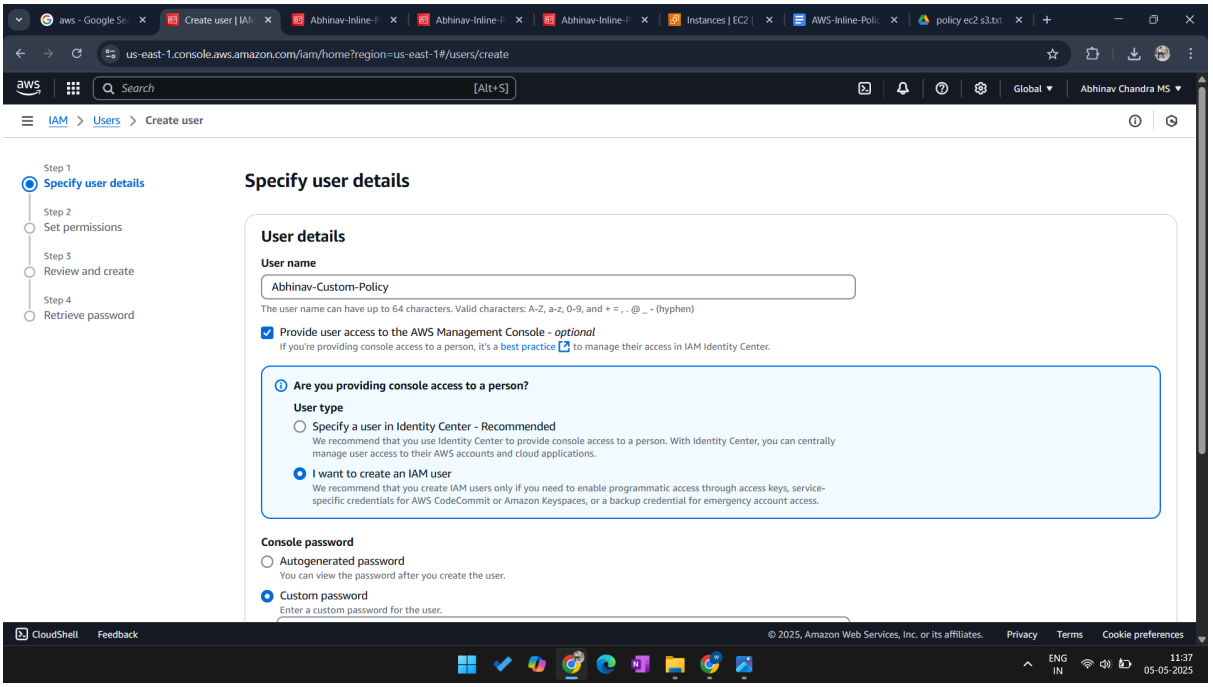
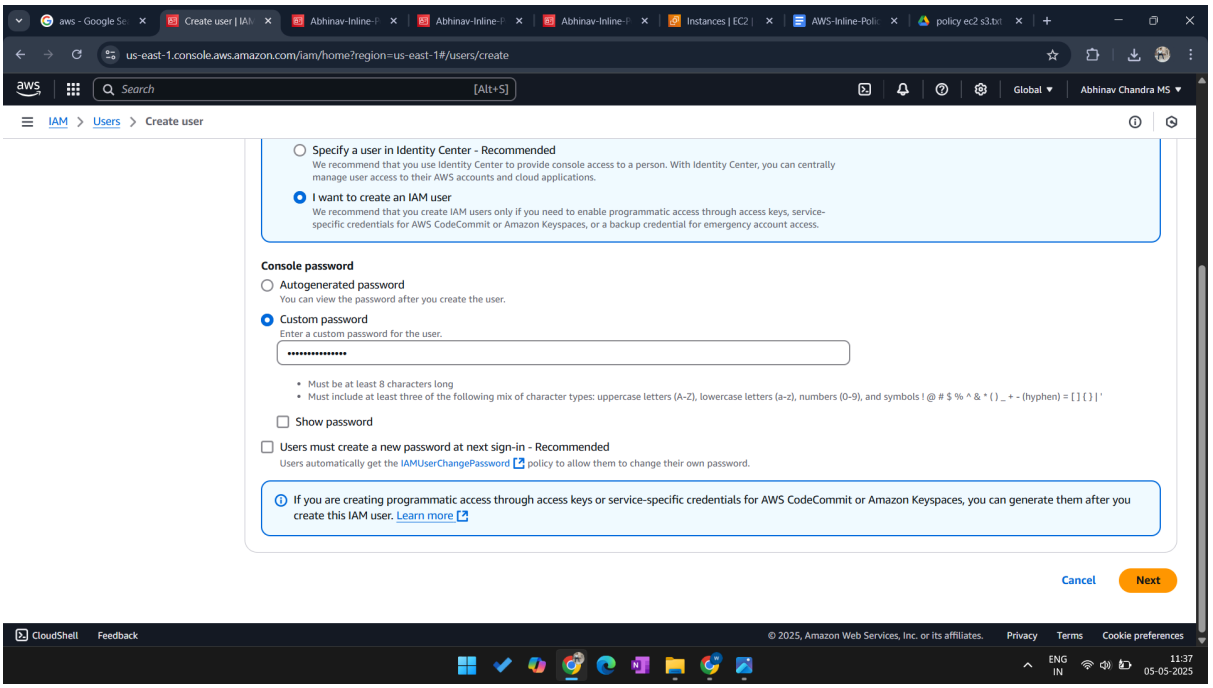
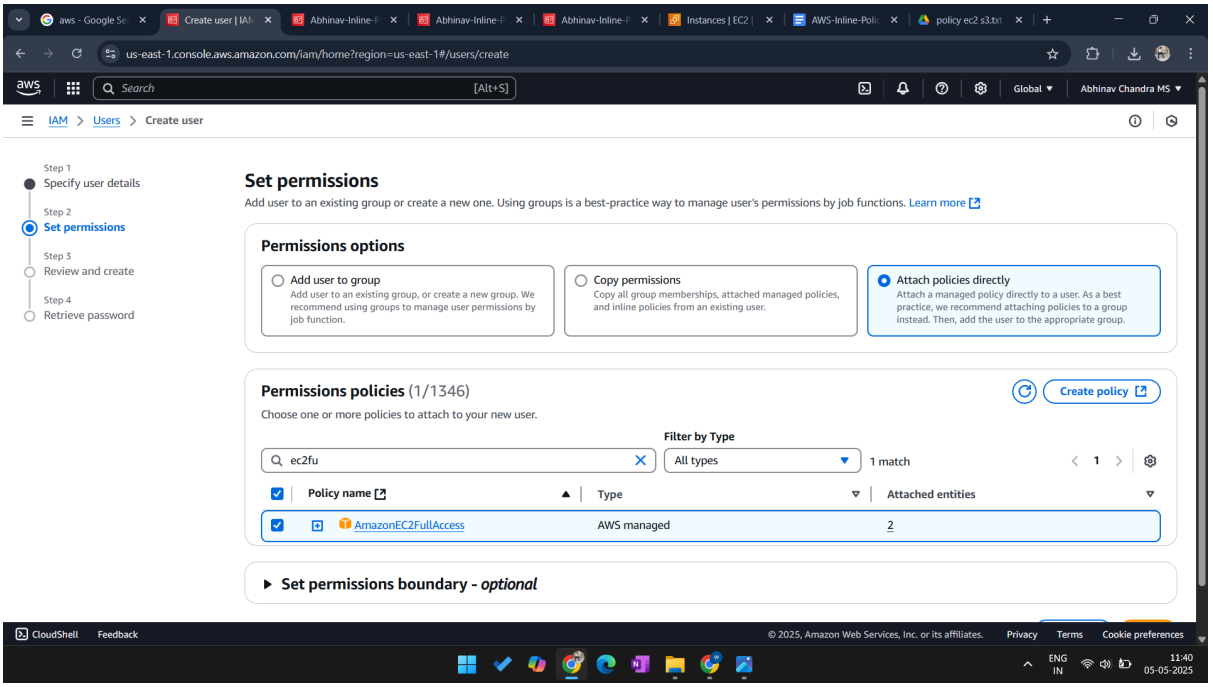
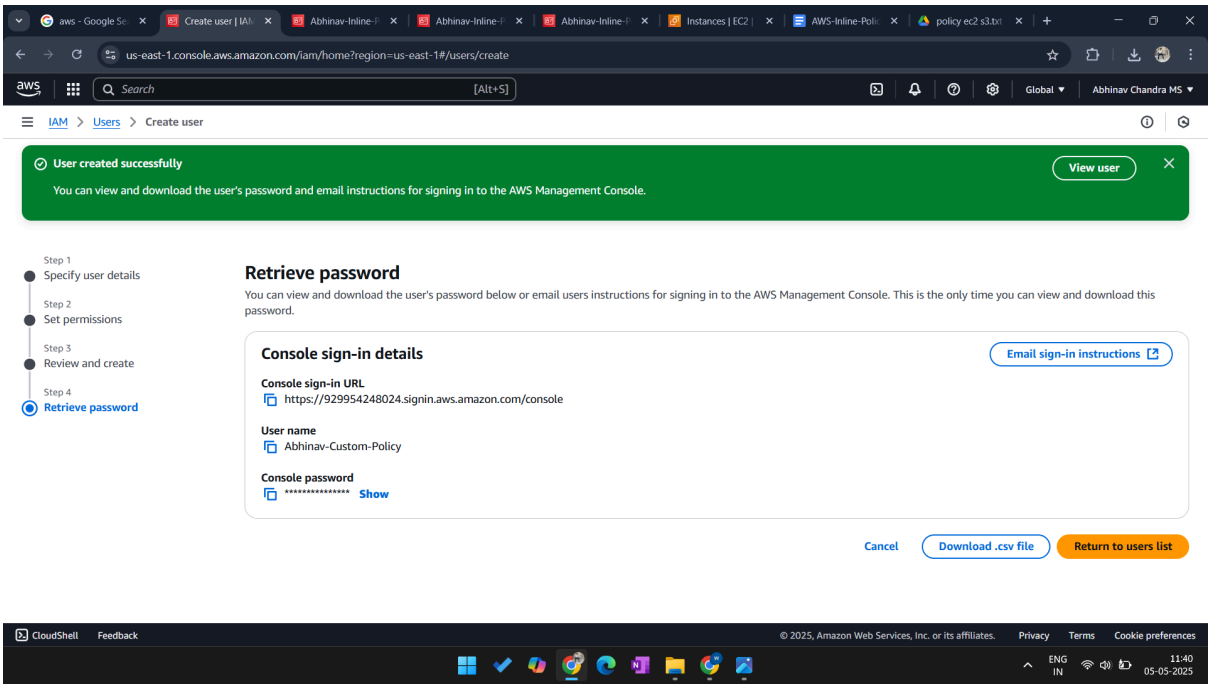
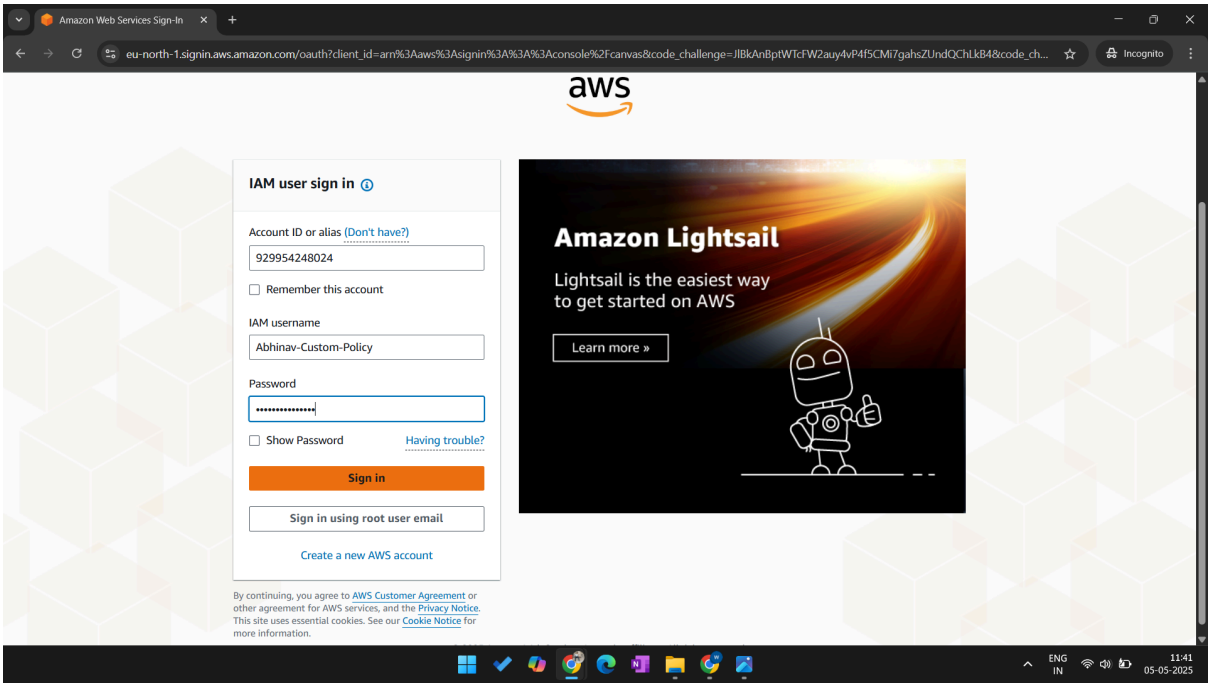
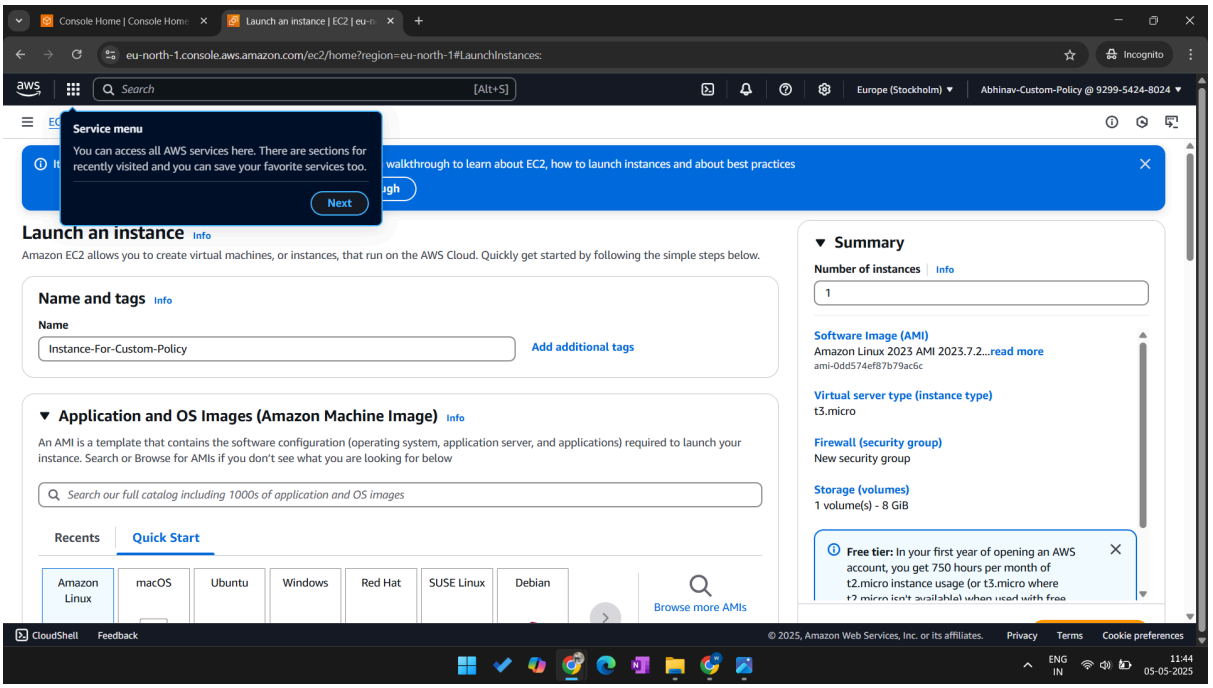

