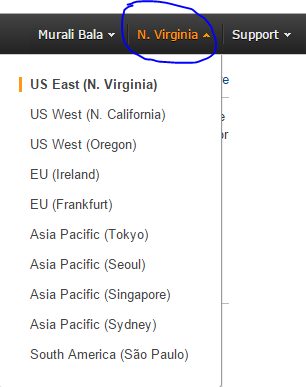
**Provisioning Your First EC2 Instance**

First thing first. You need to create an AWS Free Tier Account. This free account is only for 12months. You can access the site by visiting <http://aws.amazon.com/free/>.

The first thing you see when you login is the Oregon Region assigned to your account. Pick the region that is closest to you. You can find the option to change the region on the top right corner. I have picked N. Virginia because it is closest to me.

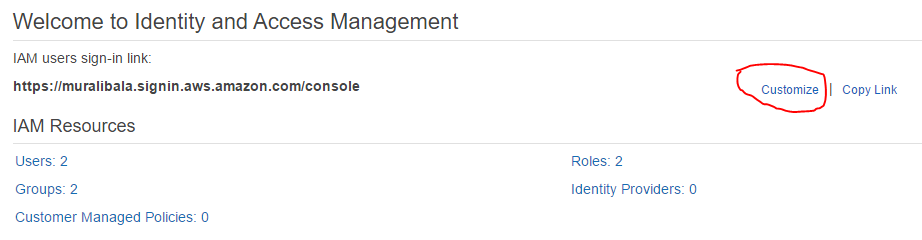


Point to remember is the Identity Access Management (IAM) is not region specific and is global.

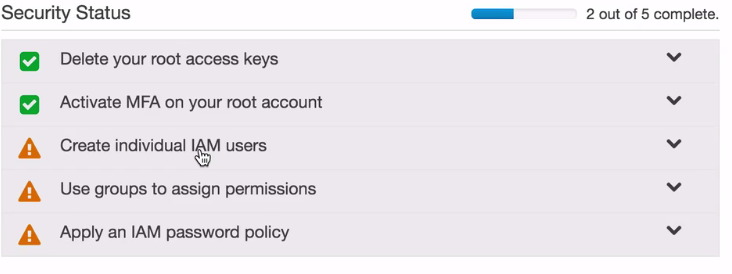
Now you are ready to setup Identity Access Management (IAM) – a centralized control for managing access to AWS resources for an organization and consists of Users, Group and Roles.

Let’s get started.

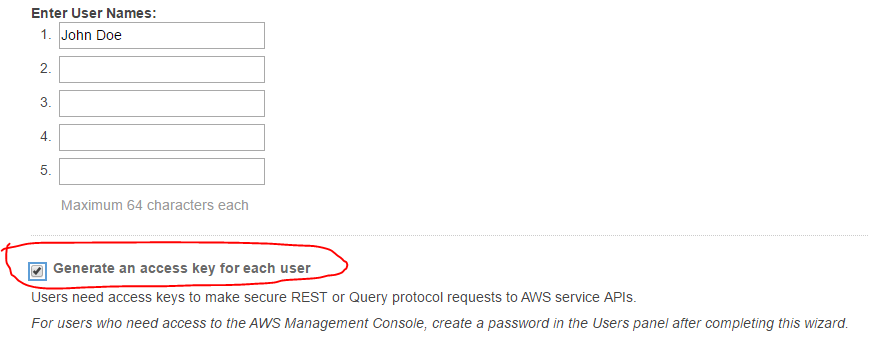
* **Customize your sign-in link.** AWS assigns a random url for you login into the console. You can customize the url, so you can share with other users/staff. To customize the url, click on the customize button and enter alias name.  Please note this does share a global DNS namespace and thus you need to make sure it is unique.



