Amazon IAM: IAM Roles -Task

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.

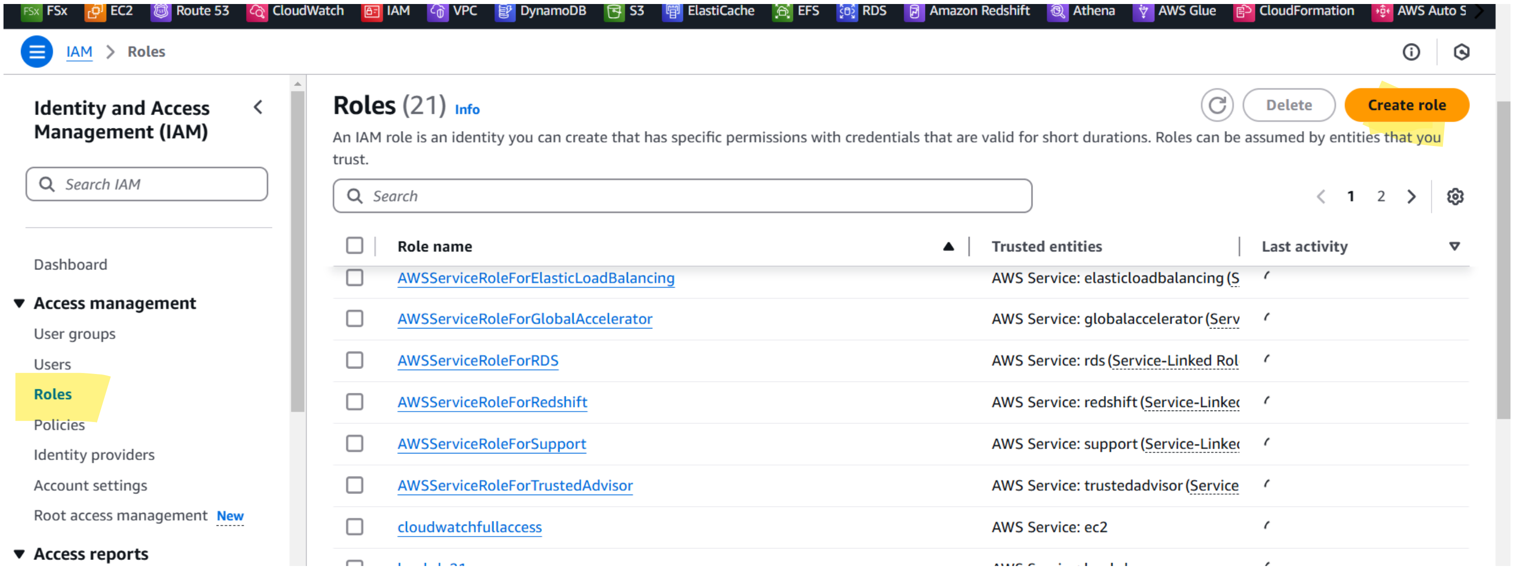
Tasks To Be Performed:

1. Create a role which only lets user1 and user2 from task 1 to have complete access to VPCs and DynamoDB.
2. Login into user1 and shift to the role to test out the feature.

---

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

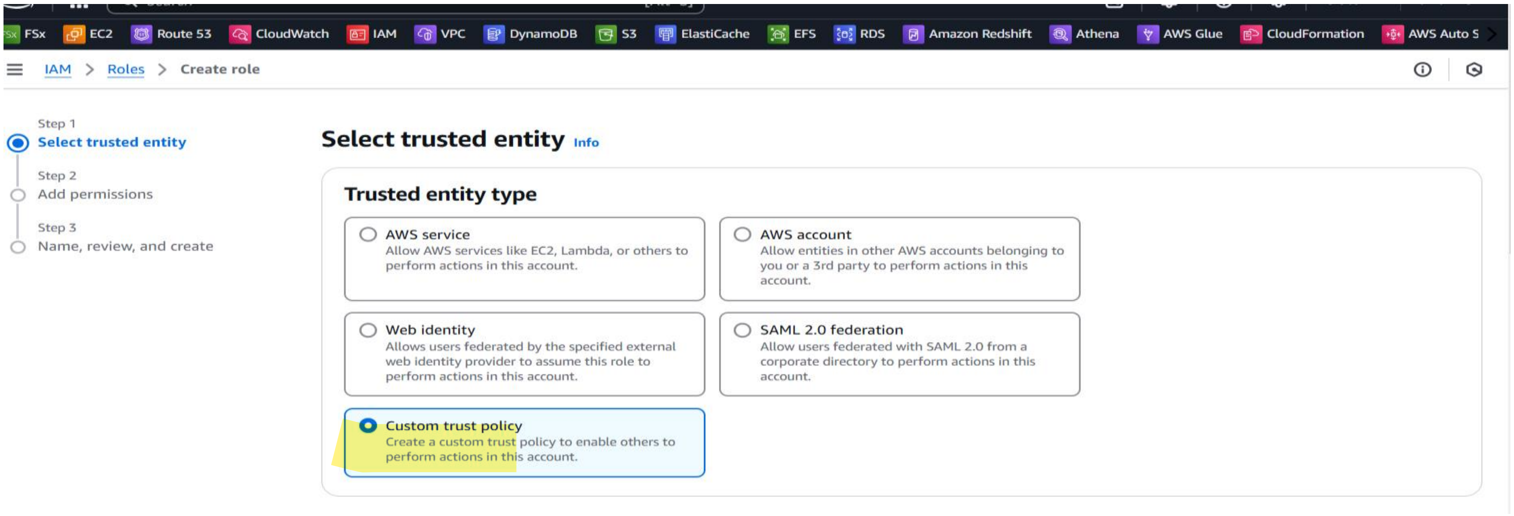
- Go to IAM dashboard , click roles , click create role, click custom trust policy, provides ARN of Dev1,Dev2, here user1,user2,.click next add permission , provides role name and click create role.



