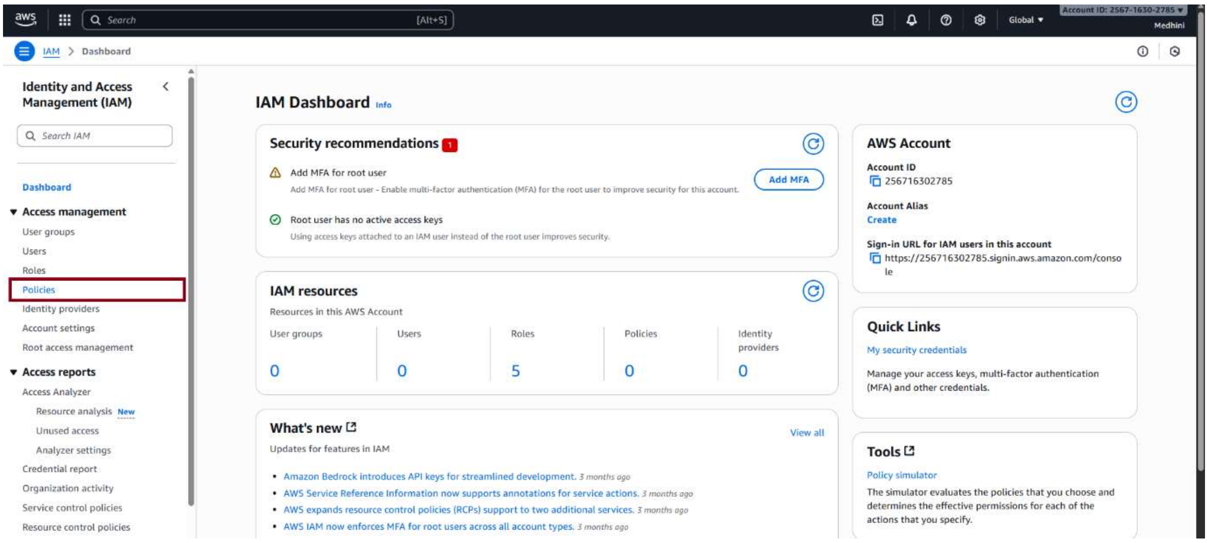
Assignement 2 - IAM User Roles

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

Step 1: Login to your account and search for IAM, then click on **“Policies”** as shown in below picture



IAM Dashboard Info

Security recommendations 1

Add MFA for root user

Add MFA for root user - Enable multi-factor authentication (MFA) for the root user to improve security for this account.

Add MFA

Root user has no active access keys

Using access keys attached to an IAM user instead of the root user improves security.

IAM resources

Resources in this AWS Account

User groups	Users	Roles	Policies	Identity providers
0	0	5	0	0

What's new

Updates for features in IAM

View all

- Amazon Bedrock introduces API keys for streamlined development. 3 months ago
- AWS Service Reference Information now supports annotations for service actions. 3 months ago
- AWS expands resource control policies (RCPs) support to two additional services. 3 months ago
- AWS IAM now enforces MFA for root users across all account types. 3 months ago

AWS Account

Account ID
256716302785

Account Alias
Create

Sign-in URL for IAM users in this account
https://256716302785.signin.aws.amazon.com/console

Quick Links

My security credentials

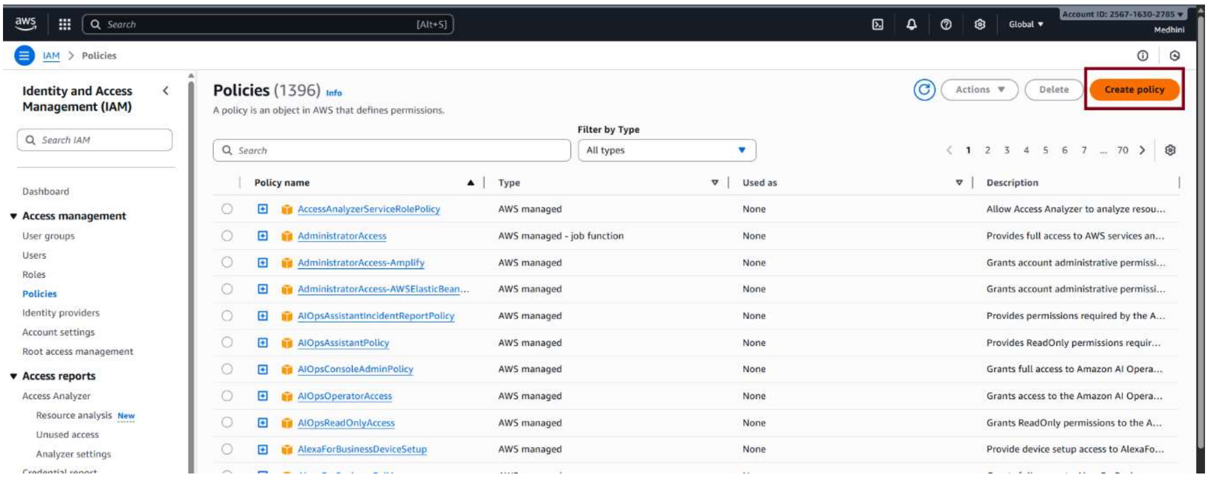
Manage your access keys, multi-factor authentication (MFA) and other credentials.

Tools

Policy simulator

The simulator evaluates the policies that you choose and determines the effective permissions for each of the actions that you specify.

