

**Deploying VM Series with Autoscale via VPN Attachments to a Transit Gateway**

[http://www.paloaltonetworks.com](http://www.paloaltonetworks.com/)

© 2019 Palo Alto Networks. Proprietary and Confidential

Table of Contents

[Version History 3](#_Toc536788186)

[1. About 4](#_Toc536788187)

[2. Topology 4](#_Toc536788188)

[3. Support Policy 6](#_Toc536788189)

[4. Prerequisites 6](#_Toc536788190)

[5. Create S3 Buckets for Security VPC 6](#_Toc536788191)

[6. Deploy the Transit Gateway Stack 9](#_Toc536788192)

[9. When everything works 13](#_Toc536788193)

[10. Accessing the Firewall 15](#_Toc536788194)

[11. Cleanup 15](#_Toc536788195)

# Version History

|  |  |
| --- | --- |
| **Version number** | **Comments** |
| **1.0** | Initial GitHub check-in |
| **1.1** | Fixed issue with lambda files |

# About

This document will explain how to deploy an AWS Transit Gateway with the VM-Series on AWS. A Transit Gateway uses a hub and spoke architecture that allows security teams to centralize secure connectivity for VPC-to-VPC, VPC to corporate and VPC to the internet communications.

AWS Transit Gateway is a service that enables customers to connect their Amazon Virtual Private Clouds (VPCs) and their on-premises networks to a single gateway. As you grow the number of workloads running on AWS, you need to be able to scale your networks across multiple accounts and Amazon VPCs to keep up with the growth. Today, you can connect pairs of Amazon VPCs using peering. However, managing point-to-point connectivity across many Amazon VPCs, without the ability to centrally manage the connectivity policies, can be operationally costly and cumbersome. For on-premises connectivity, you need to attach your AWS VPN to each individual Amazon VPC. This solution can be time consuming to build and hard to manage when the number of VPCs grows into the hundreds.

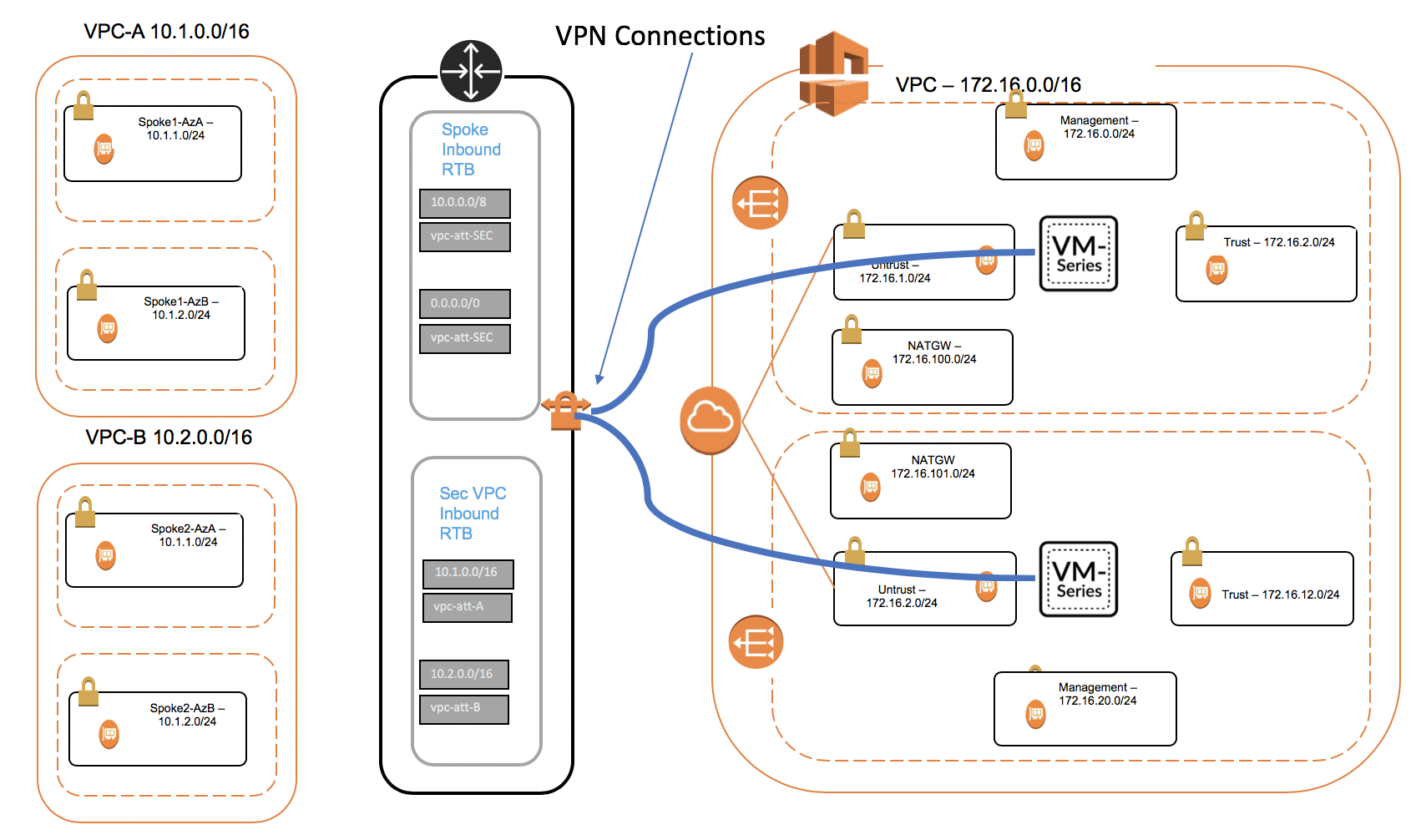
With an AWS Transit Gateway, you only have to create and manage a single connection from the central gateway in to each VPC, on-premises data center, or remote office across your network. Transit Gateway acts as a hub that controls how traffic is routed among all the connected networks which act like spokes. This hub and spoke model simplifies management and reduces operational costs because each network only connects to the Transit Gateway and not to every other network. Any new VPC is simply connected to the Transit Gateway and is then automatically available to every other network that is connected to the Transit Gateway. This ease of connectivity makes it easy to scale your network as you grow.

