Module 3: IAM Roles Assignment

SUBMITTED BY :-HITESH CHAUHAN

COURSES OFFERED:ADVANCED CLOUD COMPUTING AND DEVELOPS

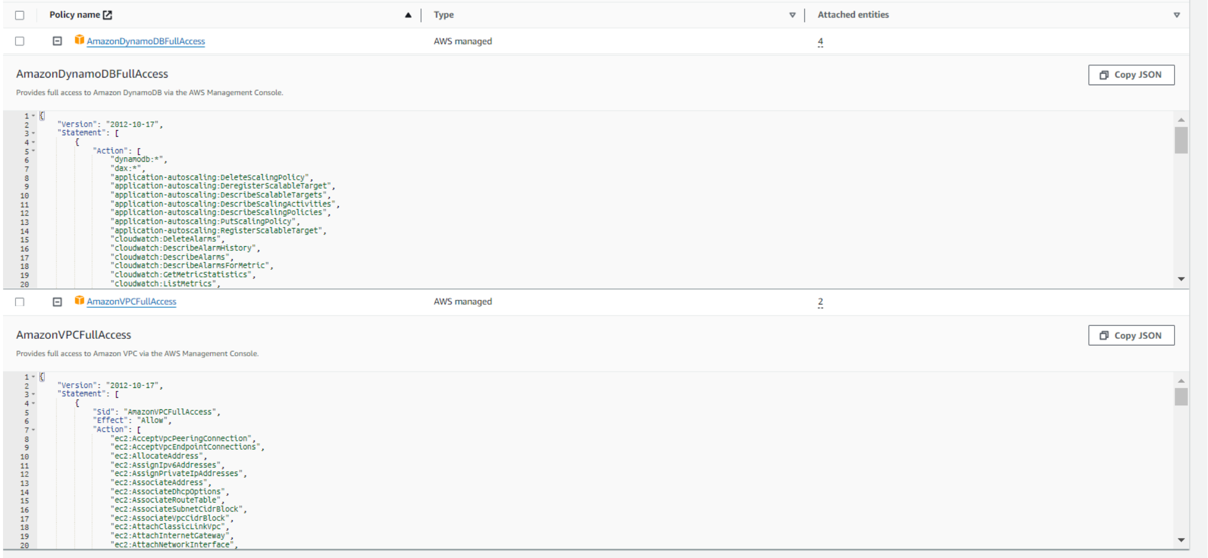
Problem Statement:

You work for XYZ Corporation. To maintain the security of the AWS account and the resources you have been asked to implement a solution that can help easily recognize and monitor the different users..

Tasks To Be Performed:

1.Create a role which only lets user1 and user2 from task 1 to have complete access to VPCs and DynamoDB.

This is VPC Role And DynamoDB Role Full Access.



