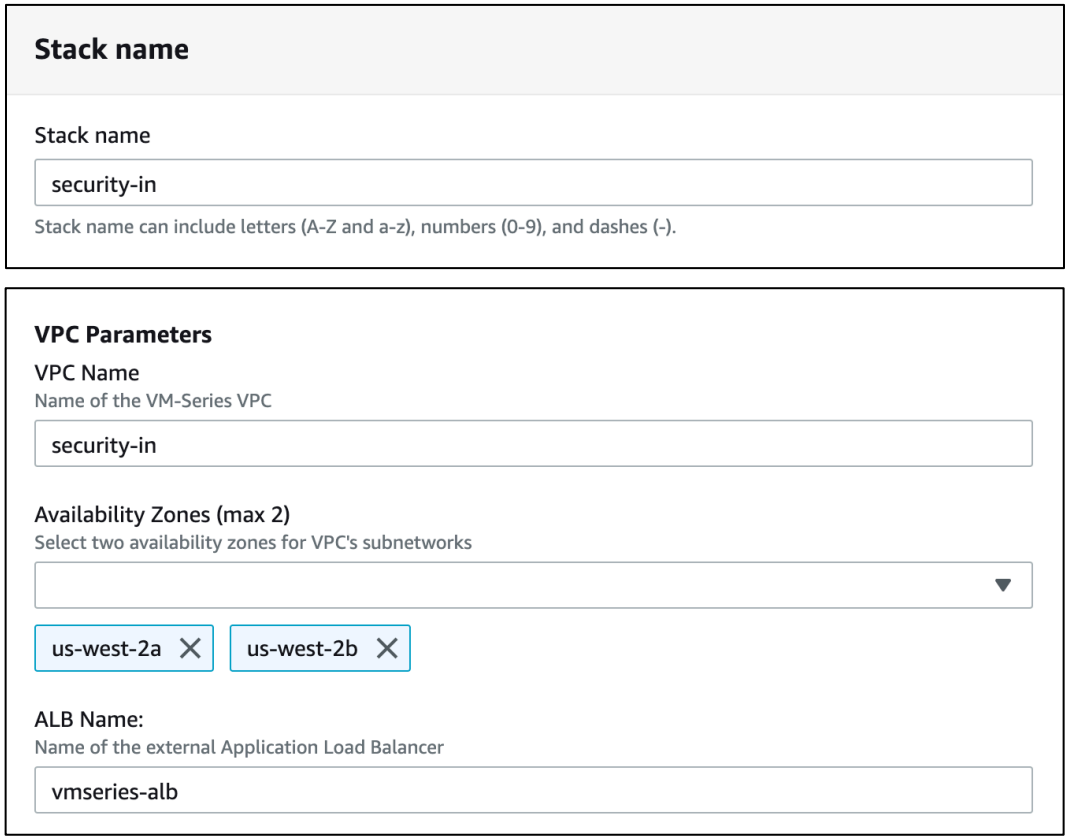
LAUNCH
VM-SERIES TEMPLATE

LAUNCH THE VM-SERIES AUTOSCALING CFT

1. Go to **CloudFormation → Create Stack**
2. Select **Upload a template file**
3. Upload the **vmseries_asg_tgw.template**



