Amazon Web Services
Hands-On IAM

December, 2012

Table of Contents

Overview 3

Sign-up for EC2 3

Create Identity & Access Management Credentials 4

- Create Admin Group 4
- Grant Permissions 5
- Add Users 6
- Login as User 9

Overview

This lab will walk the user through creating an account and signing-up for EC2, creating an IAM administrator group, IAM user account, and assigning the user to the administrator group. The following is high-level overview of this lab:

- Create Account & Sign-up for EC2
- Create & Use an IAM Account

Sign-up for EC2

To use Amazon EC2, you need an AWS account. If you don't already have one, you'll be prompted to create one when you sign up for Amazon EC2. Signing up for Amazon EC2 also automatically signs you up for Amazon Simple Storage Service (Amazon S3) and Amazon Virtual Private Cloud (Amazon VPC), which are closely integrated with Amazon EC2.You're not charged for any of the services unless you use them.

To sign up for Amazon EC2

1. Go to http://aws.amazon.com/ec2 and click **Sign Up for Amazon EC2**.
2. Follow the on-screen instructions.

Part of the sign-up procedure involves receiving a phone call and entering a PIN using the phone keypad.

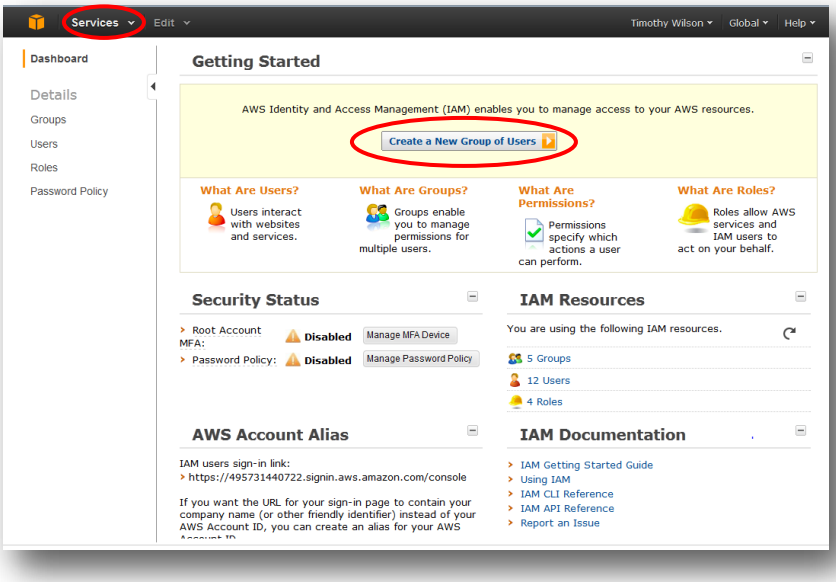
Create Identity & Access Management Credentials

After logging into the AWS console for the first time, you are connecting into AWS as the account owner. AWS Identity and Access Management (IAM) enables you to create and manage users under the umbrella of your AWS account. You use IAM in conjunction with other AWS products to control access to the AWS resources in your AWS account. This section will walk you through the following:

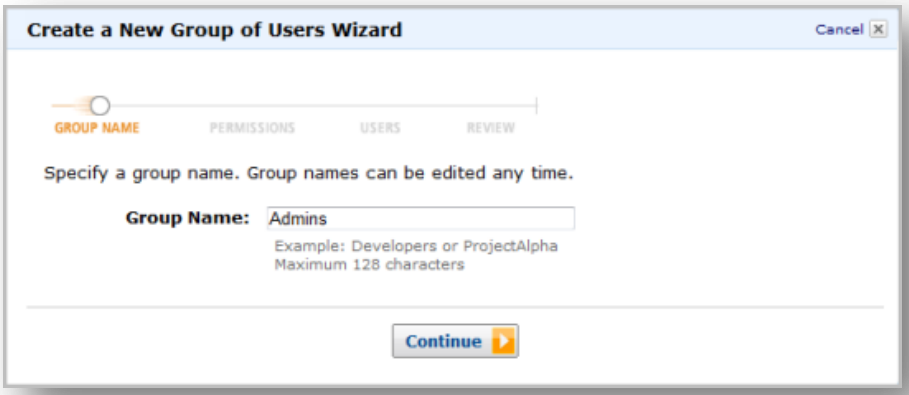
1. Create Admin Group
2. Grant Permissions
3. Add Users
4. Login as User

Create Admin Group

1. Sign in to the AWS Management Console and go to the **IAM Dashboard** by navigating to IAM through the Services drop-down menu.
2. From the IAM Dashboard, click Create a New Group of Users.