□	Policy name	Type	Attached entities
□	⊟ AmazonDynamoDBFullAccess	AWS managed	4

AmazonDynamoDBFullAccess

Provides full access to Amazon DynamoDB via the AWS Management Console.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Action": [
                "dynamodb:*",
                "dax:*",
                "application-autoscaling:DeleteScalingPolicy",
                "application-autoscaling:DeregisterScalableTarget",
                "application-autoscaling:DescribeScalableTargets",
                "application-autoscaling:DescribeScalingActivities",
                "application-autoscaling:DescribeScalingPolicies",
                "application-autoscaling:PutScalingPolicy",
                "application-autoscaling:RegisterScalableTarget",
                "cloudwatch:DeleteAlarms",
                "cloudwatch:DescribeAlarmHistory",
                "cloudwatch:DescribeAlarms",
                "cloudwatch:DescribeAlarmsForMetric",
                "cloudwatch:GetMetricStatistics",
                "cloudwatch:ListMetrics",
```

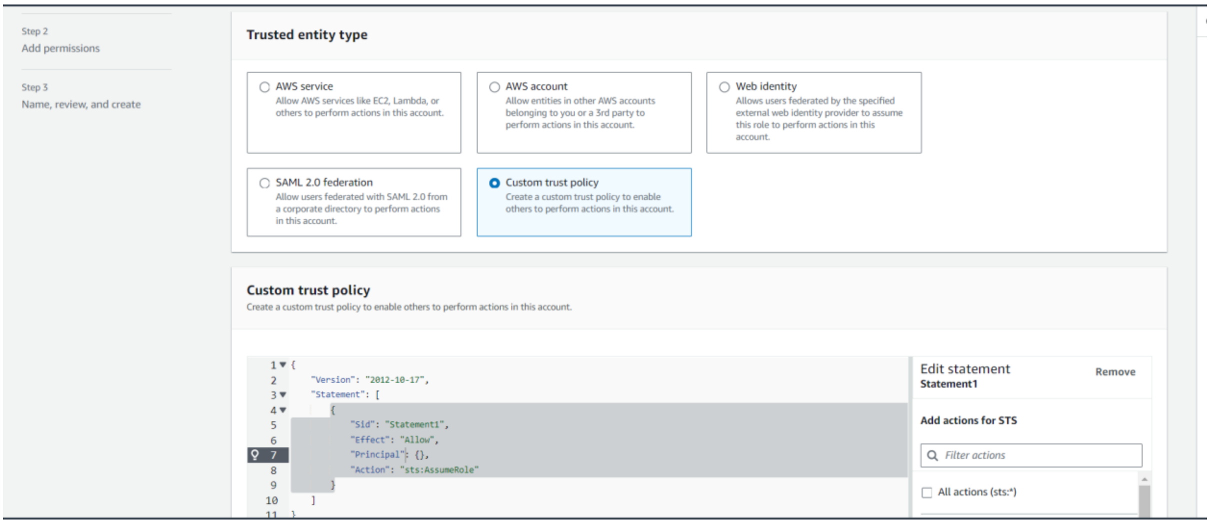
□	Policy name	Type	Attached entities
□	⊟ AmazonVPCFullAccess	AWS managed	2

AmazonVPCFullAccess

Provides full access to Amazon VPC via the AWS Management Console.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "AmazonVPCFullAccess",
            "Effect": "Allow",
            "Action": [
                "ec2:AcceptVpcPeeringConnection",
                "ec2:AcceptVpcEndpointConnections",
                "ec2:AllocateAddress",
                "ec2:AssignIpv6Addresses",
                "ec2:AssignPrivateIpAddresses",
                "ec2:AssociateAddress",
                "ec2:AssociateDhcpOptions",
                "ec2:AssociateRouteTable",
                "ec2:AssociateSubnetCidrBlock",
                "ec2:AssociateVpcCidrBlock",
                "ec2:AttachClassicLinkVpc",
                "ec2:AttachInternetGateway",
                "ec2:AttachNetworkInterface",
```

We can create custom trust policy



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.

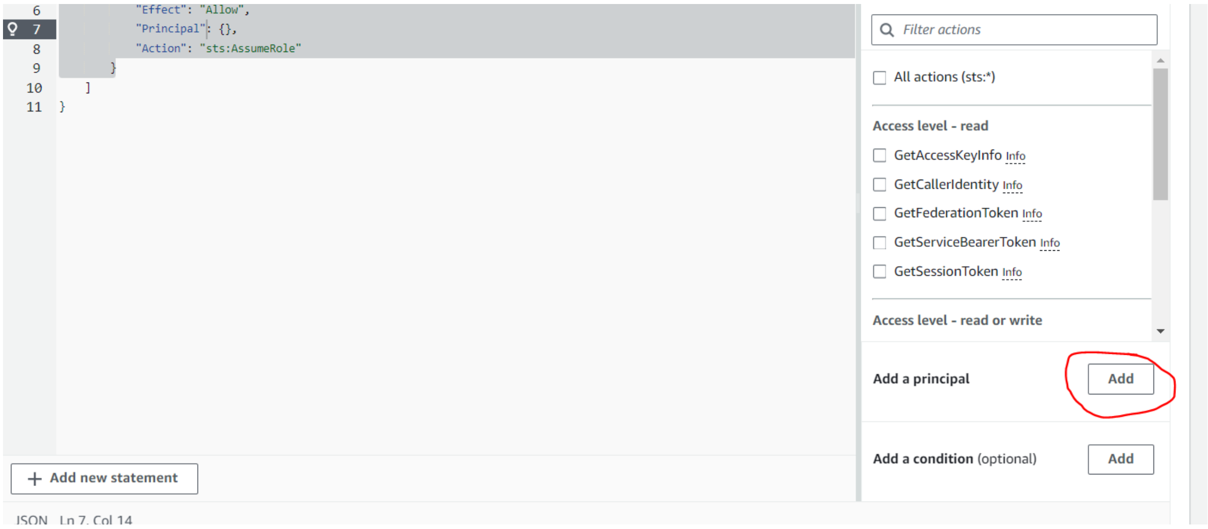
● Custom trust policy
Create a custom trust policy to enable others to perform actions in this account.