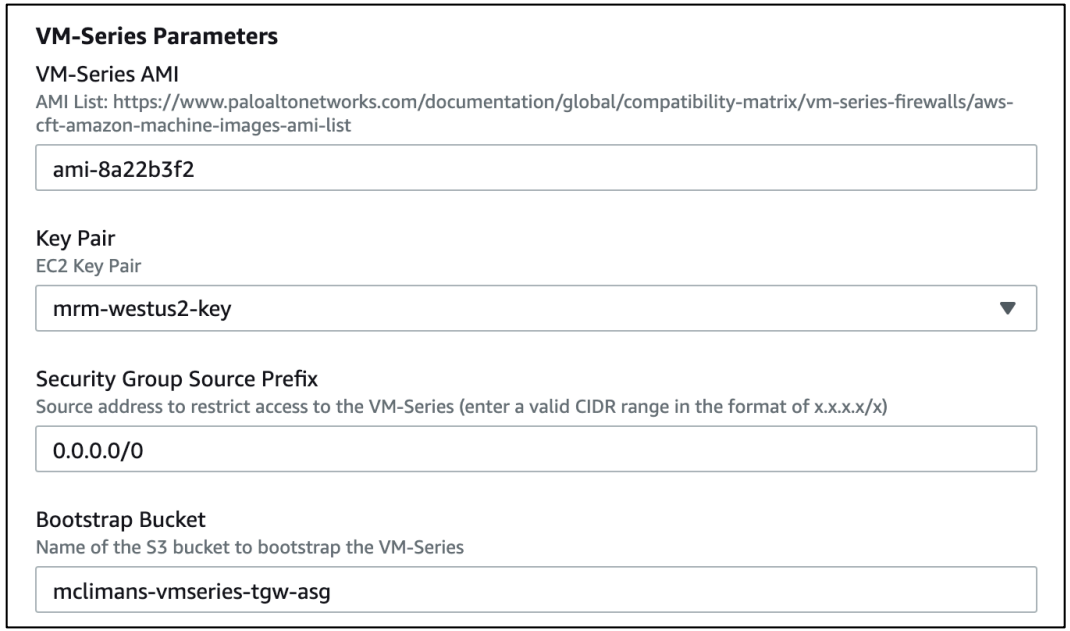
VPC Parameters



Enter name for Stack.

Select 2 Availability Zones.

