⌛00:38:56 Exit Lab ✓ Complete Lab

Introduction to AWS Identity and Access Management (IAM)

⏱ 1 hour duration

Apprentice

Rate this lab

VIDEOS GUIDE

Introduction to AWS Identity and Access Management (IAM)

AWS Identity and Access Management (IAM) is a service that allows AWS customers to manage user access and permissions for the accounts and available APIs/services within AWS. IAM can manage users, security credentials (such as API access keys), and allow users to access AWS resources. In this lab, we will walk through the foundations of IAM. We'll focus on user and group management as well as how to assign access to specific resources using IAM managed policies. We'll learn how to find the login URL where AWS users can log in to their account and explore this from a real-world use case perspective.

Solution

Log in to the live AWS environment using the credentials provided. Make sure you're in the N. Virginia (`us-east-1`) region throughout the lab.

Environment Walkthrough

Explore the Users

1. Navigate to **IAM**.
2. From the left-hand menu, click **Users**.
3. Click **user-1**.
4. At the top, under *Summary*, observe the user’s ARN (Amazon Resource Name), path, and creation time.
5. Select **Permissions** and **Groups**, where we'll see `user-1` does not have any permissions assigned to it and does not belong to any groups.
6. Select **Security credentials** to see user access keys, SSH public keys, and HTTPS Git credentials for AWS CodeCommit.
7. Select **Access Advisor** to see which services the user has accessed and when.
8. From the left-hand menu, click **Users**.

9. Click **user-2** and **user-3** to check out their permissions, groups, security credentials, and services.

Explore the Groups

There are three groups we're going to focus on:

- `EC2-Admin` : Provides permissions to view, start, and stop EC2 instances.
- `EC2-Support` : Provides read-only access to EC2.
- `S3-Support` : Provides read-only access to S3.

1. Click **Groups** in the left-hand menu.
2. Click any of the groups to see which policy is attached to it.
   Note: There are two different kinds of policies for these groups:
   - **Managed policies:** Policies shared among users and/or groups that are pre-built either by AWS or an administrator within the AWS account. When it's updated, the changes to this policy are immediately applied for all users and groups to which it's attached.
   - **Inline policies:** Policies assigned to just one user or group that are typically used in one-off situations.
3. Click **EC2-Admin**.
4. Click **Permissions**, where we'll see `EC2-Admin` has an inline policy with a set of permissions associated with it.
5. Click **Show Policy** to see the actions the group is allowed to take (and which resources the action can be taken on) or if it has read-only access.
   Note: From this policy, we have permission to view, start, and stop EC2 instances on all resources, view elastic load balancers, list metrics, get metric statistics, and describe metrics (which our CloudWatch metrics automatically configured with our EC2 instance). The same permissions apply to our Auto Scaling service.
6. Click **Cancel**.
7. Click **Groups** in the left-hand menu.
8. Click **EC2-Support**.
9. Click **Permissions**, where we'll see it has a managed policy created by AWS.
10. Click **Show Policy**.
    Note: This group can describe EC2 instances, elastic load balancers, CloudWatch metrics, and our autoscaling configurations. It doesn't allow us to stop, start, or create EC2 instances. It's a read-only policy, meaning we can view what's happening inside EC2, but we can't make changes to the resource.
11. Click **Cancel**.
12. Click **Groups** in the left-hand menu.
13. Click **S3-Support**.
14. Click **Permissions**. Our `S3-Support` group is only allowed read-only access.

15. Click **Show Policy**, where we'll see the `Get` and `List` actions that allow us to view the S3 bucket and the objects in it.
16. Click **Cancel**.

Add Users to Groups

1. Click **S3-Support**.
2. Click **Users** > **Add Users to Group**.
3. Select `user-1` and click **Add Users**.
4. Click **Groups** in the left-hand menu.
5. Repeat the process, adding `user-2` to the `EC2-Support` group and `user-3` to the `EC2-Admin` group.

Use the IAM Sign-In Link to Sign In As a User

Log In as `user-1`

1. From the left-hand menu, click **Dashboard**.
2. Copy the IAM users sign-in link to the clipboard.
3. Open an incognito browser window and paste the link into the browser.
4. Log in as `user-1` using the password `123456` .
5. Navigate to S3.
6. Click **Create bucket**.
7. Enter a globally unique bucket name.
8. Click **Next** > **Next** > **Create bucket**. We receive an "access denied" error.
9. Close out of the bucket creation window.
10. Navigate to **EC2** > **Running instances**. We receive an error message.
11. From the top menu, click **user-1** > **Sign Out**.

Log In as `user-2`

1. Click **Log back in**.
2. Log in as `user-2` using the password `123456` .
3. Navigate to **EC2** > **Running instances**. We should immediately notice `user-2` has more permissions than `user-1` , as we'll be able to view the running instance.
4. With the running instance selected, click **Actions** > **Instance State** > **Stop**.
5. Click **Yes, Stop** . We receive a "Error stopping instances" message.
6. Click **Cancel**.
7. Navigate to S3. We receive an "access denied" error message.
8. From the top menu, click **user-2** > **Sign Out**.

Log In as `user-3`

1. Click **Log back in**.
2. Log in as `user-3` using the password `123456` .
3. Navigate to **EC2** > **Running instances**.
4. With the running instance selected, click **Actions** > **Instance State** > **Stop**.

5. Click **Yes, Stop**.
6. Click the refresh icon. The instance stopped this time.
7. Once stopped, click **Actions** > **Instance State** > **Start**.
8. Click **Yes, Start**. The instance starts again.

Conclusion

Congratulations on successfully completing this hands-on lab!

Tools

Lab Diagram   Instant Terminal

Credentials

How do I connect?

AWS Account

Username

cloud_user

Password

&7Usnziyks

Open Link in Incognito Window

How do I connect?

Additional Resources

Ensure you are operating out of the **N. Virginia** (`us-east-1`) region.

- `user-1` password: `123456`
- `user-2` password: `123456`
- `user-3` password: `12345`

Learning Objectives

0 of 2 completed

○ Add the Users to the Proper Groups

○ Use the IAM Sign In Link to Sign In As a User