Step 2: To create Policy, click on **“Create Policy”**



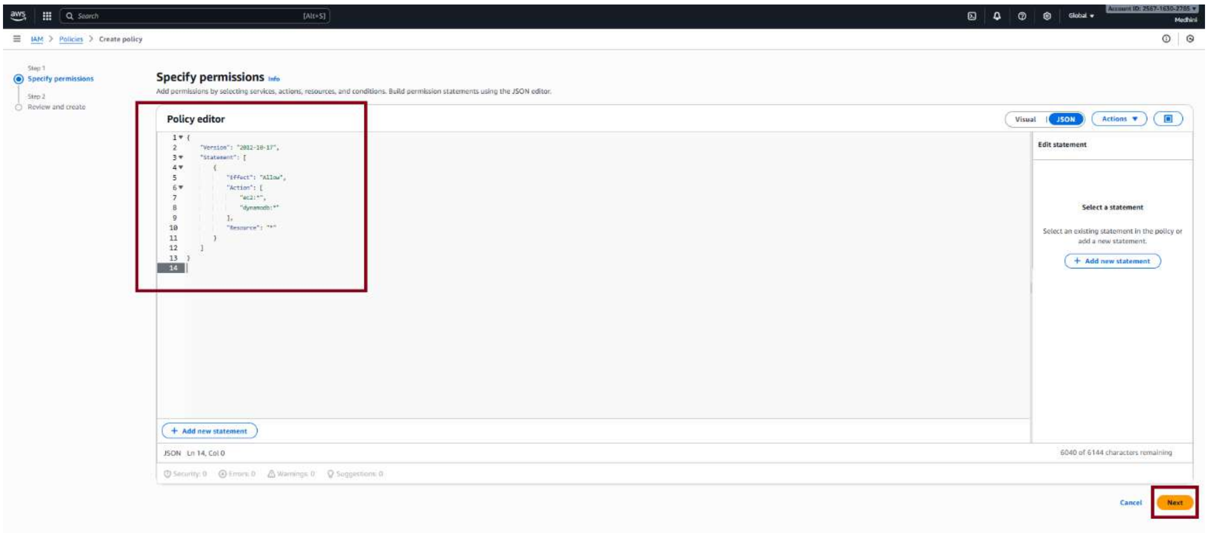
Policies (1396) Info

A policy is an object in AWS that defines permissions.

Filter by Type: All types

Policy name	Type	Used as	Description
AccessAnalyzerServiceRolePolicy	AWS managed	None	Allow Access Analyzer to analyze resou...
AdministratorAccess	AWS managed - job function	None	Provides full access to AWS services an...
AdministratorAccess-Amplify	AWS managed	None	Grants account administrative permissi...
AdministratorAccess-AWSElasticBean...	AWS managed	None	Grants account administrative permissi...
AIOpsAssistantIncidentReportPolicy	AWS managed	None	Provides permissions required by the A...
AIOpsAssistantPolicy	AWS managed	None	Provides ReadOnly permissions requir...
AIOpsConsoleAdminPolicy	AWS managed	None	Grants full access to Amazon AI Opera...
AIOpsOperatorAccess	AWS managed	None	Grants access to the Amazon AI Opera...
AIOpsReadOnlyAccess	AWS managed	None	Grants ReadOnly permissions to the A...
AlexaForBusinessDeviceSetup	AWS managed	None	Provide device setup access to AlexaFo...

Step 3: Paste the below mentioned code and click on “Next”



Specify permissions Info

Add permissions by selecting services, actions, resources, and conditions. Build permission statements using the JSON editor.

Policy editor

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "ec2:*",
                "dynamodb:*"
            ],
            "Resource": "*"
        }
    ]
}
```

Select a statement

Select an existing statement in the policy or add a new statement.

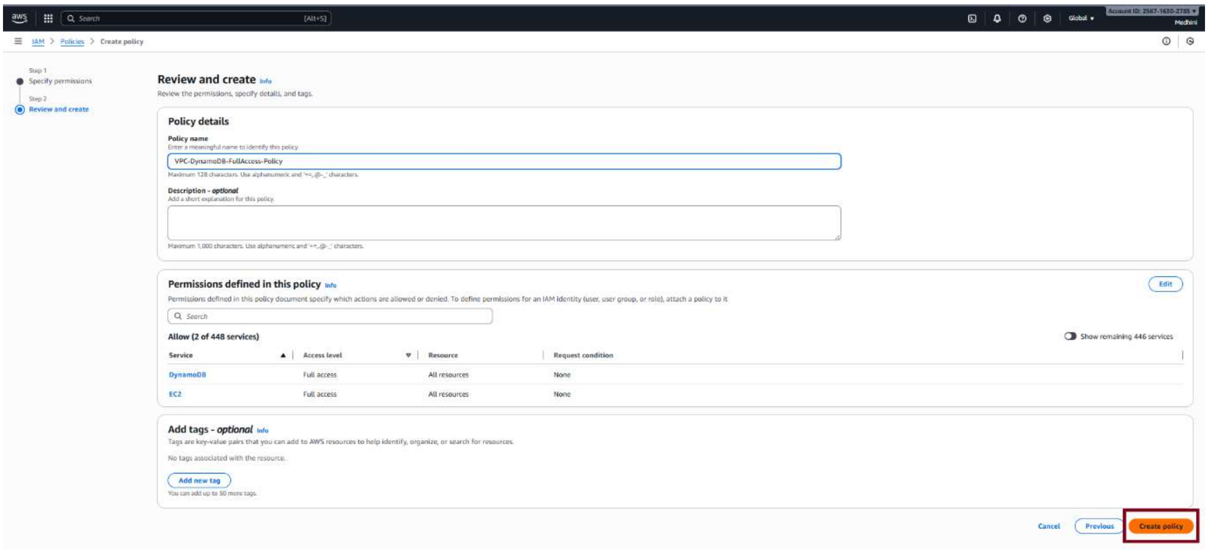
JSON Ln 14, Col 0

6040 of 6144 characters remaining

Security: 0 Errors: 0 Warnings: 0 Suggestions: 0

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "ec2:*",
        "dynamodb:*"
      ],
      "Resource": "*"
    }
  ]
}
```

Step 4: Give a name and click on **“Create Policy”**



IAM > Policies > Create policy

Step 1
Specify permissions
Step 2
Review and create

Review and create Info
Review the permissions, specify details, and tags.

Policy details

Policy name
Enter a meaningful name to identify this policy
VPC-DynamoDB-FullAccess-Policy
Maximum 128 characters. Use alphanumeric and '+=,.@-_' characters.

Description - *optional*
Add a short explanation for this policy.
Maximum 1,000 characters. Use alphanumeric and '+=,.@-_' characters.

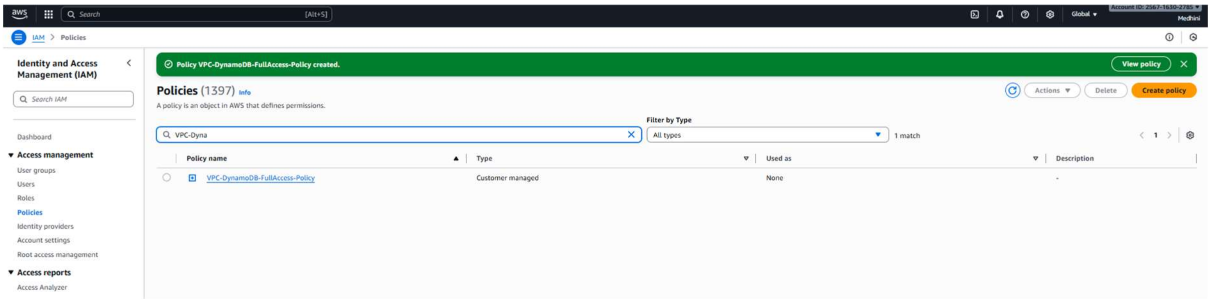
Permissions defined in this policy Info
Permissions defined in this policy document specify which actions are allowed or denied. To define permissions for an IAM identity (user, user group, or role), attach a policy to it

Allow (2 of 448 services)
Show remaining 446 services

Service	Access level	Resource	Request condition
DynamoDB	Full access	All resources	None
EC2	Full access	All resources	None

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.
Add new tag
You can add up to 50 more tags.

