

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.



Services

Search

[Option+S]



Global

rsujithsri16@gmail.com



IAM > Roles > Create role

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.

Use case

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

Service or use case



Service or use case

EC2

Choose a use case for the specified service.

Use case

☒ EC2

Allows EC2 instances to call AWS services on your behalf.

☐ EC2 Role for AWS Systems Manager

Allows EC2 instances to call AWS services like CloudWatch and Systems Manager on your behalf.

☐ EC2 Spot Fleet Role

Allows EC2 Spot Fleet to request and terminate Spot Instances on your behalf.

☐ EC2 - Spot Fleet Auto Scaling

Allows Auto Scaling to access and update EC2 spot fleets on your behalf.

☐ EC2 - Spot Fleet Tagging

Allows EC2 to launch spot instances and attach tags to the launched instances on your behalf.

☐ EC2 - Spot Instances

Allows EC2 Spot Instances to launch and manage spot instances on your behalf.

☐ EC2 - Spot Fleet

Allows EC2 Spot Fleet to launch and manage spot fleet instances on your behalf.

☐ EC2 - Scheduled Instances

Allows EC2 Scheduled Instances to manage instances on your behalf.


















Cancel

Next

Permissions policies (1/921) Info

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

Filter by Type All types 13 matches

| | Policy name  | Type | Description |
|-------------------------------------|--|-------------|--|
| <input type="checkbox"/> |   AmazonRDSCustomInstancePro... | AWS managed | Allows Amazon RDS Custom to perform... |
| <input checked="" type="checkbox"/> |   AmazonRDSDataFullAccess | AWS managed | Allows full access to use the RDS data ... |
| <input type="checkbox"/> |   AmazonRDSDirectoryServiceAc... | AWS managed | Allow RDS to access Directory Service ... |
| <input type="checkbox"/> |   AmazonRDSEnhancedMonitorin... | AWS managed | Provides access to Cloudwatch for RDS... |
| <input type="checkbox"/> |   AmazonRDSFullAccess | AWS managed | Provides full access to Amazon RDS via... |
| <input type="checkbox"/> |   AmazonRDSPerformanceInsig... | AWS managed | Provides full access to RDS Performan... |
| <input type="checkbox"/> |   AmazonRDSPerformanceInsig... | AWS managed | Read-Only policy for RDS Performance... |
| <input type="checkbox"/> |   AmazonRDSReadOnlyAccess | AWS managed | Provides read only access to Amazon R... |

us-east-1.console.aws.amazon.com/iam/home?region=us-east-1#/roles/create?selectedUseCase=EC2&trustedEntityType=AWS_SERVICE&selectedSe...

Finish update

aws

Services

Search

[Option+S]

Global

rsujithsri16@gmail.com

EC2

| | | | | |
|-------------------------------------|--|---|-------------|--|
| <input checked="" type="checkbox"/> | | AmazonRDSDataFullAccess | AWS managed | Allows full access to use the RDS data ... |
| <input type="checkbox"/> | | AmazonRDSDirectoryServiceAc... | AWS managed | Allow RDS to access Directory Service ... |
| <input type="checkbox"/> | | AmazonRDSEnhancedMonitorin... | AWS managed | Provides access to Cloudwatch for RDS... |
| <input type="checkbox"/> | | AmazonRDSFullAccess | AWS managed | Provides full access to Amazon RDS via... |
| <input type="checkbox"/> | | AmazonRDSPerformanceInsigh... | AWS managed | Provides full access to RDS Performan... |
| <input type="checkbox"/> | | AmazonRDSPerformanceInsigh... | AWS managed | Read-Only policy for RDS Performance... |
| <input type="checkbox"/> | | AmazonRDSReadOnlyAccess | AWS managed | Provides read only access to Amazon R... |
| <input type="checkbox"/> | | AWS ElasticBeanstalkRoleRDS | AWS managed | (Elastic Beanstalk operations role) Allo... |
| <input type="checkbox"/> | | AWSFaultInjectionSimulatorRD... | AWS managed | This policy grants the Fault Injection Si... |
| <input type="checkbox"/> | | AWSQuickSightDescribeRDS | AWS managed | Allow QuickSight to describe the RDS r... |
| <input type="checkbox"/> | | CloudWatchAutomaticDashboa... | AWS managed | Provides access to the non-CloudWatc... |
| <input type="checkbox"/> | | RDS CloudHsmAuthorizationRole | AWS managed | Default policy for the Amazon RDS ser... |

► Set permissions boundary - optional

Cancel

Previous

Next



[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

Enter a meaningful name to identify this role.

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

Description

Add a short explanation for this role.

