



Aviatrix Cloud Controller Getting Started Guide For Azure

Last updated: April 11, 2017

Aviatrix Systems, Inc.

411 High Street

Palo Alto CA 94301

USA

<http://www.aviatrix.com>

Tel: +1 844.262.3100

TABLE OF CONTENTS

1	Overview.....	3
1.1	Aviatrix Features.....	3
2	Pre Deployment Checklist	4
2.1	Create an Azure Account.....	4
2.2	Allow Aviatrix Controller Access to Azure	4
2.2.1	Azure Resource Manager	4
2.2.2	Azure Classic	4
3	Deploying the Aviatrix Controller	6
3.1	Launch the Aviatrix Controller for Azure RM	7
3.1.1	Add Azure RM Account information	8
3.2	Launch the Aviatrix Controller for Azure Classic	9
3.2.1	Add Azure Classic Account Information	11
4	Appendix –Support.....	13
4.1	Aviatrix Support.....	13

1 Overview

Aviatrix is a next generation cloud networking solution built from the ground up for the public cloud. It simplifies the way you enable site to cloud, user to cloud, and cloud to cloud secure connectivity and access. The Aviatrix solution requires no new hardware and deploys in minutes.

The Aviatrix solution comprise of two components – Aviatrix Gateway and a Controller.

This start up guide provides step by step instructions on how to deploy the Aviatrix Controller. Once the controller is deployed then you can deploy Aviatrix Gateways to connect your users to your VNet, VNet to VNet or sites to VNet.

1.1 Aviatrix Features

Aviatrix is a scale out VPC peering solution for AWS, Azure, and Google Cloud. It offers encrypted peering across regions and clouds, and remote access to VPC from any device running OpenVPN clients. Aviatrix Gateways offer the following functionality for your cloud:

- Complete replacement for Jump Hosts or Bastion stations to SSH into VPCs – convenience for developers that security teams would approve and is a cloud best practice.
- VPC Isolation and VPC internetworking– Expand to multiple VPCs, regulate access to VPCs and connect them securely with Private IPs addresses.
- Encrypted VPC peering across AWS regions and AZs, and to Azure VNETs or branch offices – a full mesh encrypted Hybrid Cloud.
- Geo Aware SSL VPN solution that connects users securely to the nearest VPCs with support for latest SSL ciphers and MFA with Duo, Okta, Google and AD/LDAP.
- Scale Out solution integrated with ELB and all cloud native services – AWS S3, SQS, SNS, R53, CloudTrail
- Ease of deployment making it simple to onboard users or environments with overlapping CIDRs.
- Access and Event logging for audit and compliance support – log forwarding to Splunk, Logstash and Sumo Logic.
- IAM and Billing Management, Notifications and Triggers across AWS and Azure accounts.
- Guarantees higher network uptime with high availability with failover.

2 Pre Deployment Checklist

Before deploying the Aviatrix Controller, make sure the following is completed.

Pre Installation Check List

1. Create an Azure account.
2. Allow Aviatrix Controller access to Azure.

These prerequisites are explained in detail below.

2.1 Create an Azure Account

An Azure account is needed in order to deploy the Aviatrix Controller in Azure. Please reference the following URL to create your Azure Account:

<https://azure.microsoft.com>

2.2 Allow Aviatrix Controller Access to Azure

The Aviatrix Controller (AC) uses native Azure API calls to manage networking between the controller and other entities (i.e Aviatrix Gateway, on site Gateway, etc.) within Azure. The way permissions are granted depends on the Azure platform that is used; Azure Resource Manager, Azure Classic. The following sections provide instructions on how to configure permission for the Aviatrix Controller on both platforms. Configure the one that is appropriate for your environment.

2.2.1 Azure Resource Manager

Setting up access for the Aviatrix Controller for Azure Resource Manager involves registering the Aviatrix Controller, granting permissions and creating an endpoint.

Please use the following document to configure Azure RM permission for Aviatrix.

[How to setup an Aviatrix Cloud Account for Azure RM](#)

2.2.2 Azure Classic

Setting up the Aviatrix Controller for access to Azure Classic involves downloading a management API certificate from the Aviatrix Controller and then uploading it to the Azure Classic portal.