us-east-1.console.aws.amazon.com/iam/home?region=us-east-1#/users/create
Search [Alt+S]
Global
Abhinav Chandra MS
IAM > Users > Create user
Step 1
Specify user details
Step 2
Set permissions
Step 3
Review and create
Step 4
Retrieve password
Specify user details
User details
User name
Abhinav-Custom-Policy
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.
Are you providing console access to a person?
User type
Specify a user in Identity Center - Recommended
We recommend that you use Identity Center to provide console access to a person. With Identity Center, you can centrally manage user access to their AWS accounts and cloud applications.
I want to create an IAM user
We recommend that you create IAM users only if you need to enable programmatic access through access keys, service-specific credentials for AWS CodeCommit or Amazon Keyspaces, or a backup credential for emergency account access.
Console password
Autogenerated password
You can view the password after you create the user.
Custom password
Enter a custom password for the user.
CloudShell
Feedback
© 2025, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences
ENG
IN
11:37
05-05-2025

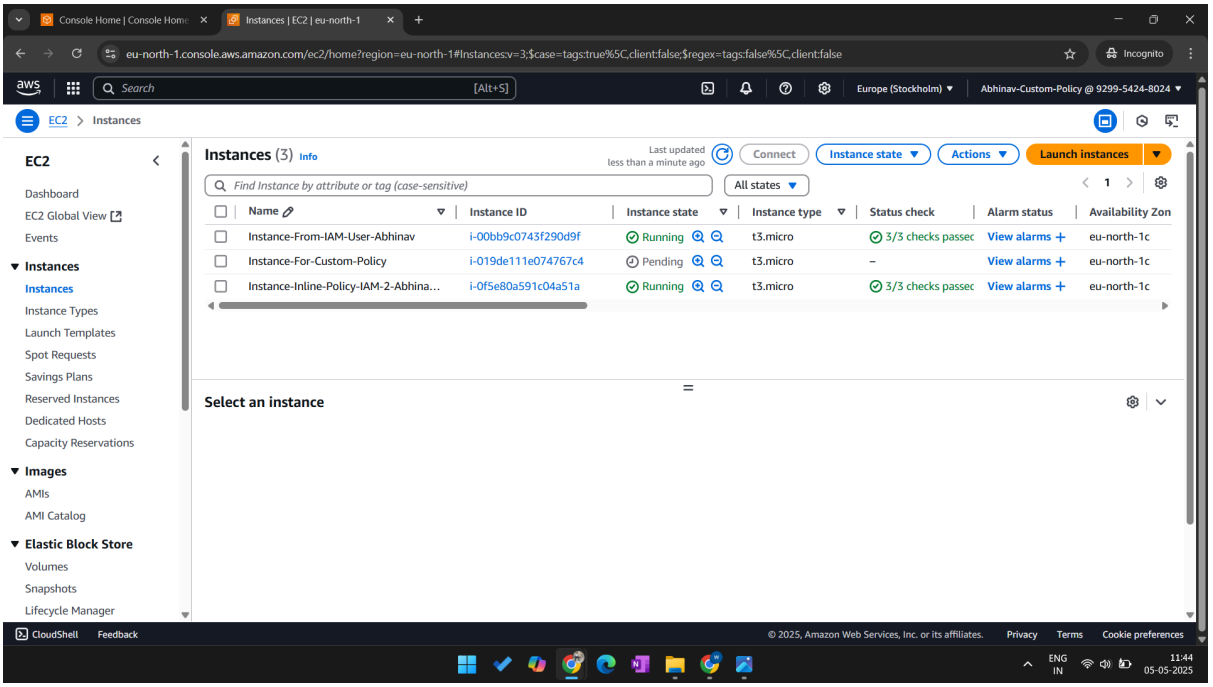

us-east-1.console.aws.amazon.com/iam/home?region=us-east-1#/users/create
Search [Alt+S]
Global
Abhinav Chandra MS
IAM > Users > Create user
Specify a user in Identity Center - Recommended
We recommend that you use Identity Center to provide console access to a person. With Identity Center, you can centrally manage user access to their AWS accounts and cloud applications.
I want to create an IAM user
We recommend that you create IAM users only if you need to enable programmatic access through access keys, service-specific credentials for AWS CodeCommit or Amazon Keyspaces, or a backup credential for emergency account access.
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
Cancel
Next
CloudShell
Feedback
© 2025, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences
ENG
IN
11:37
05-05-2025

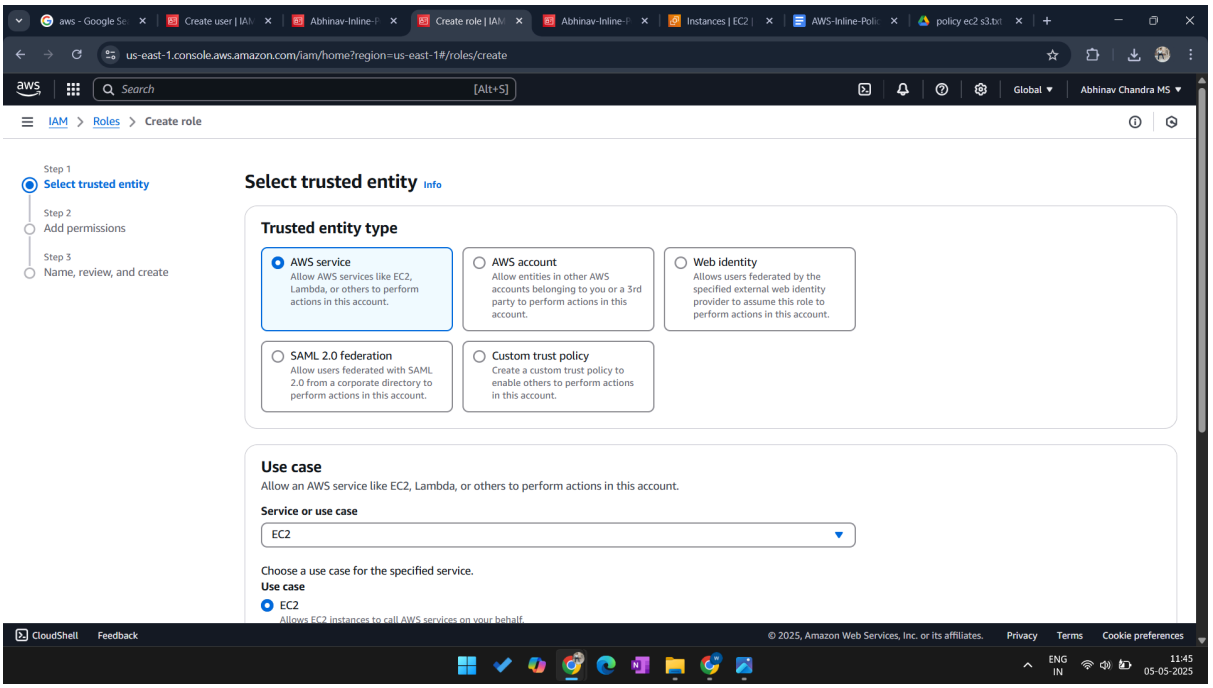

us-east-1.console.aws.amazon.com/iam/home?region=us-east-1#/users/create
Search [Alt+S]
Global
Abhinav Chandra MS
IAM > Users > Create user
Step 1
Specify user details
Step 2
Set permissions
Step 3
Review and create
Step 4
Retrieve password
Set permissions
Add user to an existing group or create a new 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.
Permissions policies (1/1346)
Choose one or more policies to attach to your new user.
Create policy
Filter by Type
ec2fu
All types
1 match
Policy name
Type
Attached entities
AmazonEC2FullAccess
AWS managed
2
Set permissions boundary - optional
CloudShell
Feedback
© 2025, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences
ENG
IN
11:40
05-05-2025

