Aviatrix Transit Architecture on the AWS Cloud

Quick Start Reference Deployment

November 2017

Aviatrix Systems

AWS Quick Start Reference Team

Contents

This Quick Start reference deployment guide was created by Amazon Web Services (AWS) in partnership with *Aviatrix Systems*.

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 Aviatrix Transit Architecture on the Amazon Web Services (AWS) Cloud.

This Quick Start is for users who need secure connectivity between VPCs, whether it is intra or inter region. Aviatrix automates the deployment of the required infrastructure to enable a wide variety of Cloud architectures, including a Global Transit Network architecture.

Aviatrix Systems on AWS

Aviatrix is a leader in cloud networking, and in 2017 was recognized by Gartner as a "Cool Vendor" in Cloud Computing. With Aviatrix software, Cloud operations, architects and networking engineers can utilize the one-click power of cloud-native networking to set up secure connections across their private data centers and Amazon AWS VPCs in minutes.

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 the 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.

Aviatrix Systems utilizes a BYOL licensing model. For more information, contact the Aviatrix sales team at sales@aviatrix.com

Architecture

Deploying this Quick Start for a new virtual private cloud (VPC) with **default parameters** builds the following Aviatrix environment in the AWS Cloud.

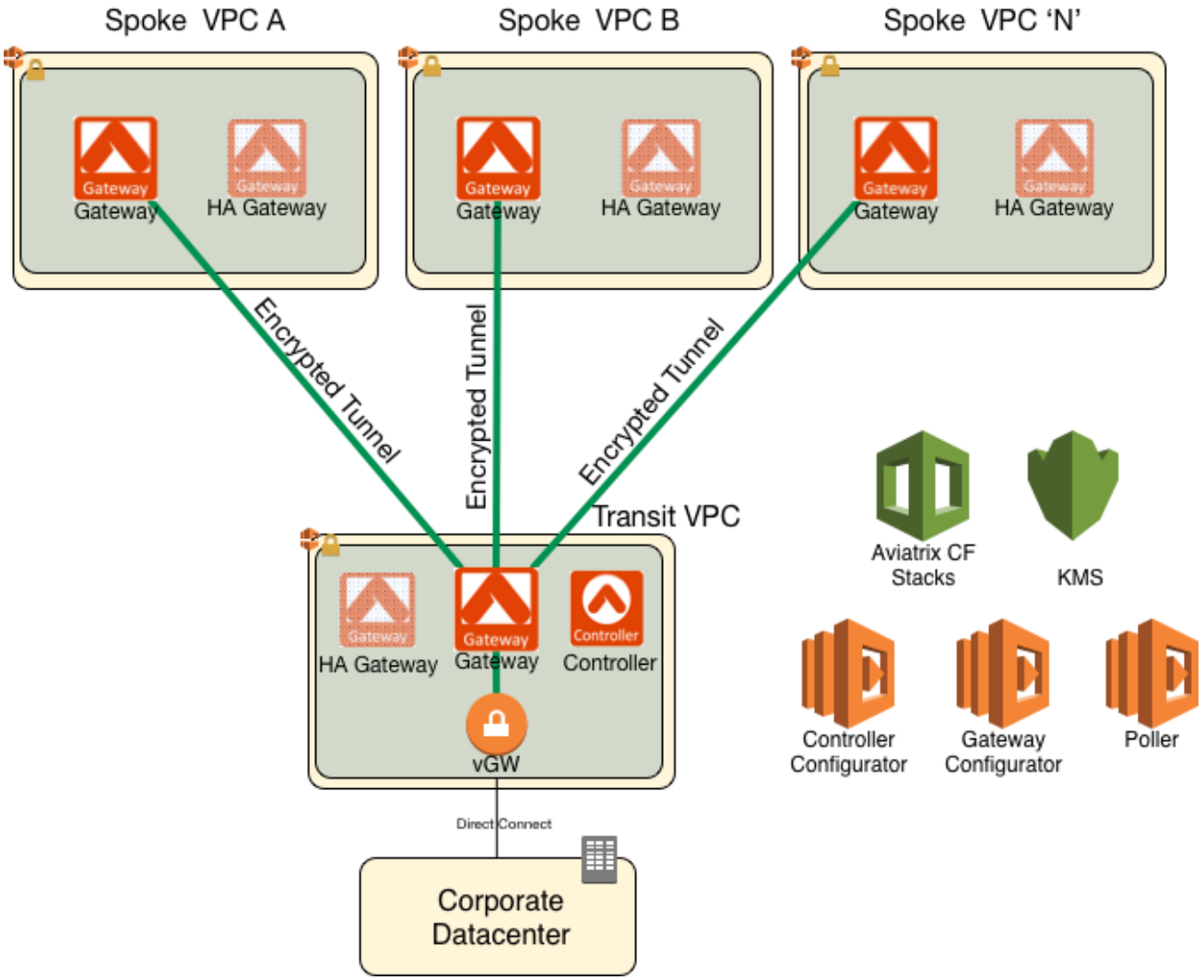


Figure 1: Quick Start *Aviatrix* architecture on AWS

The Quick Start sets up the following:

- One Aviatrix Role for EC2 (named aviatrix-role-ec2) with corresponding role policy (named aviatrix-assume-role-policy). Click here for this policy's details.

- One Aviatrix Role for Apps (named aviatrix-role-app) with corresponding role policy (named aviatrix-app-policy) Click here for this policy's details.

- One Aviatrix Controller EC2 Instance (named Aviatrix Controller).
- One Aviatrix Security Group (named AviatrixSecurityGroup).
- Lambda Script to automatically configure the Controller and deploy hub gateway(s) using API calls
- Lambda Script to detect VPC tags of aviatrix-spoke=true/false in order to deploy/delete the Aviatrix gateway on that VPC and connect/disconnect it to the hub gateway

