

AWS IAM Cloud Security Project

Project Summary

This project focused on implementing cloud security controls within Amazon Web Services (AWS), specifically using Identity and Access Management (IAM) to enforce least privilege access. The goal was to restrict user actions on EC2 instances based on role requirements, while also hardening the AWS Management Console against unauthorized access.

Objectives

- Design and apply a **least privileged IAM policy** tailored to specific EC2 roles.
- Attach the policy to a **user group** for scalable role-based access control.
- Validate policy effectiveness by testing access restrictions on two EC2 instances:
 - **Audit Instance** – read-only access for compliance monitoring.
 - **Sales Instance** – limited access for operational tasks.
- Harden the AWS Console by configuring MFA, password policies, and access logging.

Tools & Technologies

Tool/Service Purpose

AWS IAM	Policy creation, user/group management
---------	--

EC2	Target resources for access control
-----	-------------------------------------

IAM Policy Simulator	Policy testing and validation
----------------------	-------------------------------

JSON policy syntax	Effect, Action, Resource
--------------------	--------------------------

Principles of least privilege

Implementation Steps

1. Created IAM Users & Groups

- Defined roles for audit and sales teams.
- Grouped users based on access needs.

2. Built Custom IAM Policies

- Used JSON policy editor to define least-privilege rules.
- Included Allow and Deny statements for EC2 actions.

3. Attached Policies to Groups

- Ensured scalable access control via group assignments.

4. Tested Access with IAM Policy Simulator

- Verified that users could only perform permitted actions.
- Confirmed that restricted actions were blocked.

5. Hardened AWS Console

- Enabled MFA for all users.
- Set strong password policies.
- Activated CloudTrail for auditing.

Results & Impact

- Achieved **100% compliance** with least-privilege principles.
- Prevented unauthorized access to EC2 instances.
- Improved overall security posture of the AWS environment.
- Demonstrated practical skills in IAM, EC2, and cloud security best practices.

CREATING EC2 INSTANCES

The screenshot shows the AWS Management Console home page for the United States (Ohio) region. The 'Launch instance' button is circled in red. The page includes a 'Resources' section with a table of EC2 resources, a 'Launch instance' section with a 'Launch instance' button, a 'Service health' section, and an 'Account attributes' section.

Resources		
Instances (running)	0	Auto Scaling Groups
Dedicated Hosts	0	Elastic IPs
Key pairs	0	Load balancers
Security groups	0	Snapshots
Capacity Reservations	0	Instances
	0	Placement groups
	0	Volumes

Launch instance
To get started, launch an Amazon EC2 Instance, which is a virtual server in the cloud.

[Launch instance](#) [Migrate a server](#)

Note: Your instances will launch in the United States (Ohio) Region

Service health
Region: United States (Ohio)
Status: ✔ This service is operating normally.

Zones

Zone name	Zone ID
us-east-2a	use2-az1

EC2 Free Tier
Offers for all AWS Regions.
0 EC2 free tier offers in use
End of month forecast: ⚠ 0 offers forecasted to exceed free tier limit.
Exceeds free tier: ⚠ 0 offers exceeded and is now pay-as-you-go pricing.
[View Global EC2 resources](#)

Account attributes
Default VPC: none
Settings: Data protection and security, Allowed AMIs, Zones, EC2 Serial Console

The screenshot shows the Amazon Elastic Compute Cloud (EC2) console page. The 'Launch instance' button is circled in red. The page includes a 'Benefits and features' section, an 'Additional actions' section, and a 'Pricing (US)' section.

Amazon Elastic Compute Cloud (EC2)

Create, manage, and monitor virtual servers in the cloud.

Amazon Elastic Compute Cloud (Amazon EC2) offers the broadest and deepest compute platform, with over 600 instance types and a choice of the latest processors, storage, networking, operating systems, and purchase models to help you best match the needs of your workload.

Launch a virtual server
[Launch instance](#)
[View dashboard](#)
[Get started walkthroughs](#)
[Get started tutorial](#)

Benefits and features
EC2 offers ultimate scalability and control
Fully resizable compute capacity to support virtually any workload. This service is best if you want:

- Highest level of control of the entire technology stack, allowing full integration with all AWS services
- Widest variety of server size options
- Widest availability of operating systems to choose from including Linux, Windows, and macOS
- Global scalability

Additional actions
[View running instances](#)
[Migrate a server](#)

Pricing (US)

Search

[Alt+S]

United States (Ohio)

Account ID: 7772-3009-3900

jarisat%20kareem

EC2 > Instances > Launch an instance

It seems like you may be new to launching instances in EC2. Take a walkthrough to learn about EC2, how to launch instances and about best practices.

Take a walkthrough

Do not show me this message again.

Launch an instance

Amazon EC2 allows you to create virtual machines, or instances, that run on the AWS Cloud. Quickly get started by following the simple steps below.

Name and tags

Name

jatech-audit-JJ

Add additional tags

Application and OS Images (Amazon Machine Image)

An AMI contains the operating system, application server, and applications for your instance. If you don't see a suitable AMI below, use the search field or choose [Browse more AMIs](#).

Search our full catalog including 1000s of application and OS images

Recents

Quick Start

Amazon Linux

macOS

Ubuntu

Windows

Red Hat

SUSE Linux

Debian

Browse more AMIs

Summary

Number of instances

1

Software Image (AMI)

Amazon Linux 2023 AMI 2023.9.2...read more

ami-0199d4b5b8b4fde0e

Virtual server type (instance type)

t2.micro

Firewall (security group)

New security group

Storage (volumes)

1 volume(s) - 8 GiB

Cancel

Launch instance

Preview code

CloudShell Feedback

© 2025, Amazon Web Services, Inc. or its affiliates. Privacy Terms Cookie preferences

Search

[Alt+S]

United States (Ohio)

Account ID: 7772-3009-3900

jarisat%20kareem

EC2 > Instances > Launch an instance

It seems like you may be new to launching instances in EC2. Take a walkthrough to learn about EC2, how to launch instances and about best practices.

