



Training and
Certification

Introduction to Identity and Access Management (IAM)

Table of Contents

Introduction.....	3
Overview.....	3
Topics Covered.....	3
Login to the AWS Management Console	3
Using qwikLAB to login to the AWS Management Console.....	3
Access Identity and Access Management (IAM).....	4
Create a Group and User with Full Permissions (Administrators).....	4
Create an Administrators Group and a Corresponding User	4
Update Password Policy and Generate a Password.....	6
Update Password Policy	6
Generate a Password for Adele.....	7
Log in with the IAM Sign-In URL as an Administrator	8
Login as the Administrator (Adele)	8
Create a Group and User with Limited Permissions (Developers).....	8
Create a Group with EC2 Access Only and a Corresponding User	8
Generate a Password for Dave	10
Login as a User with Limited Permissions.....	10
Login as a Developer (Dave)	10
Conclusion.....	12
Resources	12

Copyright © 2013 Amazon Web Services, Inc. and its affiliates. All rights reserved.
This work may not be reproduced or redistributed, in whole or in part,
without prior written permission from Amazon Web Services, Inc.
Commercial copying, lending, or selling is prohibited.

Questions, feedback or corrections? Email us at aws-course-feedback@amazon.com.

Introduction

Overview

AWS Identity and Access Management (IAM) enables you to securely control access to AWS services and resources for your users. Using IAM you can create and manage AWS users and groups and use permissions to allow and deny their permissions to AWS resources.

Topics Covered



The goal of this lab is to allow you to:

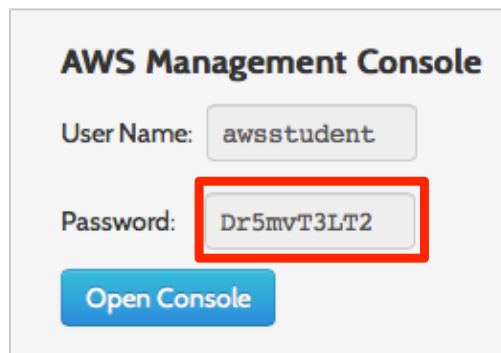
- Familiarize yourself with the Identity and Access Management (AWS) Console.
- Create a group with full, administrator permissions.
- Add a user to the Administrator group.
- Update the password policy.
- Locate and use the IAM sign-in URL.
- Create a group with limited permissions.
- Add a user to the group with limited permissions.

Login to the AWS Management Console

Using qwikLAB to login to the AWS Management Console

Welcome to this self-paced lab! The first step is for you to login to Amazon Web Services.

1. Start your qwikLAB by clicking the  button.
2. **Copy the password** into the clipboard:
3. Click the  button.
4. Login to the console:
 - a. **User Name:** `awsstudent`
 - b. **Password:** Use the password in your clipboard



AWS Management Console

User Name:

Password:

Amazon Web Services Sign In

Please enter the AWS Identity & Access Management (IAM) User name and password assigned by your system administrator to sign in.

AWS Account: 174335992060

User Name:

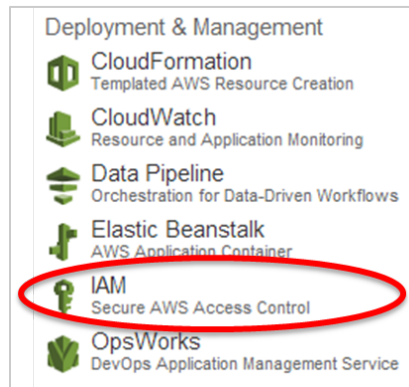
Password:

[Sign in using our secure server](#)

5. This will simulate you logging into the AWS root account.

Access Identity and Access Management (IAM)

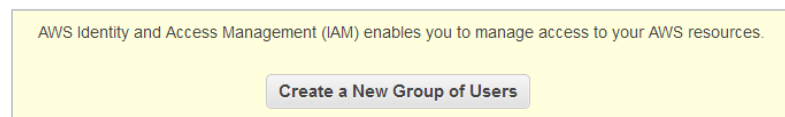
1. From the list of services, select IAM.



Create a Group and User with Full Permissions (Administrators)