Custom trust policy

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

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "Statement1",
            "Effect": "Allow",
            "Principal": {},
            "Action": "sts:AssumeRole"
        }
    ]
}
```

Then we go Add A principal



```
            "Effect": "Allow",
            "Principal": {},
            "Action": "sts:AssumeRole"
        }
    ]
}
```

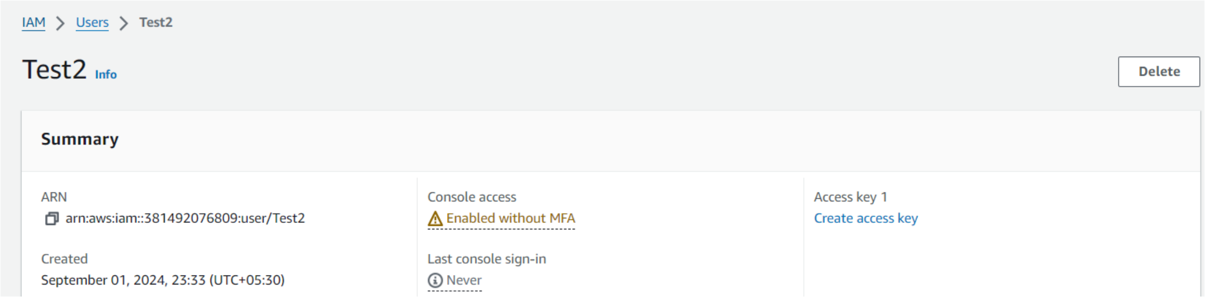
Now we need to specify the user through IAM users

So we have selected IAM Users and ARN we need to require for the below users.how can check and confirm ARN for specific user

Go IAM>Users>Test1

Below Screenshot ARN (This is the ARN of Test2 User)

Note:-ARN is unique for All IAM users.We can check ARN Look like this.



IAM > Users > Test2

Test2 Info

Summary

ARN
arn:aws:iam::381492076809:user/Test2

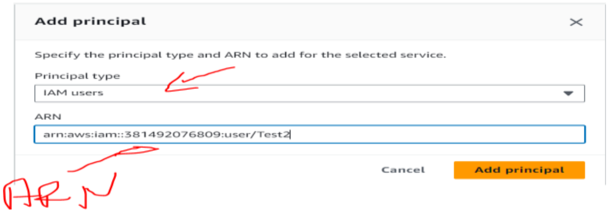
Created
September 01, 2024, 23:33 (UTC+05:30)

Console access
Enabled without MFA

Last console sign-in
Never

Access key 1
Create access key

So we need to specify the role to Test1 And Test2 Users Then Click Add Principal



Add principal

Specify the principal type and ARN to add for the selected service.

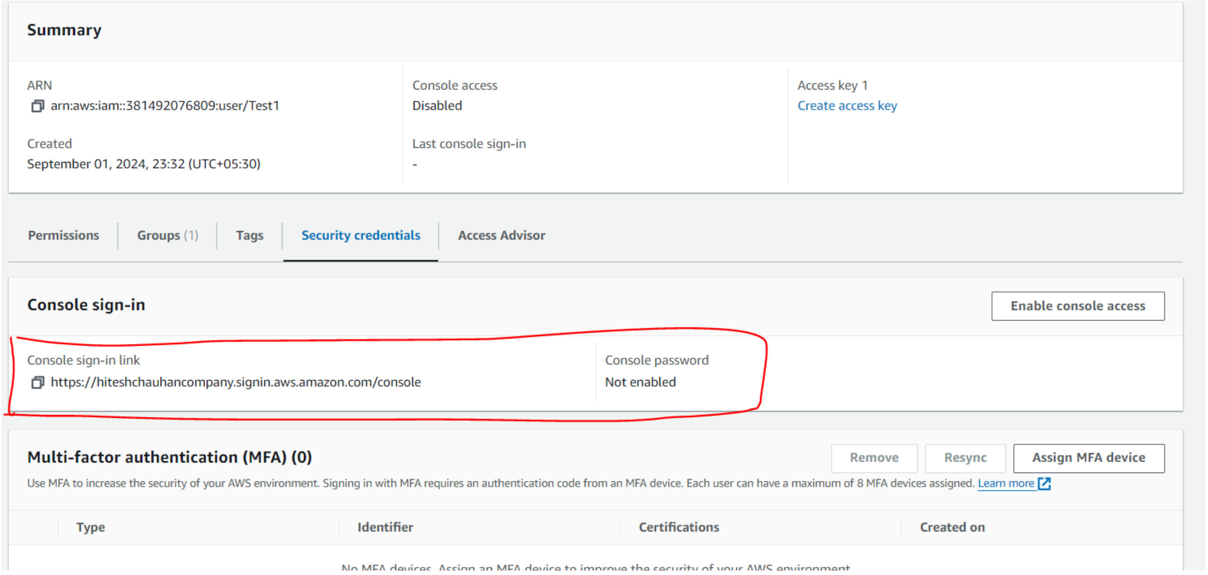