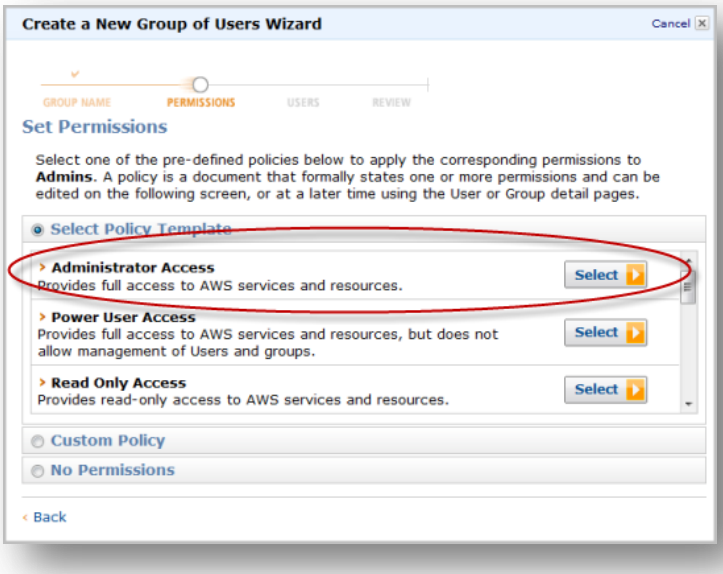


3. Name the group *Admins*, and then click Continue.



Grant Permissions

4. Next, you need use a policy to assign permissions to your Admins group. A policy is a document that formally states one or more permissions. To select a policy template, next to Administrator Access, click Select.

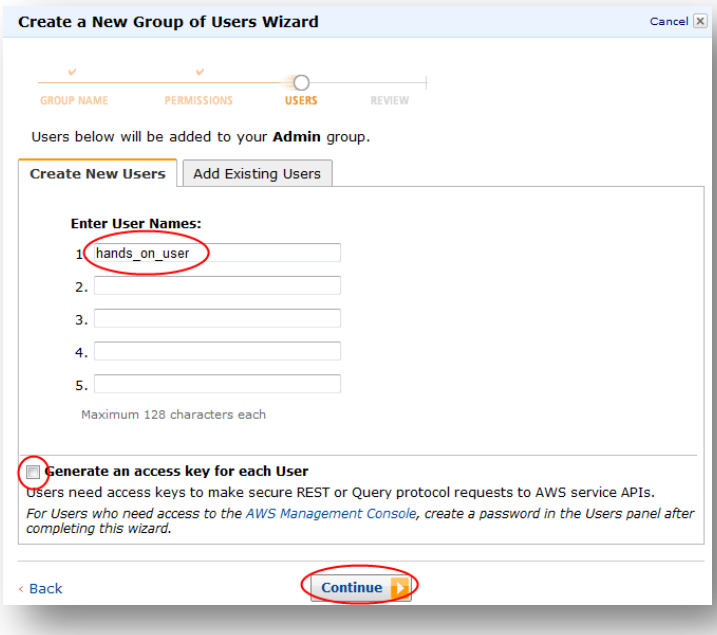


   IAM provides several policy templates you can use to automatically assign permissions to the groups you create. The Administrator Access policy template gives the Admins group permission to access all account resources, *except* your AWS account information as described previously.
5. **Click Continue** on the Edit Permissions page. For future reference, you can optionally edit the policy and the policy name before applying the policy to a group. If you used a

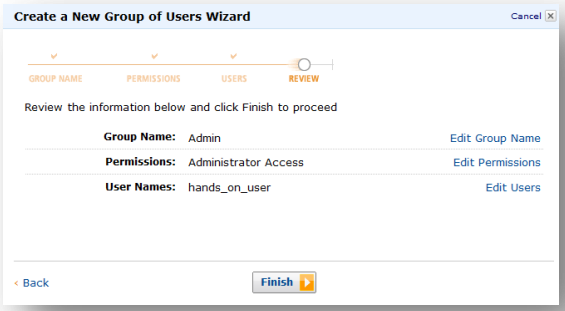
policy template, the default policy name includes the template name and today's date.

Add Users

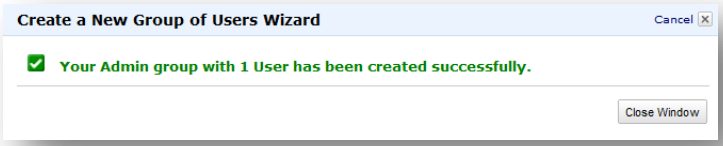
6. Add yourself as an administrator for your AWS account. Also add any other users you want to be administrators for your AWS account. Uncheck *Generate an access key for each User* (these can be created later if required). Click Continue.