Roles (21)

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
□	AWSServiceRoleForElasticLoadBalancing	AWS Service: elasticloadbalancing (S	
□	AWSServiceRoleForGlobalAccelerator	AWS Service: globalaccelerator (Serv	
□	AWSServiceRoleForRDS	AWS Service: rds (Service-Linked Rol	
□	AWSServiceRoleForRedshift	AWS Service: redshift (Service-Linkec	
□	AWSServiceRoleForSupport	AWS Service: support (Service-Linkec	
□	AWSServiceRoleForTrustedAdvisor	AWS Service: trustedadvisor (Service	
□	cloudwatchfullaccess	AWS Service: ec2	



Select trusted entity Info

Trusted entity type

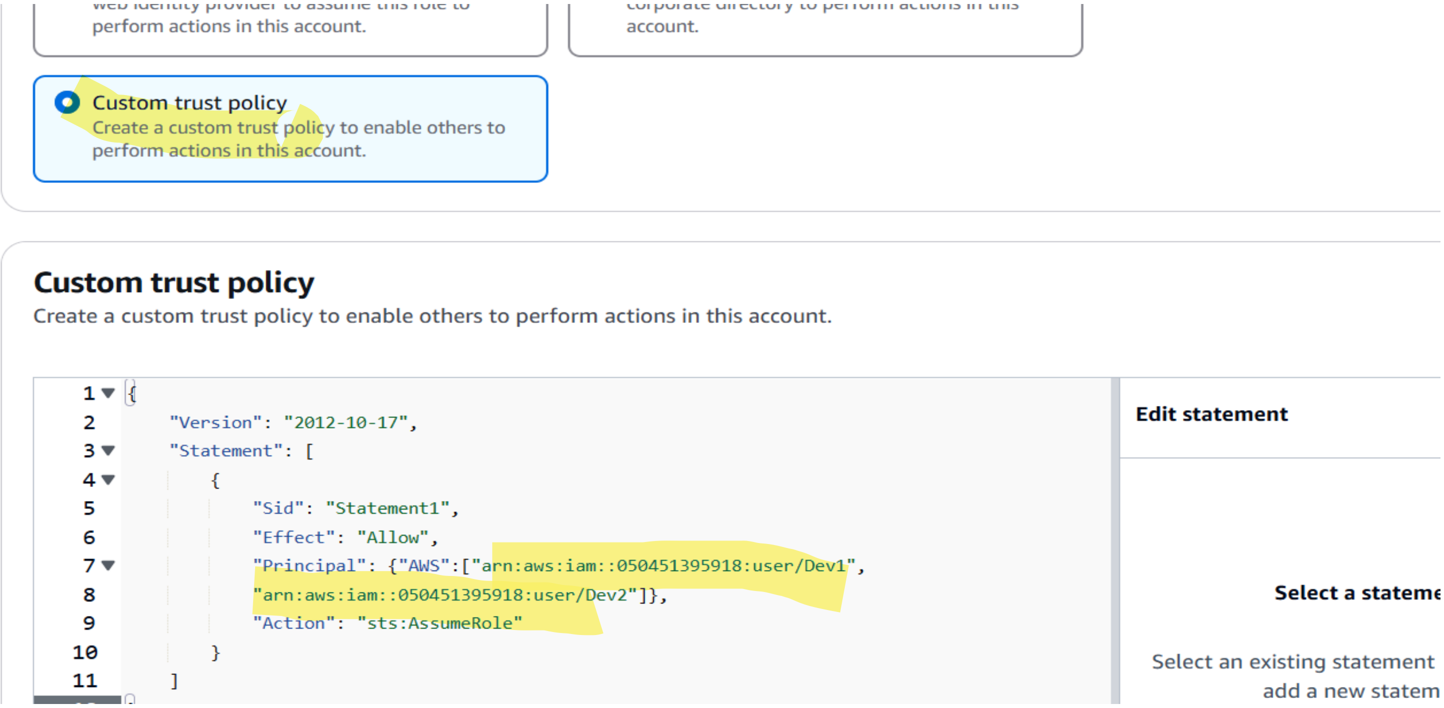
○ AWS service
Allow AWS services like EC2, Lambda, or others to perform actions in this account.