Take a walkthrough

Do not show me this message again.

Launch an instance

Amazon EC2 allows you to create virtual machines, or instances, that run on the AWS Cloud. Quickly get started by following the simple steps below.

Name and tags

Name

jatech-audit-JJ

Add additional tags

Application and OS Images (Amazon Machine Image)

An AMI contains the operating system, application server, and applications for your instance. If you don't see a suitable AMI below, use the search field or choose [Browse more AMIs](#).

Search our full catalog including 1000s of application and OS images

Recents

Quick Start

Amazon Linux

macOS

Ubuntu

Windows

Red Hat

SUSE Linux

Debian

Browse more AMIs

Summary

Number of instances

1

Software Image (AMI)

Amazon Linux 2023 AMI 2023.9.2...read more

ami-0199d4b5b8b4fde0e

Virtual server type (instance type)

t2.micro

Firewall (security group)

New security group

Storage (volumes)

1 volume(s) - 8 GiB

Cancel

Launch instance

Preview code

CloudShell Feedback

© 2025, Amazon Web Services, Inc. or its affiliates. Privacy Terms Cookie preferences

On-Demand SUSE, base pricing: 0.0116 USD per Hour

On-Demand RHEL, base pricing: 0.026 USD per Hour

On-Demand Linux, base pricing: 0.0116 USD per Hour

Additional costs apply for AMIs with pre-installed software

▼ Key pair (login) Info

You can use a key pair to securely connect to your instance. Ensure that you have access to the selected key pair before you launch the instance.

Key pair name - required

Proceed without a key pair (Not recommended)Default valueCreate new key pair

▼ Network settings Info

Network Info

vpc-01d7d28ff2cb7b38e

Subnet Info

No preference (Default subnet in any availability zone)

Auto-assign public IP Info

Enable

Additional charges apply when outside of free tier allowance

Firewall (security groups) Info

A security group is a set of firewall rules that control the traffic for your instance. Add rules to allow specific traffic to reach your instance.

Create security groupSelect existing security group

▼ Summary

Number of instances Info

1

Software Image (AMI)

Amazon Linux 2023 AMI 2023.9.2...read more

ami-0341d95f75f311023

Virtual server type (instance type)

t2.micro

Firewall (security group)

New security group

Storage (volumes)

1 volume(s) - 8 GiB

Free tier: In your first year of opening an AWS account, you get 750 hours per month of t2.micro instance usage (or t3.micro where

CancelLaunch instancePreview code

EC2 > Instances

Dashboard

EC2 Global View

Events

▼ Instances

Instances

Instance Types

Launch Templates

Spot Requests

Savings Plans

Reserved Instances

Dedicated Hosts

Capacity Reservations

Capacity Manager New

▼ Images

AMIs

AMI Catalog

▼ Elastic Block Store

Volumes

Snapshots

Instances (1) Info

Find Instance by attribute or tag (case-sensitive)

All states

1

	Name	Instance ID	Instance state	Instance type	Status check	Alarm status	Availability Zone	Public IP
<input type="checkbox"/>	Jacyber-Audit-JJ	i-07200cc8c8078d742	Running	t2.micro	Initializing	View alarms +	us-east-1c	ec2-54-23-

Select an instance

aws

Search

[Alt+S]

United States (N. Virginia)

Account ID: 7772-3009-3900

jarist%20kareem

EC2 > Instances > Launch an instance

Launch an instance

Amazon EC2 allows you to create virtual machines, or instances, that run on the AWS Cloud. Quickly get started by following the simple steps below.

Name and tags

Name

Jacyber-Sale-JJ

Add additional tags

Application and OS Images (Amazon Machine Image)

An AMI contains the operating system, application server, and applications for your instance. If you don't see a suitable AMI below, use the search field or choose [Browse more AMIs](#).

Search our full catalog including 1000s of application and OS images

Recents

Quick Start

Amazon Linux

macOS

Ubuntu

Windows

Red Hat

SUSE Linux

Debian

Browse more AMIs

Including AMIs from AWS, Marketplace and the Community

Summary

Number of instances

1

Software Image (AMI)

Amazon Linux 2023 AMI 2023.9.2...[read more](#)

ami-0341d95f75f311023

Virtual server type (instance type)

t2.micro

Firewall (security group)

New security group

Storage (volumes)

1 volume(s) - 8 GiB

Free tier: In your first year of opening an AWS account, you get 750 hours per month of t2.micro instance usage (or t3.micro where

Cancel

Launch instance

Preview code

CloudShell Feedback

© 2025, Amazon Web Services, Inc. or its affiliates. Privacy Terms Cookie preferences

aws

Search

[Alt+S]

United States (N. Virginia)

Account ID: 7772-3009-3900

jarist%20kareem

EC2 > Instances > Launch an instance

Launch an instance

Amazon EC2 allows you to create virtual machines, or instances, that run on the AWS Cloud. Quickly get started by following the simple steps below.

Name and tags

Key	Value	Resource types
Name	Jacyber-Sale-JJ	Select resource types
Env	Sale	Select resource types

Add new tag

You can add up to 48 more tags.

Application and OS Images (Amazon Machine Image)

An AMI contains the operating system, application server, and applications for your instance. If you don't see a suitable AMI below, use the search field or choose [Browse more AMIs](#).

