Aviatrix Next-Gen Global Transit Hub on the AWS Cloud

Quick Start Reference Deployment

February 2018
Last update: April 2018 (revisions)

Jing Zhou, Jorge Bonilla, Sunil Kishen, and Frank Cabri — Aviatrix Systems
Shivansh Singh, Wayne Davis, and Josh Hammer — Amazon Web Services

Contents
Overview.................................................................................................................................................. 2
Transit VPCs ........................................................................................................................................... 3
Aviatrix Next-Gen Global Transit Hub vs. Traditional Global Transit Hub .................................. 3
Features of Aviatrix Next-Gen Global Transit Hub ........................................................................... 4
Costs and Licenses ................................................................................................................................. 5
Architecture........................................................................................................................................... 5
Quick Start Components ...................................................................................................................... 7
Additional Functionality ......................................................................................................................... 8
Prerequisites .......................................................................................................................................... 8
Specialized Knowledge ......................................................................................................................... 8
License Requirements ............................................................................................................................ 8
Technical Requirements .......................................................................................................................... 9
Deployment Options ............................................................................................................................... 9
Deployment Steps .................................................................................................................................. 10
Step 1. Prepare Your AWS Account .................................................................................................. 10
Step 2. Subscribe to the Aviatrix AMI ................................................................. 10
Step 3. Launch the Quick Start ............................................................................... 11
Step 4. Initial Setup of the Aviatrix Controller ...................................................... 15
Step 5. Create a Primary Access Account ............................................................... 17
Step 6: Deploy AWS Global Transit Network ......................................................... 19
Best Practices Using Aviatrix on AWS ................................................................. 26
   Gateway Sizing .................................................................................................. 26
   Backups ............................................................................................................. 26
Security .................................................................................................................. 27
Troubleshooting ...................................................................................................... 27
Support .................................................................................................................. 28
GitHub Repository ................................................................................................. 28
Additional Resources ............................................................................................. 28
Document Revisions .............................................................................................. 29

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 Next-Gen Global Transit Hub architecture on the AWS Cloud.

This Quick Start uses AWS APIs to automatically deploy a virtual private cloud (VPC) and Aviatrix Controller to enable the Aviatrix Next-Gen Global Transit Hub. The deployment enables a central transit hub VPC that connects multiple spoke VPCs to facilitate communication between the spoke VPCs and an on-premises network.
Transit VPCs

A transit VPC is a common strategy for connecting multiple, geographically disperse VPCs and remote networks to create a global network transit center. A transit VPC simplifies network management and minimizes the number of connections required to connect multiple VPCs and remote networks.

This Quick Start deploys the Aviatrix Next-Gen Global Transit Hub solution, which provides a hub-and-spoke model to perform routing between spoke networks and on-premises data centers or physical sites through a central hub. This solution allows you to connect spoke VPCs to the transit hub VPC using the Aviatrix Controller point-and-click Aviatrix Global Transit Network Wizard. The in-product Transit Network Wizard allows you to launch and configure two Aviatrix Gateways in the transit hub VPC and the designated spoke VPCs, in high-availability (HA) mode. If one Aviatrix Gateway fails, the second Aviatrix Gateway automatically connects in seconds to reduce network downtime.

For more information about transit VPCs and the hub-and-spoke model, see AWS Global Transit Network on the AWS Answers website.

Aviatrix Next-Gen Global Transit Hub vs. Traditional Global Transit Hub

The Next-Gen Global Transit Hub is part of a second-generation of networking technology, which combines a traditional global transit hub with additional security, scale, and operational functionalities. This Aviatrix solution provides enhanced security by maintaining VPC segmentation. This allows the user to control policy-based connectivity, and use encrypted links everywhere. From an operations perspective, this Aviatrix solution includes:

- Higher levels of automation via REST APIs
- Configuration wizards to simplify and streamline orchestration of networking services
- Troubleshooting with Aviatrix EC2 FlightPath
- Other integrated tests
- Visibility with global dashboards

Also, teams can grow easily because this Aviatrix solution removes route table limitations and extends the Next-Gen Global Transit Hub with additional uses cases for cloud networking:

- Remote user VPN
- Egress security
• Site to cloud
• Multicloud peering

Features of Aviatrix Next-Gen Global Transit Hub

Aviatrix Next-Gen Global Transit Hub includes the following features:

• **Centralized controller with the Aviatrix Global Transit Network Wizard** – Point-and-click, centralized management console (with REST API support) manages distributed gateways that both CloudOps and network engineers can easily operate. No deep networking skills are required (no network router CLI knowledge needed). You can use the Aviatrix Controller to implement changes or customizations quickly and easily.

