Aviatrix FQDN Egress Filtering on the AWS Cloud

Quick Start Reference Deployment

July 2018

Jing Zhou, Sunil Kishen — Aviatrix Systems, Inc.
Shivansh Singh — Amazon Web Services

Overview.................................................................................................................................2
Aviatrix Egress Filtering on AWS.........................................................................................2
Benefits of Aviatrix Egress Filtering ..................................................................................3
Costs and Licenses................................................................................................................4
Architecture.........................................................................................................................5
Quick Start Components .....................................................................................................6
Additional Functionality .......................................................................................................6
Prerequisites ..........................................................................................................................7
Specialized Knowledge.........................................................................................................7
License Requirements............................................................................................................7
Technical Requirements.......................................................................................................7
Deployment Options.............................................................................................................8
Deployment Steps................................................................................................................8
Step 1. Prepare Your AWS Account......................................................................................8
Step 2. Subscribe to the Aviatrix AMI ..................................................................................9
Step 3. Launch the Quick Start ............................................................................................9
Step 4. Performing the Initial Setup of the Aviatrix Controller ............................................14
Step 5. Create a Primary Access Account .........................................................................16
Step 6: Deploy Egress Filtering.................................................................................................................... 17

Best Practices Using Aviatrix on AWS............................................................................................................ 20

Gateway Sizing.................................................................................................................................................. 20

Backups............................................................................................................................................................ 20

Security............................................................................................................................................................ 21

Troubleshooting.............................................................................................................................................. 21

Support........................................................................................................................................................... 22

GitHub Repository........................................................................................................................................... 22

Additional Resources ....................................................................................................................................... 22

Document Revisions ...................................................................................................................................... 22

This Quick Start deployment guide was created by Aviatrix Systems in collaboration with Amazon Web Services (AWS). Aviatrix Systems is an AWS Advanced Technology and Networking Competency Partner.

**Quick Starts** are automated reference deployments that use AWS CloudFormation templates to deploy key technologies on AWS, following AWS best practices.

**Overview**

This Quick Start reference deployment guide provides step-by-step instructions for deploying the Aviatrix Fully Qualified Domain Name (FQDN) Egress Filtering service on the AWS Cloud.

This Quick Start uses AWS APIs to automatically deploy an Aviatrix Controller for enabling the [Egress Filtering service](#) in a new or existing virtual private cloud (VPC). You can connect to VPCs in the AWS Cloud with enhanced security, and access your Amazon Elastic Compute Cloud (Amazon EC2) instances, applications, and services.

**Aviatrix Egress Filtering on AWS**

AWS offers you different methods for helping to secure resources in Amazon Virtual Private Cloud (Amazon VPC) networks. One important security measure is to effectively control inbound (ingress) and outbound (egress) VPC network traffic, so that you can distinguish between legitimate and illegitimate requests.
Workloads in AWS are typically limited to applications and services where the destination of outbound traffic is known. For example, a reporting application might connect to google.com for authentication, and might also query salesforce.com for data. Another application might connect with a hosted database service or a file sharing service.

Specifying policies by IP address isn't practical for these types of services because the domain names can be translated to many different IP addresses. Also, security groups for EC2 instances have to be managed on each server, and there's a strict limit on the number of entries that can be added.

For these environments, filtering outbound traffic by an expected list of domain names is more effective for securing egress traffic from a VPC. The hostnames of these services are typically known at deployment time. This because the list of hosts that an application needs to access is a small list that does not change often. Plus, hostnames rarely change, whereas IP addresses may change frequently.

Consider any company that is trying to meet the stringent requirements of compliance standards such as Payment Card Industry (PCI) and Health Insurance Portability and Accountability Act (HIPAA). These standards may require administrators to deny certain outbound internet traffic. Maintaining a list of IP addresses and updating security groups for multiple servers isn't practical and puts additional burden on resources at deployment and audit times. Instead, a better approach is to maintain a list of allowed domain names in one place where administrators, auditors, and others can see exactly what is allowed. Rules can automatically be maintained and deployed to VPCs from a central controller.

