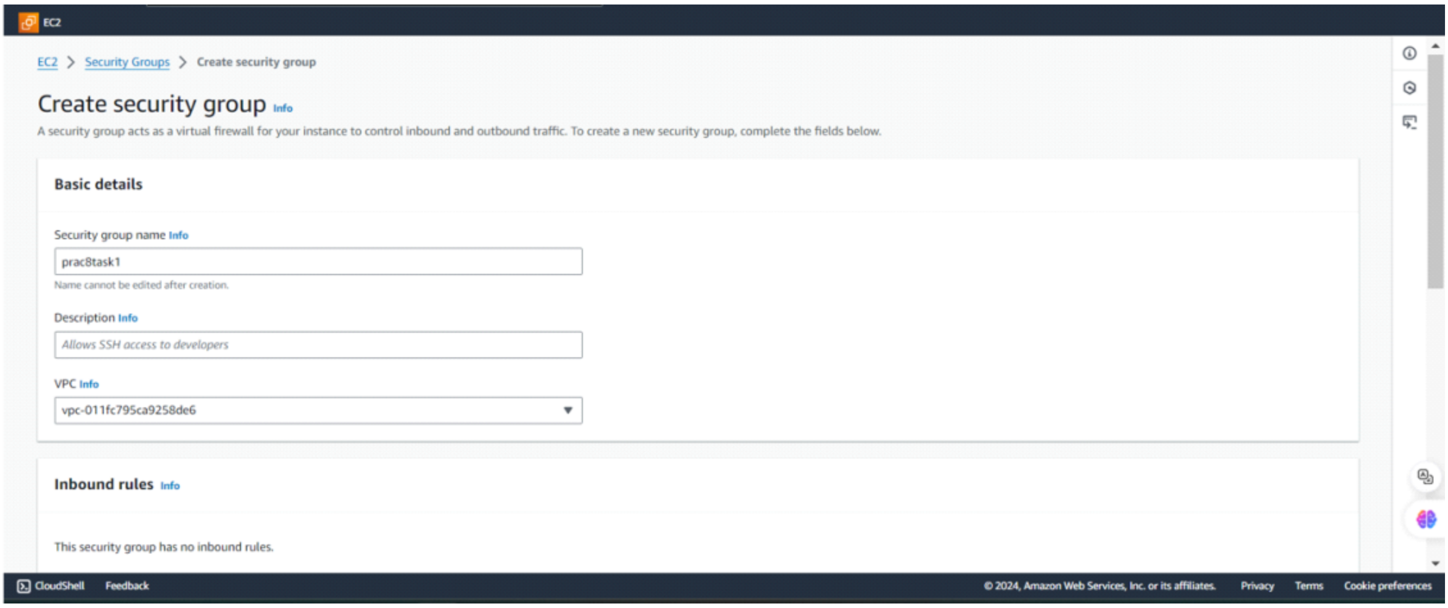
Cloud Computing

Cloud Security - Security and IAM roles

Task 1 : Security groups

Creating security groups



EC2 > Security Groups > Create security group

Create security group Info

A security group acts as a virtual firewall for your instance to control inbound and outbound traffic. To create a new security group, complete the fields below.

Basic details

Security group name Info: prac8task1

Name cannot be edited after creation.