• **BGP required in Transit Hub VPC only** – The Aviatrix Next-Gen Global Transit Hub is API-based and uses policy-based routing from the spokes to the transit hub VPC. The spoke VPC routes are advertised to the Transit Hub Gateways by the Aviatrix Controller. Those gateways exchange routes with the on-premises network using the Border Gateway Protocol (BGP) via the AWS virtual private gateway (VGW). Conversely, the learned on-premises routes from the Transit Hub Gateways are sent to the Aviatrix Controller for propagation to the spoke VPCs. Spoke VPCs do not run BGP.

• **Simplified troubleshooting** – The Aviatrix Next-Gen Global Transit Hub includes integrated diagnostic tools that make troubleshooting much easier, compared with traditional networking products that use BGP everywhere. The integrated EC2 FlightPath troubleshooting tool helps identify Amazon EC2 connectivity problems to minimize downtime.

• **Built-in security** – Encrypted links, integrated stateful firewalls for policy enforcement, and control of outbound traffic using fully qualified domain name (FQDN) filtering help ensure that security is fully integrated with your global transit network. VPC isolation and segmentation are created by design such that spoke-to-spoke connectivity through the transit hub is not allowed. Instead, Aviatrix supports spoke-to-spoke connectivity using AWS Peering or Aviatrix Encrypted Peering only where required. This peering option allows direct Spoke-to-Spoke connectivity, eliminating the transit hop and reduces traffic load on the transit hub by separating the on-premises-bound traffic from the in-cloud traffic. You can enable Direct Peering using the Aviatrix Controller’s Encrypted Peering or AWS Peering configuration option.

• **Monitoring and visibility** – The Aviatrix Controller dashboard provides a visual representation of your global transit network. It also monitors, displays, and alerts on link status, performance, and link latency for transit hubs and spoke VPCs.
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, the solution creates a unique AWS Key Management Service (AWS KMS) customer master key (CMK), which has a low monthly cost, to protect network configuration information. For details, see the AWS KMS pricing webpage.

You are also responsible for the Aviatrix license that is required to deploy the Aviatrix Next-Gen Global Transit Hub. As explained in step 2 of the deployment steps, you subscribe to an Amazon Machine Image (AMI) for Aviatrix software in AWS Marketplace, choosing the licensing option:

- **Aviatrix Secure Networking Platform PAYG - Metered** – Hourly subscription license based on the prices listed on the AWS Marketplace webpage. This pay-as-you-grow license allows you to build and scale your Next-Gen Global Transit Hub network to any size, consisting of one transit hub VPC and many spoke VPCs.

Architecture

This Quick Start sets up a secure Aviatrix Next-Gen Global Transit Hub architecture that includes the Aviatrix Controller and Aviatrix Gateways in a highly available configuration. You can create a new VPC or use an existing VPC for the transit hub.

Deploying this Quick Start for a new VPC with **default parameters** builds the following Aviatrix Next-Gen Global Transit Hub architecture in the AWS Cloud, shown in Figure 1. The architecture in the figure also shows a **Shared Services VPC** that can be optionally configured to extend your Next-Gen Global Transit Hub architecture to a Next-Gen Global Transit and Services Hub architecture.
The Quick Start deploys the Aviatrix Controller into an existing VPC or a new VPC. After you deploy the Aviatrix Controller using this Quick Start, you can use the Aviatrix Global Transit Network Wizard in the Aviatrix Controller to deploy the Hub Gateway instances into a VPC that will be designated as the Next-Gen Global Transit Hub. The
The Transit Network Wizard lets you add spoke VPCs in any AWS Region to your global transit network by attaching those VPCs to the Next-Gen Global Transit Hub. VPN connections are automatically established between the spoke VPCs and the Next-Gen Global Transit Hub VPC.

**Note** The Aviatrix Controller allows you to deploy spoke VPCs from one or multiple AWS accounts. Use the Aviatrix Controller to add/onboard one or more accounts to your Next-Gen Global Transit Hub VPC architecture. Contact support@aviatrix.com for more information.

