www.tngsllc.com info@tngsllc.com

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

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.

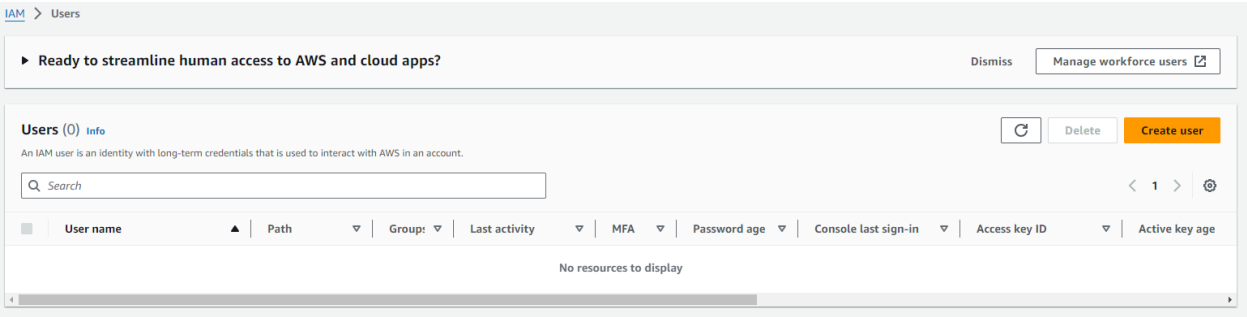
- **Manage federated users and their permissions:** You can enable *identity federation* to allow existing users in your enterprise to access the AWS Management Console, to call AWS APIs and to access resources, without the need to create an IAM User for each identity.