For other best practices and common approaches for controlling egress traffic as part of a holistic network security strategy, see the AWS Answers article about [Controlling VPC Egress Traffic](https://aws.amazon.com/answers/questions/ask/).  

Once you’ve used this Quick Start to deploy the Aviatrix Controller in one of your VPCs, the Egress Security wizard in the controller helps you deploy and configure Aviatrix gateways for egress security and filtering.

For more information, see [Aviatrix Control Filter](https://aws.amazon.com/answers/questions/ask/), [Egress FQDN Discovery](https://aws.amazon.com/answers/questions/ask/), and [Egress FQDN View Log](https://aws.amazon.com/answers/questions/ask/) in the Aviatrix documentation.

**Benefits of Aviatrix Egress Filtering**

Aviatrix Egress Filtering provides the following benefits:

- **Cloud-native design.** With this design, cloud teams can instantly assign policies to one or hundreds of VPCs.
- **Reduced AWS costs.** To help reduce the costs of cloud operations, you can centrally deploy Aviatrix Egress Security in a shared-services VPC by using a t2.micro instance.

- **Centralized management console.** With the Aviatrix point-and-click interface, engineers and non-engineers can configure and monitor security and policies from a single console.

- **Security-policy tagging.** Engineers and operations staff can combine a variety of network attributes or security rules to a custom tag to create and apply policies to your cloud environment.

- **Auditing of security events.** It’s easy to integrate security policies and events with Splunk, Sumo Logic, Datadog, and other tools to standardize reporting and event correlation.

### Costs and Licenses

You are responsible for the cost of the AWS services used while running this Quick Start reference deployment. There is no additional cost for using this Quick Start.

The AWS CloudFormation template for this Quick Start includes configuration parameters that you can customize. Some of these settings, such as instance type, will affect the cost of deployment. For cost estimates, see the pricing pages for each AWS service you will be using. Prices are subject to change.

Additionally, to protect network configuration information, the Quick Start creates a unique AWS Key Management Service (AWS KMS) customer master key (CMK), which has a low monthly cost. For details, see the [AWS KMS pricing webpage](https://aws.amazon.com/kms/pricing/).

You are also responsible for the Aviatrix license that is required to deploy Aviatrix Egress Filtering. As explained in Step 2: Subscribe to the Aviatrix AMI of the deployment steps, you subscribe to an Amazon Machine Image (AMI) for Aviatrix software in AWS Marketplace, choosing the [Aviatrix Secure Networking Platform PAYG - Metered](https://aws.amazon.com/marketplace/product/AV-012292) licensing option. This is an hourly-subscription license based on the prices listed in AWS Marketplace. With this pay-as-you-go license, you can build and scale your Egress Filtering service to any size.
Architecture

This Quick Start sets up an Aviatrix Egress Filtering service that includes the Aviatrix Controller and Aviatrix gateways in a highly available configuration. You can deploy the controller in a new VPC or use an existing VPC.

Deploying this Quick Start for a new VPC with **default parameters** builds the following Egress Filtering service in the AWS Cloud.

![Architecture Diagram](image)

**Figure 1: Aviatrix Egress Filtering architecture**

This architecture diagram shows the end-to-end solution, which includes:

- The Aviatrix Controller
- Aviatrix gateways deployed in your VPCs in high availability (HA) configuration
The Aviatrix Controller deploys the Aviatrix gateways in your VPCs and configures the egress security policies across all gateways. The Aviatrix Controller also provides a user-friendly Egress Security wizard for centrally configuring FQDN whitelists. Aviatrix Egress Filtering also includes the Egress FQDN Discovery service. This service enables you to see the external sites (URLs) that users and applications are accessing within your VPCs, which helps you configure Egress Filtering accordingly.

**Quick Start Components**

The Quick Start sets up the functional and automation components shown in Figure 2.