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.) The Aviatrix solution does not require advanced networking skills to deploy and maintain.

- Amazon VPC
- Amazon EC2

Technical Requirements

The Aviatrix Transit Hub Solution deploys an Aviatrix Controller, a Transit Hub Gateway and up to 5 spoke gateways, utilizing the AWS Marketplace AMI for 5 tunnels. All licensing is included. The Aviatrix Transit Hub Solution can grow beyond 5 spokes. For more information, or for additional licenses, please contact us at sales@aviatrix.com

To start, an AWS account is required. The current solution cannot spawn spokes gateways across multiple accounts. The solution also requires that you create your spoke VPCs (within the same account) in the different regions and tag those as instructed in the deployment steps.

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 the Global Transit VPC, subnets, Internet

Gateway, Default Route and other infrastructure components, and then deploys an Aviatrix Controller and one Aviatrix Hub Gateway into this new VPC.

- **Deploy Aviatrix into an existing VPC**. This option provisions an Aviatrix Controller, one Aviatrix Hub Gateway and other infrastructure components into your existing AWS infrastructure.

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.

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 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 on AWS.
3. Create a key pair in your preferred region.
4. If necessary, request a service limit increase for the Amazon EC2 <type> instance type. You might need to do this if you already have an existing deployment that uses this instance type, and you think you might exceed the default limit with this reference deployment.

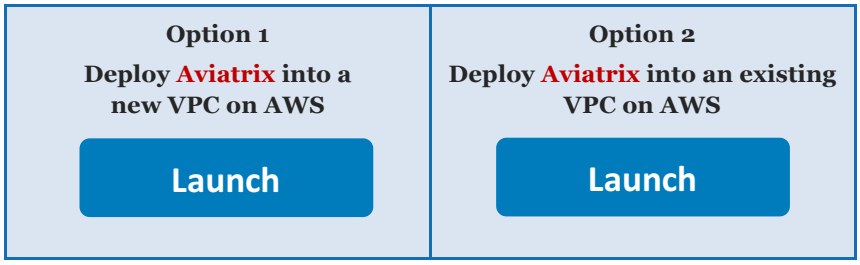
Step 2. Subscribe to the Aviatrix AMI

1. Log in to the AWS Marketplace at https://aws.amazon.com/marketplace/.
2. Open the page for Aviatrix, and choose **Continue**.
3. Use the **Manual Launch** option to launch the AMI into your account on Amazon EC2. This involves accepting the terms of the license agreement and receiving a confirmation email. For detailed instructions, see the AWS Marketplace documentation.

