



Introduction to AWS Identity and Access Management (IAM)

Lab Overview

AWS Identity and Access Management (IAM) is a web service that enables Amazon Web Services (AWS) customers to manage users and user permissions in AWS. With IAM, you can centrally manage **users**, **security credentials** such as access keys, and **permissions** that control which AWS resources users can access.

This lab will demonstrate:

- Creating **IAM Users and Groups**
- Creating **IAM policies** and applying to groups
- Following a **real-world scenario**, adding users to groups with specific capabilities enabled
- Locating and using the **IAM sign-in URL**
- **Experimenting** with the effects of policies on service access

Other AWS Services

AWS Identity and Access Management



www.tngslearningsolutions.com info@tngslearningsolutions.com

AWS Identity and Access Management (IAM) can be used to:

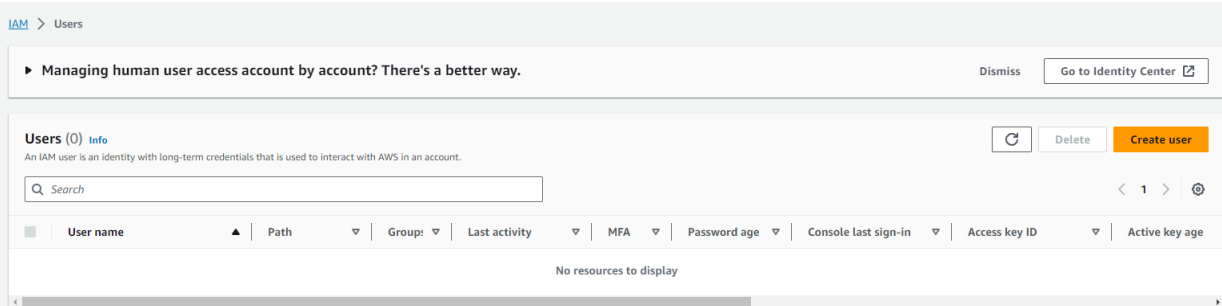
- **Manage IAM Users and their access:** You can create Users and assign them individual security credentials (access keys, passwords, and multi-factor authentication devices). You can manage permissions to control which operations a User can perform.
- **Manage IAM Roles and their permissions:** An IAM Role is similar to a User, in that it is an AWS identity with permission policies that determine what the identity can and cannot do in AWS. However, instead of being uniquely associated with one person, a Role is intended to be *assumable* by anyone who needs it.
- **Manage federated users and their permissions:** You can enable *identity federation* to allow existing users in your enterprise to access the AWS Management Console, to call AWS APIs and to access resources, without the need to create an IAM User for each identity.



Start Lab

Creating IAM Users

1. Sign into the [AWS Management Console](#), on the **Services** menu, click **IAM**.
2. In the navigation pane on the left, click **Users**
3. Click **Create user**



4. **User Name:** `user-1`
5. Select **Provide user access to the AWS Management Console - optional**
6. Select the options below

User details

User name

The user name can have up to 64 characters. Valid characters: A-Z, a-z, 0-9, and * ^ _ . @ - (hyphen)

☒ **Provide user access to the AWS Management Console - optional**
If you're providing console access to a person, it's a [best practice](#) to manage their access in IAM Identity Center.

Are you providing console access to a person?

User type

☐ **Specify a user in Identity Center - Recommended**
We recommend that you use Identity Center to provide console access to a person. With Identity Center, you can centrally manage user access to their AWS accounts and cloud applications.

☒ **I want to create an IAM user**
We recommend that you create IAM users only if you need to enable programmatic access through access keys, service-specific credentials for AWS CodeCommit or Amazon Keyspaces, or a backup credential for emergency account access.

Console password

☒ **Autogenerated password**
You can view the password after you create the user.

☐ **Custom password**
Enter a custom password for the user.

☐ **Show password**

☒ **Users must create a new password at next sign-in - Recommended**
Users automatically get the [IAMUserChangePassword](#) policy to allow them to change their own password.