![Figure 2: Quick Start components of Aviatrix Egress Filtering on AWS](image)

It creates, deploys, and configures the following components and services, mapped to Figure 2:

- An EC2 instance for the Aviatrix Controller
- An Aviatrix security group (named AviatrixSecurityGroup)
- An Elastic IP address assigned to the Aviatrix Controller
- An Aviatrix IAM EC2 role and attached policy
- An Aviatrix IAM App role and attached policy
- AWS Key Management Service (AWS KMS)

**Additional Functionality**

After you deploy the Quick Start, you can use the Egress Security wizard to enable Egress Filtering. See [Configuring Egress Security](#) for detailed documentation.
Prerequisites

Specialized Knowledge

Before you deploy this Quick Start, we recommend that you become familiar with the following AWS services. (If you are new to AWS, see Getting Started with AWS.) You don’t need advanced networking skills to deploy and maintain the Aviatrix environment on AWS.

- Amazon Elastic Compute Cloud (Amazon EC2)
- Amazon Simple Queue Service (Amazon SQS)
- Amazon Virtual Private Cloud (Amazon VPC)

License Requirements

By default, this Quick Start deploys an Aviatrix Controller with Metered license included in the AWS Marketplace AMI for Aviatrix Secure Networking Platform PAYG - Metered

Technical Requirements

AWS Accounts

You will need an AWS account to deploy this Quick Start. Once the Quick Start deploys the Aviatrix Controller, you can use it to add one or more AWS accounts, and to connect spoke VPCs in those AWS accounts. You can also connect spoke VPCs across AWS Regions.

For more information about how to use the Aviatrix Controller to add accounts, see the Aviatrix Onboarding and Account FAQs documentation.

IAM Requirements

This Quick Start requires the following IAM roles to be created in the primary AWS account:

- An Aviatrix role for Amazon EC2 (aviatrix-role-ec2) with a corresponding role policy (aviatrix-assume-role-policy). See policy details.
- An Aviatrix role for apps (aviatrix-role-app) with a corresponding role policy (aviatrix-app-policy). See policy details.
You can configure the IAM roles for the primary AWS account in one of the following ways:

- If this is the first time you’re launching the Aviatrix Controller, this Quick Start creates the required IAM roles. See Quick Start Deployment Option 1 and Option 2.
- If the required IAM roles already exist, select `aviatrix-role-ec2` in the Quick Start Deployment Option 1 and Option 2.

**Important** If you have existing Aviatrix IAM roles, make sure they are up to date by checking the preceding links for policy details.

### Deployment Options

This Quick Start provides two deployment options:

- **Deploy Aviatrix into a new VPC** (end-to-end deployment). This option builds a new AWS environment consisting of a VPC, subnets, internet gateway, default route, and other infrastructure components, and then deploys an Aviatrix Controller.
- **Deploy Aviatrix into an existing VPC**. This option provisions an Aviatrix Controller into an existing VPC.

The Quick Start provides separate templates for these options. It also lets you configure CIDR blocks, instance types, and Aviatrix settings, as discussed later in this guide.

**Note** The Aviatrix Controller is normally deployed in a shared-services VPC where your DevOps and management tools and services are hosted.

### Deployment Steps

**Step 1. Prepare Your AWS Account**

1. If you don’t already have an AWS account, create one at [https://aws.amazon.com](https://aws.amazon.com) by following the on-screen instructions.
2. Use the region selector in the navigation bar to choose the AWS Region where you want to deploy the Aviatrix Egress Filtering service on AWS.
3. Create a key pair in your preferred region.
4. If necessary, request a service limit increase for the EC2 instance type that you want to use for the Aviatrix Controller (by default, t2.large). You might need to do this if you already have an existing deployment that uses these instance types, and you think you might exceed the default limit with this deployment.
Step 2. Subscribe to the Aviatrix AMI


2. Open the page for Aviatrix Secure Networking Platform PAYG - Metered. For more information about this option, see License Requirements earlier in this guide.

