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	

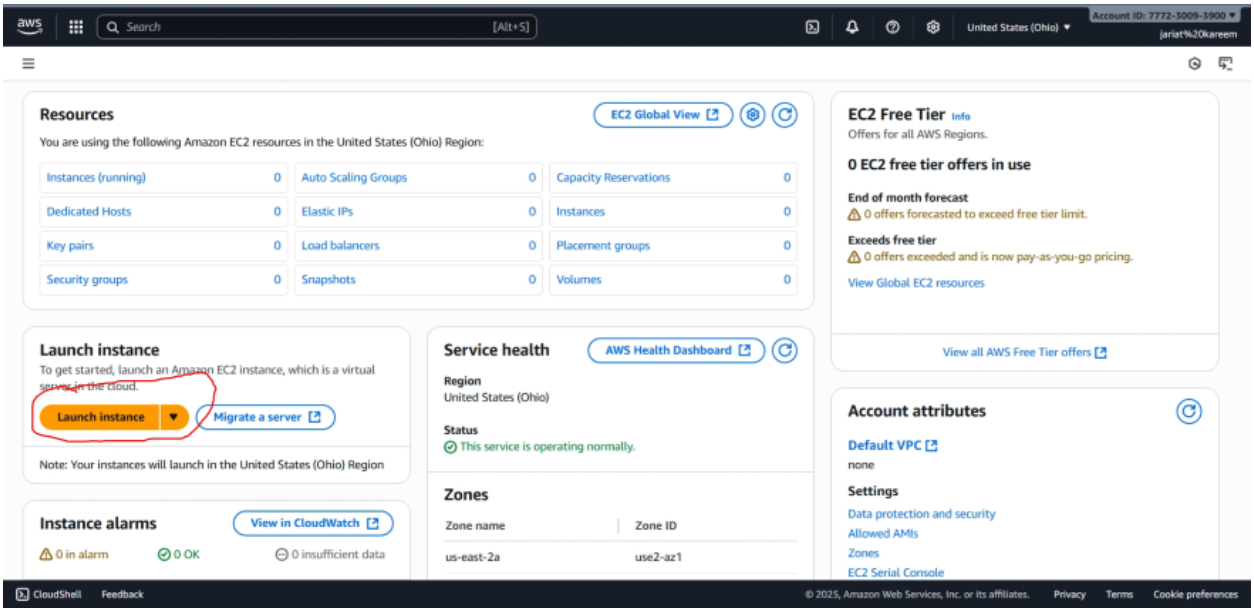
Implementation Steps

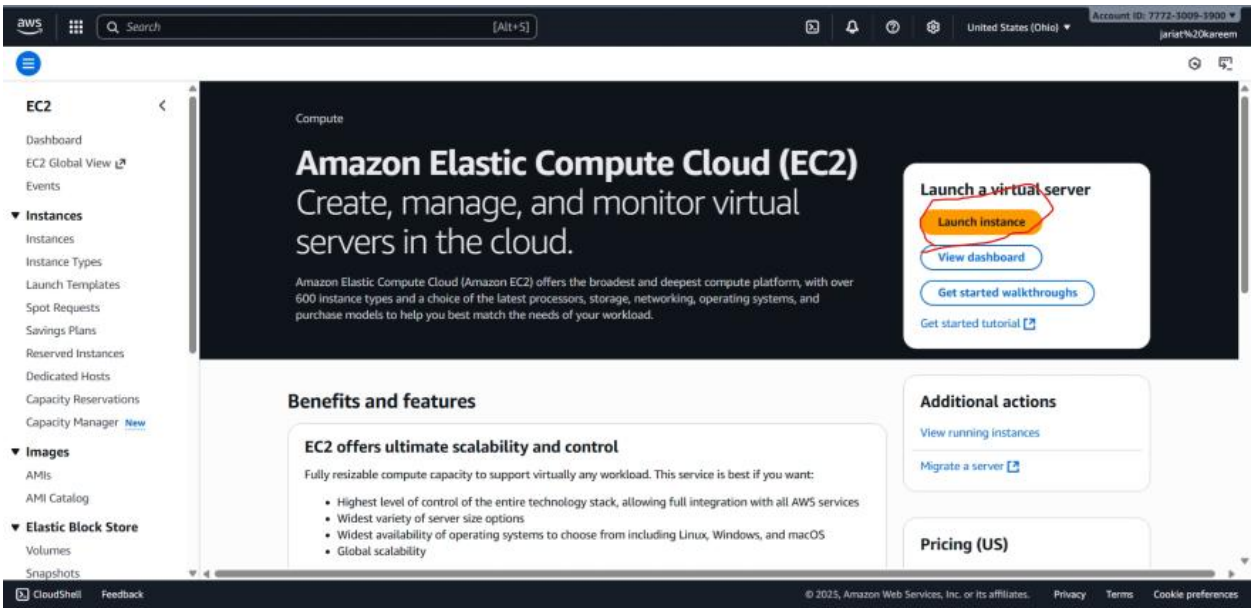
1. **Created IAM Users & Groups**
    - Defined roles for audit and sales teams.
    - Grouped users based on access needs.
2. **Built Custom IAM Policies**
    - Used JSON policy editor to define least-privilege rules.
    - Included Allow and Deny statements for EC2 actions.
3. **Attached Policies 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.

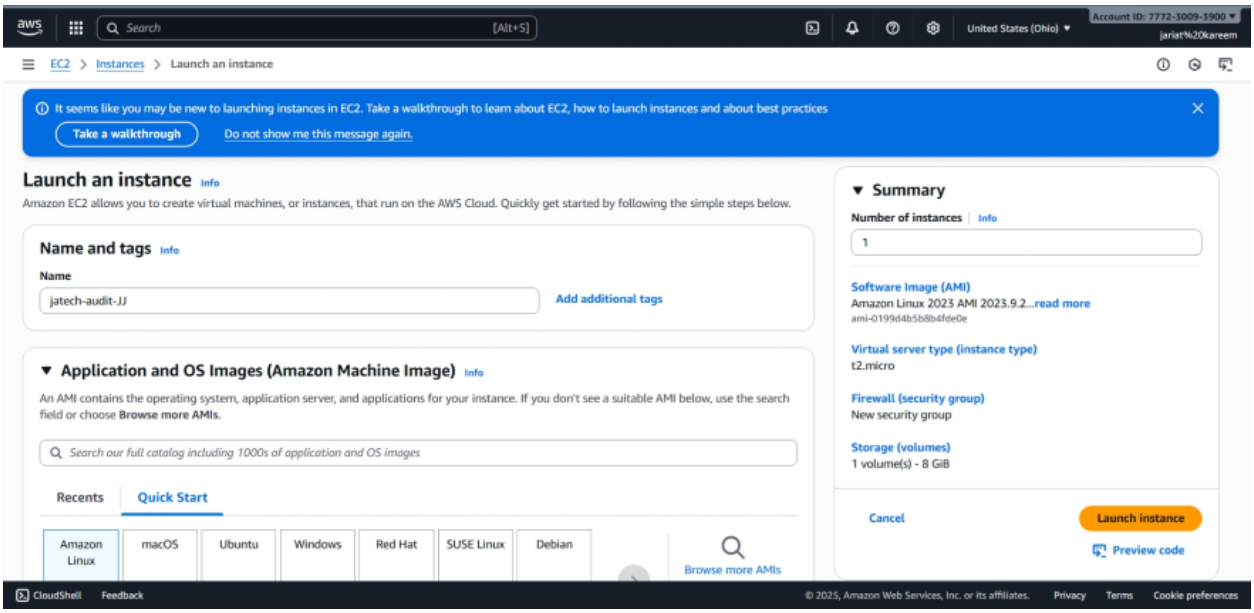
Results & Impact

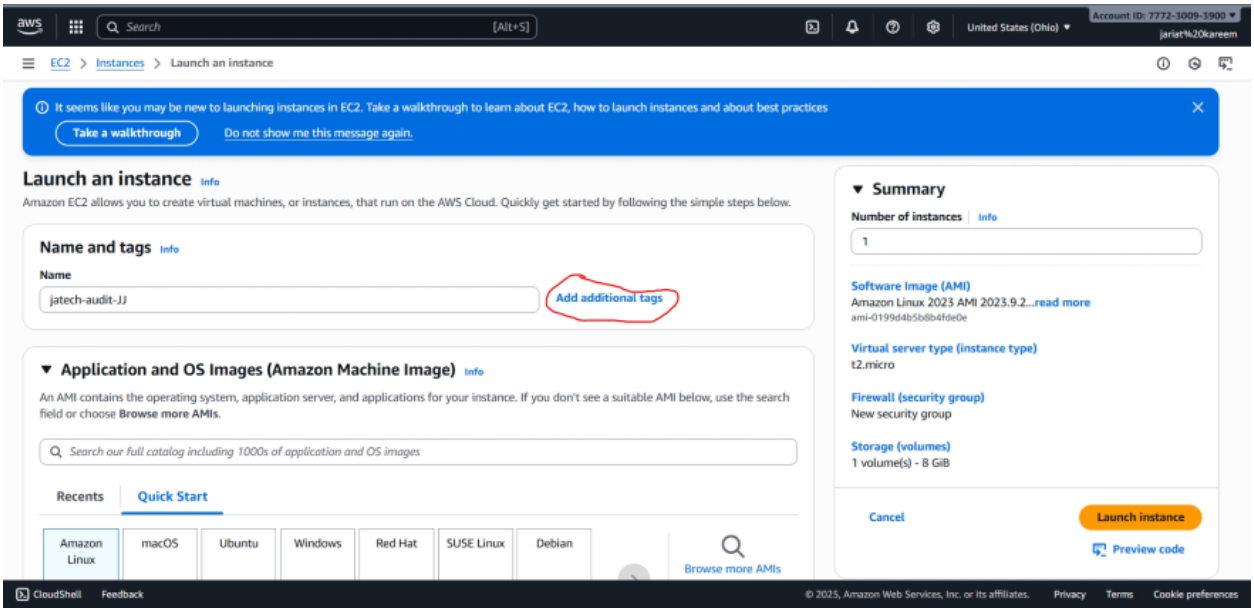
- Achieved **100% compliance** with least-privilege principles.
- Prevented unauthorized access to EC2 instances.
- Improved overall security posture of the AWS environment.
- Demonstrated practical skills in IAM, EC2, and cloud security best practices.