Step 5: The Policy is create as shown in below picture



IAM > Policies

Policy VPC-DynamoDB-FullAccess-Policy created.

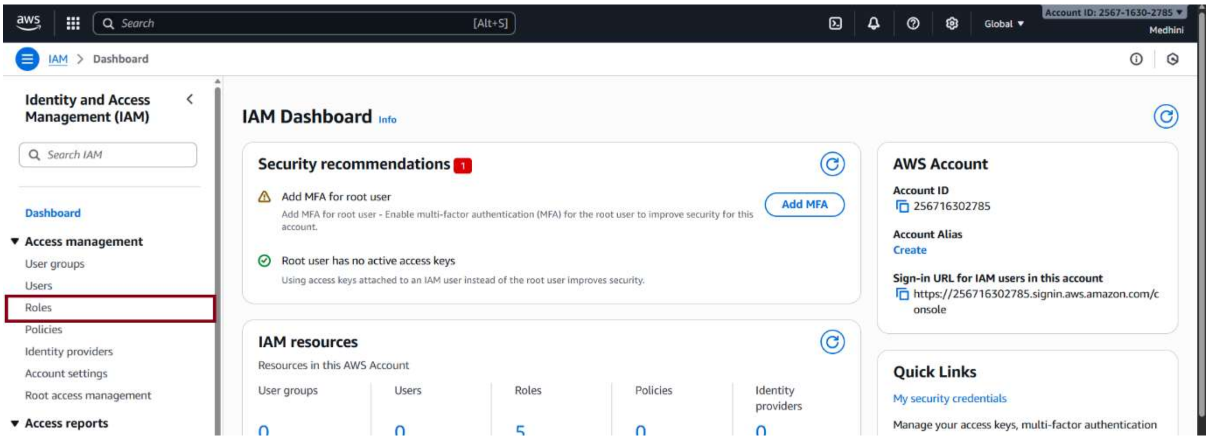
Policies (1397) Info
A policy is an object in AWS that defines permissions.

Filter by Type: All types
VPC-Dyna
1 match

Policy name	Type	Used as	Description
VPC-DynamoDB-FullAccess-Policy	Customer managed	None	-

Create Roles

Step 1: Click on **“Roles”** in the **IAM Dashboard** as shown in below picture



IAM > Dashboard

IAM Dashboard Info

Security recommendations 1

Add MFA for root user
Add MFA for root user - Enable multi-factor authentication (MFA) for the root user to improve security for this account.

Root user has no active access keys
Using access keys attached to an IAM user instead of the root user improves security.

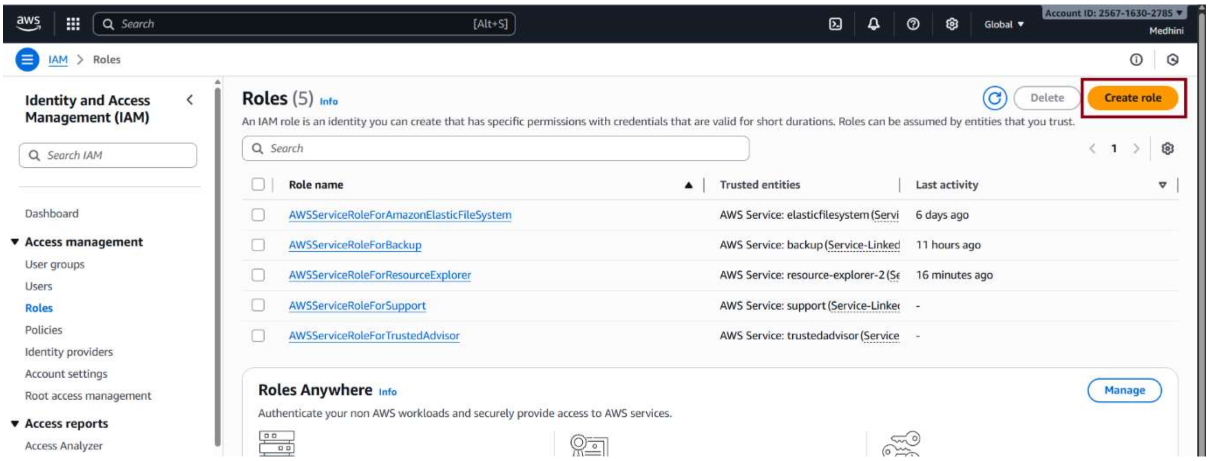
IAM resources
Resources in this AWS Account

User groups	Users	Roles	Policies	Identity providers
0	0	5	0	0

AWS Account
Account ID
256716302785
Account Alias
Create
Sign-in URL for IAM users in this account
https://256716302785.signin.aws.amazon.com/console

Quick Links
My security credentials
Manage your access keys, multi-factor authentication

Step 2: Click on **“Create Role”**



Identity and Access Management (IAM)

- Dashboard
- ▾ Access management
  - User groups
  - Users
  - Roles
  - Policies
  - Identity providers
  - Account settings
  - Root access management
- ▾ Access reports
  - Access Analyzer

