IAM Role Configuration Guide

Version 08-24-2016

With the support of AWS IAM role, there is no need to enter AWS access key and secret key when creating a cloud account on Aviatrix controller. Instead, two IAM roles will be created. Aviatrix controller will use the dynamically obtained security credentials to request access to AWS resources. Role-based IAM cloud account helps to reduce the risk of AWS credentials being compromised.

To use IAM role, the Aviatrix Controller you launch must have IAM role enabled.

Setup IAM policies and roles for your own account

Before you launch an Aviatrix Controller from AWS marketplace, create the two necessary IAM roles and its corresponding policies.

Step 1. Create two IAM custom policies

1.1 Create "aviatrix-assume-role-policy":

- Login in to AWS console with your own account.
- Go to Services -> IAM -> Policies -> Create Policy -> Create Your Own Policy
- Enter the policy name, **aviatrix-assume-role-policy** , copy and paste the policy text from this link.
- Click Valid Policy to validate the policy.
- Click Create Policy button.

1.2 Create "aviatrix-app-policy":

- Login to AWS console with your own account.
- Go to Services -> IAM -> Policies -> Create Policy -> Create Your Own Policy
- Enter the policy name, **aviatrix-app-policy** , copy and paste the policy provided by this link into "Policy Document" section. In this example, the policy name is "aviatrix-app-policy", as shown below.

- Click Create Policy button.

Step 2. Create Two IAM Roles

2.1 Create "aviatrix-role-ec2" role

This role will be associated with the Aviatrix Controller. The role name MUST be exactly "**aviatrix-role-ec2**".

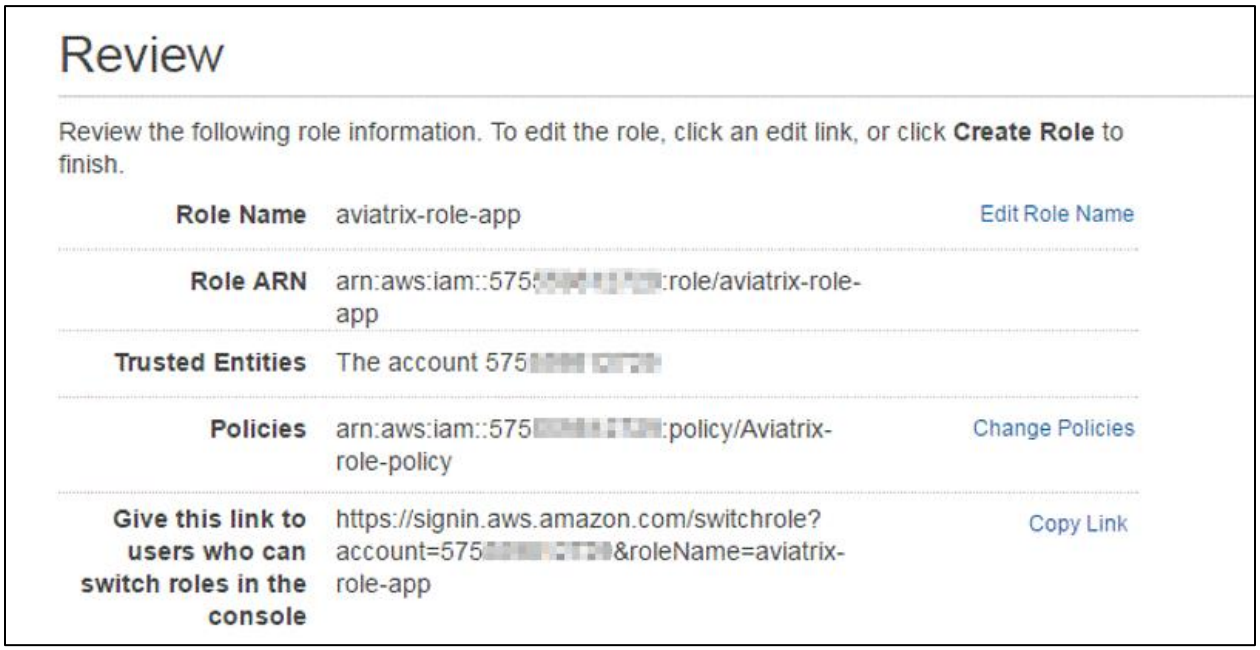
- Go to AWS console -> IAM service -> Roles -> Create New Role -> Set Role Name
- Enter a Role Name **aviatrix-role-ec2** . Click "Next Step".
- Select "**Amazon EC2**"
- Select the policy you created in the previous step, in this example, "aviatrix-assume-role-policy". Click "Next Step".
- Review the Role, and click on "Create Role". You should see something like this for Role ARN: arn:aws:iam::575xxxxx729:role/aviatrix-role-ec2
- Make a note of the above Role ARN string, it will be used for setup Aviatrix Cloud Account later.