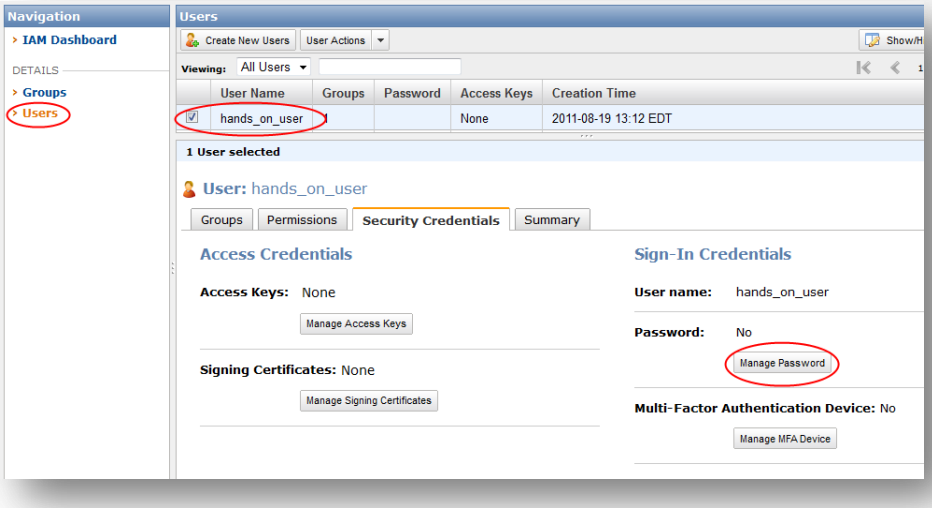
7. Review the group details on the confirmation screen, and then click Finish.



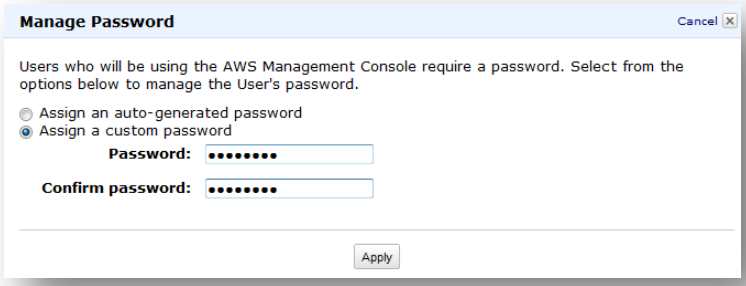
8. Click **Close Window** to continue. Now you are now ready to add passwords to your users' profiles.



9. Users who will access the AWS Management Console will need a password. To add a password to a user profile
    a. On the Navigation pane, click Users.
    b. Select the user who you want to create a password for, and then select the user Security Credentials tab.
    c. Click Manage Password.

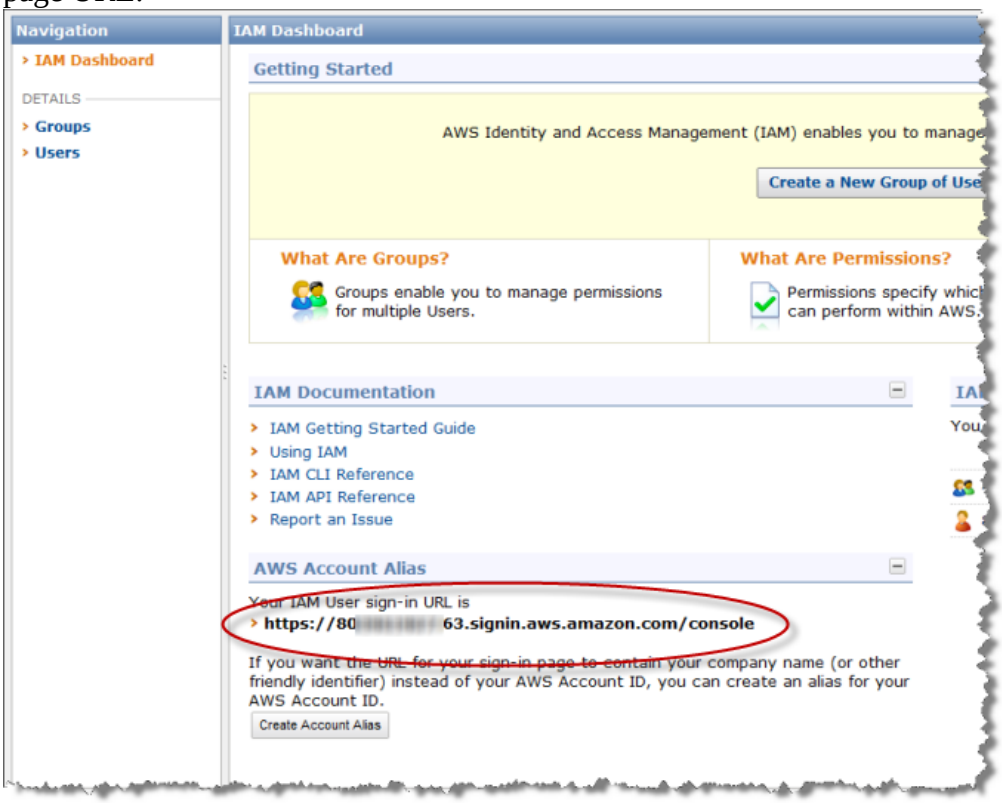


    d. Click *Assign a custom password* and then enter and confirm the password. When you are finished, click Apply.



Login as User

10. You have now created an Admins group, added permissions for the group, and added users to the group. Navigate to the IAM dashboard and locate the AWS account sign-in page URL:



11. Use this URL to login as your newly created IAM admin account.