Roles (5) Info

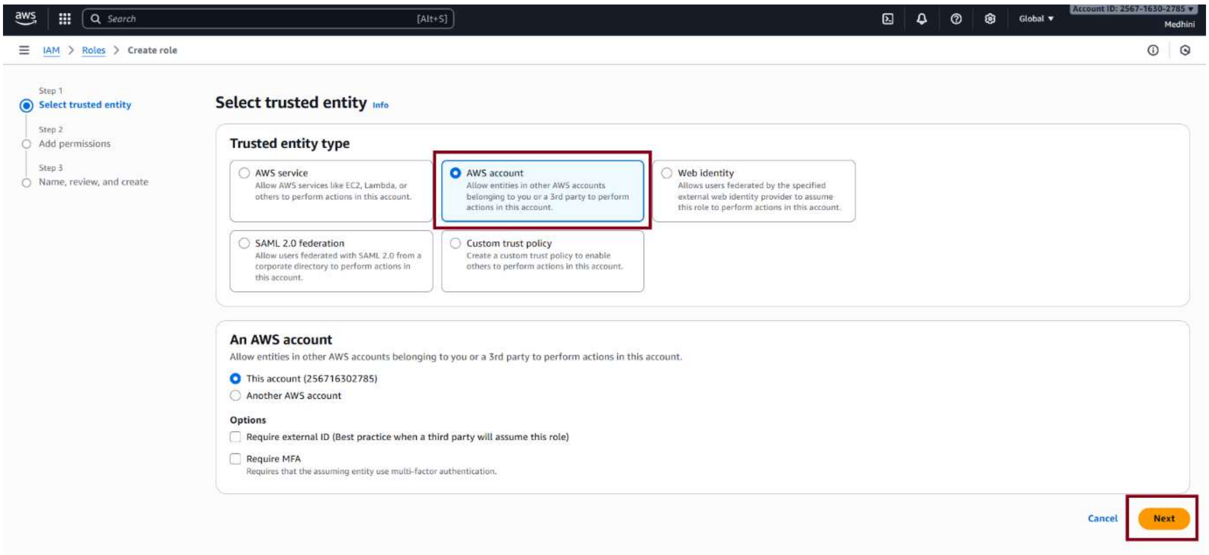
An IAM role is an identity you can create that has specific permissions with credentials that are valid for short durations. Roles can be assumed by entities that you trust.

□	Role name	Trusted entities	Last activity
□	AWSServiceRoleForAmazonElasticFileSystem	AWS Service: elasticfilesystem (Servi	6 days ago
□	AWSServiceRoleForBackup	AWS Service: backup (Service-Linked	11 hours ago
□	AWSServiceRoleForResourceExplorer	AWS Service: resource-explorer-2 (Se	16 minutes 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.

Step 3: Select **“AWS Account”** and click on **“Next”**



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.

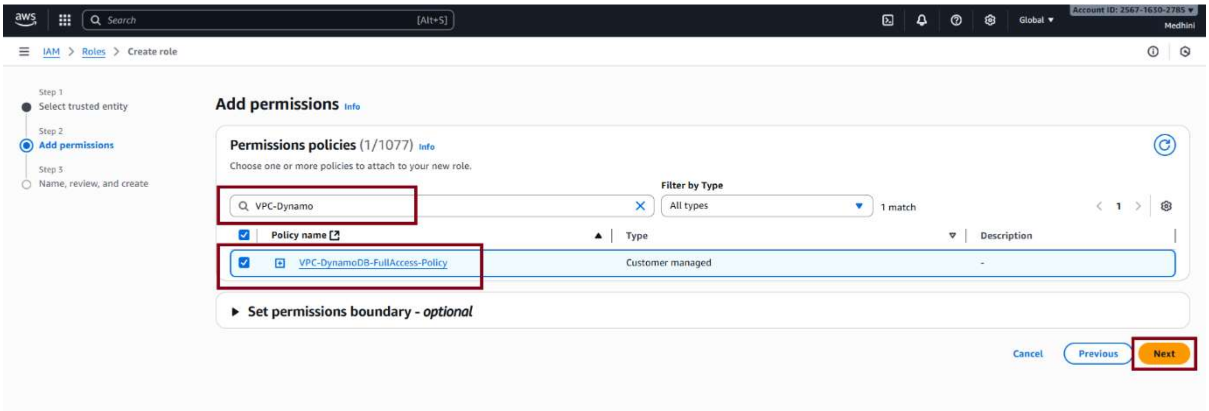
● This account (256716302785)
○ Another AWS account

Options

□ Require external ID (Best practice when a third party will assume this role)

□ Require MFA
Requires that the assuming entity use multi-factor authentication.

Step 4: Search for your policy created, and click on **“Next”**



Step 1
● Select trusted entity

Step 2
● Add permissions

Step 3
○ Name, review, and create

Add permissions Info

Permissions policies (1/1077) Info

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

Search: VPC-Dynamo

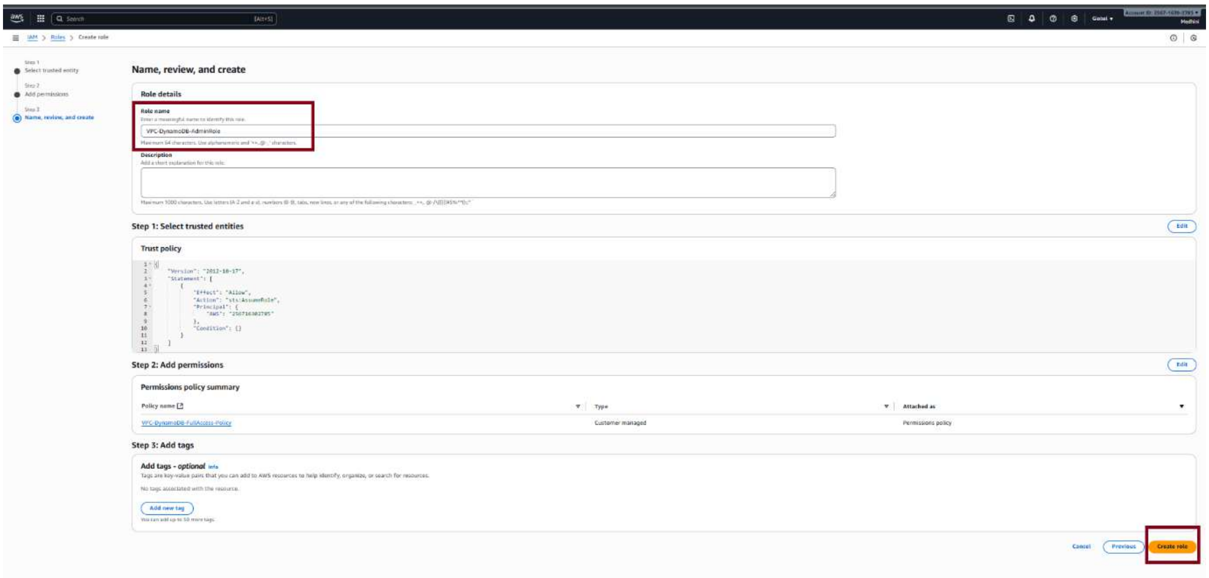
Filter by Type: All types ▾ 1 match

☑	Policy name	Type	Description
☑	⊞ VPC-DynamoDB-FullAccess-Policy	Customer managed	-