Search our full catalog including 1000s of application and OS images

Summary

Number of instances

1

Software Image (AMI)

Amazon Linux 2023 AMI 2023.9.2...[read more](#)

ami-0341d95f75f311023

Virtual server type (instance type)

t2.micro

Firewall (security group)

New security group

Storage (volumes)

1 volume(s) - 8 GiB

Free tier: In your first year of opening an AWS account, you get 750 hours per month of t2.micro instance usage (or t3.micro where

Cancel

Launch instance

Preview code

CloudShell Feedback

© 2025, Amazon Web Services, Inc. or its affiliates. Privacy Terms Cookie preferences

aws

Search

[Alt+S]

United States (N. Virginia)

Account ID: 7772-3009-3900

jarist%20kareem

EC2 > Instances > Launch an instance

Recents

Quick Start

Amazon Linux

aws

macOS

Mac

Ubuntu

ubuntu

Windows

Microsoft

Red Hat

Red Hat

SUSE Linux

SUSE

Debian

debian

Browse more AMIs

Including AMIs from AWS, Marketplace and the Community

Amazon Machine Image (AMI)

Amazon Linux 2023 kernel-6.1 AMI
ami-0341d95f75f311023 (64-bit (x86), uefi-preferred) / ami-0B58e76ce571eb464 (64-bit (ARM), uefi)
Virtualization: hvm ENA enabled: true Root device type: ebs

Free tier eligible

Description

Amazon Linux 2023 (kernel-6.1) is a modern, general purpose Linux-based OS that comes with 5 years of long term support. It is optimized for AWS and designed to provide a secure, stable and high-performance execution environment to develop and run your cloud applications.

Amazon Linux 2023 AMI 2023.9.20251014.0 x86_64 HVM kernel-6.1

Architecture

64-bit (x86)

Boot mode

uefi-preferred

AMI ID

ami-0341d95f75f311023

Publish Date

2025-10-09

Username

ec2-user

Verified provider

▼ Summary

Number of instances [Info](#)

1

Software Image (AMI)
Amazon Linux 2023 AMI 2023.9.2...[read more](#)
ami-0341d95f75f311023

Virtual server type (instance type)
t2.micro

Firewall (security group)
New security group

Storage (volumes)
1 volume(s) - 8 GiB

Free tier: In your first year of opening an AWS account, you get 750 hours per month of t2.micro instance usage (or t3.micro where

Cancel

Launch instance

Preview code

▼ Instance type [Info](#) [Get advice](#)

CloudShell Feedback

© 2025, Amazon Web Services, Inc. or its affiliates. [Privacy](#) [Terms](#) [Cookie preferences](#)

aws

Search

[Alt+S]

United States (N. Virginia)

Account ID: 7772-3009-3900

jarist%20kareem

EC2 > Instances > Launch an instance

▼ Instance type [Info](#) [Get advice](#)

Instance type

t2.micro

Family: t2 1 vCPU 1 GiB Memory - Current generation: true
On-Demand Windows base pricing: 0.0162 USD per Hour
On-Demand Ubuntu Pro base pricing: 0.0134 USD per Hour
On-Demand SUSE base pricing: 0.0116 USD per Hour On-Demand RHEL base pricing: 0.026 USD per Hour
On-Demand Linux base pricing: 0.0116 USD per Hour

Free tier eligible

All generations

Compare instance types

Additional costs apply for AMIs with pre-installed software

▼ Key pair (login) [Info](#)

You can use a key pair to securely connect to your instance. Ensure that you have access to the selected key pair before you launch the instance.

Key pair name - required

Select

Create new key pair

▼ Network settings [Info](#)

Network [Info](#)

vpc-01d7d28ff2cb7b39e

Subnet [Info](#)

Edit

▼ Summary

Number of instances [Info](#)

1

Software Image (AMI)
Amazon Linux 2023 AMI 2023.9.2...[read more](#)
ami-0341d95f75f311023

Virtual server type (instance type)
t2.micro

Firewall (security group)
New security group

Storage (volumes)
1 volume(s) - 8 GiB

Free tier: In your first year of opening an AWS account, you get 750 hours per month of t2.micro instance usage (or t3.micro where

Cancel

Launch instance

Preview code

CloudShell Feedback

© 2025, Amazon Web Services, Inc. or its affiliates. [Privacy](#) [Terms](#) [Cookie preferences](#)

Key pair (login) Info

You can use a key pair to securely connect to your instance. Ensure that you have access to the selected key pair before you launch the instance.

Key pair name - required

Proceed without a key pair (Not recommended) Default value [Create new key pair](#)

Network settings Info Edit

Network Info

vpc-01d7d28f2cb7b38e

Subnet Info

No preference (Default subnet in any availability zone)

Auto-assign public IP Info

Enable

Additional charges apply when outside of free tier allowance

Firewall (security groups) Info

A security group is a set of firewall rules that control the traffic for your instance. Add rules to allow specific traffic to reach your instance.

☒ Create security group ☐ Select existing security group

We'll create a new security group called 'launch-wizard-2' with the following rules:

☒ Allow SSH traffic from Anywhere

Helps you connect to your instance

Summary

Number of instances Info

1

Software Image (AMI)

Amazon Linux 2023 AMI 2023.9.2...[read more](#)
ami-0341d95f75f311023

Virtual server type (instance type)

t2.micro

Firewall (security group)

New security group

Storage (volumes)

1 volume(s) - 8 GiB

Free tier: In your first year of opening an AWS account, you get 750 hours per month of t2.micro instance usage (or t3.micro where

[Cancel](#) [Launch instance](#) [Preview code](#)

EC2 Info Last updated less than a minute ago Connect Instance state Actions Launch instances

All states

<input type="checkbox"/>	Name	Instance ID	Instance state	Instance type	Status check	Alarm status	Availability Zone	Public IP
<input type="checkbox"/>	Jacyber-Sale-JJ	i-025f880db565c5f1a	Running	t2.micro	⏸ Initializing	View alarms +	us-east-1c	ec2-54-90
<input type="checkbox"/>	Jacyber-Audit-JJ	i-07200cc8c8078d742	Running	t2.micro	✅ 2/2 checks passed	View alarms +	us-east-1c	ec2-54-23

Select an instance

Creating the IAM policy

I Authored a custom AWS IAM policy to enforce least-privilege access by explicitly blocking start/stop actions on the Audit EC2 instance while permitting those actions on the Sales EC2 instance. This policy ensured operational control was limited to designated resources, aligning with cloud security best practices and role-based access requirements.

