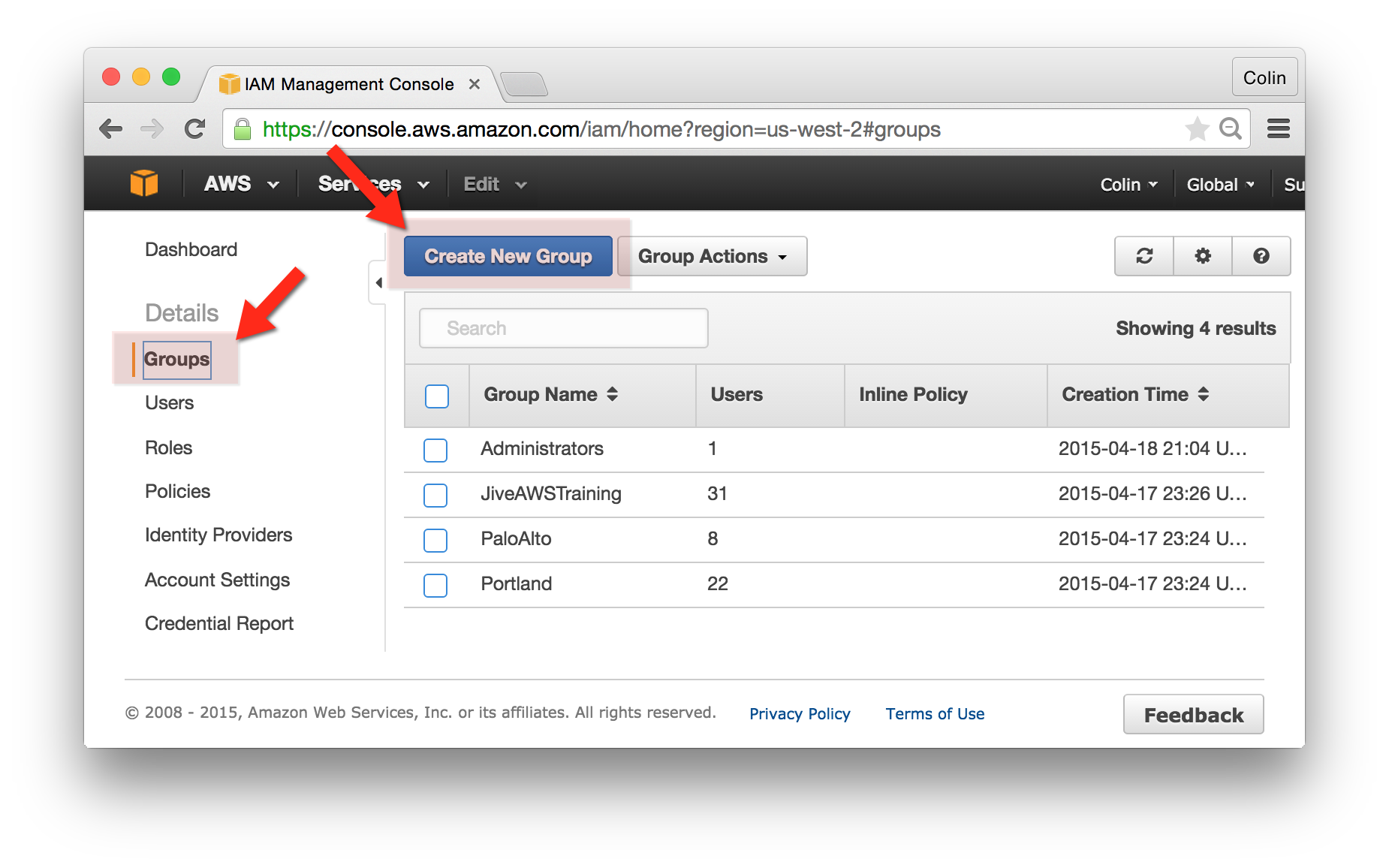