Principal type: IAM users

ARN: arn:aws:iam::381492076809:user/Test2

Then Go IAM Users and Copy This url

https://hiteshchauhancompany.signin.aws.amazon.com/console

Login the with urls with Test1 User And Password



Summary

ARN: arn:aws:iam::381492076809:user/Test1

Created: September 01, 2024, 23:32 (UTC+05:30)

Console access: Disabled

Last console sign-in: -

Access key 1: Create access key

Console sign-in

Console sign-in link: https://hiteshchauhancompany.signin.aws.amazon.com/console

Console password: Not enabled

Multi-factor authentication (MFA) (0)

Use MFA to increase the security of your AWS environment. Signing in with MFA requires an authentication code from an MFA device. Each user can have a maximum of 8 MFA devices assigned. Learn more

Type	Identifier	Certifications	Created on

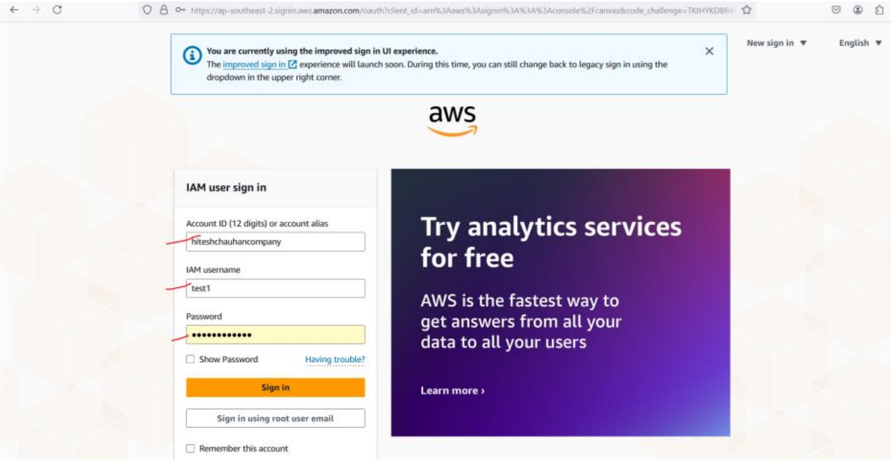
No MFA devices. Assign an MFA device to improve the security of your AWS environment

After Login the Urls you need to fill this below information like

Account ID Or Account Alias Name

My Account Alias Name is hiteshchauhancompany then

IAM User will be test1 and login with current password.



https://ap-southeast-2.signin.aws.amazon.com/oauth?client_id=arn%3Aaws%3Asignin%3A%3A%3Aconsole%2Fcanvas&code_challenge=TKIHYKDBfr