**Quick Start Components**

The Quick Start creates, deploys, and configures the functional and automation components shown in Figure 2.
These components and services include the following:

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

**Additional Functionality**

After you deploy the Quick Start and use the Transit Network Wizard to establish your transit VPC network, you can extend the environment beyond the AWS Cloud. By using the Aviatrix Controller, you can automatically configure VPN connections to network providers, on-premises infrastructure, or even other public cloud providers.

You can also optionally expand your global transit architecture to include a Shared Services layer (see Figure 1) with AWS Direct Peering. You can easily configure this with the Aviatrix Controller. This architecture enables cloud or DevOps teams who require a shared services or management VPC for common DevOps tools and services. Contact info@aviatrix.com for more information.

**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 EC2
- 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 add one or more AWS accounts, and connect spoke VPCs in those AWS accounts. You can also connect spoke VPCs across different AWS Regions.

**Note**  The Aviatrix Controller supports multiple AWS accounts. Use the Aviatrix Controller to add multiple accounts. For more information, see the [Aviatrix Onboarding and Account FAQs documentation](#).

IAM Requirements

Aviatrix Next-Gen Global Transit Hub VPC Quick Start requires the following IAM roles to be created in the primary AWS account:

- An Aviatrix role for 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 these ways:

- If this is the first time you launch Aviatrix Controller, this Quick Start will create the required IAM roles. See the Quick Start [Deployment Options](#) below.

- If the required IAM roles already exist, select aviatrix-role-ec2 in the Quick Start [Deployment Options](#) below.

**Important**  If you have existing Aviatrix IAM roles, ensure 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** Aviatrix Controller is normally deployed in a Shared Services VPC where your DevOps and management tools and services are hosted. We do not recommend deploying the Controller in the Next-Gen Global Transit Hub VPC.

## 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 Aviatrix Next-Gen Global Transit Hub 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 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.

4. Use the Manual Launch option to read the license agreement and Accept Software Terms.

**Important** Do not launch the instance manually (by choosing Manual Launch) from the AWS Marketplace. This will be handled by the Quick Start.
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 Aviatrix into a new VPC on AWS](Launch)
   ![Option 2: Deploy Aviatrix into an existing VPC on AWS](Launch)

   This deployment takes less than 5 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 your Aviatrix Next-Gen Global Transit Hub 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 <strong>aviatrix-role-ec2</strong> 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, lowercase letters, uppercase letters, and hyphens, but should not start or end with a hyphen.</td>
</tr>
<tr>
<td>Quick Start S3 Key Prefix QSS3KeyPrefix</td>
<td>quickstart-aviatrix-controller/</td>
<td>The S3 key name prefix used to simulate a folder for your copy of Quick Start assets, if you decide to customize or extend the Quick Start for your own use. This prefix can include numbers, lowercase letters, uppercase letters, hyphens, and forward slashes.</td>
</tr>
</tbody>
</table>

- **Option 2: Parameters for deploying Aviatrix Controller into an existing 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 ID VPCID</td>
<td>Requires input</td>
<td>The ID of your existing VPC where the Aviatrix Controller will be deployed. (e.g., vpc-0343606e)</td>
</tr>
<tr>
<td>Public Subnet ID SubnetID</td>
<td>Requires input</td>
<td>The Aviatrix Controller must be launched on a public subnet.</td>
</tr>
</tbody>
</table>

### Amazon EC2 Configuration:

**Note** Make sure you have subscribed to the Aviatrix PAYG (Metered) AMI on the 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 (first-time launch). Select <strong>aviatrix-role-ec2</strong> if there is already an Aviatrix IAM role created.</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 option 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.

**Important** Make sure you have subscribed to the Aviatrix PAYG (Metered) AMI on the AWS Marketplace before you proceed.

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 statuses are **CREATE_COMPLETE**, the Aviatrix Next-Gen Global Transit Hub Controller is ready.

**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 CloudFormation stack. You can change Termination Protection by using the Amazon EC2 console.

10. Click the primary stack, and then click the **Outputs** tab to view the AWS account ID, and the public and private IPs of the Aviatrix Controller, as shown in Figure 3. You will need these IP addresses to access the Controller console in the next step.