Info If you are creating programmatic access through access keys or service-specific credentials for AWS CodeCommit or Amazon Keyspaces, you can generate them after you create this IAM user. [Learn more](#)

Cancel **Next**

7. For **Console password**, select **Autogenerated password**.
8. Select **Users must create a new password at next sign-in**
9. Click **Next**



Set permissions

Add user to an existing group or create a new one. Using groups is a best-practice way to manage user's permissions by job functions. [Learn more](#)

Permissions options

☒ **Add user to group**
Add user to an existing group, or create a new group. We recommend using groups to manage user permissions by job function.

☐ **Copy permissions**
Copy all group memberships, attached managed policies, and inline policies from an existing user.

☐ **Attach policies directly**
Attach a managed policy directly to a user. As a best practice, we recommend attaching policies to a group instead. Then, add the user to the appropriate group.

Get started with groups
Create a group and select policies to attach to the group. We recommend using groups to manage user permissions by job function, AWS service access, or custom permissions. [Learn more](#)

Create group

► Permissions boundary - optional
Set a permissions boundary to control the maximum permissions for this user. Use this advanced feature used to delegate permission management to others. [Learn more](#)

Cancel Previous **Next**

- Click **Next**
 - Click **Next**
 - Click **Create user**.
 - Finally, download the csv file to your computer containing user credentials.
- Retrieve password

You can view and download the user's password below or email users instructions for signing in to the AWS Management Console. This is the only time you can view and download this password.

Console sign-in details [Email sign-in instructions](#)

Console sign-in URL
 <https://220816069512.signin.aws.amazon.com/console>

User name
 user-1

Console password
 ***** [Show](#)

Download .csv file **Return to users list**

- Repeat above steps for **user-2** and **user-3**

Creating IAM Groups

- In the navigation pane on the left, click **User Groups**
- Let's create 3 user groups
 - EC2-Admin**
 - EC2-Support**
 - S3-Support**
- To create the first group,
- Click **Create Group**

[IAM](#) > User groups

User groups (0) [Info](#)

Create group

A user group is a collection of IAM users. Use groups to specify permissions for a collection of users.

< 1 >

Group name	Users	Permissions	Creation time
No resources to display			

- User Group Name:** EC2-Admin



20. Scroll down to the bottom of the page and click **Create Group**

Cancel Create group

We need to setup inline policy for **EC2-Admin** Group

1. Navigate to the newly created **EC2-Admin** Group and click on it
2. Select **Permission** tab

[IAM](#) > [User groups](#) > [EC2-Admin](#)

EC2-Admin

Summary

User group name
EC2-Admin

Users **Permissions** Access Advisor

Permissions policies (0) [Info](#)
You can attach up to 10 managed policies.

Filter policies by property or policy name and pres

Policy name [↗](#)

3. Click on **Add Permission**

Users **Permissions** Access Advisor

Permissions policies (0) [Info](#)
You can attach up to 10 managed policies.

Filter by Type
Search All types

Simulate Remove Add permissions ▲
Attach policies
Create inline policy

Policy name [↗](#) Type Attached entities

No resources to display

4. Select **Create inline Policy**.
5. Click on Json
6. Remove the content in the policy editor and Copy and paste the below policy in **Policy editor**
 - a) Make sure to clear out the content within the box before pasting below policy.



```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "Ec2:StopInstances",
        "Ec2:DescribeInstances",
        "Ec2:StartInstances"
      ],
      "Resource": [
        "*"
      ]
    }
  ]
}
```



Policy editor

```
1 {
2   "Version": "2012-10-17",
3   "Statement": [
4     {
5       "Effect": "Allow",
6       "Action": [
7         "Ec2:StopInstances",
8         "Ec2:DescribeInstances",
9         "Ec2:StartInstances"
10      ],
11      "Resource": [
12        "*"
13      ]
14    }
15  ]
16 }
```

