


Users (4) Info

An IAM user is an identity with long-term credentials that is used to interact with AWS in an account.



Delete

Add users

 Find users by username or access key

< 1 > 

<input type="checkbox"/>	User name ▾	Groups ▾	Last activity ▾	MFA ▾	Password age ▾	Active key age ▾
<input type="checkbox"/>	user1	Dev_team and Ops_team	Never	None	✔ 50 minutes ago	✔ 50 minutes ago
<input type="checkbox"/>	user2	Dev_team	Never	None	✔ 50 minutes ago	✔ 50 minutes ago
<input type="checkbox"/>	user3	Ops_team	Never	None	✔ 50 minutes ago	✔ 50 minutes ago
<input type="checkbox"/>	user4	Ops_team	Never	None	✔ 50 minutes ago	✔ 50 minutes ago

User groups (2) [Info](#)

A user group is a collection of IAM users. Use groups to specify permissions for a collection of users.



Delete

Create group

 *Filter User groups by property or group name and press enter*

< 1 > 

<input type="checkbox"/>	Group name ▾	Users	Permissions	Creation time ▾
<input type="checkbox"/>	Dev_team	⌂ Loading	⌂ Loading	41 minutes ago
<input type="checkbox"/>	Ops_team	⌂ Loading	⌂ Loading	40 minutes ago

Select trusted entity

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.

Common use cases

☒ **EC2**

Allows EC2 instances to call AWS services on your behalf.

☐ **Lambda**

Allows Lambda functions to call AWS services on your behalf.

Use cases for other AWS services:

Choose a service to view use case




Cancel

Next

Step 2: Add permissions

[Edit](#)

Permissions policy summary

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

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.

[Add tag](#)

You can add up to 50 more tags.

[Cancel](#)[Previous](#)[Create role](#)

Add permissions to user1

Permissions summary

The following policies will be attached to the user shown above.

Type	Name
Managed policy	AmazonVPCFullAccess
Managed policy	AmazonDynamoDBFullAccess

Add permissions to user2

Permissions summary

The following policies will be attached to the user shown above.

Type	Name
Managed policy	AmazonDynamoDBFullAccess
Managed policy	AmazonVPCFullAccess

[IAM](#) > [Roles](#) > [myroles](#) > Edit trust policy

Edit trust policy

```
1 ▼ {  
2   "Version": "2012-10-17",  
3 ▼   "Statement": [  
4 ▼     {  
5       "Effect": "Allow",  
6 ▼       "Principal": {  
7         "Service": "ec2.amazonaws.com"  
8       },  
9       "Action": "sts:AssumeRole"  
10    }  
11  ]  
12 }
```

User ARN arn:aws:iam::951490220303:user/user1 

Path /

Creation time 2022-02-23 21:15 UTC+0530

Edit trust policy

```
1 ▼ {  
2     "Version": "2012-10-17",  
3     "Statement": [  
4         {  
5             "Effect": "Allow",  
6             "Principal": {  
7                 "AWS": [  
8                     "arn:aws:iam::951490220303:user/user1",  
9                     "arn:aws:iam::951490220303:user/user2"  
10                ],  
11                "Service": "ec2.amazonaws.com"  
12            },  
13            "Action": "sts:AssumeRole"  
14        }  
15    ]  
16 }
```

AWS account 951490220303

IAM user name user1

Old password

New password

Retype new password

Confirm password change

[Sign in using root user email](#)

English ▼



Services



Search for services, features, blogs, docs, and more

[Alt+S]



Ohio ▾

user1 @ 9514-9022-0303 ▾

AWS Management Console

Amazon S3

Buckets

Access Points

Object Lambda Access Points

Multi-Region Access Points

Batch Operations

Access analyzer for S3

Block Public Access settings for this account

Storage Lens

Dashboards

AWS Organizations settings

Feature spotlight 3

AWS Marketplace for S3

Amazon S3

Account snapshot

Storage lens provides visibility into storage usage and activity trends. [Learn more](#)

View Storage Lens dashboard

Buckets (0)

Info

Refresh

Copy ARN

Empty

Delete

Create bucket

Find buckets by name

< 1 > ⚙

Name ▲

AWS Region ▼

Access ▼

Creation date ▼

No buckets

You don't have any buckets.

Create bucket

Here no errors in VPC and S3, i.e, Our role is working.

VPC Dashboard

EC2 Global View New

Filter by VPC:

 Select a VPC

▼ VIRTUAL PRIVATE CLOUD

Your VPCs

Subnets

Route Tables

Internet Gateways

Egress Only Internet Gateways

DHCP Options Sets

Elastic IPs

Managed Prefix Lists

Endpoints New

Endpoint Services

NAT Gateways

Peering Connections

▼ SECURITY

Launch VPC Wizard

Launch EC2 Instances

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

Resources by Region Refresh Resources

You are using the following Amazon VPC resources

VPCs

US East 1

[See all regions ▼](#)

NAT Gateways

US East 0

[See all regions ▼](#)

Subnets

US East 3

[See all regions ▼](#)

VPC Peering Connections

US East 0

[See all regions ▼](#)

Route Tables

US East 1

[See all regions ▼](#)

Network ACLs

US East 1

[See all regions ▼](#)

Internet Gateways

US East 1

[See all regions ▼](#)

Security Groups

US East 1

[See all regions ▼](#)

Egress-only Internet Gateways

US East 0

[See all regions ▼](#)

Customer Gateways

US East 0

[See all regions ▼](#)

DHCP options sets

US East 1

[See all regions ▼](#)

Virtual Private Gateways

US East 0

[See all regions ▼](#)

If we want to switch the role , then we copy the Switch role link, then paste into chrome.



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](#).

Switch Role

Get started in 3 simple steps

The console will track the last five roles that you have used so that you don't have to.



Create role

Before you can switch roles, an administrator must create the role in the account you want



Role access

Your administrator provides you with the account ID or alias and the role name to use.



Switch roles

Click your user name in the navigation bar, then select Switch Role. Enter the account

We give our acc. details.