<table>
<thead>
<tr>
<th>Key</th>
<th>Value</th>
<th>Description</th>
<th>Export Name</th>
</tr>
</thead>
<tbody>
<tr>
<td>AviatrixControllerIP</td>
<td></td>
<td>AviatrixController External IP</td>
<td></td>
</tr>
<tr>
<td>AccountId</td>
<td></td>
<td>Amazon Account ID</td>
<td></td>
</tr>
<tr>
<td>AviatrixControllerPrivateIP</td>
<td>13.0.19.241</td>
<td>AviatrixController Private IP</td>
<td></td>
</tr>
</tbody>
</table>

**Figure 3: Stack outputs**
Step 4. 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 3).

   **Note** You must prefix the IP address with https:// or the site will not be reached.

   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 click 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” (AviatrixControllerPrivateIP) 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 3).

2. Enter your email address, as shown in Figure 4. This email will be used for alerts and password recovery (if needed).

   ![Figure 4: Entering the email address for password recovery](image-url)
3. Change your admin password, as shown in Figure 5.

![Figure 5: Changing the default password]

4. Click **Skip**, as shown in Figure 6, unless the Controller instance VPC has an HTTP or HTTPS proxy configured for internet access.

![Figure 6: Configuring the proxy server]
5. Click **Run**, as shown in Figure 7. The Controller will upgrade to the latest software version. Wait for about 3-5 minutes for the process to finish.

![Figure 7: 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 Controller, you should be on the **Onboarding** page. Otherwise, on the navigation bar, click **Onboarding**.

   The Aviatrix primary access account is set up in the **Onboarding** page. This setup gives permissions to the Controller to configure the cloud networking within that public cloud provider, including deploying Aviatrix Gateways. You then operate the 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**.

3. Set up a primary access account. The Aviatrix primary access account contains the Controller instance's AWS account credential.
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 8).</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, click Create, as shown in Figure 8.

![Create Primary Access Account](image)

Figure 8: Creating the account

Note If the Controller needs to build connectivity in AWS accounts that are different from the Controller instance’s AWS account, secondary access accounts need to be created. 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 AWS Global Transit Network

Planning and Prerequisites

Identify a VPC that will become your Transit Hub VPC, in a region where you want to launch the Aviatrix Transit Gateway (GW), and create a VGW in the same region.

Note The VGW should not be attached to the Transit Hub VPC. It can be attached to a different VPC if its CIDR is different from the Transit Hub VPC CIDR. (See the 10Gbps Transit Network use case.) This VGW should be connected to an on-premises network either over Direct Connect or over the internet by using the AWS Hardware VPN.

Set up a transit network using the Aviatrix Global Transit Network Wizard

Perform the following steps to set up a transit network using the Aviatrix Global Transit Network Wizard, or see the Aviatrix documentation. From the Aviatrix Controller console, click Transit Network to access the wizard, as shown in Figure 9.

1. Launch a Transit Gateway.

   The Transit GW is the hub gateway. It moves traffic between a spoke VPC and on-premises network. The Transit GW must be launched on a public subnet where its associated route table has a route 0.0.0.0/0 that points to AWS internet gateway (IGW).
<table>
<thead>
<tr>
<th>Setting</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cloud Type</td>
<td>Currently the Transit GW can only be launched in AWS.</td>
</tr>
<tr>
<td>Gateway Name</td>
<td>A unique name to identify the Transit GW</td>
</tr>
<tr>
<td>Account Name</td>
<td>An Aviatrix account that corresponds to an IAM role or account in AWS</td>
</tr>
<tr>
<td>Region</td>
<td>One of the AWS regions</td>
</tr>
<tr>
<td>VPC ID</td>
<td>The Transit VPC ID</td>
</tr>
<tr>
<td>Public Subnet</td>
<td>The public subnet on which the Transit GW instance is deployed</td>
</tr>
<tr>
<td>Gateway Size</td>
<td>Transit GW instance size</td>
</tr>
<tr>
<td>Specify a Reachable DNS Server IP Address</td>
<td>Leave it unselected</td>
</tr>
<tr>
<td>Add/Edit Tags</td>
<td>Additional AWS Tags for the Transit GW instance</td>
</tr>
</tbody>
</table>

**Note** When selecting a Transit GW instance size, choose a t2 series for Proof of Concept (POC) or prototyping only. Transit GW of t2 series instance type has a random packet drop of 3% for a packet size less than 150 bytes, when interoperating with VGW. This packet drop does not apply to Spoke GW.