* **Activate MFA on your root account.** Activate multi factor authentication by adding another layer protection to keep your account secure.
  + Click on Manage MFA.
  + Select virtual MFA device option. We will be using Google Authenticator. Please install the app on your phone. Click Next.
  + You will see QR Code and two boxes for Authentication code.
  + Open the App and scan the QR Code.
  + Once you have successfully scanned the code, Authenticator screen will generate a random code.
  + Now plug in this code into AWS Authentication Code1. Wait for the first code time out in your phone.
  + Add the new code into the second box.
  + Click on Activate Virtual MFA.
  + Refresh screen.



* **Create individual user -** You can enter up to 5 users at one time. Access Key ID is essentially your ID and Secret Access Key your password. This secret credential is used to interact with AWS services using API. Please note that this screen is available only once. Make sure to download the information. Once you navigate away from the screen you will not be able to go back. We will create *John Doe* user.

****

*For users who need access to the AWS Management Console, create a password in the Users panel after completing this wizard. User Actions-> Create Password.*

* **Use groups to assign permission -** Policies can be attached to users, groups and role.
  + Click on Group and create a new group - *AdminGroup*.
  + Click Next Step.
  + Under Attach Policy, search for AdministratorAccess policy and select it. Click on Next.
  + Review the information, click on Create Group.
  + Next, select the *AdminGroup* and add users to the group.
* **Apply an IAM password Policy -** Here you basically set up rules that define the type of password an IAM user can set. For example, your company may require that the password be at least one number or uppercase and so forth. This is the screen where you will configure those rules.

**Now we are ready to Provision our first EC2 instance. Oh, almost forgot. Before your provision an instance we need to set up a Role. We will be needing this Role during our launch process. So let’s create that.**

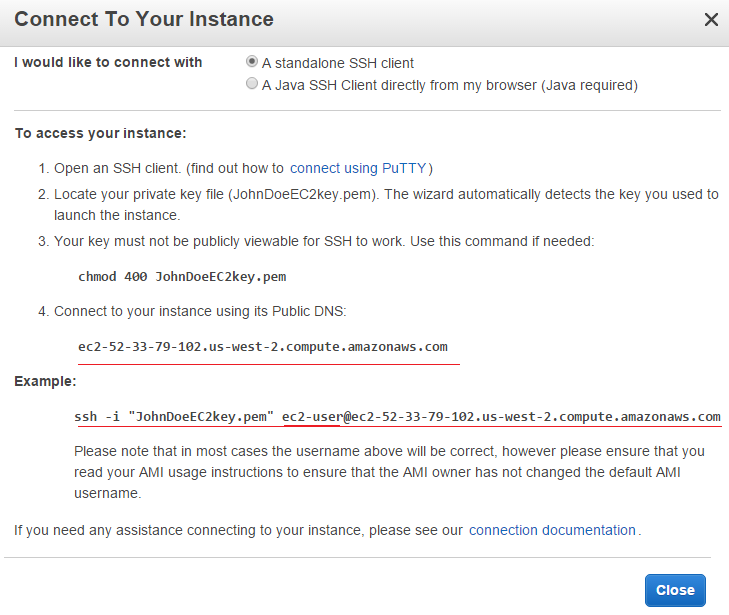
* **Create Roles.**
  + In the Set Role Name screen, enter *S3\_Access\_Role.*
  + Under Role Type, select Amazon EC2. Click Next.
  + Under Attach Policy, click on AmazonS3FullAccess, click on Next.
  + Click on Create Role.
* **Let’s Provision our first EC2 instance.**
  + In the home screen, click EC2.
  + Under Create Instance, click on the Launch Instance button.
  + Make sure free tier only is selected (left side).
  + Select Amazon Linux AMI.
  + Select the default t2.micro instance
  + Click Next Configuration.
  + You can leave everything as-is.
  + For IAM Role, select the Role you (S3\_Access\_Role) that we created.
  + Check the Protect against accidental termination under Enable termination protection.
  + Under Advance Details (**Optional**). This is really optional but can do some really cool stuff here. You can type the commands you want the instance to execute automatically.

