PRINTED BY: gleung@datapipe.com. Printing is for personal, private use only. No part of this book may be reproduced or transmitted without publisher's prior permission. Violators will be prosecuted.

Lab 1: Working with Amazon Identity and Access Management

Lab Overview

Introduction

In this lab, you will use the Amazon Identity and Access Management service to create users and roles within an AWS environment. You will then test the permissions of these users and roles to verify that they can only perform the specified actions within the AWS environment.

Allotted time

The allotted time for this lab is listed as follows:

Component	Time
Overview	5 minutes
Lab	30 minutes
Total:	**35 minutes**

Prerequisites

This lab requires:

- Access to a notebook computer with Wi-Fi on a Microsoft Windows, Mac OS X, or Linux (Ubuntu, SuSE, or Red Hat) system
  - The qwikLABS lab environment is not accessible on an iPad or tablet device, but you may use these devices to access the student guide (PDF).
- For Microsoft Windows users: Administrator access to the computer
- An Internet browser such as Chrome, Firefox, or IE 9 (previous versions of Internet Explorer are not supported)

Objectives

After completing this lab, you will be able to:

- Familiarize yourself with the Identity and Access Management (IAM) Console.
- Grant permissions to users to use a specific AWS service.
- Grant limited permissions to users in a group.
- Locate and use the IAM sign-in URL.
- Use the IAM Policy Simulator to test the effects of changing a policy.

© 2015 Amazon Web Services, Inc. and its affiliates. All rights reserved.

PRINTED BY: gleung@datapipe.com. Printing is for personal, private use only. No part of this book may be reproduced or transmitted without publisher's prior permission. Violators will be prosecuted.

Creating IAM Users

Introduction

In this part of the lab, you will create two users in IAM and then assign specific security policies to each of them.

Task 1.1: Create users in IAM

To start, you first need to create the users:

Step	Action
1.1.1	In the AWS Management Console, on the **Services** menu, click **IAM**.
1.1.2	In the IAM Dashboard, click **Users**.
1.1.3	Click **Create New Users**.
1.1.4	In the first **Enter User Names** box, type **AsperatusTechS3TestUser**.
1.1.5	In the second **Enter User Names** box, type **AsperatusTechEC2TestUser**
1.1.6	Verify that the **Generate an access key for each user** option is selected.
1.1.7	Click **Create**.
1.1.8	Click **Download Credentials** to download the users' credentials.
1.1.9	Open the file and re-save it as **AsperatusTechTestUserCredentials.txt**
1.1.10	Return to your browser and click **Close**.

Task 1.2: Create a password

By default, users that you create do not have access to the AWS Management Console. To grant this access, you need to create a password for the user:

Step	Action
1.2.1	Return to the **Users** menu in the IAM Management Console.
1.2.2	Select the check box next to **AsperatusTechS3TestUser**.
1.2.3	In the **User Actions** drop-down list, click **Manage Password**.
1.2.4	Select the **Assign an auto-generated password** option, and then click **Apply**. A new page confirms that IAM has generated the user's password.
1.2.5	Click **Show User Security Credentials**.
1.2.6	Open the AsperatusTechTestUserCredentials.txt file you saved earlier in a text editor, and add a **Password** column by appending the string ",Password" to the first row of text.
1.2.7	Enter the password in the **Password** column of the **AsperatusTechS3TestUser** entry by adding a comma to the end of the user's record, followed by the password generated by IAM.
1.2.8	In the IAM Management Console, click **Close**.

Continued on next page

© 2015 Amazon Web Services, Inc. and its affiliates. All rights reserved.

PRINTED BY: gleung@datapipe.com. Printing is for personal, private use only. No part of this book may be reproduced or transmitted without publisher's prior permission. Violators will be prosecuted.

Creating IAM Users, Continued

Task 1.2: Create a password, continued

Step	Action
1.2.9	IAM asks you to confirm the closing of the window, because you haven't downloaded the user's password. Because you copied the password to an existing file, click **Close** again to close the window.
1.2.10	Repeat this process for the **AsperatusTechEC2TestUser**.