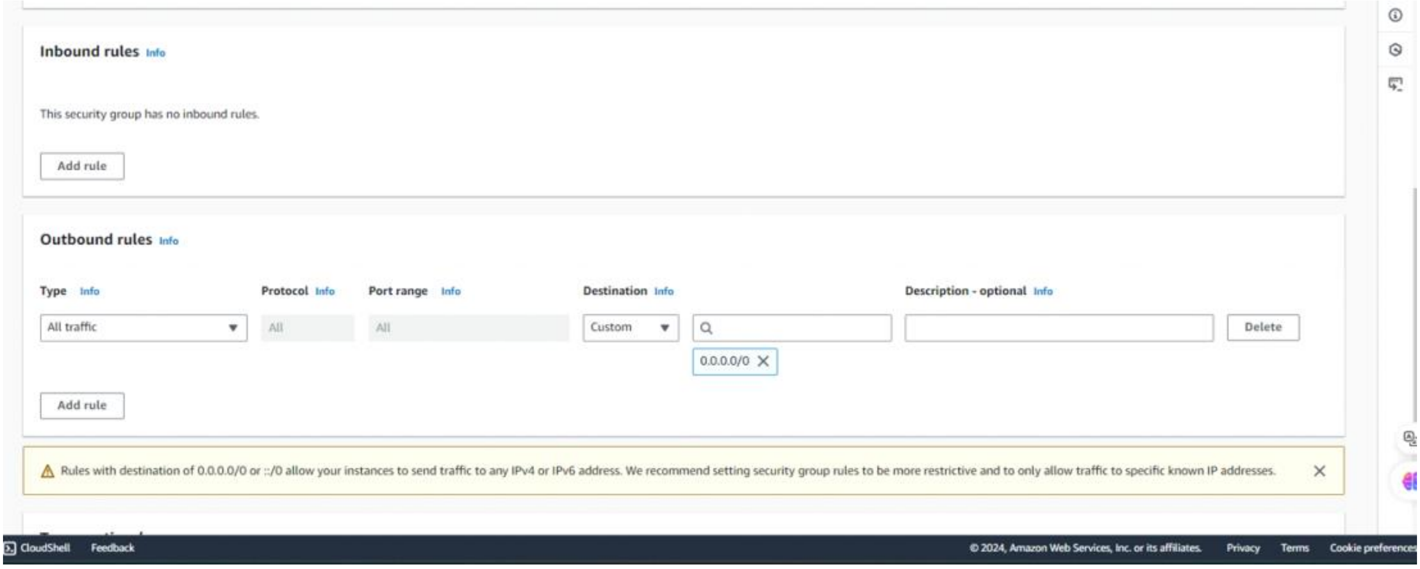
Description Info: Allows SSH access to developers

VPC Info: vpc-011fc795ca9258de6

Inbound rules Info

This security group has no inbound rules.

Setting the inbound outbound rules



Inbound rules Info

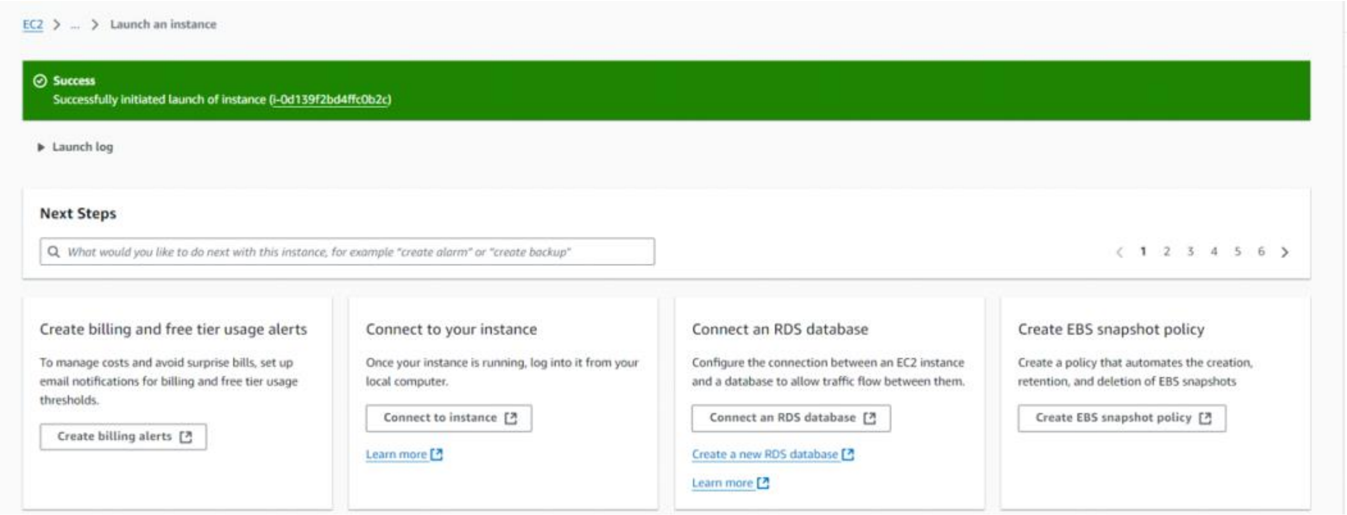
This security group has no inbound rules.

Outbound rules Info

Type Info	Protocol Info	Port range Info	Destination Info		Description - optional Info
All traffic	All	All	Custom	0.0.0.0/0	

⚠ Rules with destination of 0.0.0.0/0 or ::/0 allow your instances to send traffic to any IPv4 or IPv6 address. We recommend setting security group rules to be more restrictive and to only allow traffic to specific known IP addresses.