Create an Administrators Group and a Corresponding User

1. In the IAM console, click "Create a new group of users".



2. Name this group Administrators.

Create a New Group of Users

Cancel X

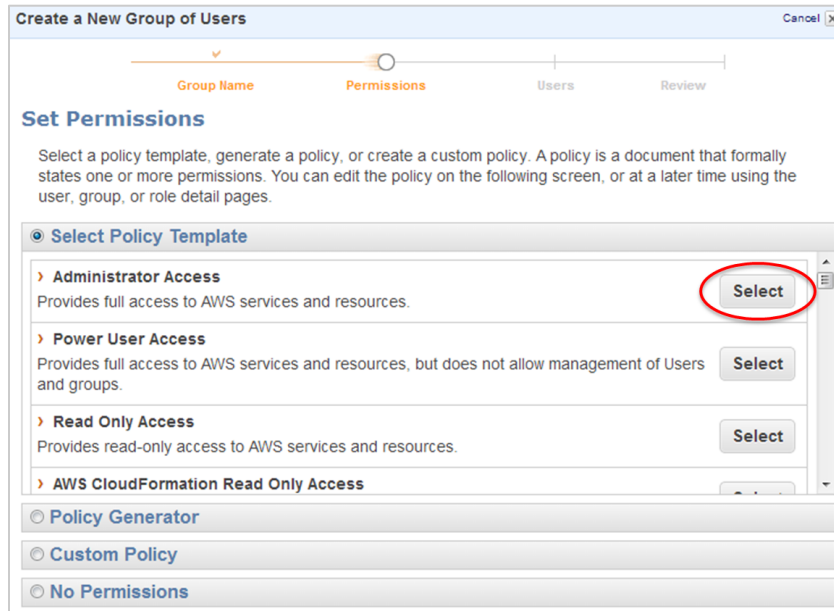
Group Name Permissions Users Review

Specify a group name. Group names can be edited any time.

Group Name:

Example: Developers or ProjectAlpha
Maximum 128 characters.

3. Click "Continue".
4. Permissions are defined in a document called a policy. In a policy, you can define what actions are allowed or denied for specific AWS resources. You can use a custom policy or use a pre-defined set of permissions by selecting a policy template.
5. Set the permissions for the Administrators group using the Administrator Access policy template.



6. Click Continue.
7. In the next screen, you will see that you can customize the permissions by editing the following policy document. In this example, we'll keep the default. Click Continue.
8. Click the "Create New Users" tab.
9. Type Adele in the users box.
10. Because Adele will only be accessing AWS through the management console, we do not need to create access keys. Uncheck the generate access keys box.
11. Click Continue.

Create a New Group of Users [Cancel X]

Group Name Permissions **Users** Review

Users below will be added to your **Administrators** group.

Create New Users Add Existing Users

Enter User Names:

1. Adele
- 2.
- 3.
- 4.
- 5.

Maximum 128 characters each

☒ **Generate an access key for each User**

Users need access keys to make secure REST or Query protocol requests to AWS service APIs.

For Users who need access to the AWS Management Console, create a password in the Users panel after completing this wizard.

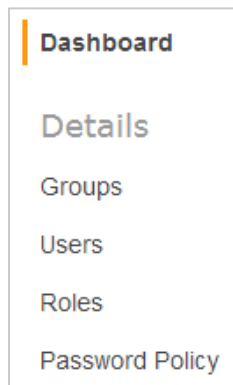
Back Continue

12. Verify that the information for the group is correct, then click “Finish” to create the Administrators group and the IAM user, Adele.

Update Password Policy and Generate a Password

Update Password Policy

1. Click “Password Policy” under Details in the left column.



2. Change the Minimum Password Length to 8.
3. Check all policies:
 - a. Require at least one uppercase letter
 - b. Require at least one lowercase letter
 - c. Require at least one number
 - d. Require at least one non-alphanumeric character
 - e. Allow users to change their own password

4. Click “Apply Password Policy”.

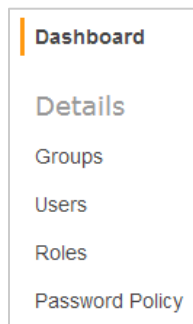
Modify your existing password policy below.

Minimum Password Length:

- ☒ Require at least one uppercase letter ?
- ☒ Require at least one lowercase letter ?
- ☒ Require at least one number ?
- ☒ Require at least one non-alphanumeric character ?
- ☒ Allow users to change their own password ?

Generate a Password for Adele

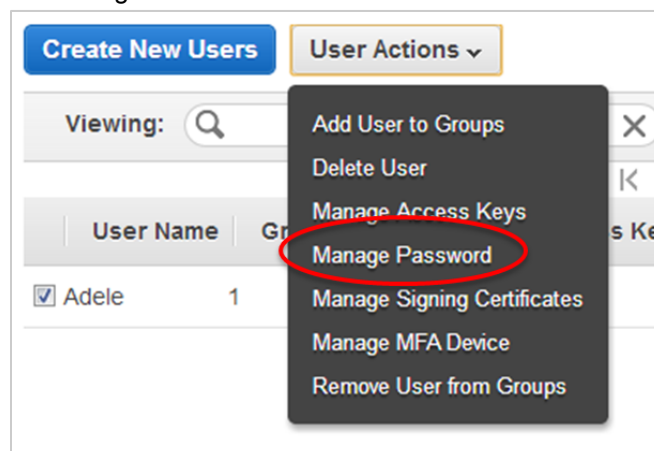
1. Click “Users” under Details in the left column.