www.tngsllc.com info@tngsllc.com

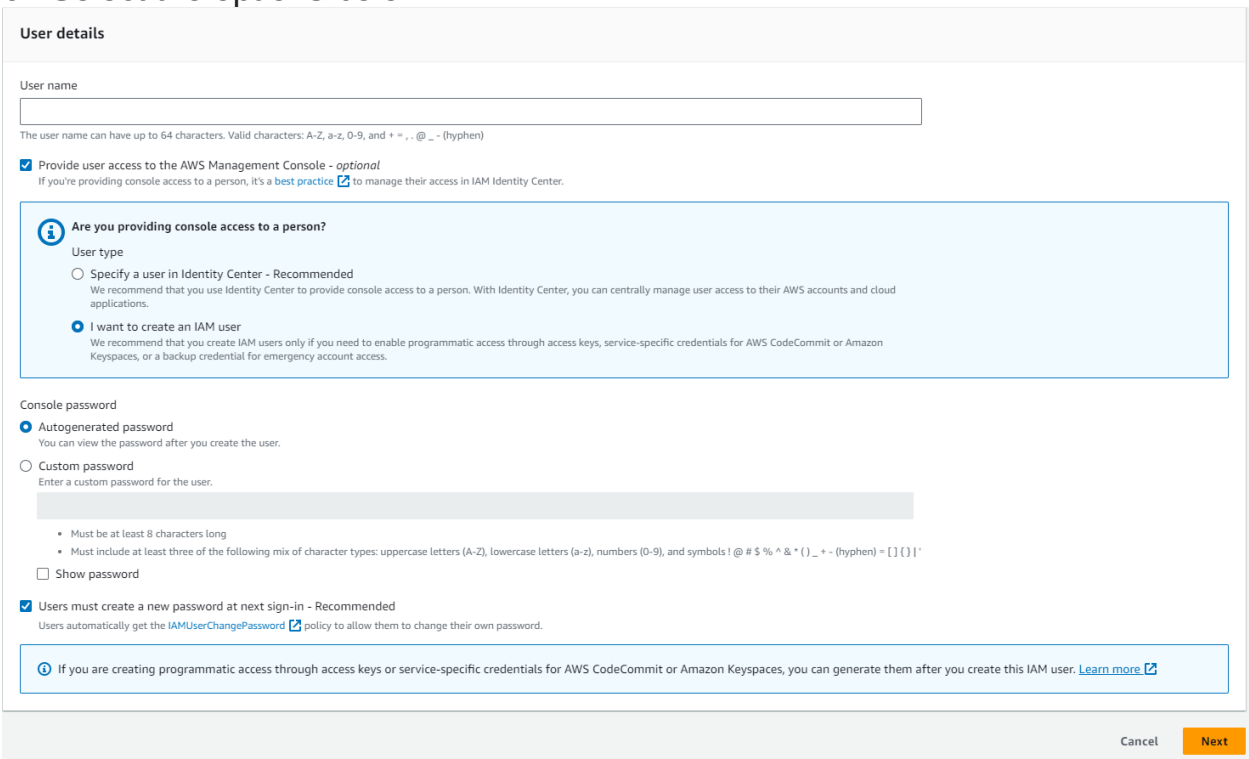
Start Lab

Creating IAM Users

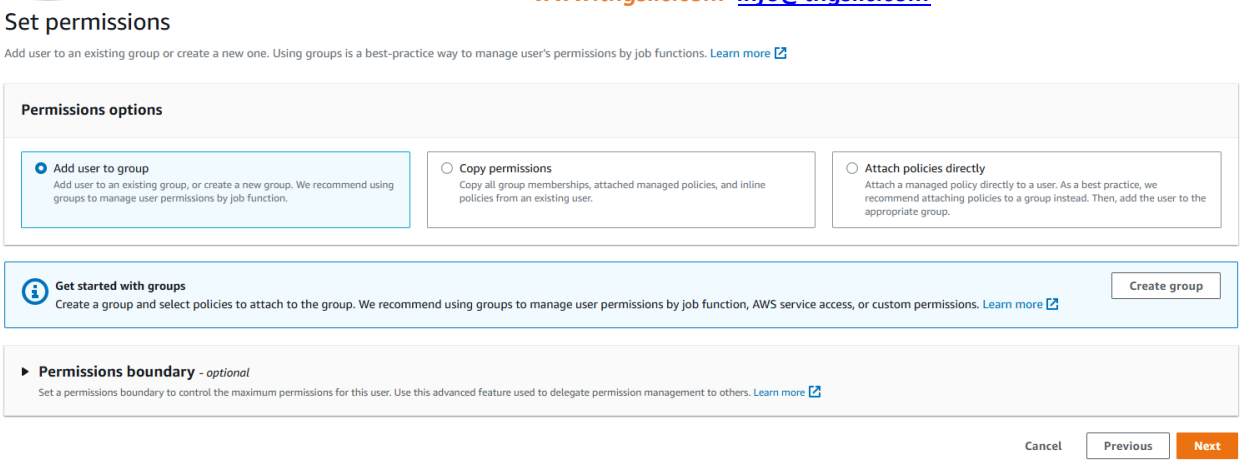
1. Sign into the **AWS Management Console**, on the **Services** menu, click **IAM**.
2. In the navigation pane on the left, click **Users**
3. Click **Create user.**



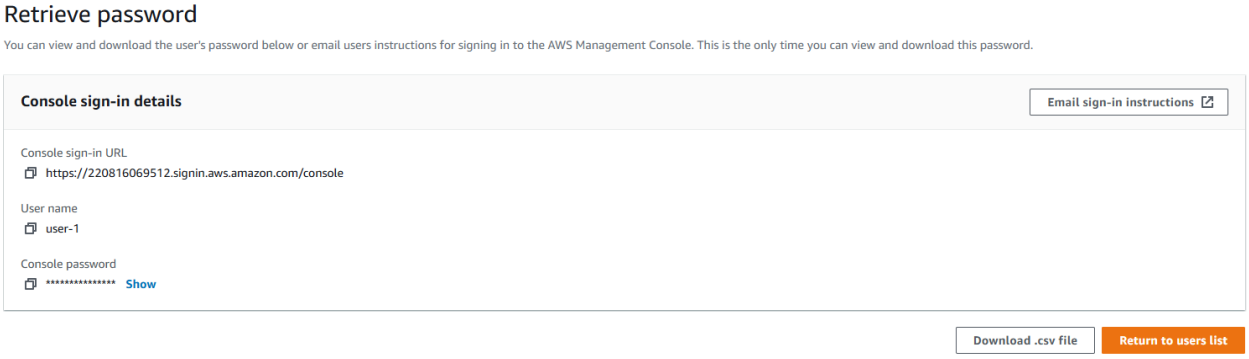
4. **User Name:** user-1
5. Select **Provide user access to the AWS Management Console - *optional***
6. Select the options below