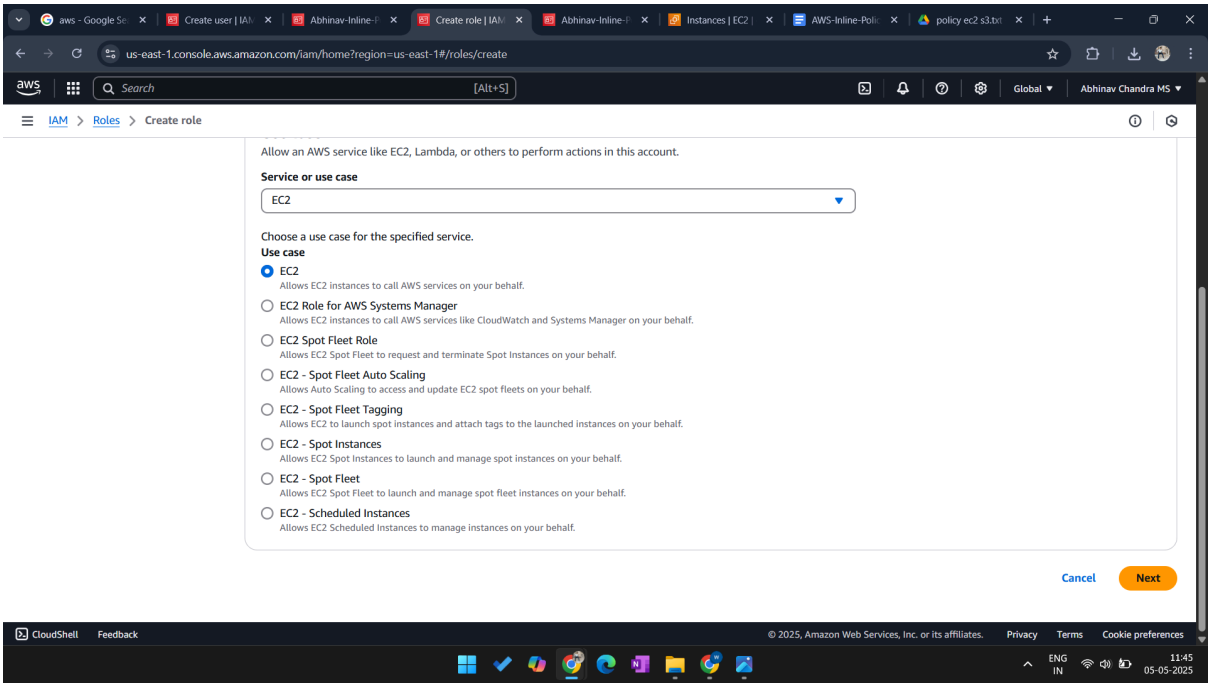

us-east-1.console.aws.amazon.com/iam/home?region=us-east-1#/users/create
Search [Alt+S]
Global
Abhinav Chandra MS
IAM > Users > Create user
User created successfully
You can view and download the user's password and email instructions for signing in to the AWS Management Console.
View user
Step 1
Specify 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://929954248024.signin.aws.amazon.com/console
User name
Abhinav-Custom-Policy
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
ENG
IN
11:40
05-05-2025

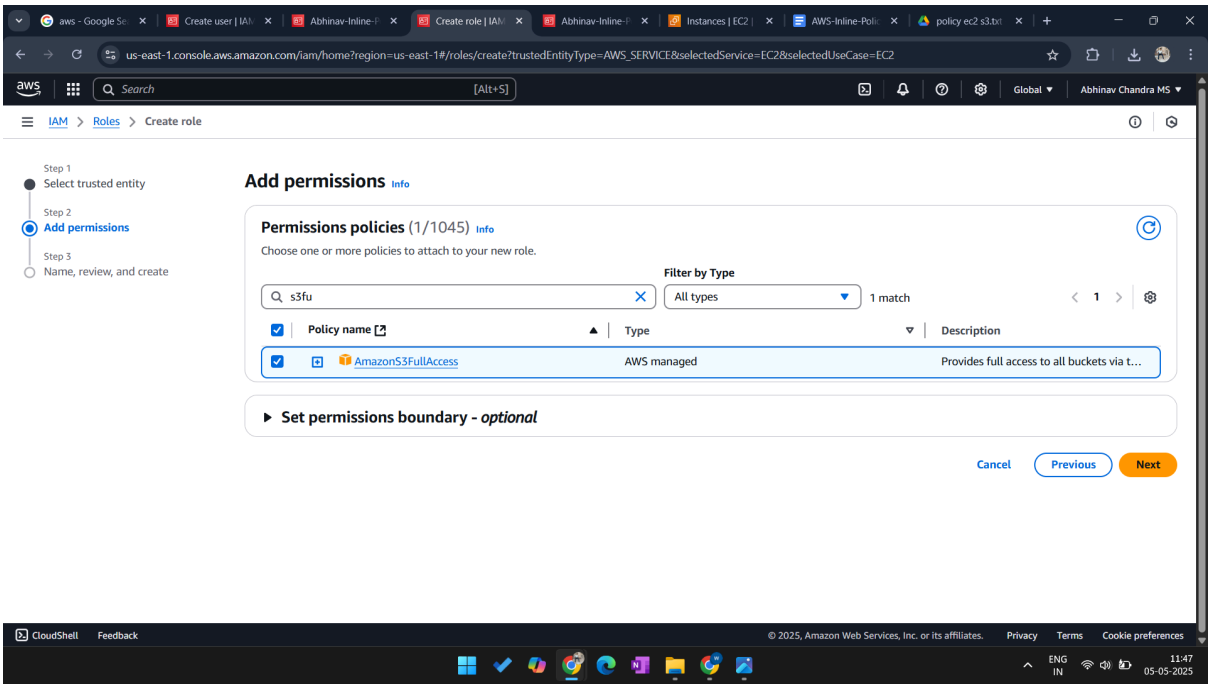

Amazon Web Services Sign-In
eu-north-1.signin.aws.amazon.com/oauth?client_id=arn%3Aaws%3Asignin%3A%3A%3Aconsole%2Fcanvas&code_challenge=JlBkAnBptWTcFW2auy4vP4f5CMi7gahsZUndQChLkB48&code_ch...
Incognito
aws
IAM user sign in
Account ID or alias (Don't have?)
929954248024
Remember this account
IAM username
Abhinav-Custom-Policy
Password
Show Password
Having trouble?
Sign in
Sign in using root user email
Create a new AWS account
By continuing, you agree to AWS Customer Agreement or other agreement for AWS services, and the Privacy Notice. This site uses essential cookies. See our Cookie Notice for more information.
Amazon Lightsail
Lightsail is the easiest way to get started on AWS
Learn more »
ENG IN
11:41
05-05-2025

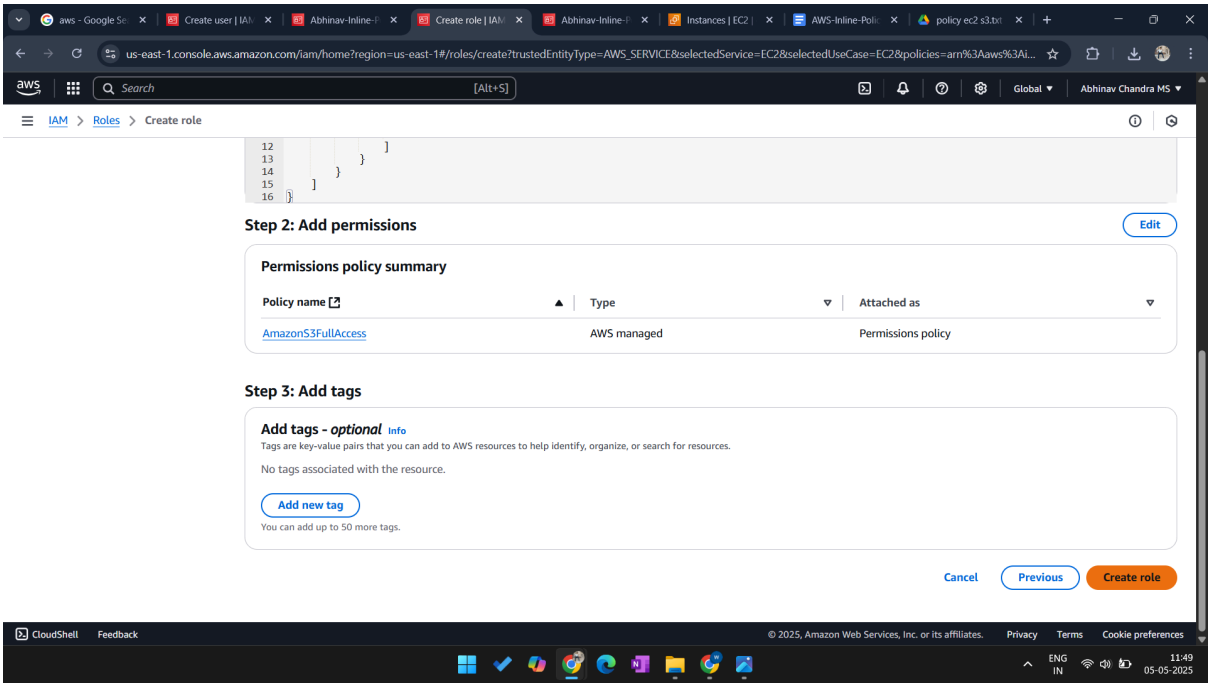

Console Home | Console Home
Launch an instance | EC2 | eu-n
eu-north-1.console.aws.amazon.com/ec2/home?region=eu-north-1#LaunchInstances:
Incognito
aws
Search
[Alt+S]
Europe (Stockholm)
Abhinav-Custom-Policy @ 9299-5424-8024
Service menu
You can access all AWS services here. There are sections for recently visited and you can save your favorite services too.
Next
walkthrough to learn about EC2, how to launch instances and about best practices
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
Instance-For-Custom-Policy
Add additional tags
Application and OS Images (Amazon Machine Image) Info
An AMI is a template that contains the software configuration (operating system, application server, and applications) required to launch your instance. Search or Browse for AMIs if you don't see what you are looking for below
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 2023.7.2...read more
ami-0dd574ef87b79ac6c
Virtual server type (instance type)
t3.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
CloudShell
Feedback
© 2025, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences
ENG IN
11:44
05-05-2025

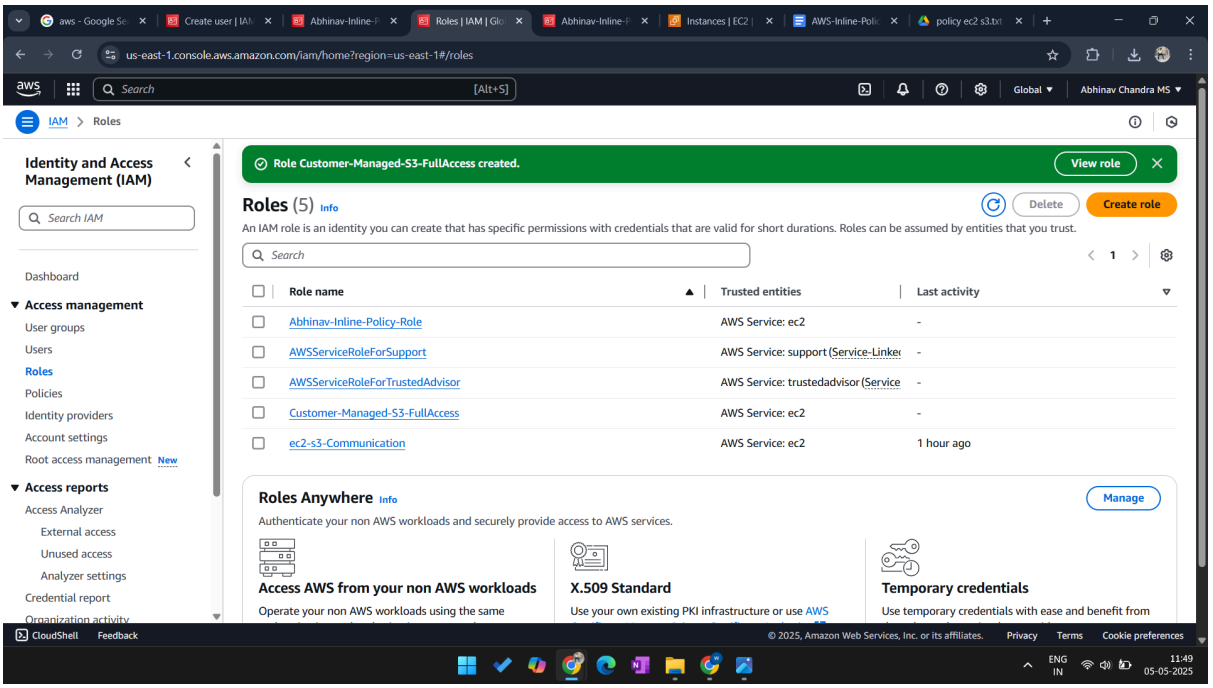

Console Home | Console Home
Instances | EC2 | eu-north-1
eu-north-1.console.aws.amazon.com/ec2/home?region=eu-north-1#Instances:v=3;$case=tags:true%5C,client:false;$regex=tags:false%5C,client:false
Incognito
Search
[Alt+S]
Europe (Stockholm)
Abhinav-Custom-Policy @ 9299-5424-8024
EC2 > Instances
EC2
Dashboard
EC2 Global View
Events
Instances
Instances
Instance Types
Launch Templates
Spot Requests
Savings Plans
Reserved Instances
Dedicated Hosts
Capacity Reservations
Images
AMIs
AMI Catalog
Elastic Block Store
Volumes
Snapshots
Lifecycle Manager
Instances (3) Info
Last updated less than a minute ago
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 Zon
Instance-From-IAM-User-Abhinav
i-00bb9c0743f290d9f
Running
t3.micro
3/3 checks passec
View alarms
eu-north-1c
Instance-For-Custom-Policy
i-019de111e074767c4
Pending
t3.micro
–
View alarms
eu-north-1c
Instance-Inline-Policy-IAM-2-Abhina...
i-0f5e80a591c04a51a
Running
t3.micro
3/3 checks passec
View alarms
eu-north-1c
Select an instance
CloudShell
Feedback
© 2025, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences
ENG
IN
11:44
05-05-2025