Note: You must deploy the controller before you can do this step.

Step 1: Download Management API Certificate

1. Login to the Aviatrix Controller.

2. Click Onboarding -> Next -> Skip or enter in Customer ID and Save & Next.
3. Select Azure Classic.
4. Click "Save Certificate".

Step 2: Upload Certificate to Azure Classic Portal

1. Login to Azure Classic Portal (<http://manage.windowsazure.com>).
2. On the left navigation menu click "Settings".
3. Click "Management Certificates".
4. Towards the bottom click "Upload".
5. Select the certificate file that was downloaded from the Aviatrix Controller and click the check icon.
6. Done.

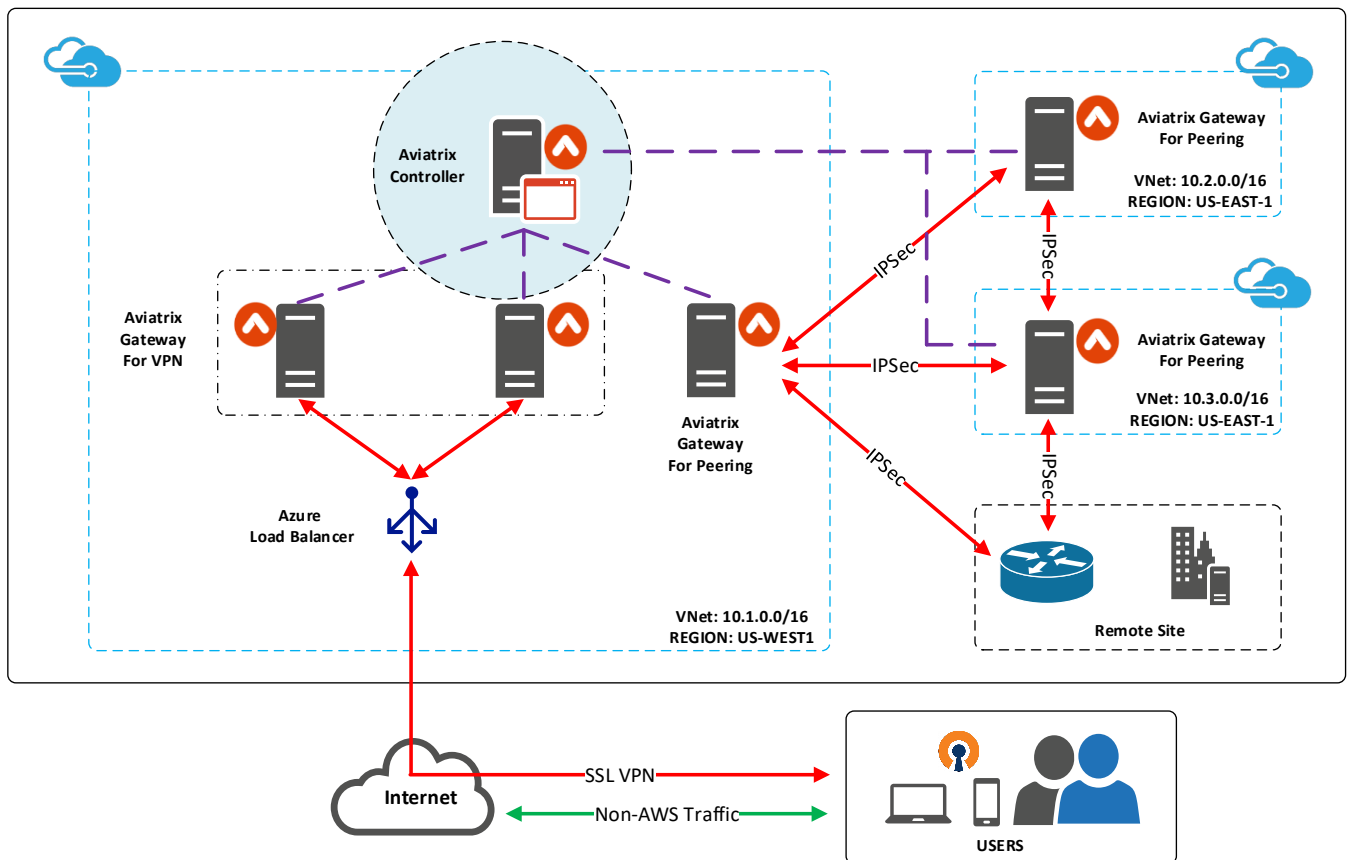
3 Deploying the Aviatrix Controller

The Aviatrix Controller exists in the form of an VM in the Azure marketplace.

