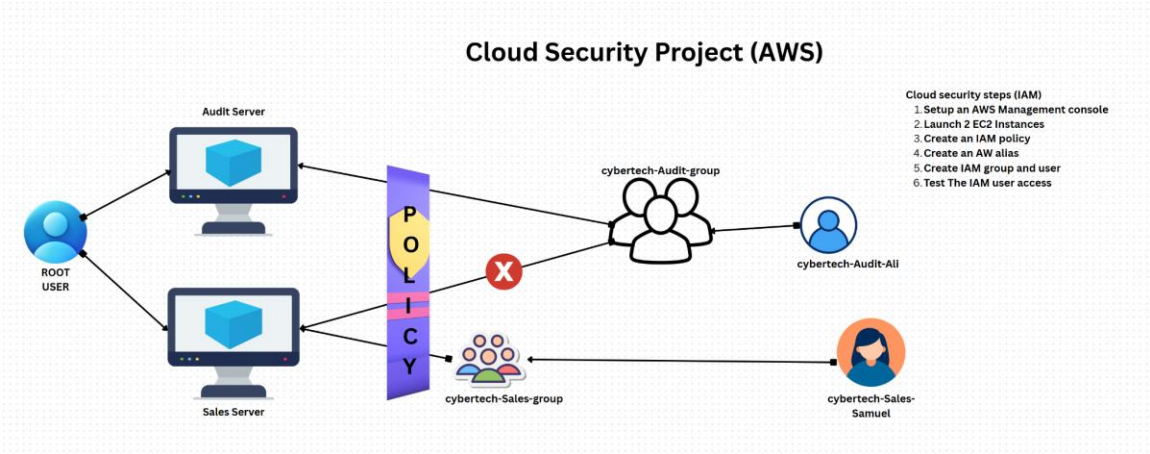
AWS IAM Cloud Security Project

1. Project Overview

I completed this project on cloud security controls in Amazon Web Services (AWS), focusing on Identity and Access Management (IAM). The goal was to create a least- privilege policy, attach it to a user or group, and verify that the policy correctly restricts actions on Amazon EC2 instance.



In this project, we will be creating Users, User groups, buckets, trails, polices implementing those policies and verifying them.

Standard practice prescribes that we don't do anything on root user, however we can use it to create a user with admin privileges.

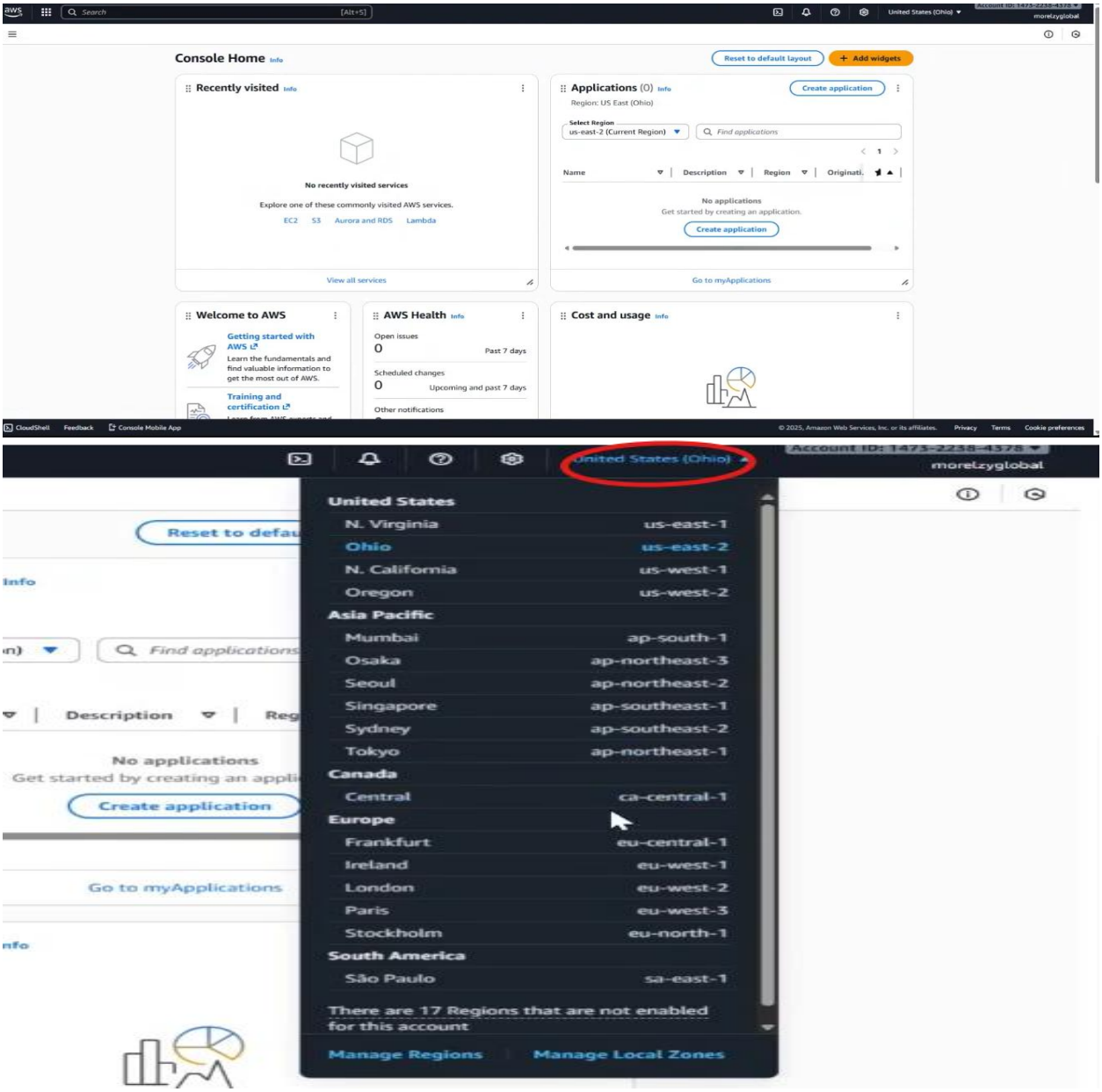
In AWS, we use services to create everything

Firstly we can create an AWS trail account for 6 month on the website at [Cloud Computing Services - Amazon Web Services (AWS)](), a credit card will be required however you will get a credit to use to run your simulation.

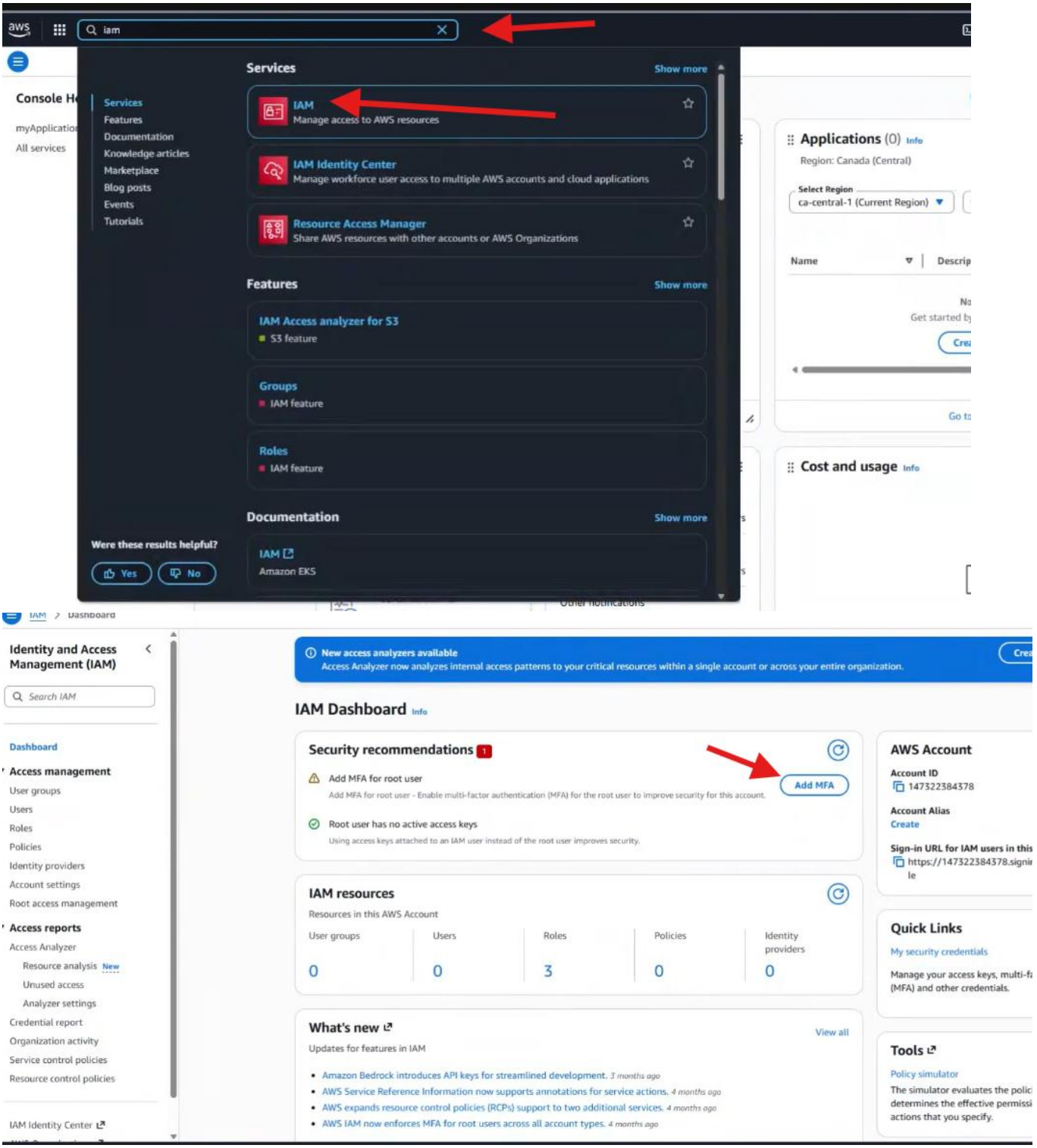
CREATING THE IAM USER AND GROUPS

Upon creating an account and logging in, it will be a root user, so we will set up MFA (to make it secure) and create a user with admin privileges.

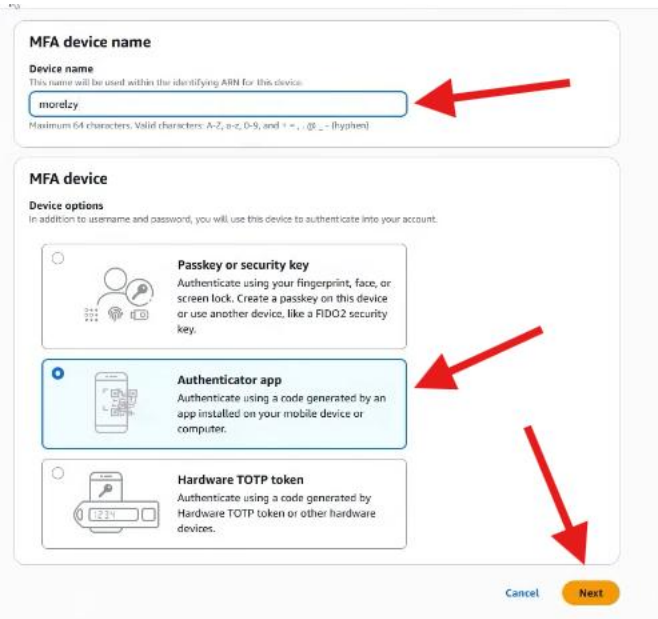
Firstly, we change our geographical location

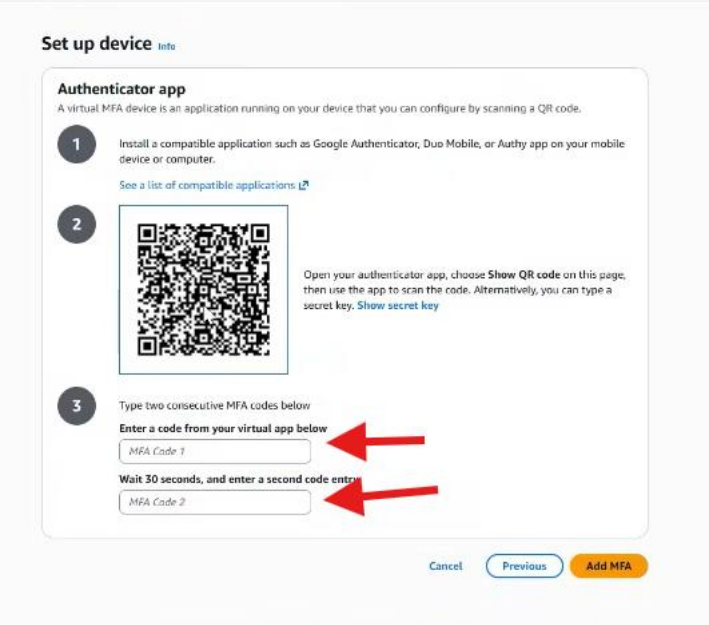


In the search bar, find the IAM service , as best practice, set up MFA

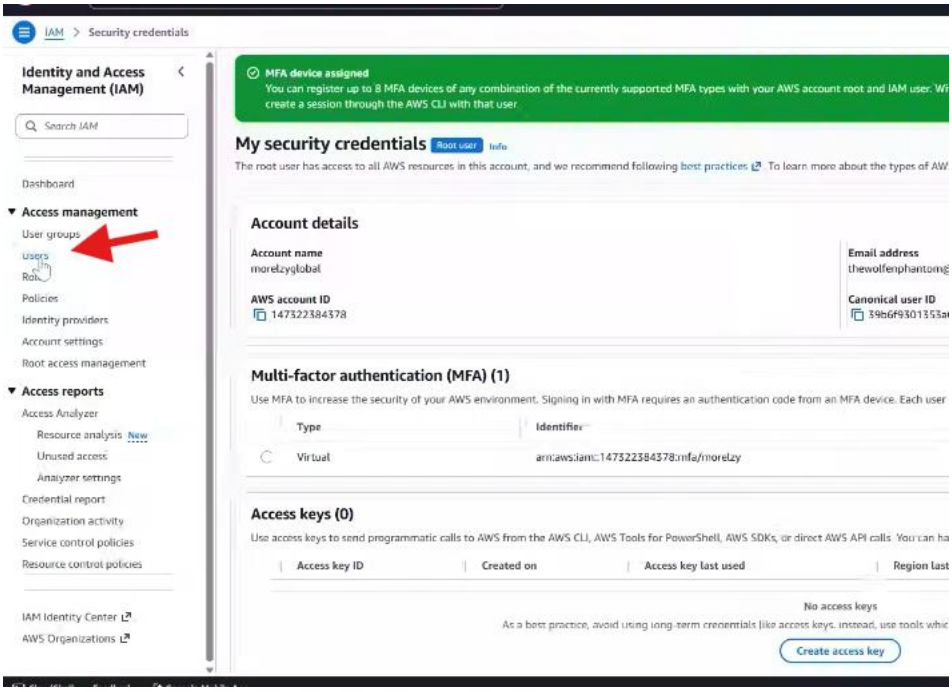


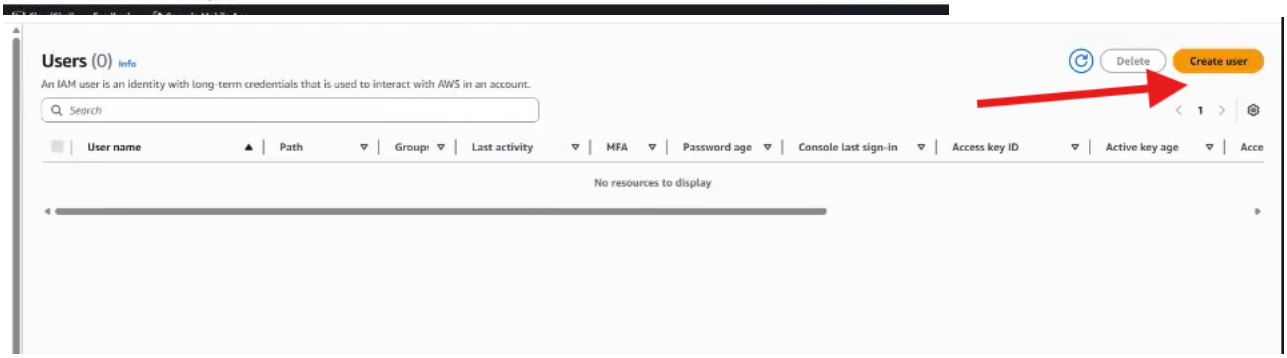
Give the device a name and select a MFA device of your choice, in this instance we will use an Authentication app





Now, we will set up our user, on the left side, under Access management, select user and select “create user”

