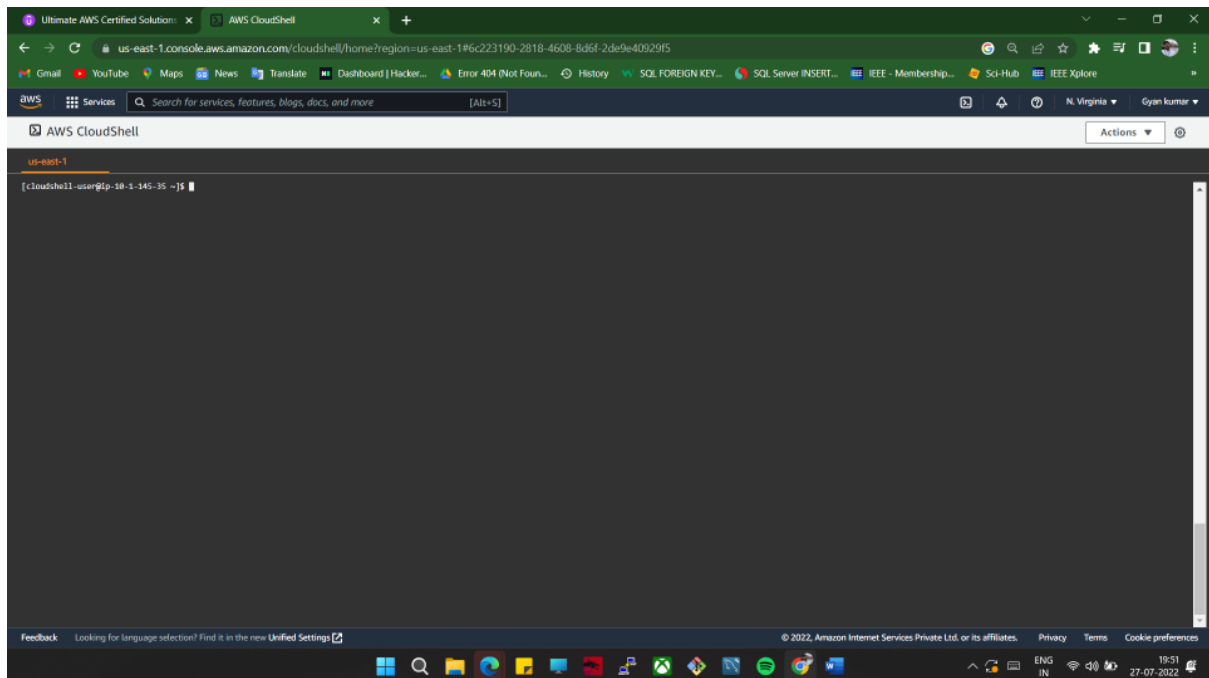


AWS CLOUD SHELL & IAM ROLES

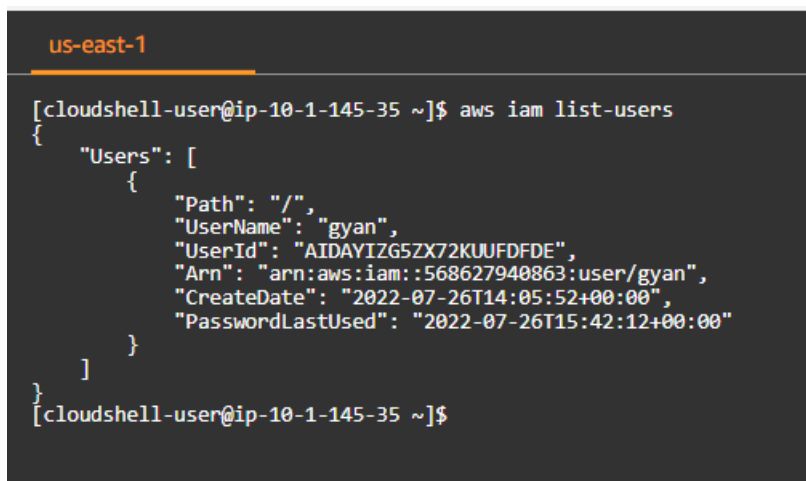
AWS cloud shell is available in some of the regions only so make sure that it is available in your region .



AWS CLOUD SHELL :- A terminal in the cloud of AWS .