3. Choose Continue to Subscribe, as shown in Figure 3.

![Figure 3: Subscribing to the AMI, with the required license](image)

4. On the Subscribe to this software page, read the license agreement, and then choose Accept Terms, as shown in Figure 4.

![Figure 4: Subscribing to the AMI—Accept Terms](image)

**Important** After you’ve finished subscribing in step 4, do not choose Continue to Configuration. The Quick Start will handle this.

Step 3. Launch the Quick Start

**Note** You are responsible for the cost of the AWS services used while running this Quick Start reference deployment. There is no additional cost for using this Quick
Start. For full details, see the pricing pages for each AWS service you will be using in this Quick Start. Prices are subject to change.

1. Choose one of the following options to launch the AWS CloudFormation template into your AWS account. For help choosing an option, see deployment options earlier in this guide.

   - **Option 1**
     - Deploy the Aviatrix Controller into a new VPC on AWS
     - Launch

   - **Option 2**
     - Deploy the Aviatrix Controller into an existing VPC on AWS
     - Launch

   This deployment takes about 10 minutes to complete.

2. Check the region that’s displayed in the upper-right corner of the navigation bar, and change it if necessary. *This is where the network infrastructure for Aviatrix Egress Filtering will be built*. The template is launched in the US East (N. Virginia) Region by default.

3. On the **Select Template** page, keep the default setting for the template URL, and then choose **Next**.

4. On the **Specify Details** page, the stack name field is pre-populated; change it if needed. Review the parameters for the template. Provide values for the parameters that require input. For all other parameters, review the default settings and customize them as necessary. When you finish reviewing and customizing the parameters, choose **Next**.

5. In the following tables, parameters are listed by category and described separately for the two deployment options:
   - [Parameters for deploying Aviatrix Controller into a new VPC](#)
   - [Parameters for deploying Aviatrix Controller into an existing VPC](#)

   - **Option 1: Parameters for deploying Aviatrix Controller into a new VPC**
     - View template
Network Configuration:

<table>
<thead>
<tr>
<th>Parameter label (name)</th>
<th>Default</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>VPC CIDR (VPCCIDR)</td>
<td>10.0.0.0/16</td>
<td>The CIDR block for the VPC.</td>
</tr>
<tr>
<td>Public Subnet 1 CIDR (PublicSubnet1CIDR)</td>
<td>10.0.10.0/24</td>
<td>The CIDR block for the public (DMZ) subnet located in Availability Zone 1. This is where the Aviatrix Controller will be deployed.</td>
</tr>
<tr>
<td>Public Subnet 2 CIDR (PublicSubnet2CIDR)</td>
<td>10.0.20.0/24</td>
<td>The CIDR block for the public (DMZ) subnet located in Availability Zone 2. This is where the high availability hub gateway will be deployed.</td>
</tr>
<tr>
<td>Availability Zones (AvailabilityZones)</td>
<td>Requires input</td>
<td>The list of Availability Zones to use for the subnets in the VPC. The Quick Start uses two Availability Zones from your list and preserves the logical order you specify.</td>
</tr>
</tbody>
</table>

Amazon EC2 Configuration:

<table>
<thead>
<tr>
<th>Parameter label (name)</th>
<th>Default</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Key Pair (KeyNameParam)</td>
<td>Requires input</td>
<td>A public/private key pair, which allows you to connect securely to the Aviatrix Controller instance after it launches. When you created an AWS account, this is the key pair you created in your preferred region.</td>
</tr>
<tr>
<td>Aviatrix Controller Instance Type (InstanceTypeParam)</td>
<td>t2.large</td>
<td>The instance size for the controller. The default is t2.large.</td>
</tr>
</tbody>
</table>

IAM Roles:

<table>
<thead>
<tr>
<th>Parameter label (name)</th>
<th>Default</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Create the IAM Roles (IAMRoleParam)</td>
<td>New</td>
<td>Determine if IAM roles aviatrix-role-ec2 and aviatrix-role-app should be created. Select New if an Aviatrix IAM role has not been created (first-time launch). Select aviatrix-role-ec2 if there is already an Aviatrix IAM role created.</td>
</tr>
</tbody>
</table>