VM-Series Parameters

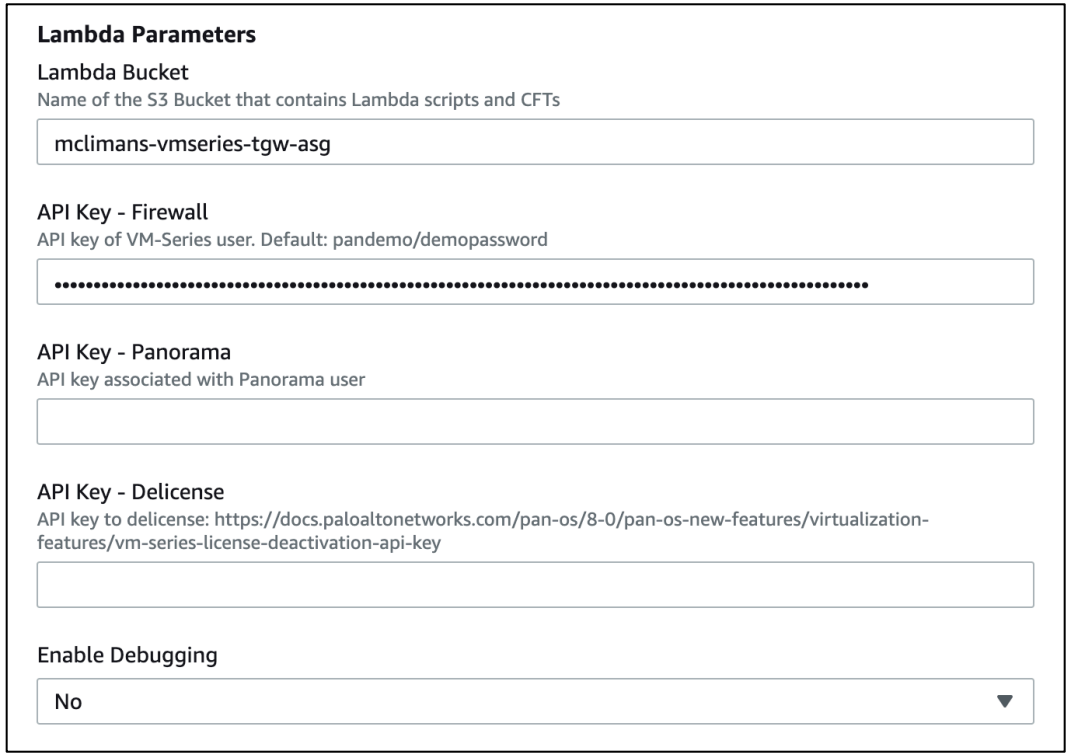


Enter the VM-Series AMI to match the license SKU, PAN-OS Version, and AWS Region

* screenshot shows: bundle1, 8.1, us-west-2

Enter the S3 Bucket name from step 1

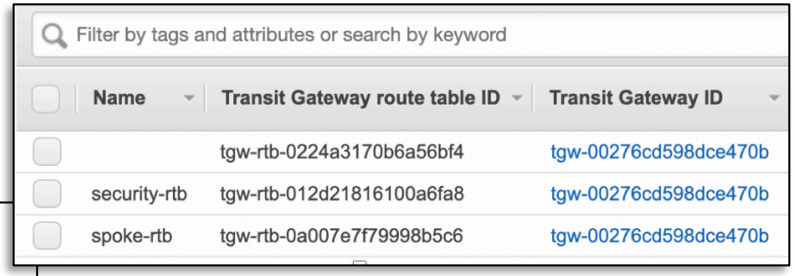
Lambda Parameters



Enter the S3 Bucket name from step 1.

If you are using the default bootstrap.xml, leave the default key. Do **not** use default bootstrap.xml for any real environments.

Transit Gateway Parameters



Transit Gateway Parameters

Transit Gateway ID:

Transit Gateway resource ID (i.e. tgw-xxxxxx)

tgw-00276cd598dce470b

Transit Gateway Route Table - TO ASSOCIATE

Transit Gateway Route Table to associate with the VM-Series VPC attachment (i.e. tgw-rtb-xxxxxx)

tgw-rtb-012d21816100a6fa8

Transit Gateway Route Table - TO PROPAGATE

Transit Gateway route table resource ID to propagate the VM-Series VPC attachment (i.e. tgw-rtb-xxxxxx)