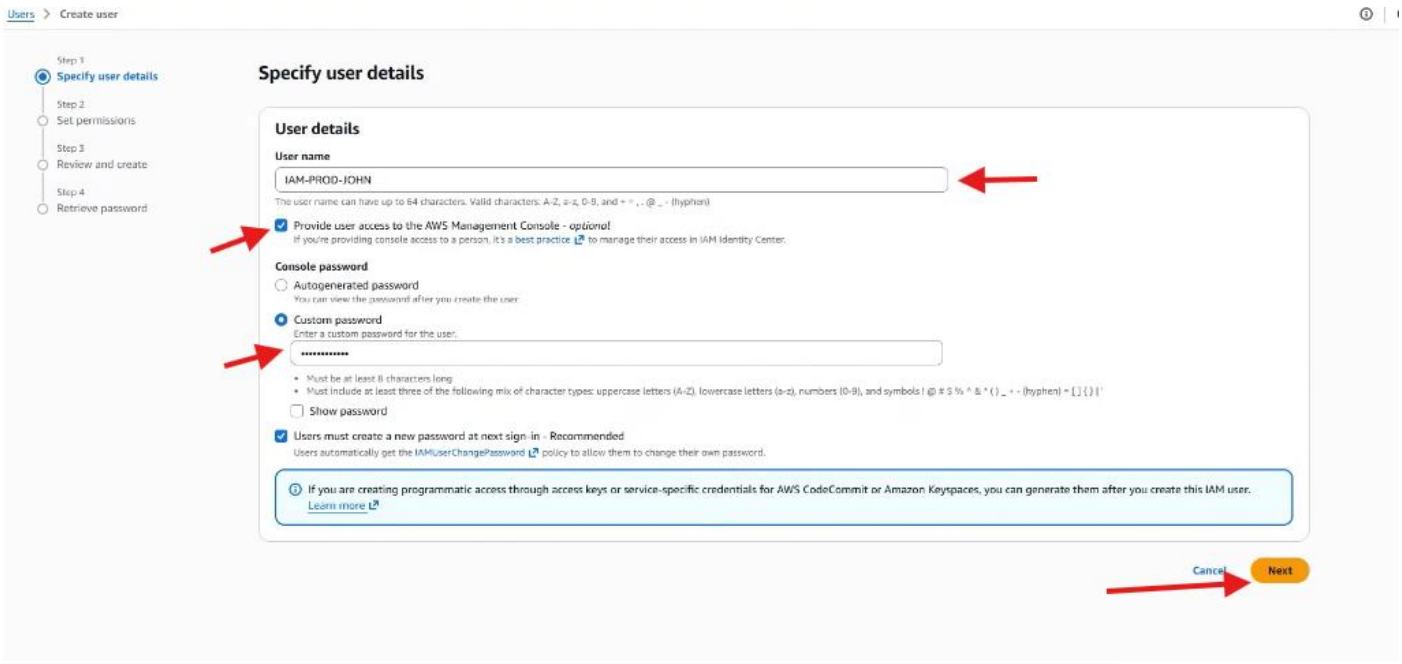


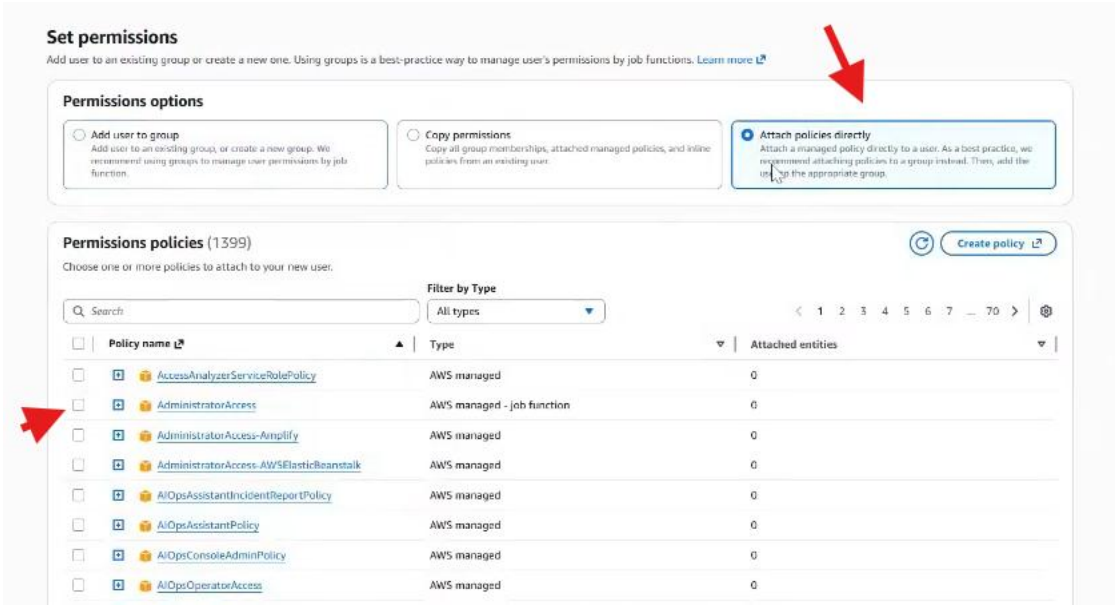


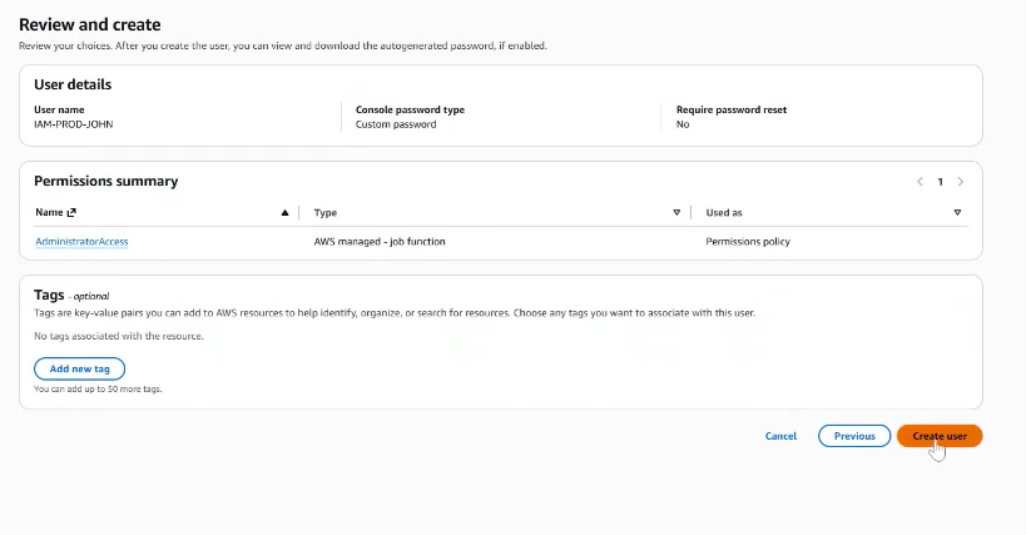
Give the user a name (have a naming convention that easily allows you identify the user, their unit and job)

Ensure you select “access to AWS management console” so this user can be used as admin account instead of the root account, create a password (and best practice select create a new password on sign in, however for this project we won’t choose this option)

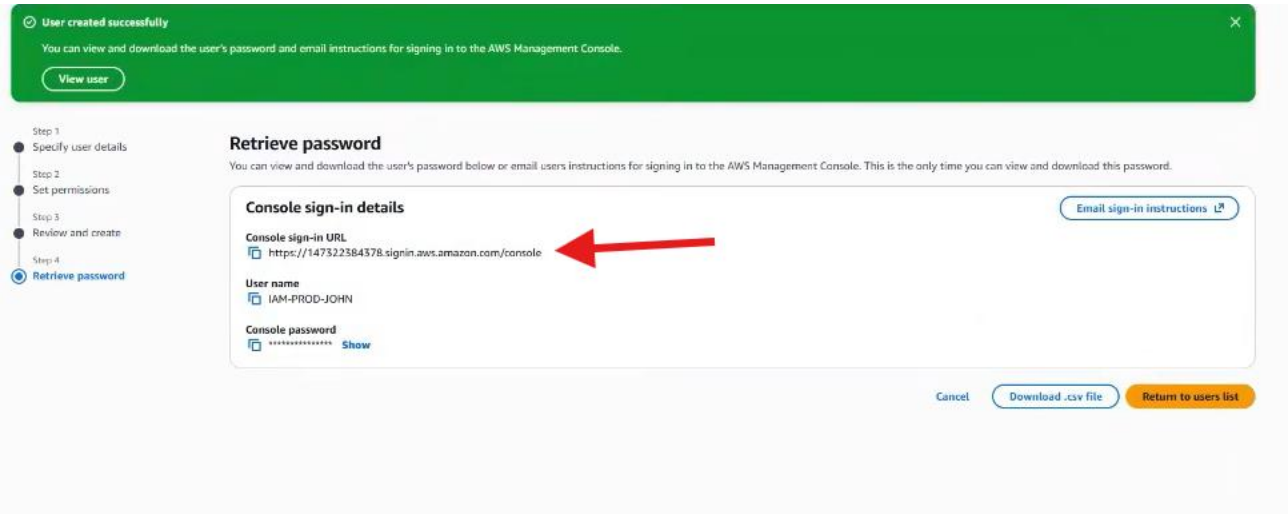
Then set permission using the steps below and create the user

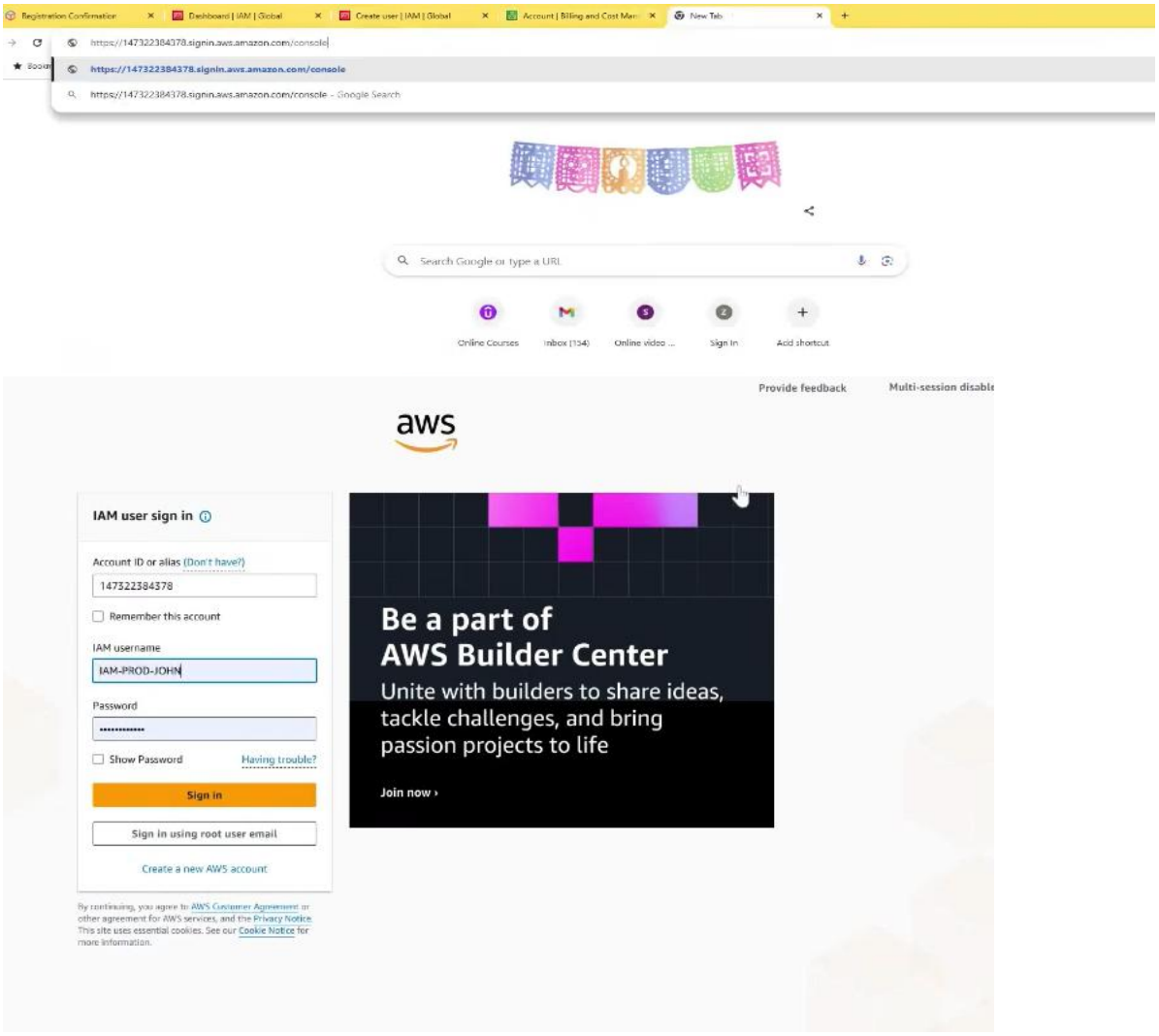

Users > Create user
Step 1
Specify user details
Step 2
Set permissions
Step 3
Review and create
Step 4
Retrieve password
Specify user details
User details
User name
IAM-PROD-JOHN
The user name can have up to 64 characters. Valid characters: A-Z, a-z, 0-9, and + = , . @ _ - (hyphen)
Provide user access 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
Cancel
Next


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 (1399)
Choose one or more policies to attach to your new user.
Create policy
Filter by Type
Search
All types
1 2 3 4 5 6 7 ... 70
Policy name
Type
Attached entities
AccessAnalyzerServiceRolePolicy AWS managed 0
AdministratorAccess AWS managed - job function 0
AdministratorAccess-Amplify AWS managed 0
AdministratorAccess-AWSElasticBeanstalk AWS managed 0
AIOpsAssistantIncidentReportPolicy AWS managed 0
AIOpsAssistantPolicy AWS managed 0
AIOpsConsoleAdminPolicy AWS managed 0
AIOpsOperatorAccess AWS managed 0