▸ Set permissions boundary - *optional*

Assignement 2 - IAM User Roles

Step 5: Give a name and then click on **“Create Role”** as shown in below picture



IAM > Roles > Create role

Step 1 Select trusted entity
Step 2 Add permissions
Step 3 Name, review, and create

Name, review, and create

Role details

Role name: VPC-DynamoDB-AdminRole

Description:

Step 1: Select trusted entities

Trust policy

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": "sts:AssumeRole",
            "Principal": {
                "AWS": "256716302785"
            },
            "Condition": {}
        }
    ]
}
```

Step 2: Add permissions

Permissions policy summary

Policy name	Type	Attached as
VPC-DynamoDB-FullAccess-Policy	Customer managed	Permissions policy

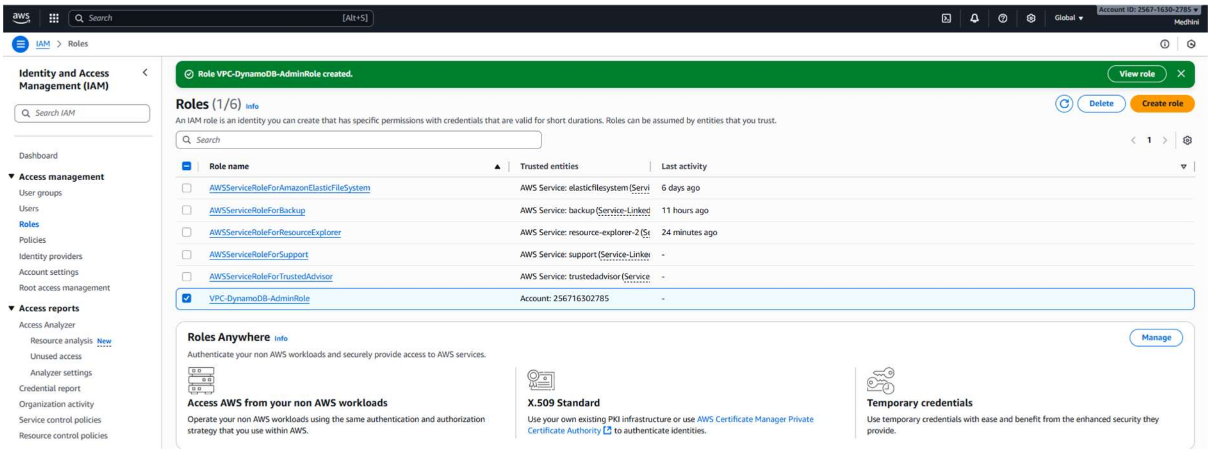
Step 3: Add tags

Add tags - *optional*

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.

Role has been created



IAM > Roles

Role VPC-DynamoDB-AdminRole created.

Roles (1/6)

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
☐	AWSServiceRoleForAmazonElasticFileSystem	AWS Service: elasticfilesystem (Servi	6 days ago
☐	AWSServiceRoleForBackup	AWS Service: backup (Service-Linked	11 hours ago
☐	AWSServiceRoleForResourceExplorer	AWS Service: resource-explorer-2 (Se	24 minutes ago
☐	AWSServiceRoleForSupport	AWS Service: support (Service-Linke	-
☐	AWSServiceRoleForTrustedAdvisor	AWS Service: trustedadvisor (Service	-
☑	VPC-DynamoDB-AdminRole	Account: 256716302785	-

Roles Anywhere

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

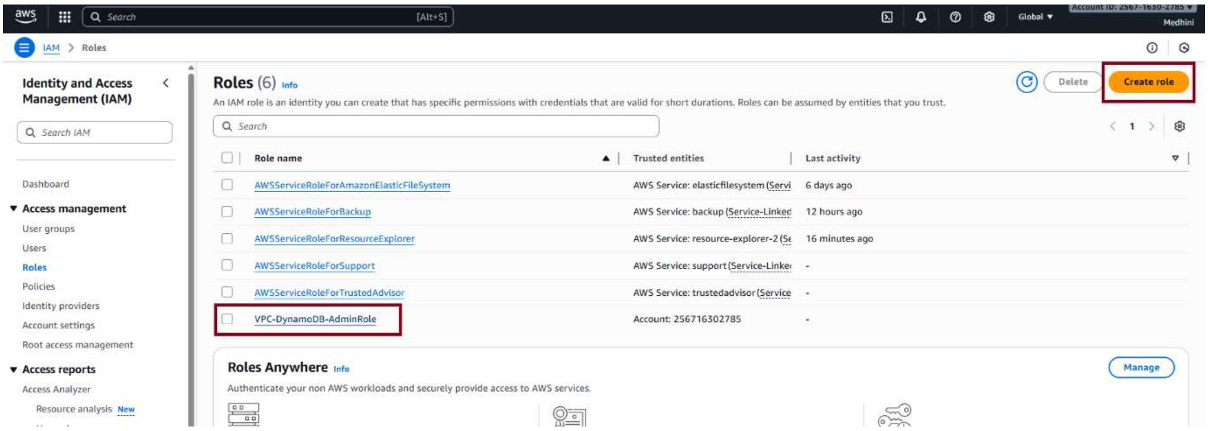
Access AWS from your non AWS workloads
Operate your non AWS workloads using the same authentication and authorization strategy that you use within AWS.

X.509 Standard
Use your own existing PKI infrastructure or use AWS Certificate Manager Private Certificate Authority to authenticate identities.

Temporary credentials
Use temporary credentials with ease and benefit from the enhanced security they provide.

Assign User 1 and User 2 to created Role

Step 1: Go to User Role, and click on User Role you have created