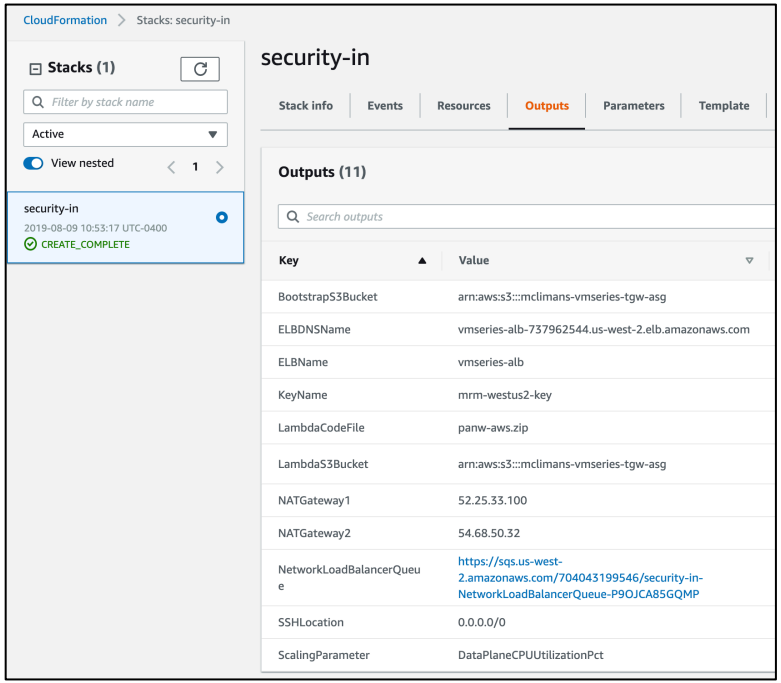
tgw-rtb-0a007e7f79998b5c6

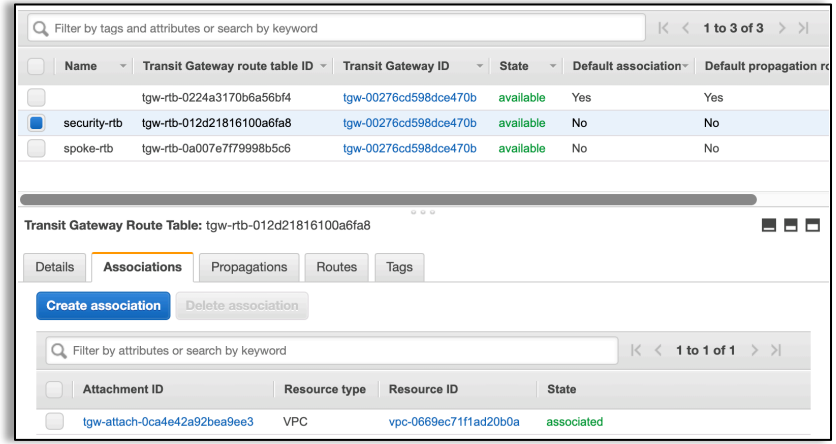
Paste TGW ID from Step 2

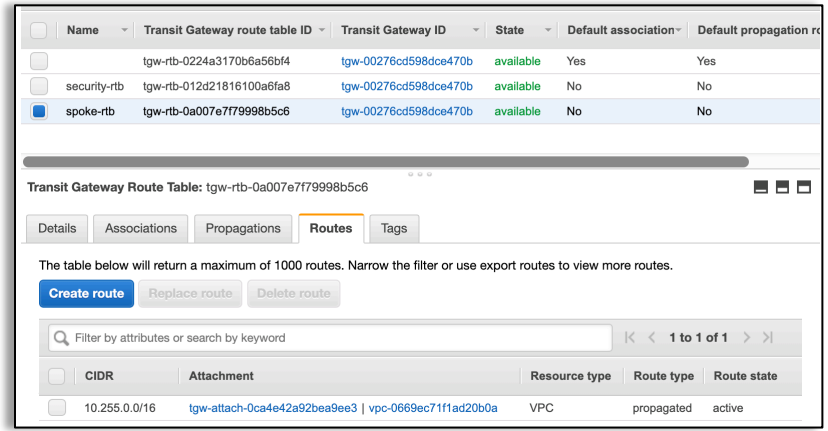
Paste Security TGW-RTB ID. This will be associated with the VM-Series VPC.

Paste the Spoke TGW-RTB. The VM-Series VPC will propagate its route to it.

