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

Answer:

Allow full Access to DynamoDB and VPC.
Create a role which allows Users Dev1 and Dev2

```
   3 ▾        "Statement": [
   4 ▾            {
   5                  "Effect": "Allow",
   6                  "Action": "sts:AssumeRole",
   7 ▾                "Principal": {
   8                      "AWS": "601568096541"
   9                  },
  10                  "Condition": {}
  11              }
  12          ]
  13  }
```

Step 2: Add permissions   [Edit]

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.

⊘ Role Role1 created.   [View role]   X

Identity and Access Management (IAM)   X

🔍 Search IAM

Roles (1/5) 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.

[↻] [Delete] [**Create role**]

Dashboard

▼ **Access management**
 User groups
 Users
 Roles
 Policies
 Identity providers
 Account settings

🔍 Rol   X   5 matches   ⟨ 1 ⟩ ⚙

☐	Role name ▲	Trusted entities	Last activity ▽
☐	AWSServiceRoleForAmazonElasticFileSystem	AWS Service: elasticfilesystem (Servi:	5 days ago
☐	AWSServiceRoleForBackup	AWS Service: backup (Service-Linked	8 hours ago
☐	AWSServiceRoleForSupport	AWS Service: support (Service-Linked	-
☐	AWSServiceRoleForTrustedAdvisor	AWS Service: trustedadvisor (Service	-
☑	Role1	Account: 601568096541	-

▼ **Access reports**
 Access analyzer
  Archive rules
  Analyzers
  Settings
 Credential report