Step 1

Specify permissions

Specify permissions

Account ID: 7772-3009-1900

IAM > Policies > Create policy

CloudShell Feedback

1 {
2 "Version": "2012-10-17",
3 "Statement": [
4 {
5 "Effect": "Allow",
6 "Action": "ec2:*",
7 "Resource": "*",
8 "Condition": {
9 "StringEquals": {
10 "ec2:ResourceTag/Env": "Audit"
11 }
12 }
13 },
14 {
15 "Effect": "Allow",
16 "Action": "ec2:describe*",
17 "Resource": "*"
18 },
19 {
20 "Effect": "Deny",
21 "Action": [
22 "ec2:DeleteTags",
23 "ec2:CreateTags"
24],
25 "Resource": "*"
26 }
27]
28 }
29]
30 }

+ Add new statement

Edit statement

Select a statement

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

+ Add new statement

© 2025, Amazon Web Services, Inc. or its affiliates. Privacy Terms Cookie preferences

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

Cancel Next

Step 1

Specify permissions

Review and create

Account ID: 7772-3009-1900

IAM > Policies > Create policy

CloudShell Feedback

Review and create

Review the permissions, specify details, and tags.

Policy details

Policy name

JatechAuditEnvPolicy

Description - optional

IAM policy for users in the Audit Environment

Permissions defined in this policy

Explicit deny (1 of 450 services)

Service	Access level	Resource	Request condition
EC2	Full: List, Permissions management, Read, Write	All resources	ec2:ResourceTag/Env = Audit

Add tags - optional

Add new tag

Cancel Previous Create policy

Step 1
Specify permissions

Step 2
Review and create

Review and create

Review the permissions, specify details, and tags.

Policy details

Policy name
Enter a meaningful name to identify this policy.

JatechAuditEnvPolicy

Maximum 128 characters. Use alphanumeric and "+=, @>_." characters.

Description - optional
Add a short explanation for this policy.

IAM policy for users in the Audit Environment

Maximum 1,000 characters. Use alphanumeric and "+=, @>_." characters.

Cancel

Previous

Create policy

CloudShell

Feedback

© 2025, Amazon Web Services, Inc. or its affiliates. [Privacy](#) [Terms](#) [Cookie preferences](#)

Identity and Access Management (IAM)

Search IAM

Dashboard

Access management

- User groups
- Users
- Roles
- Policies
- Identity providers
- Account settings
- Root access management

Access reports

- Access Analyzer
 - Resource analysis
 - Unused access
 - Analyzer settings
- Credential report

Policies (1400)

A policy is an object in AWS that defines permissions.

Filter by Type

All types

1 match

Policy name	Type	Used as	Description
<div><div></div><div>JatechAuditEnvPolicy</div></div>	Customer managed	None	IAM policy for users in the Audit Environ...

Account Alias

The screenshot displays the AWS IAM Dashboard for account ID 7772-3009-3900. A green notification banner at the top states "Alias deleted for this account." The left sidebar contains navigation links for Identity and Access Management (IAM), including Dashboard, Access management, Access reports, and CloudShell. The main content area features several sections: "Security recommendations" with two green checkmarks indicating MFA and no active access keys for the root user; "IAM resources" showing counts for user groups (0), users (0), roles (2), policies (0), and identity providers (0); "What's new" with a list of recent AWS updates; "AWS Account" with the account ID and a circled "Account Alias" link; "Quick Links" for security credentials; and "Additional information" with links to best practices and documentation.

Identity and Access Management (IAM)

Search IAM

Dashboard

- Access management
 - User groups
 - Users
 - Roles
 - Policies
 - Identity providers
 - Account settings
 - Root access management
- Access reports
 - Access Analyzer
 - Resource analysis **New**
 - Unused access
 - Analyzer settings
 - Credential report

Alias deleted for this account.

IAM Dashboard info

Security recommendations 0

- Root user has MFA
Having multi-factor authentication (MFA) for the root user improves 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	2	0	0

What's new 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. 4 months ago
- AWS IAM now enforces MFA for root users across all account types. 4 months ago

AWS Account

Account ID: 7772-3009-3900

Account Alias
[Create](#)

Sign-in URL for IAM users in this account
<https://777230093900.signin.aws.amazon.com/console>

Quick Links

[My security credentials](#)