○ 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.



web identity provider to assume this role to perform actions in this account.

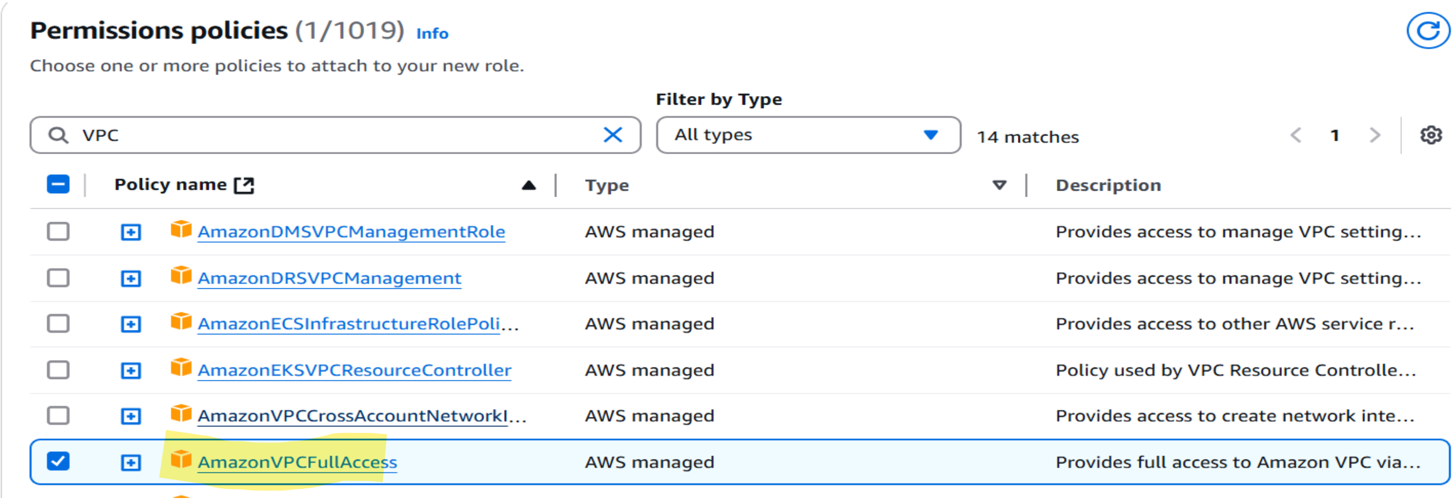
corporate directory to perform actions in this account.