Creating instance with security group



EC2 > ... > Launch an instance

Success
Successfully initiated launch of instance (i-0d139f2bd4ffc0b2c)

▸ Launch log

Next Steps

What would you like to do next with this instance, for example "create alarm" or "create backup"

< 1 2 3 4 5 6 >

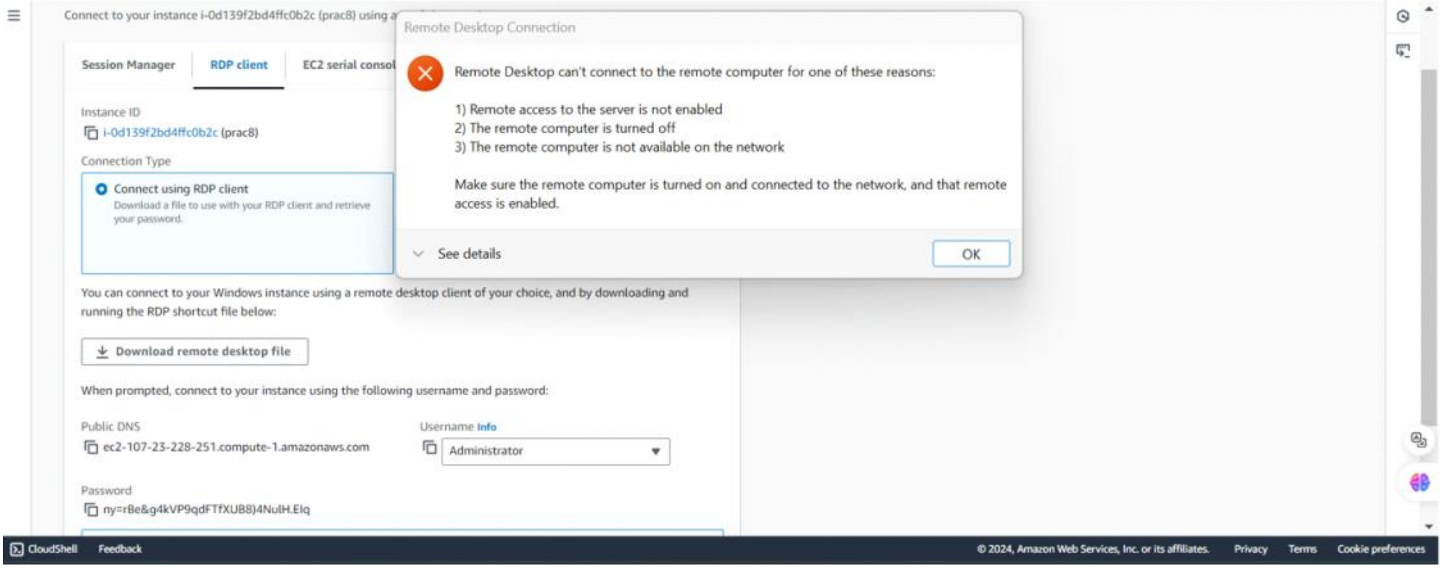
Create billing and free tier usage alerts
To manage costs and avoid surprise bills, set up email notifications for billing and free tier usage thresholds.
Create billing alerts

Connect to your instance
Once your instance is running, log into it from your local computer.
Connect to instance
Learn more

Connect an RDS database
Configure the connection between an EC2 instance and a database to allow traffic flow between them.
Connect an RDS database
Create a new RDS database
Learn more

Create EBS snapshot policy
Create a policy that automates the creation, retention, and deletion of EBS snapshots
Create EBS snapshot policy

As I have set the inbound rules as ssh so it not allowing rdp to access.



Connect to your instance i-0d139f2bd4ffc0b2c (prac8) using a

Session Manager | RDP client | EC2 serial consol

Instance ID
i-0d139f2bd4ffc0b2c (prac8)

Connection Type
● Connect using RDP client
Download a file to use with your RDP client and retrieve your password.