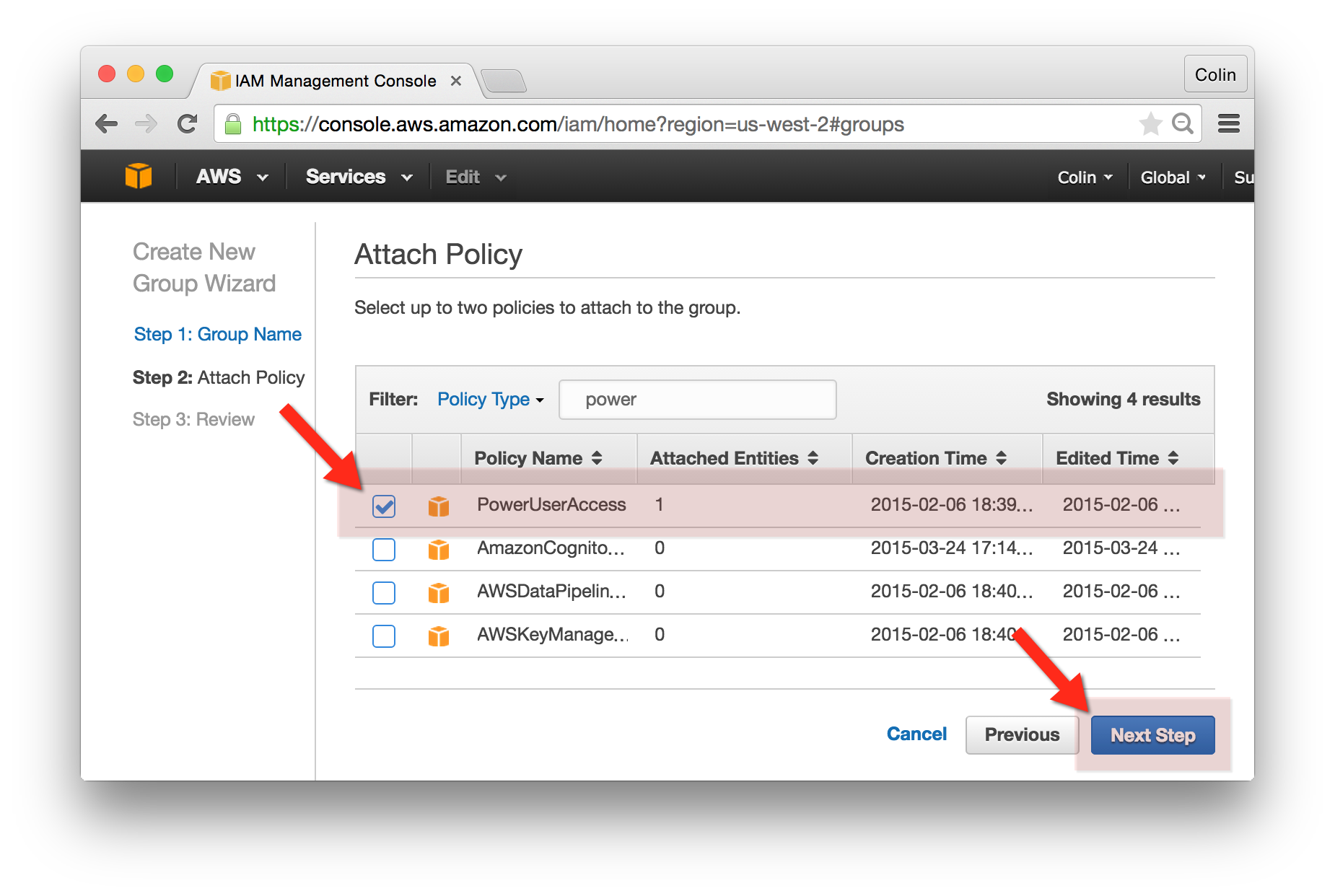
## Overview:

We will be creating one IAM Group named “Developers” and two “Developer” IAM Users.

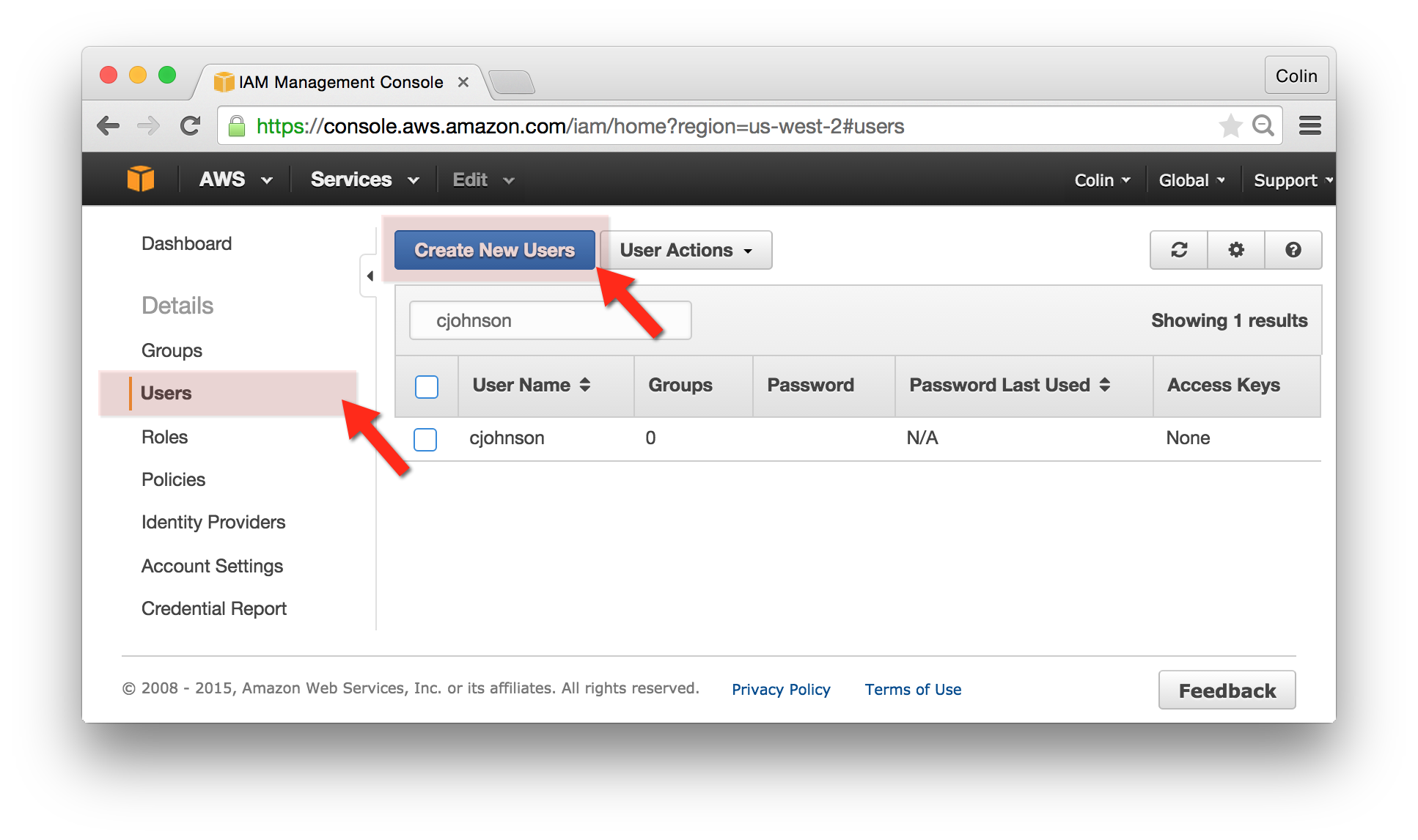
## Create an IAM Group:

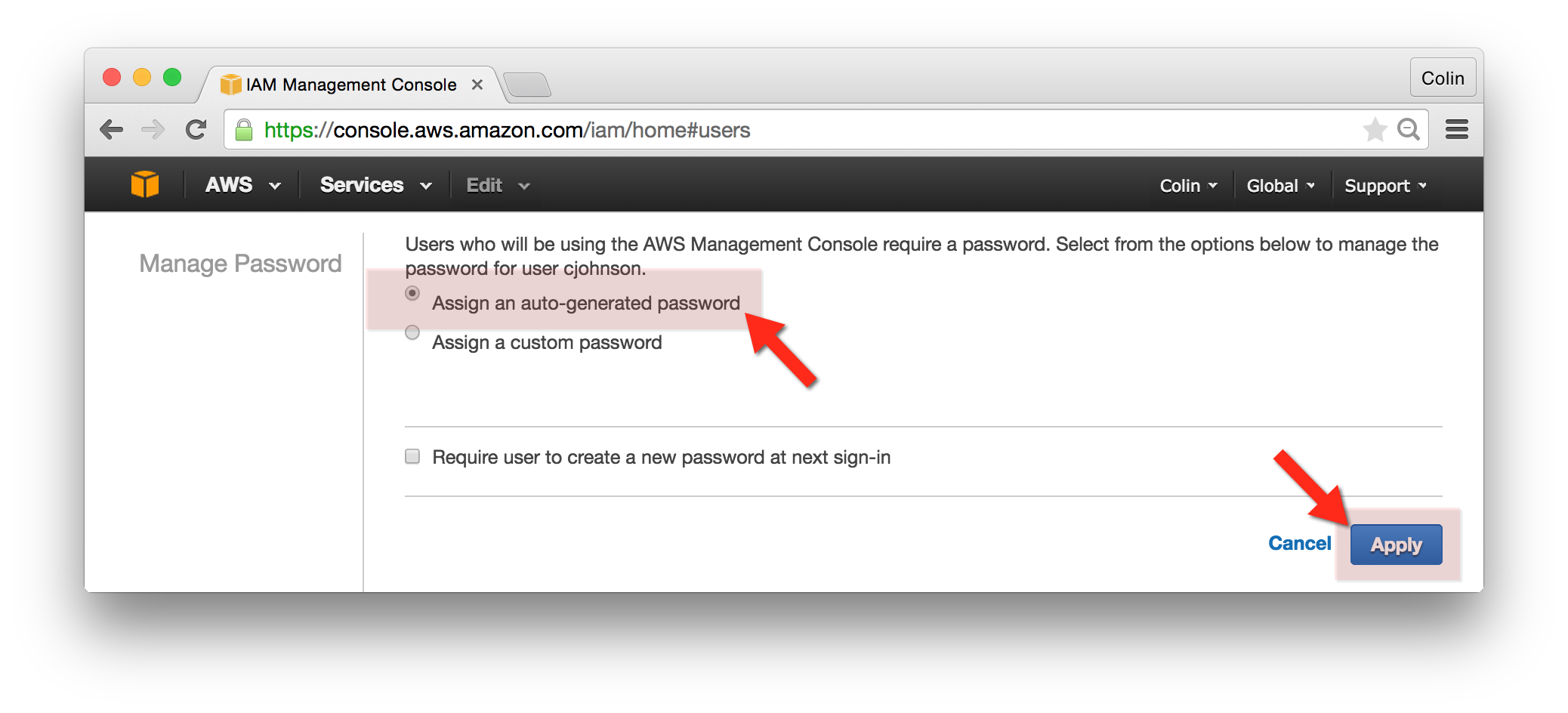
1. Go the AWS Identity and Access Management Console and click “Groups” from the left-hand navigation.
2. Click “Create Group”  
   
3. Group Name:
   1. Group Name: yourgroup-yourname
   2. Attach a Policy:
      1. select a policy – I might suggest the “PowerUserAccess” or the “ReadOnlyAccess” policy