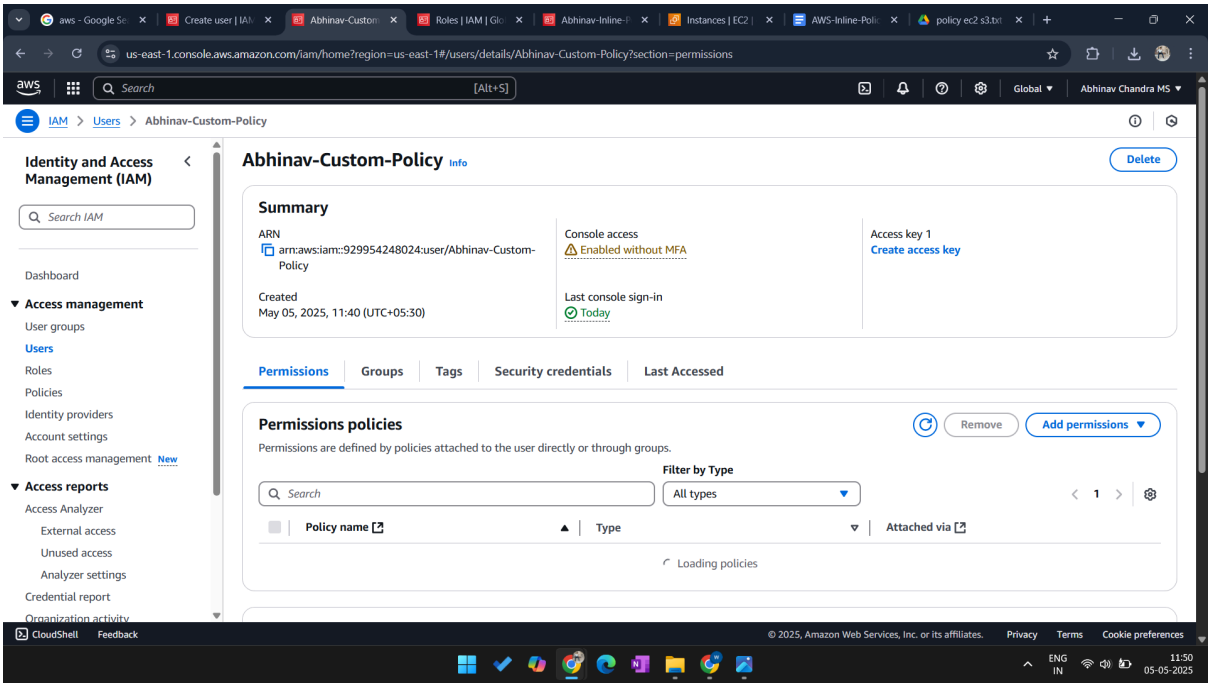

us-east-1.console.aws.amazon.com/iam/home?region=us-east-1#/roles/create
Search
[Alt+S]
Global
Abhinav Chandra MS
IAM > Roles > Create role
Step 1
Select trusted entity
Step 2
Add permissions
Step 3
Name, review, and create
Select trusted entity Info
Trusted entity type
AWS service
Allow AWS services like EC2, Lambda, or others to perform actions in this account.
AWS account
Allow entities in other AWS accounts belonging to you or a 3rd party to perform actions in this account.
Web identity
Allows users federated by the specified external web identity provider to assume this role to perform actions in this account.
SAML 2.0 federation
Allow users federated with SAML 2.0 from a corporate directory to perform actions in this account.
Custom trust policy
Create a custom trust policy to enable others to perform actions in this account.
Use case
Allow an AWS service like EC2, Lambda, or others to perform actions in this account.
Service or use case
EC2
Choose a use case for the specified service.
Use case
EC2
CloudShell
Feedback
© 2025, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences
ENG
IN
11:45
05-05-2025

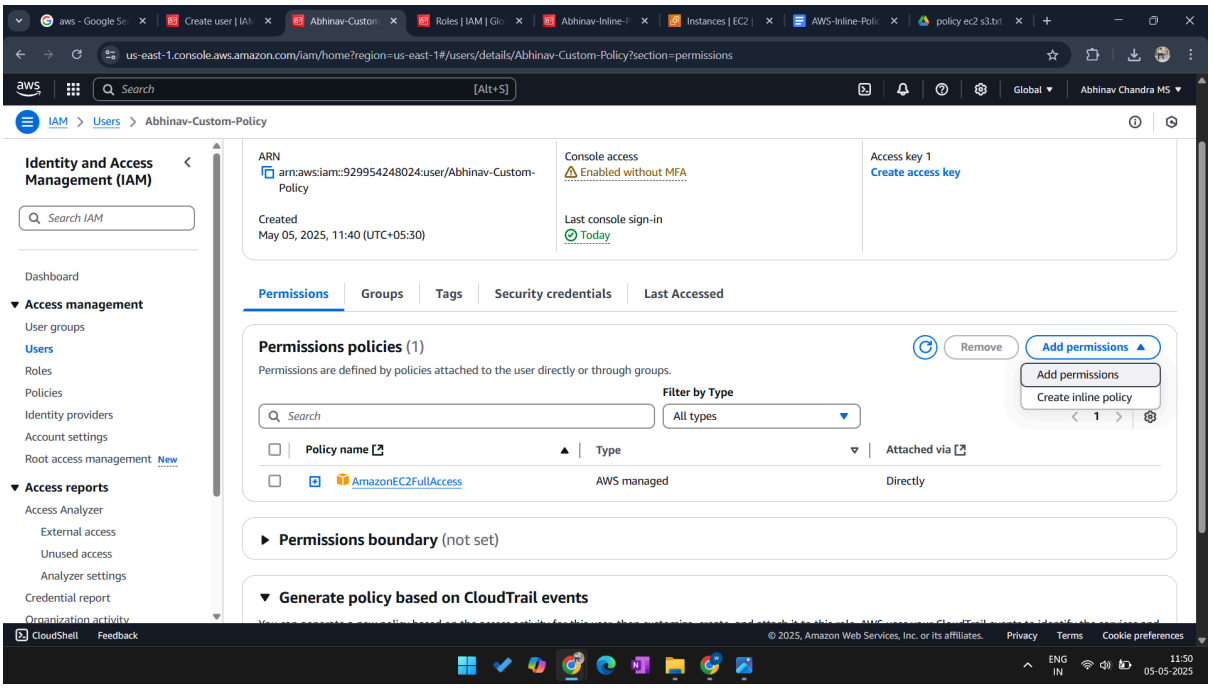

us-east-1.console.aws.amazon.com/iam/home?region=us-east-1#/roles/create
Search [Alt+S]
Global
Abhinav Chandra MS
IAM > Roles > Create role
Allow an AWS service like EC2, Lambda, or others to perform actions in this account.
Service or use case
EC2
Choose a use case for the specified service.
Use case
EC2
Allows EC2 instances to call AWS services on your behalf.
EC2 Role for AWS Systems Manager
Allows EC2 instances to call AWS services like CloudWatch and Systems Manager on your behalf.
EC2 Spot Fleet Role
Allows EC2 Spot Fleet to request and terminate Spot Instances on your behalf.
EC2 - Spot Fleet Auto Scaling
Allows Auto Scaling to access and update EC2 spot fleets on your behalf.
EC2 - Spot Fleet Tagging
Allows EC2 to launch spot instances and attach tags to the launched instances on your behalf.
EC2 - Spot Instances
Allows EC2 Spot Instances to launch and manage spot instances on your behalf.
EC2 - Spot Fleet
Allows EC2 Spot Fleet to launch and manage spot fleet instances on your behalf.
EC2 - Scheduled Instances
Allows EC2 Scheduled Instances to manage instances on your behalf.
Cancel
Next
CloudShell
Feedback
© 2025, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences
ENG IN
11:45
05-05-2025

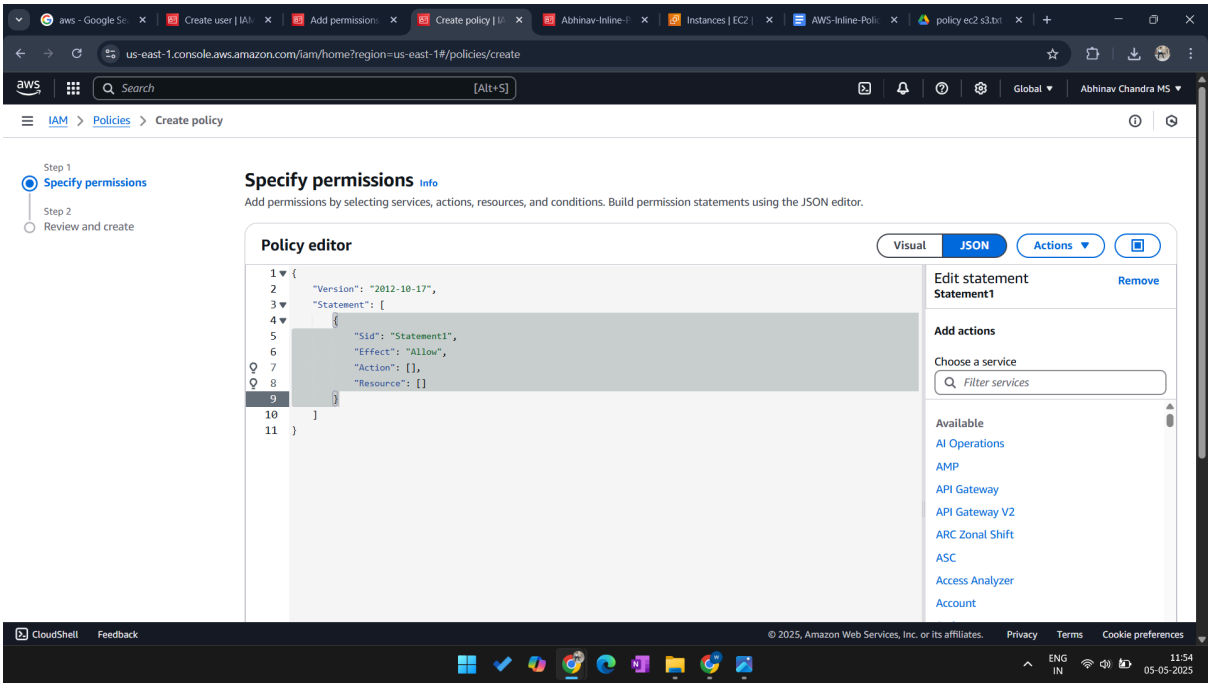

us-east-1.console.aws.amazon.com/iam/home?region=us-east-1#/roles/create?trustedEntityType=AWS_SERVICE&selectedService=EC2&selectedUseCase=EC2
Search [Alt+S]
Global
Abhinav Chandra MS
IAM > Roles > Create role
Step 1
Select trusted entity
Step 2
Add permissions
Step 3
Name, review, and create
Add permissions Info
Permissions policies (1/1045) Info
Choose one or more policies to attach to your new role.
Filter by Type
s3fu
All types
1 match
Policy name
Type
Description
AmazonS3FullAccess
AWS managed
Provides full access to all buckets via t...
Set permissions boundary - optional
Cancel
Previous
Next
CloudShell
Feedback
© 2025, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences
ENG IN
11:47
05-05-2025