+ Add new statement

7. Click **Next**.
8. Policy name: **Ec2-Inline_Policy**
9. Click **Create policy**.

21. To create the second Group,
22. Click **Create Group**
23. **Group Name** EC2-Support
24. Under **Attach permissions policy** in the search bar, type **AmazonEC2ReadOnlyAccess**
25. Press **Enter**
26. Select **AmazonEC2ReadOnlyAccess**
27. Click **Create Group**
28. To create the third Group,
29. Click **Create New Group**
30. **Group Name** S3-Support
31. Under **Attach permissions policy** in the search bar, type **AmazonS3ReadOnlyAccess**
32. Press **Enter**
33. Select **AmazonS3ReadOnlyAccess**
34. Click **Create Group**

Task 1: Explore the Users and Groups



www.tngslearningsolutions.com info@tngslearningsolutions.com

In this task, you will explore the Users and Groups that you just been created in IAM.

3. In the **AWS Management Console**, on the **Services** menu, click **IAM**.
4. In the navigation pane on the left, click **Users**.

View the following IAM Users that you created:

- user-1
 - user-2
 - user-3
5. Click **user-1**.

This will bring to a summary page for user-1. The **Permissions** tab will be displayed.

6. Notice that user-1 does not have any permissions.
7. Click the **Groups** tab.

user-1 also is not a member of any groups.

8. Click the **Security credentials** tab.

user-1 is assigned a **Console password**

9. In the navigation pane on the left, click **Groups**.

View the following groups that you already created:

- EC2-Admin
 - EC2-Support
 - S3-Support
10. Click the **EC2-Support** group.

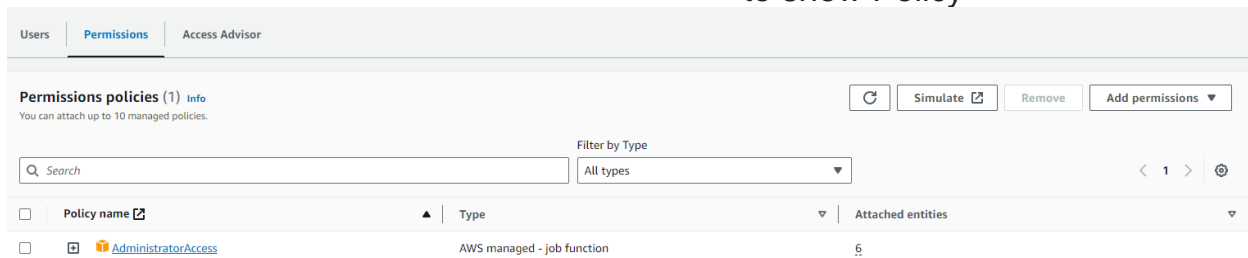
This will bring you to the summary page for the **EC2-Support** group.



11. Click the **Permissions** tab.

This group has a Managed Policy associated with it, called **AmazonEC2ReadOnlyAccess**. Managed Policies are pre-built policies (built either by AWS or by your administrators) that can be attached to IAM Users and Groups. When the policy is updated, the changes to the policy are immediately apply against all Users and Groups that are attached to the policy.

12. Click the plus icon next to **AmazonEC2ReadOnlyAccess** to show Policy



A policy defines what actions are allowed or denied for specific AWS resources. This policy is granting permission to List and Describe information about EC2, Elastic Load Balancing, CloudWatch and Auto Scaling. This ability to view resources, but not modify them, is ideal for assigning to a Support role.

The basic structure of the statements in an IAM Policy is:

- **Effect** says whether to *Allow* or *Deny* the permissions.
- **Action** specifies the API calls that can be made against an AWS Service (eg *cloudwatch:ListMetrics*).
- **Resource** defines the scope of entities covered by the policy rule (eg a specific Amazon S3 bucket or Amazon EC2 instance, or * which means *any resource*).

13. Close the **Show Policy** window.

14. In the navigation pane on the left, click **Groups**.



www.tngslearningsolutions.com info@tngslearningsolutions.com

15. Click the **S3-Support** group.

The S3-Support group has the **AmazonS3ReadOnlyAccess** policy attached.