2.2 Create an app role

This role is to be assumed by a granted AWS account. The Aviatrix controller acquires the "assume role" capability authorized by its "aviatrix-ec2-role" role. It then assumes to this service role that is granted by its own AWS account or other AWS accounts to perform AWS APIs.

- Go to AWS console -> IAM service -> Roles -> Create New Role -> Set Role Name
- Enter a Role Name, in this case **aviatrix-role-app** . Click "Next Step"
- Select "Role for Cross-Account Access"
- Select "**Provide access between AWS accounts you own**"
- Enter "Account ID" (your own account ID) and then "Next Step".
- Select the policy you created in the previous step, in this example, "aviatrix-app-policy". Click "Next Step".

- Click on “Create Role”.
- You should see something like this for Role ARN: arn:aws:iam::575xxxxxx729:role/aviatrix-role-app
- Make a note of the above Role ARN string, it will be used to setup Aviatrix Cloud Account later.



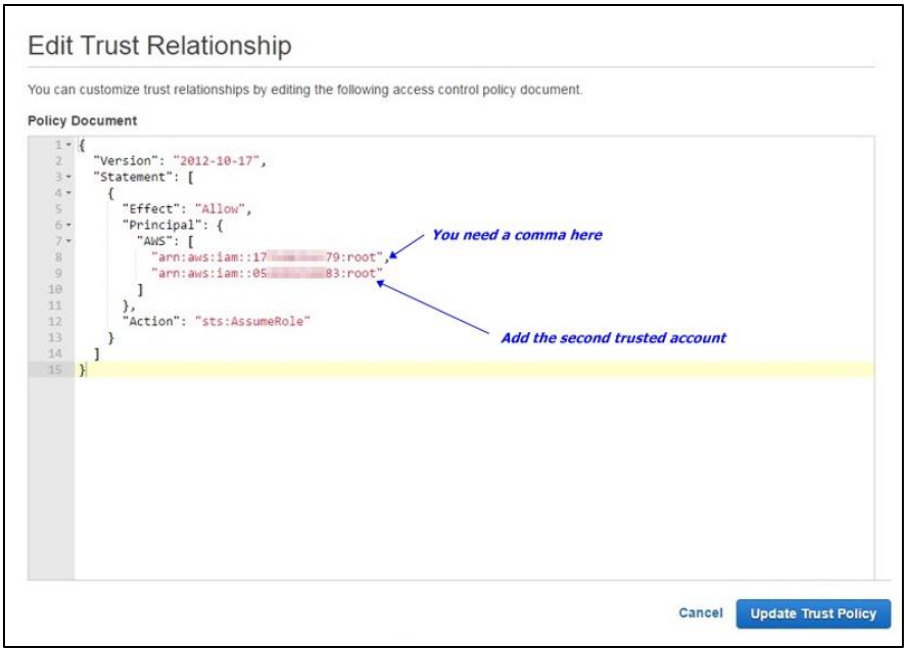
Setup IAM policies and roles for a secondary AWS account

Aviatrix supports multiple AWS account. To launch a gateway for a different AWS account, you must create the same IAM policies and roles listed above for the second account (or third, fourth, etc.). The only difference is that the IAM role in the non-primary account must trust the primary account.

Instructions:

From the secondary account

1. Create the IAM policies and roles listed above (Setup IAM policies and roles for your own account).
    a. Remember to note the ARN identifier for both roles.
2. Grant the primary account access to the aviatrix-role-app in the second account
    a. AWS console -> IAM service -> Roles > aviatrix-role-app
    b. Click Trust Relationships > Edit Trust Relationship
    c. Edit the trust relationship as follow



d. Click Update Trust Policy

3. Done

Repeat this procedure for each non-primary AWS account that will be managed by Aviatrix.