Cloud Gateway AWS Controller Startup Guide

Version 08-21-2016

1 Welcome

This is a startup guide for the initial AWS AMI image launch of Aviatrix Cloud Gateway. If you are a first time user, this document is for you.

Aviatrix Cloud Gateway provides end to end cloud secure networking for you, from accessing to VPCs to inter-VPC routing, all done seamlessly and securely, so that you can have the same experience you enjoy for your on-prem network (where you never have to login to a bastion station or use a jump house to hop from environment to environment.)

Highlights of the Aviatrix Cloud Gateway:

- Scalable and highly available user VPN solution.
    - Integrated with AWS ELB, the solution scales to unlimited number of users and bandwidth.
    - Supports multi factor authentication: Google 2-step, DUO, LDAP and Okta.
    - User profile defined dynamic security access rules that allow administrator to determine access privilege to any resources in AWS at the network perimeter.
    - Supports wide range of clients: Windows, OSX, Linux, Chromebook, Android and iOS.
    - Supports log forwarders Logstash, SumoLogic, Splunk and remote syslog for complete user and network visibility.
    - Support Elasticsearch and Kibana on the controller for easy viewing of syslog events.
    - Supports Split tunnel and full tunnel mode.
    - No extra hop to access instances in different VPCs.
- Encrypted peering.
    - Multi-region and multi-cloud for AWS, Azure, Google GCloud, Azure China and Azure ARM.

    - Transitive encrypted peering
- Supports multi cloud accounts on a single platform.

The Aviatrix Cloud Gateway consists of two components, controller and gateway which is launched from the controller browser console. This guide helps you to launch the controller image in AWS. The controller image is also available in Azure and GCloud.

For the rest of the document, controller is used to refer the controller component of the solution.

2 Create an AWS EC2 Account

You need to have an AWS EC2 account to use the solution. Note that the controller supports multiple accounts with each one associated with a different AWS account, but there needs to be at least one to start with.

This AWS account can be a root account, IAM role, IAM administrator account or IAM user account with access privileges required by Aviatrix solution.

We strongly recommend you to use an IAM role for security reasons, follow instructions during onboarding time of the controller instance to setup custom security policy.

Aviatrix controller is launched with IAM role.

Before you launch the controller with IAM role, you must first create 2 IAM roles and its associated policies. Follow this link to have them setup.

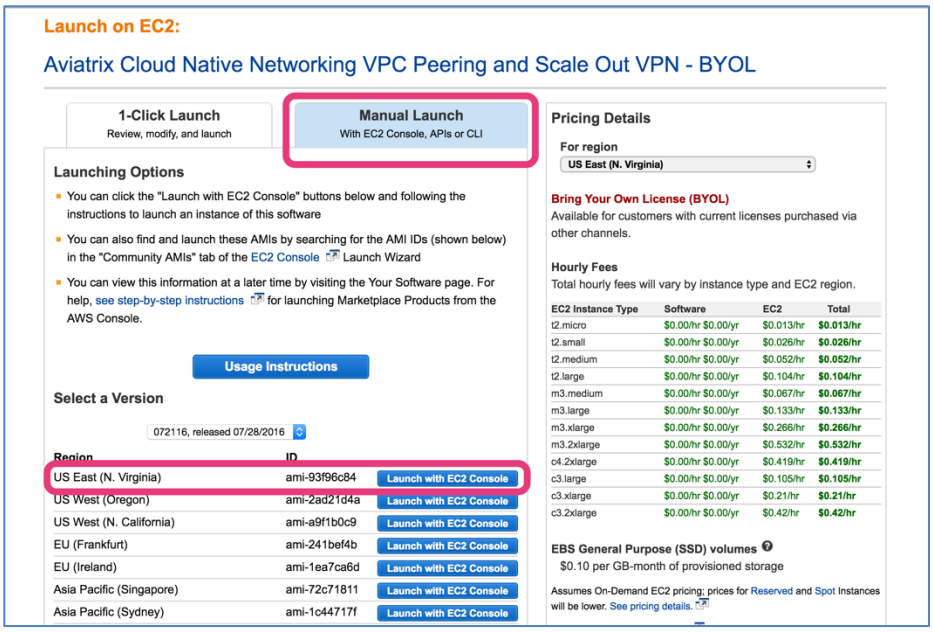
3 Launch Aviatrix Controller from AWS Marketplace

Go to https://aws.amazon.com/marketplace, search for “Aviatrix” and select the image type you wish to launch.

