

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

Answer:

The screenshot shows the AWS IAM console 'Add permissions' page. The search filter is 'dyna' and 4 matches are shown. The selected policy is 'AmazonDynamoDBFullAccess'.

Policy name	Type	Description
<input checked="" type="checkbox"/> AmazonDynamoDBFullAccess	AWS managed	Provides full access to Amazon DynamoD...
<input type="checkbox"/> AmazonDynamoDBReadOnlyAccess	AWS managed	Provides read only access to Amazon Dyn...
<input type="checkbox"/> AWSLambdaDynamoDBExecutionRole	AWS managed	Provides list and read access to DynamoD...
<input type="checkbox"/> AWSLambdaInvocation-DynamoDB	AWS managed	Provides read access to DynamoDB Strea...

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

The screenshot shows the AWS IAM console 'Add permissions' page. The search filter is 'VPC' and 13 matches are shown. The selected policy is 'AmazonVPCFullAccess'.

Policy name	Type	Description
<input type="checkbox"/> AmazonDMSVPCManagementRole	AWS managed	Provides access to manage VPC setting...
<input type="checkbox"/> AmazonDRSVPCManagement	AWS managed	Provides access to manage VPC setting...
<input type="checkbox"/> AmazonEKSVPCResourceController	AWS managed	Policy used by VPC Resource Controlle...
<input type="checkbox"/> AmazonVPCCrossAccountNetworkInter...	AWS managed	Provides access to create network inte...
<input checked="" type="checkbox"/> AmazonVPCFullAccess	AWS managed	Provides full access to Amazon VPC via...
<input type="checkbox"/> AmazonVPCNetworkAccessAnalyzerFul...	AWS managed	Provides permissions to describe AWS ...
<input type="checkbox"/> AmazonVPCReachabilityAnalyzerFullAc...	AWS managed	Provides permissions to describe AWS ...
<input type="checkbox"/> AmazonVPCReachabilityAnalyzerPathC...	AWS managed	This policy is attached to the role IAM...

aws

Services

Search

[Alt+S]

Global

sasi

3

4

5

6

7

8

9

10

11

12

13

```
Statement: [{
  "Effect": "Allow",
  "Action": "sts:AssumeRole",
  "Principal": {
    "AWS": "601568096541"
  },
  "Condition": {}
}]
```

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

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.

CloudShell

Feedback

© 2023, Amazon Web Services India Private Limited or its affiliates.

Privacy

Terms

Cookie preferences

aws

Services

Search

[Alt+S]

Global

sasi

Identity and Access Management (IAM)

Search IAM

Dashboard

Access management

- User groups
- Users
- Roles**
- Policies
- Identity providers
- Account settings

Access reports

- Access analyzer
- Archive rules
- Analizers
- Settings
- Credential report

Role Role1 created.

View role

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.

Refresh

Delete

Create role

Q Rol 5 matches

Role name	Trusted entities	Last activity
<input type="checkbox"/> AWSServiceRoleForAmazonElasticFileSystem	AWS Service: elasticfilesystem (Service-Linked)	5 days ago
<input type="checkbox"/> AWSServiceRoleForBackup	AWS Service: backup (Service-Linked)	8 hours ago
<input type="checkbox"/> AWSServiceRoleForSupport	AWS Service: support (Service-Linked)	-
<input type="checkbox"/> AWSServiceRoleForTrustedAdvisor	AWS Service: trustedadvisor (Service-Linked)	-
<input checked="" type="checkbox"/> Role1	Account: 601568096541	-