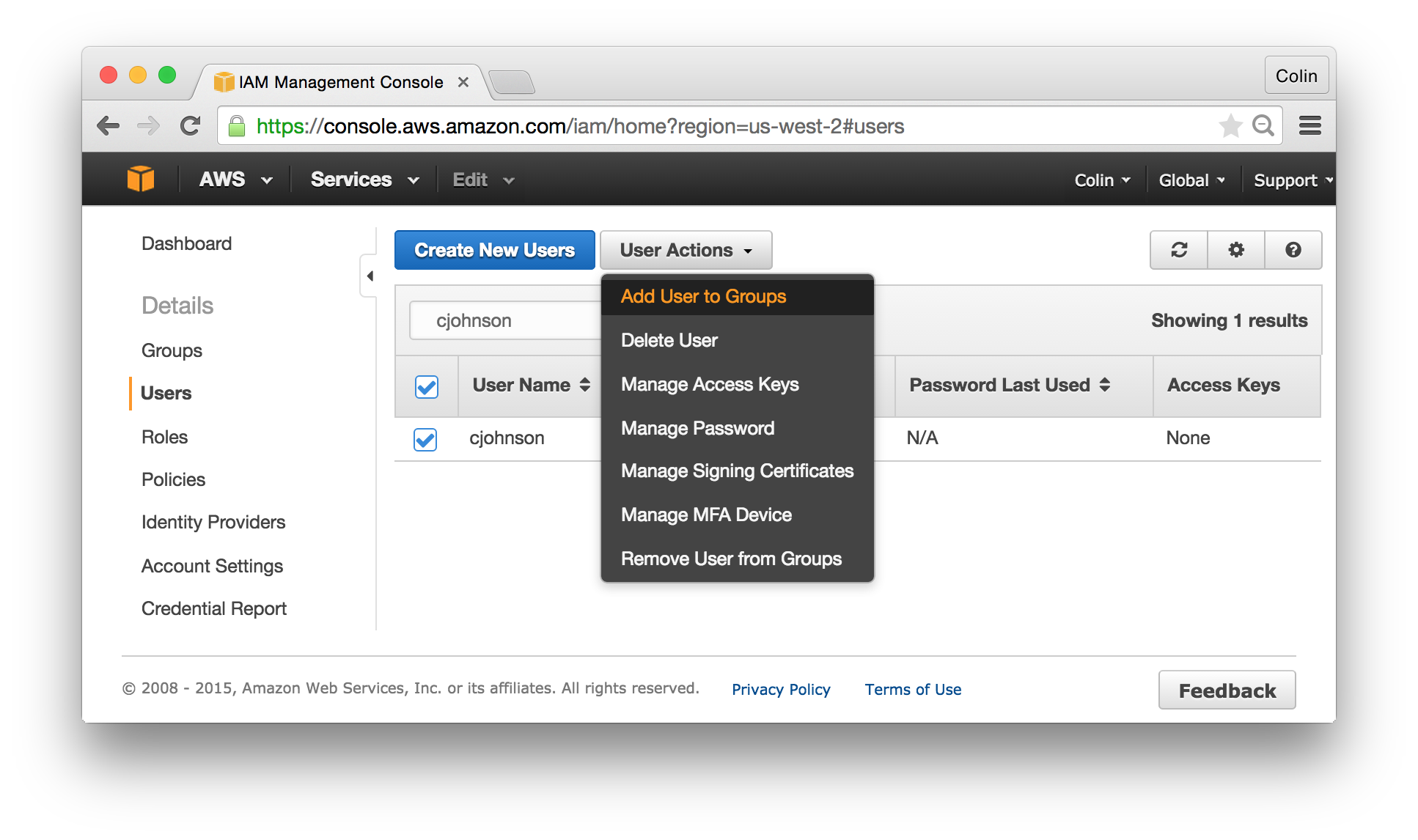
1. Review:
   1. Review the new group
   2. Click “Create Group” when done