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

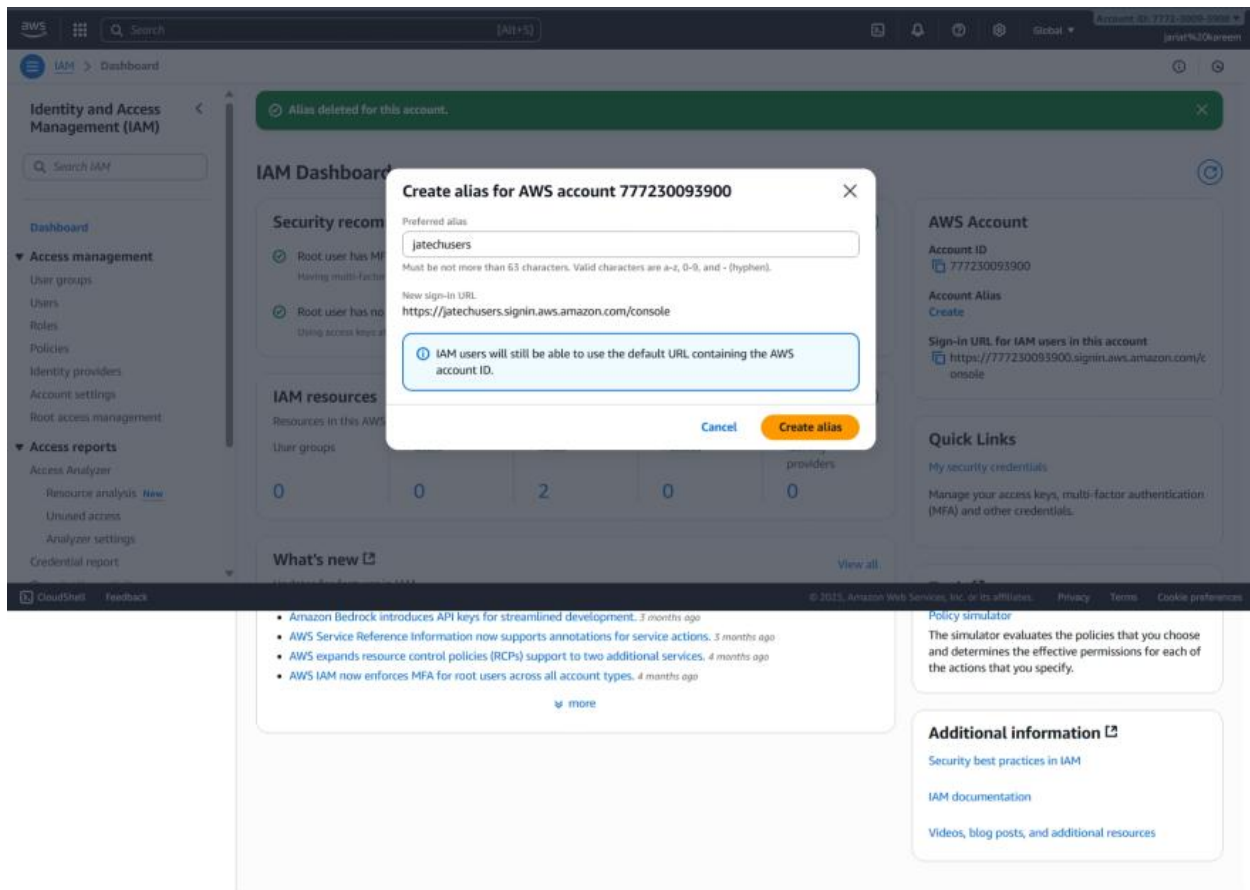
Additional information

[Security best practices in IAM](#)

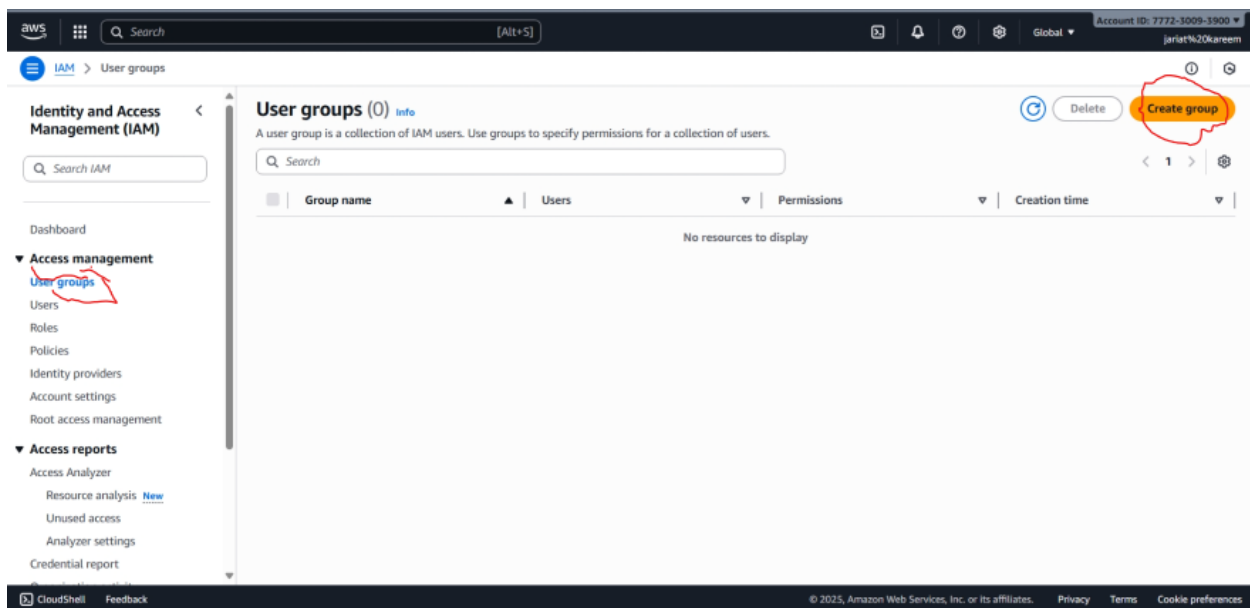
[IAM documentation](#)

Videos, blog posts, and additional resources

© 2025, Amazon Web Services, Inc. or its affiliates. [Privacy](#) [Terms](#) [Cookie preferences](#)



IAM Users and Group



aws

Search

[Alt+S]

Global

Account ID: 7772-3009-1900

jarlat%20kareem

Identity and Access Management (IAM)

Search IAM

Dashboard

Access management

User groups

Users

Roles

Policies

Identity providers

Account settings

Root access management

Access reports

Access Analyzer

Resource analysis

Unused access

Analyzer settings

Credential report

Create user group

name the group

User group name

Enter a meaningful name to identify this group.

jatech-Audit-Group

Maximum 128 characters. Use alphanumeric and "+, @, _" characters.

Add users to the group - Optional (0)

An IAM user is an entity that you create in AWS to represent the person or application that uses it to interact with AWS.

Search

1

Group: Last activity Creation time

No resources to display

Attach permissions policies - Optional (1/1078)

You can attach up to 10 policies to this user group. All the users in this group will have permissions that are defined in the selected policies.

Filter by Type

Ja

All types

1 match

1

Policy nameTypeUsed asDescription

☒JatechAuditEnvPolicyCustomer managedNoneIAM policy for users in the Audit Enviro...

CloudShell

Feedback

© 2025, Amazon Web Services, Inc. or its affiliates. Privacy Terms Cookie preferences

Cancel

Create user group

aws

Search

[Alt+S]

Global

Account ID: 7772-3009-1900

jarlat%20kareem

Identity and Access Management (IAM)

Search IAM

Dashboard

Access management

User groups

Users

Roles

Policies

Identity providers

Account settings

Root access management

Access reports

Access Analyzer

Resource analysis

Unused access

Analyzer settings

Credential report

jatech-Audit-Group user group created.