The follow instructions describe how to deploy the Aviatrix Controller.

note: Only one controller is needed to managed the entire Aviatrix solution.

Below is an architecture diagram of an Azure network with multiple regions and how the Aviatrix solution can connect each network. This guide is focus on deploying the controller only.



3.1 Launch the Aviatrix Controller for Azure RM

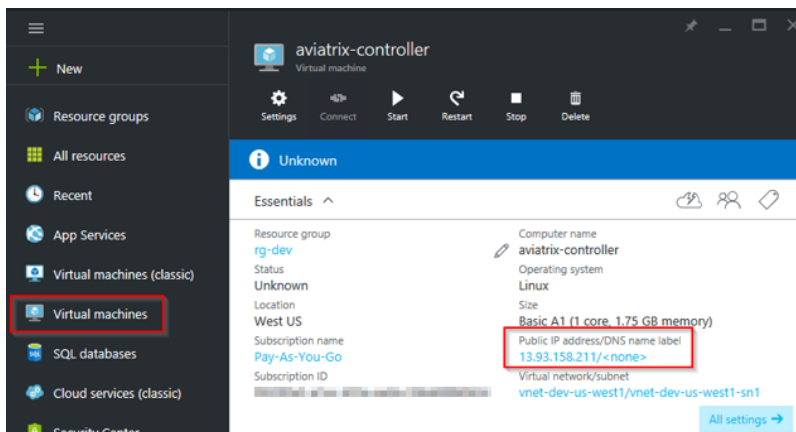
The Aviatrix Controller (AC) is available from the AWS marketplace and comes in two licensing models; BYOL and pay as you go. If you chose the BYOL model, make sure you obtain a license key (i.e. customer ID) from Aviatrix prior to deploying the AC. Please see support contact information in the appendix on how to connect with Aviatrix support.

Procedure:

1. Login to Azure Portal.
2. Navigate to the Marketplace, click Browse on the lower left and then click Marketplace.
3. From the Marketplace, search for “Aviatrix”.
4. Select either the BYOL or Pay as you go VM.
5. Click Create for “Select a deployment model”
6. At the Basics column, fill in the Name, User name, Password, Subscription, Resource group, location and then click OK.
7. At Choose a size, select the VM size, click Select.
8. At Settings, Click Network security group. (This is a critical configuration step).
9. Create a new security group and add an Inbound Rule for HTTPS (port 443). Make sure Source is Any, Source Protocol is Any and Source Port range is *. Destination Port range is 443.

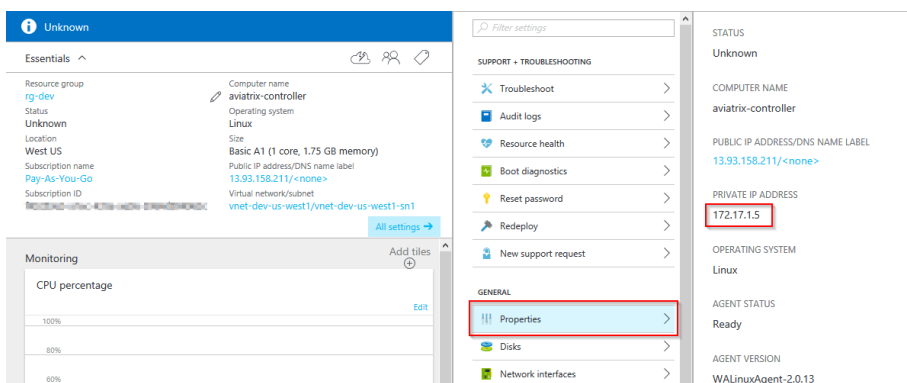
The image shows two side-by-side screenshots from the Azure Portal. The left screenshot shows the 'Add an inbound rule' button highlighted in the 'Inbound rules' section. The right screenshot shows the configuration for a new inbound rule named 'allow-https'. The configuration includes: Name 'allow-https', Priority '100', Source 'Any', Protocol 'Any', Source port range '*', Destination 'Any', Destination port range '443', and Action 'Allow'.