Task 1.3: Set permissions

Grant full permissions to only Amazon S3:

Step	Action
1.3.1	Return to the **Users** menu in the IAM Management Console if you are not already there.
1.3.2	From the list of users, click the name of **AsperatusTechS3TestUser** to open the **Details** page.
1.3.3	Scroll down to the **Permissions** section.
1.3.4	Click **Attach User Policy**.
1.3.5	Locate the **Amazon S3 Full Access** policy, and then click **Select**. This will display a policy that grants the selected user full access to all Amazon S3 functions. **Note:** You can use your browser's Find function to locate this policy name more easily.
1.3.6	Click **Apply Policy**. Verify that *AmazonS3FullAccess-AsperatusTechS3TestUser* is listed under **User Policies** within the **Permissions** group.

© 2015 Amazon Web Services, Inc. and its affiliates. All rights reserved.

PRINTED BY: gleung@datapipe.com. Printing is for personal, private use only. No part of this book may be reproduced or transmitted without publisher's prior permission. Violators will be prosecuted.

Creating an IAM Group

Introduction

In this part of the lab, you are going to create a user who has full permissions (Start, Stop, Terminate, and so on) with Amazon EC2 instances. Now, instead of creating a single user with these permissions, you will create a user group that has these permissions, and then create a user who belongs to that group.

Task 1.4: Create a user group

To create a user group:

Step	Action
1.4.1	In the IAM Dashboard, click **Groups**.
1.4.2	Click **Create New Group**.
1.4.3	In the **Group Name** box, type **AsperatusTechEC2TestGroup**
1.4.4	Click **Next Step**.
1.4.5	On the **Set Permissions** page, verify that the **Select Policy Template** option is selected.
1.4.6	Locate the **Amazon EC2 Full Access** policy and click **Select**. This will display a policy that will give any members of the group full access to all Amazon EC2 functions.
1.4.7	Click **Next Step**.
1.4.8	Click **Create Group**.
1.4.9	Select the **AsperatusTechEC2TestGroup** check box.
1.4.10	In the **Group Actions** drop-down list, click **Add Users to Group**.
1.4.11	Select **AsperatusTechEC2TestUser**, and then click **Add Users**.

© 2015 Amazon Web Services, Inc. and its affiliates. All rights reserved.

PRINTED BY: gleung@datapipe.com. Printing is for personal, private use only. No part of this book may be reproduced or transmitted without publisher's prior permission. Violators will be prosecuted.

Creating an IAM Role

Introduction

In this part of the lab, you will create a role within IAM. A role is an IAM entity that defines a set of permissions for making AWS service requests. IAM roles are not associated with a specific user or group. Instead, roles are ***assumed*** by trusted entities such as IAM users, applications, or AWS services such as Amazon EC2.

You are going to create an IAM role that allows anyone using that resource to have "describe" permissions to Amazon EC2 instances when it is assigned to a resource. This means that the user can list the Amazon EC2 instances that are running, but cannot start, stop, or otherwise change them.

Task 1.5: Create a role

To create an IAM role:

Step	Action
1.5.1	In the IAM Dashboard, click **Roles**.
1.5.2	Click **Create New Role**.
1.5.3	In the **Role Name** box, type **AsperatusTechEC2Describe**
1.5.4	Click **Next Step**.
1.5.5	Verify that the **AWS Service Roles** option is selected.
1.5.6	Select **Amazon EC2** near the top of the list, and click **Select**.
1.5.7	On the **Set Permissions** page, verify that the **Select Policy Template** option is selected.
1.5.8	Locate the **Amazon EC2 Read Only Access** policy and click **Select**. This will display a policy that grants all entities that assume this role read-only access to Amazon EC2 instances associated with this account. In other words, entities that assume this role will be able to describe and list all existing Amazon EC2 instances, but will not be able to create instances, or stop or terminate existing instances.
1.5.9	Click **Next Step**.
1.5.10	Click **Create Role**.

© 2015 Amazon Web Services, Inc. and its affiliates. All rights reserved.

PRINTED BY: gleung@datapipe.com. Printing is for personal, private use only. No part of this book may be reproduced or transmitted without publisher's prior permission. Violators will be prosecuted.