You can connect to your Windows instance using a remote desktop client of your choice, and by downloading and running the RDP shortcut file below:

Download remote desktop file

When prompted, connect to your instance using the following username and password:

Public DNS
ec2-107-23-228-251.compute-1.amazonaws.com

Username Info
Administrator

Password
ny=rBe&g4kVP9qdFTfXUB8)4NulH.Elq

Remote Desktop Connection

Remote Desktop can't connect to the remote computer for one of these reasons:

1) Remote access to the server is not enabled
2) The remote computer is turned off
3) The remote computer is not available on the network

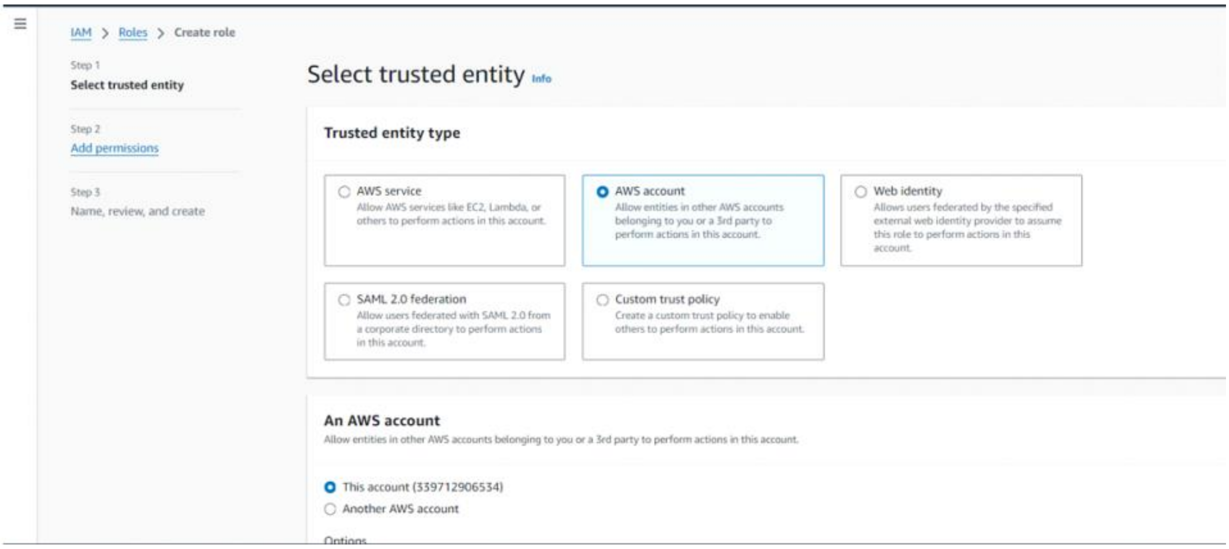
Make sure the remote computer is turned on and connected to the network, and that remote access is enabled.

See details | OK

CloudShell | Feedback | © 2024, Amazon Web Services, Inc. or its affiliates. | Privacy | Terms | Cookie preferences

Task 2 : IAM Roles

Creating IAM Roles



IAM > Roles > Create role

Step 1
Select trusted entity

Step 2
Add permissions

Step 3
Name, review, and create

Select trusted entity Info

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.

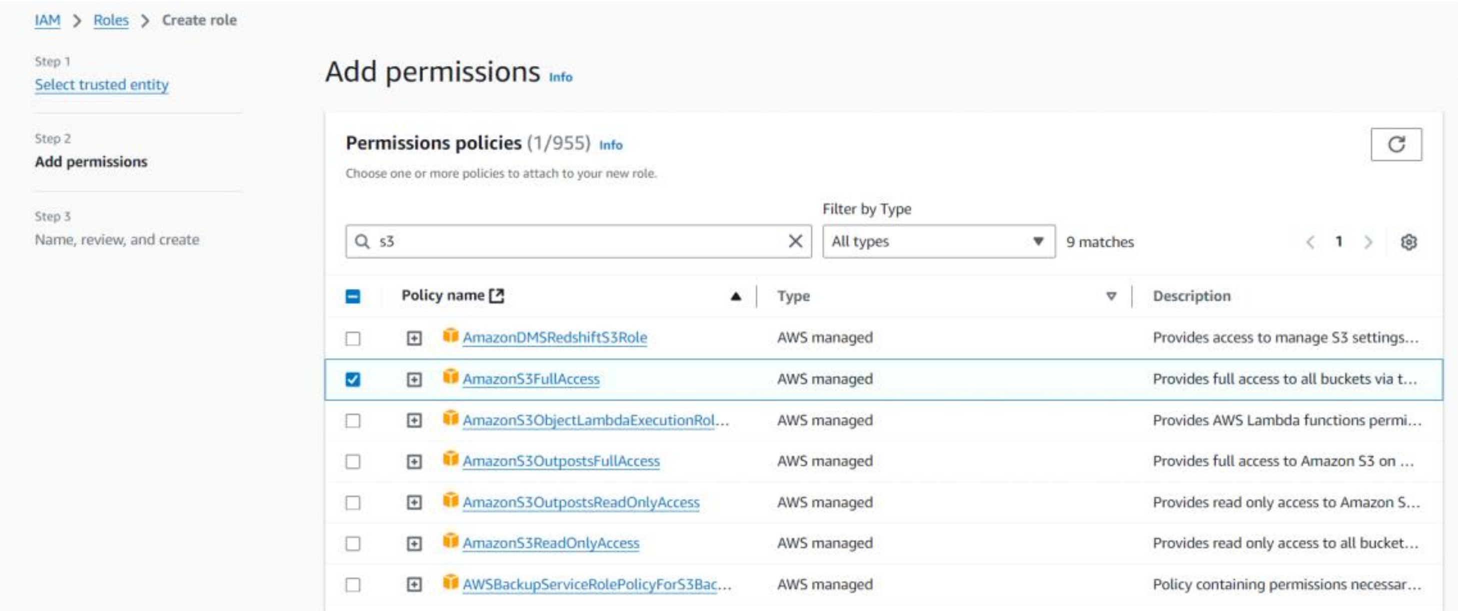
○ Custom trust policy
Create a custom trust policy to enable others to perform actions in this account.