● 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": {"AWS":["arn:aws:iam::050451395918:user/Dev1",
            "arn:aws:iam::050451395918:user/Dev2"]},
            "Action": "sts:AssumeRole"
        }
    ]
```



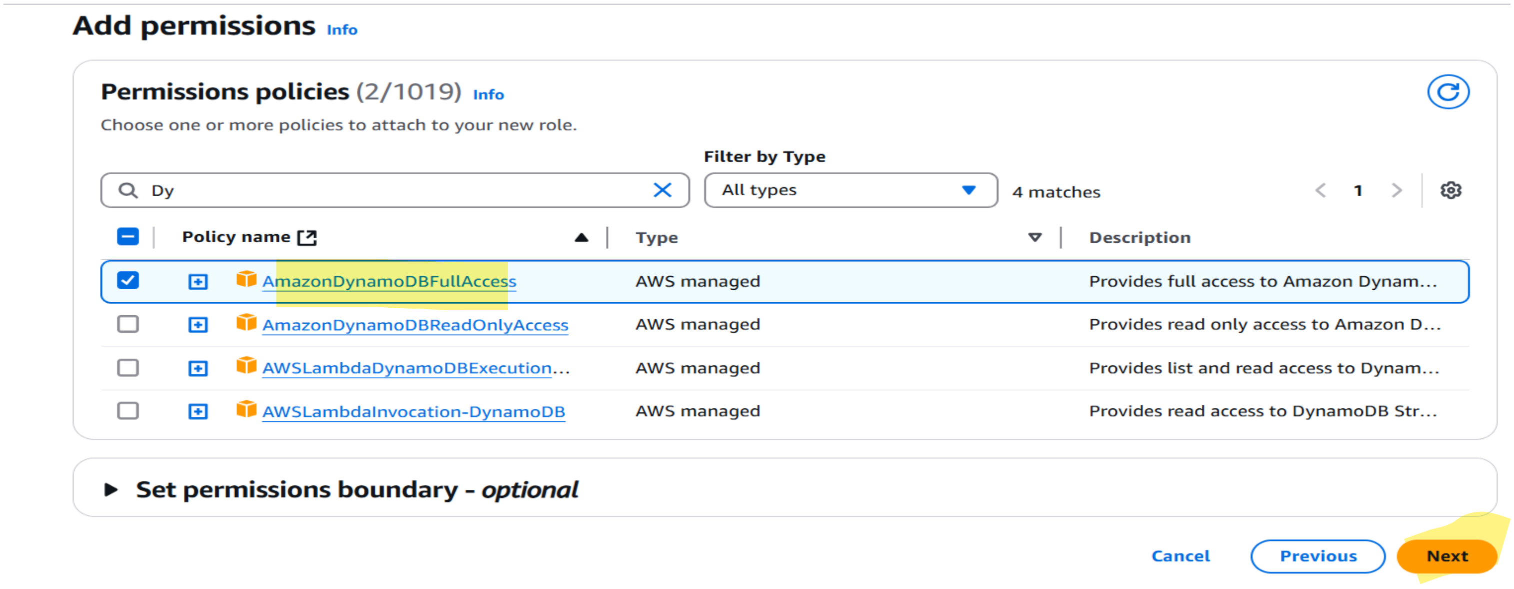
Permissions policies (1/1019) Info

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

Filter by Type

VPC | All types | 14 matches | 1

☐	Policy name	Type	Description
☐	AmazonDMSVPCManagementRole	AWS managed	Provides access to manage VPC setting…
☐	AmazonDRSVPCManagement	AWS managed	Provides access to manage VPC setting…
☐	AmazonECSInfrastructureRolePoli…	AWS managed	Provides access to other AWS service r…
☐	AmazonEKSVPCResourceController	AWS managed	Policy used by VPC Resource Controlle…
☐	AmazonVPCCrossAccountNetworkI…	AWS managed	Provides access to create network inte…
☑	AmazonVPCFullAccess	AWS managed	Provides full access to Amazon VPC via…