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.



> **Important** If you're deploying Aviatrix into an existing VPC, make sure that your VPC has at least one public subnet. This subnet requires an Internet Gateway and a default route pointing to the Internet Gateway. This allows the instances to download packages and software from the Internet. You'll be prompted for your VPC settings when you launch the Quick Start.

   Each deployment takes about 8 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 infrastructure for Aviatrix will be built. The template is launched in the US East 1 (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, provide a name for the stack (for example: Aviatrix). 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**.

   In the following tables, parameters are listed by category and described separately for the two deployment options:

   – Parameters for deploying Aviatrix into a new VPC
   – Parameters for deploying Aviatrix into an existing VPC

- **Option 1: Parameters for deploying Aviatrix into a new VPC**

  View template

Amazon Ec2 Configuration:

Parameter label (name)	Default	Description
Keypair	*Requires input*	Keypair to be used in the Aviatrix Controller for SSH access
Management Subnet	0.0.0.0/0	CIDR of network(s) that will be granted access to the Controller. Typically this will be your management network.

VPC Configuration:

Parameter label (name)	Default	Description
VPC Subnet	10.1.0.0/16	Subnet address to be assigned to the VPC
Subnet CIDR	10.1.0.0/24	Subnet CIDR where the controller will be deployed

- *Controller Configuration:*

Parameter label (name)	Default	Description
Admin Email	*Requires input*	Email for the administrator of the Aviatrix Controller
Controller Password	*Requires input*	Password for the controller. It must contain an uppercase letter, a number and a symbol.
Controller Instance Size	T2.large	Instance Size for the controller.

- *Aviatrix Transit Hub Configuration:*

Parameter label (name)	Default	Description
Hub Gateway Instance Size	T2.micro	Instance Size for the Aviatrix Transit Hub Gateway

- **Option 2: Parameters for deploying Aviatrix into an existing VPC**

  View template

Amazon Ec2 Configuration:

Parameter label (name)	Default	Description
Keypair	*Requires input*	Keypair to be used by the Aviatrix Controller for SSH access

Parameter label (name)	Default	Description
Management Subnet	0.0.0.0/0	CIDR of network(s) that will be granted access to the Controller. Typically this will be your management network.

Existing VPC Configuration:

Parameter label (name)	Default	Description
VPC	*Requires input*	Select the VPC where the controller will be deployed
Subnet	*Requires input*	Select the Subnet where the controller will be deployed

- *Controller Configuration:*

Parameter label (name)	Default	Description
Admin Email	*Requires input*	Email for the administrator of the Aviatrix Controller
Controller Password	*Requires input*	Password for the controller. It must contain an uppercase letter, a number and a symbol.
Controller Instance Size	T2.large	Instance Size of the controller.

- *Aviatrix Transit Hub Configuration:*

Parameter label (name)	Default	Description
Hub Gateway Instance Size	T2.micro	Instance Size of the Aviatrix Transit Hub Gateway

5. On the **Options** page, you can specify tags (key-value pairs) for resources in your stack and set advanced options. When you're done, choose **Next**.
6. On the **Review** page, review and confirm the template settings. Under **Capabilities**, select the checkbox to acknowledge that the template will create IAM resources.
7. Choose **Create** to deploy the stack.
8. Monitor the status of the stack. When the status is **CREATE_COMPLETE**, the Aviatrix Transit Hub Solution is ready.
9. Use the URLs displayed in the **Outputs** tab for the stack to view the resources that were created.

Step 4. Add Spoke VPC

> **Important** Make sure the spoke VPC has at least two public subnets in different Availability zones. These subnets requires an Internet Gateway and a default route pointing to the Internet Gateway.

1. Choose the **VPC(s)** that will become your spokes in the Aviatrix Transit Hub architecture.
2. Create a new tag on the VPC:

– Key: aviatrix-spoke

– Value: true

3. In less than a minute, the poller process will detect the new tag and execute the necessary API calls to deploy an Aviatrix gateway on that VPC, and it will automatically peer it with the Aviatrix Transit Hub Gateway.