## Create an IAM User:

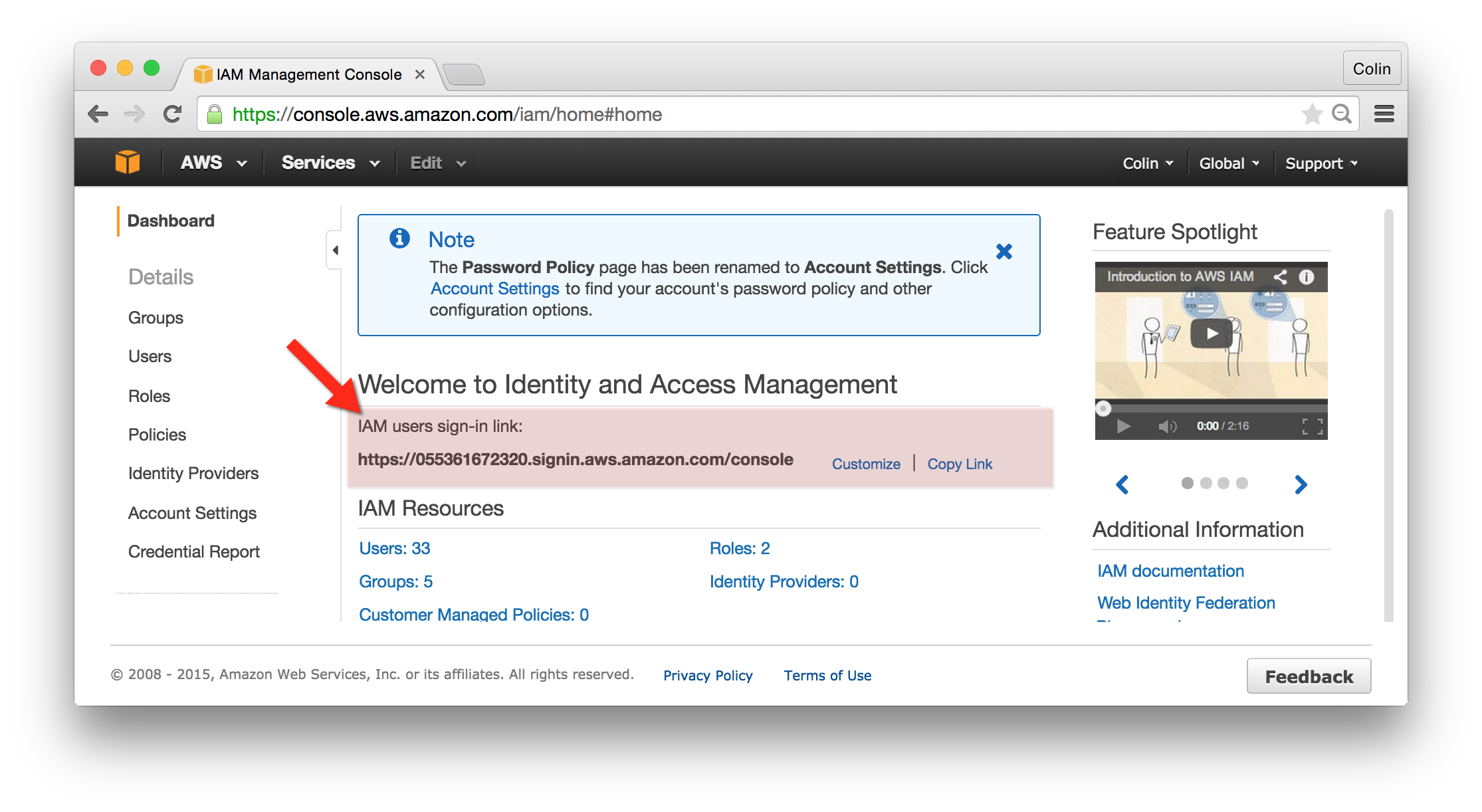
1. Go the AWS Identity and Access Management Console and click “Users” from the left-hand navigation.
2. Click “Create New Users”  
   
3. Enter a User Name and press “Create”
4. Select the newly created user in the User List, click the “User Actions” drop-down and select “Manage Password”
   1. Choose “Assign an auto-generated password”
   2. Click Apply



* 1. Click “Show User Security Credentials” on the next screen – note this password.
  2. Press Close.

1. Select the newly created user in the User List, click the “User Actions” drop-down and select “Add User to Group”
2. Search for the “yourgroup-yourname” group created in the previous step and click “Add to Groups”

## Login with the newly created IAM User:

1. Go the AWS Identity and Access Management Console and click “Dashboard” from the left-hand navigation.
2. Copy the “IAM Users Sign in Link” (it will look similar to <https://055361672320.signin.aws.amazon.com/console>)  
   
3. Open a new browser window and paste this URL in.
4. Sign in as this account
5. Attempt to perform an action that was **not** granted to this account. For instance – try to delete your usual account.