12. Click the plus icon next to **AmazonS3ReadOnlyAccess** to show Policy

This policy has permissions to Get and List resources in Amazon S3.

17. In the navigation pane on the left, click **Groups**.

18. Click the **EC2-Admin** group.

This Group is slightly different from the other two. Instead of a *Managed Policy*, it has an **Inline Policy**, which is a policy assigned to just one User or Group. Inline Policies are typically used to apply permissions for one-off situations.

20. Under **Actions**, click **Edit Policy** to view the policy.

This policy grants permission to view (Describe) information about Amazon EC2 and also the ability to Start and Stop instances.

21. At the bottom of the screen, click **Cancel** to close the policy.

Business Scenario

For the remainder of this lab, you will work with these Users and Groups to enable permissions supporting the following business scenario:

Your company is growing its use of Amazon Web Services, and is using many Amazon EC2 instances and a great deal of Amazon S3 storage. You wish to give access to new staff depending upon their job function:

User	In Group	Permissions
user-1	S3-Support	Read-Only access to Amazon S3
user-2	EC2-Support	Read-Only access to Amazon EC2



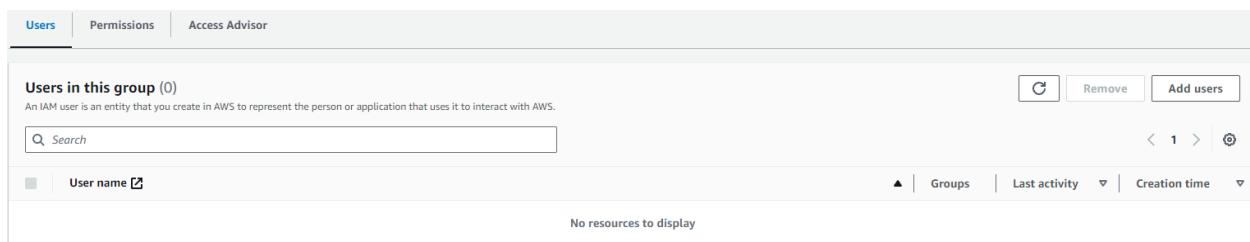
user-3	EC2-Admin	View, Start and Stop Amazon EC2 instances
--------	-----------	---

Task 2: Add Users to Groups

You have recently hired **user-1** into a role where they will provide support for Amazon S3. You will add them to the **S3-Support** group so that they inherit the necessary permissions via the attached *AmazonS3ReadOnlyAccess* policy.

Add user-1 to the S3-Support Group

22. In the left navigation pane, click **Groups**.
23. Click the **S3-Support** group.
24. Click the **Users** tab.
25. In the **Users** tab, click **Add Users**.





www.tngslearningsolutions.com info@tngslearningsolutions.com

26. In the **Add Users to S3-Support** window, configure the following:

- Select **user-1**.
- At the bottom of the screen, click **Add Users**.

In the **Users** tab you will see that **user-1** has been added to the group.

Add user-2 to the EC2-Support Group

You have hired **user-2** into a role where they will provide support for Amazon EC2.

27. Using similar steps to the ones above, add **user-2** to the **EC2-Support** group.

user-2 should now be part of the **EC2-Support** group.

Add user-3 to the EC2-Admin Group

You have hired **user-3** as your Amazon EC2 administrator, who manage your EC2 instances.

28. Using similar steps to the ones above, add **user-3** to the **EC2-Admin** group.

user-3 should now be part of the **EC2-Admin** group.

29. In the navigation pane on the left, click **Groups**.

Each Group should have a **1** in the Users column for the number of Users in each Group.



www.tngslearningsolutions.com info@tngslearningsolutions.com

If you do not have a **1** beside each group, revisit the above instructions to ensure that each user is assigned to a Group, as shown in the table in the Business Scenario section.

Conclusion

Congratulations! You now have successfully:

- Created IAM users and groups
- Inspected IAM policies as applied to the pre-created groups
- Followed a real-world scenario, adding users to groups with specific capabilities enabled