4. After the process is completed, the aviatrix-spoke tags will be changed to “peered”.

Step 5. (Optional) Delete Spoke VPC

1. Choose the **VPC(s)** that you no longer want it to be part of the Aviatrix Transit Hub architecture.
2. Change the aviatrix-spoke tag on the VPC:

– Key: aviatrix-spoke

– Value: *false*

3. In less than a minute, the poller process will detect the change in the tag and execute the necessary API calls to delete the peering with the Aviatrix Transit Hub Gateway, and will delete the Aviatrix gateway on that VPC.

4. After the process is completed, the aviatrix-spoke tags will be changed to “unpeered”.

Step 6. (Optional) Launch Aviatrix UI

1. Under the Outputs of the Stack you will find the address of the controller (AviatrixControllerEIP), utilize that information to access the controller UI. i.e: https://X.X.X.X/ .

2. From the Aviatrix UI you will be able to manage all your cloud network connectivity.

Step 7. (Optional) Transit connection of vGW for Direct connect/VPN

3. For more instruction on how to connec to a vGW that terminates your Direct Connect or VPN connection to on-prem, please follow these instructions: http://docs.aviatrix.com/HowTos/bgp_transitive_instructions.html

Best Practices Using Aviatrix on AWS

Gateway Sizing

For complete information on how to correctly size your gateway, please refer to our Aviatrix Documentation

Backups

When deployed in a cloud environment, the Aviatrix controller is not in the data path because packet processing and encryption is done by the Aviatrix gateways.

When the controller is down or out of service, your network will continue to be operational and encrypted tunnels and OpenVPN users stay connected and are not affected. Since most of the data logs are forwarded from the gateways directly, the loss of log information from the controller is minimal. The only impact is that you cannot build new tunnels or add new OpenVPN users.

This loosely coupled relationship between the controller and gateways reduces the impact of the availability of the controller and simplifies your infrastructure. Since the controller stores configuration data, it 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 info, refer to the Aviatrix Documentation.

More documentation

Please find our complete documentation at http://docs.aviatrix.com

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 controller (using TCP 22,443). Software and patch updates are provided by Aviatrix. For more info, contact us at sales@aviatrix.com.

At the time of launching the Quick start, we ask for your management network in order to narrow down the access to the controller. This is accomplished using a Security Group around the controller that allows access only from the management network provided and only using port 443.

All peering connections communication across peering connections are secured utilizing IPSEC tunnels.

FAQ

Q. What is a transit VPC?

A. A transit VPC is a common strategy for connecting multiple, geographically disperse VPCs and remote networks in order 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.

Q. How is an Aviatrix Global Transit VPC different from other solutions?

A. Aviatrix is the only cloud-native solution for creating a transit hub to enable simple point-and-click configuration of networking connections in AWS. The console (Aviatrix controller) gives users the ability to implement Global Transit VPC design via the REST API (no CLI required).

Q. Does the Aviatrix Solution offer High Availability?

A. Yes. The solution deploys dual gateways in both the transit hub and spoke VPCs. If one Aviatrix gateway fails, the standby Aviatrix gateway automatically connects in seconds to reduce network downtime.

Q. How much will it cost to run a transit VPC?

A. You are responsible for the cost of the AWS services used while running this deployment, as well as the Aviatrix licenses, which you can either purchase beforehand (BYOL) or obtain from the AWS Marketplace.

Q. How long will it take me to deploy the Aviatrix Global Transit Hub for AWS?

A. If you already have an AWS account, it should take less than 10 minutes to deploy the transit hub and up to 5 spoke VPCs.

Additional Resources

AWS services

- Amazon EC2
  https://docs.aws.amazon.com/AWSEC2/latest/WindowsGuide/
- AWS CloudFormation
  https://aws.amazon.com/documentation/cloudformation/
- Amazon VPC
  https://aws.amazon.com/documentation/vpc/
- 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/

Send Us Feedback

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

Document Revisions

Date	Change	In sections
November 2017	Initial publication	—

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.