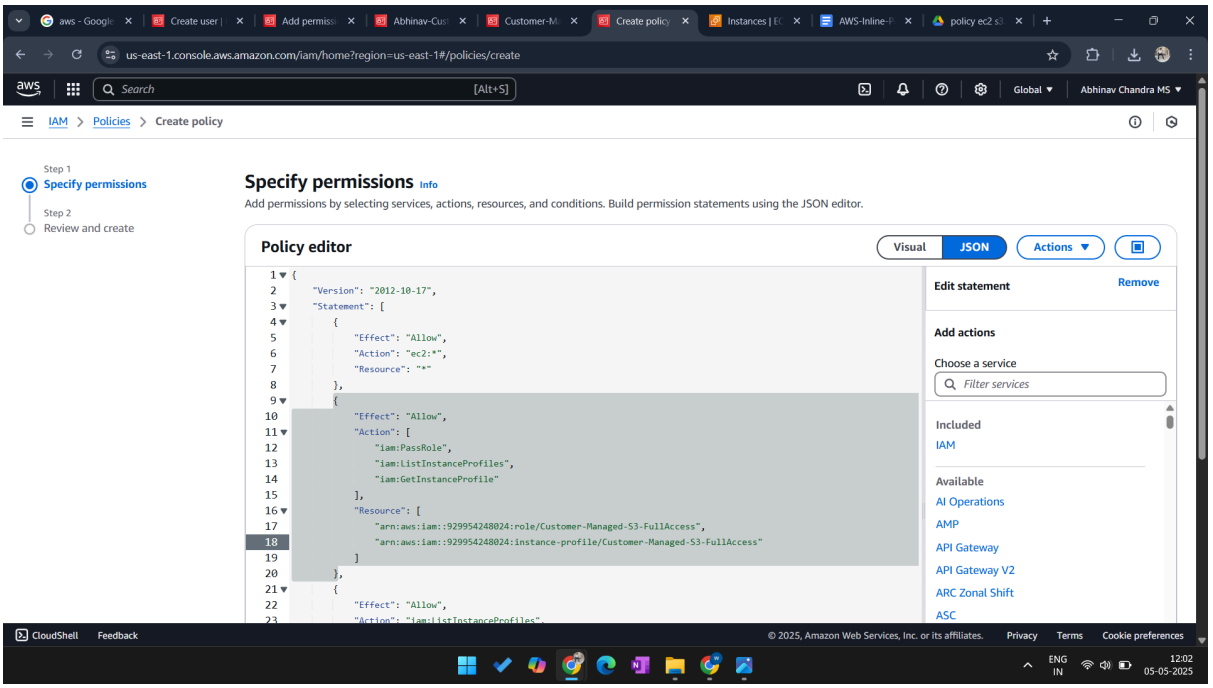

IAM > Roles > Create role
Step 2: Add permissions
Edit
Permissions policy summary
Policy name
Type
Attached as
AmazonS3FullAccess
AWS managed
Permissions policy
Step 3: Add tags
Add tags - optional Info
Tags are key-value pairs that you can add to AWS resources to help identify, organize, or search for resources.
No tags associated with the resource.
Add new tag
You can add up to 50 more tags.
Cancel
Previous
Create role

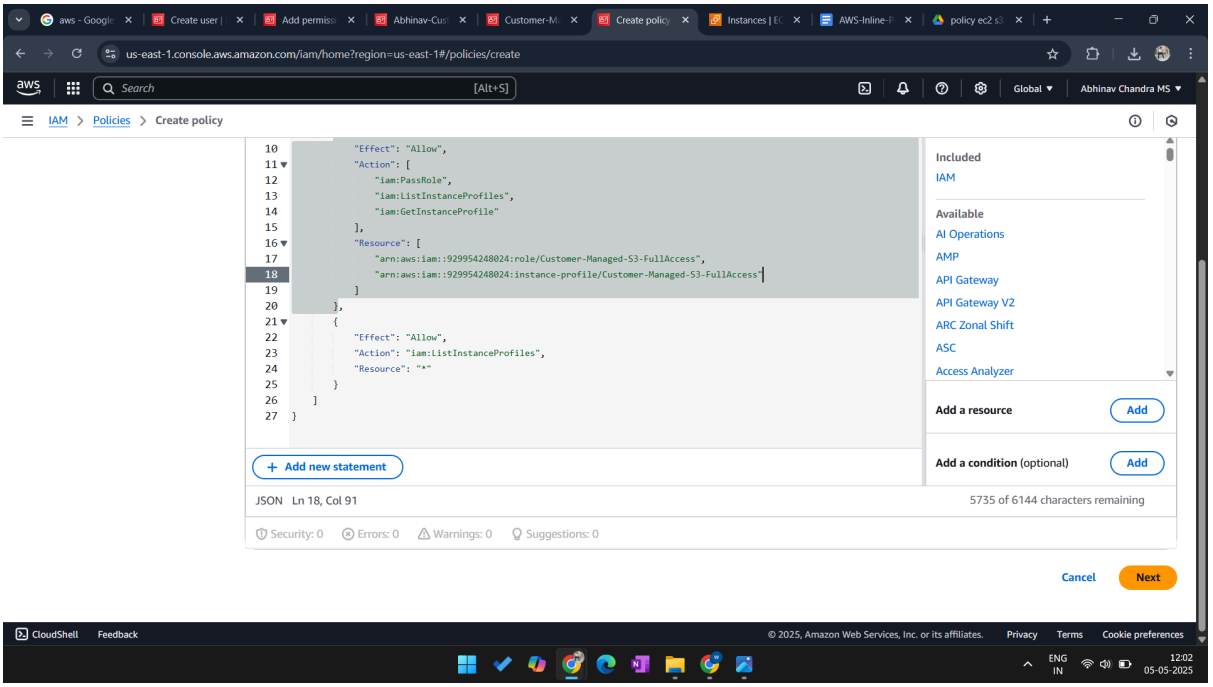

Role Customer-Managed-S3-FullAccess created.
View role
Identity and Access Management (IAM)
Search IAM
Dashboard
Access management
User groups
Users
Roles
Policies
Identity providers
Account settings
Root access management New
Access reports
Access Analyzer
External access
Unused access
Analyzer settings
Credential report
Roles (5) Info
An IAM role is an identity you can create that has specific permissions with credentials that are valid for short durations. Roles can be assumed by entities that you trust.
Delete
Create role
Role name
Trusted entities
Last activity
Abhinav-Inline-Policy-Role
AWS Service: ec2
AWSServiceRoleForSupport
AWS Service: support (Service-Linke
AWSServiceRoleForTrustedAdvisor
AWS Service: trustedadvisor (Service
Customer-Managed-S3-FullAccess
AWS Service: ec2
ec2-s3-Communication
AWS Service: ec2
1 hour ago
Roles Anywhere Info
Manage
Authenticate your non AWS workloads and securely provide access to AWS services.
Access AWS from your non AWS workloads
X.509 Standard
Temporary credentials

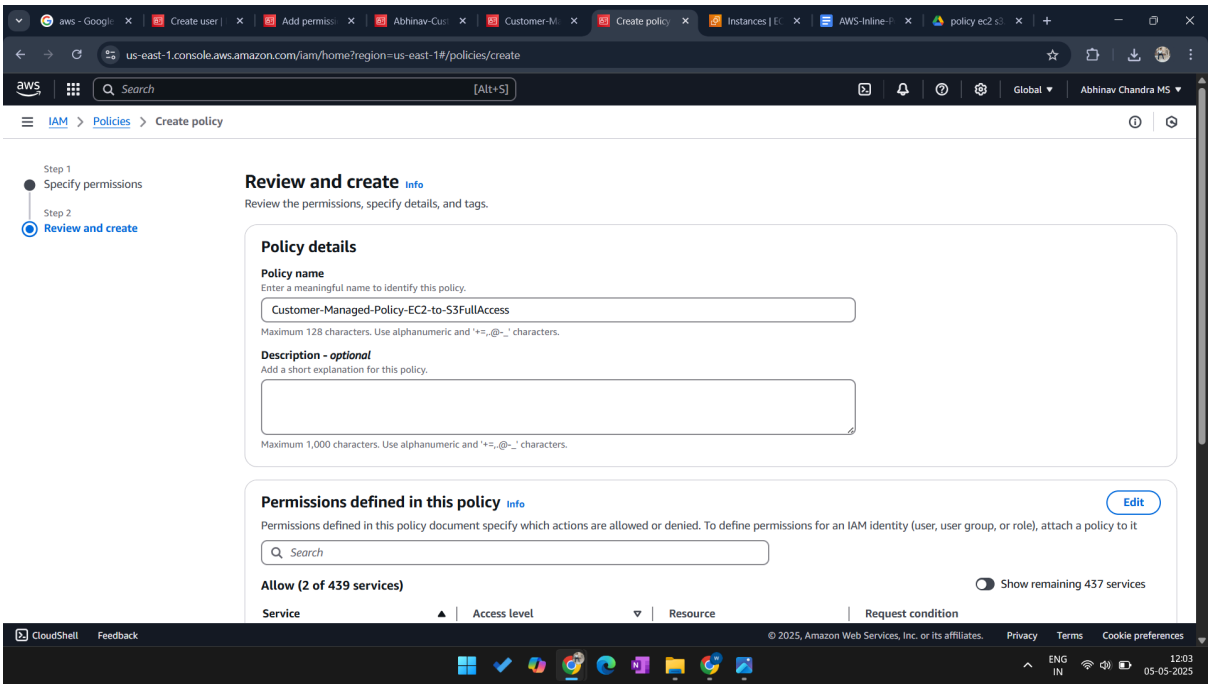

us-east-1.console.aws.amazon.com/iam/home?region=us-east-1#/users/details/Abhinav-Custom-Policy?section=permissions
Search [Alt+S]
Global
Abhinav Chandra MS
IAM > Users > Abhinav-Custom-Policy
Identity and Access Management (IAM)
Search IAM
Dashboard
Access management
User groups
Users
Roles
Policies
Identity providers
Account settings
Root access management New
Access reports
Access Analyzer
External access
Unused access
Analyzer settings
Credential report
Organization activity
Abhinav-Custom-Policy Info
Delete
Summary
ARN
arn:aws:iam::929954248024:user/Abhinav-Custom-Policy
Console access
Enabled without MFA
Access key 1
Create access key
Created
May 05, 2025, 11:40 (UTC+05:30)
Last console sign-in
Today
Permissions
Groups
Tags
Security credentials
Last Accessed
Permissions policies
Permissions are defined by policies attached to the user directly or through groups.
Remove
Add permissions
Filter by Type
Search
All types
Policy name
Type
Attached via
Loading policies
CloudShell
Feedback
© 2025, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences
ENG IN
11:50
05-05-2025