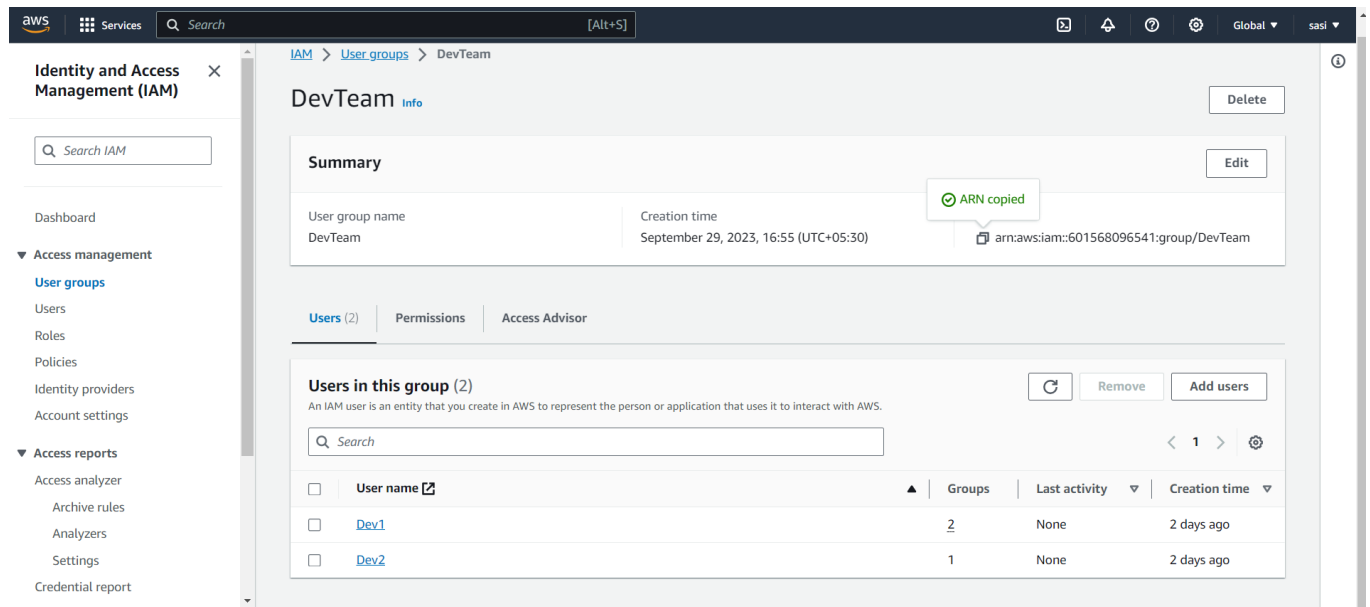
Roles Anywhere

Info

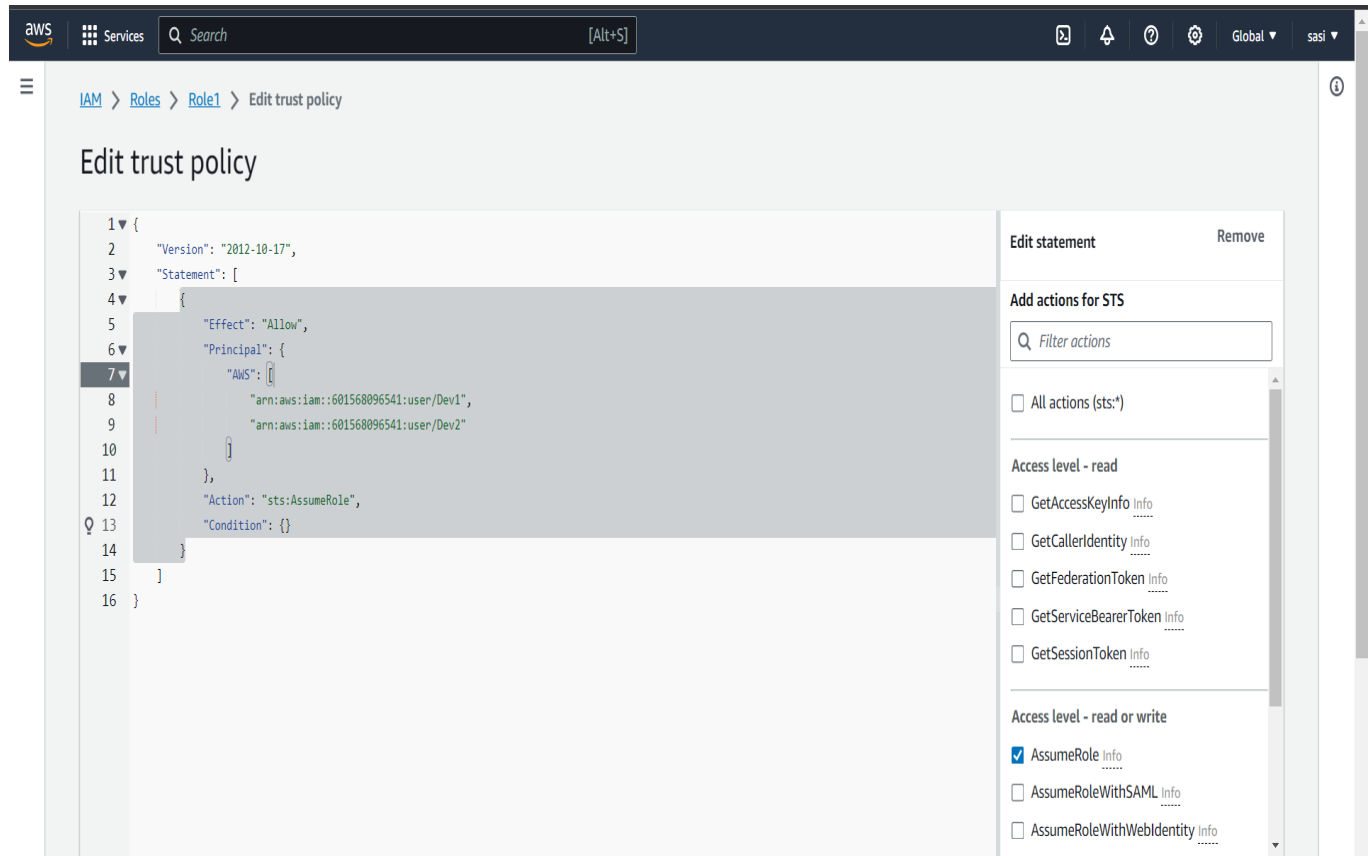
Authenticate your non AWS workloads and securely provide access to AWS services.

Manage

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 :


The screenshot shows the AWS IAM console interface. On the left is a navigation menu with sections like 'Identity and Access Management (IAM)', 'Access management', and 'Access reports'. The main content area displays the details for 'Role1', which has 'full access VPC and DynamoDB' permissions. The 'Summary' tab is active, showing the creation date (October 01, 2023, 22:27 UTC+05:30), the ARN (arn:aws:iam::601568096541:role/Role1), and the maximum session duration (1 hour). A link to switch roles is provided: <https://signin.aws.amazon.com/switchrole?roleName=Role1&account=601568096541>. Below the summary, the 'Trust relationships' tab is selected, showing a list of trusted entities with a JSON policy snippet.

Click on link to switch it will open new window.


The screenshot shows the 'Switch role' page in the AWS console. It features a 'Switch Role' button and a section titled 'Get started in 3 simple steps'. The steps are: 1. Create role: Before you can switch roles, an administrator must create the role in the account you want to switch to, and then grant it permissions to perform the task you want. 2. Role access: Your administrator provides you with the account ID or alias and the role name to use. 3. Switch roles: Click your user name in the navigation bar, then select Switch Role. Enter the account and role information provided by your administrator. You immediately begin using the permissions associated with the new role. Exit the role to resume using your previous permissions. At the bottom, there are links to learn more: 'Learn how to create an IAM role', 'Learn how to find the account ID or alias', and 'Learn how to switch roles in the console'.

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.](#)


Account*



Role*



Display Name



Color

a

a

a

a

a

a

Color

Switch Role