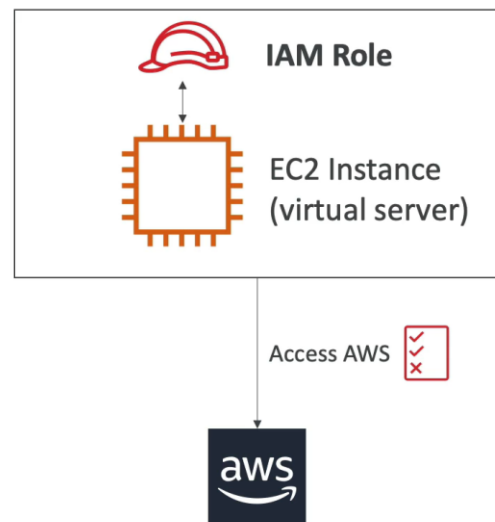
Aws iam list-users



IAM ROLES

IAM Roles for Services

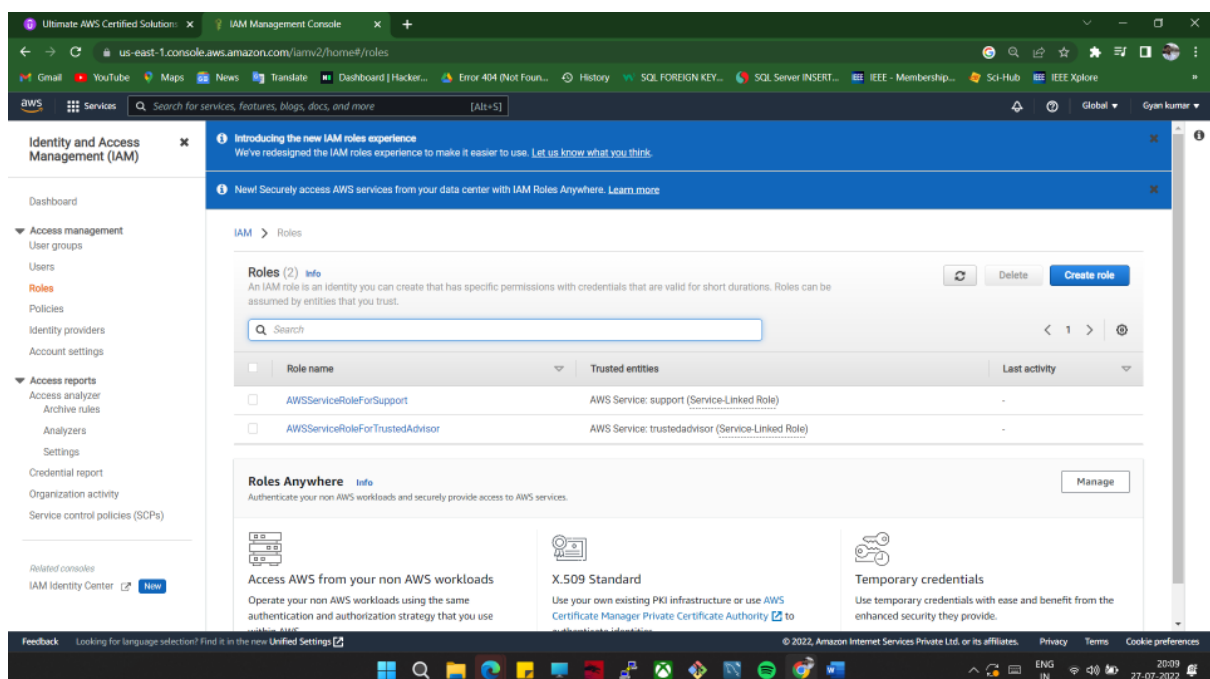
- Some AWS service will need to perform actions on your behalf
- To do so, we will assign permissions to AWS services with IAM Roles
- Common roles:



SEE Roles are something which is intended to be used not by physical people instead they will be used by AWS services.

example :- when we will create a virtual server or EC2 instance and EC2 wants to perform some action on AWS so we will attach some permission that is known as IAM role. If the EC2 wants to access some information from AWS it should have permission.