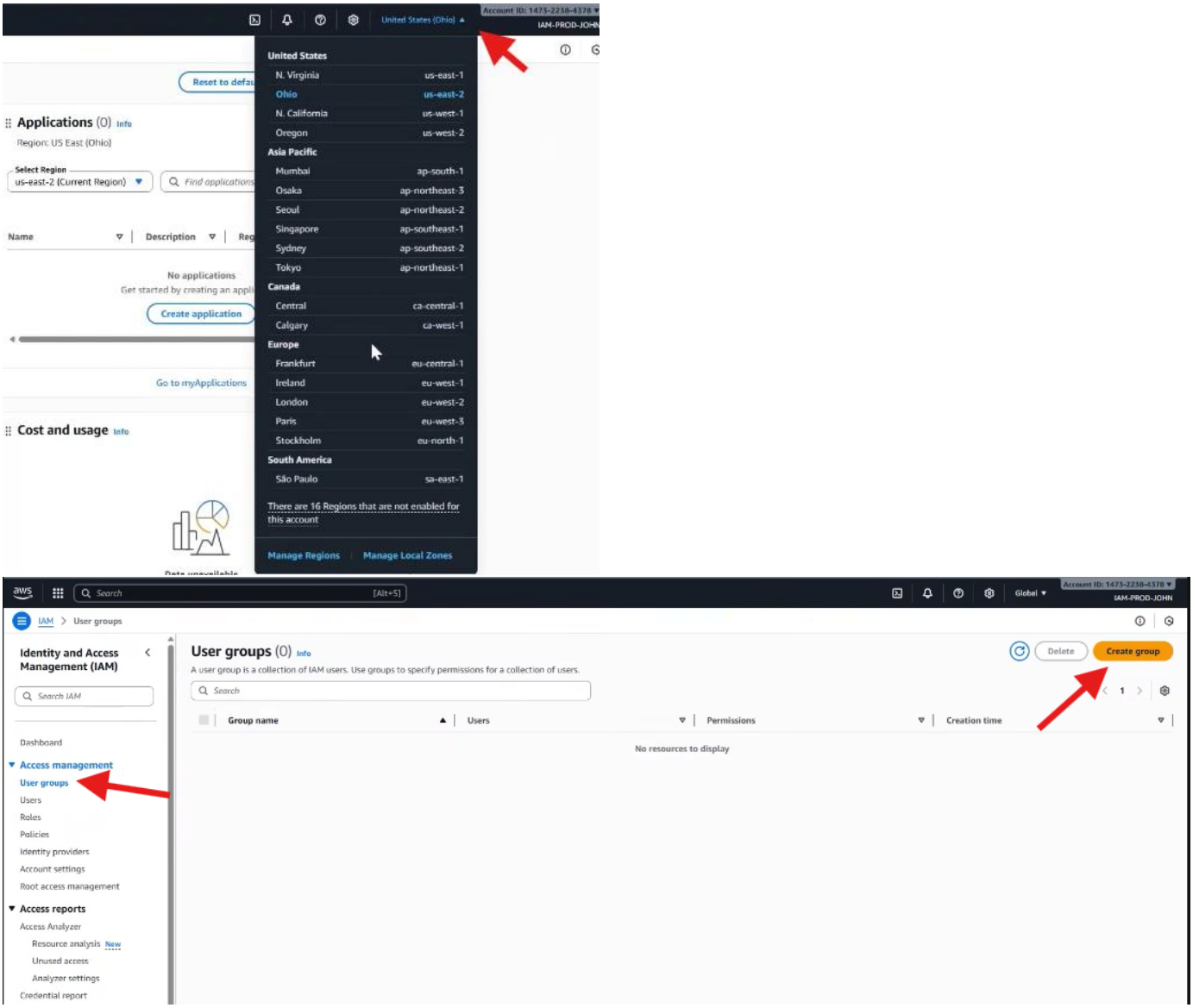


Once user is created, copy the sign-in URL and log in as the user created



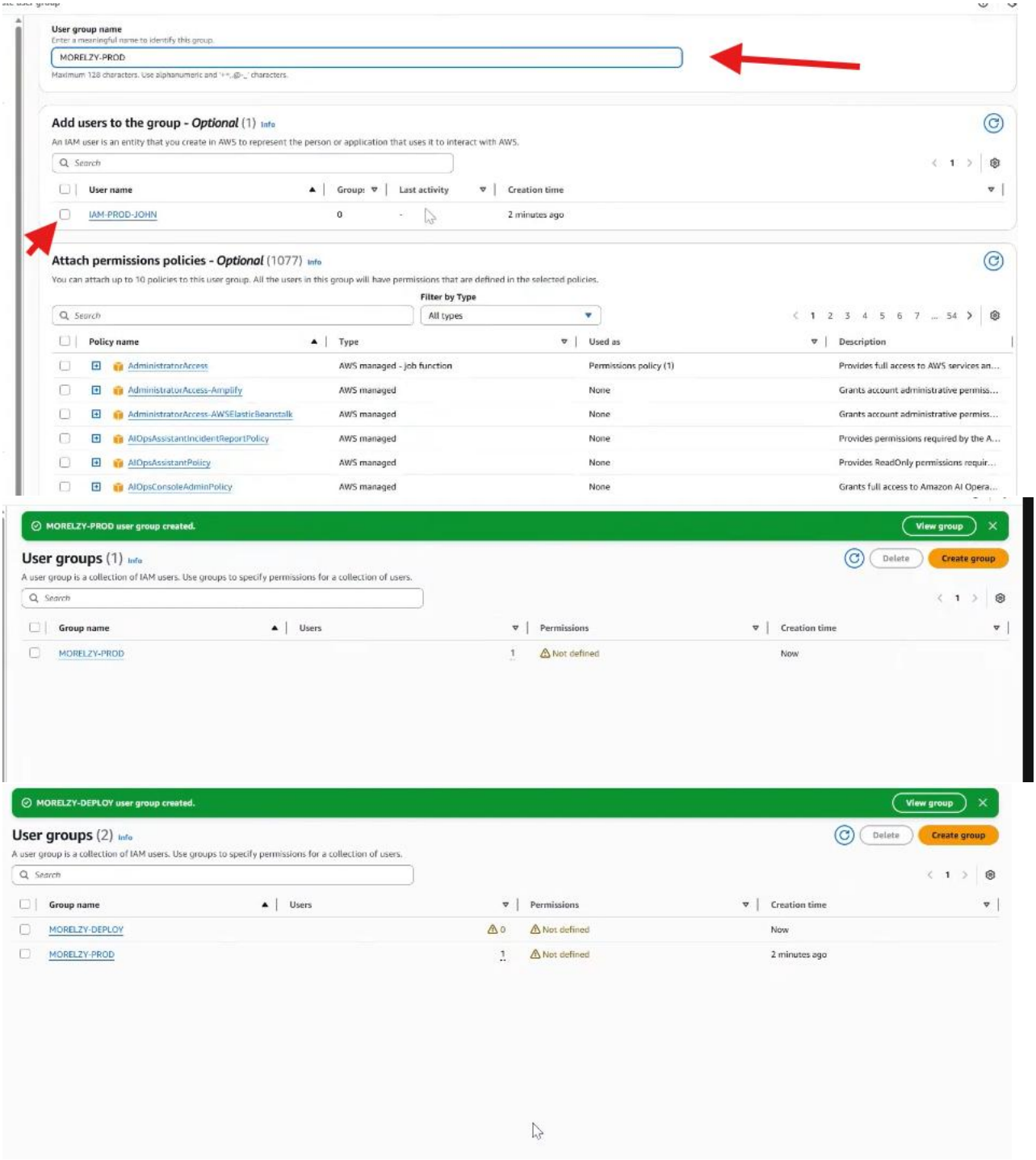


Change the location and let’s create user groups

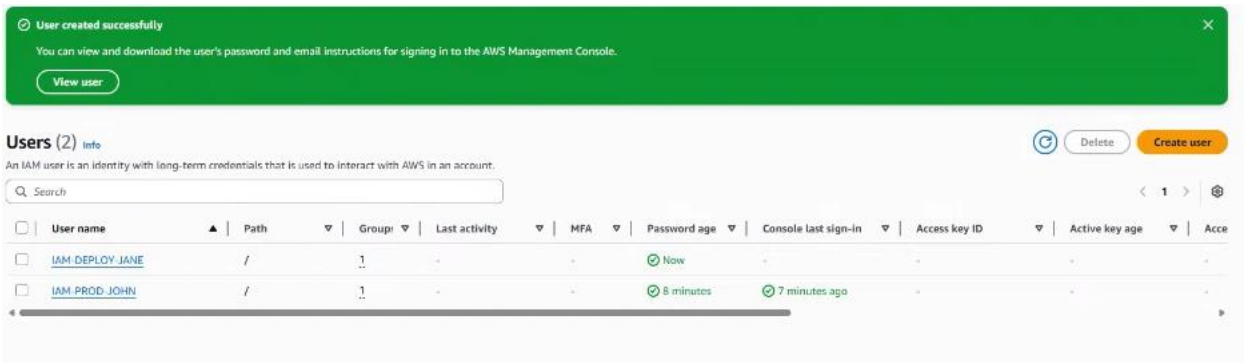


Give the group a name, select the user you want to add to the group and create group.

Create as many groups as required for the organization



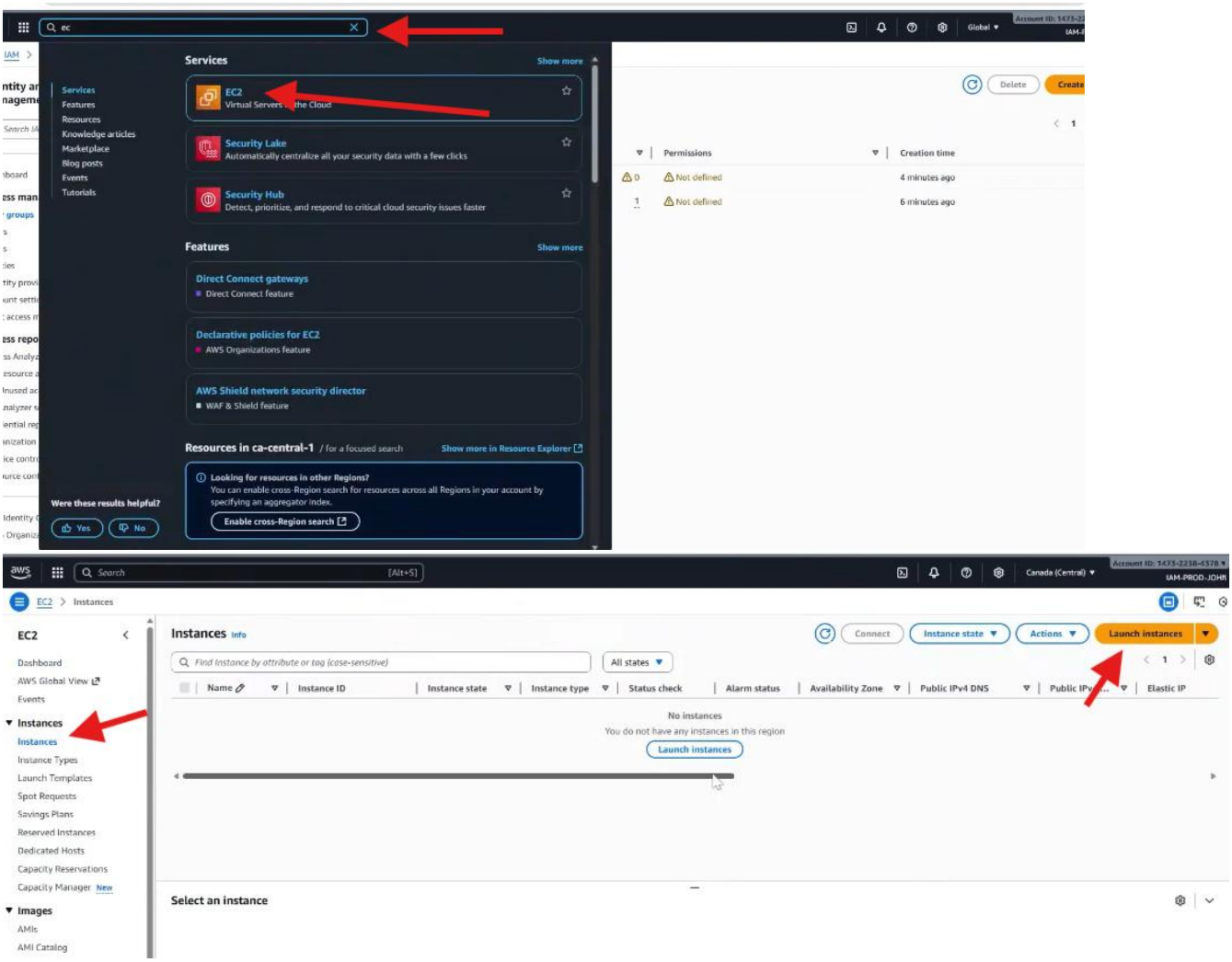
Using the same steps, create as many users as required and assign them to their respective groups



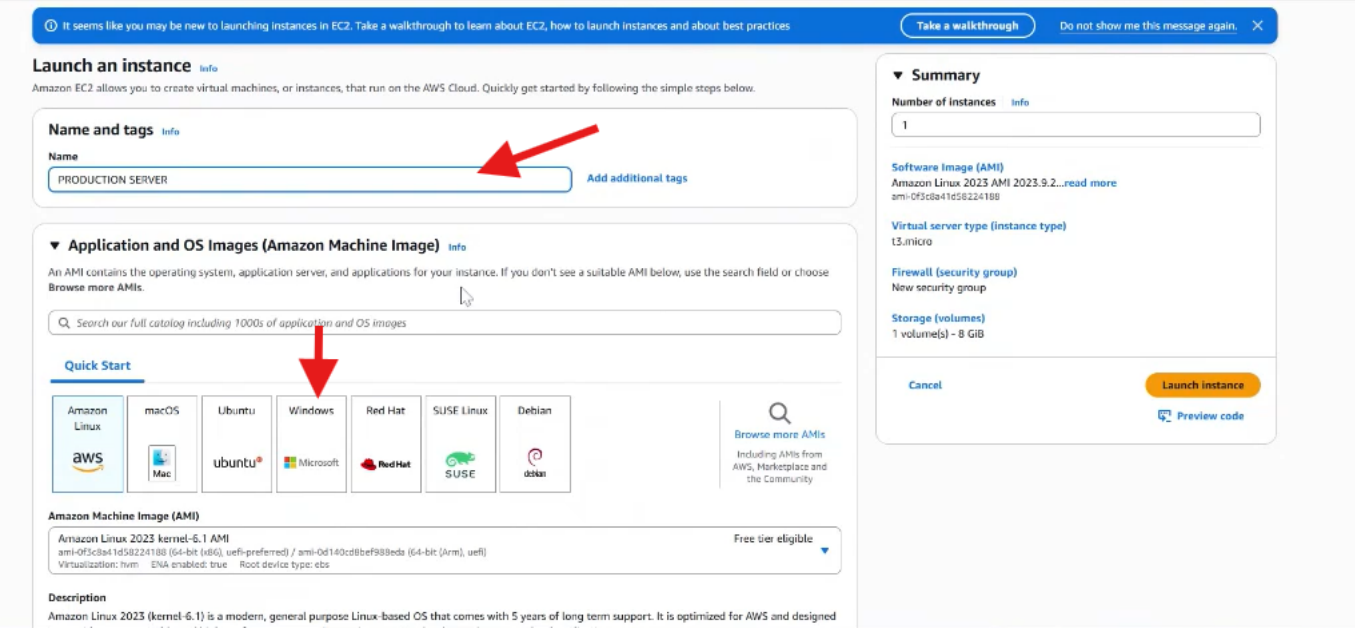
CREATING THE EC2 INSTANCE

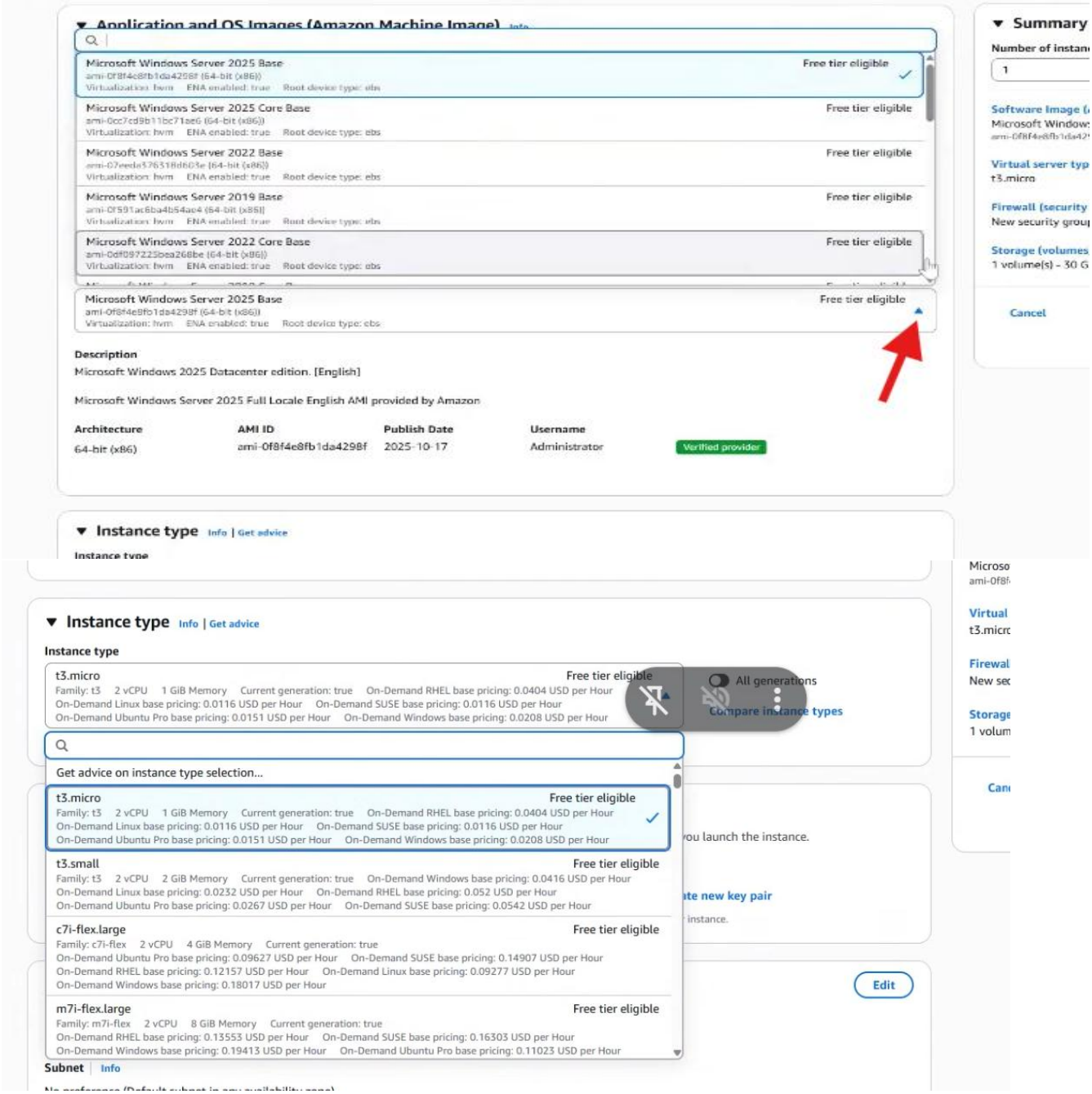
In the search bar, type EC2, under Instances select launch instance

(Instances are also referred to as Servers)

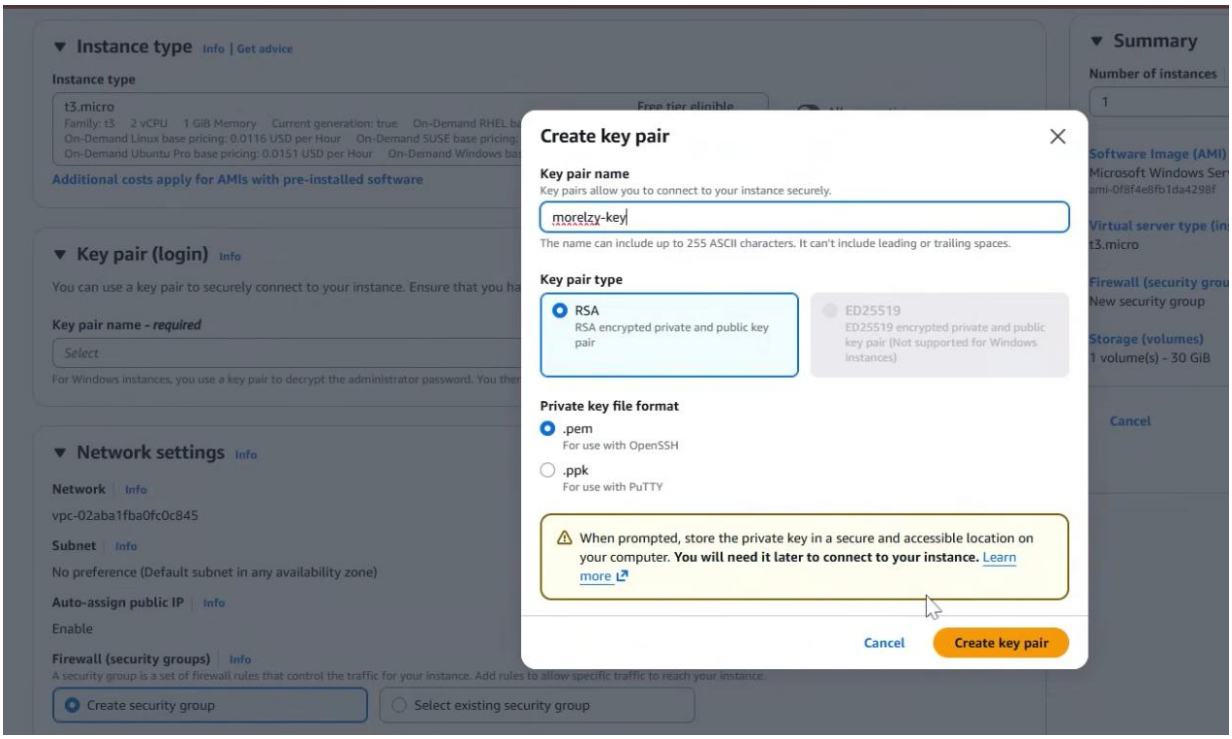


Give the instance a name and select the OS you would like to install and the configuration.