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



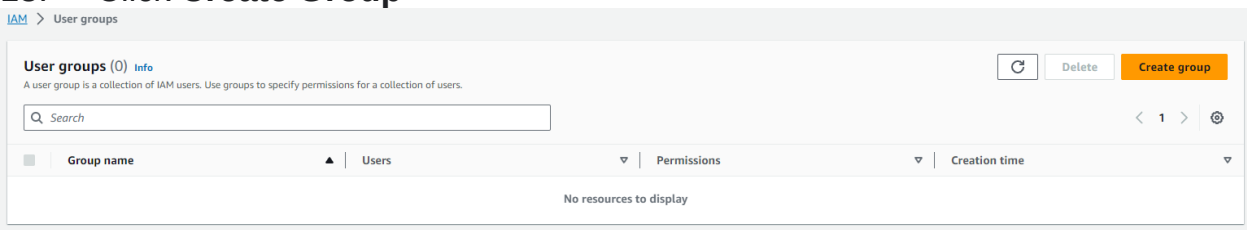
10. Click **Next**
11. Click **Next**
12. Click **Create user.**
13. Finally, download the csv file to your computer containing user credentials.



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

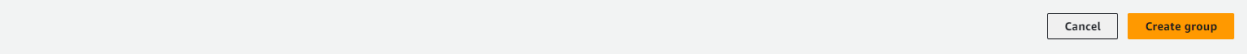
Creating IAM Groups

15. In the navigation pane on the left, click **User Groups**
16. Let's create 3 user groups
    a) **EC2-Admin**
    b) **EC2-Support**
    c) **S3-Support**
17. To create the first group,
18. Click **Create Group**