More information on the AWS Transit Gateway can be found here: <https://aws.amazon.com/transit-gateway/>

# Topology

The template will deploy a security VPC with firewalls that will connect to an existing transit gateway via VPN attachments. The firewalls advertise a default route to the transit gateway via BGP over an IPSec connection:





# Support Policy

This solution 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.

# Prerequisites

Here are the prerequisites required to successfully launch this template:

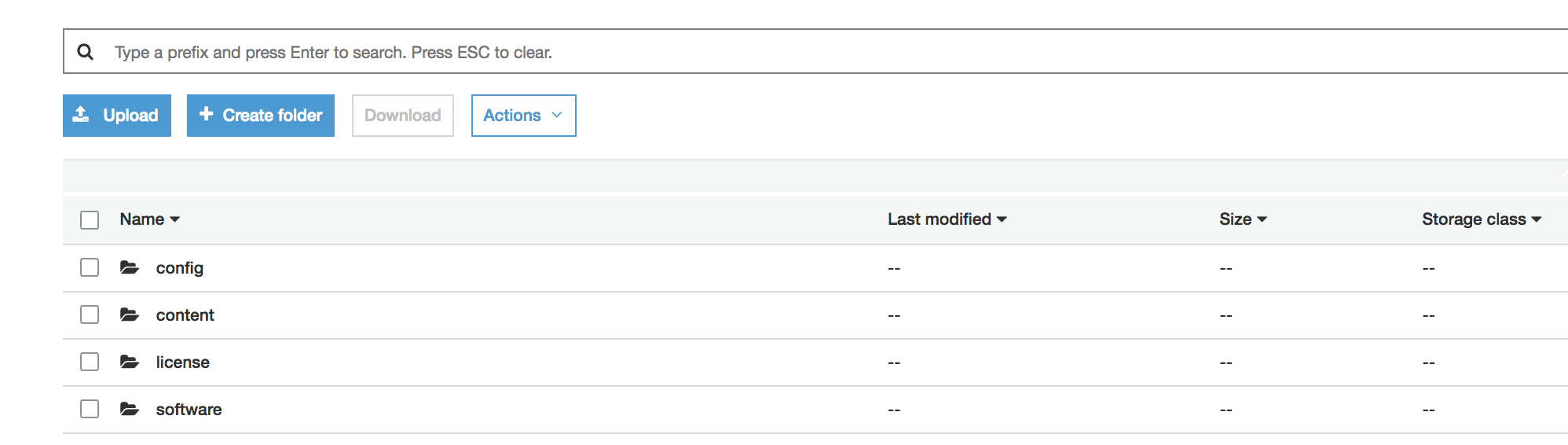
* 1. AWS account
  2. Clone or download the files from the following GitHub repository on to your local machine:

<https://github.com/wwce/aws-cft/tree/master/transitgateway-demo-v2>

# Create S3 Buckets for Autoscale Security VPC

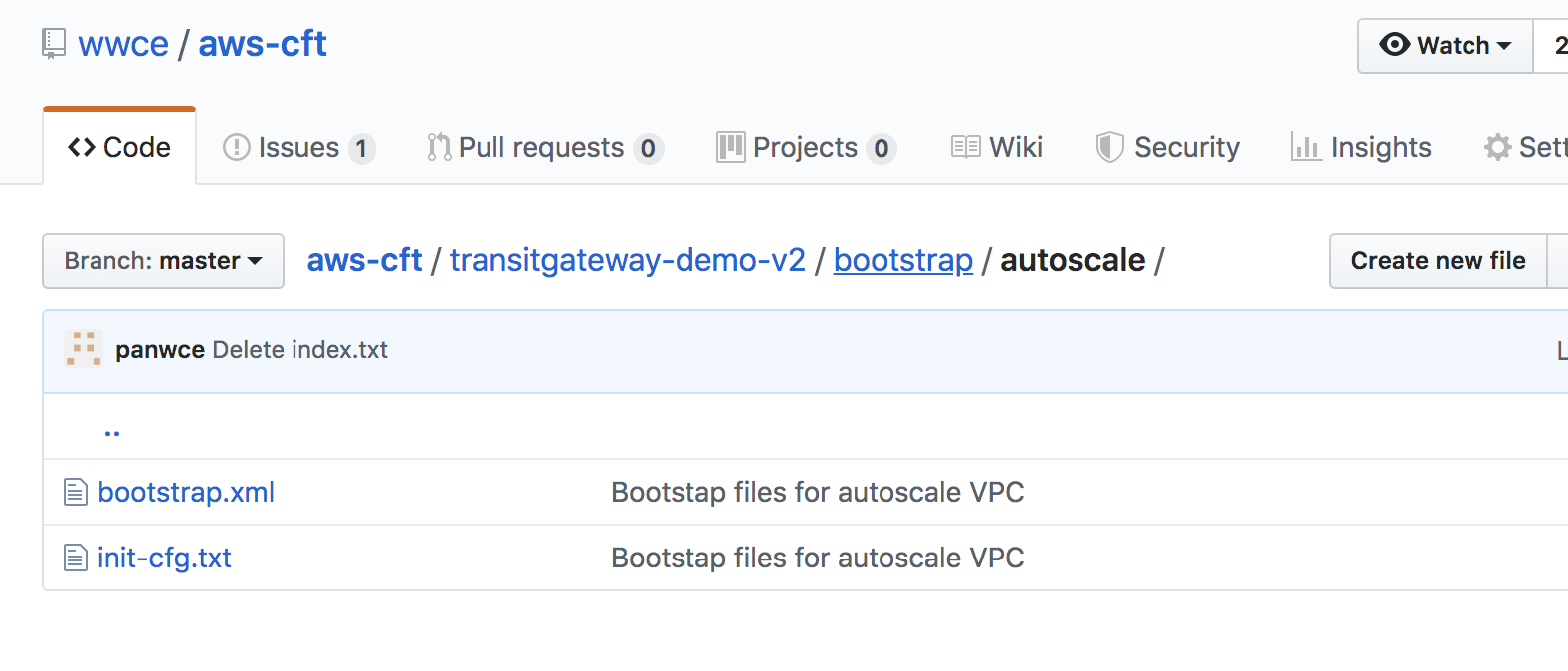
In the AWS S3 console, create an S3 bucket with config, content, license and software folders.

All the folders must exist and in lowercase.