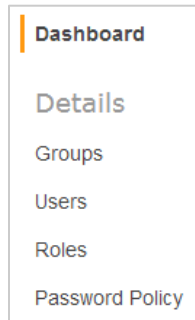
2. Check the box next to Adele.

User Name	Groups
<input checked="" type="checkbox"/> Adele	1

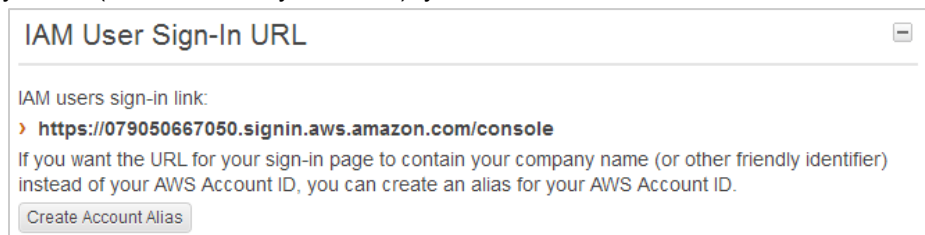
3. Under “User Actions”, click “Manage Password”.



4. Choose “Assign an auto-generated password” and click “Apply”.
5. Click “Download Credentials” button in the Manage Password window.
6. Click “Close Window”.
7. Click back to the IAM Dashboard by clicking “Dashboard” in the left column.



8. Under IAM User Sign-In URL, copy the link shown. If you want the URL for your sign-in page to contain your company name (or other friendly identifier), you can click “Create Account Alias” to change this.



Log in with the IAM Sign-In URL as an Administrator

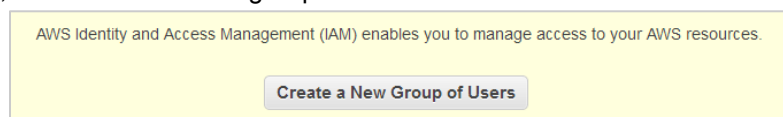
Login as the Administrator (Adele)

1. Use the IAM User Sign-In URL that you copied in the last step.
2. Login with Adele’s username and password from the credentials that you downloaded earlier.

Create a Group and User with Limited Permissions (Developers)

Create a Group with EC2 Access Only and a Corresponding User

1. From the list of services, click on IAM.
2. In the IAM console, click “Create a new group of users”.



3. Name this group Developers.

The screenshot shows the 'Create a New Group of Users' wizard with the 'Group Name' step selected. The progress bar has four steps: Group Name, Permissions, Users, and Review. The 'Group Name' step is highlighted with an orange circle. Below the progress bar, the text says 'Specify a group name. Group names can be edited any time.' There is a text input field labeled 'Group Name:' containing the text 'Developers'. Below the input field, there is a note: 'Example: Developers or ProjectAlpha' and 'Maximum 128 characters.' At the bottom, there are two buttons: 'Back' and 'Continue'.

4. Click "Continue".
5. Set the permissions for the Administrators group using the Amazon EC2 Full Access policy template.

The screenshot shows the 'Create a New Group of Users' wizard with the 'Set Permissions' step selected. The progress bar has four steps: Group Name, Permissions, Users, and Review. The 'Permissions' step is highlighted with an orange circle. Below the progress bar, the text says 'Select a policy template, generate a policy, or create a custom policy. A policy is a document that formally states one or more permissions. You can edit the policy on the following screen, or at a later time using the user, group, or role detail pages.' There are three main sections: 'Select Policy Template', 'Policy Generator', and 'Custom Policy'. Under 'Select Policy Template', there are four options: 'Amazon EC2 Full Access', 'Amazon EC2 Read Only Access', 'AWS Elastic Beanstalk Full Access', and 'AWS Elastic Beanstalk Read Only Access'. Each option has a 'Select' button. The 'Select' button for 'Amazon EC2 Full Access' is circled in red. Below these options, there are three radio buttons: 'Policy Generator', 'Custom Policy', and 'No Permissions'.

6. Click Continue.
7. As mentioned earlier - you can customize the permissions by editing the following policy document. In this example, we'll keep the default. Click Continue.
8. Click the "Create New Users" tab.
9. Type Dave in the users box.
10. Click Continue.

Create a New Group of Users [Cancel]

Group Name Permissions **Users** Review

Users below will be added to your **Developers** group.

Create New Users Add Existing Users

Enter User Names:

1. Dave

2.

3.

4.

5.

Maximum 128 characters each

☒ **Generate an access key for each User**

Users need access keys to make secure REST or Query protocol requests to AWS service APIs.

For Users who need access to the AWS Management Console, create a password in the Users panel after completing this wizard.

Back Continue

11. Verify that the information for the group is correct, then click “Continue” to create the Developers group and the IAM user, Dave.
12. Click “Close Window”.
13. Log out.