View group

X

User groups (1)

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

Search

1

Group nameUsersPermissionsCreation time

☐jatech-Audit-Group0DefinedNow

CloudShell

Feedback

© 2025, Amazon Web Services, Inc. or its affiliates. Privacy Terms Cookie preferences

Delete

Create group

aws

Search

[Alt+S]

Global

Account ID: 7772-3009-1900

jariet%20kareem

IAM

Users

Create user

Step 1

Specify user details

Step 2

Set permissions

Step 3

Review and create

Step 4

Retrieve password

Specify user details

User details

User name

jatech-Audit-JJ

The user name can have up to 64 characters. Valid characters: A-Z, a-z, 0-9, and +, -, @, _ - (hyphen)

☒ Provide user access to the AWS Management Console - optional

If you're providing console access to a person, it's a [best practice](#) to manage their access in IAM Identity Center.

Console password

☒ Autogenerated password

You can view the password after you create the user.

☐ Custom password

Enter a custom password for the user.

• 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

☒ Users must create a new password at next sign-in - Recommended

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

ⓘ If you are creating programmatic access through access keys or service-specific credentials for AWS CodeCommit or Amazon Keyspaces, you can generate them after you create this IAM user. [Learn more](#)

CloudShell

Feedback

© 2025, Amazon Web Services, Inc. or its affiliates.

Privacy

Terms

Cookie preferences

Cancel

Next

aws

Search

[Alt+S]

Global

Account ID: 7772-3009-1900

jariet%20kareem

IAM

Users

Create user

Step 3

Review and create

Step 4

Retrieve password

Specify user details

User details

User name

jatech-Audit-JJ

The user name can have up to 64 characters. Valid characters: A-Z, a-z, 0-9, and +, -, @, _ - (hyphen)

☒ Provide user access to the AWS Management Console - optional

If you're providing console access to a person, it's a [best practice](#) to manage their access in IAM Identity Center.

Console password

☐ Autogenerated password

You can view the password after you create the user.

☒ Custom password

Enter a custom password for the user.

• 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

☐ Users must create a new password at next sign-in - Recommended

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

ⓘ If you are creating programmatic access through access keys or service-specific credentials for AWS CodeCommit or Amazon Keyspaces, you can generate them after you create this IAM user. [Learn more](#)

CloudShell

Feedback

© 2025, Amazon Web Services, Inc. or its affiliates.

Privacy

Terms

Cookie preferences

Cancel

Next

Step 1

Specify user details

Step 2

Set permissions

Step 3

Review and create

Step 4

Retrieve password

Set permissions

Add user to an existing group or create a new one. Using groups is a best-practice way to manage user's permissions by job functions. [Learn more](#)

Permissions options

☒ Add user to group

Add user to an existing group, or create a new group. We recommend using groups to manage user permissions by job function.

☐ Copy permissions

Copy all group memberships, attached managed policies, and inline policies from an existing user.

☐ Attach policies directly

Attach a managed policy directly to a user. As a best practice, we recommend attaching policies to a group instead. Then, add the user to the appropriate group.

User groups (1/1)

☒

Group name

▲

Users

▼

Attached policies

▼

Created

☒

[jatech-Audit-Group](#)

0

[JatechAuditEnvPolicy](#)

2025-10-24 (8 minutes ago)

▶ Set permissions boundary - optional

Cancel

Previous

Next

CloudShell Feedback

© 2025, Amazon Web Services, Inc. or its affiliates. [Privacy](#) [Terms](#) [Cookie preferences](#)

Step 1

Specify user details

Step 2

Set permissions

Step 3

Review and create

Step 4

Retrieve password

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

jatech-Audit-JJ

Console password type

Custom password

Require password reset

No

Permissions summary

▲

Type

▼

Used as

[jatech-Audit-Group](#)

Group

Permissions group

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

CloudShell Feedback

© 2025, Amazon Web Services, Inc. or its affiliates. [Privacy](#) [Terms](#) [Cookie preferences](#)

aws

Search

[Alt+S]

Global

Account ID: 7772-3009-3900

jarlat%20kareem

iam

Users

Create user

User created successfully

You can view and download the user's password and email instructions for signing in to the AWS Management Console.

View user

Step 1

Specify user details

Step 2

Set permissions

Step 3

Review and create

Step 4

Retrieve password

Retrieve password

You can view and download the user's password below or email users instructions for signing in to the AWS Management Console. This is the only time you can view and download this password.

Console sign-in details

Email sign-in instructions

Console sign-in URL

https://jatechusers.signin.aws.amazon.com/console

User name

jatech-Audit-JJ

Console password

***** Show

Cancel

Download .csv file

Return to users list

CloudShell

Feedback

© 2025, Amazon Web Services, Inc. or its affiliates.

Privacy

Terms

Cookie preferences

aws

Search

[Alt+S]

Global

Account ID: 7772-3009-3900

jarlat%20kareem

iam

User groups

Identity and Access Management (IAM)

Search IAM

Dashboard

Access management

User groups

Users

Roles

Policies

Identity providers

Account settings

Root access management

Access reports

Access Analyzer

Resource analysis

Unused access

Analyzer settings

Credential report

User groups (1)

info

Delete

Create group

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

Search

1

Group name

jatech-Audit-Group

Users

Permissions

Defined

Creation time

12 minutes ago

CloudShell

Feedback

© 2025, Amazon Web Services, Inc. or its affiliates.