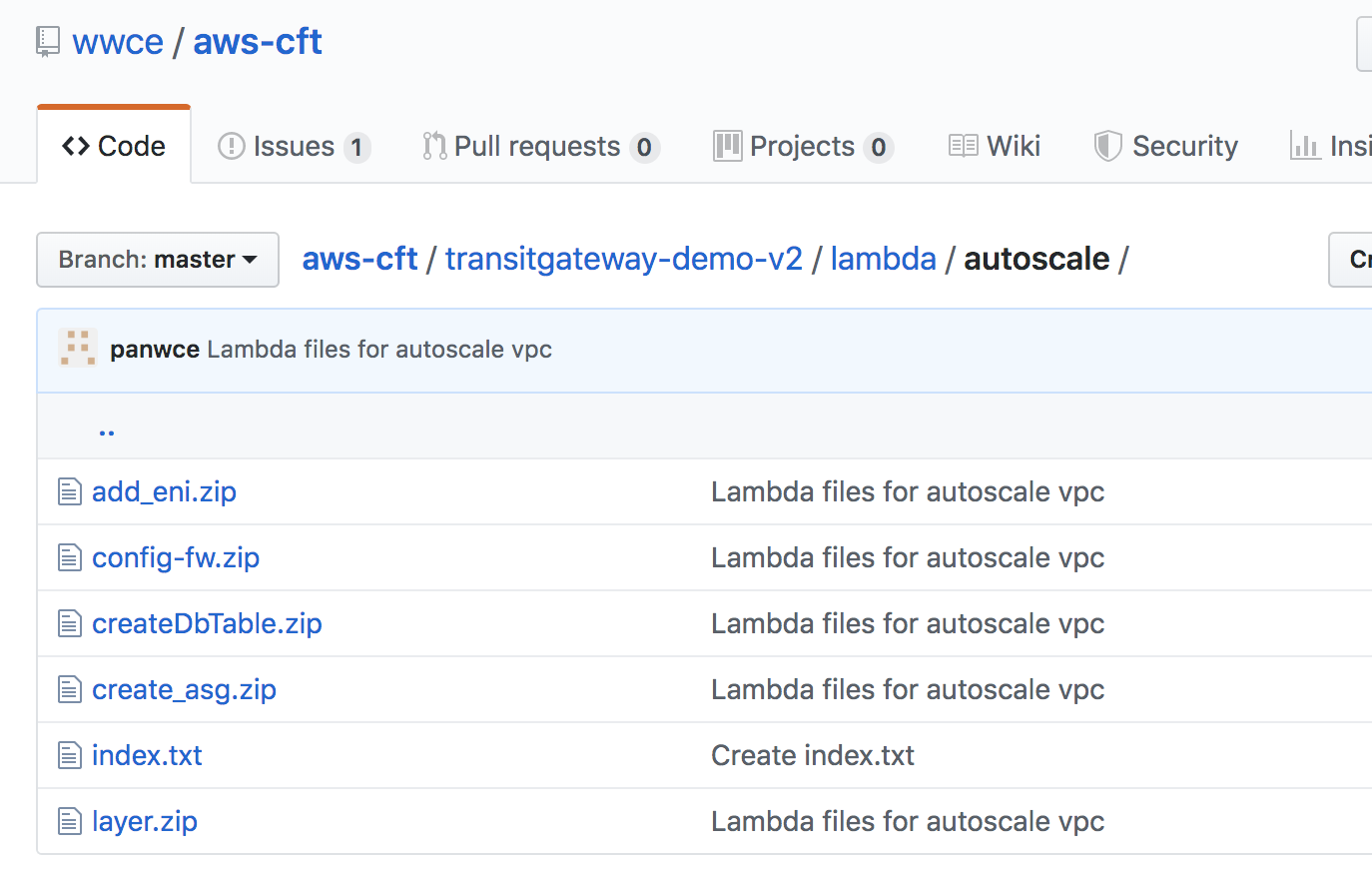
Copy the init-cfg.txt and bootstrap.xml files from the cloned ./bootstrap/autoscale folder to the config folder

NOTE: These are not the same bootstrap files that are used in the direct attached deployment. If you use those files the deployment will fail.



Either create another S3 bucket or use the existing bucket and add the lambda zip files to the folder.

All the files shown below must be present and in zip format.



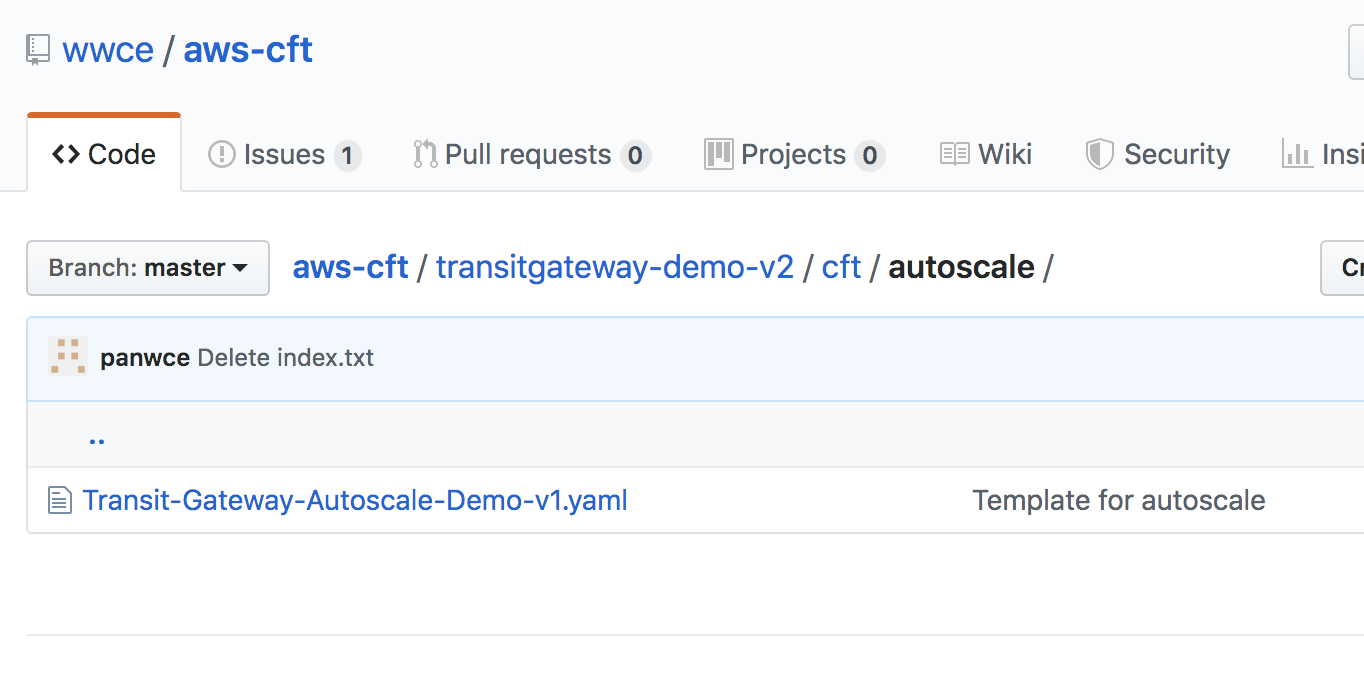
### Note: The buckets need to be in the same region in which you will deploy the Transit Gateway template.