You are currently using the improved sign in UI experience.
The improved sign in experience will launch soon. During this time, you can still change back to legacy sign in using the dropdown in the upper right corner.

IAM user sign in

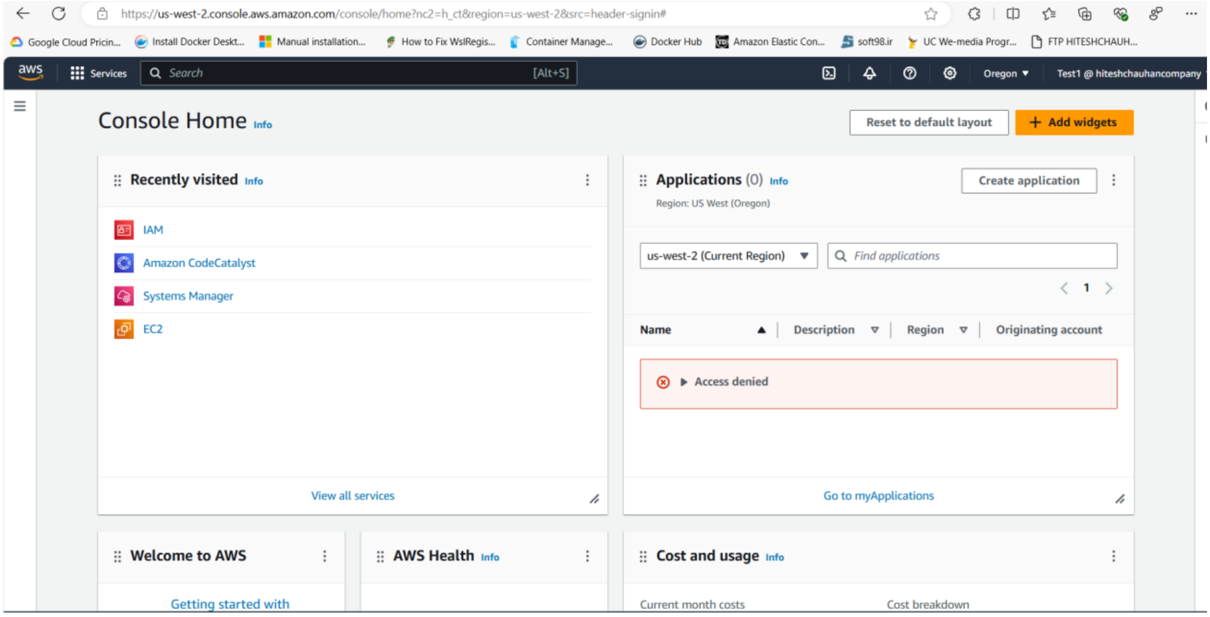
Account ID (12 digits) or account alias: hiteshchauhancompany

IAM username: test1

Password: •••••••••••••

Try analytics services for free

AWS is the fastest way to get answers from all your data to all your users



https://us-west-2.console.aws.amazon.com/console/home?nc2=h_ct&region=us-west-2&src=header-signin#

Console Home Info

Recently visited Info

- IAM
- Amazon CodeCatalyst
- Systems Manager
- EC2

Applications (0) Info

Region: US West (Oregon)

Name ▲ | Description ▽ | Region ▽ | Originating account

Access denied

Welcome to AWS

AWS Health Info

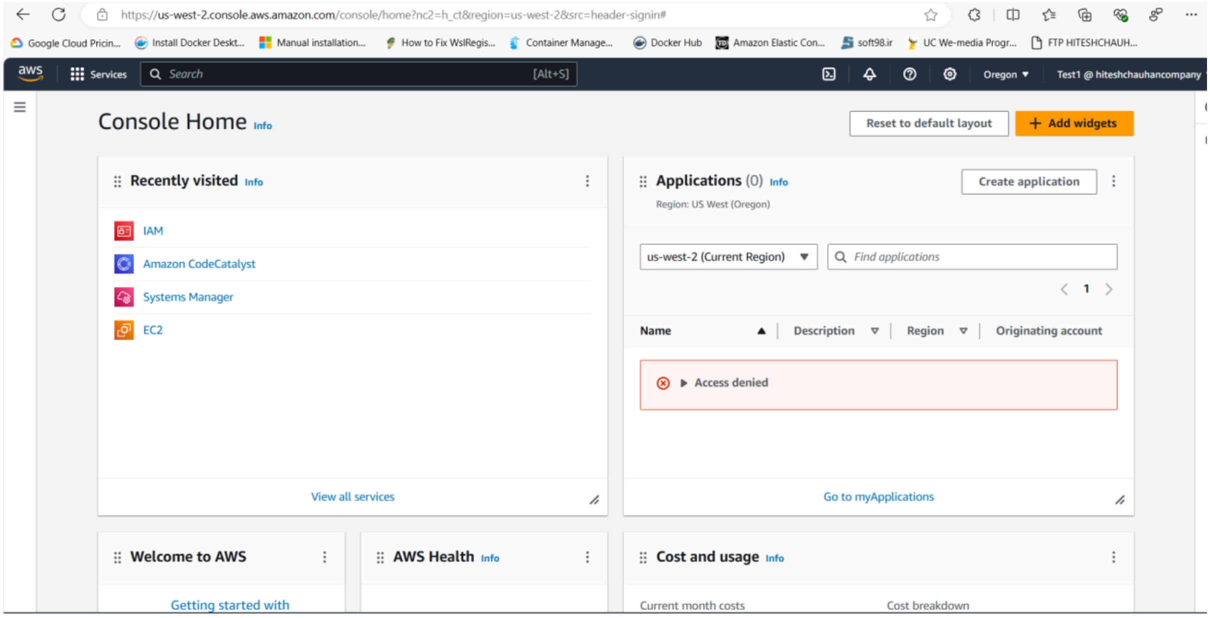
Cost and usage Info

Current month costs

Cost breakdown

2. Login into user1 and shift to the role to test out the feature.

We have assigned role of test1 user is Complete DynamoDB Access And vpc



https://us-west-2.console.aws.amazon.com/console/home?nc2=h_ct&region=us-west-2&src=header-signin#