An AWS account
Allow entities in other AWS accounts belonging to you or a 3rd party to perform actions in this account.

● This account (339712906534)
○ Another AWS account

Options

Giving S3 full_access



IAM > Roles > Create role

Step 1
Select trusted entity

Step 2
Add permissions

Step 3
Name, review, and create

Add permissions Info

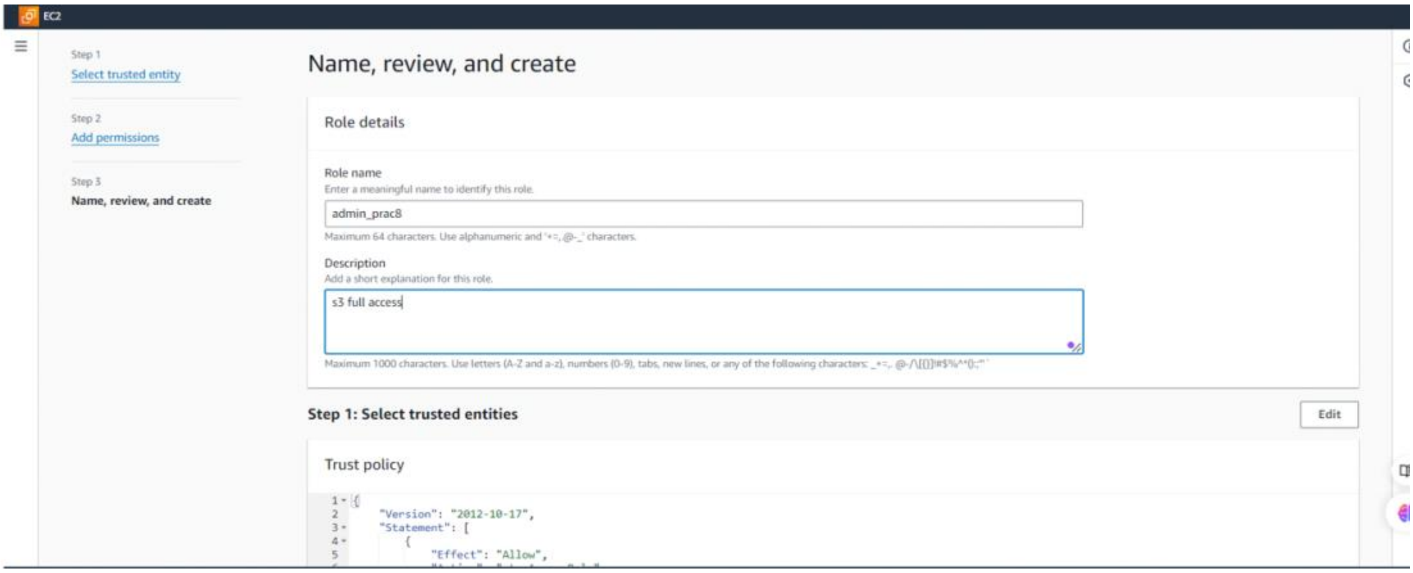
Permissions policies (1/955) Info

Choose one or more policies to attach to your new role.