# Deploy the Transit Gateway Direct Attach Stack

In the AWS CloudFormation console create a new stack and select the

Transit-Gateway-Autoscale-Demo-v1.yaml template

and fill in the parameters



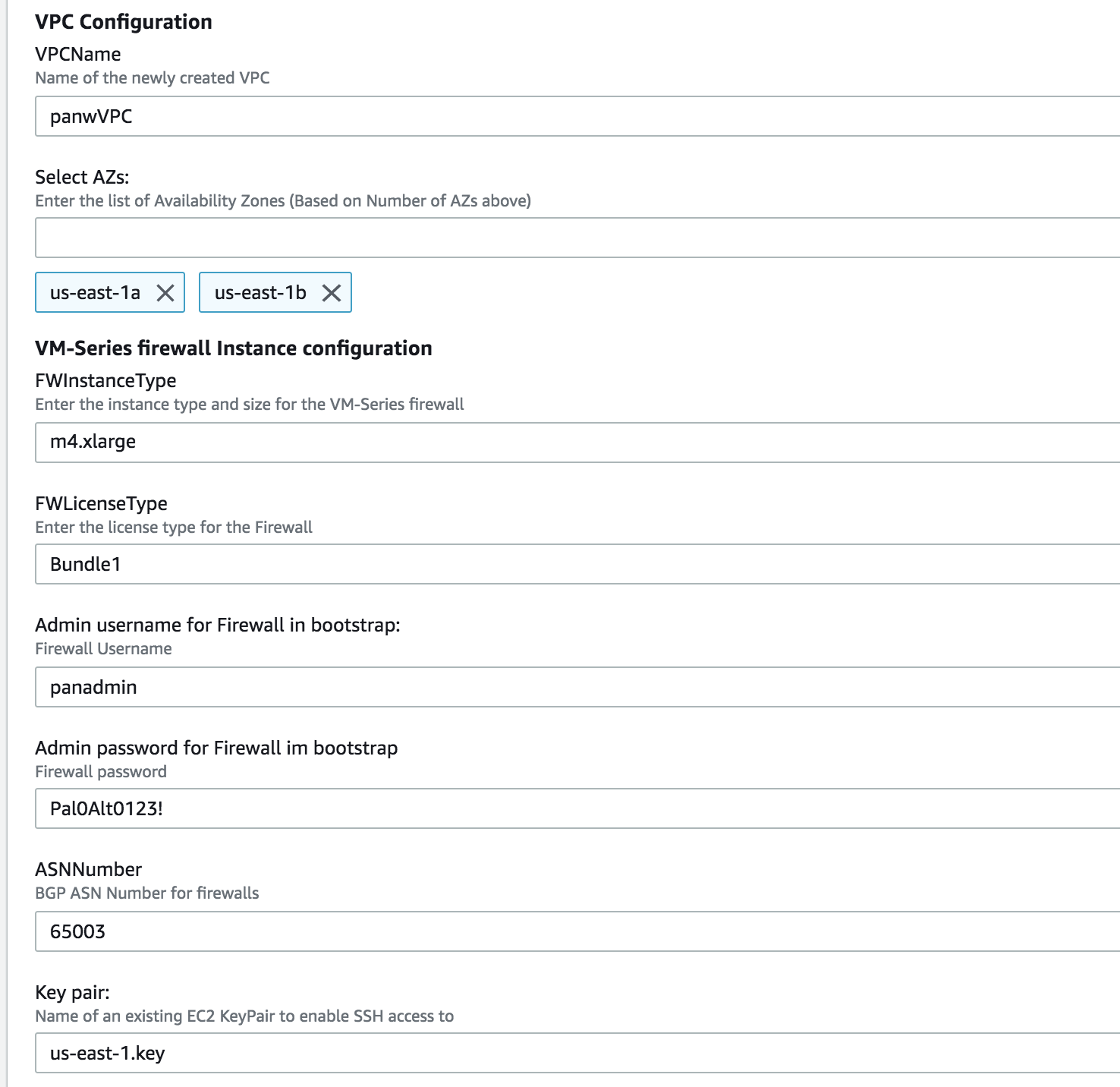
* 1. VPC Configuration

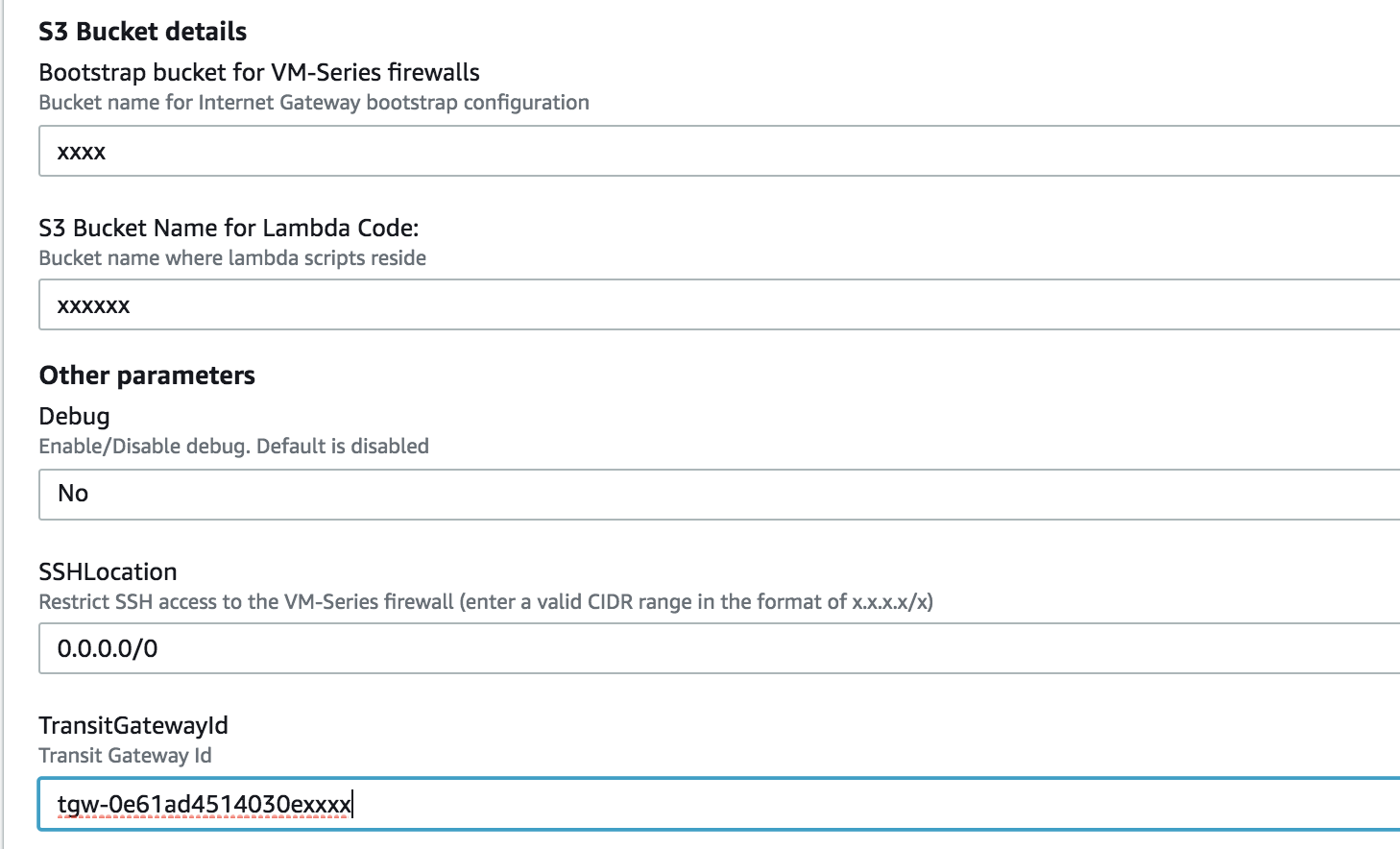
Select the number of VPCs required. Two is recommended for most deployments

The firewall admin name and password should be used unless you have modified the bootstrap.xml file. Once the firewall has been configured it is recommended that the firewalls are connected to Panorama and the account credentials modified or deleted. In a production environment it is recommended that all credentials are stored in a secure vault.