Google Cloud Pricin... Install Docker Deskt... Manual installation... How to Fix WslRegis... Container Manage... Docker Hub Amazon Elastic Con... soft98.ir UC We-media Progr... FTP HITESHCHAUH...

aws Services Search [Alt+S] Oregon ▾ Test1 @ hiteshchauhancompany

Console Home Info

Reset to default layout

+ Add widgets

Recently visited Info

- IAM
- Amazon CodeCatalyst
- Systems Manager
- EC2

View all services

Applications (0) Info

Region: US West (Oregon)

Create application

us-west-2 (Current Region) ▾

Find applications

Name ▲	Description ▽	Region ▽	Originating account

⊗ ▸ Access denied

Go to myApplications

Welcome to AWS

Getting started with

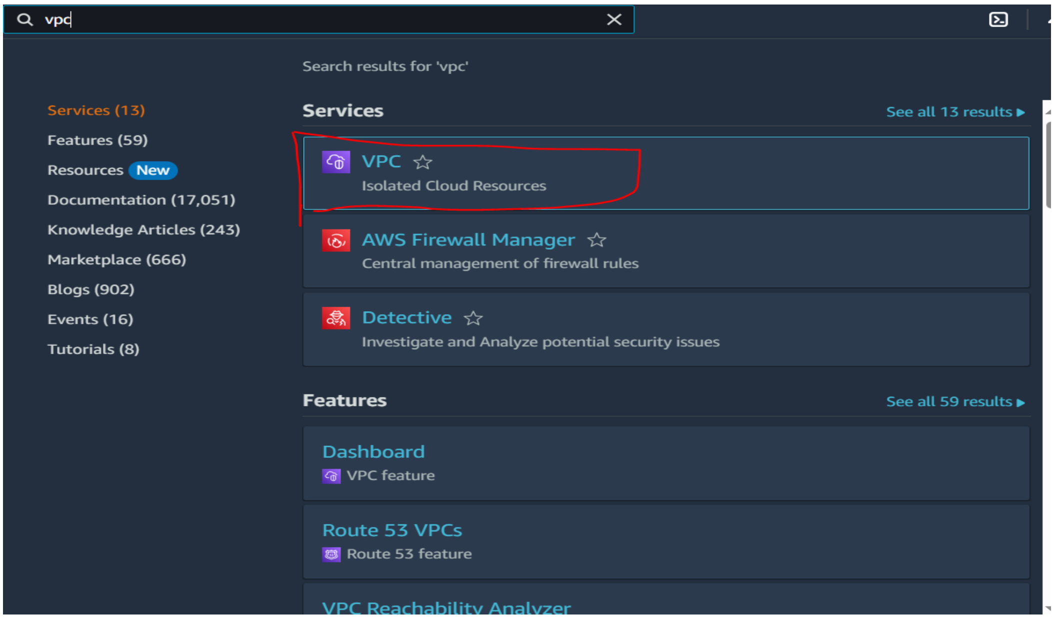
AWS Health Info

Cost and usage Info

Current month costs

Cost breakdown

Go to search the VPC



vpc

Search results for 'vpc'

- Services (13)
- Features (59)
- Resources New
- Documentation (17,051)
- Knowledge Articles (243)
- Marketplace (666)
- Blogs (902)
- Events (16)
- Tutorials (8)

Services

See all 13 results ▸

VPC ☆

Isolated Cloud Resources

AWS Firewall Manager ☆

Central management of firewall rules

Detective ☆

Investigate and Analyze potential security issues

Features

See all 59 results ▸

Dashboard

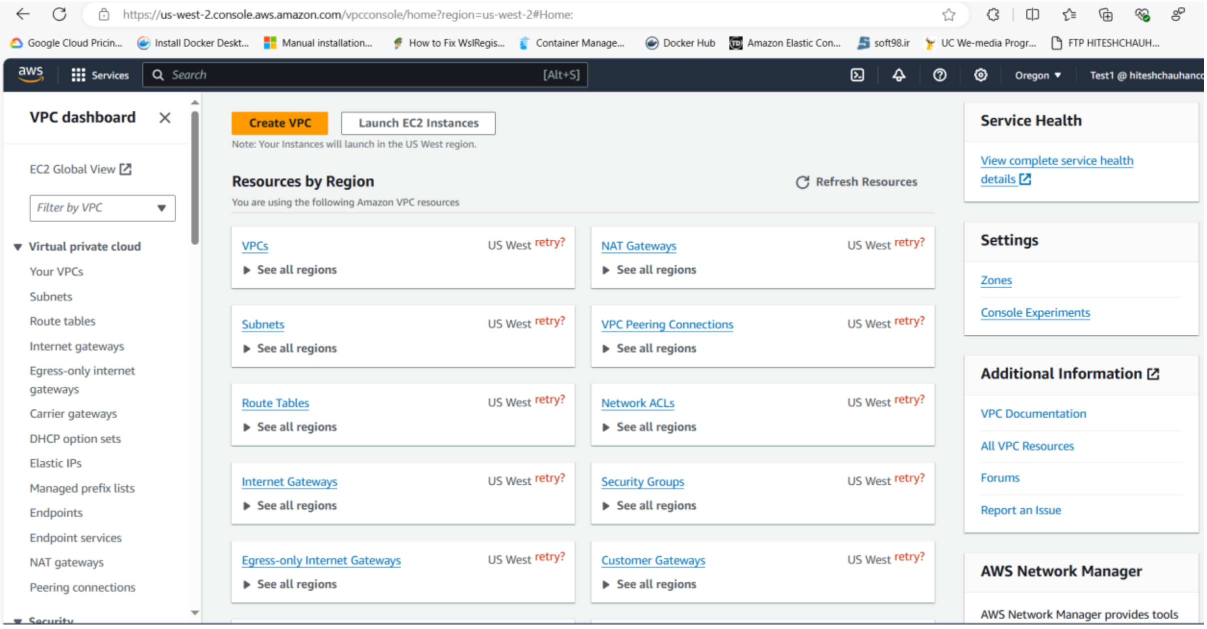
VPC feature

Route 53 VPCs

Route 53 feature

VPC Reachability Analyzer