Privacy

Terms

Cookie preferences

Logging in as an IAM User

The image is a composite of two screenshots. The left screenshot shows the 'IAM user sign in' page. It includes a header with 'Provide feedback', 'Multi-session disabled', and 'English'. The main form has fields for 'Account ID or alias (Don't have?)' (containing 'jatechusers'), 'Remember this account' (checkbox), 'IAM username' (containing 'jatech-audit-11'), 'Password' (masked with dots), and a 'Show Password' checkbox. A red circle highlights the 'IAM username' and 'Password' fields. Below the form is a 'Sign in' button, a 'Sign in using root user email' button, and a 'Create a new AWS account' link. At the bottom, there is a disclaimer about the AWS Customer Agreement and Privacy Notice. The right screenshot is an advertisement for 'Amazon Quick Suite', described as 'Agentic AI-powered digital workspace for business users'. It features a dark blue background with a green-to-blue gradient at the top. The text 'Amazon Quick Suite' is in large white font, followed by the description. At the bottom, it says 'Get insights with AI agents'.

aws

Search

[Alt+S]

United States (Ohio)

jatechusers (7772-3009-3900)

jatech-Audit-11

Console Home

Reset to default layout

Add widgets

Recently visited

No recently visited services

EC2S3Aurora and RDSLambda

View all services

Applications (0)

Region: US East (Ohio)

Select Regionus-east-2 (Current Region)

Find applications

Name	Description	Region	Originati
Access denied to servicecatalog:ListApplications			
Diagnose with Amazon Q			

Go to myApplications

Welcome to AWS

Getting started with

find valuable information to get the most out of AWS.

Training and certification

Learn from AWS experts and advance your skills and knowledge.

AWS Builder Center

Learn, build, and connect with builders in the AWS community.

Go to AWS Health

AWS Health

No health data

You don't have permissions to access AWS Health.

Go to AWS Health

Cost and usage

Current month

Cost breakdown

Forecasted month end

Access denied

Savings opportunities

Access denied

Go to Billing and Cost Management

Solutions

Vetted Solutions from AWS for popular business and technical use cases.

Go to AWS Solutions Library

Explore AWS

Security

Region: US East (Ohio)

Go to Security Hub CSPM

Trusted Advisor

Go to Trusted Advisor

Latest announcements

View all announcements

Recent AWS blog posts

View all blog posts

Want to see another widget? Tell us!

Add widgets

aws

Search

[Alt+S]

United States (Ohio)

jatechusers (7772-3009-3900)

jatech-Audit-11

Console Home

Reset to default layout

Add widgets

Recently visited

No recently visited services

EC2S3Aurora and RDSLambda

View all services

Applications (0)

Region: US East (Ohio)

Select Regionus-east-2 (Current Region)

Find applications

Name	Description	Region	Originati
Access denied to servicecatalog:ListApplications			
Diagnose with Amazon Q			

Go to myApplications

Welcome to AWS

Getting started with

find valuable information to get the most out of AWS.

Training and certification

Learn from AWS experts and advance your skills and knowledge.

AWS Builder Center

Learn, build, and connect with builders in the AWS community.

Go to AWS Health

AWS Health

No health data

You don't have permissions to access AWS Health.

Go to AWS Health

Cost and usage

Current month

Cost breakdown

Forecasted month end

Access denied

Savings opportunities

Access denied

Go to Billing and Cost Management

Solutions

Vetted Solutions from AWS for popular business and technical use cases.

Go to AWS Solutions Library

Explore AWS

Security

Region: US East (Ohio)

Go to Security Hub CSPM

Trusted Advisor

Go to Trusted Advisor

Latest announcements

View all announcements

Recent AWS blog posts

View all blog posts

Want to see another widget? Tell us!

Add widgets

Testing the policy

The screenshot shows the AWS Management Console 'Instances' page. The left sidebar contains navigation links for EC2, Images, and Elastic Block Store. The main content area displays a table of instances. The instance 'Jacyber-Audit-JJ' (ID: i-07200cc8c8078d742) is selected. The 'Instance state' dropdown menu is open, showing options: 'All states', 'Stop instance', 'Start instance', 'Reboot instance', 'Hibernate instance', and 'Terminate (delete) instance'. The 'Stop instance' option is highlighted. Below the table, the details for the selected instance are shown, including its ID, public and private IP addresses, and its current state (Running).

Name	Instance ID	Instance state	Instance type	Status
Jacyber-Sale-JJ	i-025f880db565c5f1a	Running	t2.micro	2/2
Jacyber-Audit-JJ	i-07200cc8c8078d742	Running	t2.micro	2/2

i-07200cc8c8078d742 (Jacyber-Audit-JJ)

Instance summary

Instance ID: i-07200cc8c8078d742

Public IPv4 address: 54.234.185.241 | [open address](#)

Private IPv4 addresses: 172.31.31.60

Instance state: Running

Public DNS: ec2-54-234-185-241.compute-1.amazonaws.com | [open address](#)

The screenshot shows the AWS Management Console 'Instances' page with a red error message overlay. The message states: 'Failed to stop the instance i-07200cc8c8078d742. You are not authorized to perform this operation. User: arn:aws:iam::7772-3009-3900:user/jatech-Audit-JJ is not authorized to perform: ec2:StopInstances on resource: arn:aws:ec2:us-east-1:7772-3009-3900:instance/i-07200cc8c8078d742 because no identity-based policy allows the ec2:StopInstances action. Encoded authorization failure message: rgl_xfZ-5CxV1DmvHTsQvdy5NQI_Bbrvq994weeMur28hYqHpB5m5bCjI-Kex7IHgr44Y_huTuVT35xBe6xUjtCwelduk_S_eay35mLSyxJNwc8haDF35lcGhLVjpedYdOzrCkWDGgyk-c6JhpS8DW6Yzy_2PKarcev9GOPORH4YKvb-LxLLAXk00HTZaYLZKoBalZd00Vd_GewgBkLcShZvIBM28nfUvlylc2CvFubsUPwQphoDE0Qh6-H4lglHtP5sztLIZKo_pHsH8Pnl-61lwGku1Vc-uxrNCF9YvK1OPn5BYWgvBeuHsblyqjB2zn8TL5E7sGB52J5kPyNT30ReIZFeveDc89o2a7iZ0B64oTCESChyG5o2kvZeRYMT_jFimMQYulHxI-9Kvm5S5yhcuSKCM07Nb9_DejubFjwWgpyINUKkoiOv_x8AbpzmoxsPZ7iChK4VgDqREHYz36CLKEuWPA1s919La0xZkaZyk_NJADaE47nEJO-DFWlPv1t6Ug4kg_ESKwehZ8BvDooou89qNMfWjB5cR75D1J_cGZPleQndGXGbpPwq9K9K41INSUWaa_Ko1lITve-O96blmV3aM59251PlS9P6-vmR5e1OHxaxTykJfth733pDU-IYNZRCgmUR5DTCaVWbEY96hrXlXOJ6Xy783eFIA7IOGJnsfNz95Mz71e9xc5410KahzHyhy60dzB5r4xVGc5aHcsha_HAP2WDFyIVBN'. Below the error message, the details for the selected instance are shown, including its ID, public and private IP addresses, and its current state (Running).