Any private ASN number can be used apart from the AWS default of 64512.

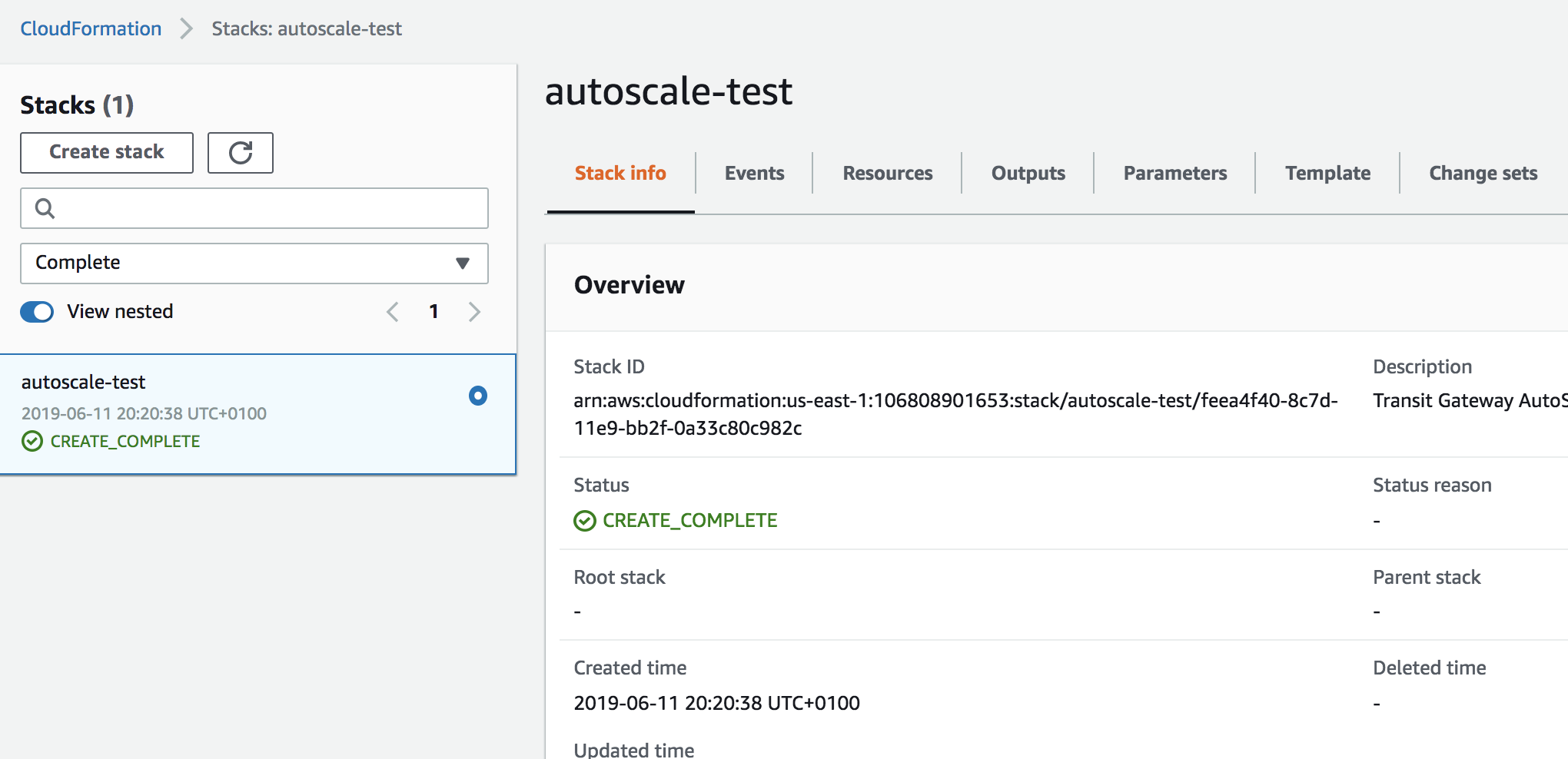
In most cases the same lambda bucket can be used for firewall bootstrap and for the lambda code.