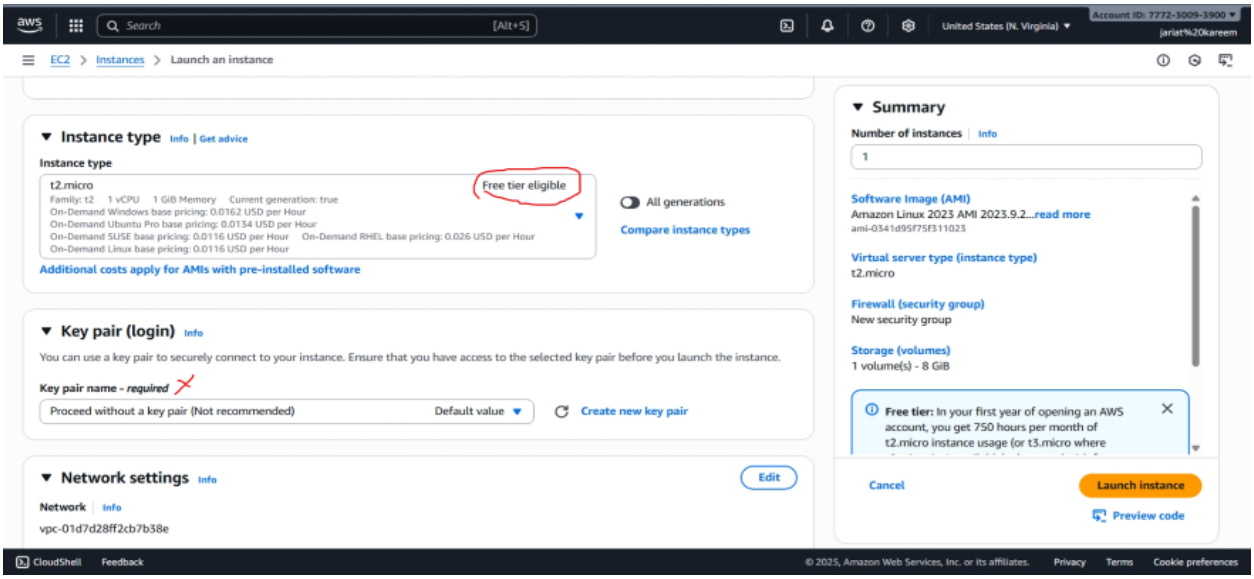
CREATING EC2 INSTANCES

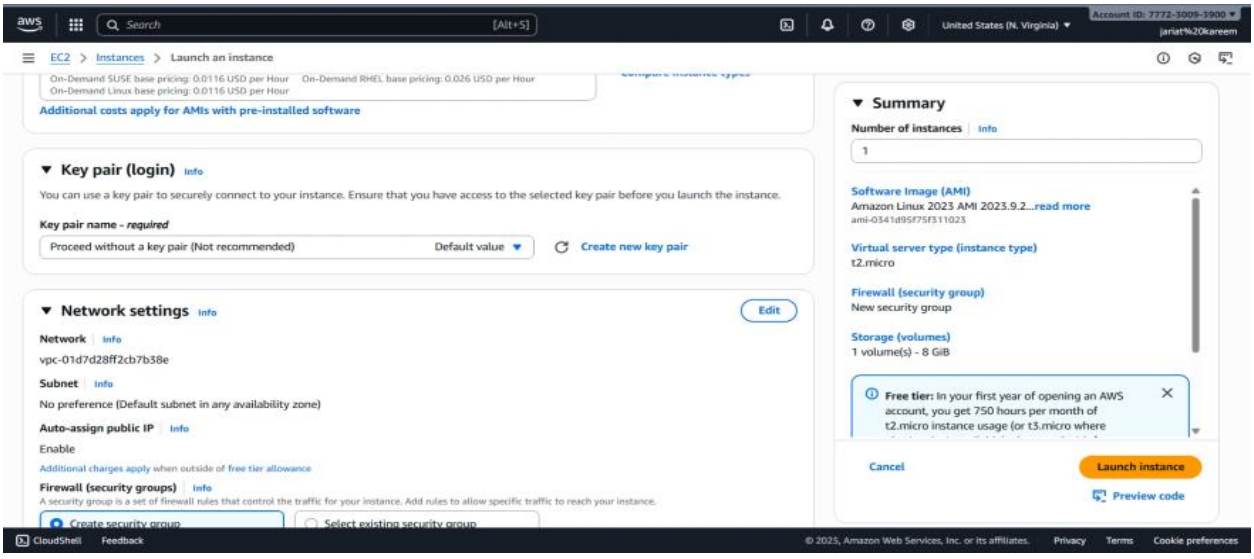


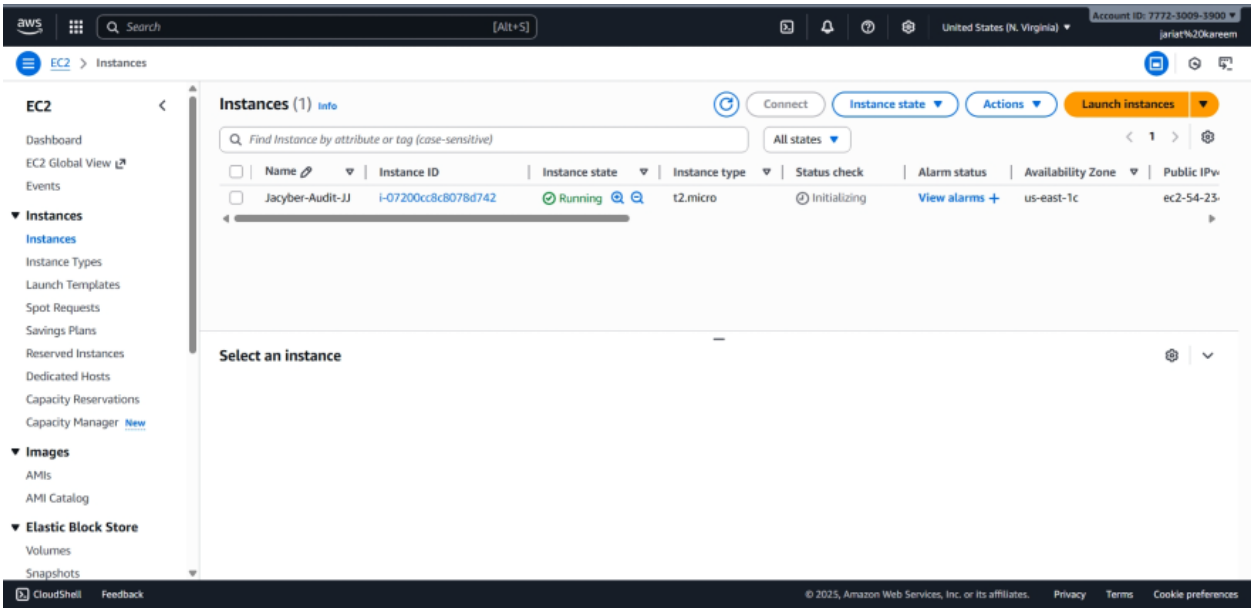


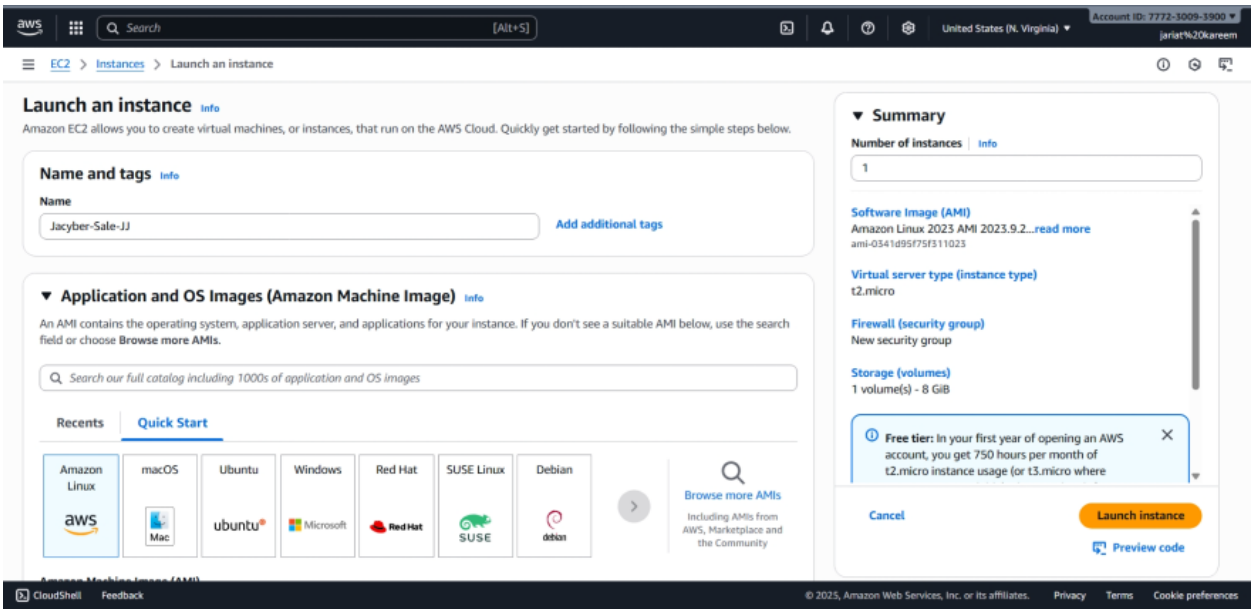

Search [Alt+S]
United States (Ohio)
Account ID: 7772-3009-3900
jariat%20kareem
EC2 > Instances > Launch an instance
It seems like you may be new to launching instances in EC2. Take a walkthrough to learn about EC2, how to launch instances and about best practices
Take a walkthrough
Do not show me this message again.
Launch an instance Info
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 Info
Name
jatech-audit-JJ
Add additional tags
Application and OS Images (Amazon Machine Image) Info
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 Info
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

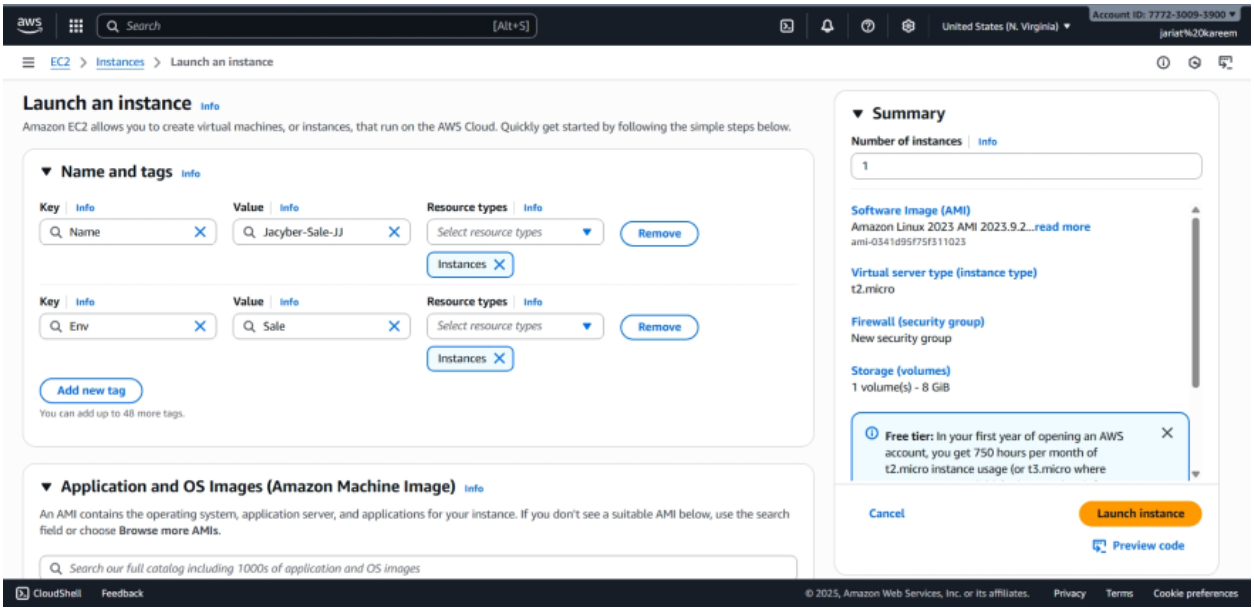

Search [Alt+S]
United States (Ohio)
Account ID: 7772-3009-3900
jariat%20kareem
EC2 > Instances > Launch an instance
It seems like you may be new to launching instances in EC2. Take a walkthrough to learn about EC2, how to launch instances and about best practices
Take a walkthrough
Do not show me this message again.
Launch an instance Info
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 Info
Name
jatech-audit-JJ
Add additional tags
Application and OS Images (Amazon Machine Image) Info
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 Info
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

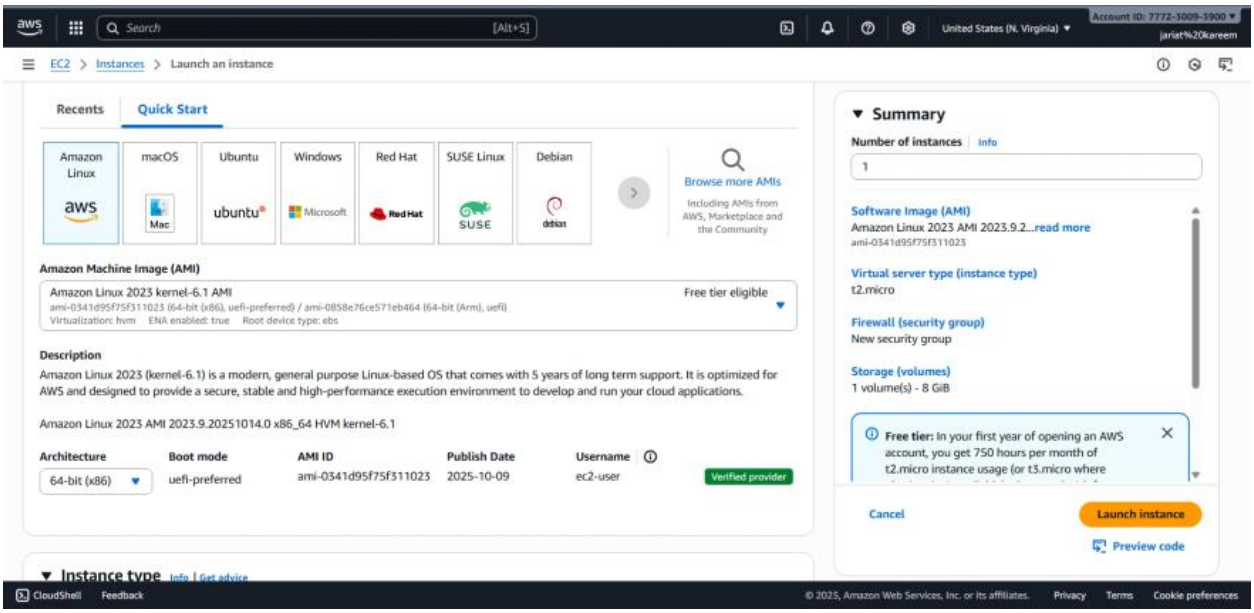

Search
[Alt+S]
United States (N. Virginia)
Account ID: 7772-3009-3900
jariat%20kareem
EC2 > Instances > Launch an instance
Instance type Info | Get advice
Instance type
t2.micro
Free tier eligible
Family: t2 1 vCPU 1 GiB Memory Current generation: true
On-Demand Windows base pricing: 0.0162 USD per Hour
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
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
Proceed without a key pair (Not recommended)
Default value
Create new key pair
Network settings Info
Edit
Network Info
vpc-01d7d28ff2cb7b38e
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

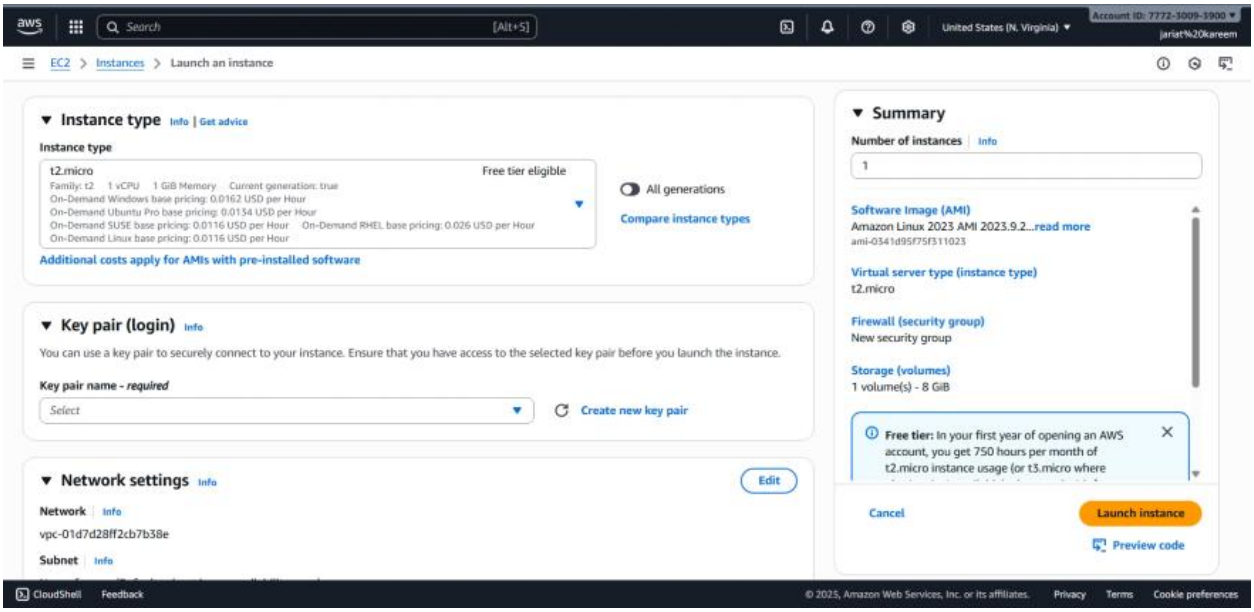

Search
[Alt+S]
United States (N. Virginia)
EC2 > Instances > Launch an instance
Additional costs apply for AMIs with pre-installed software
Key pair (login) Info
You can use a key pair to securely connect to your instance. Ensure that you have access to the selected key pair before you launch the instance.
Key pair name - required
Proceed without a key pair (Not recommended)
Default value
Create new key pair
Network settings Info
Edit
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 group
Select 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
Cancel
Launch instance
Preview code
CloudShell
Feedback
© 2025, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences

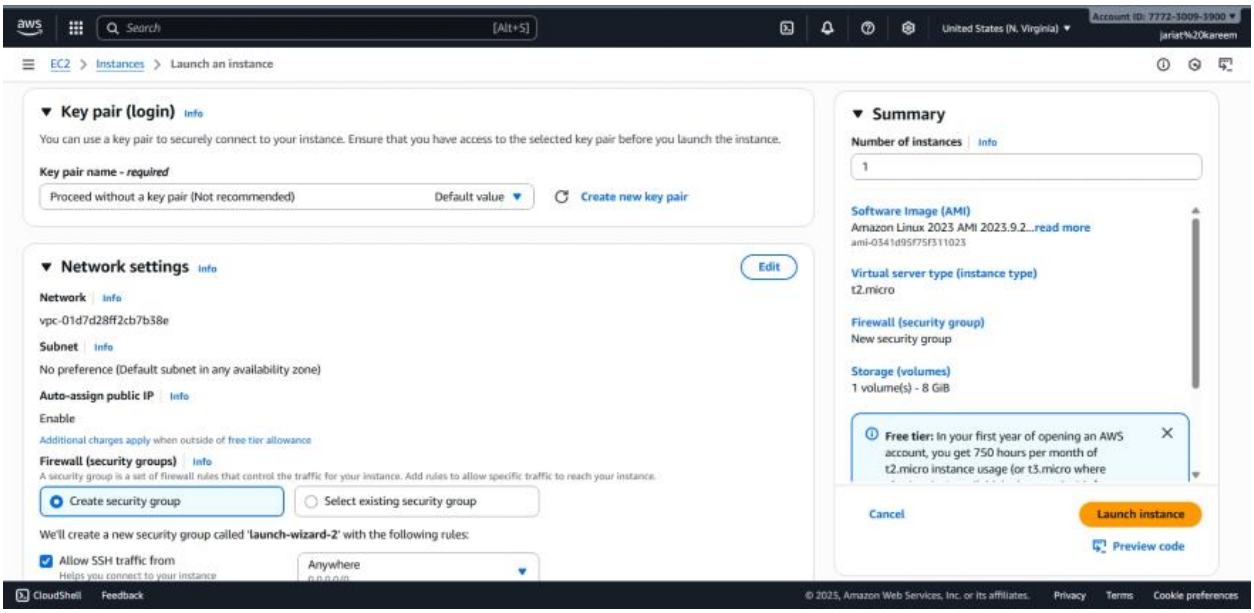

Search
[Alt+S]
United States (N. Virginia)
EC2 > Instances
EC2
Dashboard
EC2 Global View
Events
Instances
Instances
Instance Types
Launch Templates
Spot Requests
Savings Plans
Reserved Instances
Dedicated Hosts
Capacity Reservations
Capacity Manager New
Images
AMIs
AMI Catalog
Elastic Block Store
Volumes
Snapshots
Instances (1) Info
Connect
Instance state
Actions
Launch instances
Find Instance by attribute or tag (case-sensitive)
All states
Name
Instance ID
Instance state
Instance type
Status check
Alarm status
Availability Zone
Public IPv
Jacyber-Audit-JJ
i-07200cc8c8078d742
Running
t2.micro
Initializing
View alarms +
us-east-1c
ec2-54-23-
Select an instance
CloudShell
Feedback
© 2025, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences

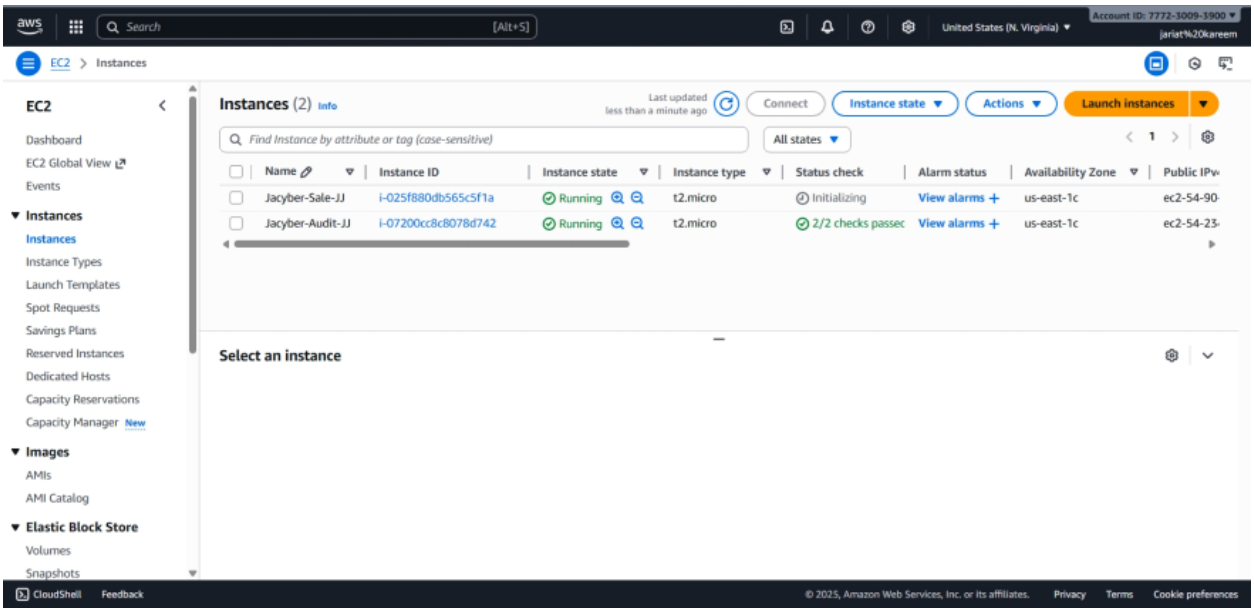

Search [Alt+S]
United States (N. Virginia)
Account ID: 7772-3009-3900
jariat%20kareem
EC2 > Instances > Launch an instance
Launch an instance Info
Amazon EC2 allows you to create virtual machines, or instances, that run on the AWS Cloud. Quickly get started by following the simple steps below.
Name and tags Info
Name
Jacyber-Sale-JJ
Add additional tags
Application and OS Images (Amazon Machine Image) Info
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 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


Search [Alt+S]
United States (N. Virginia)
Account ID: 7772-3009-3900
jariat%20kareem
EC2 > Instances > Launch an instance
Launch an instance Info
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 Info
Key Info
Name
Value Info
Jacyber-Sale-JJ
Resource types Info
Select resource types
Instances
Remove
Key Info
Env
Value Info
Sale
Resource types Info
Select resource types
Instances
Remove
Add new tag
You can add up to 48 more tags.
Application and OS Images (Amazon Machine Image) Info
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 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


Search [Alt+S]
United States (N. Virginia)
Account ID: 7772-3009-3900
jariat%20kareem
EC2 > Instances > Launch an instance
Recents
Quick Start
Amazon Linux
macOS
Ubuntu
Windows
Red Hat
SUSE Linux
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-0858e76ce571eb464 (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
Boot mode
AMI ID
Publish Date
Username
64-bit (x86)
uefi-preferred
ami-0341d95f75f311023
2025-10-09
ec2-user
Verified provider
Instance type Info | Get advice
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

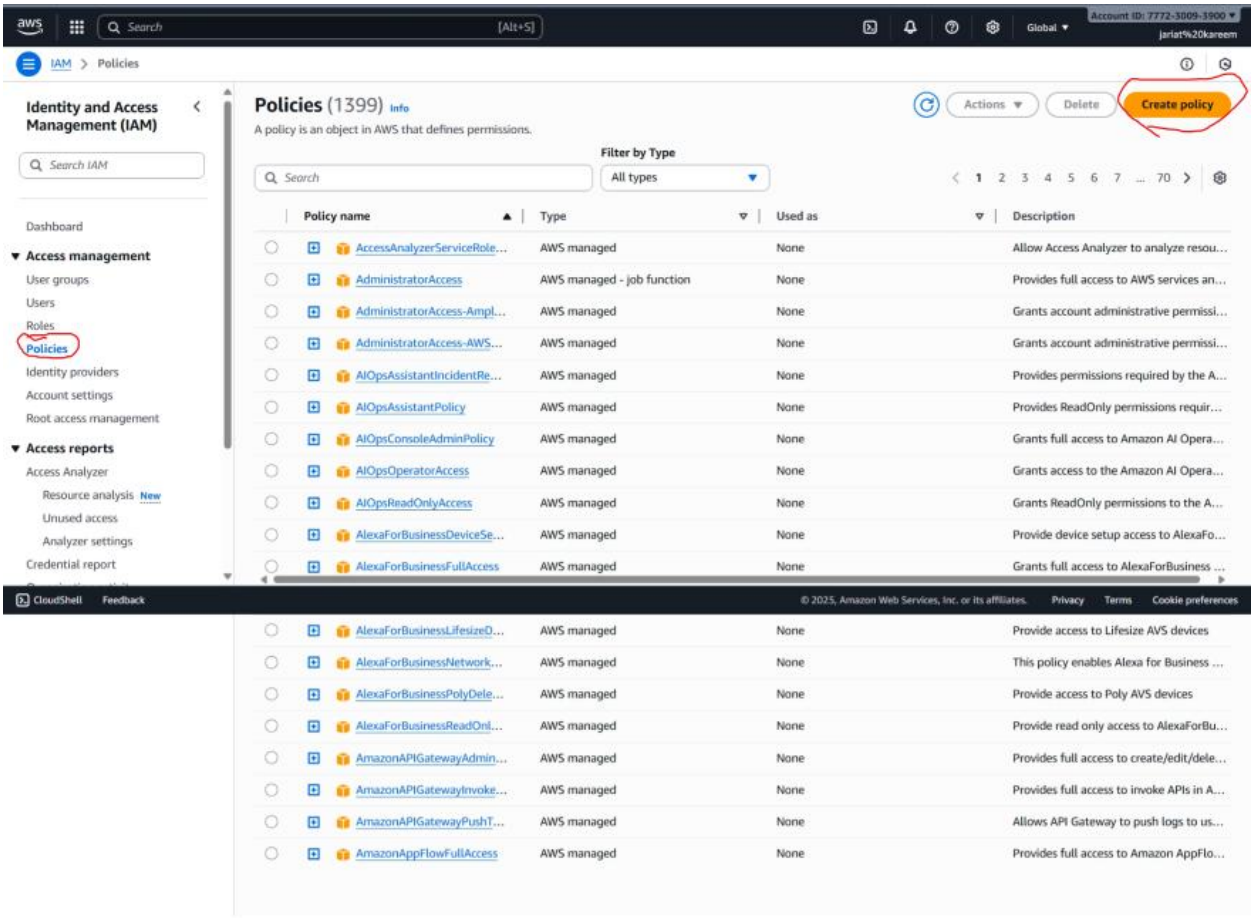

Search [Alt+S]
United States (N. Virginia)
Account ID: 7772-3009-3900
jariat%20kareem
EC2 > Instances > Launch an instance
Instance type Info | Get advice
Instance type
t2.micro
Free tier eligible
Family: t2 1 vCPU 1 GiB Memory Current generation: true
On-Demand Windows base pricing: 0.0162 USD per Hour
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
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
Edit
Network Info
vpc-01d7d28ff2cb7b38e
Subnet Info
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