Post Completion Check



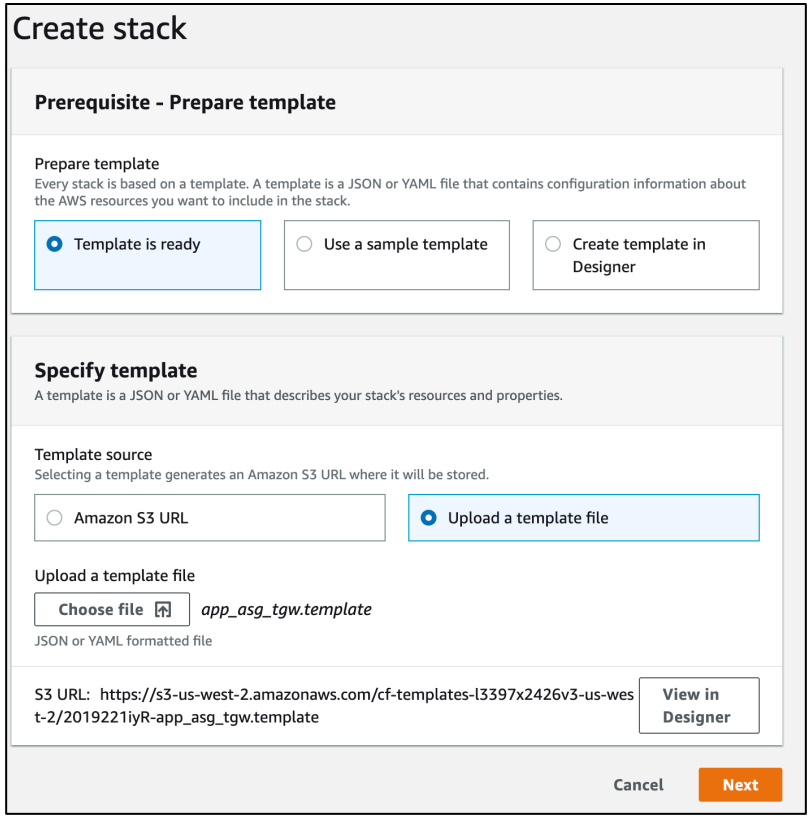




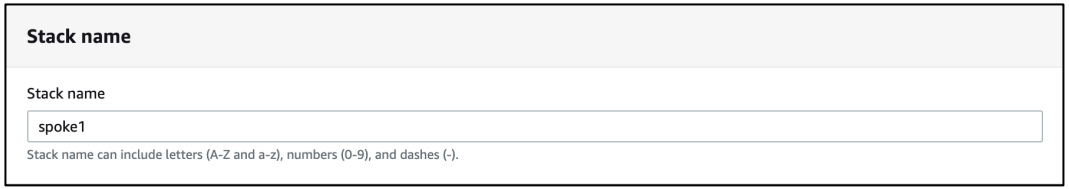
LAUNCH
APPLICATION TEMPLATE

LAUNCH THE APPLICATION CFT

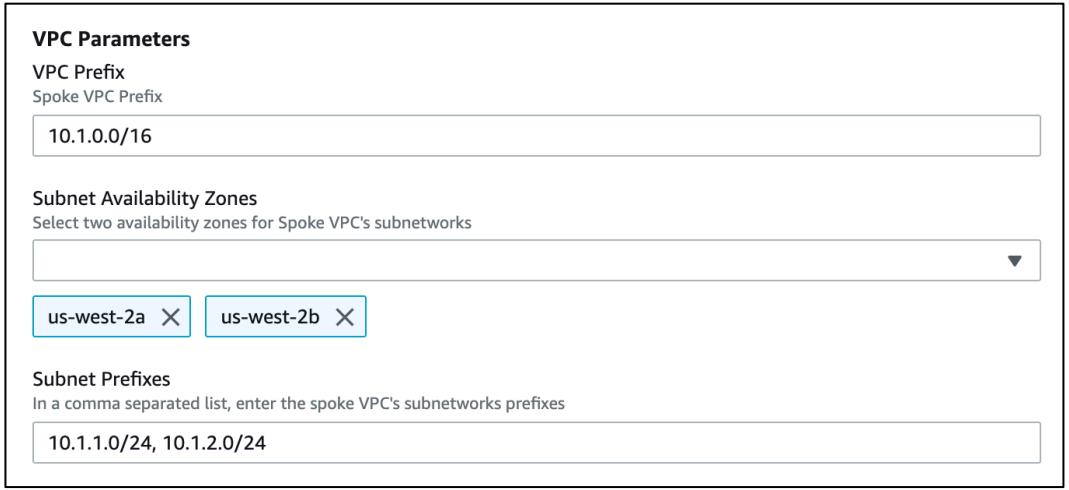
1. Go to **CloudFormation → Create Stack**
2. Select **Upload a template file**
3. Upload the **app_tgw_template.template**