Testing IAM Users and Group

Introduction

You should now have the following:

- A user who has full access to only Amazon S3 resources.
- A user who has full access to only Amazon EC2 resources.
- A role that has read access to only Amazon EC2 resources.

Next, you'll test each of these to see how they function. Before you start, obtain the URL associated with your main AWS account for this lab.

Task 1.6: Test the S3 user

You'll need the password you created for AsperatusTechS3TestUser.

Step	Action
1.6.1	Click **Dashboard**, and then copy the URL shown under **IAM users sign-in link** to a text file somewhere on your local computer.
1.6.2	Open a different web browser such as Firefox or Chrome. **Note:** You can open another tab within the same browser; however, a new session will log off **awsstudent**; therefore, you will need to log in again using the password provided by qwikLABS. If you have been using Firefox, using a Chrome or Safari web browser will maintain the session for **awsstudent** while you test **AsperatusTechS3TestUser**.
1.6.3	Navigate to the AWS Account Alias URL that you copied in step 1.6.1.
1.6.4	In the **User Name** box, type **AsperatusTechS3TestUser**.
1.6.5	In the **Password** box, type the password that you saved in the **AsperatusTechTestUserCredentials.txt** file.
1.6.6	Click **Sign In**. The AWS Management Console opens.
1.6.7	On the **Services** menu, click **EC2**. Messages in the center pane state that you are not authorized to describe various aspects of an EC2 instance.
1.6.8	In the navigation pane, click **Instances**. This message appears: "An error occurred fetching instance data. You are not authorized to perform this operation." This is because the user that you have used for login has no permissions to Amazon EC2. Next, you will verify whether the user has permissions for Amazon S3.

Task 1.7: Create an S3 bucket

To create an Amazon S3 bucket:

Step	Action
1.7.1	On the **Services** menu, click **S3**.
1.7.2	Click **Create Bucket**.

Continued on next page

© 2015 Amazon Web Services, Inc. and its affiliates. All rights reserved.

PRINTED BY: gleung@datapipe.com. Printing is for personal, private use only. No part of this book may be reproduced or transmitted without publisher's prior permission. Violators will be prosecuted.

Testing IAM users and group, Continued

Task 1.7: Create an S3 bucket, continued

Step	Action
1.7.3	In the **Create a Bucket – Select a Bucket Name and Region** window: • For **Bucket Name**, type a unique bucket name (e.g., **awsst-lab01-1126**). • For **Region**, select a region you want to create a bucket in **Note:** The bucket name you choose must be **unique** across all existing bucket names in Amazon S3. One way to help ensure uniqueness is to prefix your bucket names with the name of your organization. Bucket names must comply with certain rules: • Bucket names must be at least 3 characters and no more than 63 characters long. • Bucket names must start and end with a lowercase letter or a number. For more detailed information, see Bucket Restrictions and Limitations in the Amazon Simple Storage Service Developer Guide.
1.7.4	Click **Create**.
1.7.5	Click the bucket you just created. The bucket is currently empty.
1.7.6	Click **Upload**.
1.7.7	Click **Add Files**. A file selection dialog box opens.
1.7.8	Select a file from your computer that you want to upload, and then click **Open**.
1.7.9	Click **Start Upload**. The file should upload successfully. This demonstrates that **AsperatusTechS3TestUser** has full permissions to work with **Amazon S3**.

Task 1.8: Test the EC2 user

In this step, you will log in as the user AsperatusTechEC2User and verify that this user has full permissions to work with Amazon EC2.

Step	Action
1.8.1	Open a new browser window, and then paste the URL that you copied in step 1.6.1 in the address bar.
1.8.2	In the **User Name** box, type **AsperatusTechEC2TestUser**.
1.8.3	In the **Password** box, type the password that you saved in the **AsperatusTechTestUserCredentials.txt** file.
1.8.4	Click **Sign In**. The AWS Management Console opens.
1.8.5	On the **Services** menu, click **EC2**.
1.8.6	Click **Launch Instance**. The Launch Wizard should start successfully. This demonstrates that **AsperatusTechEC2TestUser** has full permissions to work with Amazon EC2. (There is no need to complete the Wizard.)
1.8.7	On the **Services** menu, click **S3**. Notice that you cannot access any S3 resources.