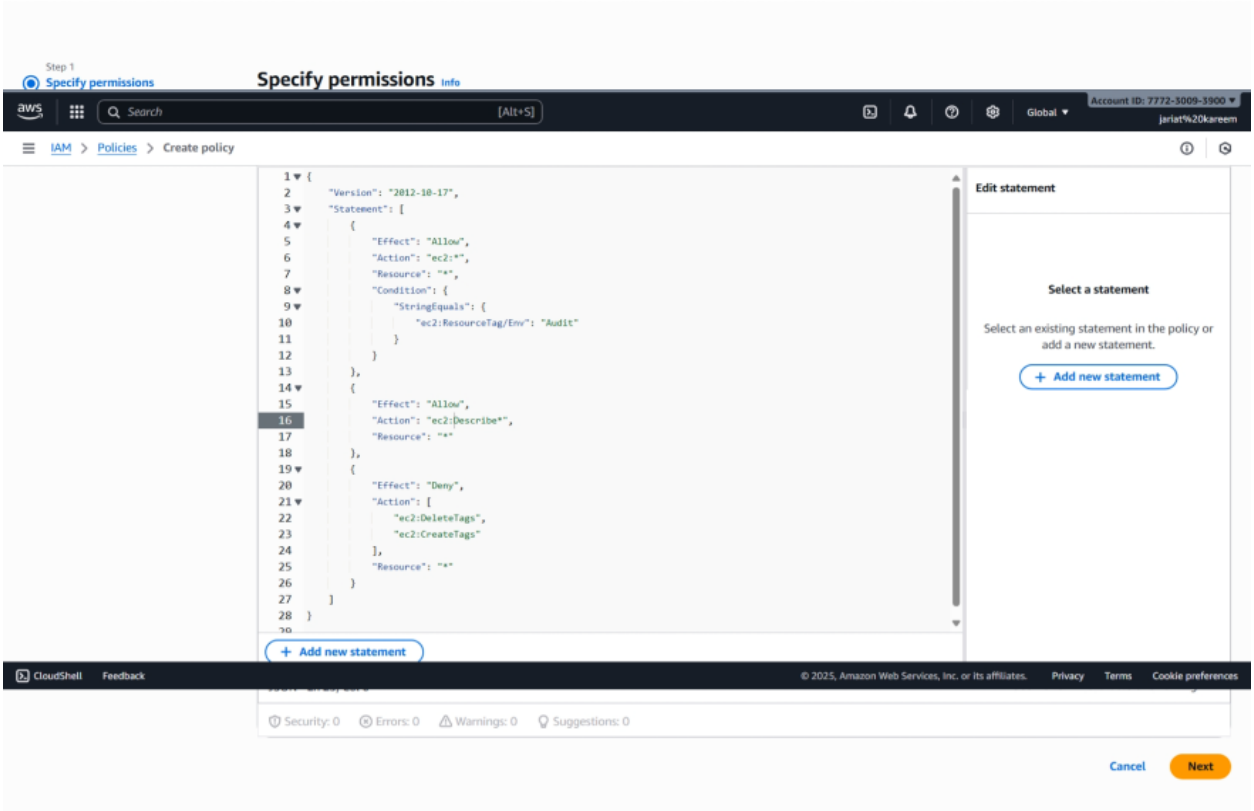


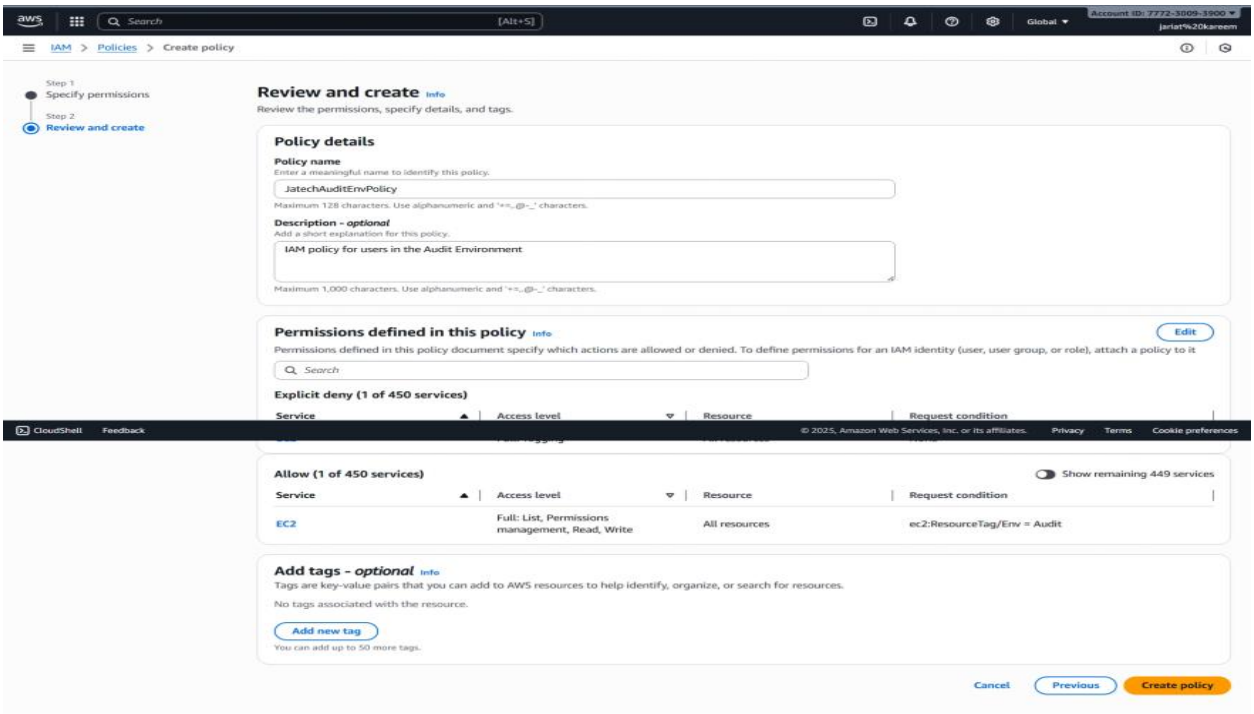


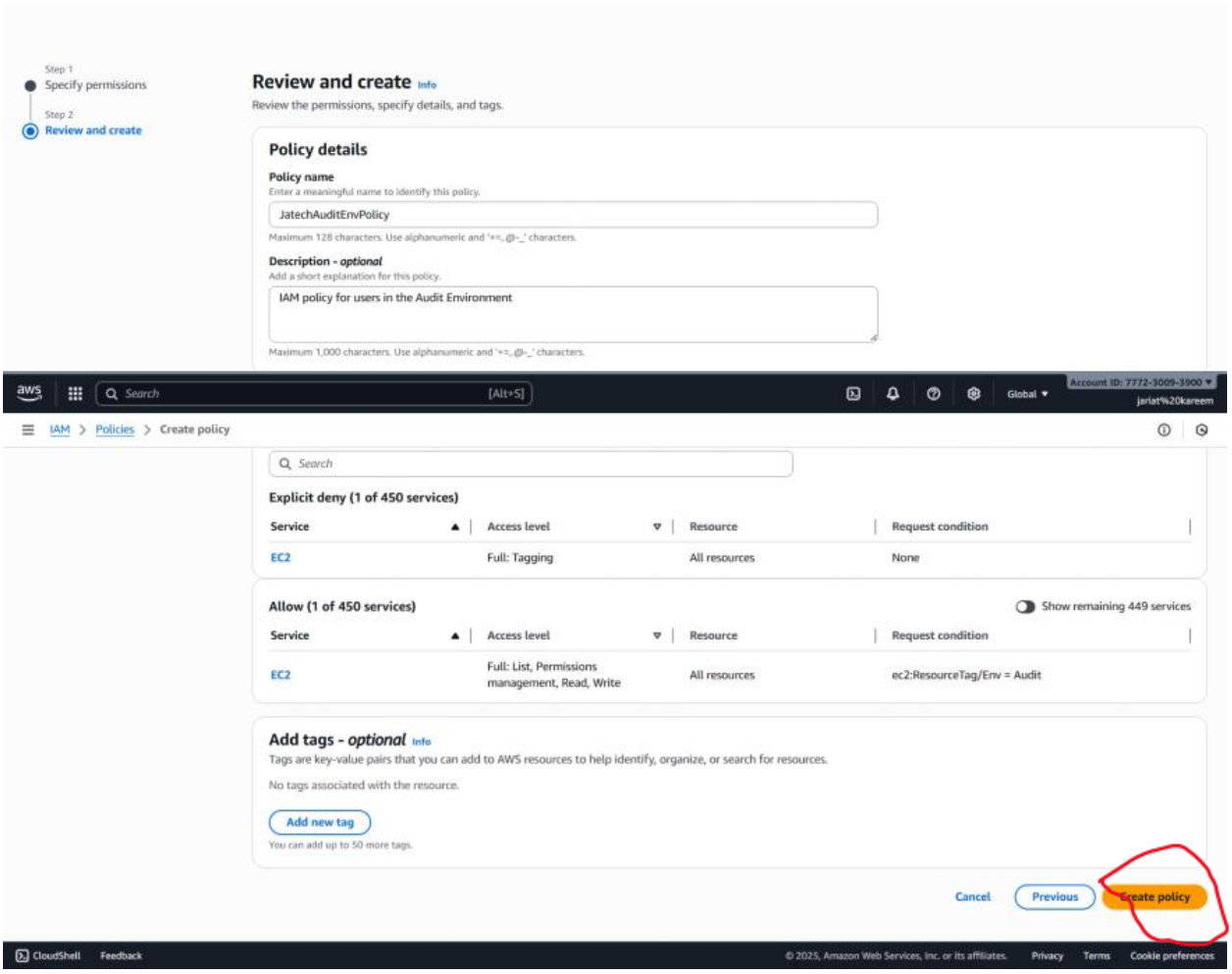
Creating the IAM policy

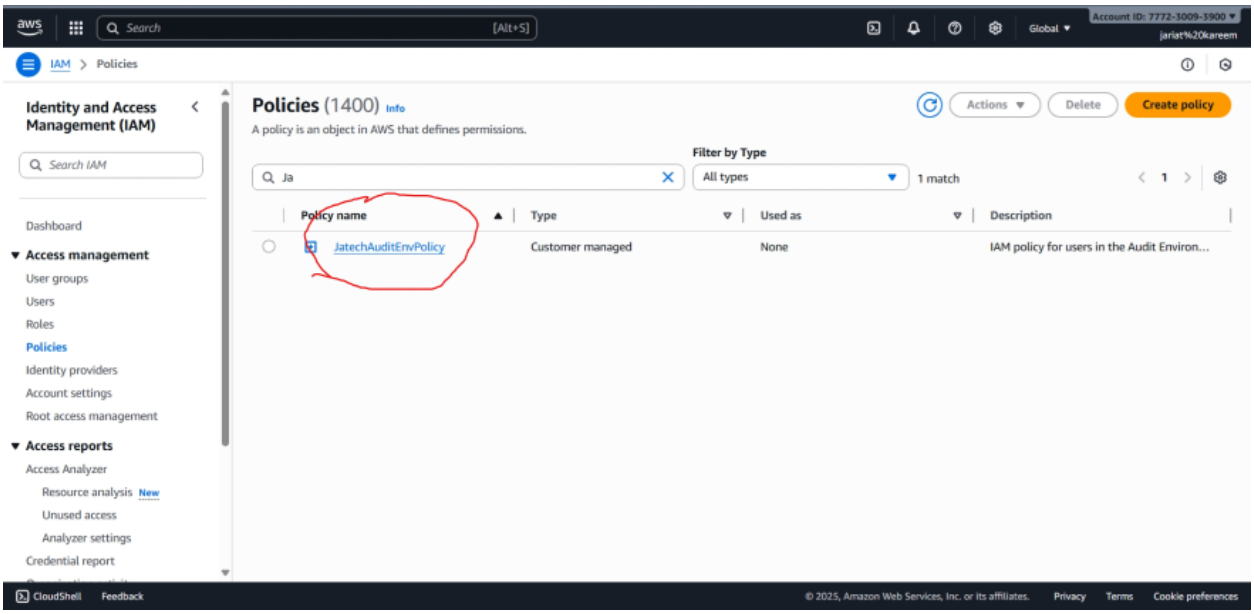
I Authored a custom AWS IAM policy to enforce least-privilege access by explicitly blocking start/stop actions on the Audit EC2 instance while permitting those actions on the Sales EC2 instance. This policy ensured operational control was limited to designated resources, aligning with cloud security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


Search [Alt+S]
Global
Account ID: 7772-3009-3900
jariat%20kareem
IAM > Policies
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
Policies (1399) Info
A policy is an object in AWS that defines permissions.
Actions
Delete
Create policy
Filter by Type
Search
All types
1 2 3 4 5 6 7 ... 70
Policy name
Type
Used as
Description
AccessAnalyzerServiceRole... AWS managed None Allow Access Analyzer to analyze resou...
AdministratorAccess AWS managed - job function None Provides full access to AWS services an...
AdministratorAccess-Ampl... AWS managed None Grants account administrative permissi...
AdministratorAccess-AWS... AWS managed None Grants account administrative permissi...
AIOpsAssistantIncidentRe... AWS managed None Provides permissions required by the A...
AIOpsAssistantPolicy AWS managed None Provides ReadOnly permissions requir...
AIOpsConsoleAdminPolicy AWS managed None Grants full access to Amazon AI Opera...
AIOpsOperatorAccess AWS managed None Grants access to the Amazon AI Opera...
AIOpsReadOnlyAccess AWS managed None Grants ReadOnly permissions to the A...
AlexaForBusinessDeviceSe... AWS managed None Provide device setup access to AlexaFo...
AlexaForBusinessFullAccess AWS managed None Grants full access to AlexaForBusiness ...
CloudShell Feedback
© 2025, Amazon Web Services, Inc. or its affiliates. Privacy Terms Cookie preferences
AlexaForBusinessLifesizeD... AWS managed None Provide access to Lifesize AVS devices
AlexaForBusinessNetwork... AWS managed None This policy enables Alexa for Business ...
AlexaForBusinessPolyDele... AWS managed None Provide access to Poly AVS devices
AlexaForBusinessReadOnl... AWS managed None Provide read only access to AlexaForBu...
AmazonAPIGatewayAdmin... AWS managed None Provides full access to create/edit/dele...
AmazonAPIGatewayInvoke... AWS managed None Provides full access to invoke APIs in A...
AmazonAPIGatewayPushT... AWS managed None Allows API Gateway to push logs to us...
AmazonAppFlowFullAccess AWS managed None Provides full access to Amazon AppFlo...

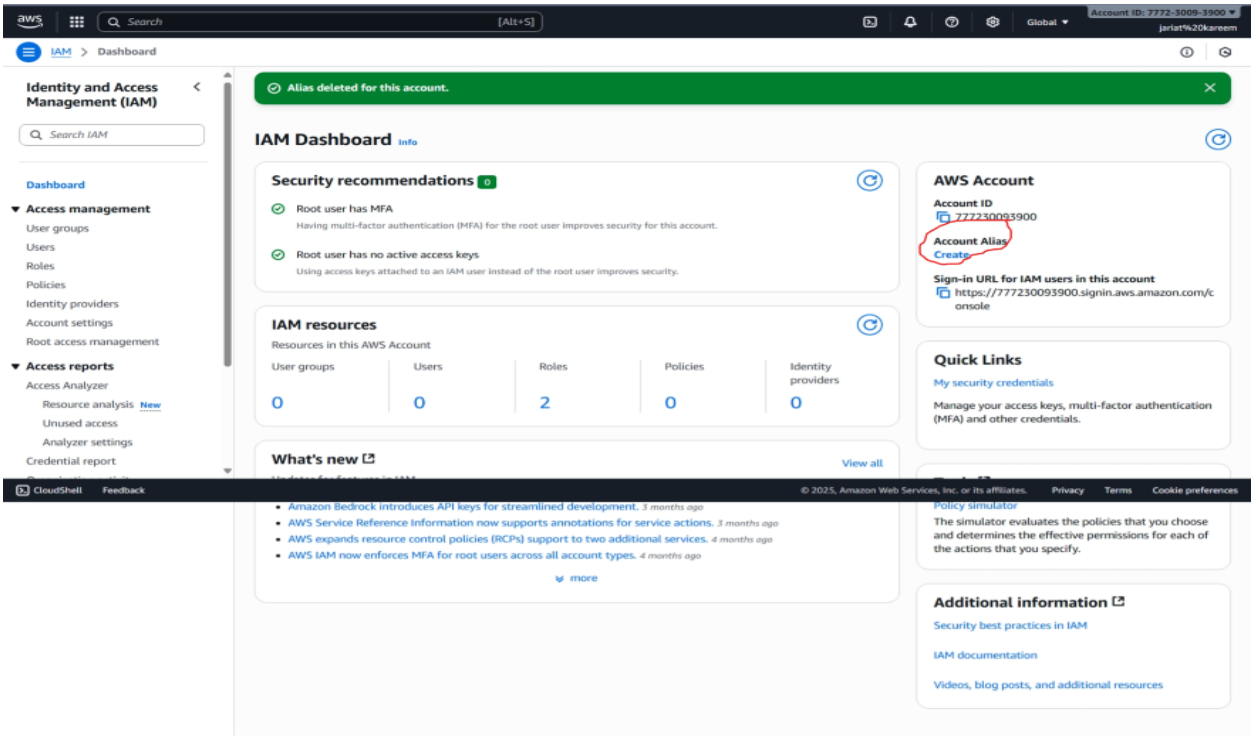

Step 1
Specify permissions
Specify permissions Info
Search
[Alt+S]
Global
Account ID: 7772-3009-3900
jariat%20kareem
IAM > Policies > Create policy
{
"Version": "2012-10-17",
"Statement": [
{
"Effect": "Allow",
"Action": "ec2:*",
"Resource": "*",
"Condition": {
"StringEquals": {
"ec2:ResourceTag/Env": "Audit"
}
}
},
{
"Effect": "Allow",
"Action": "ec2:Describe*",
"Resource": "*"
},
{
"Effect": "Deny",
"Action": [
"ec2:DeleteTags",
"ec2:CreateTags"
],
"Resource": "*"
}
]
}
Edit statement
Select a statement
Select an existing statement in the policy or add a new statement.
+ Add new statement
+ Add new statement
CloudShell
Feedback
© 2025, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences
Security: 0
Errors: 0
Warnings: 0
Suggestions: 0
Cancel
Next