Generate a Password for Dave

We’ll repeat the same steps to generate a password for Dave, as we did for Adele.

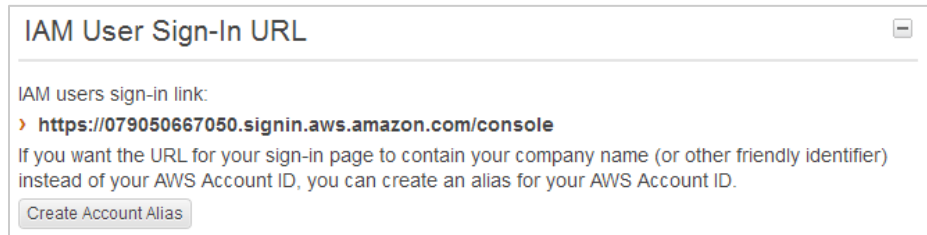
1. Click “Users” under Details in the left column.
2. Check the box next to Dave.
3. Under “User Actions”, click “Manage Password”.
4. Choose “Assign an auto-generated password” and click “Apply”.
5. Click “Download Credentials”.
6. Click “Close Window”.

Login as a User with Limited Permissions

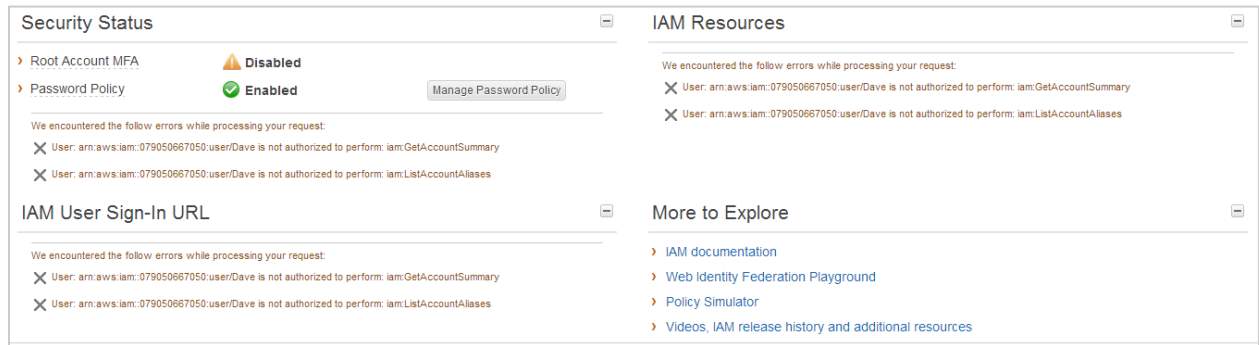
Login as a Developer (Dave)

1. Use the IAM Sign-In URL that you copied earlier (and used to login as Adele).

Introduction to Identity and Access Management (IAM)



2. Use the credentials that you just created for Dave to login.
3. From the list of services, click IAM.
4. Notice that although Dave gets into the IAM console screen, there are many things that he cannot see because he does not have access to IAM. For example, if he tries to create a group of users, he will receive an error and not be able to access it.



5. Click the cube in the upper left corner to go back to the AWS Management Console dashboard.
6. From the list of services, click EC2.
7. Notice that because we used the Amazon EC2 Full Access policy template, Dave has access to all EC2 services.
8. Log out.

End Your Lab

1. Return to the QwikLab lab homepage and click **End Lab** to conclude your lab.

Conclusion

Congratulations! You now have successfully:

- Familiarized yourself with the Identity and Access Management (AWS) Console.
- Created a group with full, administrator permissions.
- Added a user to the Administrator group.
- Updated the password policy.
- Located and use the IAM sign-in URL.
- Created a group with limited permissions.
- Added a user to the group with limited permissions.

Resources

In order to learn more about Amazon Identity and Access Management, we recommend that you visit the IAM [product page](#).

- IAM FAQs: <http://aws.amazon.com/iam/faqs/>
- IAM Documentation: <http://aws.amazon.com/documentation/iam/>
- IAM Release Notes: http://aws.amazon.com/releases/notes/AWS%20Identity%20and%20Access%20Management?_encoding=UTF8&jiveRedirect=1
- IAM Sample Code and Library: http://aws.amazon.com/code/AWS%20Identity%20and%20Access%20Management?_encoding=UTF8&jiveRedirect=1
- IAM Developer Tools: http://aws.amazon.com/developertools/AWS%20Identity%20and%20Access%20Management?_encoding=UTF8&jiveRedirect=1
- Discussion Forums: <https://forums.aws.amazon.com/forum.jspa?forumID=76#>
- Additional Resources: <http://aws.amazon.com/iam/additionalresources/>

For feedback, suggestions and corrections to this lab, please email aws-course-feedback@amazon.com.