Failed to stop the instance i-07200cc8c8078d742

You are not authorized to perform this operation. User: arn:aws:iam::7772-3009-3900:user/jatech-Audit-JJ is not authorized to perform: ec2:StopInstances on resource: arn:aws:ec2:us-east-1:7772-3009-3900:instance/i-07200cc8c8078d742 because no identity-based policy allows the ec2:StopInstances action. Encoded authorization failure message: rgl_xfZ-5CxV1DmvHTsQvdy5NQI_Bbrvq994weeMur28hYqHpB5m5bCjI-Kex7IHgr44Y_huTuVT35xBe6xUjtCwelduk_S_eay35mLSyxJNwc8haDF35lcGhLVjpedYdOzrCkWDGgyk-c6JhpS8DW6Yzy_2PKarcev9GOPORH4YKvb-LxLLAXk00HTZaYLZKoBalZd00Vd_GewgBkLcShZvIBM28nfUvlylc2CvFubsUPwQphoDE0Qh6-H4lglHtP5sztLIZKo_pHsH8Pnl-61lwGku1Vc-uxrNCF9YvK1OPn5BYWgvBeuHsblyqjB2zn8TL5E7sGB52J5kPyNT30ReIZFeveDc89o2a7iZ0B64oTCESChyG5o2kvZeRYMT_jFimMQYulHxI-9Kvm5S5yhcuSKCM07Nb9_DejubFjwWgpyINUKkoiOv_x8AbpzmoxsPZ7iChK4VgDqREHYz36CLKEuWPA1s919La0xZkaZyk_NJADaE47nEJO-DFWlPv1t6Ug4kg_ESKwehZ8BvDooou89qNMfWjB5cR75D1J_cGZPleQndGXGbpPwq9K9K41INSUWaa_Ko1lITve-O96blmV3aM59251PlS9P6-vmR5e1OHxaxTykJfth733pDU-IYNZRCgmUR5DTCaVWbEY96hrXlXOJ6Xy783eFIA7IOGJnsfNz95Mz71e9xc5410KahzHyhy60dzB5r4xVGc5aHcsha_HAP2WDFyIVBN

i-07200cc8c8078d742 (Jacyber-Audit-JJ)

Instance summary

Instance ID: i-07200cc8c8078d742

Public IPv4 address: 54.234.185.241 | [open address](#)

Private IPv4 addresses: 172.31.31.60

Instance state: Running

Public DNS: ec2-54-234-185-241.compute-1.amazonaws.com | [open address](#)

aws

Search

[Alt+S]

Global

jatechusers (7772-3009-3900)

jatech-Audit-JJ

Identity and Access Management (IAM)

Search IAM

Dashboard

Access management

Users

Roles

Policies

Identity providers

Account settings

Root access management

Access reports

Access Analyzer

Resource analysis

Unused access

Analyzer settings

Credential report

User groups (0)

info

Delete

Create group

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

Search

Group name

Users

Permissions

Creation time

Access denied to iam:ListGroup

You don't have permission to iam:ListGroup. 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::777230093900:user/jatech-Audit-JJ

Action: iam:ListGroup

On resource(s): arn:aws:iam::777230093900:group/

Context: no identity-based policy allows the action

Diagnose with Amazon Q

CloudShell

Feedback

© 2025, Amazon Web Services, Inc. or its affiliates. Privacy Terms Cookie preferences

aws

Search

[Alt+S]

Global

jatechusers (7772-3009-3900)

jatech-Audit-JJ

Identity and Access Management (IAM)

Search IAM

Dashboard

Access management

User groups

Users

Roles

Policies

Identity providers

Account settings

Root access management

Access reports

Access Analyzer

Resource analysis

Unused access

Analyzer settings

Credential report

Users (0)

info

Delete

Create user

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

Search

User name

Path

Group

Last activity

MFA

Password age

Console last sign-in

Ac

Access denied to iam:ListUsers

You don't have permission to iam:ListUsers. 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::777230093900:user/jatech-Audit-JJ

Action: iam:ListUsers

On resource(s): arn:aws:iam::777230093900:user/

Context: no identity-based policy allows the action

Diagnose with Amazon Q

CloudShell

Feedback

© 2025, Amazon Web Services, Inc. or its affiliates. Privacy Terms Cookie preferences

AWS

Search

[Alt+S]

Global

jatechusers (7772-3009-3900)

jatech-Audit-JJ

IAM

Dashboard

Identity and Access Management (IAM)

Search IAM

Dashboard

Access management

Access reports

CloudShell

Feedback

New access analyzers available

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

Create new analyzer

IAM Dashboard

Info

Security recommendations

Access denied to iam:ListMFADevices

Access denied to iam:ListAccessKeys

AWS Account

Access denied to iam:ListAccountAliases

Quick Links

Policy simulator

Additional information

What's new

Amazon Bedrock introduces API keys for streamlined development.

AWS Service Reference Information now supports annotations for service actions.

AWS expands resource control policies (RCPs) support to two additional services.

AWS IAM now enforces MFA for root users across all account types.

j