© 2015 Amazon Web Services, Inc. and its affiliates. All rights reserved.

PRINTED BY: gleung@datapipe.com. Printing is for personal, private use only. No part of this book may be reproduced or transmitted without publisher's prior permission. Violators will be prosecuted.

Testing IAM Policy

Introduction

You can use the IAM policy simulator to test the effects of IAM policies before you commit the policies into production, and test your existing IAM policies to verify that they have the intended effect.

Task 1.9: Test the EC2 group permission

To test the AsperatusTechEC2TestGroup permission using Policy Simulator:

Step	Action
1.9.1	Return to your main AWS Management Console and confirm that you are in the browser tab that has **awsstudent** listed as the current user on the navigation bar.
1.9.2	On the **Services** menu, click **IAM**.
1.9.3	Click **Groups**.
1.9.4	Click the name of **AsperatusTechEC2TestGroup** to open the **Details** page.
1.9.5	Scroll down to **Permissions**, and click **Simulate Policy** under **Actions** for the existing policy. This launches the **IAM Policy Simulator** tool.
1.9.6	Under **Policy Simulator**, in the **Select service** drop-down list, click **EC2**.
1.9.7	Click **Select All** to select all Amazon EC2 actions.
1.9.8	Click **Run Simulation**. **Result:** All actions should show **allowed** in the **Permission** column.
1.9.9	In **Policies**, modify the policy by adding: **{** **"Action": "ec2:TerminateInstances",** **"Effect": "Deny",** **"Resource": "*"** **},** The policy should now look like this: 

Continued on next page

© 2015 Amazon Web Services, Inc. and its affiliates. All rights reserved.

PRINTED BY: gleung@datapipe.com. Printing is for personal, private use only. No part of this book may be reproduced or transmitted without publisher's prior permission. Violators will be prosecuted.

Testing IAM policy, Continued

Task 1.9: Test the EC2 group permission, continued

Step	Action
1.9.10	Click **Apply**.
1.9.11	Click **Clear Results**.
1.9.12	Click **Select All** again to select all Amazon EC2 actions.
1.9.13	Click **Run Simulation**. **Result:** This time, the simulation result shows **denied** for the **TerminateInstances** action but the rest should be **allowed**.

Ending your lab

If you choose not to complete the optional portion of this lab, follow the instructions in Appendix B to end your lab.

© 2015 Amazon Web Services, Inc. and its affiliates. All rights reserved.

PRINTED BY: gleung@datapipe.com. Printing is for personal, private use only. No part of this book may be reproduced or transmitted without publisher's prior permission. Violators will be prosecuted.

Optional

Introduction

This part of the lab is a challenge; step-by-step instructions are not provided. Use online documentation to help you if necessary.

http://docs.aws.amazon.com/IAM/latest/UserGuide/Using_WorkingWithGroupsAndUsers.html.

Challenge 1

First, create an IAM role for Amazon EC2. Log in to the AWS Management Console as AsperatusTechEC2TestUser, and try to launch an Amazon EC2 instance with the IAM Role set to the role that you created previously.

Discussion

Were you able to launch an instance into the new role? Why?

Instance Profile

An instance profile is a container for an IAM role. Instance profiles are used to pass role information to an Amazon EC2 instance when the instance starts.

To launch an instance with a role, the developer must have permission to launch Amazon EC2 instances and permission to pass IAM roles.

Here is an example policy that grants a user permission to launch an instance with any role by using the Amazon EC2 console:

```
{
  "Version": "2012-10-17",
  "Statement": [{
    "Effect": "Allow",
    "Action": [
      "iam:PassRole",
      "iam:ListInstanceProfiles",
      "ec2:*"
    ],
    "Resource": "*"
  }]
}
```

To learn more about **Instance Profile**, see the online documentation at http://docs.aws.amazon.com/IAM/latest/UserGuide/instance-profiles.html.

Continued on next page

© 2015 Amazon Web Services, Inc. and its affiliates. All rights reserved.