Roles (6) Info

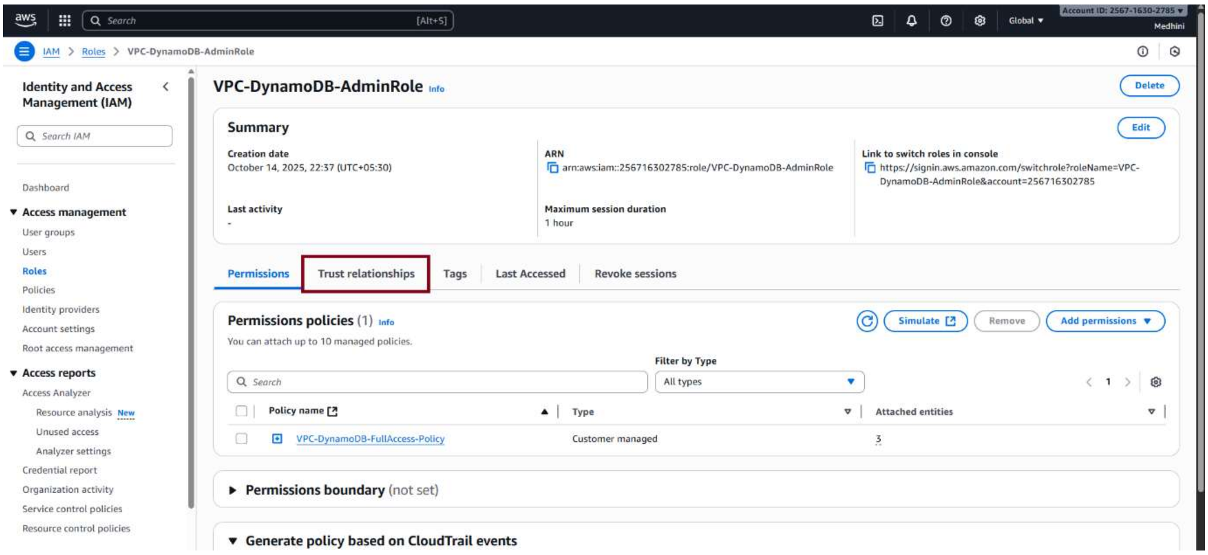
An IAM role is an identity you can create that has specific permissions with credentials that are valid for short durations. Roles can be assumed by entities that you trust.

	Role name	Trusted entities	Last activity
□	AWSServiceRoleForAmazonElasticFileSystem	AWS Service: elasticfilesystem (Servi	6 days ago
□	AWSServiceRoleForBackup	AWS Service: backup (Service-Linked	12 hours ago
□	AWSServiceRoleForResourceExplorer	AWS Service: resource-explorer-2 (Se	16 minutes ago
□	AWSServiceRoleForSupport	AWS Service: support (Service-Linke	-
□	AWSServiceRoleForTrustedAdvisor	AWS Service: trustedadvisor (Service	-
□	VPC-DynamoDB-AdminRole	Account: 256716302785	-

Roles Anywhere Info

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

Step 2: Click on **"Trust Policy"**



VPC-DynamoDB-AdminRole Info

Summary

Creation date
October 14, 2025, 22:37 (UTC+05:30)

ARN
arn:aws:iam::256716302785:role/VPC-DynamoDB-AdminRole

Link to switch roles in console
https://signin.aws.amazon.com/switchrole?roleName=VPC-DynamoDB-AdminRole&account=256716302785

Last activity
-

Maximum session duration
1 hour

Permissions policies (1) Info

You can attach up to 10 managed policies.

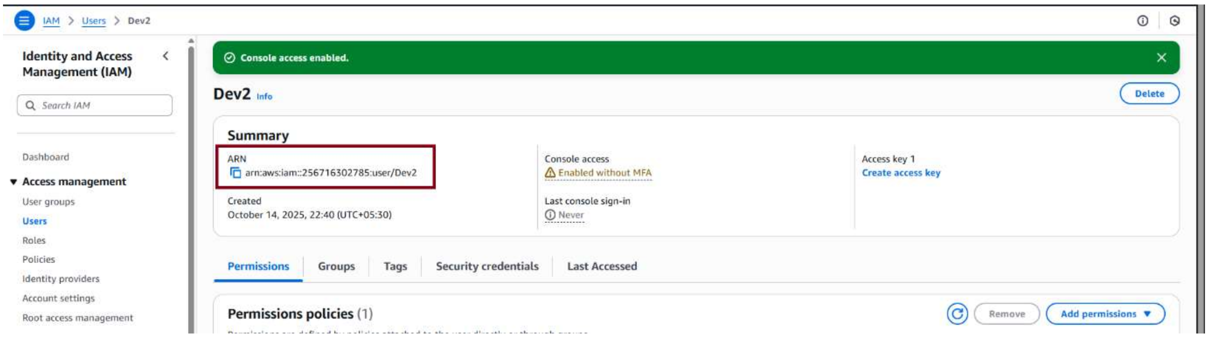
Filter by Type: All types

	Policy name	Type	Attached entities
□	VPC-DynamoDB-FullAccess-Policy	Customer managed	3

▸ Permissions boundary (not set)

▾ Generate policy based on CloudTrail events

Step 3: From your user dashboard, copy the mentioned ARN



Console access enabled.

Dev2 Info

Summary

ARN
arn:aws:iam::256716302785:user/Dev2

Created
October 14, 2025, 22:40 (UTC+05:30)

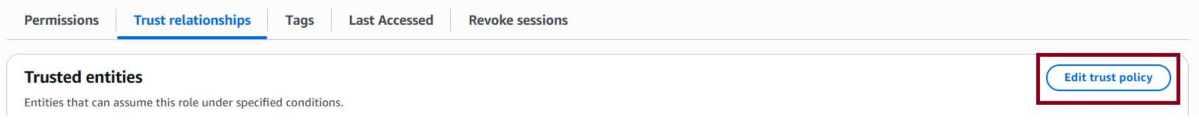
Console access
Enabled without MFA

Last console sign-in
Never

Access key 1
Create access key

Permissions policies (1)

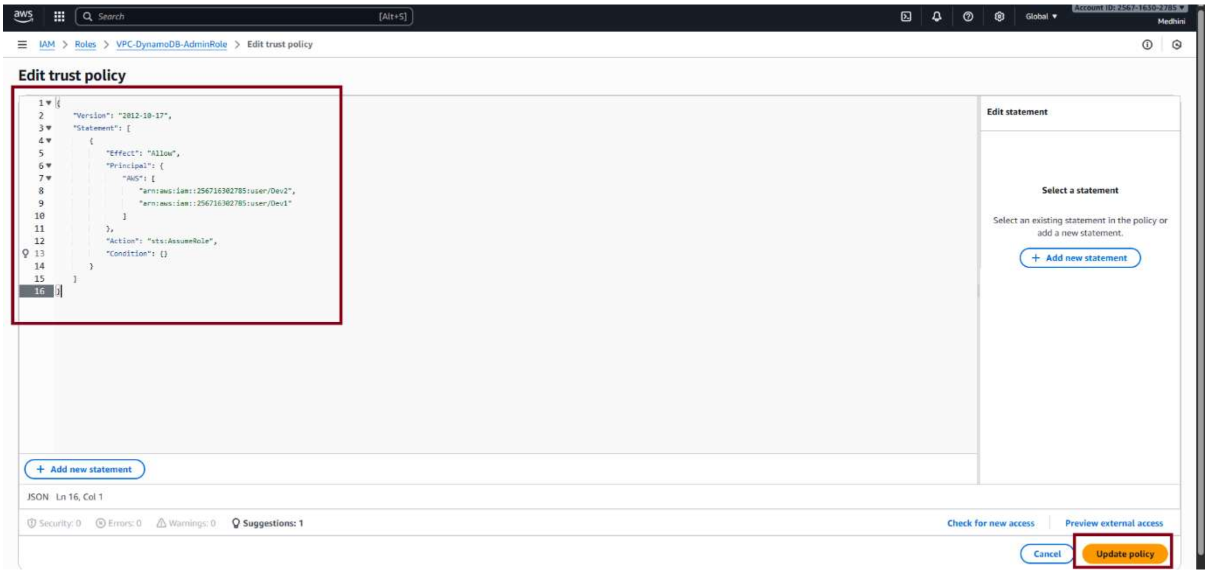
Step 4: Click on **"Edit Trust Policy"**



Trusted entities

Entities that can assume this role under specified conditions.

Step 5: Add the mentioned code and click on **“Update Policy”**

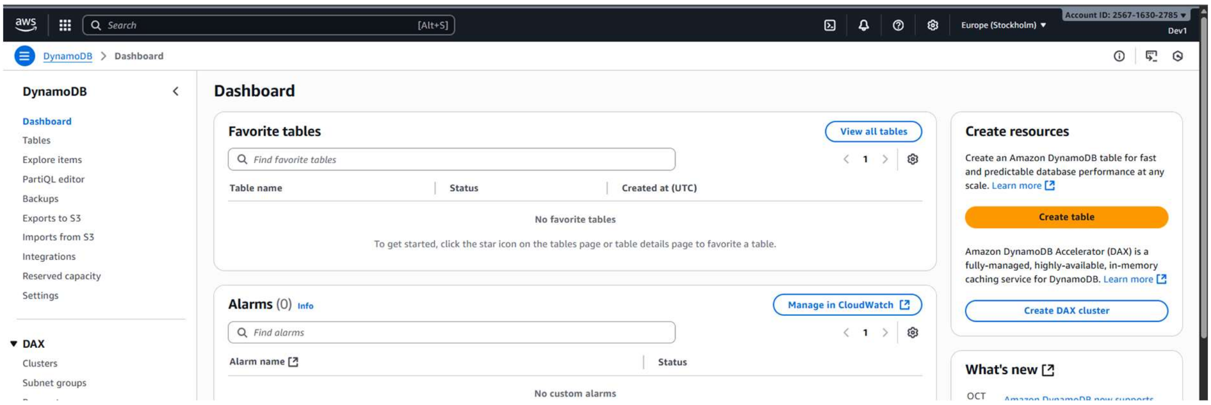