ROLE CREATION



Step 1:- Click on create role

Step 2:- Choose Trusted entity type(AWS Service)

Introducing the new IAM roles experience
We've redesigned the IAM roles experience to make it easier to use. [Let us know what you think](#)

IAM > Roles > Create role

Step 1
Select trusted entity

Step 2
Add permissions

Step 3
Name, review, and create

Select trusted entity

Trusted entity type

- ☒ **AWS service**
Allow AWS services like EC2, Lambda, or others to perform actions in this account.
- ☐ **AWS account**
Allow entities in other AWS accounts belonging to you or a 3rd party to perform actions in this account.
- ☐ **Web identity**
Allows users federated by the specified external web identity provider to assume this role to perform actions in this account.
- ☐ **SAML 2.0 federation**
Allow users federated with SAML 2.0 from a corporate directory to perform actions in this account.
- ☐ **Custom trust policy**
Create a custom trust policy to enable others to perform actions in this account.

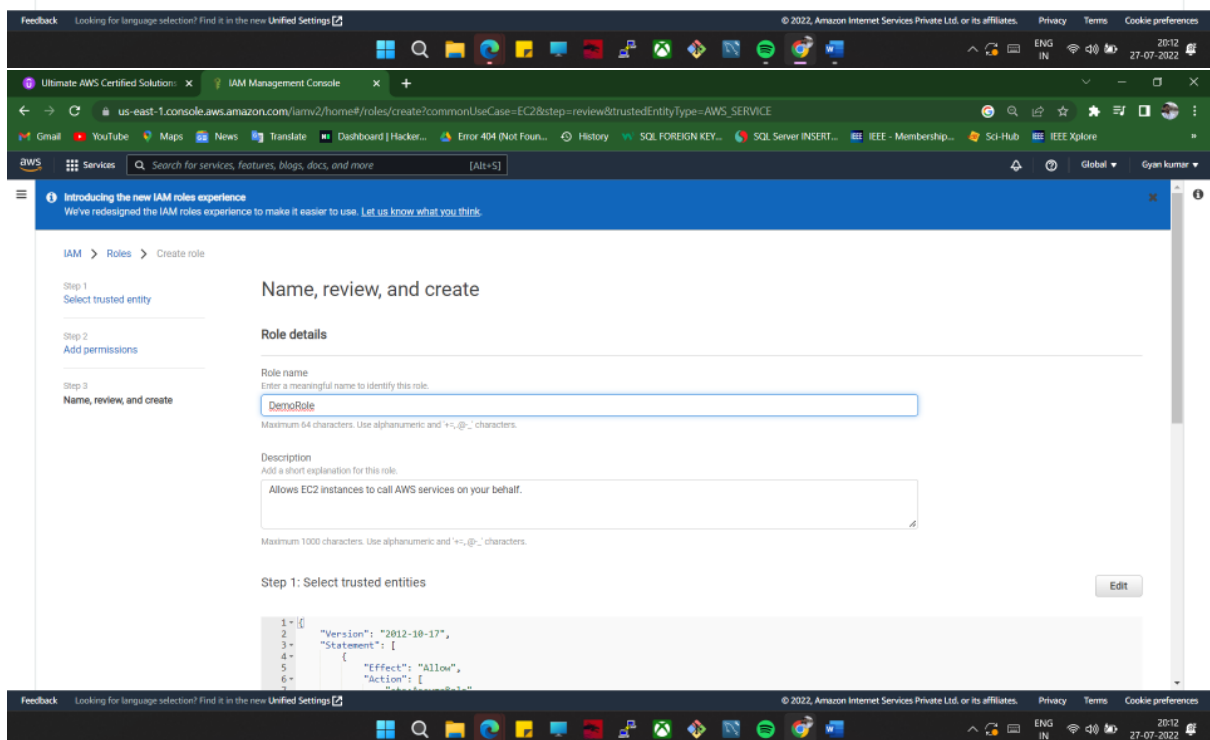
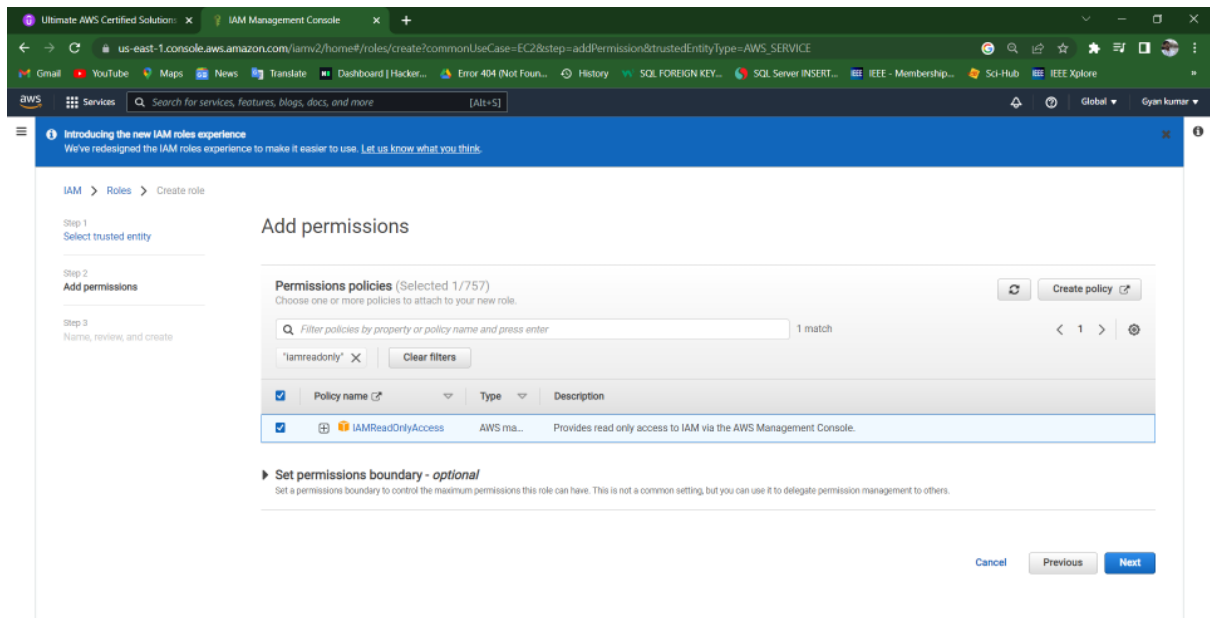
Use case
Allow an AWS service like EC2, Lambda, or others to perform actions in this account.