10. After the new security rule is added, click OK.
11. Finish launching the VM.
12. Find the VM's public IP address as show below.



13. Use a browser to access the controller VM. In this example, it is <https://13.93.158.11>

14. At the login page, enter admin as the username. The initial password is the internal IP address of the VM as shown below.



15. Done

3.1.1 Add Azure RM Account information

For the Aviatrix controller to communicate with Azure RM, the Azure RM account information must be added to the controller. How to gather the Azure RM account information is detailed in the “Allow Aviatrix Controller Access to Azure – Azure Resource Manager” section in this doc.

Procedure:

1. Login to the Aviatrix Controller console.
2. Click Onboarding -> Next.
3. If you selected a BYOL VM, enter in your customer ID; otherwise, click skip.
4. When prompted for Cloud Type, choose Azure RM Cloud.
5. Enter in the following information:
 - a. Account Name (this is an arbitrary value, ex. Devops).
 - b. Account Password (choose a password for the account).

- c. Email: (set an email for the admin account).
- d. Azure Subscription ID: (your Azure subscription id).
- e. Application Endpoint:
- f. Application Client ID:
- g. Application Client Secret:
6. Click Save & Next.
7. The Aviatrix Gateway image must be downloaded into your storage account in each region that you plan to deploy the Aviatrix solution. Select the Region and Storage Account Name and click Download. Repeat for each region.
8. Done.

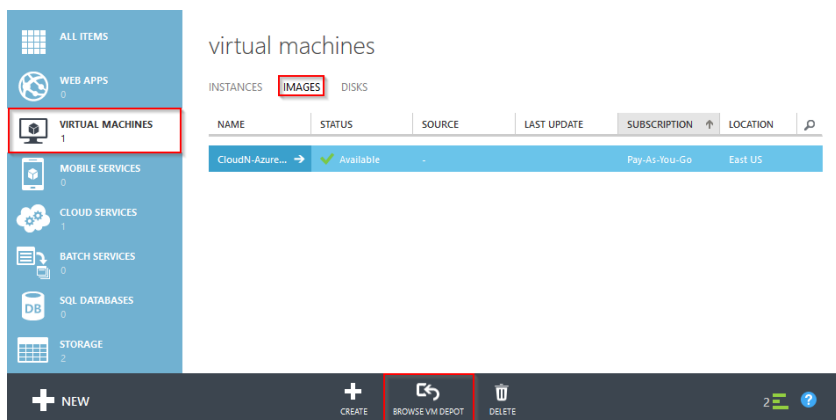
The basic Aviatrix Controller setup is now complete.

3.2 Launch the Aviatrix Controller for Azure Classic

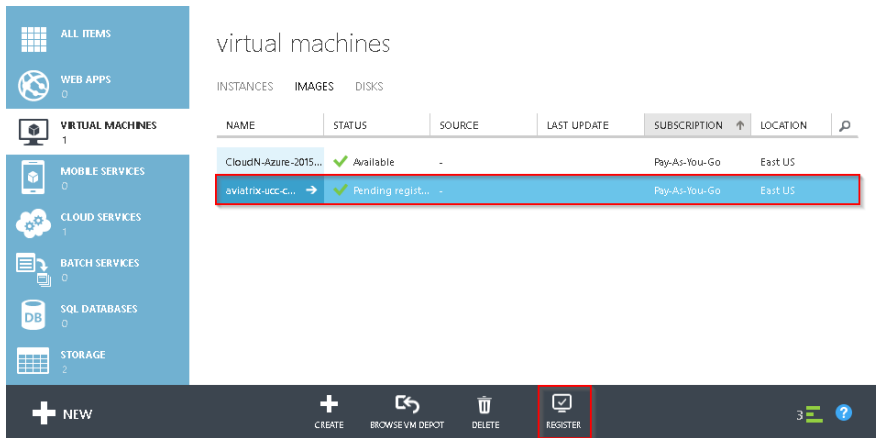
For Azure Classic deployments, the Aviatrix Controller is available as a community VM from the Azure Classic Portal. The Azure Classic Aviatrix Controller only supports the BYOL licensing model. Make sure you obtain a license key (i.e. customer ID) from Aviatrix prior to deploying the AC. Please see support contact information in the appendix on how to connect with Aviatrix support.