Add permissions Info

Permissions policies (2/1019) Info

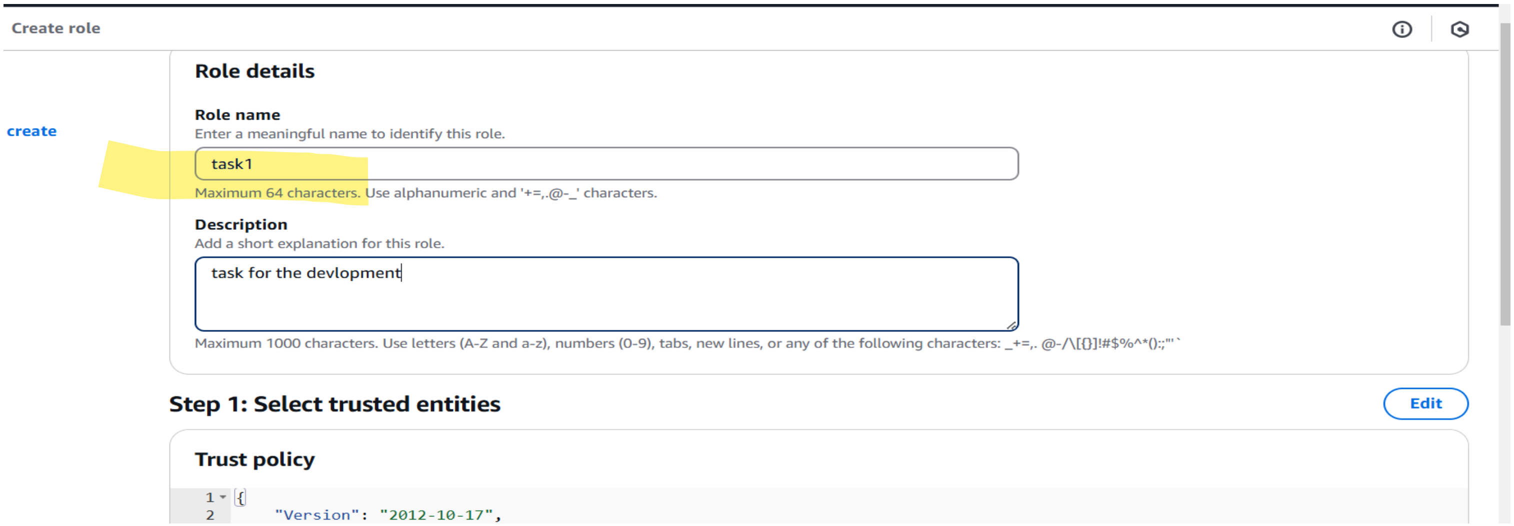
Choose one or more policies to attach to your new role.

Filter by Type

Dy | All types | 4 matches

☐		Policy name	Type	Description
☑	⊞	AmazonDynamoDBFullAccess	AWS managed	Provides full access to Amazon Dynam…
☐	⊞	AmazonDynamoDBReadOnlyAccess	AWS managed	Provides read only access to Amazon D…
☐	⊞	AWSLambdaDynamoDBExecution…	AWS managed	Provides list and read access to Dynam…
☐	⊞	AWSLambdaInvocation-DynamoDB	AWS managed	Provides read access to DynamoDB Str…

▶ **Set permissions boundary - *optional***



Role details

Role name
Enter a meaningful name to identify this role.

task1

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

Description
Add a short explanation for this role.

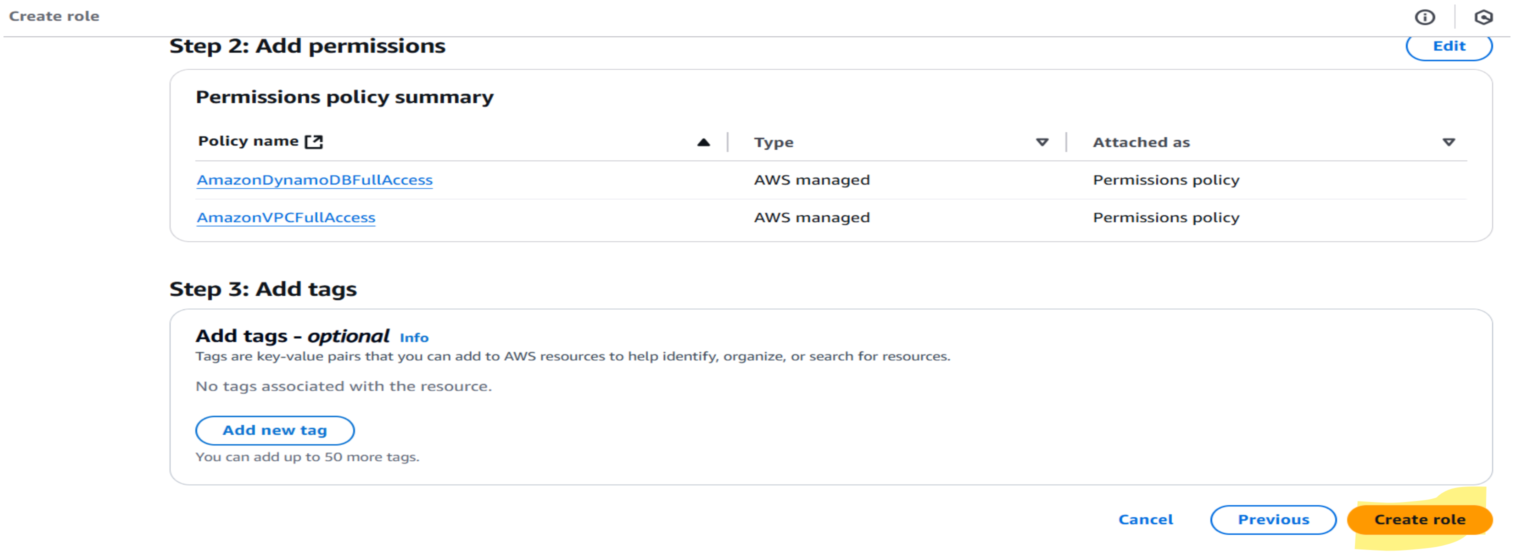
task for the devlopment

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",
```