You can change the Transit GW size later. To do so, see [How do I resize the Transit GW instance?](#) in the Aviatrix documentation.

2. (Optionally) Enable HA for the Transit Gateway

When HA is enabled, a second Transit GW will be launched, as shown in Figure 11. Both Transit GWs will forward traffic in an event of tunnel failure between a spoke VPC and transit VPC, and between the Transit GW and VGW.

As a best practice, the HA GW should be launched on a different public subnet in a different AZ.

![Figure 11: Enabling high availability for the transit gateway](#)
To disable Transit GW HA, go to the **Gateway** page and delete the Transit GW with -hagw in the name extension. If the Transit GW is connected to VGW, you cannot disable Transit GW HA. Also, if there are still Spoke GWs, you cannot disable Transit GW HA.

3. **Connect the Transit GW to AWS VGW**

This step builds a site2cloud IPSEC tunnel with VGW and establishes a BGP session with VGW to exchange routes between on-premises and the cloud.

![Diagram of Transit VPC Hub with VGW connected to it](image)

**Figure 12: Connecting the Transit GW to the AWS VGW**

<table>
<thead>
<tr>
<th>Setting</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>VPC ID</td>
<td>The Transit VPC ID where the Transit GW was launched</td>
</tr>
<tr>
<td>Connection Name</td>
<td>A unique name to identify the connection to VGW</td>
</tr>
<tr>
<td>BGP Local AS Number</td>
<td>The BGP AS number that the Transit GW will use to exchange routes with VGW</td>
</tr>
<tr>
<td>Primary Cloud Gateway</td>
<td>The Transit GW that you created in Step 1</td>
</tr>
<tr>
<td>AWS VGW Account Name</td>
<td>The Aviatrix account that VGW is created with; this account might or might not be the same as the account used by Transit GW</td>
</tr>
<tr>
<td>VGW Region</td>
<td>The AWS region where the VGW is created</td>
</tr>
<tr>
<td>VGW ID</td>
<td>The VGW that is created in the VGW Region in the AWS VGW account</td>
</tr>
</tbody>
</table>

**Note** The Aviatrix Transit GW can connect to a VGW that belongs to a different AWS account in a different region.
It takes a few minutes for the VPN connection to come up and for routes from VGW to propagate. When the IPSEC tunnel with VGW is up, the Controller admin should receive an email notification.

**Note** Log in to the AWS Management Console. To see the Customer Gateway and VPN Connections that have been created, under **Services**, select **VPC** in the region where the VGW is launched. Do not delete or modify them from the AWS Management Console. These resources are deleted when you disconnect the VGW in step 8.

You can check if routes are properly propagated:

a. In the Aviatrix Controller navigation bar, go to **Advanced Config**, and select BGP.

b. Select the Transit GW, and click **Detail**. The Learned Routes should be the list of the routes propagated from VGW. Scroll down to see the total number of learned routes.

4. Launch a Spoke Gateway

![Figure 13: Launching a spoke gateway](image)
<table>
<thead>
<tr>
<th>Setting</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cloud Type</td>
<td>Currently, the Spoke GW can only be launched in AWS</td>
</tr>
<tr>
<td>Gateway Name</td>
<td>A unique name to identify the Spoke GW</td>
</tr>
<tr>
<td>Account Name</td>
<td>An <a href="#">Aviatrix account</a> that corresponds to an IAM role or account in AWS</td>
</tr>
<tr>
<td>Region</td>
<td>One of the AWS regions</td>
</tr>
<tr>
<td>VPC ID</td>
<td>The Spoke VPC-id</td>
</tr>
<tr>
<td>Public Subnet</td>
<td>The public subnet where the Spoke GW instance is deployed</td>
</tr>
<tr>
<td>Gateway Size</td>
<td>Spoke GW instance size</td>
</tr>
<tr>
<td>Specify a Reachable DNS Server IP Address</td>
<td>Leave it unselected</td>
</tr>
<tr>
<td>Enable NAT</td>
<td>Select the option if the Spoke GW will also be the NAT gateway for the Spoke VPC</td>
</tr>
<tr>
<td>Add/Edit Tags</td>
<td>Additional AWS Tags for the Transit GW instance</td>
</tr>
</tbody>
</table>

**Note** You can enable the NAT function on the Spoke GW, if internet-bound egress traffic is intended to go through the Spoke GW. Once the NAT is enabled, you can further configure [FQDN whitelists for egress filtering](#).