AWS Quick Start Configuration:

<table>
<thead>
<tr>
<th>Parameter label (name)</th>
<th>Default</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Quick Start S3 Bucket Name (QSS3BucketName)</td>
<td>aws-quickstart</td>
<td>The S3 bucket you have created for your copy of Quick Start assets, if you decide to customize or extend the Quick Start for your own use. The bucket name can include numbers,</td>
</tr>
</tbody>
</table>
### Amazon EC2 Configuration:

**Note** Make sure you have subscribed to the [Aviatrix PAYG (Metered) AMI](https://aws.amazon.com/ami/) on AWS Marketplace.

<table>
<thead>
<tr>
<th>Parameter label (name)</th>
<th>Default</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Key Pair (KeyNameParam)</td>
<td>Requires input</td>
<td>A public/private key pair, which allows you to connect securely to the Aviatrix Controller instance after it launches. When you created an AWS account, this is the key pair you created in your preferred region.</td>
</tr>
<tr>
<td>Aviatrix Controller Instance Type (InstanceTypeParam)</td>
<td>t2.large</td>
<td>The instance size for the controller. The default is t2.large.</td>
</tr>
</tbody>
</table>

**IAM Roles:**

<table>
<thead>
<tr>
<th>Parameter label (name)</th>
<th>Default</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Create the IAM Roles (IAMRoleParam)</td>
<td>New</td>
<td>Determine if IAM roles aviatrix-role-ec2 and aviatrix-role-app should be created. Select <strong>New</strong> if an Aviatrix IAM role has not been created before.</td>
</tr>
</tbody>
</table>
6. On the **Options** page, you can **specify tags** (key-value pairs) for resources in your stack and **set advanced options**. These are all options and can be configured later. When you’re done, choose **Next**.

7. On the **Review** page, review and confirm the template settings. Under **Capabilities**, select the check box to acknowledge that the template will create IAM resources.

8. Choose **Create** to deploy the stack. You may need to refresh the browser or console to see the status.

9. Monitor the status of the stacks. A primary stack and other nested stacks will be created. When the status of the stacks is **CREATE_COMPLETE**, Aviatrix Egress Filtering is ready to be configured.

**Note**  This Quick Start creates the EC2 instance that runs the Aviatrix Controller AMI. This instance is termination-protected. If you delete the Quick Start stack, you must manually turn off Termination Protection on the Aviatrix Controller EC2 instance before you delete the AWS CloudFormation stack. You can change Termination Protection by using the Amazon EC2 console.

10. Choose the primary stack, and then choose the **Outputs** tab to view the AWS account ID, and the public and private IPs of the Aviatrix Controller, as shown in Figure 5. You will need these IP addresses to access the Controller console in the next step.
Step 4. Performing the Initial Setup of the Aviatrix Controller

1. Use the public address of the controller (AviatrixControllerEIP=x.x.x.x) in your web browser to access the Aviatrix Controller console (https://x.x.x.x/). You can see the public address of the controller in the Outputs tab (shown in Figure 5).

   **Note**  To access the site, you must prefix the IP address with https://.

   Also, because a new instance was just created, you will see a browser message that “Your connection is not private.” This message appears because there is a self-signed SSL certificate on your new instance. You may ignore this warning. Depending on your browser, you may need to select Advanced > Proceed or Show Details > Visit this website. Later, you can remove this warning by uploading your own signed certificates.

   Use the default user name admin and your controller’s private IP address “x.x.x.x” (AviatrixControllerPrivateKey) as the password to log in to your controller. You can see the private IP address of the controller in the primary Outputs tab (shown in Figure 5).

2. Enter your email address, as shown in Figure 6. This email is used for alerts and password recovery (if needed).

   ![Figure 6: Entering the email address for password recovery](image-url)
3. Change your admin password, as shown in Figure 7.