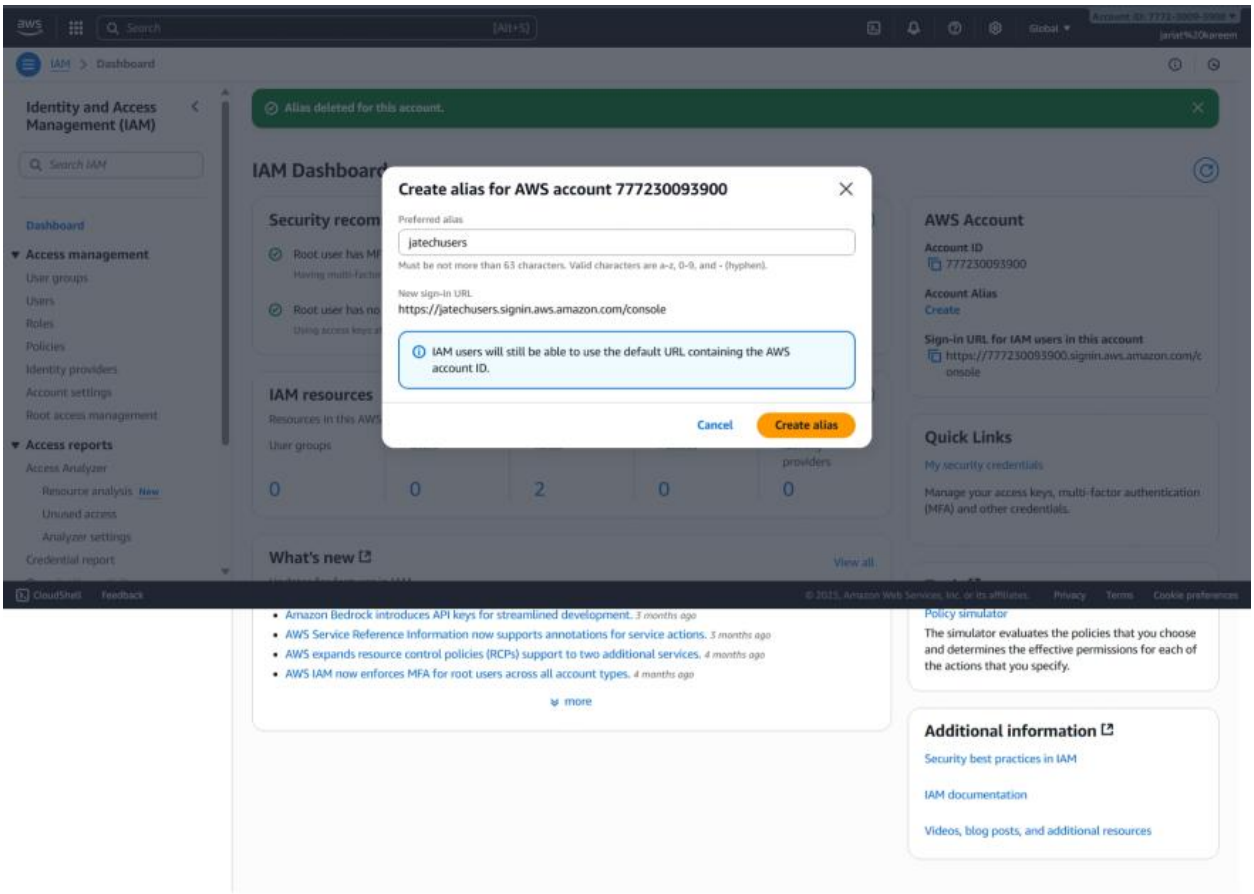

Search
[Alt+S]
Global
Account ID: 7772-3009-3900
jariat%20kareem
IAM > Policies > Create policy
Step 1
Specify permissions
Step 2
Review and create
Review and create Info
Review the permissions, specify details, and tags.
Policy details
Policy name
Enter a meaningful name to identify this policy.
JatechAuditEnvPolicy
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.
Permissions defined in this policy Info
Edit
Permissions defined in this policy document specify which actions are allowed or denied. To define permissions for an IAM identity (user, user group, or role), attach a policy to it
Search
Explicit deny (1 of 450 services)
Service
Access level
Resource
Request condition
CloudShell
Feedback
© 2025, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences
Allow (1 of 450 services)
Show remaining 449 services
Service
Access level
Resource
Request condition
EC2
Full: List, Permissions management, Read, Write
All resources
ec2:ResourceTag/Env = Audit
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.
Cancel
Previous
Create policy


Step 1
Specify permissions
Step 2
Review and create
Review and create Info
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.
Search
[Alt+S]
Global
Account ID: 7772-3009-3900
jariat%20kareem
IAM > Policies > Create policy
Search
Explicit deny (1 of 450 services)
Service
Access level
Resource
Request condition
EC2
Full: Tagging
All resources
None
Allow (1 of 450 services)
Show remaining 449 services
Service
Access level
Resource
Request condition
EC2
Full: List, Permissions management, Read, Write
All resources
ec2:ResourceTag/Env = Audit
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.
Cancel
Previous
Create policy
CloudShell
Feedback
© 2025, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences

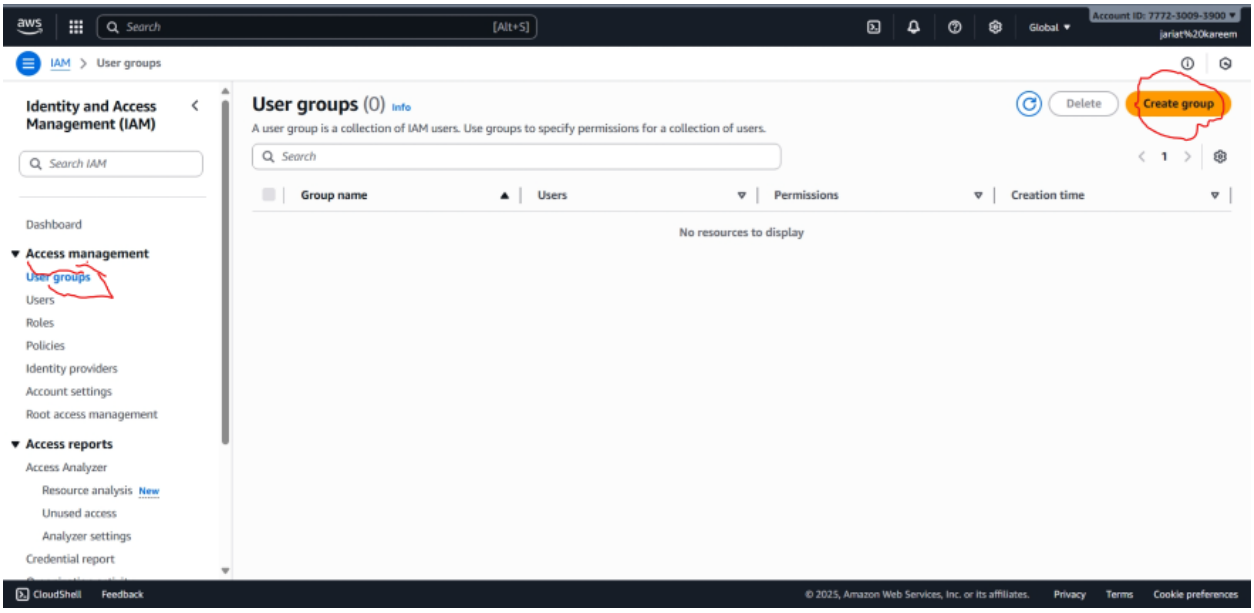

Search
[Alt+S]
Global
Account ID: 7772-3009-3900
jariat%20kareem
IAM > Policies
Identity and Access Management (IAM)
Search IAM
Dashboard
Access management
User groups
Users
Roles
Policies
Identity providers
Account settings
Root access management
Access reports
Access Analyzer
Resource analysis New
Unused access
Analyzer settings
Credential report
Policies (1400) Info
A policy is an object in AWS that defines permissions.
Actions
Delete
Create policy
Filter by Type
Ja
All types
1 match
1
Policy name
Type
Used as
Description
JatechAuditEnvPolicy
Customer managed
None
IAM policy for users in the Audit Environ...
CloudShell
Feedback
© 2025, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences

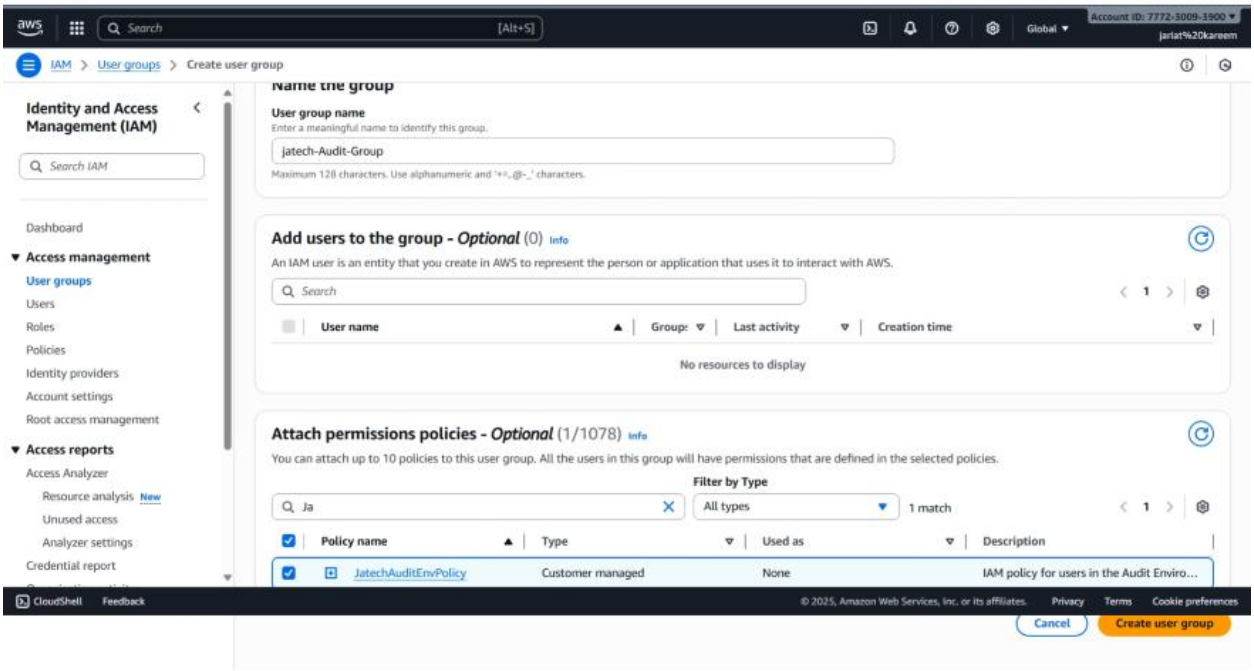
Account Alias

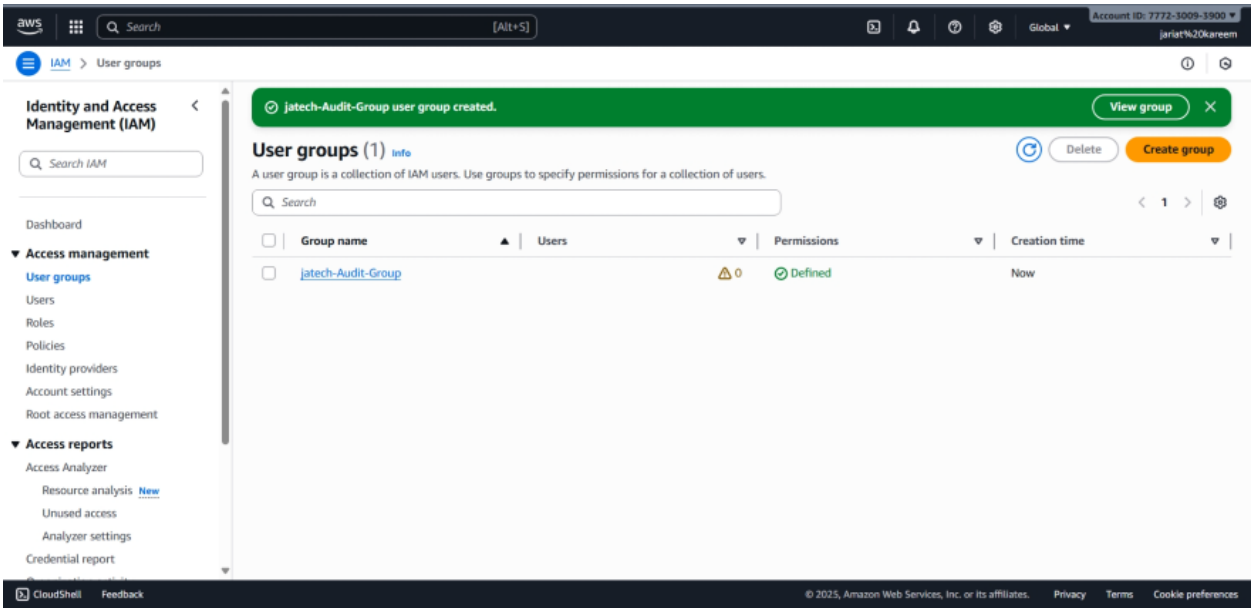


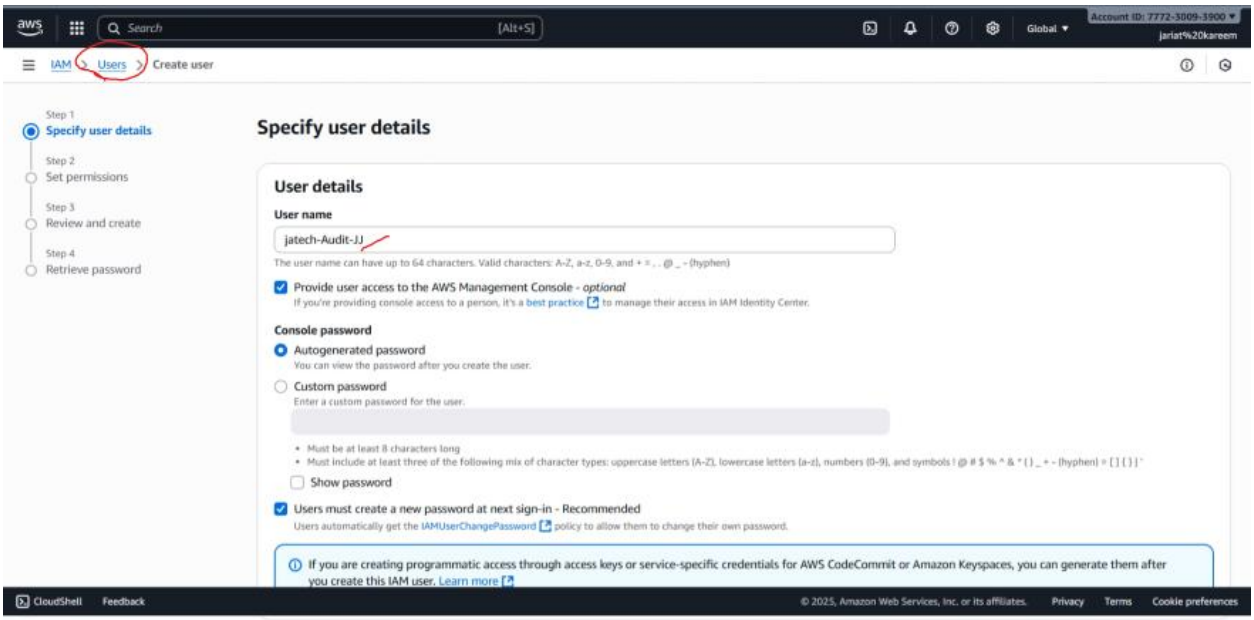


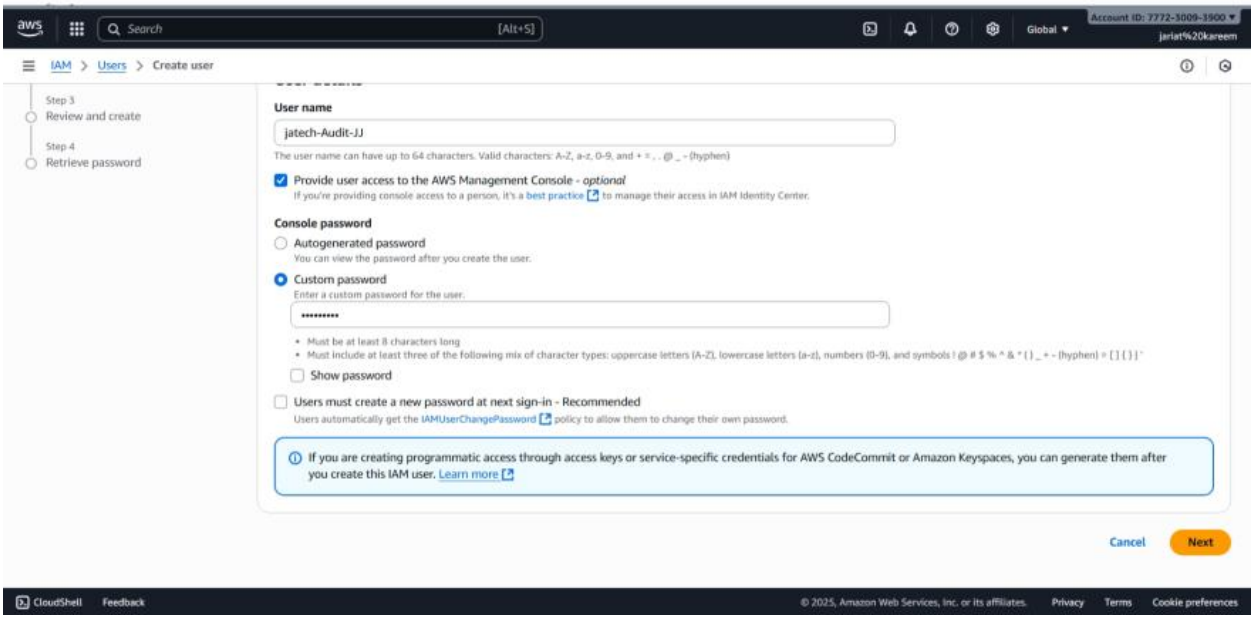
IAM Users and Group

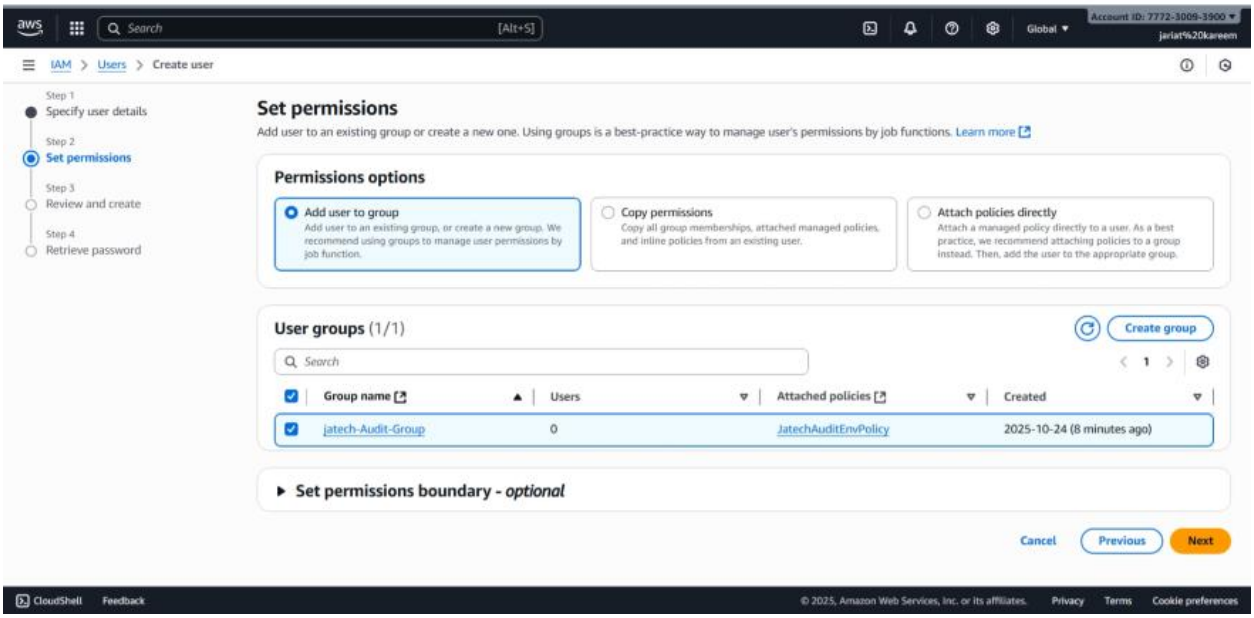


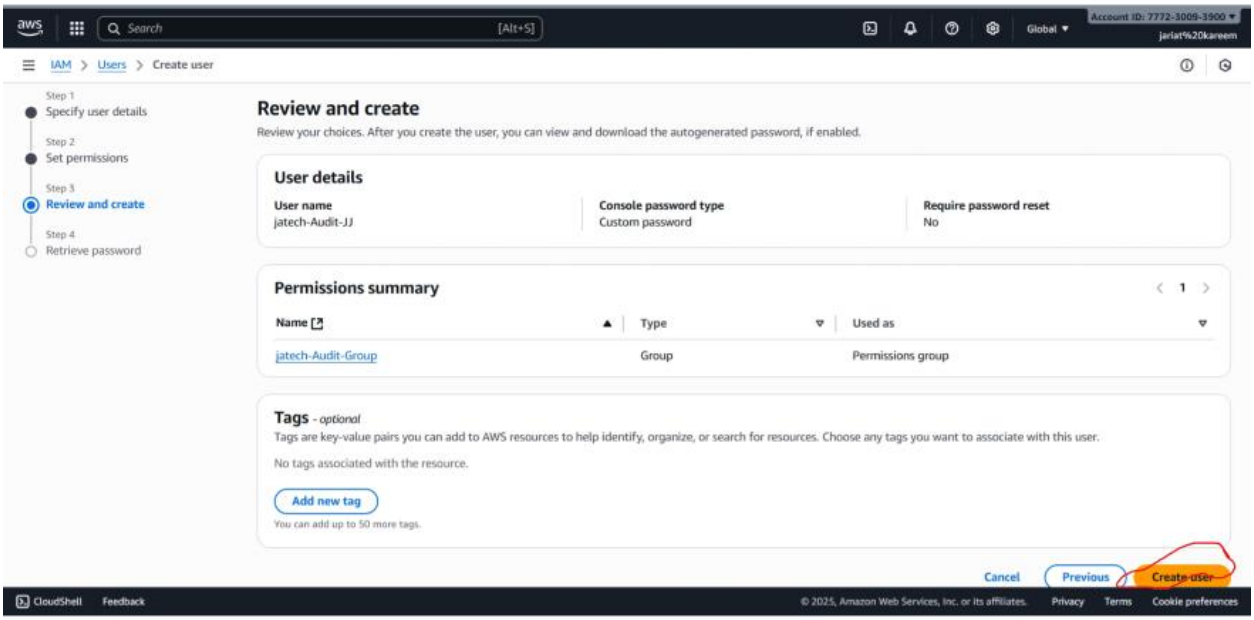

Search
[Alt+S]
Global
Account ID: 7772-3009-3900
jariat%20kareem
IAM > User groups > Create user group
Identity and Access Management (IAM)
Search IAM
Dashboard
Access management
User groups
Users
Roles
Policies
Identity providers
Account settings
Root access management
Access reports
Access Analyzer
Resource analysis New
Unused access
Analyzer settings
Credential report
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) Info
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
User name
Groups
Last activity
Creation time
No resources to display
Attach permissions policies - Optional (1/1078) Info
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
Policy name
Type
Used as
Description
JatechAuditEnvPolicy
Customer managed
None
IAM 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

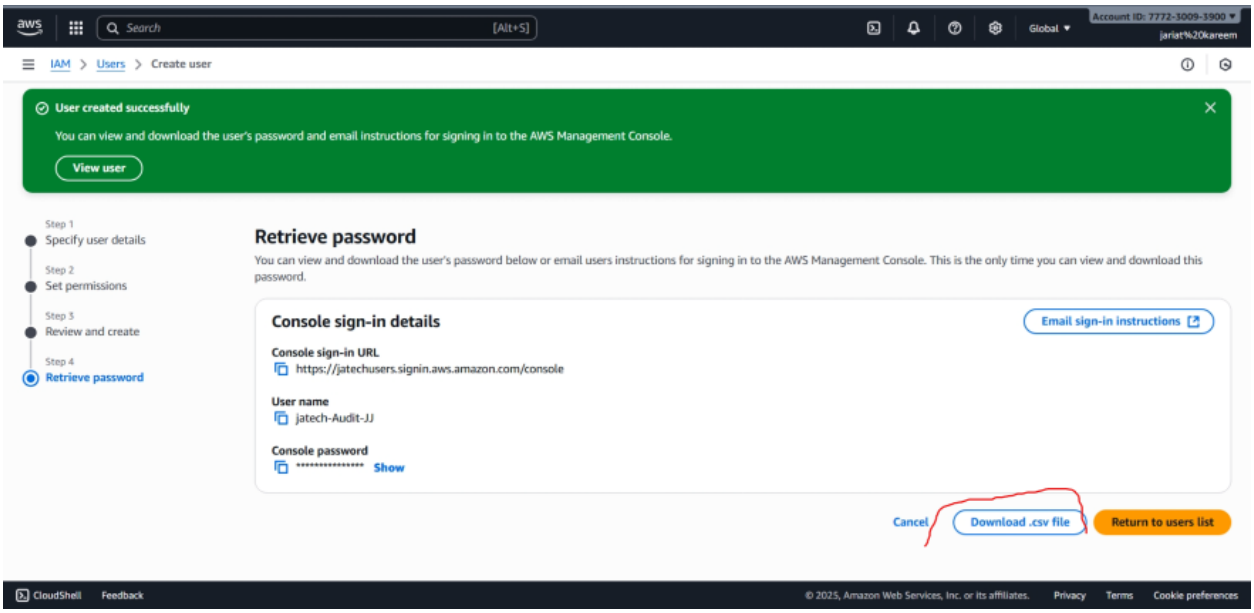

Search
[Alt+S]
Global
Account ID: 7772-3009-3900
jariat%20kareem
IAM > User groups
Identity and Access Management (IAM)
Search IAM
Dashboard
Access management
User groups
Users
Roles
Policies
Identity providers
Account settings
Root access management
Access reports
Access Analyzer
Resource analysis New
Unused access
Analyzer settings
Credential report
jatech-Audit-Group user group created.
View group
User groups (1) Info
A user group is a collection of IAM users. Use groups to specify permissions for a collection of users.
Delete
Create group
Search
Group name
Users
Permissions
Creation time
jatech-Audit-Group
0
Defined
Now
CloudShell
Feedback
© 2025, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences

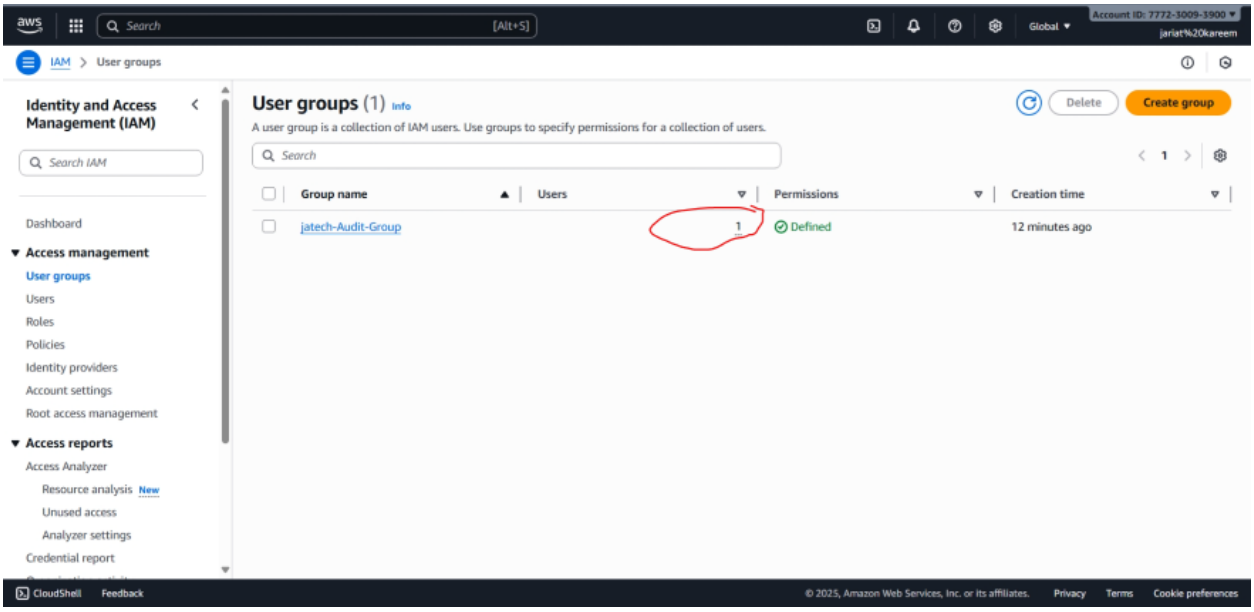

Search
[Alt+S]
Global
Account ID: 7772-3009-3900
jariat%20kareem
IAM > Users > Create user
Step 1
Specify user details
Step 2
Set permissions
Step 3
Review and create
Step 4
Retrieve password
Specify user details
User details
User name
jatech-Audit-JJ
The user name can have up to 64 characters. Valid 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


Search
[Alt+S]
Global
Account ID: 7772-3009-3900
jariat%20kareem
IAM > Users > Create user
Step 3
Review and create
Step 4
Retrieve password
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