VPC Parameters

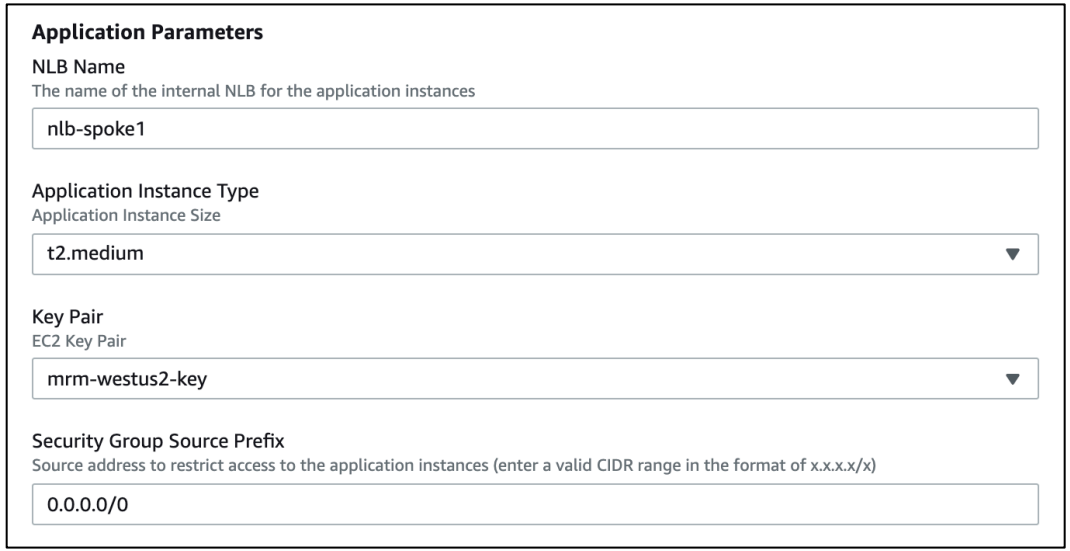


Enter name for Stack.



Select 2 Availability Zones.

Application Parameters



Name for NLB. The name cannot conflict with an existing NLB.

Select existing EC2 Key Pair.

Lambda Parameters

Lambda Parameters

Lambda Bucket

Name of the S3 Bucket that contains Lambda scripts and CFTs

mclimans-vmseries-tgw-asg

VM-Series SQS URL

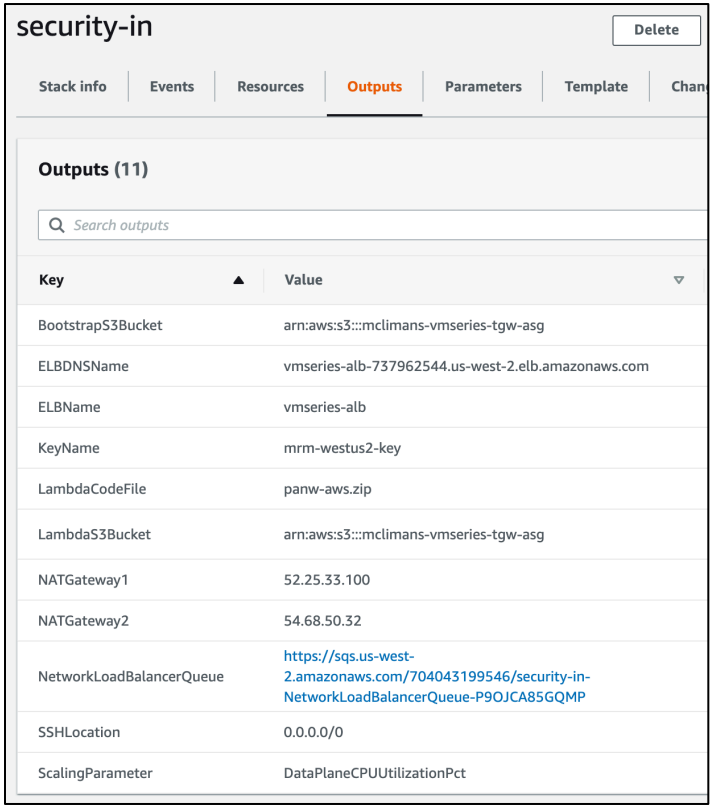
Enter the URL of the Queue (SQS) to send NLB updates

https://sqs.us-west-2.amazonaws.com/704043199546/security-in-NetworkLoadBalancerQueue-P9OJCA85GC

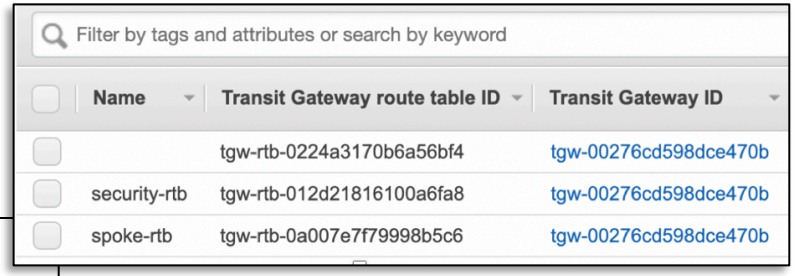
DynamoDB Table

Enter the name of the DynamoDB table

nlb_db_tbl



Transit Gateway Parameters



Transit Gateway Parameters

Transit Gateway ID

Transit Gateway resource ID (i.e. tgw-xxxxxx)