Step 2: Add permissions

Permissions policy summary

Policy name	Type	Attached as
AmazonDynamoDBFullAccess	AWS managed	Permissions policy
AmazonVPCFullAccess	AWS managed	Permissions policy

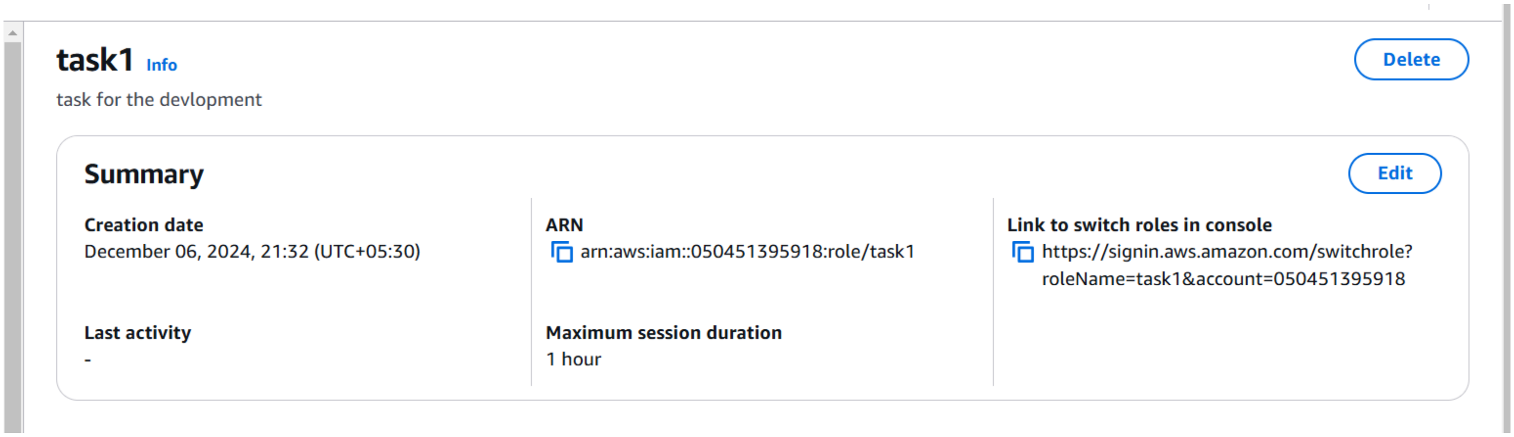
Step 3: Add tags

Add tags - *optional* Info

Tags are key-value pairs that you can add to AWS resources to help identify, organize, or search for resources.

No tags associated with the resource.

You can add up to 50 more tags.



task1 Info

task for the devlopment

Summary

Creation date
December 06, 2024, 21:32 (UTC+05:30)

ARN
arn:aws:iam::050451395918:role/task1

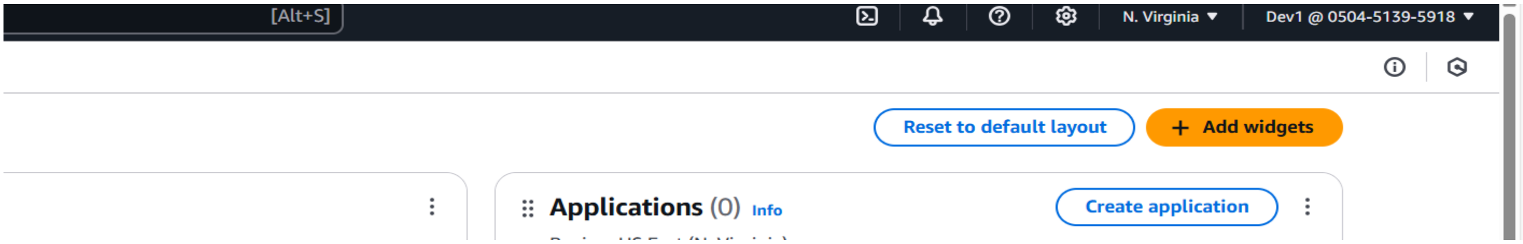
Link to switch roles in console
https://signin.aws.amazon.com/switchrole?roleName=task1&account=050451395918