Procedure:

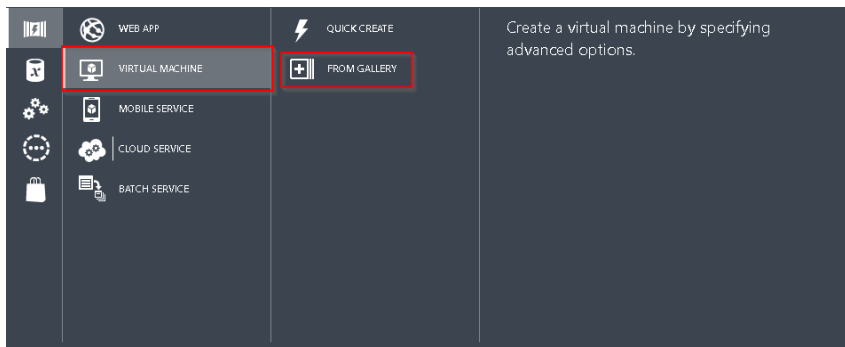
1. Login to the Azure Classic Portal (<http://manage.windowsazure.com>).
2. Click Virtual Machines on the left and then click the IMAGES tab.
3. Towards the bottom, click BROWS VM DEPOT.



4. Select “aviatrix_ucc_controller_byol_900315” image and click the next arrow (->).
5. Choose a region where you wish to launch the controller and a storage account. Then click start (check sign). The image copying will start; it should take 10-20 minutes to complete.
6. Once the image is copied, it should be in Pending registration state. Click Register to register the image.



7. Once the image is registered, the image is stored in Virtual Machines -> Gallery -> MY IMAGES.
8. Click the “+ NEW” button the lower left, then Virtual Machine -> From Gallery.



9. Choose MY IMAGES -> Select Aviatix Image (from previous step).
10. Virtual Machine Configuration
 - a. Virtual Machine Name: Enter a name of the VM.
 - b. TIER: default (standard).
 - c. Size: A1 or higher.
 - d. NEW USER NAME: default (azureuser).
 - e. AUTHENTICATION: SSH key or Password is fine.
 - f. Make sure to add a HTTPS endpoint to open port 443 as shown below.

Virtual machine configuration

CLOUD SERVICE [?]

CLOUD SERVICE DNS NAME
 aviatrix-ctl1 ✓ .cloudapp.net

REGION/VIRTUAL NETWORK [?]
 vnet-dev-use1-cl ▼

VIRTUAL NETWORK SUBNETS
 vnet-dev-use1-cl-sn1(10.132.0.0/24) ▼

AVAILABILITY SET [?]
 (None) ▼

ENDPOINTS

NAME	PROTOCOL	PUBLIC PORT	PRIVATE PORT
SSH	TCP	22	22
HTTPS	TCP	443	443
<input type="button" value="ENTER OR SELECT A VALUE"/>			

PRICING INFORMATION
 Pricing varies based on the subscription you select to provision your virtual machine.