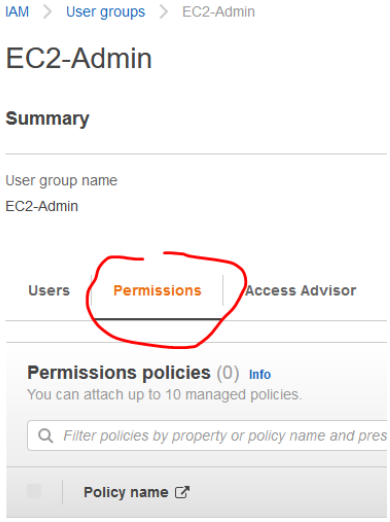
19. **User Group Name:** EC2-Admin

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

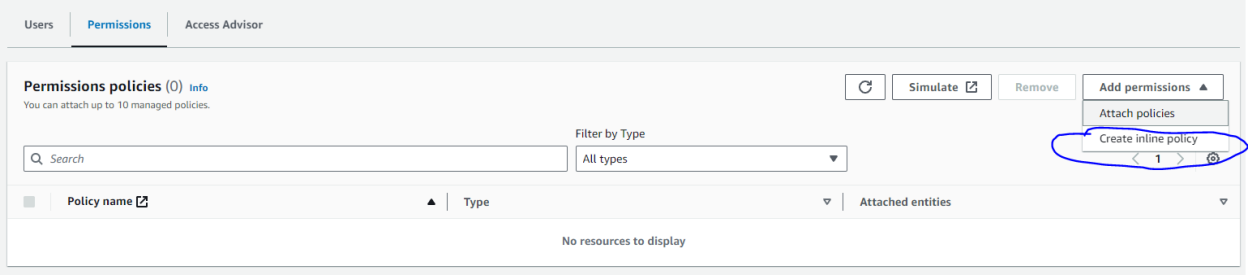


We need to setup inline policy for **EC2-Admin** Group

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

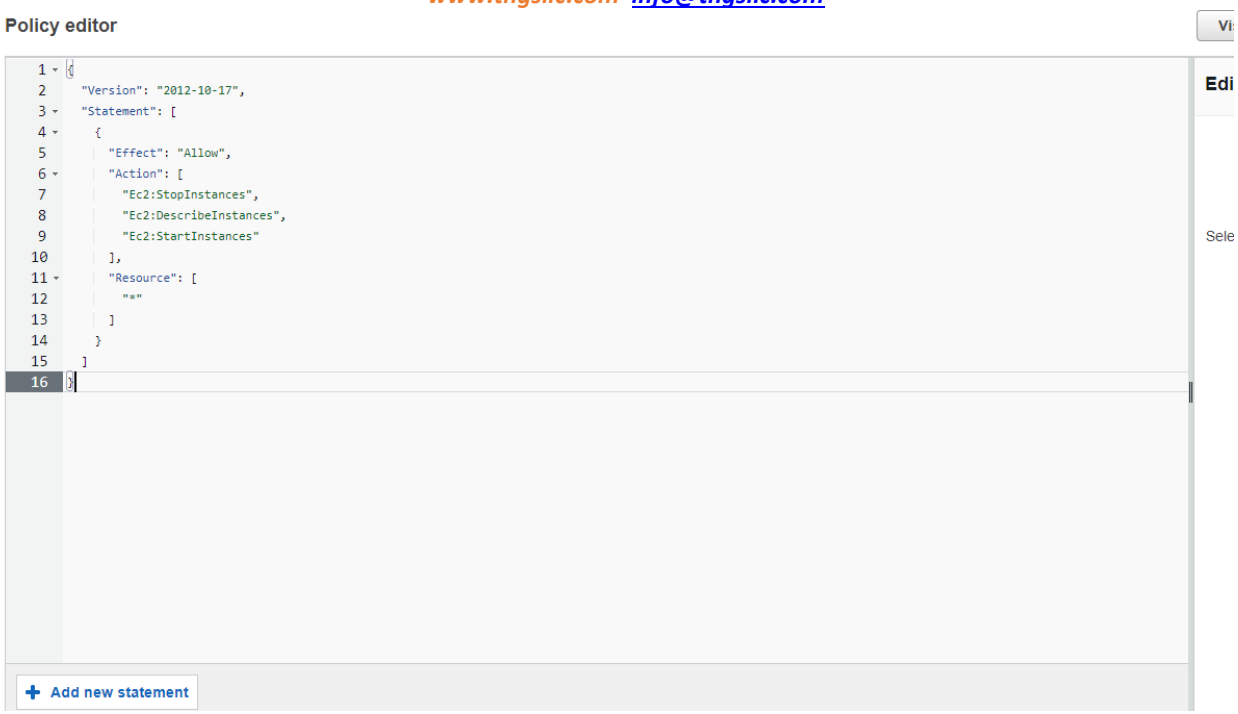


3. Click on **Add Permission**



4. Select **Create inline Policy.**
5. Click to select **Json**
6. Remove the content in the policy editor, 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": [
        "*"
      ]
    }
  ]
}
```



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-Suppot
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

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

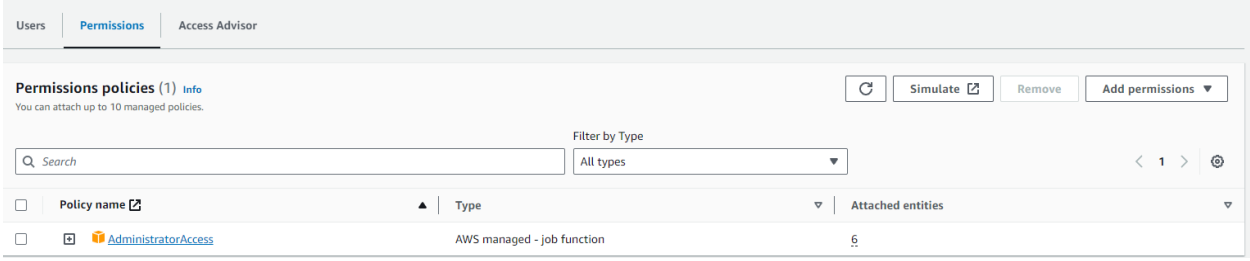
10. Click the **EC2-Support** group.

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**.

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.

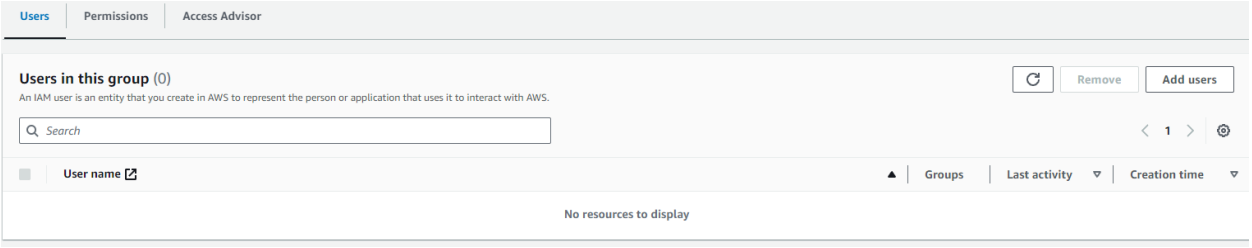
Add user-1 to the S3-Support Group

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**.



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.

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