Note if you select the BYOL image, you need a customer ID from Aviatrix for launching gateways. Send email to support@aviatrix.com or info@aviatrix.com to request a customer ID.

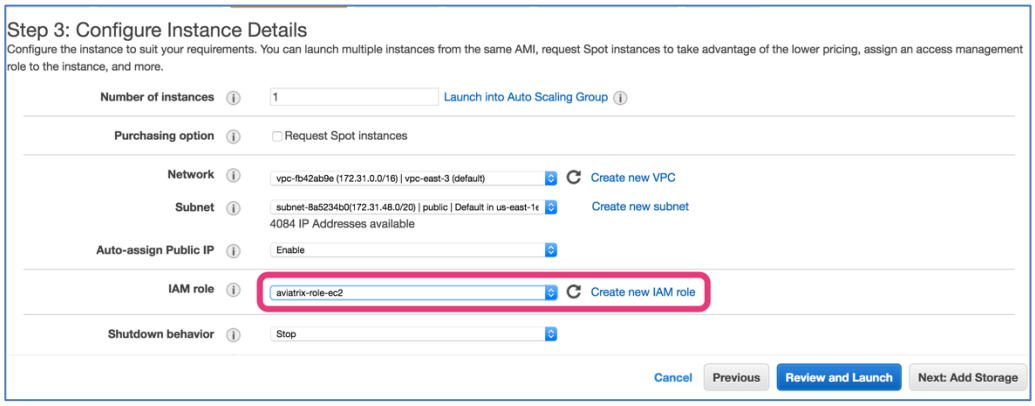
Customer ID is not needed if you select utility images such as “5 Connections” and “10 Connections”.

AWS marketplace console, select “**Manual Launch**” that takes you to EC2 console to launch with IAM role. Once you select Manual Launch, click at a region where you wish to launch the controller.

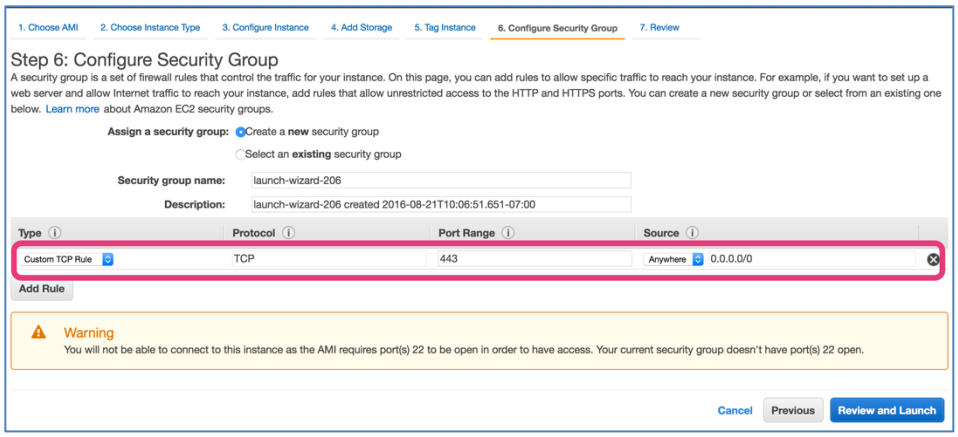


Once you are at AWS EC2 console, follow the steps below:

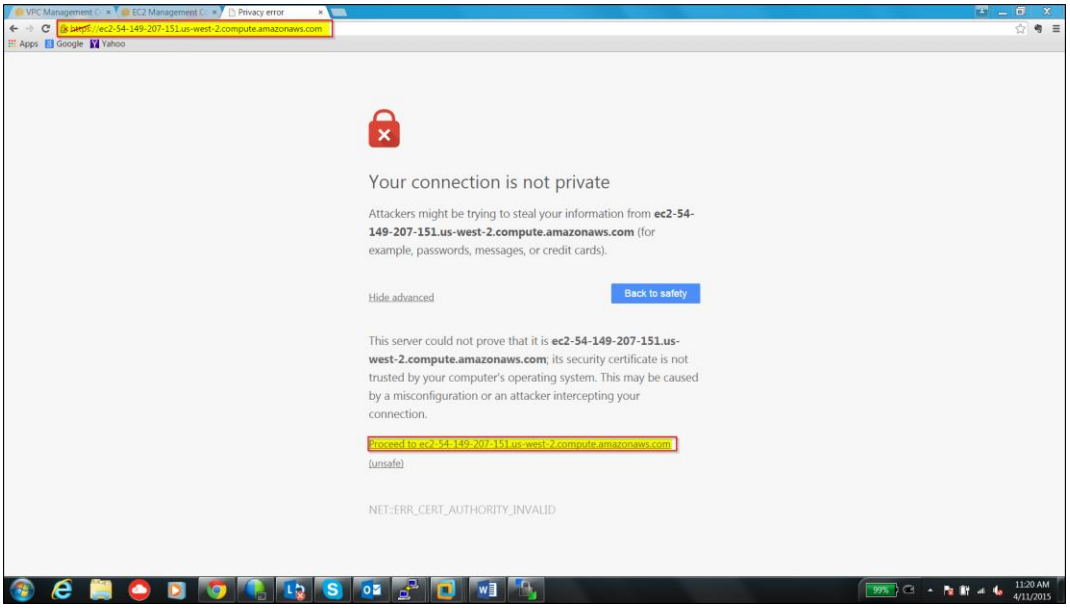
1. instance size, “t2.medium” of 4GB of memory is the minimum instance required.
2. VPC where you like to launch the controller.
3. Subnet. Make sure the subnet you select is a public subnet with IGW as its default gateway, otherwise the controller is not accessible as it does not have public IP address.
4. Enable IAM role by selecting “aviatrix-role-ec2” you created earlier, as shown below



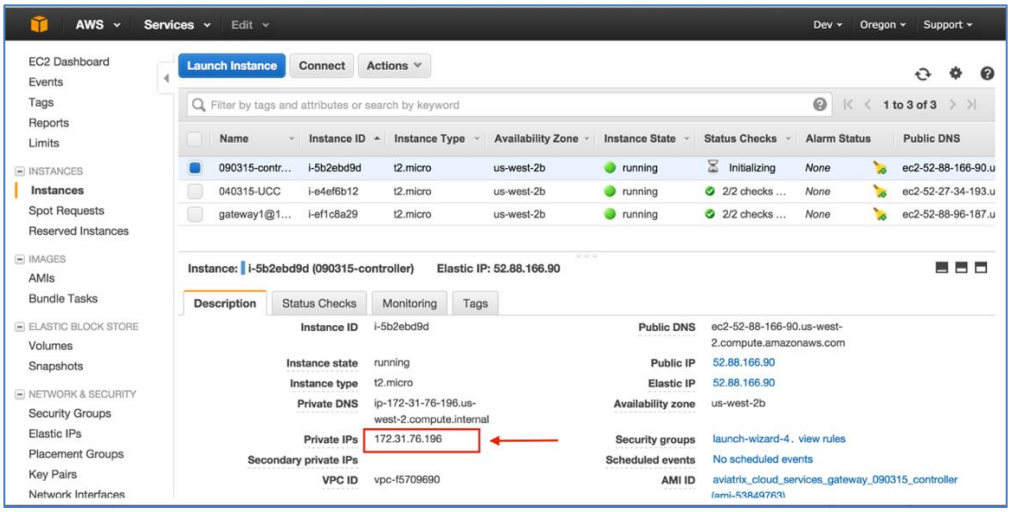
5. Edit security groups to allow inbound TCP port 443 open to anywhere, as shown below:

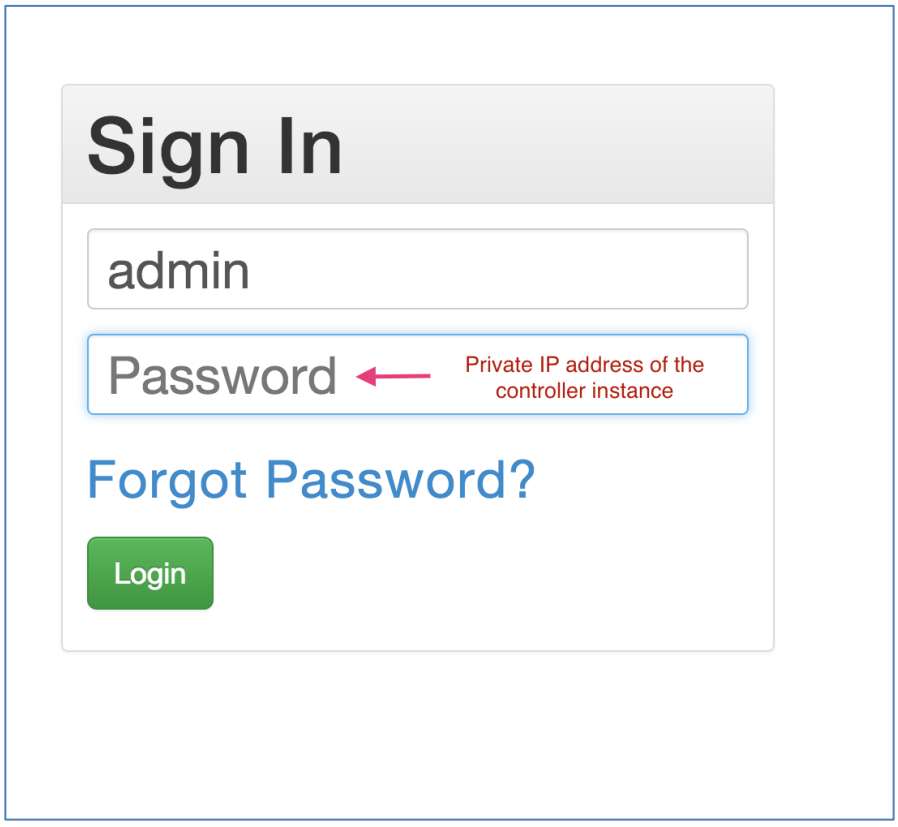


6. We recommend you to use an Elastic IP address for the controller.
7. After launch the instance, note down the instance's Private IP address and Public IP.
8. Use a browser to Login to the console.
   Use a web browser, go to https://controller_Public_IP to access the controller console, as shown below.



At the SignIn page, login in with username admin. The default password is the instance's Private IP address. You can retrieve the Private IP address from the AWS console instance panel, as shown below.





9. Once login, change your password for future accessing the console.
10. Go through the initial installation of software.
11. After the installation is complete, re-login to the controller by typing at the browser: https://controller_public_IP

12. Troubleshooting tips:

a. If you experience Login timeout error, check your instance outbound security policy to make sure it opens on port 443.
b. If you cannot find your instance's public IP address, you may have launched the instance from a private subnet. The controller instance must be launched from a public IP address.
c. The controller needs to have its inbound port 443 open to AWS address ranges as Aviatrix gateways need to communicate to the controller on this port.

4 Onboarding

After login to the browser console again, go through a few steps of onboarding to setup Aviatrix Cloud account which corresponds to AWS, Azure or GCloud account.

Under Help menu check out Frequently Asked Questions (FAQs), Reference Designs and Release Notes. All features have descriptions embedded and should be self-explanatory.

An alert message will be displayed on the Dashboard menu when a new release becomes available.

For support, send email to support@aviatrix.com. Enjoy!