You will see vpc dashboard but I want access ec2 instance for checking it is role proper work or not.role is working properly ec2 instance is not allow to create the permission



Note: Your Instances will launch in the US West region.

Resources by Region

Refresh Resources

You are using the following Amazon VPC resources

VPCs US West retry? ▶ See all regions	NAT Gateways US West retry? ▶ See all regions
Subnets US West retry? ▶ See all regions	VPC Peering Connections US West retry? ▶ See all regions
Route Tables US West retry? ▶ See all regions	Network ACLs US West retry? ▶ See all regions
Internet Gateways US West retry? ▶ See all regions	Security Groups US West retry? ▶ See all regions
Egress-only Internet Gateways US West retry? ▶ See all regions	Customer Gateways US West retry? ▶ See all regions

Service Health

View complete service health details

Settings

Zones

Console Experiments

Additional Information

VPC Documentation

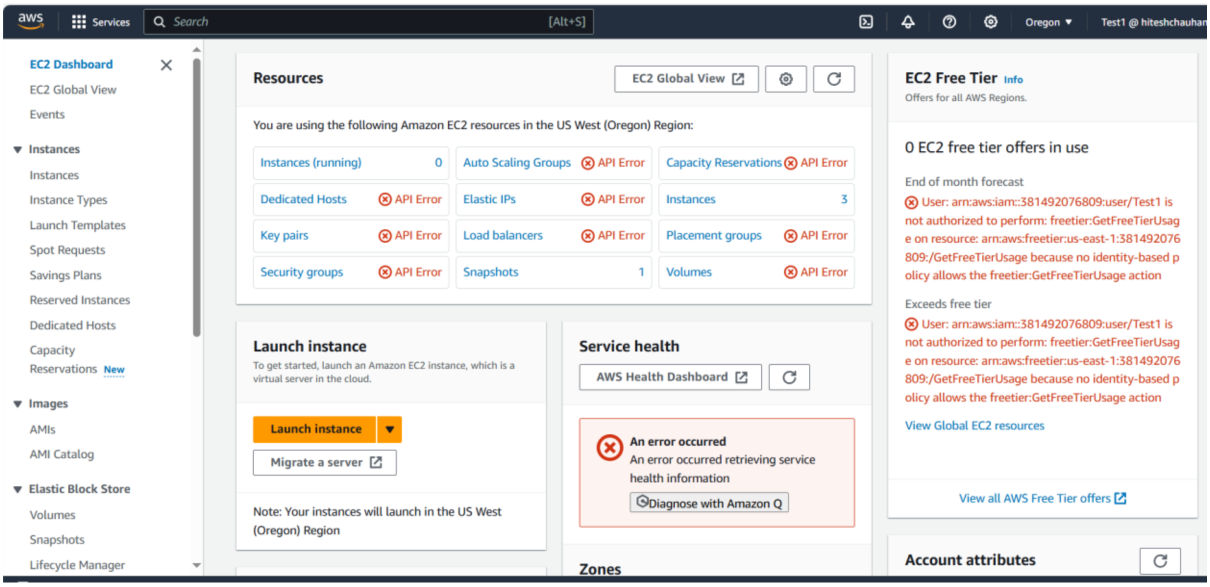
All VPC Resources

Forums

Report an Issue

AWS Network Manager

AWS Network Manager provides tools



Resources

You are using the following Amazon EC2 resources in the US West (Oregon) Region:

Instances (running)	0	Auto Scaling Groups	⊗ API Error	Capacity Reservations	⊗ API Error