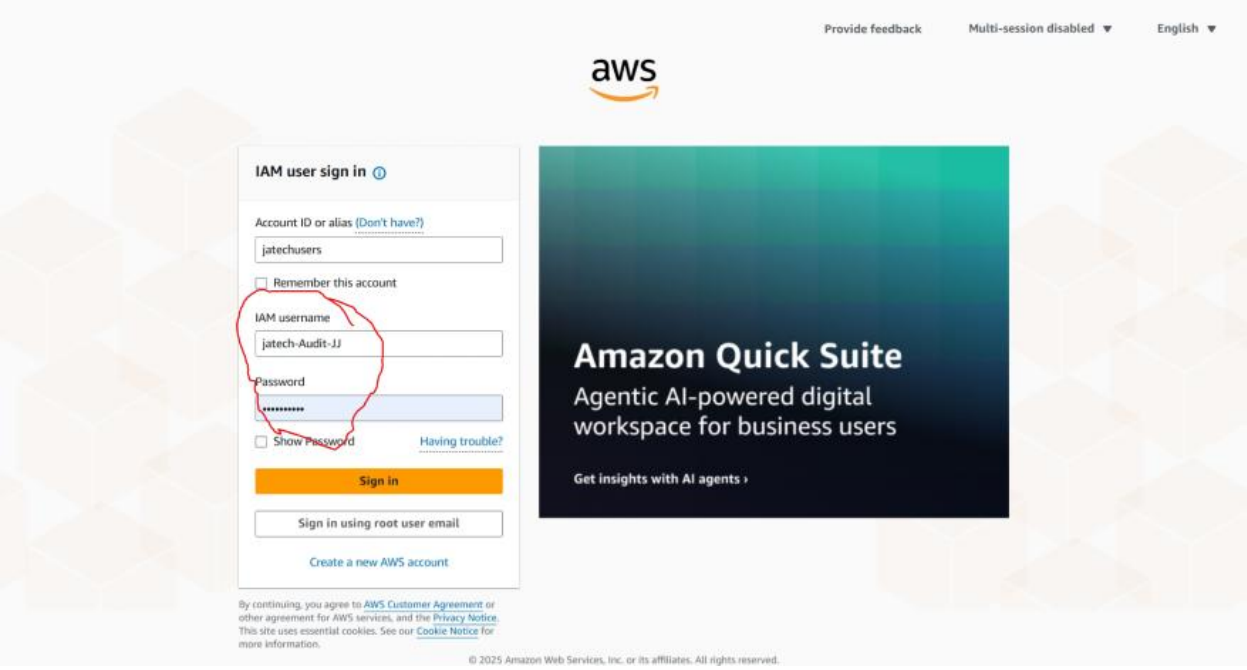

Search [Alt+S]
Global
Account ID: 7772-3009-3900
jariat%20kareem
IAM > Users > Create user
Step 1
Specify user details
Step 2
Set permissions
Step 3
Review and create
Step 4
Retrieve password
Set permissions
Add user to an existing group or create a new one. Using groups is a best-practice way to manage 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)
Create group
Search
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

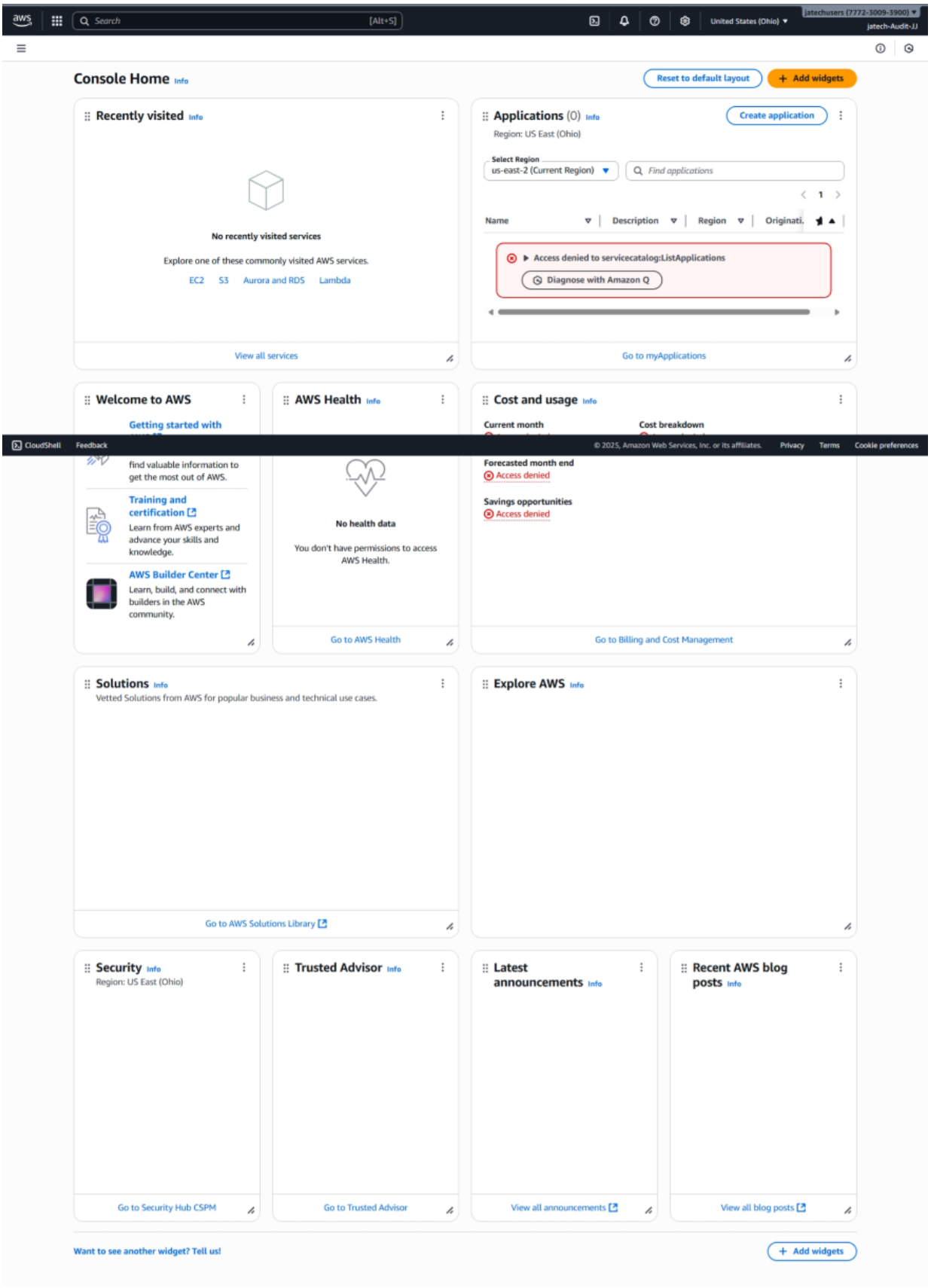

Search [Alt+S]
Global
Account ID: 7772-3009-3900
jariat%20kareem
IAM > Users > Create user
Step 1
Specify user details
Step 2
Set permissions
Step 3
Review and create
Step 4
Retrieve password
Review and create
Review your choices. After you create the user, you can view and download the autogenerated password, if enabled.
User details
User name
jatech-Audit-JJ
Console password type
Custom password
Require password reset
No
Permissions summary
1
Name
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

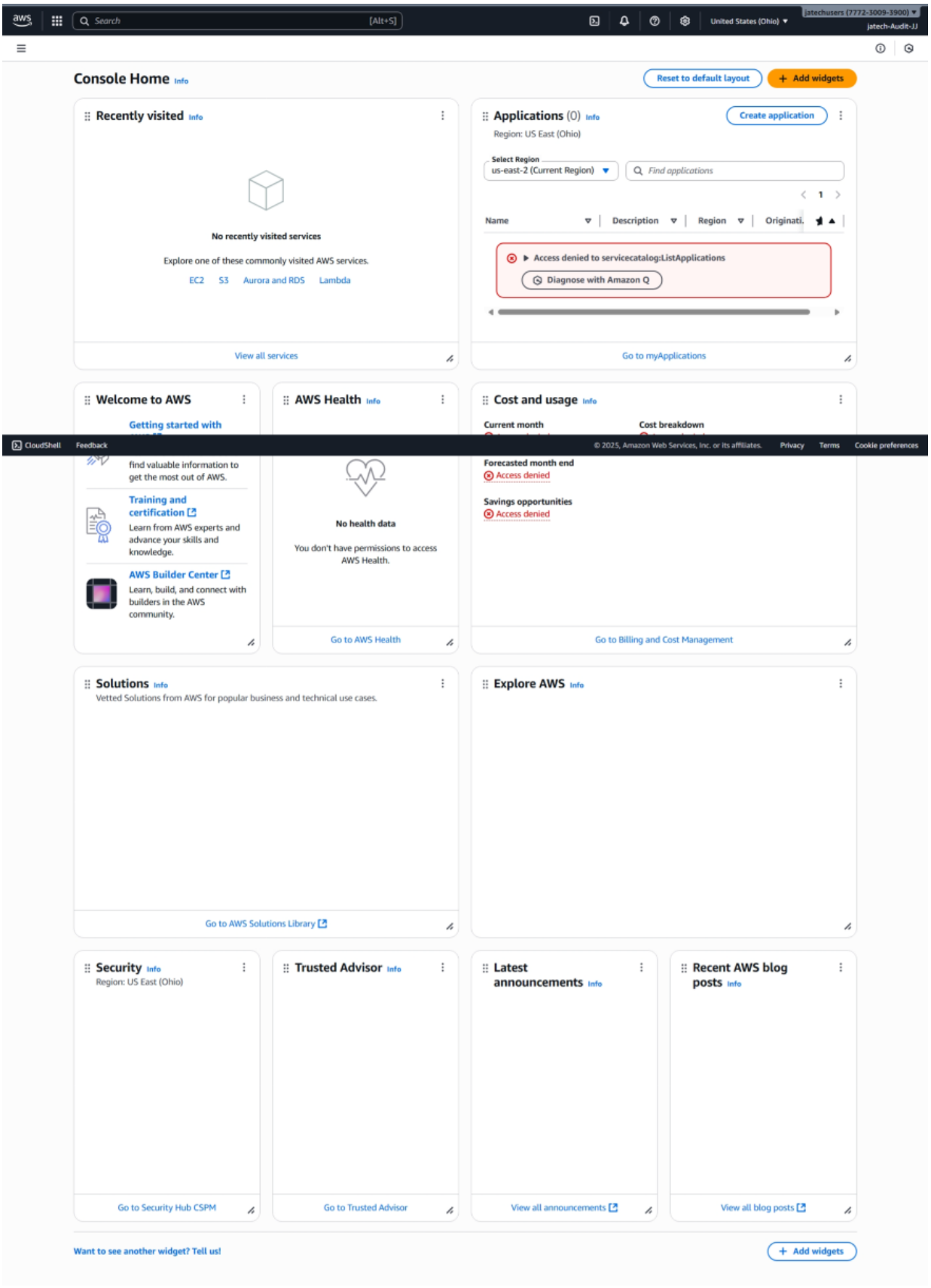

Search
[Alt+S]
Global
Account ID: 7772-3009-3900
jariat%20kareem
IAM > Users > Create user
User created successfully
You can view and download the user's password and email instructions for signing in to the AWS Management Console.
View user
Step 1
Specify user details
Step 2
Set permissions
Step 3
Review 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


Search
[Alt+S]
Global
Account ID: 7772-3009-3900
jariat%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 New
Unused access
Analyzer settings
Credential report
User groups (1) Info
A user group is a collection of IAM users. Use groups to specify permissions for a collection of users.
Delete
Create group
Search
Group name
Users
Permissions
Creation time
jatech-Audit-Group
1
Defined
12 minutes ago
CloudShell
Feedback
© 2025, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences

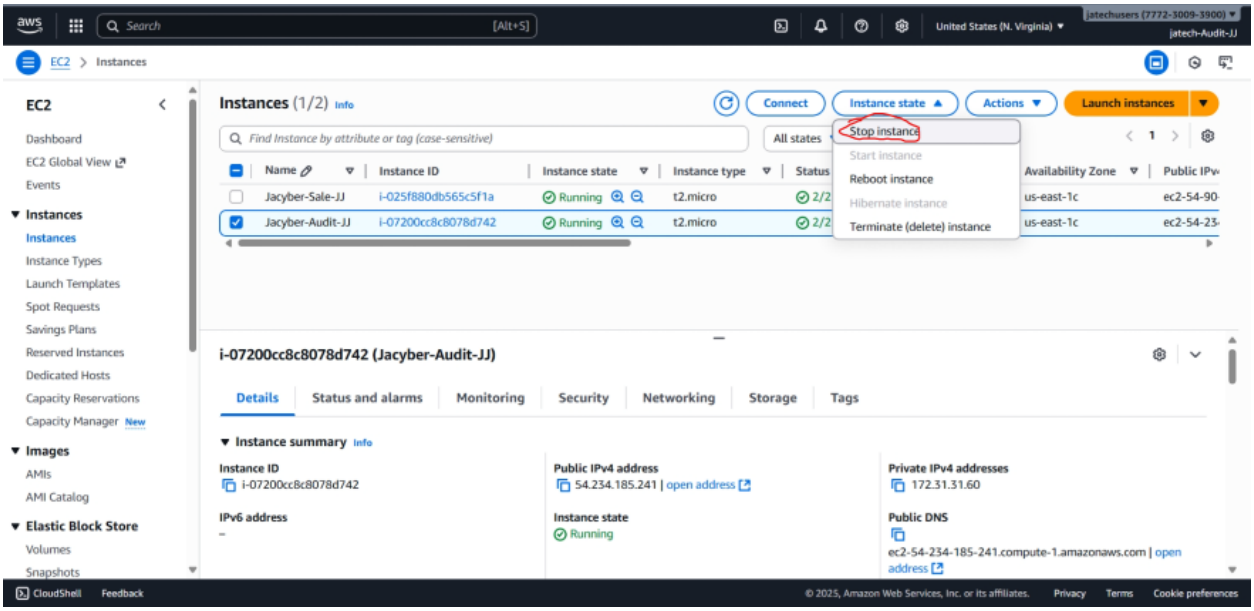
Logging in as an IAM User

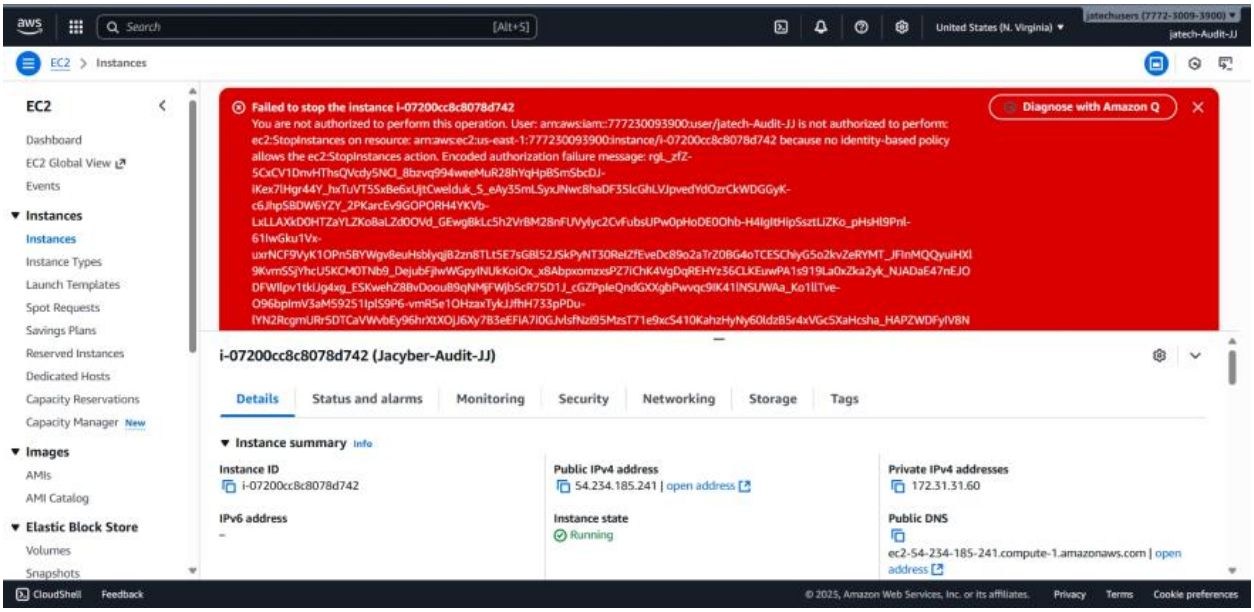


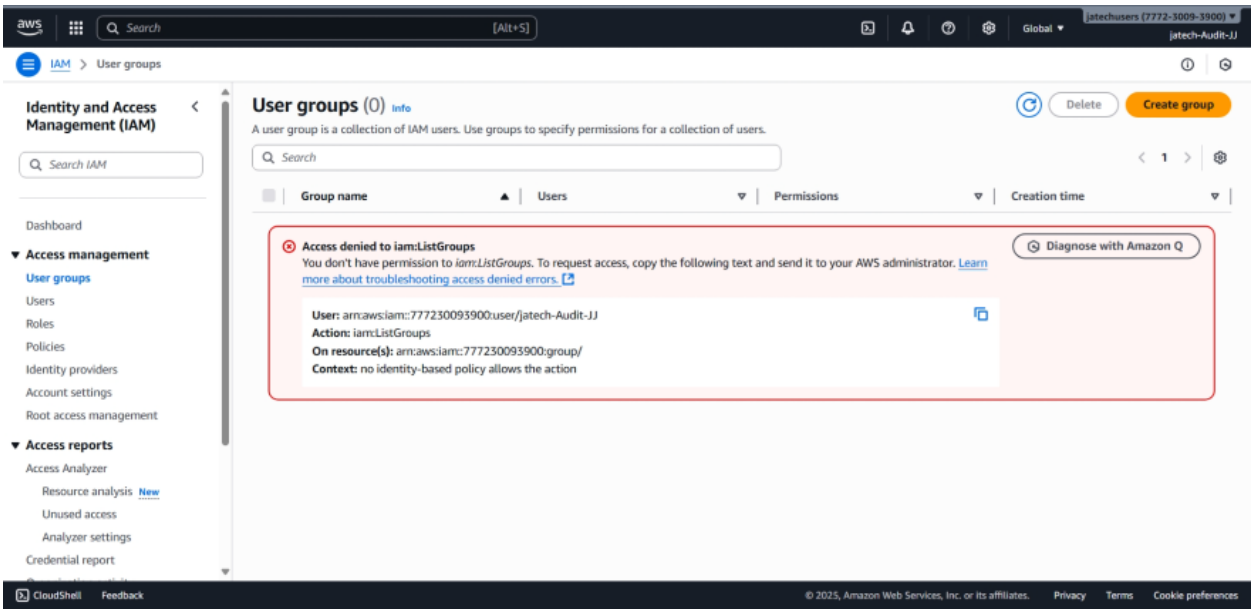

Search
[Alt+S]
United States (Ohio)
jatechusers (7772-3009-3900)
jatech-Audit-JJ
Console Home Info
Reset to default layout
Add widgets
Recently visited Info
No recently visited services
Explore one of these commonly visited AWS services.
EC2
S3
Aurora and RDS
Lambda
View all services
Applications (0) Info
Region: US East (Ohio)
Create application
Select Region
us-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.
AWS Health Info
No health data
You don't have permissions to access AWS Health.
Go to AWS Health
Cost and usage Info
Current month
Cost breakdown
Forecasted month end
Access denied
Savings opportunities
Access denied
Go to Billing and Cost Management
CloudShell
Feedback
© 2025, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences
Solutions Info
Vetted Solutions from AWS for popular business and technical use cases.
Go to AWS Solutions Library
Explore AWS Info
Security Info
Region: US East (Ohio)
Go to Security Hub CSPM
Trusted Advisor Info
Go to Trusted Advisor
Latest announcements Info
View all announcements
Recent AWS blog posts Info
View all blog posts
Want to see another widget? Tell us!
Add widgets

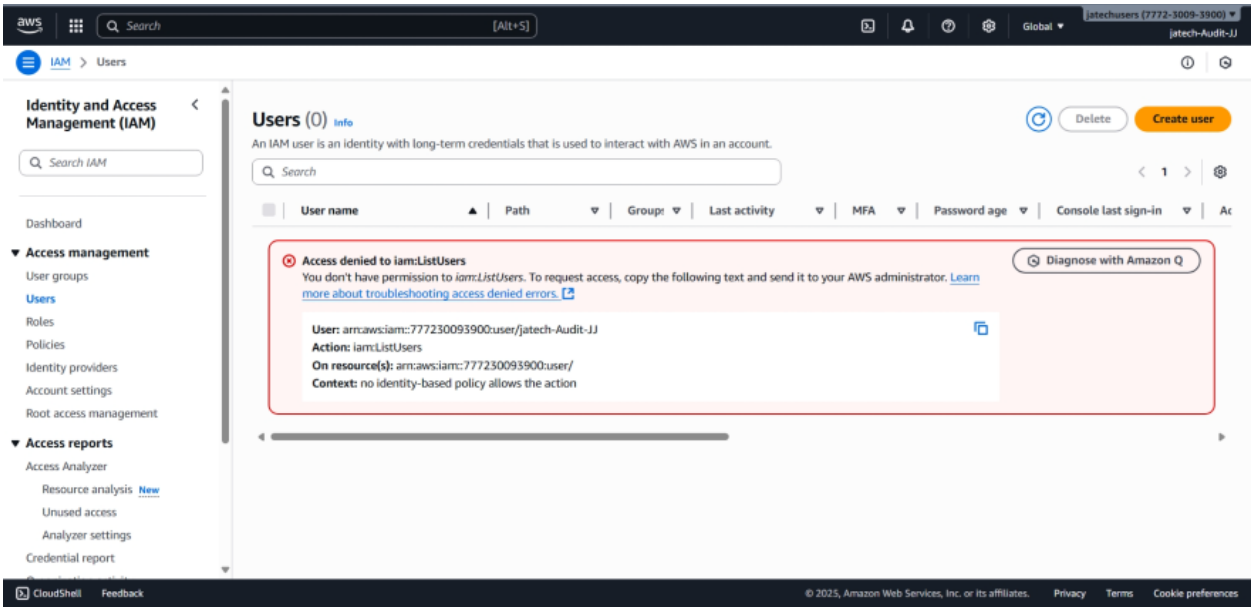

Search
[Alt+S]
United States (Ohio)
jatechusers (7772-3009-3900)
jatech-Audit-JJ
Console Home Info
Reset to default layout
Add widgets
Recently visited Info
No recently visited services
Explore one of these commonly visited AWS services.
EC2
S3
Aurora and RDS
Lambda
View all services
Applications (0) Info
Region: US East (Ohio)
Create application
Select Region
us-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.
AWS Health Info
No health data
You don't have permissions to access AWS Health.
Go to AWS Health
Cost and usage Info
Current month
Cost breakdown
Forecasted month end
Access denied
Savings opportunities
Access denied
Go to Billing and Cost Management
CloudShell
Feedback
© 2025, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences
Solutions Info
Vetted Solutions from AWS for popular business and technical use cases.
Go to AWS Solutions Library
Explore AWS Info
Security Info
Region: US East (Ohio)
Go to Security Hub CSPM
Trusted Advisor Info
Go to Trusted Advisor
Latest announcements Info
View all announcements
Recent AWS blog posts Info
View all blog posts
Want to see another widget? Tell us!
Add widgets

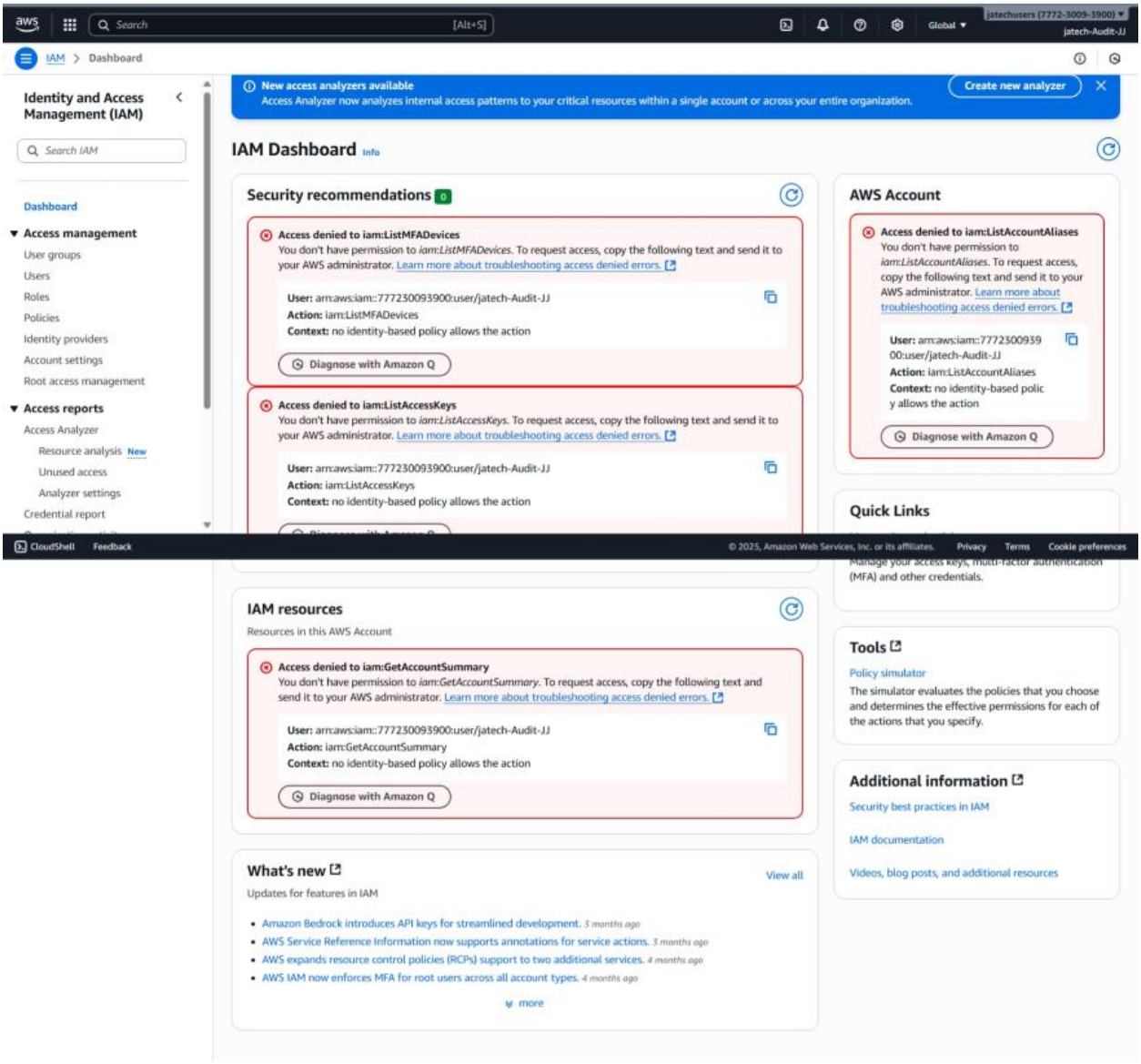
Testing the policy






Search
[Alt+S]
Global
jatechusers (7772-3009-3900)
jatech-Audit-JJ
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 New
Unused access
Analyzer settings
Credential report
User groups (0) Info
A user group is a collection of IAM users. Use groups to specify permissions for a collection of users.
Delete
Create group
Search
Group name
Users
Permissions
Creation time
Access denied to iam:ListGroups
You don't have permission to iam:ListGroups. To request access, copy the following text and send it to your AWS administrator. Learn more about troubleshooting access denied errors.
Diagnose with Amazon Q
User: arn:aws:iam::777230093900:user/jatech-Audit-JJ
Action: iam:ListGroups
On resource(s): arn:aws:iam::777230093900:group/
Context: no identity-based policy allows the action
CloudShell
Feedback
© 2025, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences


Search
[Alt+S]
Global
jatechusers (7772-3009-3900)
jatech-Audit-JJ
IAM > Users
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
Users (0) Info
An IAM user is an identity with long-term credentials that is used to interact with AWS in an account.
Delete
Create user
Search
User name
Path
Groups
Last activity
MFA
Password age
Console last sign-in
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.
Diagnose with Amazon Q
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
CloudShell
Feedback
© 2025, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences


Search
[Alt+S]
Global
jatechusers (7772-3009-3900)
jatech-Audit-JJ
IAM > Dashboard
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
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 0
Access denied to iam:ListMFADevices
You don't have permission to iam:ListMFADevices. 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:ListMFADevices
Context: no identity-based policy allows the action
Diagnose with Amazon Q
Access denied to iam:ListAccessKeys
You don't have permission to iam:ListAccessKeys. 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:ListAccessKeys
Context: no identity-based policy allows the action
AWS Account
Access denied to iam:ListAccountAliases
You don't have permission to iam:ListAccountAliases. 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:ListAccountAliases
Context: no identity-based policy allows the action
Diagnose with Amazon Q
Quick Links
Manage your access keys, multi-factor authentication (MFA) and other credentials.
IAM resources
Resources in this AWS Account
Access denied to iam:GetAccountSummary
You don't have permission to iam:GetAccountSummary. 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:GetAccountSummary
Context: no identity-based policy allows the action
Diagnose with Amazon Q
Tools
Policy simulator
The simulator evaluates the policies that you choose and determines the effective permissions for each of the actions that you specify.
Additional information
Security best practices in IAM
IAM documentation
Videos, blog posts, and additional resources
What's new
View all
Updates for features in IAM
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
more
CloudShell
Feedback
© 2025, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences

j