```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Principal": {
                "AWS": [
                    "arn:aws:iam::256716302785:user/Dev2",
                    "arn:aws:iam::256716302785:user/Dev1"
                ]
            },
            "Action": "sts:AssumeRole",
            "Condition": {}
        }
    ]
}
```

```
{
        "Version": "2012-10-17",
        "Statement": [
                {
                        "Effect": "Allow",
                        "Principal": {
                                "AWS": [
                                        "arn:aws:iam::256716302785:user/Dev2",
                                        "arn:aws:iam::256716302785:user/Dev1"
                                ]
                        },
                        "Action": "sts:AssumeRole",
                        "Condition": {}
                }
        ]
}
```

Assignement 2 - IAM User Roles

Step 6: Login as a Dev1 user and check the permission, EC2 is allowed to use and DynamoDB



No favorite tables

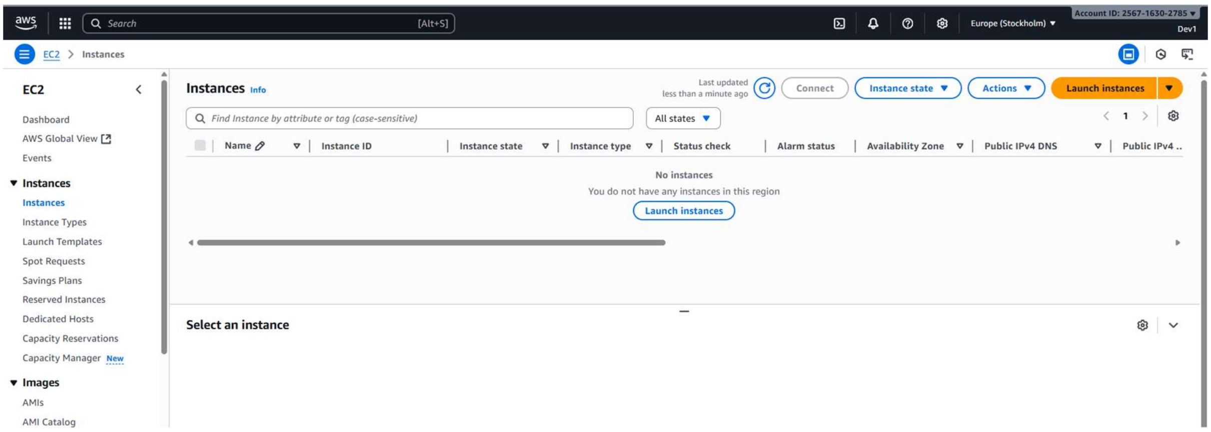
To get started, click the star icon on the tables page or table details page to favorite a table.

No custom alarms

Create an Amazon DynamoDB table for fast and predictable database performance at any scale. Learn more

Amazon DynamoDB Accelerator (DAX) is a fully-managed, highly-available, in-memory caching service for DynamoDB. Learn more

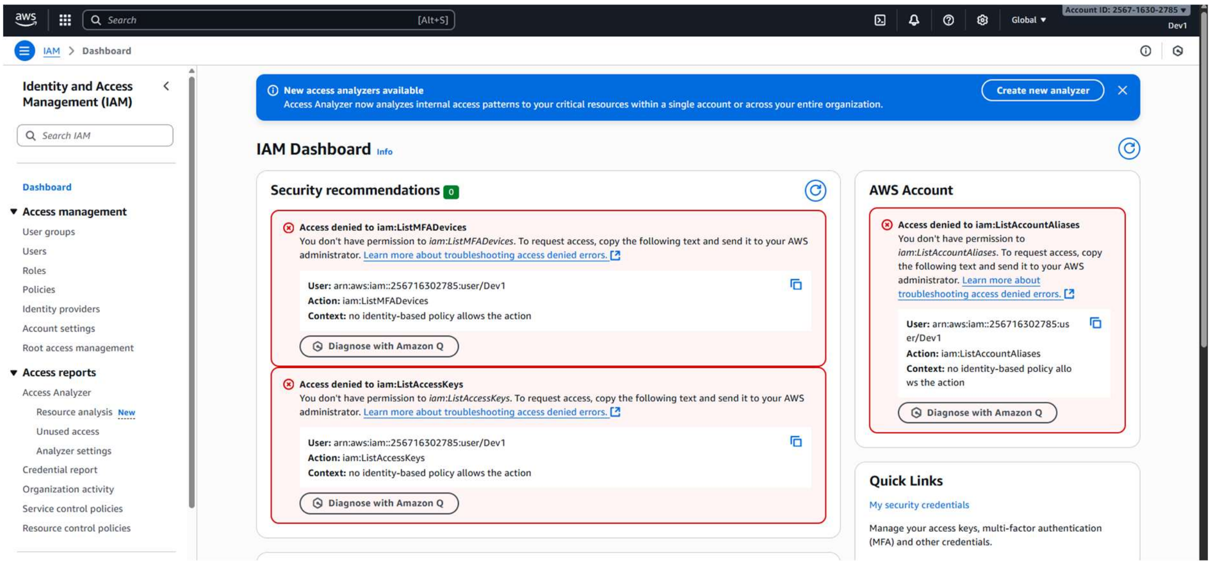
Check EC2 and DynamoDB



No instances

You do not have any instances in this region

For any other Applications permission is not given to Dev1 user



New access analyzers available
Access Analyzer now analyzes internal access patterns to your critical resources within a single account or across your entire organization.

Access denied to iam:ListMFADevices
You don't have permission to *iam:ListMFADevices*. To request access, copy the following text and send it to your AWS administrator. Learn more about troubleshooting access denied errors.

User: arn:aws:iam::256716302785:user/Dev1
Action: iam:ListMFADevices
Context: no identity-based policy allows the action

Access denied to iam:ListAccessKeys