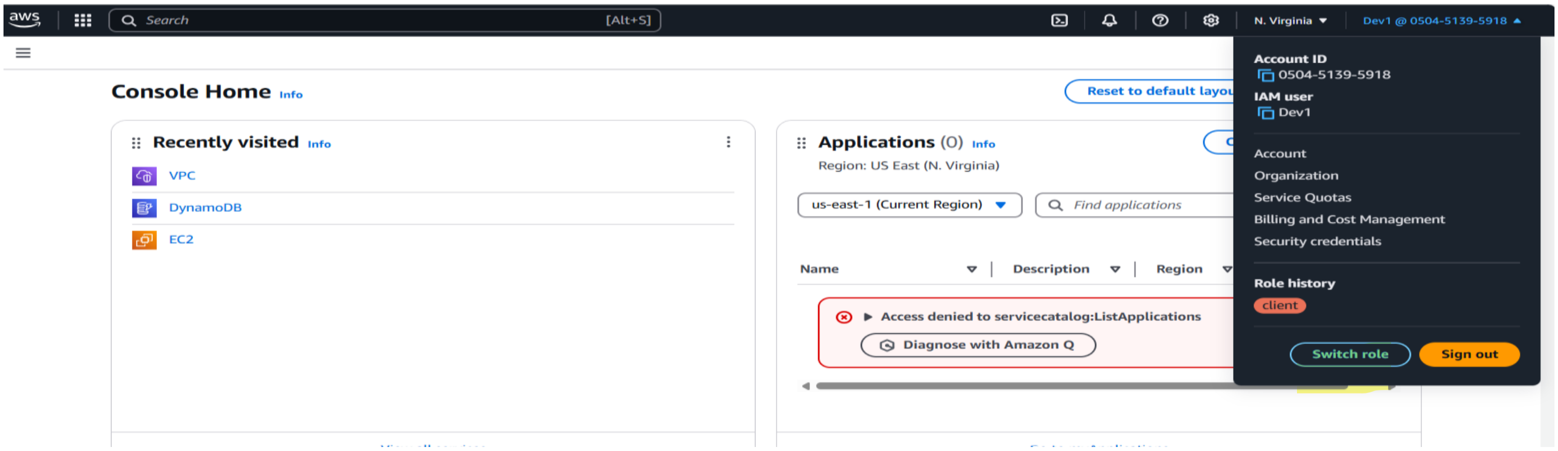
Last activity
-

Maximum session duration
1 hour

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

- Login to Dev1 user and check it .





Console Home Info

Recently visited Info
VPC
DynamoDB
EC2

Applications (0) Info
Region: US East (N. Virginia)

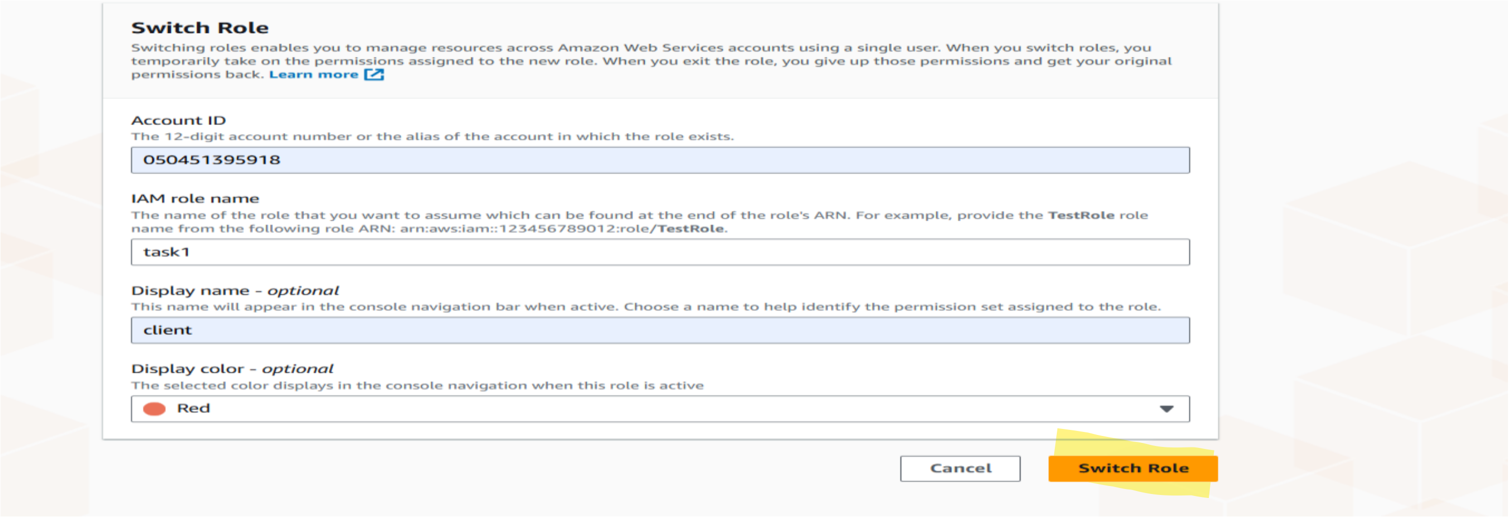
us-east-1 (Current Region)