5. (Optionally) Enable HA for the Spoke Gateway.

6. Attach a Spoke GW to the Transit GW Group.

   This attaches a spoke VPC to the Transit GW Group by building an Aviatrix encrypted peering and transitive peering between the Spoke GW and the Transit GW. The Controller also instructs the Transit GW to start advertising the Spoke VPC CIDR to VGW via the established BGP session.
Figure 14: Attaching a Spoke GW to the Transit GW group

<table>
<thead>
<tr>
<th>Setting</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Spoke Gateway/Source Gateway</td>
<td>Select the Spoke GW that will be attached</td>
</tr>
<tr>
<td>Transit Gateway/NextHop Gateway</td>
<td>Select the Transit GW</td>
</tr>
</tbody>
</table>

To attach more spoke VPCs to this Transit GW Group, repeat steps 4-6.
Modify (add, delete, change) the Global Transit Network

The following steps in the Aviatrix Global Transit Network Wizard and Controller allow you to modify (add, delete, change) the Global Transit Network.

7. Detach a Spoke GW from a Transit GW Group

This step detaches one Aviatrix spoke VPC from a Transit GW Group. The Controller also instructs the Transit GW to stop advertising the Spoke VPC CIDR to VGW.

**Note** The Spoke GW isn’t deleted. Go to step 6 to attach the Transit GW group.

To delete a Spoke GW, go to Gateway on the main Aviatrix Controller navigation tab, select the gateway, and click **Delete**.

8. Disconnect VGW Connection

You can remove the BGP and site2cloud IPSEC connection to VGW via this step. All Spoke VPCs must be detached from the Transit GW Group before you can remove the Transit GW to VGW connection.
To build the connection again, go to step 3.

9. View the Network Topology

You can view the network topology by going to the Aviatrix Controller Dashboard. Click the Map View to switch to Logical View. In the Logical View, each gateway is represented by a dot. You can rearrange the initial drawing by moving the dot, zoom in or zoom out, or move the graph around. After you are done, click Save.

10. Troubleshoot BGP

Under Advanced Config on the Aviatrix Controller main navigation bar, click BGP. The Transit GW will have BGP Mode as Enabled. Click the Transit GW and click Details to see Advertised Networks and Learned Networks. Learned Networks are network CIDR blocks that BGP learned from VGW. Advertised Networks are Spoke VPC CIDRs.

You can also click Diagnostics. Select or enter a command to see more BGP details.

To troubleshoot connectivity between a Spoke VPC instance and an on-premises host, follow these troubleshooting steps in the Aviatrix documentation.

11. Disable Transit GW HA

Go to the Gateway page, locate the Transit GW with "-hagw" in the gateway name extension, highlight the gateway, and click Delete.

**Note**  The Transit GW and its backup companion are in active/active state—that is, both gateways could be forwarding traffic. To disable Transit GW HA, it is a best practice to make sure there is no traffic going through the backup Transit GW.

**Best Practices Using Aviatrix on AWS**

**Gateway Sizing**

For complete information about how to correctly size your gateway, see Gateway in the Aviatrix documentation.

**Backups**

When you deploy the Aviatrix Next-Gen Global Transit Hub 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. However, you won’t be able to build new tunnels or add new OpenVPN users.

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 Controller Backup and Restore in the AWS documentation.

Security

The Aviatrix Controller is secured by exposing only the necessary ports (TCP 443). Each gateway created by the Aviatrix Controller is able to communicate only with other gateways (using UDP 500 and 4500) and the Aviatrix Controller (using TCP 22 and 443). Software and patch updates are provided by Aviatrix. 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 Next-Gen Global Transit Hub, 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://docs.aviatrix.com/

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>February 2018</td>
<td>Initial publication</td>
<td>—</td>
</tr>
<tr>
<td>April 2018</td>
<td>Updated to use Aviatrix Global Transit Network Wizard to configure the Global Transit Network</td>
<td></td>
</tr>
</tbody>
</table>

© 2018, Amazon Web Services, Inc. or its affiliates, and Aviatrix Systems. All rights reserved.

### 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/](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.