You don't have permission to *iam:ListAccessKeys*. To request access, copy the following text and send it to your AWS administrator. Learn more about troubleshooting access denied errors.

User: arn:aws:iam::256716302785:user/Dev1
Action: iam:ListAccessKeys
Context: no identity-based policy allows the action

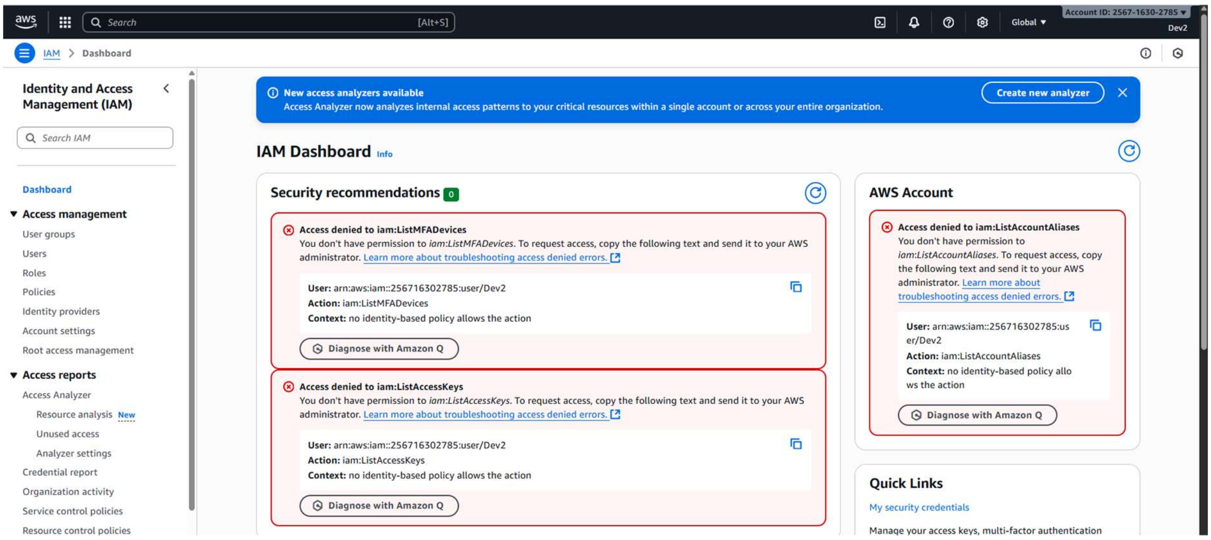
Access denied to iam:ListAccountAliases
You don't have permission to *iam:ListAccountAliases*. To request access, copy the following text and send it to your AWS administrator. Learn more about troubleshooting access denied errors.

User: arn:aws:iam::256716302785:us er/Dev1
Action: iam:ListAccountAliases
Context: no identity-based policy allo ws the action

Manage your access keys, multi-factor authentication (MFA) and other credentials.

Assignement 2 - IAM User Roles

This will be same to Dev2 user as well



Identity and Access Management (IAM)

New access analyzers available
Access Analyzer now analyzes internal access patterns to your critical resources within a single account or across your entire organization.

IAM Dashboard Info

Security recommendations 0

Access denied to iam:ListMFADevices
You don't have permission to *iam:ListMFADevices*. To request access, copy the following text and send it to your AWS administrator. Learn more about troubleshooting access denied errors.

User: arn:aws:iam::256716302785:user/Dev2
Action: iam:ListMFADevices
Context: no identity-based policy allows the action

Access denied to iam:ListAccessKeys
You don't have permission to *iam:ListAccessKeys*. To request access, copy the following text and send it to your AWS administrator. Learn more about troubleshooting access denied errors.

User: arn:aws:iam::256716302785:user/Dev2
Action: iam:ListAccessKeys
Context: no identity-based policy allows the action

AWS Account

Access denied to iam:ListAccountAliases
You don't have permission to *iam:ListAccountAliases*. To request access, copy the following text and send it to your AWS administrator. Learn more about troubleshooting access denied errors.

User: arn:aws:iam::256716302785:us
er/Dev2
Action: iam:ListAccountAliases
Context: no identity-based policy allo
ws the action

Quick Links

My security credentials

Manage your access keys, multi-factor authentication