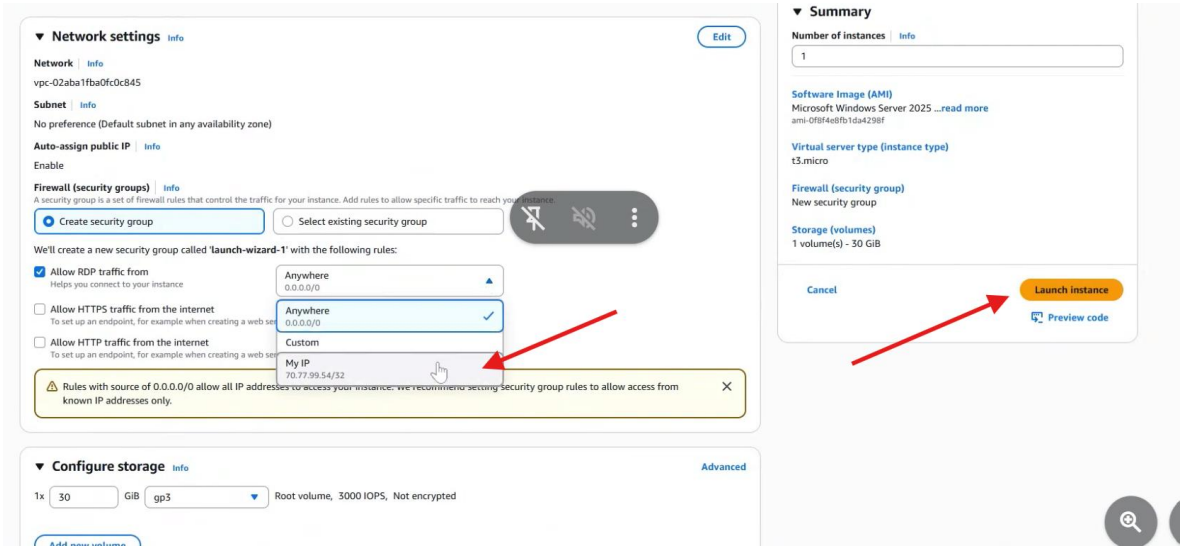


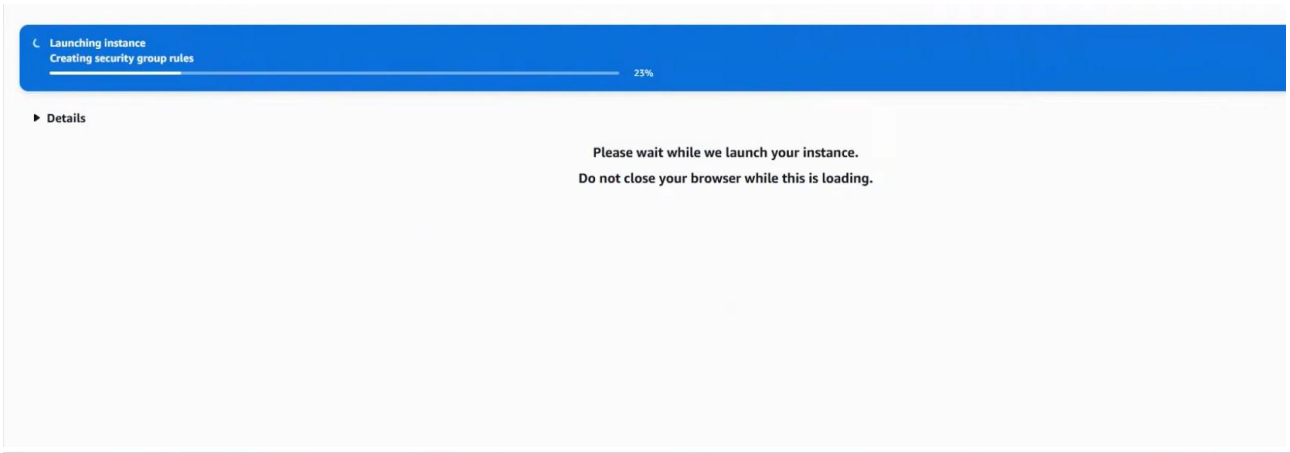


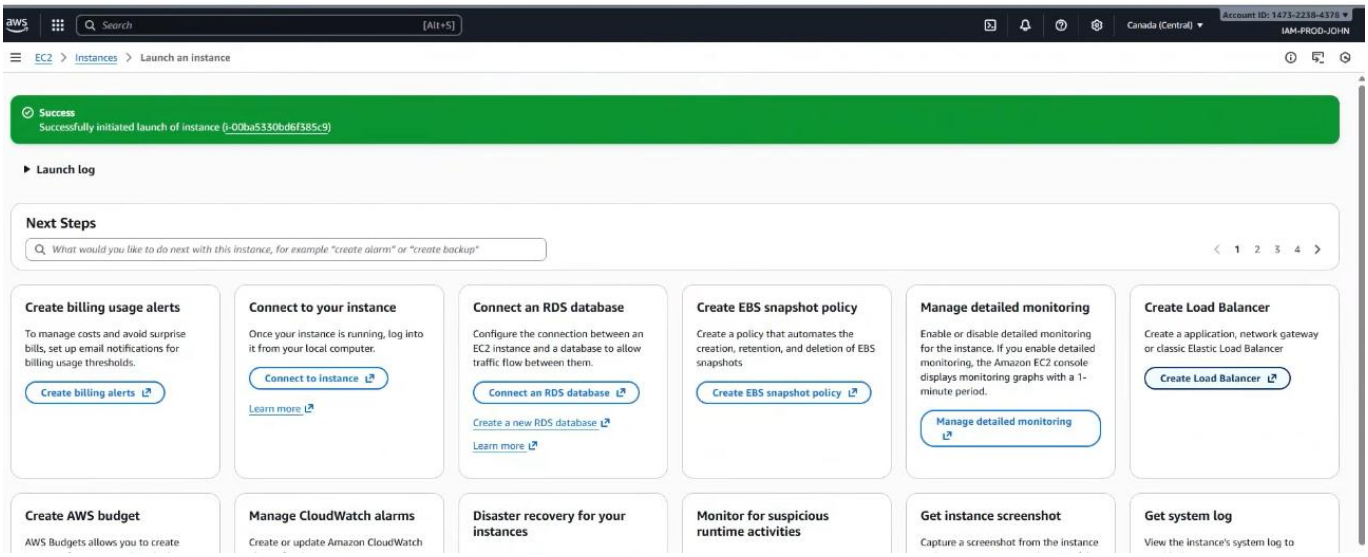
Next we create Key pair for encryption, we give it a name and create, a copy of the key will be downloaded to the PC

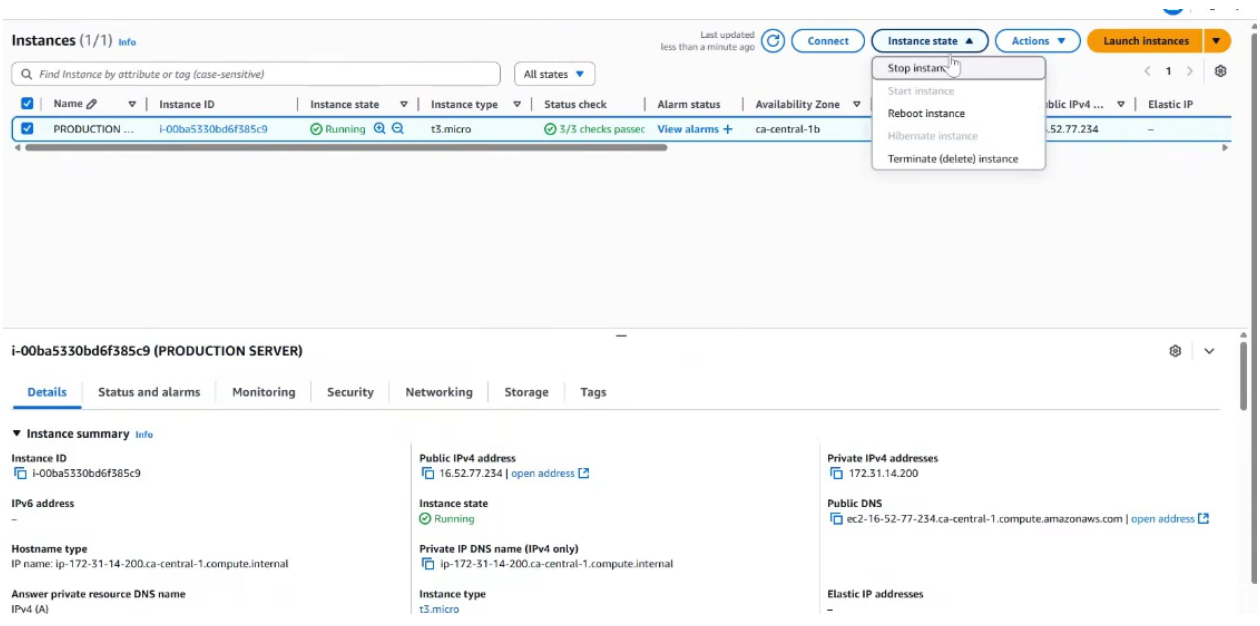


For the network setting, we choose RDP from “my IP” and launch instance



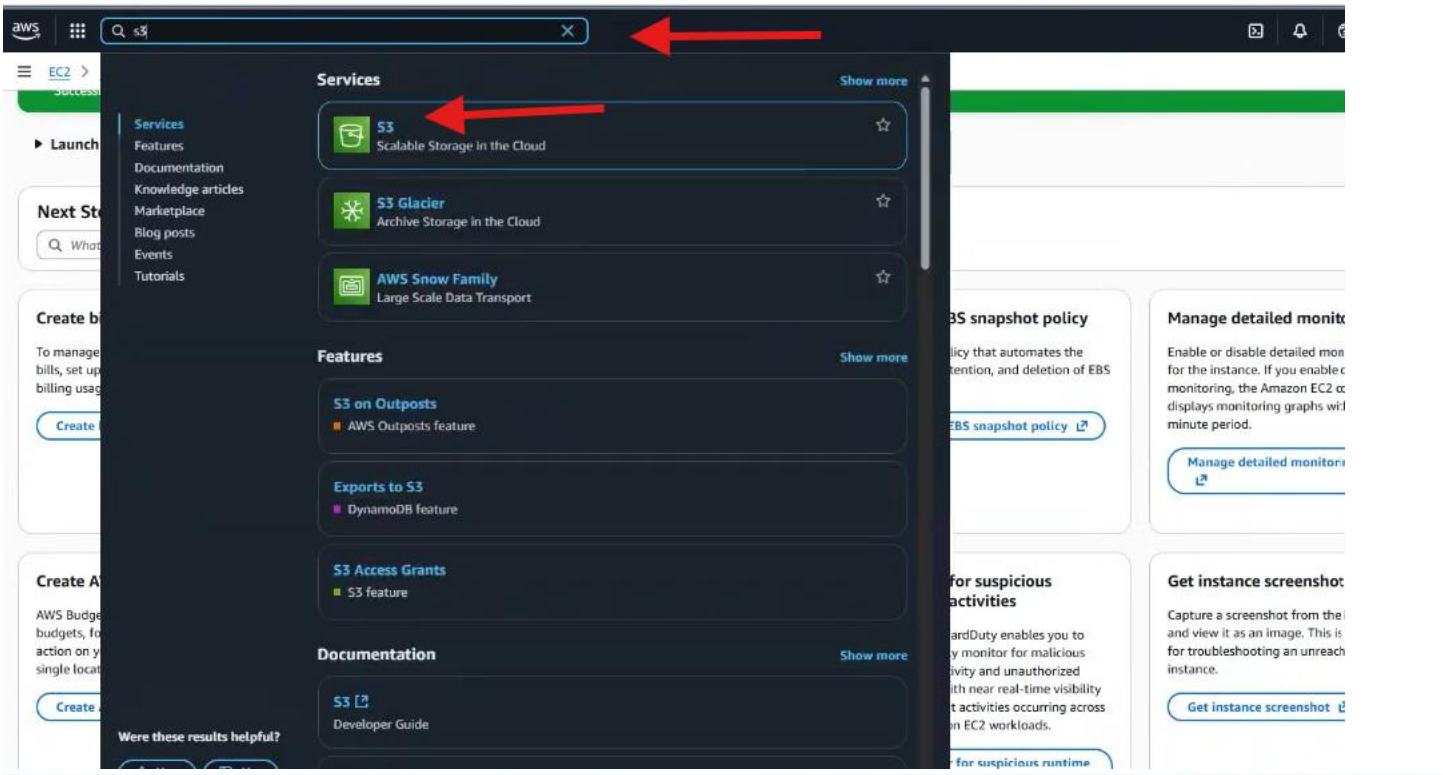

Launching instance
Creating security group rules
25%
Details
Please wait while we launch your instance.
Do not close your browser while this is loading.

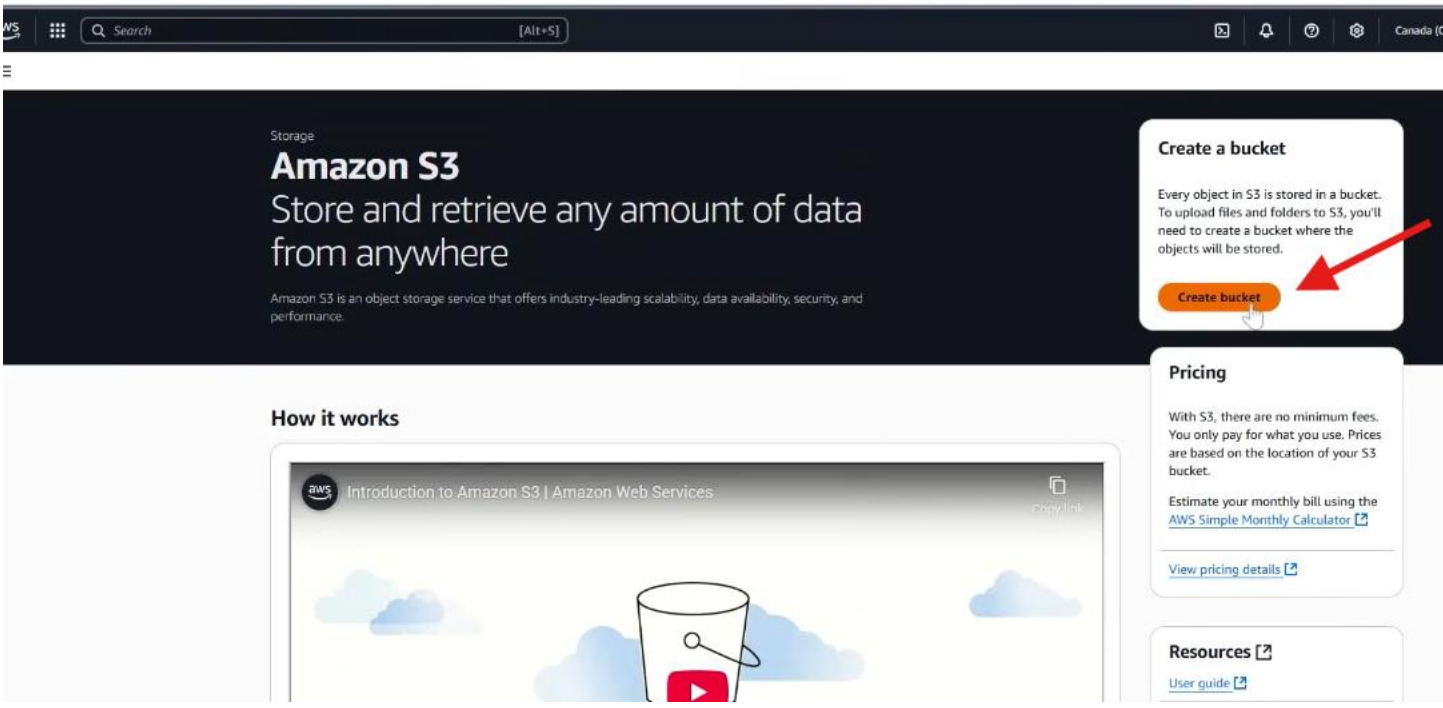

Search
[Alt+S]
Canada (Central)
IAM-PROD-JOHN
EC2 > Instances > Launch an instance
Success
Successfully initiated launch of instance (i-00ba5330bd6f385c9)
Launch log
Next Steps
What would you like to do next with this instance, for example "create alarm" or "create backup"
Create billing usage alerts
To manage costs and avoid surprise bills, set up email notifications for billing usage thresholds.
Create billing alerts
Connect to your instance
Once your instance is running, log into it from your local computer.
Connect to instance
Learn more
Connect an RDS database
Configure the connection between an EC2 instance and a database to allow traffic flow between them.
Connect an RDS database
Create a new RDS database
Learn more
Create EBS snapshot policy
Create a policy that automates the creation, retention, and deletion of EBS snapshots
Create EBS snapshot policy
Manage detailed monitoring
Enable or disable detailed monitoring for the instance. If you enable detailed monitoring, the Amazon EC2 console displays monitoring graphs with a 1-minute period.
Manage detailed monitoring
Create Load Balancer
Create a application, network gateway or classic Elastic Load Balancer
Create Load Balancer
Create AWS budget
AWS Budgets allows you to create
Manage CloudWatch alarms
Create or update Amazon CloudWatch
Disaster recovery for your instances
Monitor for suspicious runtime activities
Get instance screenshot
Capture a screenshot from the instance
Get system log
View the instance's system log to