tgw-00276cd598dce470b

Transit Gateway Route Table - SPOKE

Transit Gateway Route Table to associate with the spoke VPC attachment (i.e. tgw-rtb-xxxxxx)

tgw-rtb-0a007e7f79998b5c6

Transit Gateway Route Table - SECURITY

Transit Gateway route table resource ID to propagate the spoke VPC attachment (i.e. tgw-rtb-xxxxxx)

tgw-rtb-012d21816100a6fa8

Paste TGW ID from Step 2

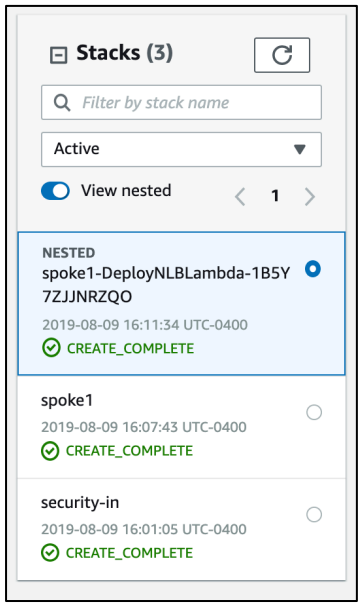
Paste the Spoke TGW-RTB. The Spoke VPC will be associated with it.

Paste Security TGW-RTB ID. The Spoke VPC will propagate its route to it.

Test Deployment

TEST DEPLOYMENT

Once deployment is complete, copy the DNS record of the public ELB and place it in a web-browser.



vmseries-alb-737962544.us-west-2.elb.amazonaws.com

SOURCE & DESTINATION ADDRESSES
INTERVAL: 0.00026297569274902
SOURCE IP: 68.0.234.87
LOCAL IP: ip-10-1-2-195
VM NAME: ip-10-1-2-195

HEADER INFORMATION
HTTP_X_FORWARDED_FOR: 68.0.234.87
HTTP_X_FORWARDED_PROTO: http
HTTP_X_FORWARDED_PORT: 80
HTTP_HOST: vmseries-alb-1281801741.us-west-2.elb.amazonaws.com
HTTP_X_AMZN_TRACE_ID: Root=1-5d4dd782-1198bd7cf4b302b0a7c235fc
HTTP_CACHE_CONTROL: max-age=0
HTTP_UPGRADE_INSECURE_REQUESTS: 1
HTTP_USER_AGENT: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_14_5) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/75.0.3770.142 Safari/537.36
HTTP_ACCEPT: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3
HTTP_ACCEPT_ENCODING: gzip, deflate
HTTP_ACCEPT_LANGUAGE: en-US,en;q=0.9

Web-App-2

SOURCE & DESTINATION ADDRESSES
INTERVAL: 0.00023698806762695
SOURCE IP: 68.0.234.87
LOCAL IP: ip-10-1-1-62
VM NAME: ip-10-1-1-62

HEADER INFORMATION
HTTP_X_FORWARDED_FOR: 68.0.234.87
HTTP_X_FORWARDED_PROTO: http
HTTP_X_FORWARDED_PORT: 80
HTTP_HOST: vmseries-alb-1281801741.us-west-2.elb.amazonaws.com
HTTP_X_AMZN_TRACE_ID: Root=1-5d4dd803-3171870cc237431cd045dd8c
HTTP_CACHE_CONTROL: max-age=0
HTTP_UPGRADE_INSECURE_REQUESTS: 1
HTTP_USER_AGENT: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_14_5) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/75.0.3770.142 Safari/537.36
HTTP_ACCEPT: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3
HTTP_ACCEPT_ENCODING: gzip, deflate
HTTP_ACCEPT_LANGUAGE: en-US,en;q=0.9

Web-App-1