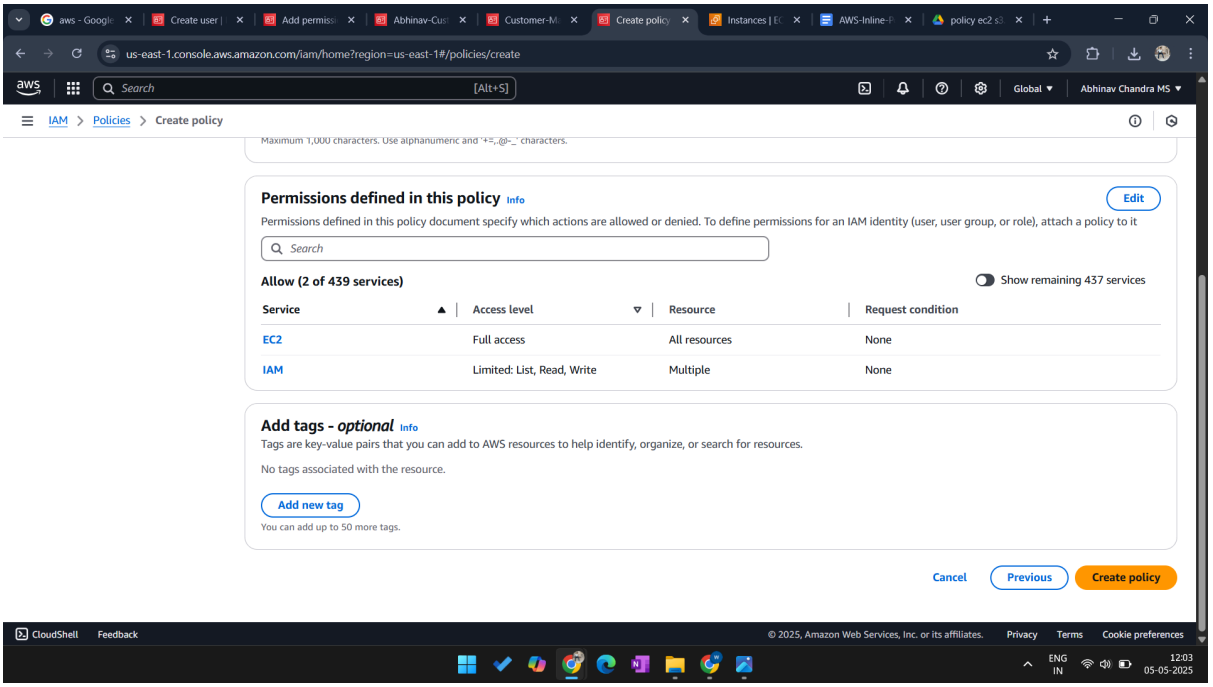

us-east-1.console.aws.amazon.com/iam/home?region=us-east-1#/users/details/Abhinav-Custom-Policy?section=permissions
Search [Alt+S]
Global
Abhinav Chandra MS
IAM > Users > Abhinav-Custom-Policy
Identity and Access Management (IAM)
Search IAM
Dashboard
Access management
User groups
Users
Roles
Policies
Identity providers
Account settings
Root access management New
Access reports
Access Analyzer
External access
Unused access
Analyzer settings
Credential report
Organization activity
ARN
arn:aws:iam::929954248024:user/Abhinav-Custom-Policy
Console access
Enabled without MFA
Access key 1
Create access key
Created
May 05, 2025, 11:40 (UTC+05:30)
Last console sign-in
Today
Permissions
Groups
Tags
Security credentials
Last Accessed
Permissions policies (1)
Permissions are defined by policies attached to the user directly or through groups.
Remove
Add permissions
Add permissions
Create inline policy
Filter by Type
Search
All types
Policy name
Type
Attached via
AmazonEC2FullAccess
AWS managed
Directly
Permissions boundary (not set)
Generate policy based on CloudTrail events
CloudShell
Feedback
© 2025, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences
ENG IN
11:50
05-05-2025

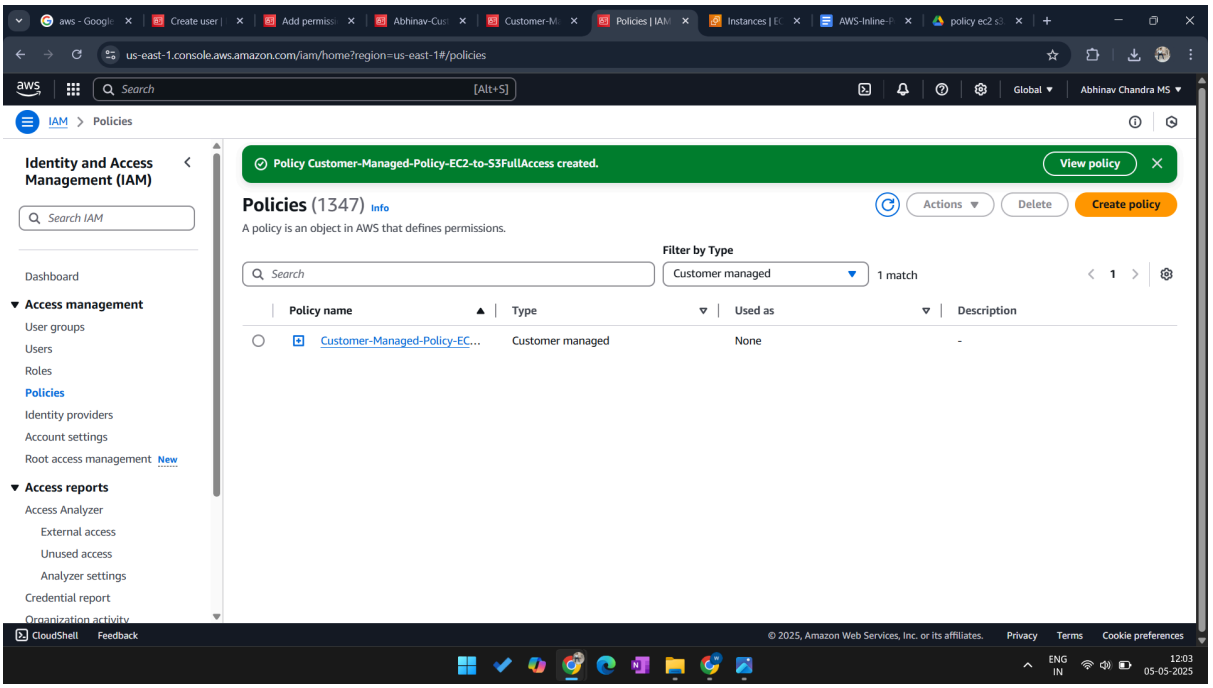

us-east-1.console.aws.amazon.com/iam/home?region=us-east-1#/policies/create
Search [Alt+S]
Global
Abhinav Chandra MS
IAM > Policies > Create policy
Step 1
Specify permissions
Step 2
Review and create
Specify permissions Info
Add permissions by selecting services, actions, resources, and conditions. Build permission statements using the JSON editor.
Policy editor
Visual
JSON
Actions
{
"Version": "2012-10-17",
"Statement": [
{
"Sid": "Statement1",
"Effect": "Allow",
"Action": [],
"Resource": []
}
]
}
Edit statement
Statement1
Remove
Add actions
Choose a service
Filter services
Available
AI Operations
AMP
API Gateway
API Gateway V2
ARC Zonal Shift
ASC
Access Analyzer
Account
CloudShell
Feedback
© 2025, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences
ENG
IN
11:54
05-05-2025

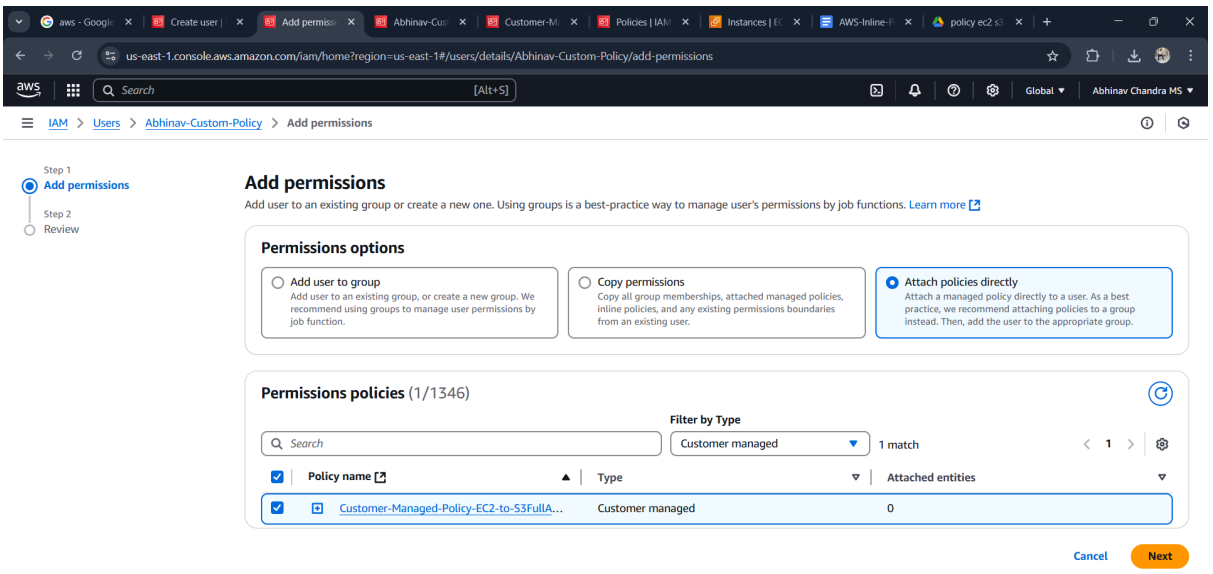

us-east-1.console.aws.amazon.com/iam/home?region=us-east-1#/policies/create
Search [Alt+S]
Global
Abhinav Chandra MS
IAM > Policies > Create policy
Step 1
Specify permissions
Step 2
Review and create
Specify permissions Info
Add permissions by selecting services, actions, resources, and conditions. Build permission statements using the JSON editor.
Policy editor
Visual
JSON
Actions
{
"Version": "2012-10-17",
"Statement": [
{
"Effect": "Allow",
"Action": "ec2:*",
"Resource": "*"
},
{
"Effect": "Allow",
"Action": [
"iam:PassRole",
"iam:ListInstanceProfiles",
"iam:GetInstanceProfile"
],
"Resource": [
"arn:aws:iam::929954248024:role/Customer-Managed-S3-FullAccess",
"arn:aws:iam::929954248024:instance-profile/Customer-Managed-S3-FullAccess"
]
},
{
"Effect": "Allow",
Edit statement
Remove
Add actions
Choose a service
Filter services
Included
IAM
Available
AI Operations
AMP
API Gateway
API Gateway V2
ARC Zonal Shift
ASC
CloudShell
Feedback
© 2025, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences
ENG
IN
12:02
05-05-2025

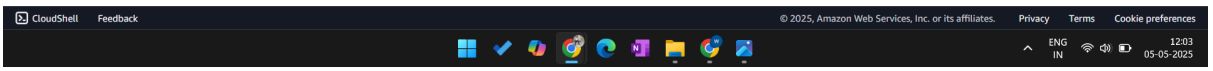

us-east-1.console.aws.amazon.com/iam/home?region=us-east-1#/policies/create
IAM > Policies > Create policy
"Effect": "Allow",
"Action": [
"iam:PassRole",
"iam:ListInstanceProfiles",
"iam:GetInstanceProfile"
],
"Resource": [
"arn:aws:iam::929954248024:role/Customer-Managed-S3-FullAccess",
"arn:aws:iam::929954248024:instance-profile/Customer-Managed-S3-FullAccess"
]
},
{
"Effect": "Allow",
"Action": "iam:ListInstanceProfiles",
"Resource": "*"
}
]
}
Included
IAM
Available
AI Operations
AMP
API Gateway
API Gateway V2
ARC Zonal Shift
ASC
Access Analyzer
Add a resource
Add
Add a condition (optional)
Add
Add new statement
JSON Ln 18, Col 91
5735 of 6144 characters remaining
Security: 0
Errors: 0
Warnings: 0
Suggestions: 0
Cancel
Next
CloudShell
Feedback
© 2025, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences

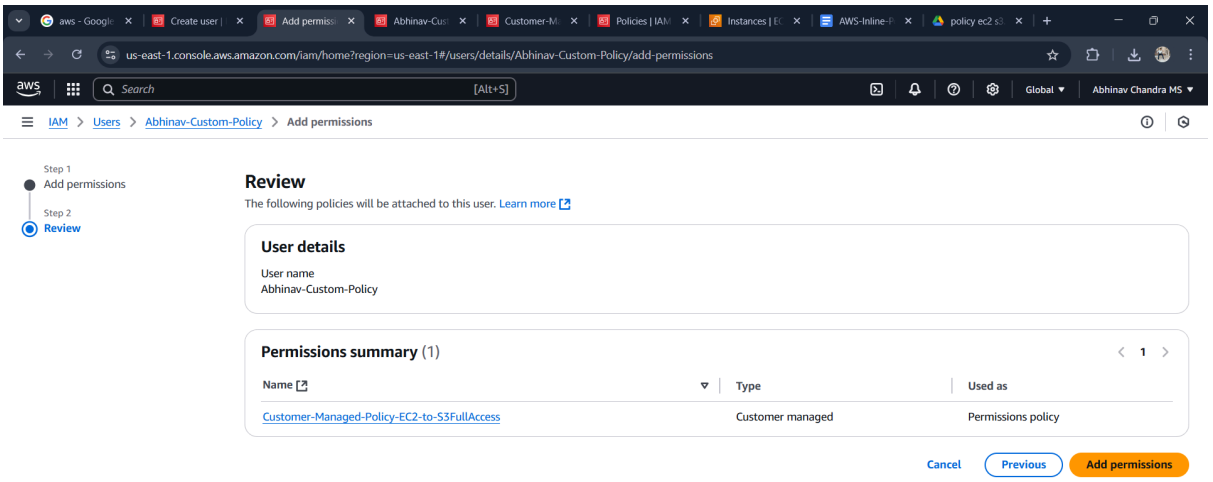

us-east-1.console.aws.amazon.com/iam/home?region=us-east-1#/policies/create
IAM > Policies > Create policy
Step 1
Specify permissions
Step 2
Review and create
Review and create Info
Review the permissions, specify details, and tags.
Policy details
Policy name
Enter a meaningful name to identify this policy.
Customer-Managed-Policy-EC2-to-S3FullAccess
Maximum 128 characters. Use alphanumeric and '+=,.@-_' characters.
Description - optional
Add a short explanation for this policy.
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
Allow (2 of 439 services)
Show remaining 437 services
Service
Access level
Resource
Request condition
CloudShell
Feedback
© 2025, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences


us-east-1.console.aws.amazon.com/iam/home?region=us-east-1#/policies/create
Search [Alt+S]
Global
Abhinav Chandra MS
IAM > Policies > Create policy
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
Allow (2 of 439 services)
Show remaining 437 services
Service
Access level
Resource
Request condition
EC2
Full access
All resources
None
IAM
Limited: List, Read, Write
Multiple
None
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
ENG
IN
12:03
05-05-2025