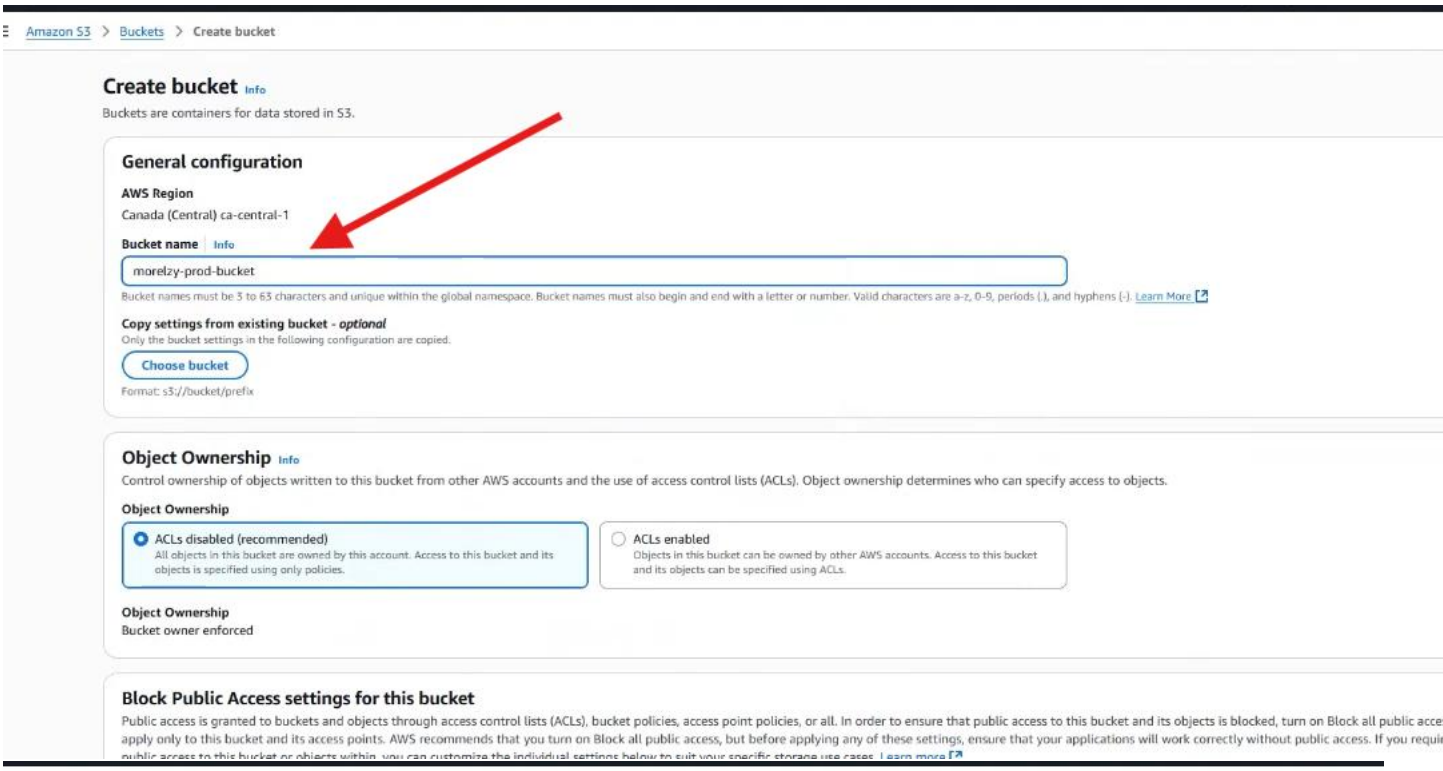

Instances (1/1) Info
Last updated less than a minute ago
Connect
Instance state
Actions
Launch instances
Find Instance by attribute or tag (case-sensitive)
All states
Stop instance
Start instance
Reboot instance
Hibernate instance
Terminate (delete) instance
Name
Instance ID
Instance state
Instance type
Status check
Alarm status
Availability Zone
Elastic IP
PRODUCTION ...
i-00ba5330bd6f385c9
Running
t3.micro
3/3 checks passed
View alarms
ca-central-1b
i-00ba5330bd6f385c9 (PRODUCTION SERVER)
Details
Status and alarms
Monitoring
Security
Networking
Storage
Tags
Instance summary Info
Instance ID
i-00ba5330bd6f385c9
IPv6 address
–
Hostname type
IP name: ip-172-31-14-200.ca-central-1.compute.internal
Answer private resource DNS name
IPv4 (A)
Public IPv4 address
16.52.77.234 | open address
Instance state
Running
Private IP DNS name (IPv4 only)
ip-172-31-14-200.ca-central-1.compute.internal
Instance type
t3.micro
Private IPv4 addresses
172.31.14.200
Public DNS
ec2-16-52-77-234.ca-central-1.compute.amazonaws.com | open address
Elastic IP addresses
–

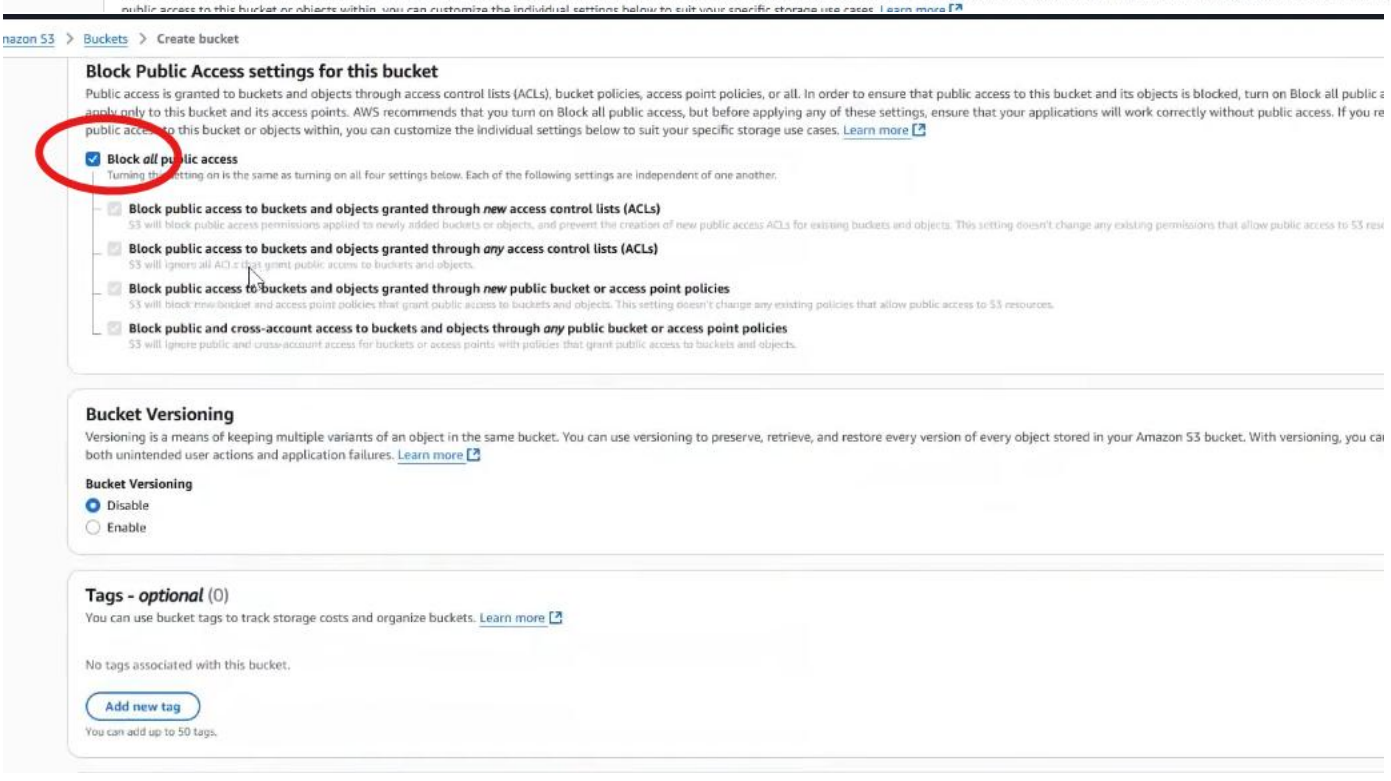
CREATING STORAGE BUCKETS

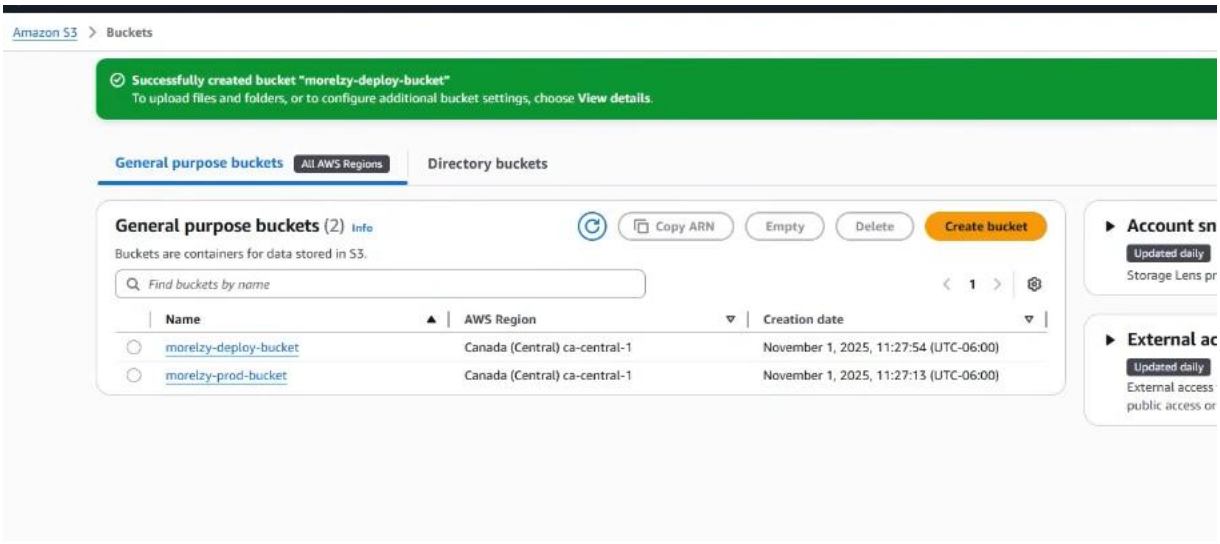
In the search bar, type S3 and create bucket, give it a name and leave default settings



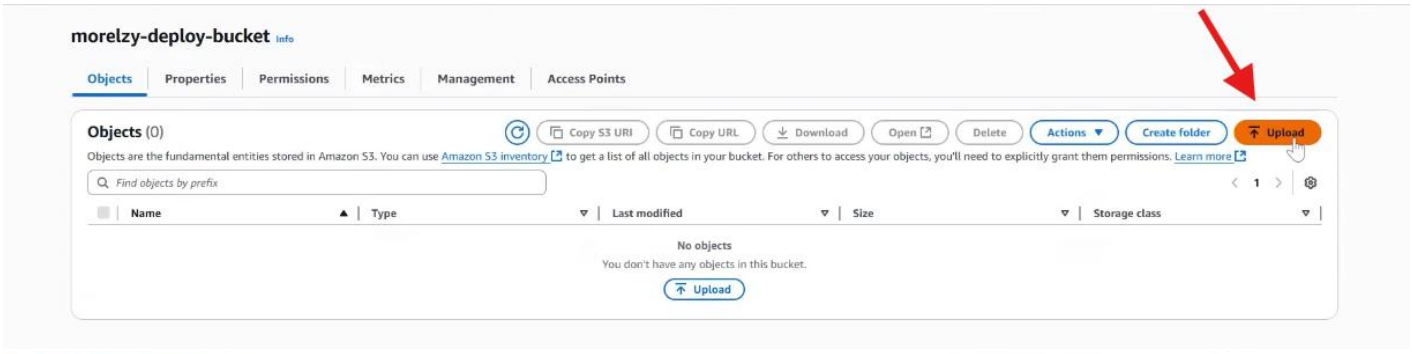


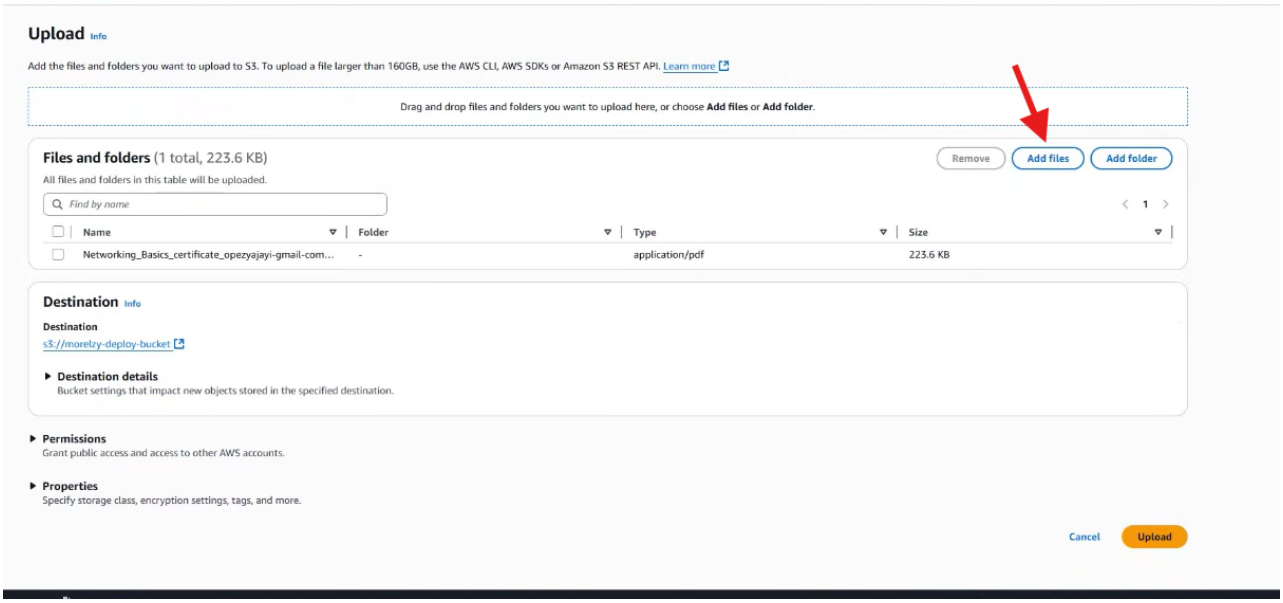

Amazon S3 > Buckets > Create bucket
Create bucket Info
Buckets are containers for data stored in S3.
General configuration
AWS Region
Canada (Central) ca-central-1
Bucket name Info
morelzy-prod-bucket
Bucket names must be 3 to 63 characters and unique within the global namespace. Bucket names must also begin and end with a letter or number. Valid characters are a-z, 0-9, periods (.), and hyphens (-). Learn More
Copy settings from existing bucket - optional
Only the bucket settings in the following configuration are copied.
Choose bucket
Format: s3://bucket/prefix
Object Ownership Info
Control ownership of objects written to this bucket from other AWS accounts and the use of access control lists (ACLs). Object ownership determines who can specify access to objects.
Object Ownership
ACLs disabled (recommended)
All objects in this bucket are owned by this account. Access to this bucket and its objects is specified using only policies.
ACLs enabled
Objects in this bucket can be owned by other AWS accounts. Access to this bucket and its objects can be specified using ACLs.
Object Ownership
Bucket owner enforced
Block Public Access settings for this bucket
Public access is granted to buckets and objects through access control lists (ACLs), bucket policies, access point policies, or all. In order to ensure that public access to this bucket and its objects is blocked, turn on Block all public acce
apply only to this bucket and its access points. AWS recommends that you turn on Block all public access, but before applying any of these settings, ensure that your applications will work correctly without public access. If you requi


nazon S3 > Buckets > Create bucket
Block Public Access settings for this bucket
Public access is granted to buckets and objects through access control lists (ACLs), bucket policies, access point policies, or all. In order to ensure that public access to this bucket and its objects is blocked, turn on Block all public a
apply only to this bucket and its access points. AWS recommends that you turn on Block all public access, but before applying any of these settings, ensure that your applications will work correctly without public access. If you re
public access to this bucket or objects within, you can customize the individual settings below to suit your specific storage use cases. Learn more
Block all public access
Turning this setting on is the same as turning on all four settings below. Each of the following settings are independent of one another.
Block public access to buckets and objects granted through new access control lists (ACLs)
S3 will block public access permissions applied to newly added buckets or objects, and prevent the creation of new public access ACLs for existing buckets and objects. This setting doesn't change any existing permissions that allow public access to S3 res
Block public access to buckets and objects granted through any access control lists (ACLs)
S3 will ignore all ACLs that grant public access to buckets and objects.
Block public access to buckets and objects granted through new public bucket or access point policies
S3 will block new bucket and access point policies that grant public access to buckets and objects. This setting doesn't change any existing policies that allow public access to S3 resources.
Block public and cross-account access to buckets and objects through any public bucket or access point policies
S3 will ignore public and cross-account access for buckets or access points with policies that grant public access to buckets and objects.
Bucket Versioning
Versioning is a means of keeping multiple variants of an object in the same bucket. You can use versioning to preserve, retrieve, and restore every version of every object stored in your Amazon S3 bucket. With versioning, you ca
both unintended user actions and application failures. Learn more
Bucket Versioning
Disable
Enable
Tags - optional (0)
You can use bucket tags to track storage costs and organize buckets. Learn more
No tags associated with this bucket.
Add new tag
You can add up to 50 tags.