← →

 aviatrix-ucc-controller-byol-090315

 Aviatrix Cloud Service Gateway Controller
[More](#)

OS FAMILY

Linux

OS STATE

Generalized

NUMBER OF

DISKS

1

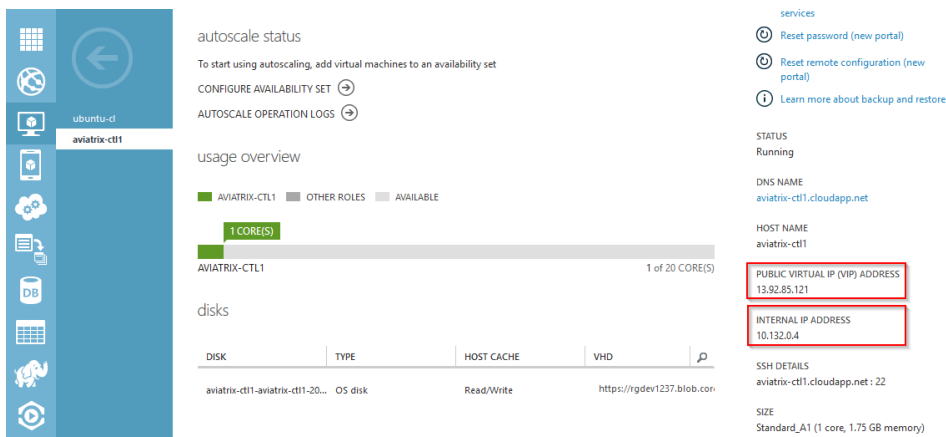
SUBSCRIPTION

Pay-As-You-Go

LOCATION

East US

11. Once the VM is launched, use its VIP to access the controller.



autoscale status
 To start using autoscaling, add virtual machines to an availability set
 CONFIGURE AVAILABILITY SET ➔
 AUTOSCALE OPERATION LOGS ➔

usage overview

■ AVIATRIX-CTL1 ■ OTHER ROLES ■ AVAILABLE

1 CORE(S)

AVIATRIX-CTL1 1 of 20 CORE(S)

disks

DISK	TYPE	HOST CACHE	VHD
aviatrix-ctl1-aviatrix-ctl1-20...	OS disk	Read/Write	https://rgdev1237.blob.com

services

- ⚙ Reset password (new portal)
- ⚙ Reset remote configuration (new portal)
- ℹ Learn more about backup and restore

STATUS
 Running

DNS NAME
 aviatrix-ctl1.cloudapp.net

HOST NAME
 aviatrix-ctl1

PUBLIC VIRTUAL IP (VIP) ADDRESS
 13.92.85.121

INTERNAL IP ADDRESS
 10.132.0.4

SSH DETAILS
 aviatrix-ctl1.cloudapp.net: 22

SIZE
 Standard_A1 (1 core, 1.75 GB memory)

12. Use a browser to Login to the console. In this example the URL would be, <http://13.92.85.121>

13. The default login is admin and the default password is the private IP address of the VM. In this example, it would be 10.132.0.4

14. Done.

3.2.1 Add Azure Classic Account Information

For the Aviatrix controller to communicate with Azure Classic, the Azure Classic account information must be added to the controller. How to gather the Azure Classic account information is detailed in the “Allow Aviatrix Controller Access to Azure – Azure Classic” section in this doc.

Procedure:

1. Login to the Aviatrix Controller console.
2. Click Onboarding -> Next.
3. Enter in your Customer ID and click "Save & Next".
4. For Cloud Type, select Azure Classic.
5. If you have not already done so, follow the instructions to download the management certificate from the Aviatrix Controller and upload it to Azure.
6. Enter in the following for Cloud Account:
 - a. Account Name (this is an arbitrary value, ex. Devops).
 - b. Account Password (choose a password for the account).
 - c. Email: (set an email for the admin account).
 - d. Azure Subscription ID: (your Azure subscription id).
7. Click Save & Next.
8. The Aviatrix Gateway image must be downloaded into your storage account in each region that you plan to deploy the Aviatrix solution. Select the Region and Storage Account Name and click Download. Repeat for each region.
9. Done.

The basic Aviatrix Controller setup is now complete.

4 Appendix –Support

4.1 Aviatrix Support

Standard: 8x5 Enterprise Phone Support, email support, product-specific knowledge-base and user forum is included. For Additional levels of support and support offers please visit:

www.aviatrix.com/support