Dedicated Hosts	⊗ API Error	Elastic IPs	⊗ API Error	Instances	3
Key pairs	⊗ API Error	Load balancers	⊗ API Error	Placement groups	⊗ API Error
Security groups	⊗ API Error	Snapshots	1	Volumes	⊗ API Error

Launch instance

To get started, launch an Amazon EC2 instance, which is a virtual server in the cloud.

Launch instance ▼

Migrate a server

Note: Your instances will launch in the US West (Oregon) Region

Service health

AWS Health Dashboard

An error occurred

An error occurred retrieving service health information

Diagnose with Amazon Q

Zones

EC2 Free Tier Info

Offers for all AWS Regions.

0 EC2 free tier offers in use

End of month forecast

⊗ User: arn:aws:iam::381492076809:user/Test1 is not authorized to perform: freetier:GetFreeTierUsage on resource: arn:aws:freetier:us-east-1:381492076809:/GetFreeTierUsage because no identity-based policy allows the freetier:GetFreeTierUsage action

Exceeds free tier

⊗ User: arn:aws:iam::381492076809:user/Test1 is not authorized to perform: freetier:GetFreeTierUsage on resource: arn:aws:freetier:us-east-1:381492076809:/GetFreeTierUsage because no identity-based policy allows the freetier:GetFreeTierUsage action

View Global EC2 resources

View all AWS Free Tier offers

Account attributes