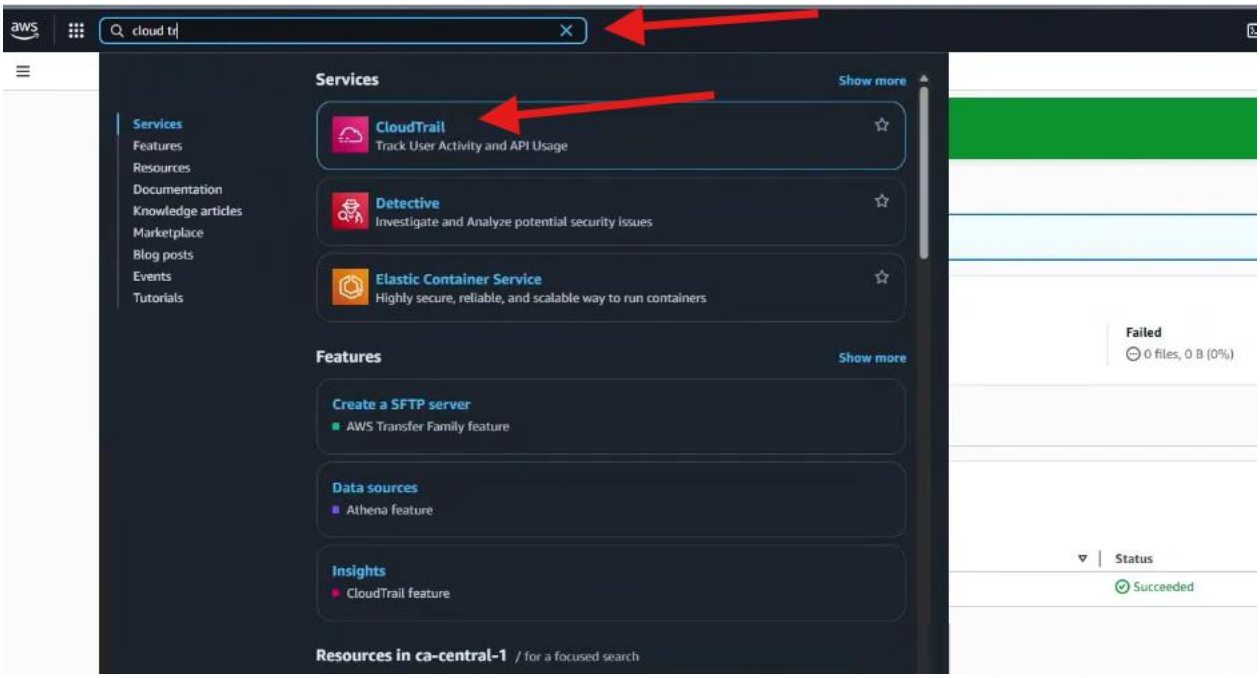
Now we can add files to the bucket

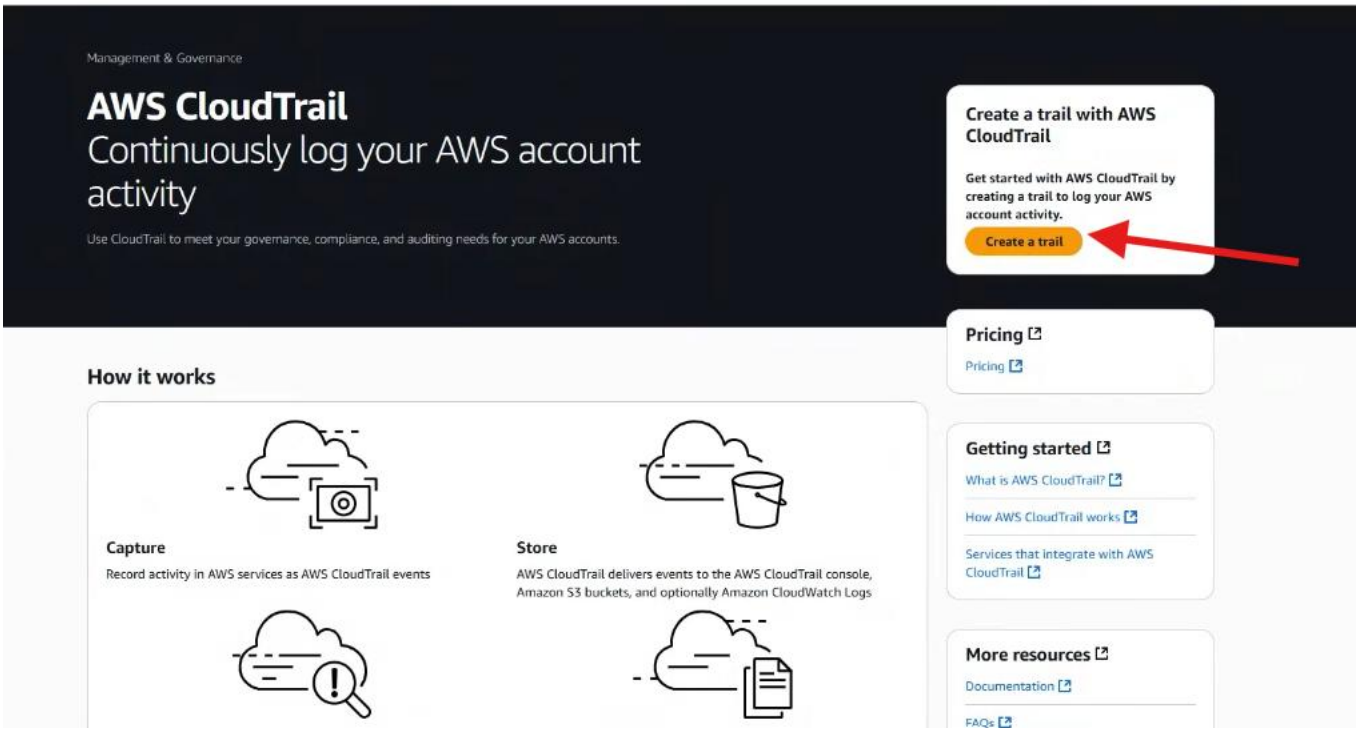




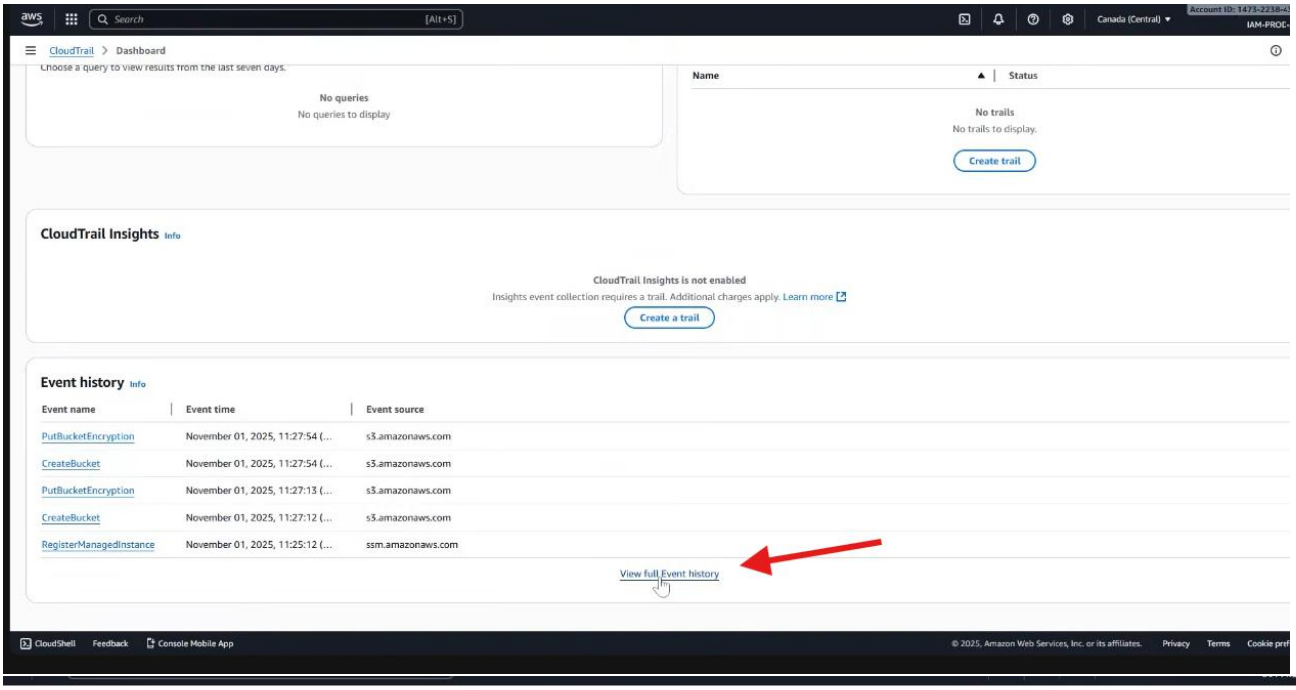
Create Trail

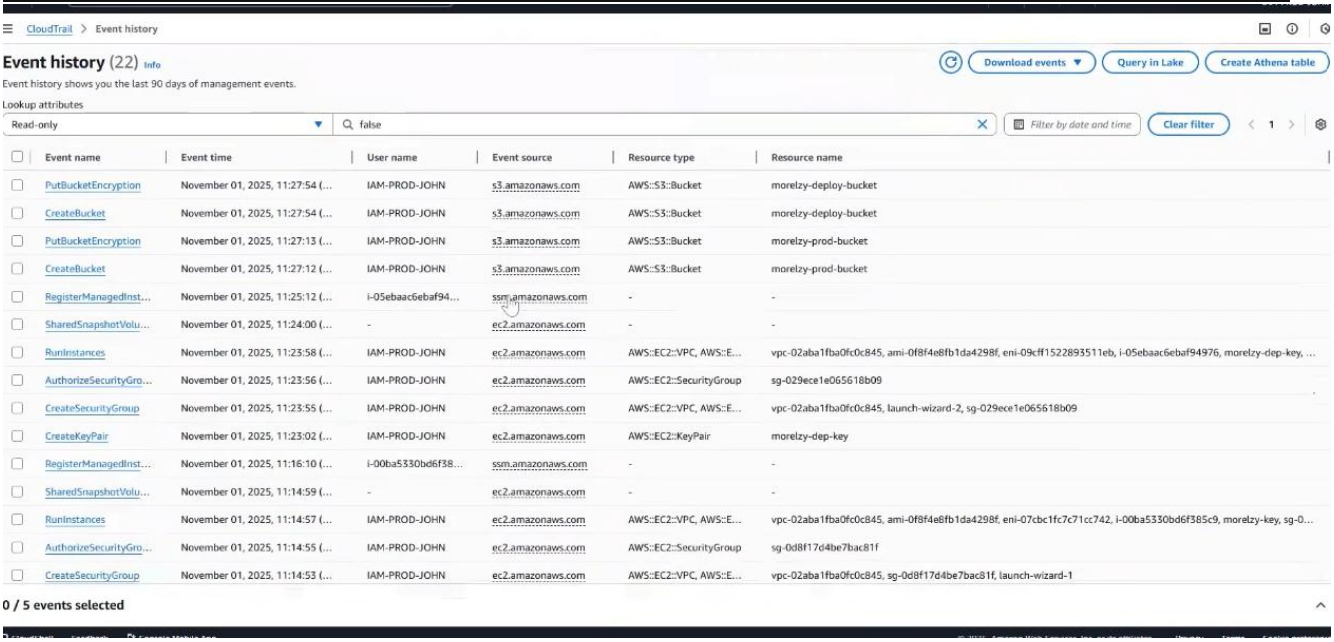
In the search bar, type Cloudtrail, this is a service to track all events and incidents

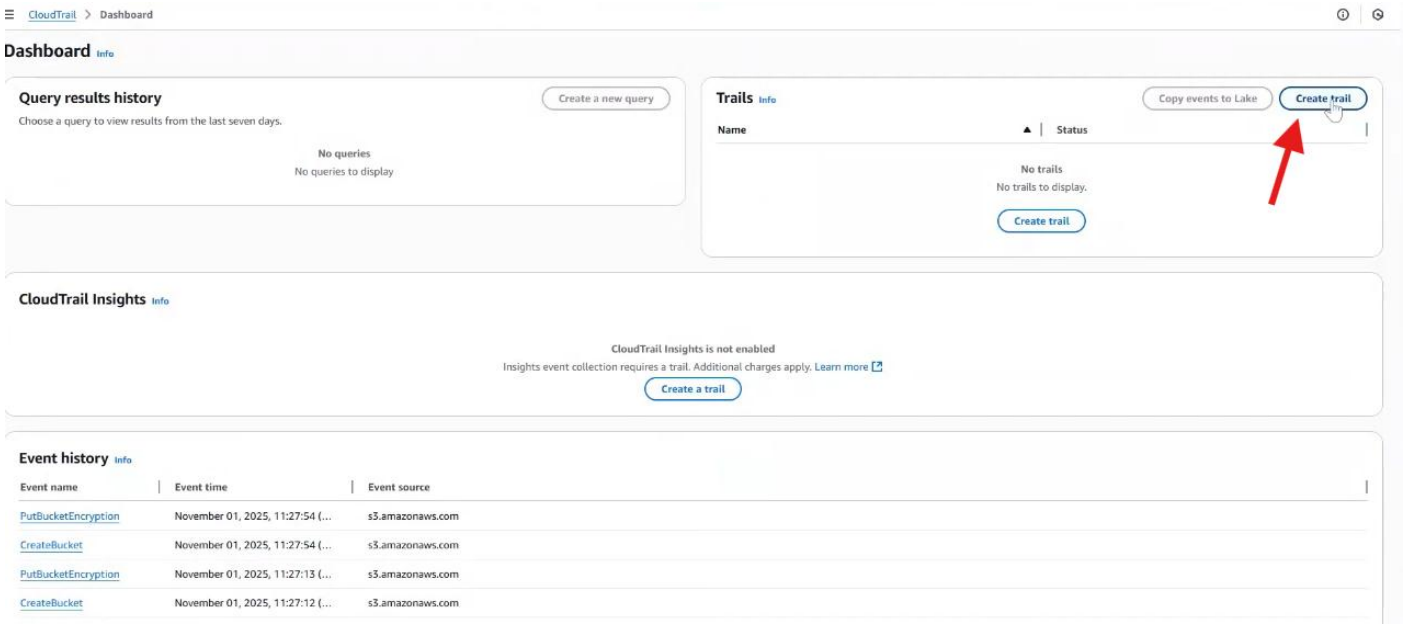




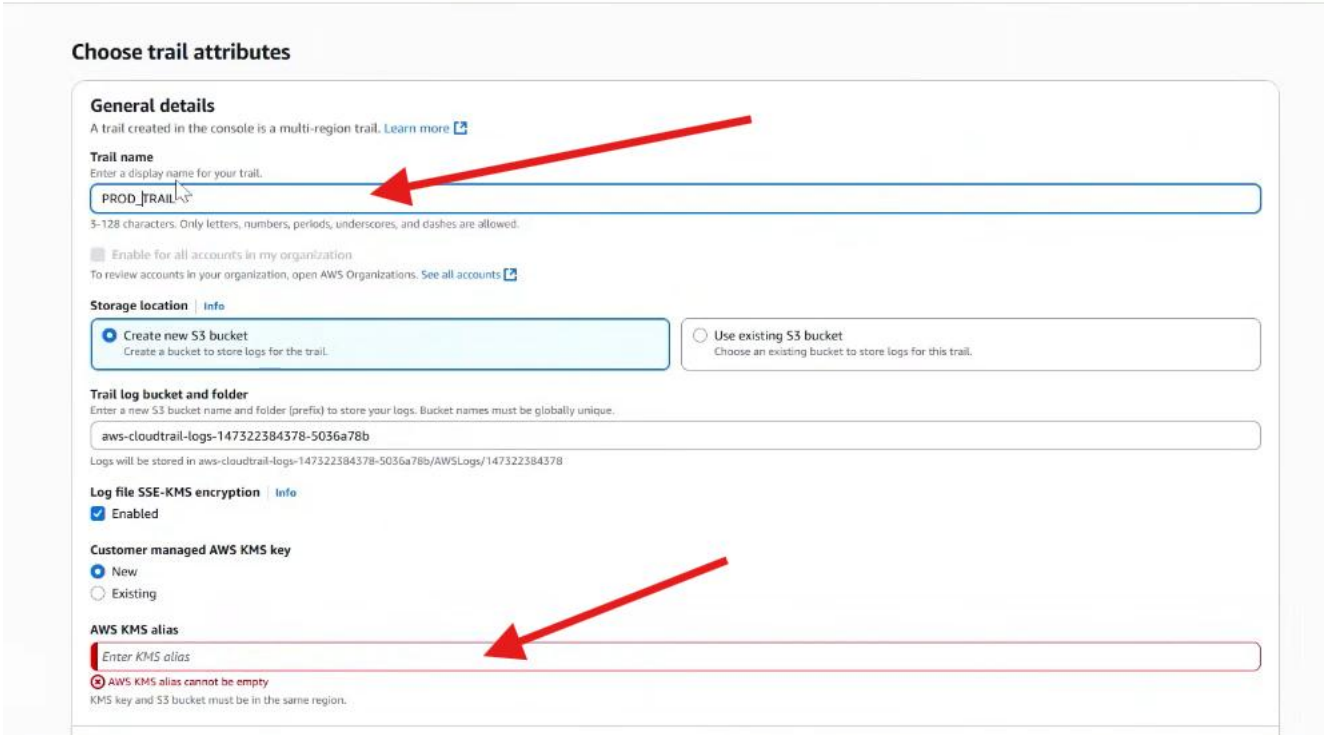
The system already has been generation logs of all we have done so far, as depicted below


CloudTrail > Dashboard
No queries
No queries to display
Name
Status
No trails
No trails to display.
Create trail
CloudTrail Insights Info
CloudTrail Insights is not enabled
Insights event collection requires a trail. Additional charges apply. Learn more
Create a trail
Event history Info
Event name
Event time
Event source
PutBucketEncryption
November 01, 2025, 11:27:54 (...
s3.amazonaws.com
CreateBucket
November 01, 2025, 11:27:54 (...
s3.amazonaws.com
PutBucketEncryption
November 01, 2025, 11:27:13 (...
s3.amazonaws.com
CreateBucket
November 01, 2025, 11:27:12 (...
s3.amazonaws.com
RegisterManagedInstance
November 01, 2025, 11:25:12 (...
ssm.amazonaws.com
View full Event history
CloudShell
Feedback
Console Mobile App
© 2025, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms

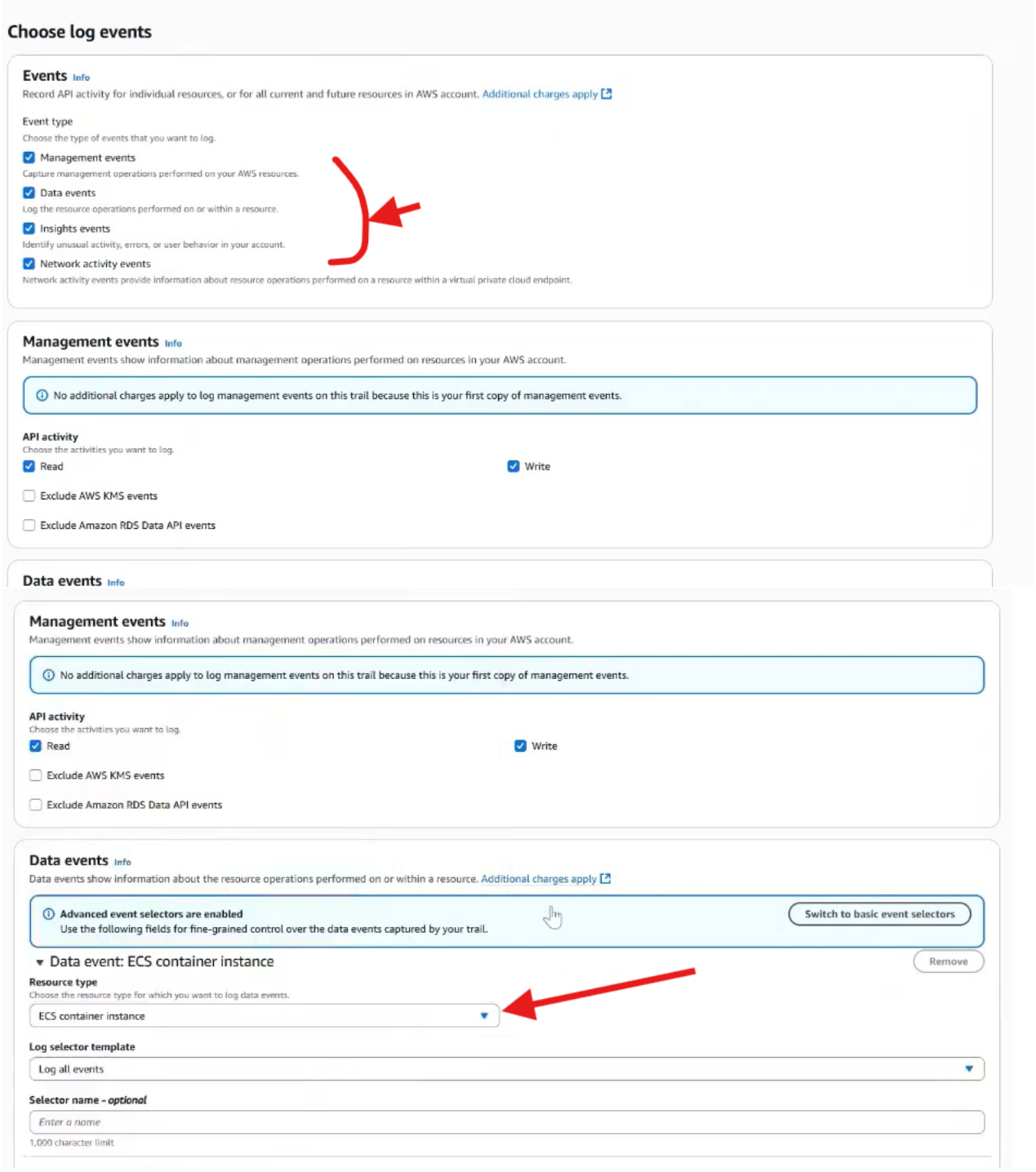

CloudTrail > Event history
Event history (22) Info
Event history shows you the last 90 days of management events.
Download events
Query in Lake
Create Athena table
Lookup attributes
Read-only
false
Filter by date and time
Clear filter
Event name
Event time
User name
Event source
Resource type
Resource name
PutBucketEncryption
November 01, 2025, 11:27:54 (...
IAM-PROD-JOHN
s3.amazonaws.com
AWS::S3::Bucket
morelzy-deploy-bucket
CreateBucket
November 01, 2025, 11:27:54 (...
IAM-PROD-JOHN
s3.amazonaws.com
AWS::S3::Bucket
morelzy-deploy-bucket
PutBucketEncryption
November 01, 2025, 11:27:13 (...
IAM-PROD-JOHN
s3.amazonaws.com
AWS::S3::Bucket
morelzy-prod-bucket
CreateBucket
November 01, 2025, 11:27:12 (...
IAM-PROD-JOHN
s3.amazonaws.com
AWS::S3::Bucket
morelzy-prod-bucket
RegisterManagedInst...
November 01, 2025, 11:25:12 (...
i-05ebaac6ebaf94...
ssm.amazonaws.com
-
-
SharedSnapshotVolu...
November 01, 2025, 11:24:00 (...
-
ec2.amazonaws.com
-
-
RunInstances
November 01, 2025, 11:23:58 (...
IAM-PROD-JOHN
ec2.amazonaws.com
AWS::EC2::VPC, AWS::E...
vpc-02aba1fba0fc0c845, ami-0f8f4e8fb1da4298f, eni-09cff1522893511eb, i-05ebaac6ebaf94976, morelzy-dep-key, ...
AuthorizeSecurityGro...
November 01, 2025, 11:23:56 (...
IAM-PROD-JOHN
ec2.amazonaws.com
AWS::EC2::SecurityGroup
sg-029ece1e065618b09
CreateSecurityGroup
November 01, 2025, 11:23:55 (...
IAM-PROD-JOHN
ec2.amazonaws.com
AWS::EC2::VPC, AWS::E...
vpc-02aba1fba0fc0c845, launch-wizard-2, sg-029ece1e065618b09
CreateKeyPair
November 01, 2025, 11:23:02 (...
IAM-PROD-JOHN
ec2.amazonaws.com
AWS::EC2::KeyPair
morelzy-dep-key
RegisterManagedInst...
November 01, 2025, 11:16:10 (...
i-00ba5330bd6f38...
ssm.amazonaws.com
-
-
SharedSnapshotVolu...
November 01, 2025, 11:14:59 (...
-
ec2.amazonaws.com
-
-
RunInstances
November 01, 2025, 11:14:57 (...
IAM-PROD-JOHN
ec2.amazonaws.com
AWS::EC2::VPC, AWS::E...
vpc-02aba1fba0fc0c845, ami-0f8f4e8fb1da4298f, eni-07cbc1fc7c71cc742, i-00ba5330bd6f385c9, morelzy-key, sg-0...
AuthorizeSecurityGro...
November 01, 2025, 11:14:55 (...
IAM-PROD-JOHN
ec2.amazonaws.com
AWS::EC2::SecurityGroup
sg-0d8f17d4be7bac81f
CreateSecurityGroup
November 01, 2025, 11:14:53 (...
IAM-PROD-JOHN
ec2.amazonaws.com
AWS::EC2::VPC, AWS::E...
vpc-02aba1fba0fc0c845, sg-0d8f17d4be7bac81f, launch-wizard-1
0 / 5 events selected

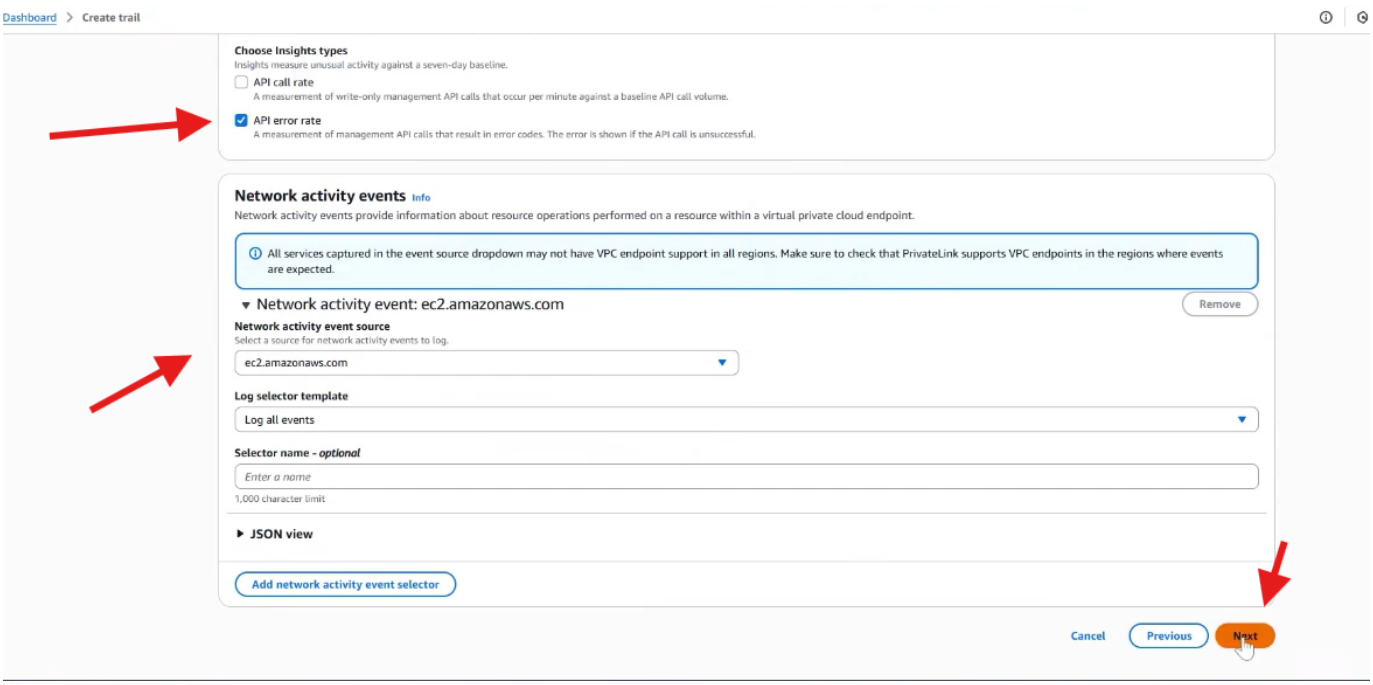


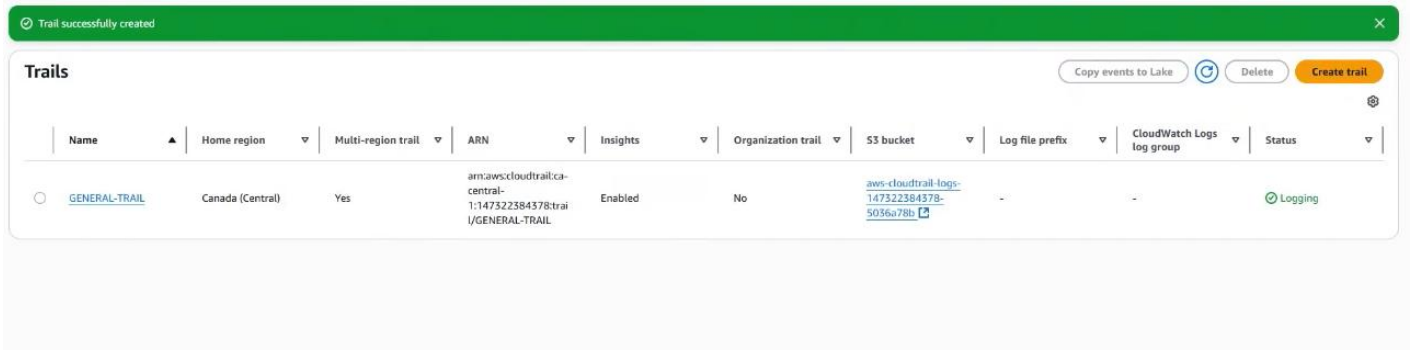
Use and existing S3 bucket or create a new one



Select the type of events you want to log and create trail





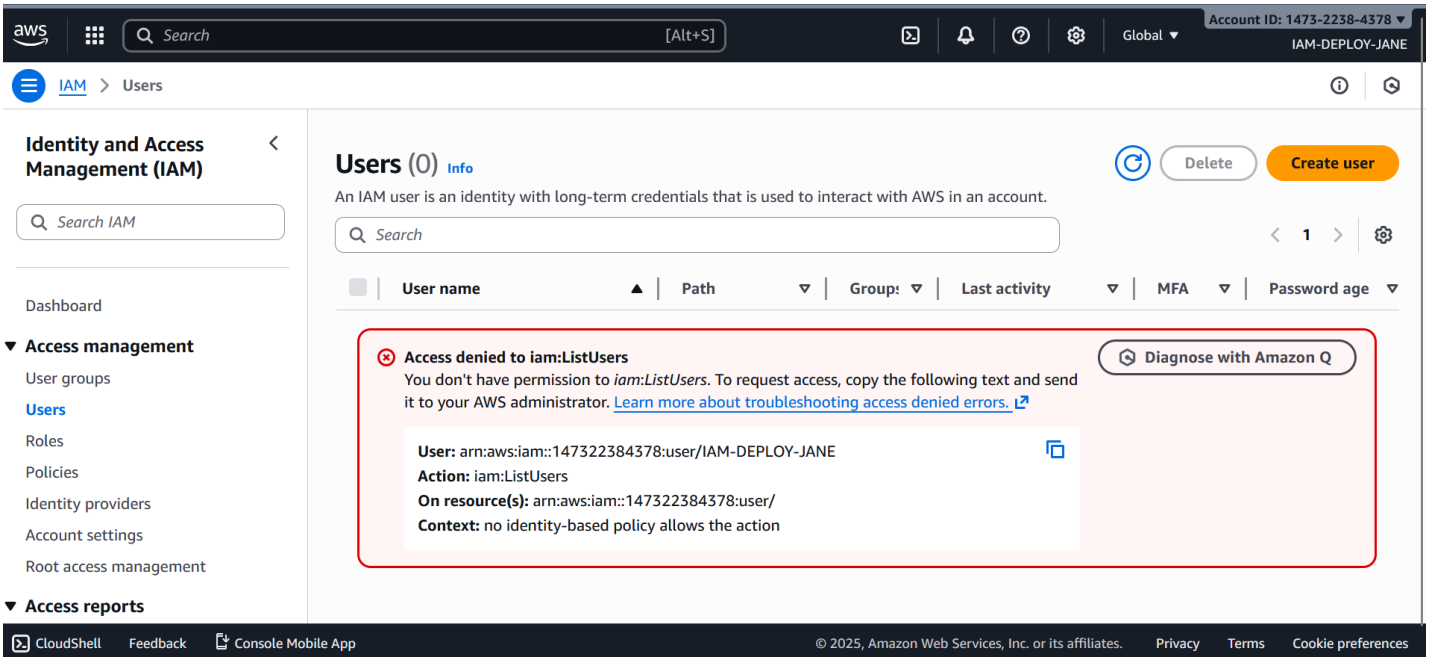


CREATE POLICES

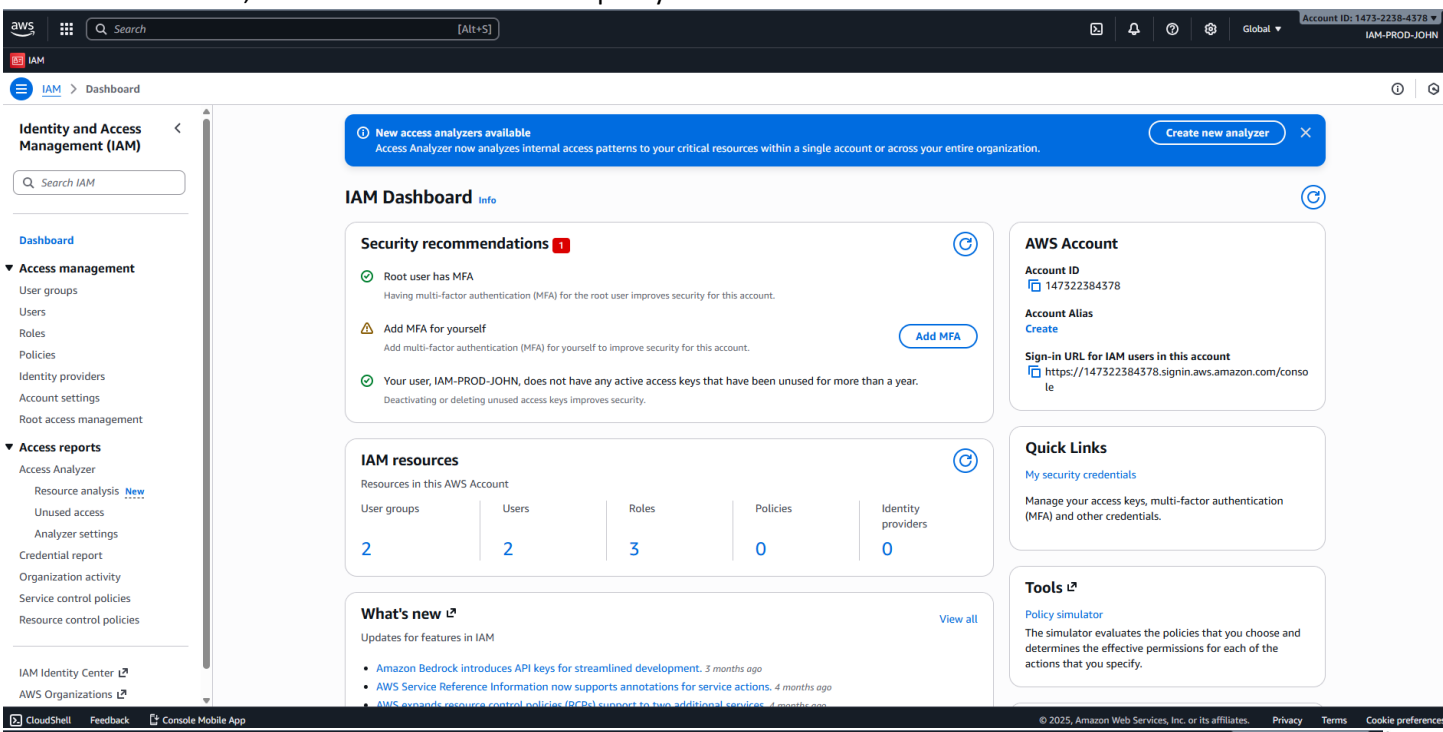
AWS comes with predefined policies we can choose from, however we will be creating some policies with the JOHN account and assigning them the JANE account to test them.

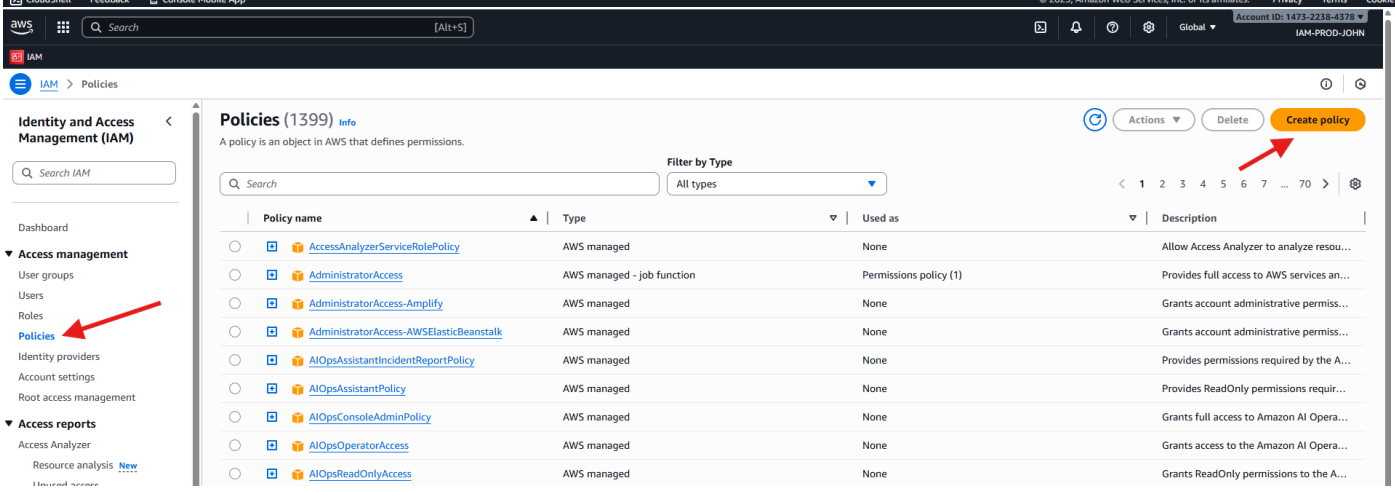
Most users once created will be assigned denied access due to least privilege.