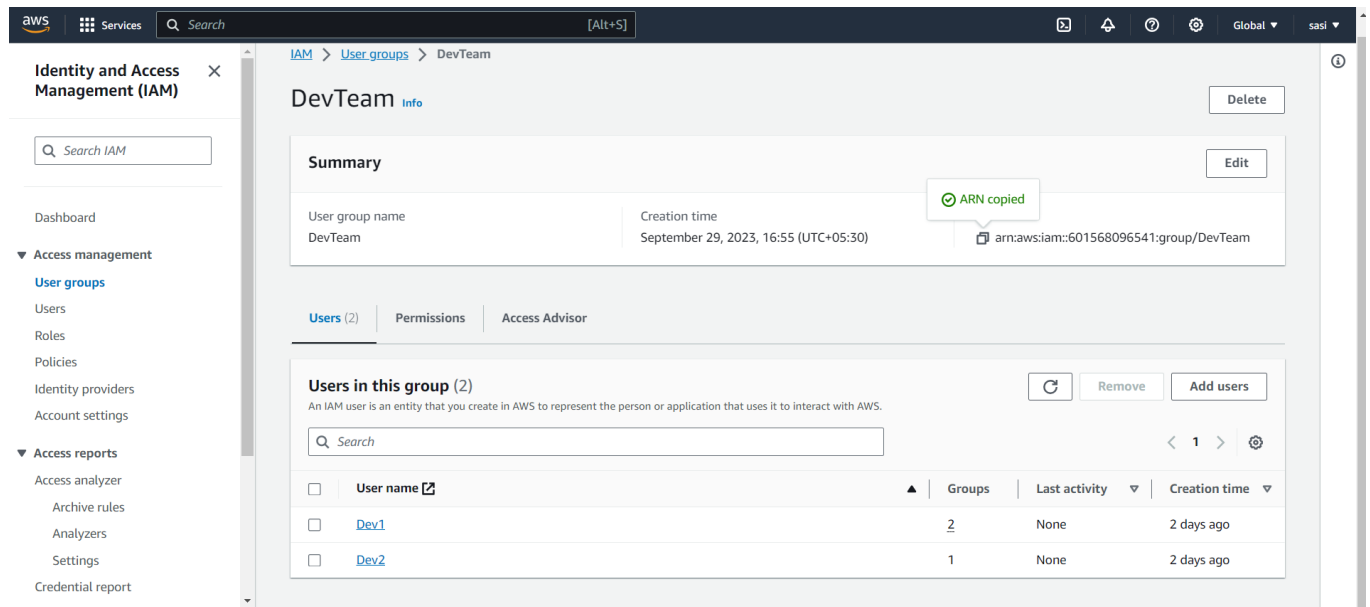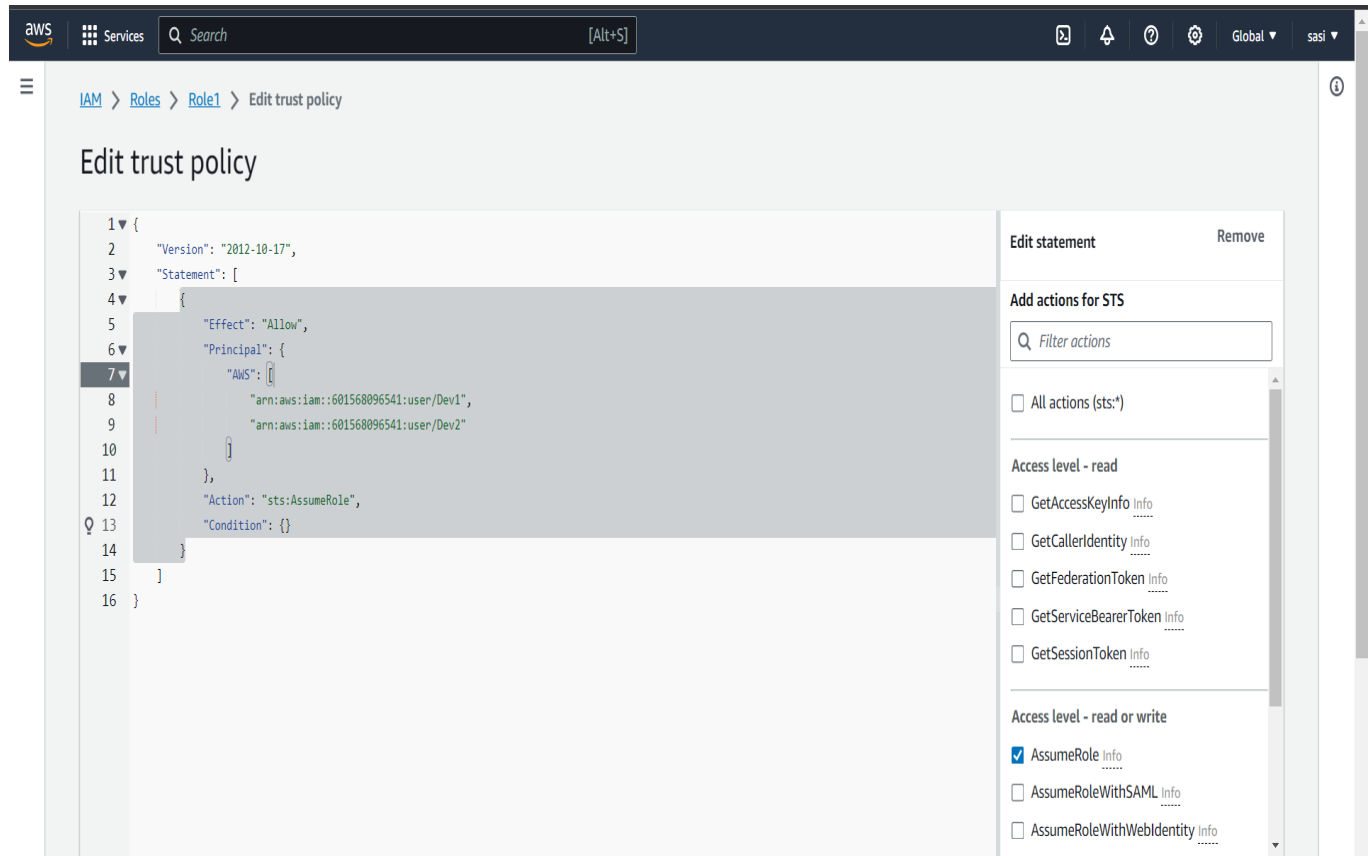**Roles Anywhere** Info   [Manage]

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

Click on the Role column it will open new window on that window go to Edit Trust policy.

There you will find add new principle click on that add the both Dev1 and Dev2 arns

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

Answer :

Click on link to switch it will open new window.

aws

Switch Role

Allows management of resources across Amazon Web Services accounts using a single user ID and password. You can switch roles after an Amazon Web Services administrator has configured a role and given you the account and role details. Learn more.

You cannot switch roles when you are signed in with AWS account credentials.

Account* 601568096541 ⓘ

Role* test ⓘ

Display Name test @ 601568096541 ⓘ

Color a a a a a a

*Required Cancel **Switch Role**

English ▾

Terms of Use Privacy Policy © 1996-2023, Amazon Web Services, Inc. or its affiliates.