Name | Description | Region

Access denied to servicecatalog:ListApplications

Account ID
0504-5139-5918
IAM user
Dev1

Role history
client



Switch Role

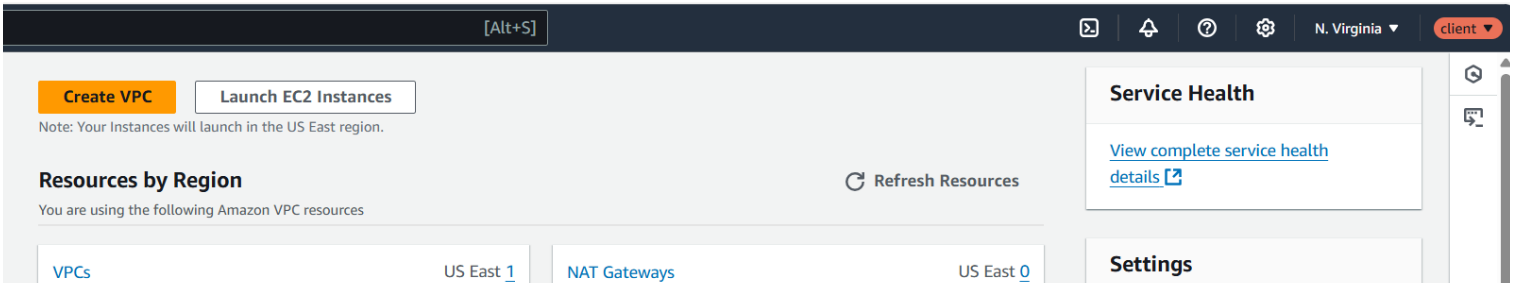
Switching roles enables you to manage resources across Amazon Web Services accounts using a single user. When you switch roles, you temporarily take on the permissions assigned to the new role. When you exit the role, you give up those permissions and get your original permissions back. Learn more

Account ID
The 12-digit account number or the alias of the account in which the role exists.
050451395918

IAM role name
The name of the role that you want to assume which can be found at the end of the role's ARN. For example, provide the TestRole role name from the following role ARN: arn:aws:iam::123456789012:role/TestRole.
task1

Display name - *optional*
This name will appear in the console navigation bar when active. Choose a name to help identify the permission set assigned to the role.
client

Display color - *optional*
The selected color displays in the console navigation when this role is active
● Red

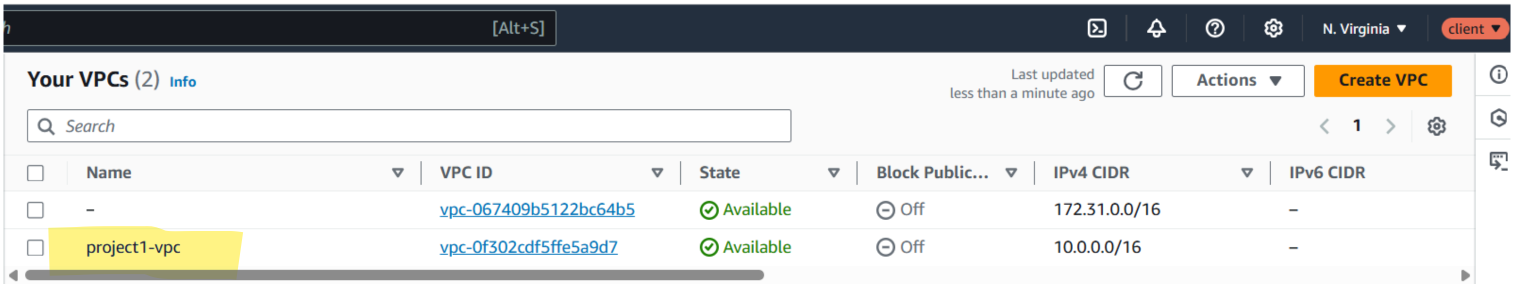


Note: Your Instances will launch in the US East region.

Resources by Region

You are using the following Amazon VPC resources

VPCs	US East 1
NAT Gateways	US East 0



□	Name	VPC ID	State	Block Public...	IPv4 CIDR	IPv6 CIDR
□	–	vpc-067409b5122bc64b5	✓ Available	⊖ Off	172.31.0.0/16	–
□	project1-vpc	vpc-0f302cdf5ffe5a9d7	✓ Available	⊖ Off	10.0.0.0/16	–

-