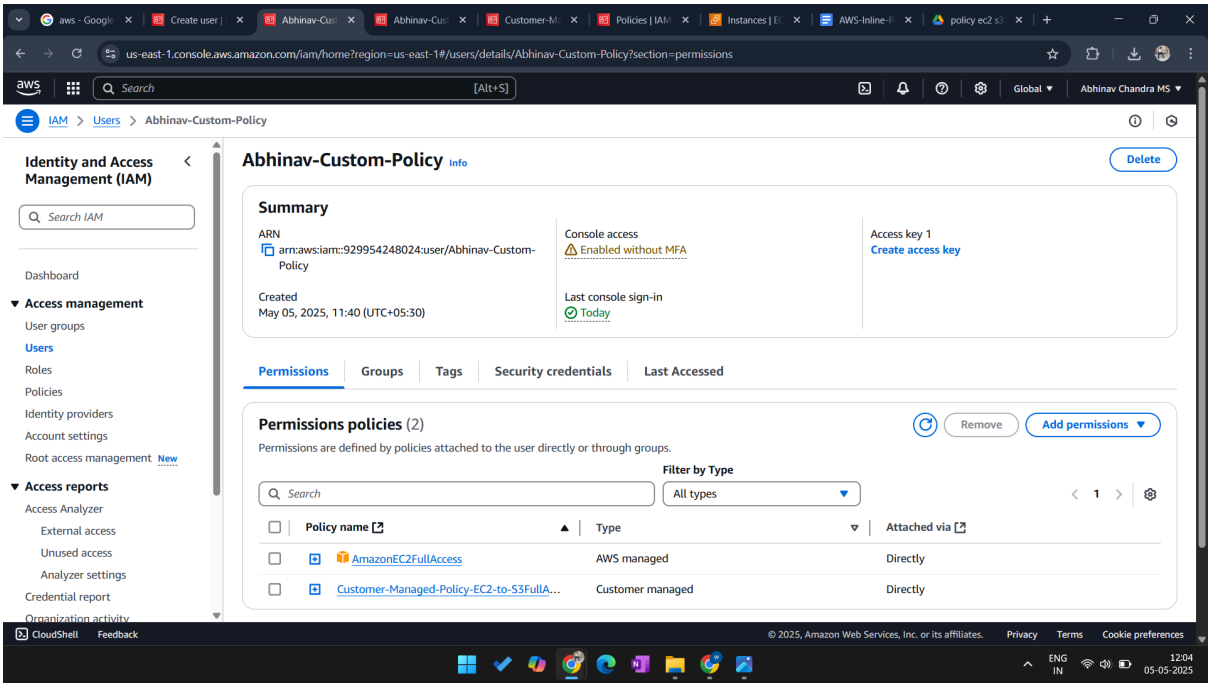

us-east-1.console.aws.amazon.com/iam/home?region=us-east-1#/policies
Search [Alt+S]
Global
Abhinav Chandra MS
IAM > Policies
Identity and Access Management (IAM)
Search IAM
Dashboard
Access management
User groups
Users
Roles
Policies
Identity providers
Account settings
Root access management New
Access reports
Access Analyzer
External access
Unused access
Analyzer settings
Credential report
Organization activity
Policy Customer-Managed-Policy-EC2-to-S3FullAccess created.
View policy
Policies (1347) Info
A policy is an object in AWS that defines permissions.
Actions
Delete
Create policy
Filter by Type
Search
Customer managed
1 match
1
Policy name
Type
Used as
Description
Customer-Managed-Policy-EC...
Customer managed
None
-
CloudShell
Feedback
© 2025, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences
ENG
IN
12:03
05-05-2025

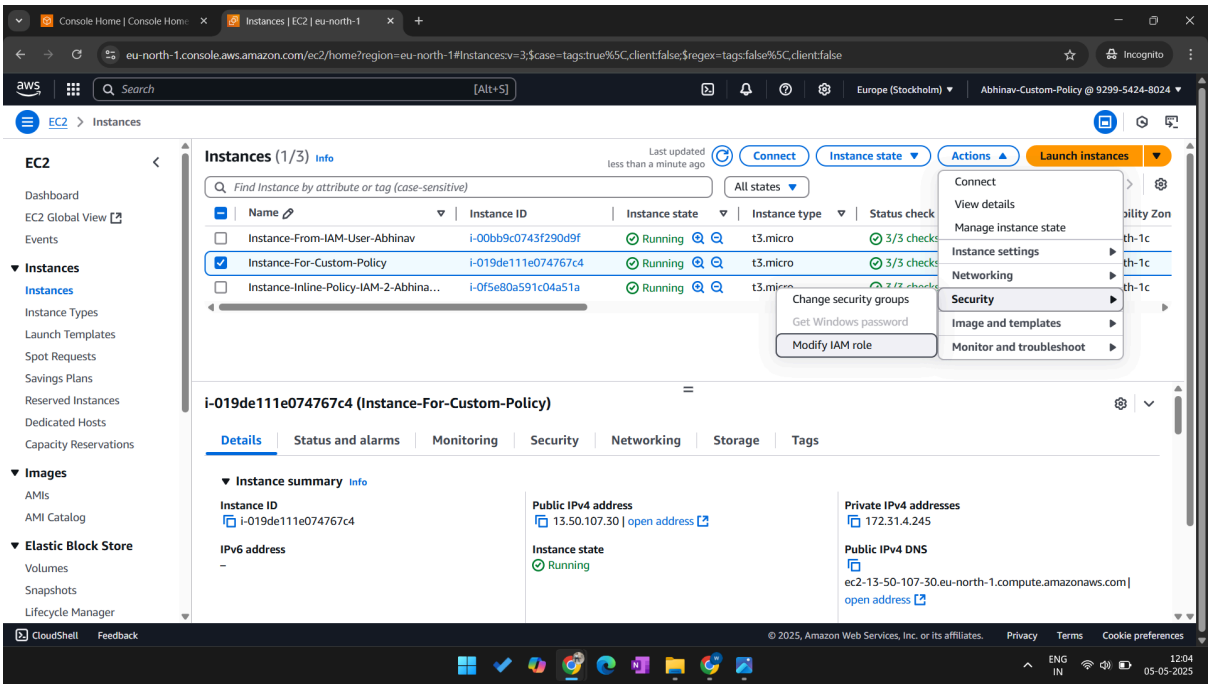

us-east-1.console.aws.amazon.com/iam/home?region=us-east-1#/users/details/Abhinav-Custom-Policy/add-permissions
Search
[Alt+S]
Global
Abhinav Chandra MS
IAM
Users
Abhinav-Custom-Policy
Add permissions
Step 1
Add permissions
Step 2
Review
Add permissions
Add user to an existing group or create a new one. 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, inline policies, and any existing permissions boundaries 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.
Permissions policies (1/1346)
Filter by Type
Search
Customer managed
1 match
Policy name
Type
Attached entities
Customer-Managed-Policy-EC2-to-S3FullA...
Customer managed
0
Cancel
Next

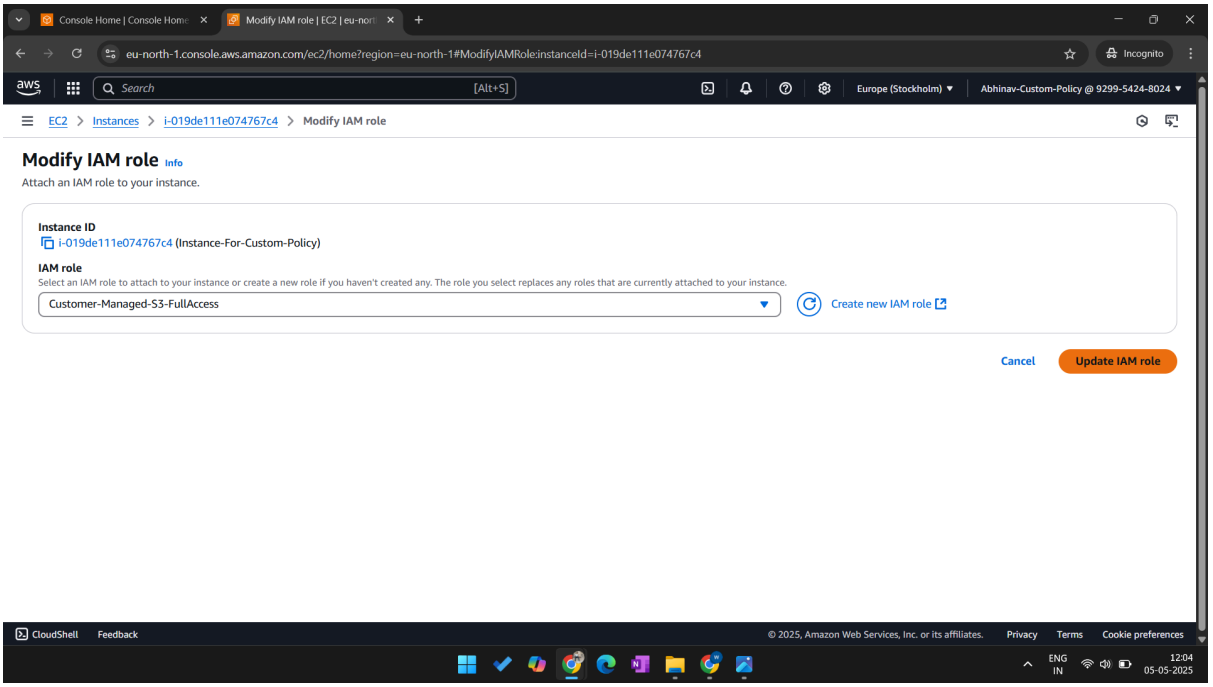

CloudShell
Feedback
© 2025, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences
ENG
IN
12:03
05-05-2025