Common use cases

- ☐ **EC2**
Allows EC2 instances to call AWS services on your behalf.
- ☐ **Lambda**
Allows Lambda functions to call AWS services on your behalf.

Use cases for other AWS services:
Choose a service to view use case

Cancel Next



Ultimate AWS Certified Solution: xIAM Management Console x

us-east-1.console.aws.amazon.com/iamv2/home#/roles

Gmail YouTube Maps News Translate Dashboard | Hacker... Error 404 (Not Foun... SQL FOREIGN KEY... SQL Server INSERT... IEEE - Membership... Sci-Hub IEEE Xplore

BWS Services Search for services, features, blogs, docs, and more [Alt+S]

Global Gyan kumar

Identity and Access Management (IAM)

Dashboard

Access management

User groups

Users

Roles

Policies

Identity providers

Account settings

Access reports

Access analyzer

Archive rules

Analizers

Settings

Credential report

Organization activity

Service control policies (SCPs)

Related consoles

IAM Identity Center New

Introducing the new IAM roles experience

We've redesigned the IAM roles experience to make it easier to use. [Let us know what you think.](#)

Role DemoRole created

View role

New! Securely access AWS services from your data center with IAM Roles Anywhere. [Learn more](#)

IAM > Roles

Roles (3) info

An IAM role is an identity you can create that has specific permissions with credentials that are valid for short durations. Roles can be assumed by entities that you trust.

Search

1

<input type="checkbox"/>	Role name	Trusted entities	Last activity
<input type="checkbox"/>	AWSServiceRoleForSupport	AWS Service: support (Service-Linked Role)	-
<input type="checkbox"/>	AWSServiceRoleForTrustedAdvisor	AWS Service: trustedadvisor (Service-Linked Role)	-
<input type="checkbox"/>	DemoRole	AWS Service: ec2	-

Roles Anywhere info

Authenticate your non-AWS workloads and securely provide access to AWS services.

Manage

Feedback

Looking for language selection? Find it in the new [Unified Settings](#)

© 2022, Amazon Internet Services Private Ltd. or its affiliates. Privacy Terms Cookie preferences

ENG IN 20:12 27-07-2022