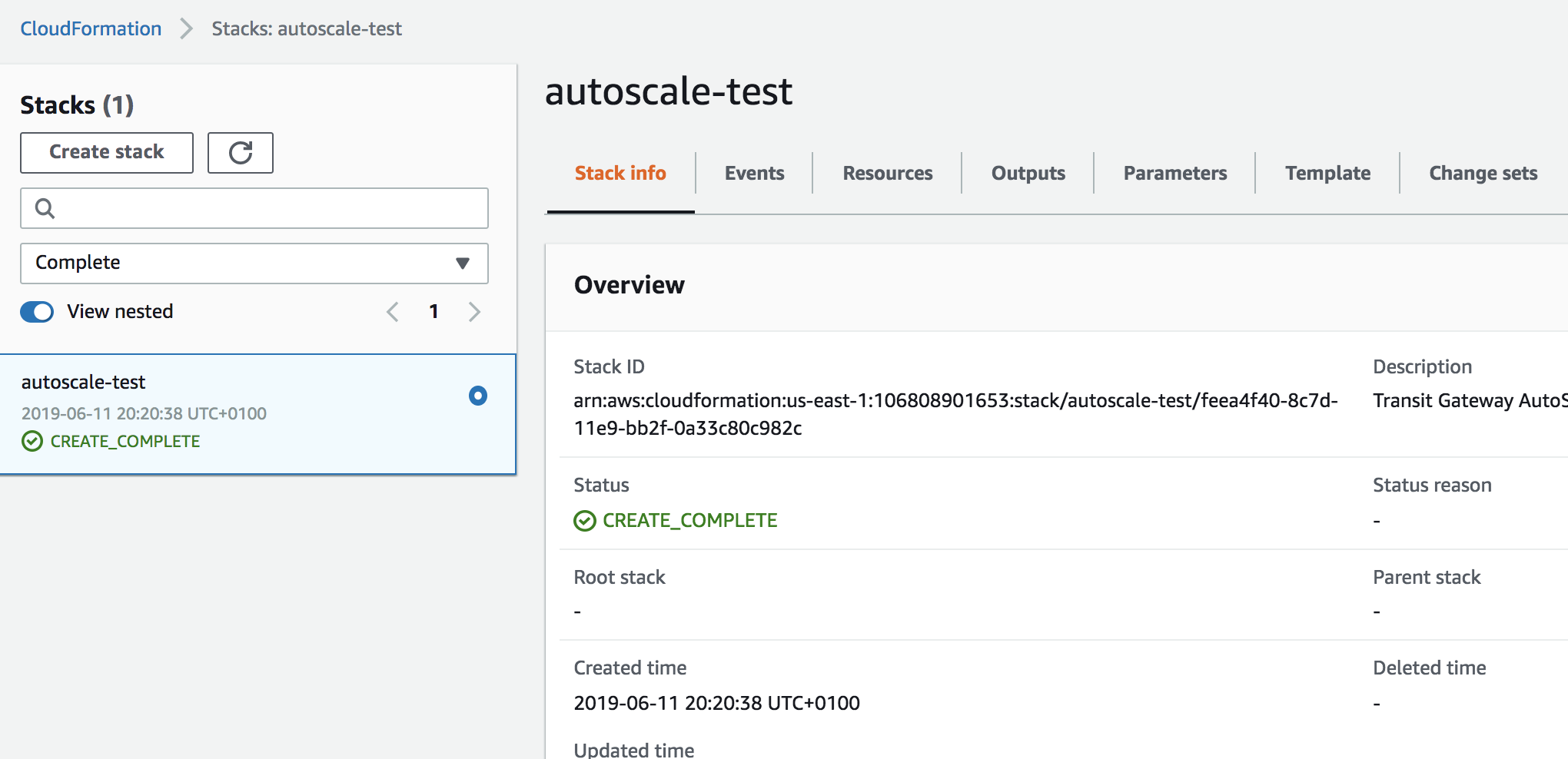
Click through to kick of stack creation.

You should see a stack create complete when the autoscale template has been successfully initialized.



# When everything works

.You should see a “create\_complete” status if the template had deployed correctly



The template will deploy and autoscale group and launch configuration with the “Desired” count set to zero. You can then add a firewall when you are ready

The template creates an autoscale group with a Desired Capacity and minimum of 0. When you wish to deploy the firewalls edit the autoscale configuration and modify these values match your desired number of firewalls. If you are deploying more that two firewalls you may be required to increase the resource limits on your account via AWS support.