![Figure 7: Changing the default password](image)

4. Choose **Skip**, as shown in Figure 8, unless the controller instance VPC has an HTTP or HTTPS proxy configured for internet access.

![Figure 8: Configuring the proxy server](image)
5. Choose Run, as shown in Figure 9. The controller will upgrade to the latest software version. Wait for about 3-5 minutes for the process to finish.

![Figure 9: Performing initial setup](image)

**Note** Once the controller upgrade is complete, the login prompt will appear. Use the user name “admin” and your new password to log in.

**Step 5. Create a Primary Access Account**

1. Once logged back in to the Aviatrix Controller, you should be on the **Onboarding** page. Otherwise, on the navigation bar, choose **Onboarding**.

   The Aviatrix primary access account is set up in the **Onboarding** page. This setup gives permissions to the Aviatrix Controller to configure the cloud networking within that public cloud provider, including deploying Aviatrix gateways. You then operate the Aviatrix Controller via the console or REST APIs. For more information about Aviatrix accounts, see **Onboarding and Account FAQs** in the Aviatrix documentation.

2. Select AWS.

![AWS](image)

3. Set up a primary access account. The Aviatrix primary access account contains the AWS account credential of the controller instance.

   For more information about the Aviatrix access account, see **What is an Aviatrix access account on the Controller?** in the Aviatrix documentation.
a. Fill out the fields as shown in the following table:

<table>
<thead>
<tr>
<th>Field</th>
<th>Expected Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Account Name</td>
<td>Enter a unique name—for example, AWSOpsTeam.</td>
</tr>
<tr>
<td>Controller’s AWS Account Number</td>
<td>The controller instance’s 12-digit AWS account number. You can find this in the Outputs section (as shown in Figure 5).</td>
</tr>
<tr>
<td>IAM role-based</td>
<td>Select this box.</td>
</tr>
</tbody>
</table>

b. At the bottom of the **Create Primary Access Account** form, choose **Create**, as shown in Figure 10.

![Create Primary Access Account](image)

**Figure 10: Creating the account**

**Note** If the Aviatrix Controller needs to build connectivity in AWS accounts that are different from the Aviatrix Controller instance’s AWS account, you must create secondary access accounts. To create a secondary access account on the controller and to create IAM roles, policies, and establish trust relationship to the primary AWS account, see [IAM Roles for Secondary Access Accounts](#).

**Step 6: Deploy Egress Filtering**

**Planning and Prerequisites**

Identify the VPCs in the region where you want to launch Aviatrix Egress Filtering gateways that will perform egress security functions.

**Important** The following steps assume that you have set up an Aviatrix Controller using this Quick Start.
There are two main steps to setting up Egress Filtering:

1. Open the Egress Security wizard.
2. Use the wizard to set up your Egress Security filters.

**Opening the Egress Security wizard**

In the dashboard, choose **UseCases** in the top-left corner, and then choose VPC Egress Security, as shown in Figure 11. This opens the Egress Security wizard.

![Diagram showing how to open the wizard from the dashboard](image)

**Figure 11: Opening the wizard from the dashboard**

**Using the wizard to set up your FQDN Egress Security Filters**

Follow the steps in the wizard to set up your FQDN Egress Security filters, as shown in Figure 12.
1. Launch the Egress Security gateway, as shown in Figure 13.

2. Perform Egress FQDN Discovery, as shown in Figure 14.

3. Configure the Egress FQDN filters, as shown in Figure 15.
4. Retrieve the Egress FQDN log, as shown in Figure 16.

![Egress FQDN View Log](Figure 16: Retrieving the FQDN log)

**Best Practices Using Aviatrix on AWS**

**Gateway Sizing**

For complete information about how to correctly size your gateway, see the [Aviatrix documentation](#).

**Backups**

When you deploy the Aviatrix Egress Filtering service in a cloud environment, the Aviatrix Controller is not in the data path because packet processing and encryption are handled by the Aviatrix gateways.