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

Edit

Trust policy

1 - {
2

"Version": "2012-10-17"



```
15 ]
16 }
```

Step 2: Add permissions Edit

| Permissions policy summary | | |
|---|-------------|--------------------|
| Policy name | Type | Attached as |
| AmazonRDSDataFullAccess | 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.

Add new tag

You can add up to 50 more tags.



Review and create

Review your choices. After you create the user, you can view and download the autogenerated password, if enabled.

User details

User name
test-user

Console password type
None

Require password reset
No

Permissions summary

< 1 >

Name



Type



Used as



No resources

Tags - optional

Tags are key-value pairs you can add to AWS resources to help identify, organize, or search for resources. Choose any tags you want to associate with this user.

←→↻us-east-1.console.aws.amazon.com/iam/home?region=us-east-1#/users/create☆☰☒👤Finish update⋮

awsServices🔍Search[Option+S]

🖨🔔🔗⚙Global▼rsujithsri16@gmail.com▼

EC2

☰

Step 3
Review and create

User name
test-user

Console password type
None

Require password reset
No

Permissions summary

< 1 >

| Name🔗 | ▲ | Type | ▼ | Used as | ▼ |
|--------------|---|------|---|---------|---|
| No resources | | | | | |

Tags - optional

Tags are key-value pairs you can add to AWS resources to help identify, organize, or search for resources. Choose any tags you want to associate with this user.

No tags associated with the resource.

Add new tag

You can add up to 50 more tags.

Cancel

Previous

Create user

← → ↺

us-east-1.console.aws.amazon.com/iam/home?region=us-east-1#/users/details/test-user?section=security_credentials

☆ ☰ 🖨 👤 Finish update ⋮

aws

Services

Q Search

[Option+S]

🔍 🔔 ? ⚙ Global ▾ rsujithsri16@gmail.com ▾

EC2

Identity and Access Management (IAM) ×

Q Search IAM

Dashboard

▼ Access management

User groups

Users

Roles

Policies

Identity providers

Account settings

▼ Access reports

Access Analyzer

External access

Unused access

Analyzer settings

Credential report

IAM > Users > test-user

test-user Info

Delete

Summary

| | | |
|---|----------------------------|---|
| ARN arn:aws:iam::602093162468:user/test-user | Console access Disabled | Access key 1 Create access key |
| Created April 22, 2024, 19:45 (UTC+05:30) | Last console sign-in - | |

Permissions

Groups

Tags

Security credentials

Access Advisor

Console sign-in

Enable console access

| | |
|--|---------------------------------|
| Console sign-in link https://602093162468.signin.aws.amazon.com/console | Console password Not enabled |
|--|---------------------------------|

us-east-1.console.aws.amazon.com/iam/home?region=us-east-1#/users/details/test-user?section=security_credentials

aws Services Search [Option+S]

EC2

Global rsujithsri15@gmail.com

Finish update

Identity and Access Management (IAM)

Search IAM

Dashboard

Access management

User groups

Users

Roles

Policies

Identity providers

Account settings

Access reports

Access Analyzer

External access

Unused access

Analyzer settings

Created April 22, 2024

Permission

Console

Console sign-in

Multi-factor authentication

De

Enable console access

Enable console access for test-user.

Console password

☐ Autogenerated password

☒ Custom password

.....

• Must be at least 8 characters long

• Must include at least three of the following mix of character types: uppercase letters (A-Z), lowercase letters (a-z), numbers (0-9), and symbols ! @ # \$ % ^ & * () _ + - (hyphen) = [] { } | ' "

☐ Show password

☐ User must create new password at next sign-in

Users automatically get the [IAMUserChangePassword](#) policy to allow them to change their own password.

Cancel

Enable console access

Enable console access

Assign MFA device

Assign MFA device

←

→

↺

us-east-1.console.aws.amazon.com/iam/home?region=us-east-1#/users/details/test-user?section=security_credentials

☆

☰

🖨

👤

Finish update ⋮

aws

Services

Search

[Option+5]

📧

🔔

?

⚙

Global ▾

rsujithsri16@gmail.com ▾

EC2

Identity and Access Management (IAM) ×

Search IAM

Dashboard

Access management ▾

User groups

Users

Roles

Policies

Identity providers

Account settings

Access reports ▾

Access Analyzer

External access

Unused access

Analyzer settings

Console access enabled.

Console password ×

✔ You have successfully enabled the user's new password.
This is the only time you can view this password. After you close this window, if the password is lost, you must create a new one.