Filter by Type

s3 | All types | 9 matches | 1

		Policy name	Type	Description
□	⊞	AmazonDMSRedshiftS3Role	AWS managed	Provides access to manage S3 settings…
☑	⊞	AmazonS3FullAccess	AWS managed	Provides full access to all buckets via t…
□	⊞	AmazonS3ObjectLambdaExecutionRol…	AWS managed	Provides AWS Lambda functions permi…
□	⊞	AmazonS3OutpostsFullAccess	AWS managed	Provides full access to Amazon S3 on …
□	⊞	AmazonS3OutpostsReadOnlyAccess	AWS managed	Provides read only access to Amazon S…
□	⊞	AmazonS3ReadOnlyAccess	AWS managed	Provides read only access to all bucket…
□	⊞	AWSBackupServiceRolePolicyForS3Bac…	AWS managed	Policy containing permissions necessar…



Step 1
Select trusted entity

Step 2
Add permissions

Step 3
Name, review, and create

Name, review, and create

Role details

Role name
Enter a meaningful name to identify this role.

admin_prac8

Maximum 64 characters. Use alphanumeric and '+=,.@-_' characters.

Description
Add a short explanation for this role.

s3 full access

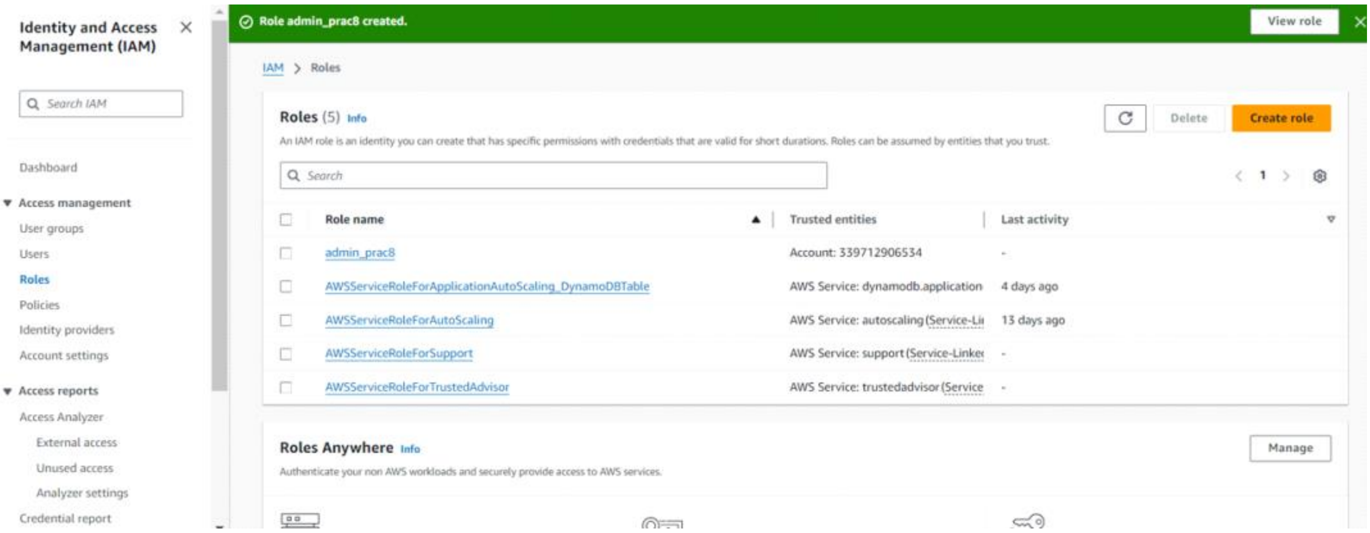
Maximum 1000 characters. Use letters (A-Z and a-z), numbers (0-9), tabs, new lines, or any of the following characters: _+=,. @-/\[{()}]!#$%^*();:"'

Step 1: Select trusted entities

Trust policy

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
```

Hence the iam role is created successfully under name admin_prac8



Role admin_prac8 created.

Roles (5) 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.

□	Role name	Trusted entities	Last activity
□	admin_prac8	Account: 339712906534	-
□	AWSServiceRoleForApplicationAutoScaling_DynamoDBTable	AWS Service: dynamodb.application	4 days ago
□	AWSServiceRoleForAutoScaling	AWS Service: autoscaling (Service-Li	13 days ago
□	AWSServiceRoleForSupport	AWS Service: support (Service-Linke	-
□	AWSServiceRoleForTrustedAdvisor	AWS Service: trustedadvisor (Service	-

Roles Anywhere Info

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