When the Aviatrix Controller is down or out of service, your network will continue to be operational, and encrypted tunnels and OpenVPN users will stay connected. Because most of the data logs are forwarded directly from the gateways, the loss of log information from the Aviatrix Controller is minimal.

This loosely coupled relationship between the Aviatrix Controller and gateways reduces the impact of controller availability issues and simplifies your infrastructure. The Aviatrix Controller stores configuration data and should be periodically backed up to the appropriate AWS account. If a replacement controller is launched, you can restore the configuration data from your backup. For more information, see the [Aviatrix documentation](#).
Security

The Aviatrix Controller is secured by exposing only the necessary ports (TCP 443). Each gateway that the Aviatrix Controller creates is able to communicate only with other gateways (using UDP 500 and 4500) and the Aviatrix Controller (using TCP 22 and 443). Aviatrix provides software and patch updates. For more information, contact Aviatrix at info@aviatrix.com.

All peering connections are secured by using IPsec encryption.

Troubleshooting

Q. I encountered a CREATE_FAILED error when I launched the Quick Start.
A. If AWS CloudFormation fails to create the stack, we recommend 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 will be retained and the instance will be left running, so you can troubleshoot the issue. (Look at the log files in %ProgramFiles%\Amazon\EC2ConfigService and C:\cfn\log.)

Important When you set Rollback on failure to No, you will continue to incur AWS charges for this stack. Please make sure to delete the stack when you finish troubleshooting.

For additional information, see Troubleshooting AWS CloudFormation on the AWS website.

Q. I encountered a size limitation error when I deployed the AWS CloudFormation templates.
A. We recommend that you launch the Quick Start templates from the links in this guide or from another S3 bucket. If you deploy the templates from a local copy on your computer or from a non-S3 location, you might encounter template size limitations when you create the stack. For more information about AWS CloudFormation limits, see the AWS documentation.
Support

Aviatrix provides customer support for all the Aviatrix components of the Aviatrix Egress Filtering service, including the automation scripts. Contact support@aviatrix.com for assistance.

GitHub Repository

You can visit our GitHub repository to download the templates and scripts for this Quick Start, to post your comments, and to share your customizations with others.

Additional Resources

AWS services

- Amazon EC2
  https://aws.amazon.com/documentation/ec2/
- Amazon VPC
  https://aws.amazon.com/documentation/vpc/
- AWS CloudFormation
  https://aws.amazon.com/documentation/cloudformation/

Aviatrix documentation

- Aviatrix website
  https://www.aviatrix.com/
- Aviatrix documentation
  https://www.aviatrix.com/docs/

Quick Start reference deployments

- AWS Quick Start home page
  https://aws.amazon.com/quickstart/

Document Revisions

<table>
<thead>
<tr>
<th>Date</th>
<th>Change</th>
<th>In sections</th>
</tr>
</thead>
<tbody>
<tr>
<td>July 2018</td>
<td>Initial publication</td>
<td>—</td>
</tr>
</tbody>
</table>
Notices

This document is provided for informational purposes only. It represents AWS’s current product offerings and practices as of the date of issue of this document, which are subject to change without notice. Customers are responsible for making their own independent assessment of the information in this document and any use of AWS’s products or services, each of which is provided “as is” without warranty of any kind, whether express or implied. This document does not create any warranties, representations, contractual commitments, conditions or assurances from AWS, its affiliates, suppliers or licensors. The responsibilities and liabilities of AWS to its customers are controlled by AWS agreements, and this document is not part of, nor does it modify, any agreement between AWS and its customers.

The software included with this paper is licensed under the Apache License, Version 2.0 (the "License"). You may not use this file except in compliance with the License. A copy of the License is located at http://aws.amazon.com/apache2.0/ or in the "license" file accompanying this file. This code is distributed on an "AS IS" BASIS, WITHOUT WARRANTIES OR CONDITIONS OF ANY KIND, either express or implied. See the License for the specific language governing permissions and limitations under the License.