#!/bin/bash

yum update –y

* + Click on Next: Add Storage.
  + Change the Volume type to use General Purpose SSD. Better and faster.
  + Click on Next: Tag Instance.
  + Add the following tags -
    - **Name**     -   *MyfirstEC2Instance*
    - **Owner**   -   *John Doe*
  + Click Next:Security group
  + Currently, you can only access this instance via SSH/22. But if you want to access the instance via Public IP over port 80, you need to add a new Rule for HTTP.
  + Click on Add Rule and Select Http.
  + Click on Review and Launch.
  + Review Instance Launch basically summarizes your selection. Now click on Launch.
  + **Very Important.** Now you will be presented an option to select an existing key pair or create a new key pair.
  + Select "Create a new key pair"
  + Enter key pair name - *JohDoePvtKey*
  + Click Download.
  + Click Launch Instances.
  + Click on View Instances on the bottom right.

Before we connect via SSH we need to collect some information. Under instances you will see *MyFirstEC2Instance*. Select it and click on Connect. You will see the following screenshot. Pay close attention to the ones underlined with red.



* **Connecting to your new EC2 instance via SSH –** 
  + - Create a SSH directory and Copy the file JohDoePvtKey.pem.
      * **Mac users** can use SSH using their terminal.
        + Under Applicaton->Utilities and open Terminal

>ls

>Cd ssh

>ssh -i "JohnDoeEC2key.pem" [ec2-user@ec2-52-33-79-102.us-west-2.compute.amazonaws.com](mailto:ec2-user@ec2-52-33-79-102.us-west-2.compute.amazonaws.com)

* + - * + You may get a prompt saying the Authenticity of the host can't be established. Enter "yes" to continue.
      * **PC users** would need to download SSH Terminal Window Program called Putty. You will also need Putty Keygen, which basically converts .pem (private key) files to .ppk. <http://www.chiark.greenend.org.uk/~sgtatham/putty/download.html>
        + Run Putty Key Generator Program.
        + Click on Load Key.
        + Navigate to you SSH folder that you created and select the .pem file. If you don’t see the file, make sure All Files (bottom right) is selected in Open dialog box.
        + Click on Save Private Key File.
        + **Run Putty.**

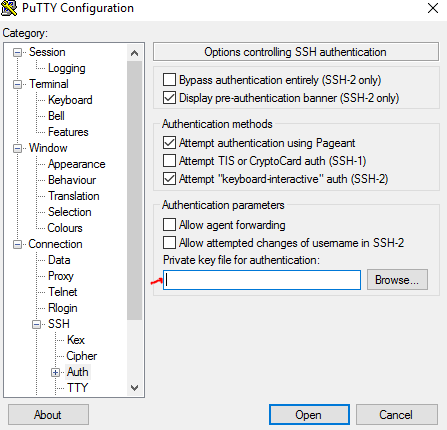
Under hostname enter **ec2-52-33-79-102.us-west-2.compute.amazonaws.com** or the public IP address. You can locate this information in the bottom right portion of your instance screen**.**

Click on Connection->Data. Enter ec2-user under Auto-login username

Under Connection->SSH->Auth, click on browse and select the .ppk file that you saved previously.

Now one last step. Click on Session, under Saved Session textbox enter a name for this session and click on the Save button. Next time when you run putty, all you have to do is select this named session and click on Load.

Now select the saved session and click on Load.



* **Update your EC2 Instance -** Once you are connected, please make the instance is up to date. For that to happen:

> sudo yum update

Troubleshooting Connecting to Your Instance

If you are having issues connecting to your instance, please click on the following link to resolve the issue -

<http://docs.aws.amazon.com/AWSEC2/latest/UserGuide/TroubleshootingInstancesConnecting.html>

And that’s it. You have provisioned your fist instance of Amazon EC2. Congratulations!!