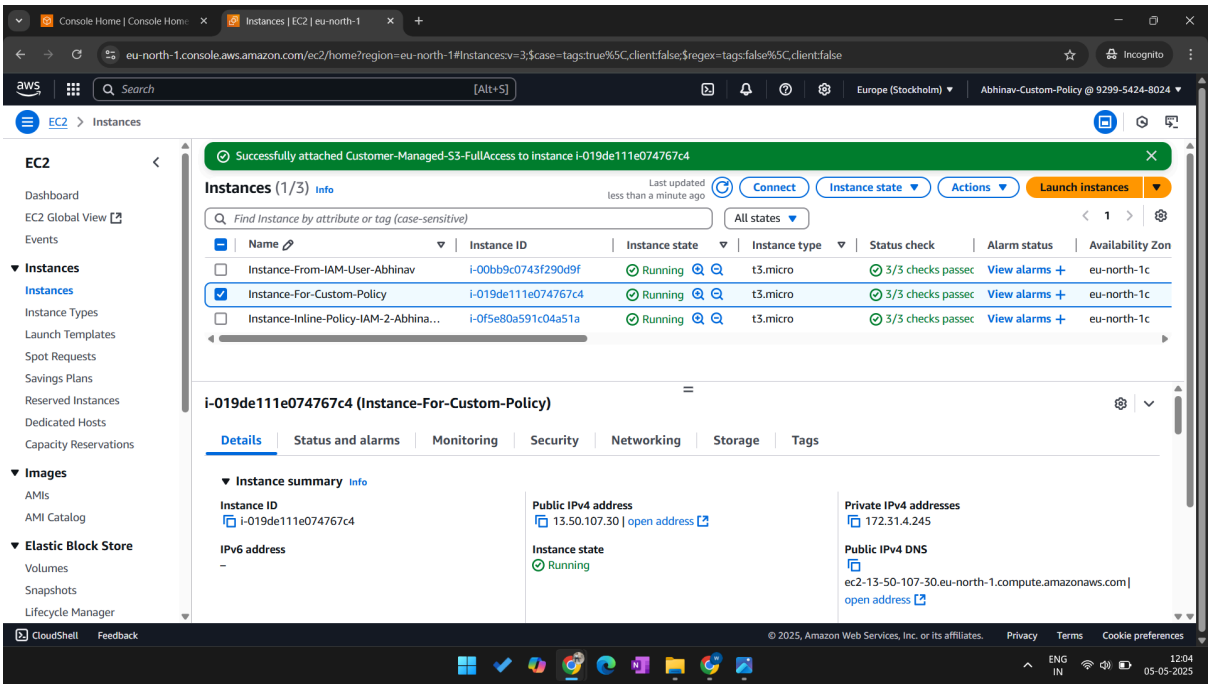

us-east-1.console.aws.amazon.com/iam/home?region=us-east-1#/users/details/Abhinav-Custom-Policy/add-permissions
Search
[Alt+S]
Global
Abhinav Chandra MS
IAM
Users
Abhinav-Custom-Policy
Add permissions
Step 1
Add permissions
Step 2
Review
Review
The following policies will be attached to this user. Learn more
User details
User name
Abhinav-Custom-Policy
Permissions summary (1)
Name
Type
Used as
Customer-Managed-Policy-EC2-to-S3FullAccess
Customer managed
Permissions policy
Cancel
Previous
Add permissions

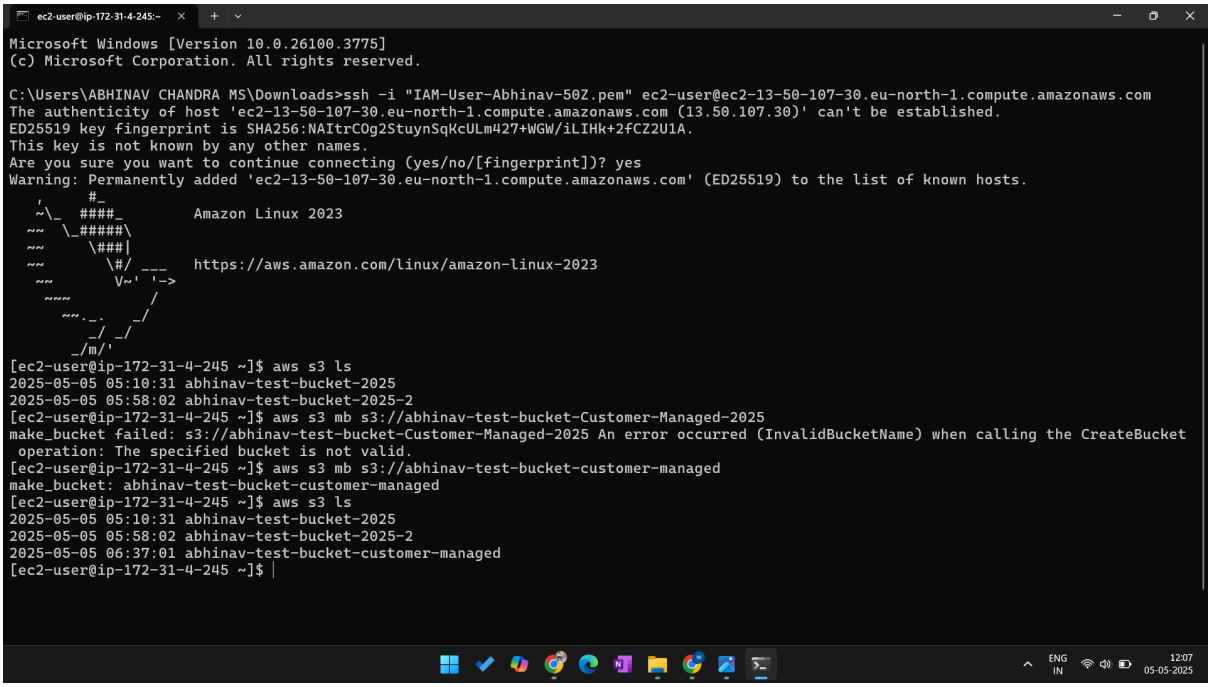

CloudShell
Feedback
© 2025, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences
ENG
IN
12:04
05-05-2025


us-east-1.console.aws.amazon.com/iam/home?region=us-east-1#/users/details/Abhinav-Custom-Policy?section=permissions
IAM > Users > Abhinav-Custom-Policy
Identity and Access Management (IAM)
Search IAM
Dashboard
Access management
User groups
Users
Roles
Policies
Identity providers
Account settings
Root access management New
Access reports
Access Analyzer
External access
Unused access
Analyzer settings
Credential report
Abhinav-Custom-Policy Info
Delete
Summary
ARN
arn:aws:iam::929954248024:user/Abhinav-Custom-Policy
Console access
Enabled without MFA
Access key 1
Create access key
Created
May 05, 2025, 11:40 (UTC+05:30)
Last console sign-in
Today
Permissions
Groups
Tags
Security credentials
Last Accessed
Permissions policies (2)
Permissions are defined by policies attached to the user directly or through groups.
Remove
Add permissions
Filter by Type
Search
All types
Policy name
Type
Attached via
AmazonEC2FullAccess
AWS managed
Directly
Customer-Managed-Policy-EC2-to-S3FullA...
Customer managed
Directly
CloudShell
Feedback
© 2025, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences


eu-north-1.console.aws.amazon.com/ec2/home?region=eu-north-1#Instances:v=3;$case=tags:true%5C,client:false;$regex=tags:false%5C,client:false
EC2 > Instances
EC2
Dashboard
EC2 Global View
Events
Instances
Instances
Instance Types
Launch Templates
Spot Requests
Savings Plans
Reserved Instances
Dedicated Hosts
Capacity Reservations
Images
AMIs
AMI Catalog
Elastic Block Store
Volumes
Snapshots
Lifecycle Manager
Instances (1/3) Info
Last updated less than a minute ago
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
Instance-From-IAM-User-Abhinav
i-00bb9c0743f290d9f
Running
t3.micro
3/3 checks
Instance-For-Custom-Policy
i-019de111e074767c4
Running
t3.micro
3/3 checks
Instance-Inline-Policy-IAM-2-Abhina...
i-0f5e80a591c04a51a
Running
Connect
View details
Manage instance state
Instance settings
Networking
Security
Image and templates
Monitor and troubleshoot
Change security groups
Get Windows password
Modify IAM role
i-019de111e074767c4 (Instance-For-Custom-Policy)
Details
Status and alarms
Monitoring
Security
Networking
Storage
Tags
Instance summary Info
Instance ID
i-019de111e074767c4
Public IPv4 address
13.50.107.30 | open address
Private IPv4 addresses
172.31.4.245
IPv6 address
Instance state
Running
Public IPv4 DNS
ec2-13-50-107-30.eu-north-1.compute.amazonaws.com | open address
CloudShell
Feedback
© 2025, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences


Console Home | Console Home
Modify IAM role | EC2 | eu-north-1
eu-north-1.console.aws.amazon.com/ec2/home?region=eu-north-1#ModifyIAMRole:instanceId=i-019de111e074767c4
Incognito
Search [Alt+S]
Europe (Stockholm)
Abhinav-Custom-Policy @ 9299-5424-8024
EC2 > Instances > i-019de111e074767c4 > Modify IAM role
Modify IAM role Info
Attach an IAM role to your instance.
Instance ID
i-019de111e074767c4 (Instance-For-Custom-Policy)
IAM role
Select an IAM role to attach to your instance or create a new role if you haven't created any. The role you select replaces any roles that are currently attached to your instance.
Customer-Managed-S3-FullAccess
Create new IAM role
Cancel
Update IAM role
CloudShell
Feedback
© 2025, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences
ENG
IN
12:04
05-05-2025


Console Home | Console Home
Instances | EC2 | eu-north-1
eu-north-1.console.aws.amazon.com/ec2/home?region=eu-north-1#Instances:v=3;$case=tags:true%5C,client:false;$regex=tags:false%5C,client:false
Incognito
Search [Alt+S]
Europe (Stockholm)
Abhinav-Custom-Policy @ 9299-5424-8024
EC2 > Instances
EC2
Dashboard
EC2 Global View
Events
Instances
Instances
Instance Types
Launch Templates
Spot Requests
Savings Plans
Reserved Instances
Dedicated Hosts
Capacity Reservations
Images
AMIs
AMI Catalog
Elastic Block Store
Volumes
Snapshots
Lifecycle Manager
Successfully attached Customer-Managed-S3-FullAccess to instance i-019de111e074767c4
Instances (1/3) Info
Last updated less than a minute ago
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 Zon
Instance-From-IAM-User-Abhinav
i-00bb9c0743f290d9f
Running
t3.micro
3/3 checks passec
View alarms
eu-north-1c
Instance-For-Custom-Policy
i-019de111e074767c4
Running
t3.micro
3/3 checks passec
View alarms
eu-north-1c
Instance-Inline-Policy-IAM-2-Abhina...
i-0f5e80a591c04a51a
Running
t3.micro
3/3 checks passec
View alarms
eu-north-1c
i-019de111e074767c4 (Instance-For-Custom-Policy)
Details
Status and alarms
Monitoring
Security
Networking
Storage
Tags
Instance summary Info
Instance ID
i-019de111e074767c4
IPv6 address
–
Public IPv4 address
13.50.107.30 | open address
Instance state
Running
Private IPv4 addresses
172.31.4.245
Public IPv4 DNS
ec2-13-50-107-30.eu-north-1.compute.amazonaws.com | open address
CloudShell
Feedback
© 2025, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences
ENG
IN
12:04
05-05-2025


ec2-user@ip-172-31-4-245:~
Microsoft Windows [Version 10.0.26100.3775]
(c) Microsoft Corporation. All rights reserved.
C:\Users\ABHINAV CHANDRA MS\Downloads>ssh -i "IAM-User-Abhinav-50Z.pem" ec2-user@ec2-13-50-107-30.eu-north-1.compute.amazonaws.com
The authenticity of host 'ec2-13-50-107-30.eu-north-1.compute.amazonaws.com (13.50.107.30)' can't be established.
ED25519 key fingerprint is SHA256:NAItrCOg2StuynSqKcULm427+WGW/iLIHk+2fCZ2U1A.
This key is not known by any other names.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added 'ec2-13-50-107-30.eu-north-1.compute.amazonaws.com' (ED25519) to the list of known hosts.
Amazon Linux 2023
https://aws.amazon.com/linux/amazon-linux-2023
[ec2-user@ip-172-31-4-245 ~]$ aws s3 ls
2025-05-05 05:10:31 abhinav-test-bucket-2025
2025-05-05 05:58:02 abhinav-test-bucket-2025-2
[ec2-user@ip-172-31-4-245 ~]$ aws s3 mb s3://abhinav-test-bucket-Customer-Managed-2025
make_bucket failed: s3://abhinav-test-bucket-Customer-Managed-2025 An error occurred (InvalidBucketName) when calling the CreateBucket operation: The specified bucket is not valid.
[ec2-user@ip-172-31-4-245 ~]$ aws s3 mb s3://abhinav-test-bucket-customer-managed
make_bucket: abhinav-test-bucket-customer-managed
[ec2-user@ip-172-31-4-245 ~]$ aws s3 ls
2025-05-05 05:10:31 abhinav-test-bucket-2025
2025-05-05 05:58:02 abhinav-test-bucket-2025-2
2025-05-05 06:37:01 abhinav-test-bucket-customer-managed
[ec2-user@ip-172-31-4-245 ~]$
ENG
IN
12:07
05-05-2025