✔ URL Copied

📄 https://602093162468.signin.aws.amazon.com/console

User name

📄 test-user

Console password

📄 ***** Show

Download .csv file

Close

Manage console access

19:46 GMT+5:30)

Resync

Assign MFA device

Created on

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

Assign MFA device

← → ↺

us-east-1.console.aws.amazon.com/dynamodbv2/home?region=us-east-1#service

☆ 📄 👤 Finish update ⋮

aws

Services

Search

[Option+S]

📄 🔔 ⓘ ⚙️

N. Virginia ▼

test-user @ 6020-9316-2468 ▼

EC2

DynamoDB

×

Dashboard

Tables

Explore items

PartiQL editor

Backups

Exports to S3

Imports from S3

Integrations New

Reserved capacity

Settings

▼ DAX

Clusters

Subnet groups

Parameter groups

Events

Database

Amazon DynamoDB

A fast and flexible NoSQL database service for any scale

DynamoDB is a fully managed, key-value, and document database that delivers single-digit-millisecond performance at any scale.

Get started

Create a new table to start exploring DynamoDB.

Create table

Pricing

DynamoDB charges for reading, writing, and storing data in your DynamoDB tables, along with any optional features you choose to turn on. DynamoDB has on-demand capacity mode and provisioned capacity mode, and these

How it works

aws

What is Amazon DynamoDB?

⋮

← → ↺

us-east-1.console.aws.amazon.com/dynamodbv2/home?region=us-east-1#create-table

☆ 📄 🖱️ 👤 Finish update ⋮

aws

Services

🔍 Search

[Option+S]

📧 🔔 ⓘ ⚙️

N. Virginia ▼ test-user @ 6020-9316-2468 ▲

EC2

☰

DynamoDB > Tables > Create table

Create table

Table details [Info](#)

DynamoDB is a schemaless database that requires only a table name and a primary key when you create the table.

Table name

This will be used to identify your table.

Enter name for table

Between 3 and 255 characters, containing only letters, numbers, underscores (_), hyphens (-), and periods (.).

Partition key

The partition key is part of the table's primary key. It is a hash value that is used to retrieve items from your table and allocate data across hosts for scalability and availability.

Enter the partition key name

String ▼

1 to 255 characters and case sensitive.

Sort key - optional

You can use a sort key as the second part of a table's primary key. The sort key allows you to sort or search among all items sharing the same partition key.

Enter the sort key name

String ▼

1 to 255 characters and case sensitive.

Account ID: 6020-9316-2468 📄

IAM user: test-user 📄

Account

Organization

Service Quotas

Billing and Cost Management

Security credentials

Switch role

Sign out



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.

6020-9316-2468

IAM role name

The name of the role that you want to assume. You can get this from the end of the role's ARN.

For example, ARN: arn:aws:iam::111111111111:role/RoleName

user1

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.

Display color - optional

The selected color displays in the console navigation when this role is active

None

Cancel

Switch Role

←→↺

us-east-1.console.aws.amazon.com/ec2/home?region=us-east-1#Home:

★☰📱👤

Finish update ⋮

aws

Services

Search

[Option+S]

🖨🔔🔍⚙

N. Virginia ▾

test-user @ 6020-9316-2468 ▾

EC2

EC2 Dashboard

×

EC2 Global View

Events

Console-to-Code [Preview](#)

► Instances

▼ Images

AMIs

AMI Catalog

▼ Elastic Block Store

Volumes

Snapshots

Lifecycle Manager

▼ Network & Security

Security Groups

Elastic IPs

Placement Groups

Key Pairs

Network Interfaces

Resources

EC2 Global view ↗⚙↺

You are using the following Amazon EC2 resources in the US East (N. Virginia) Region:

| | | | |
|---------------------|-------------|---------------------|-------------|
| Instances (running) | 0 | Auto Scaling Groups | ⊗ API Error |
| Dedicated Hosts | ⊗ API Error | Elastic IPs | ⊗ API Error |
| Instances | ⊗ API Error | Key pairs | ⊗ API Error |
| Load balancers | ⊗ API Error | Placement groups | ⊗ API Error |
| Security groups | ⊗ API Error | Snapshots | ⊗ API Error |
| 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 ↗

Service health

AWS Health Dashboard ↗↺

⊗ An error occurred

An error occurred retrieving

EC2 Free Tier [Info](#)

Offers for all AWS Regions.

0 EC2 free tier offers in use

End of month forecast

⊗ User: arn:aws:iam::602093162468:user/test-user is not authorized to perform: freetier:GetFreeTierUsage on resource: arn:aws:freetier:us-east-1:602093162468:/GetFreeTierUsage because use no identity-based policy allows the freetier:GetFreeTierUsage action

Exceeds free tier

⊗ User: arn:aws:iam::602093162468:user/test-user is not authorized to perform: freetier:GetFreeTierUsage on resource: arn:aws:freetier:us-east-1:602093162468:/GetFreeTierUsage because use no identity-based policy allows the freetier:GetFreeTierUsage action

[View Global EC2 resources](#)

[View all AWS Free Tier offers ↗](#)