First we log in to jane account and confirm what is denied and create a policy to allow it. In this case JANE has no access to list of users as shown below


aws
Search
[Alt+S]
Global
Account ID: 1473-2238-4378
IAM-DEPLOY-JANE
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
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
1
User name
Path
Groups
Last activity
MFA
Password age
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::147322384378:user/IAM-DEPLOY-JANE
Action: iam:ListUsers
On resource(s): arn:aws:iam::147322384378:user/
Context: no identity-based policy allows the action
CloudShell
Feedback
Console Mobile App
© 2025, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences

So on JOHN account, we create an allow ‘listuser’ policy and attach to user JANE

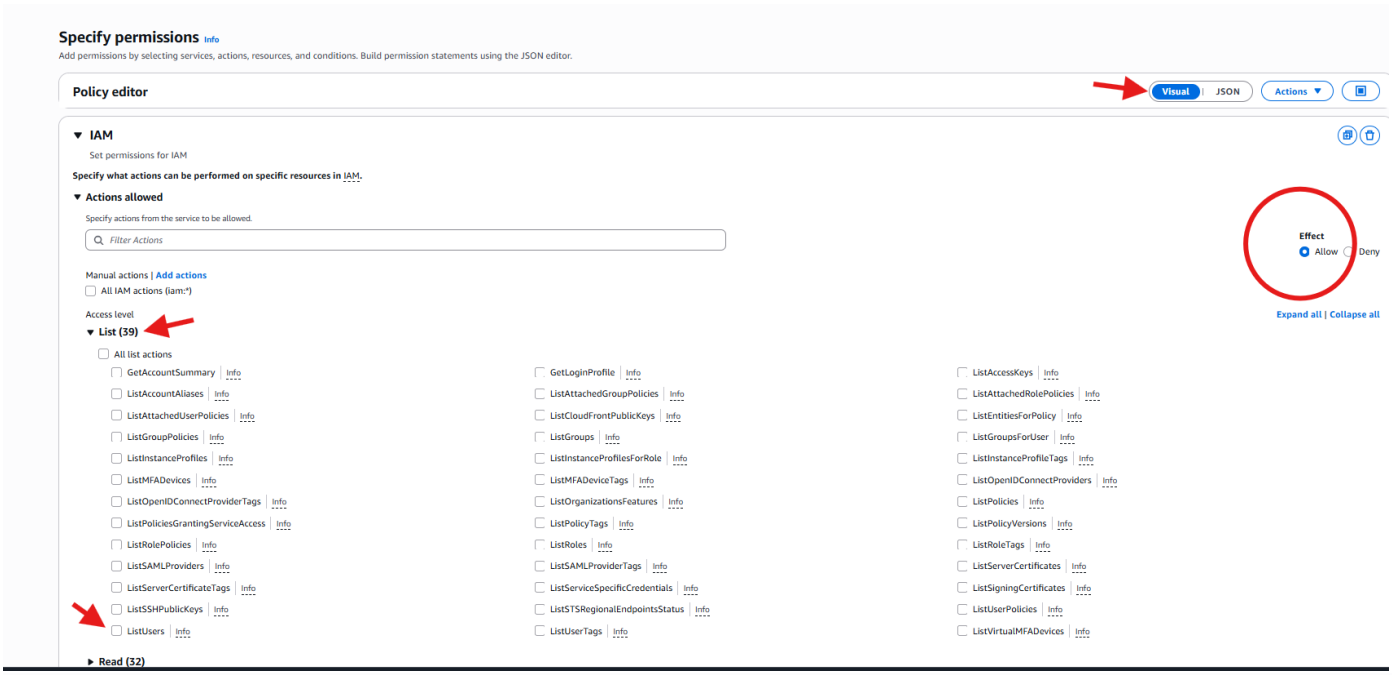


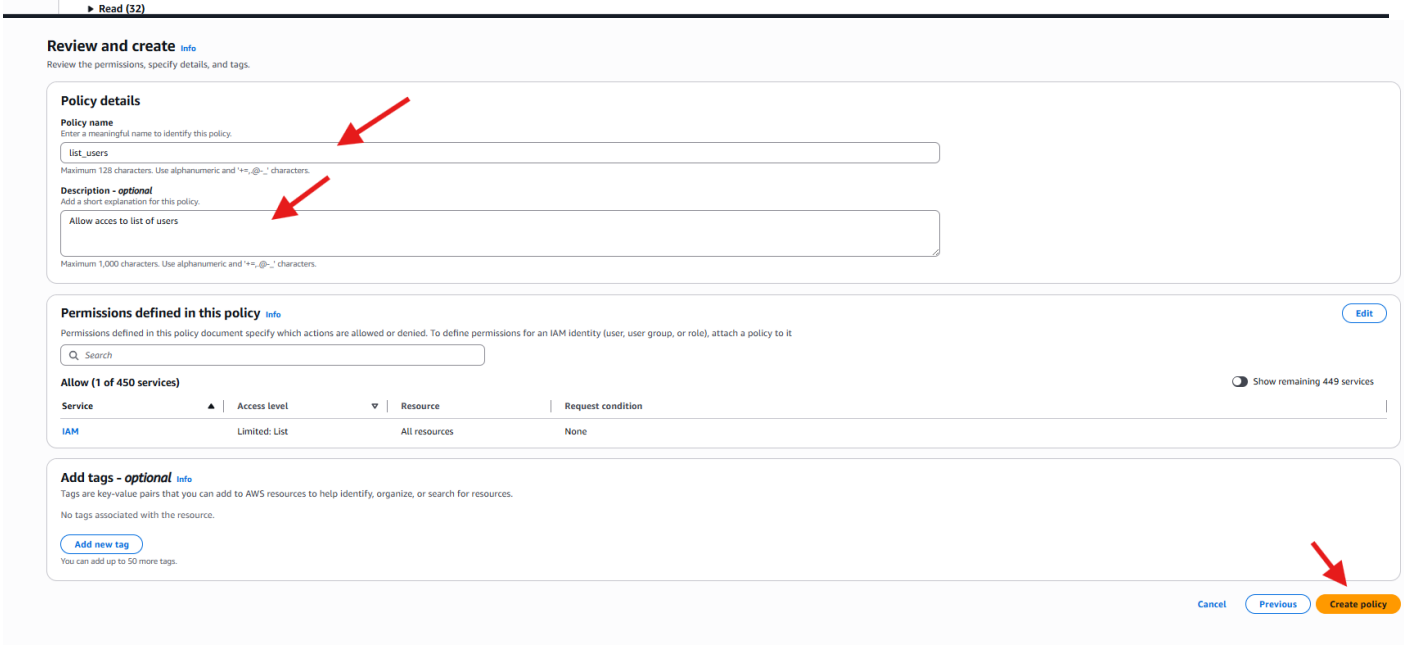


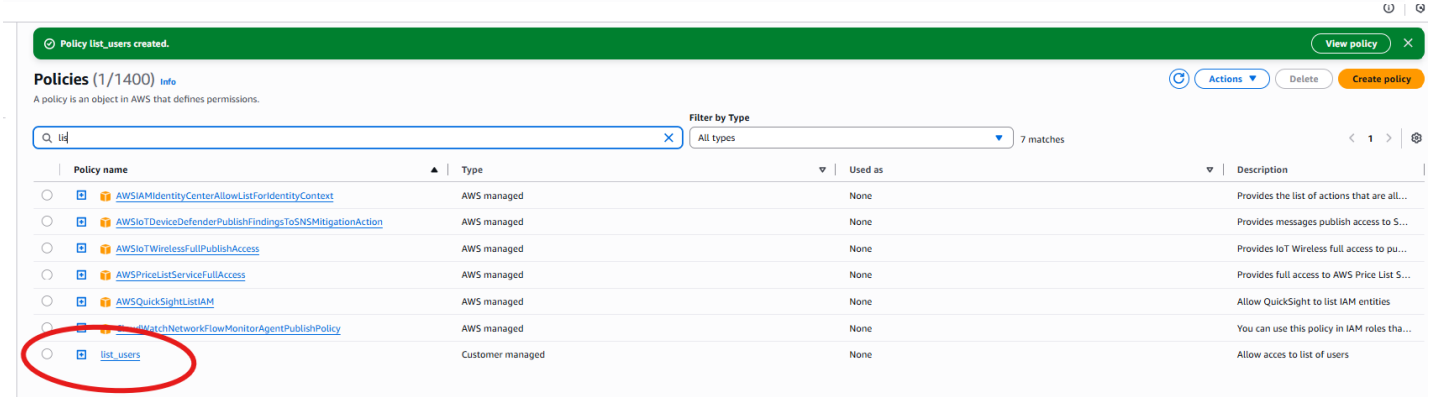
When specifying permissions we can use VISUAL OR JSON (SCRIPTS), in this example we use Visual.

Drop down list>> check listuser>> check effect ‘allow’

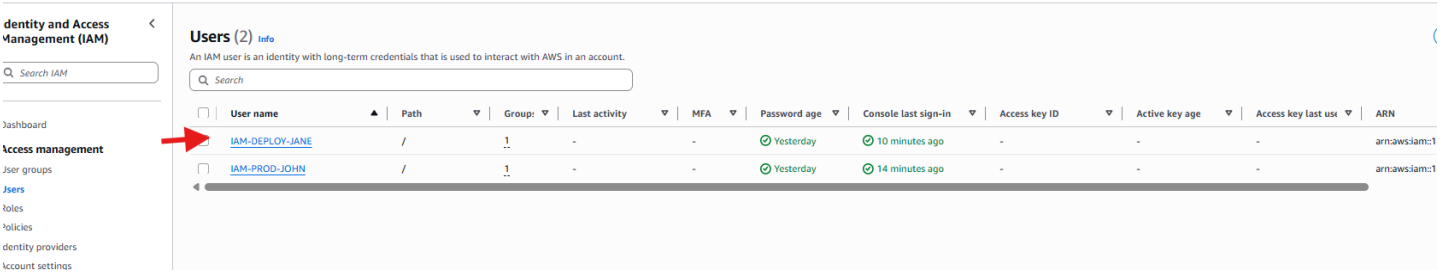
Give policy a name and description and click create policy

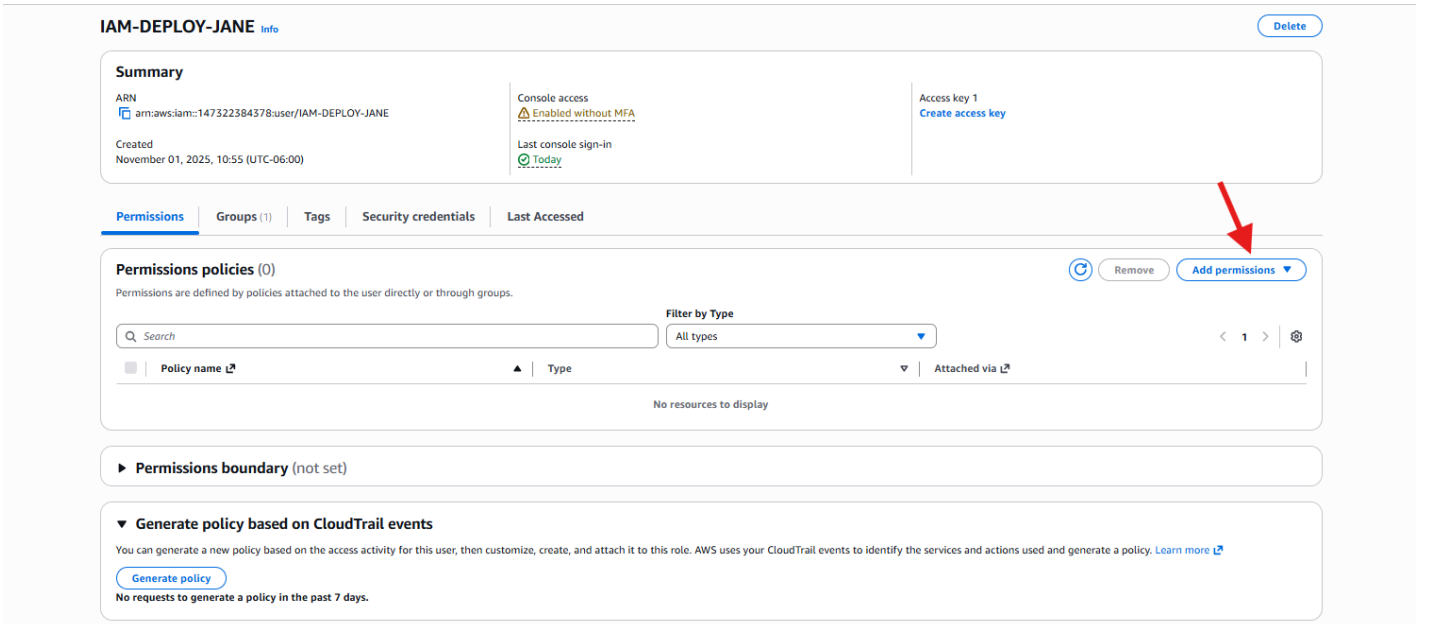

Specify permissions Info
Add permissions by selecting services, actions, resources, and conditions. Build permission statements using the JSON editor.
Policy editor
Visual
JSON
Actions
IAM
Set permissions for IAM
Specify what actions can be performed on specific resources in IAM.
Actions allowed
Specify actions from the service to be allowed.
Filter Actions
Manual actions | Add actions
All IAM actions (iam:*)
Access level
List (39)
All list actions
GetAccountSummary
ListAccountAliases
ListAttachedUserPolicies
ListGroupPolicies
ListInstanceProfiles
ListMFADevices
ListOpenIDConnectProviderTags
ListPoliciesGrantingServiceAccess
ListRolePolicies
ListSAMLProviders
ListServerCertificateTags
ListSSHPublicKeys
ListUsers
GetLoginProfile
ListAttachedGroupPolicies
ListCloudFrontPublicKeys
ListGroups
ListInstanceProfilesForRole
ListMFADeviceTags
ListOrganizationsFeatures
ListPolicyTags
ListRoles
ListSAMLProviderTags
ListServiceSpecificCredentials
ListSTSRegionalEndpointsStatus
ListUserTags
ListAccessKeys
ListAttachedRolePolicies
ListEntitiesForPolicy
ListGroupsForUser
ListInstanceProfileTags
ListOpenIDConnectProviders
ListPolicies
ListPolicyVersions
ListRoleTags
ListServerCertificates
ListSigningCertificates
ListUserPolicies
ListVirtualMFADevices
Effect
Allow
Deny
Expand all | Collapse all
Read (32)

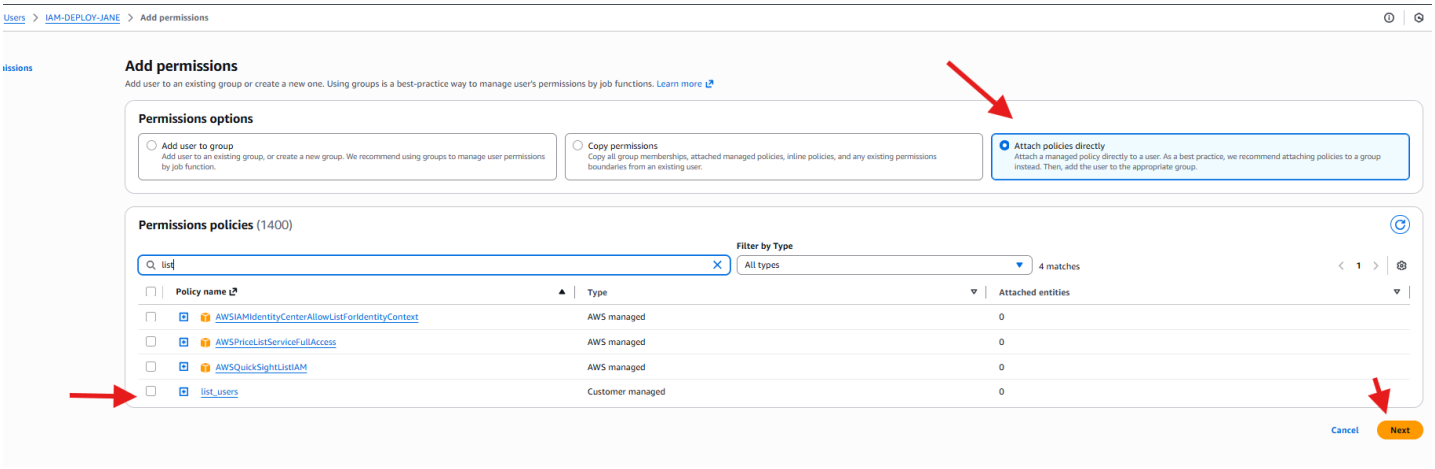

Review and create Info
Review the permissions, specify details, and tags.
Policy details
Policy name
Enter a meaningful name to identify this policy.
list_users
Maximum 128 characters. Use alphanumeric and '+=,.@-_' characters.
Description - optional
Add a short explanation for this policy.
Allow acces to list of users
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 (1 of 450 services)
Show remaining 449 services
Service
Access level
Resource
Request condition
IAM
Limited: List
All resources
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

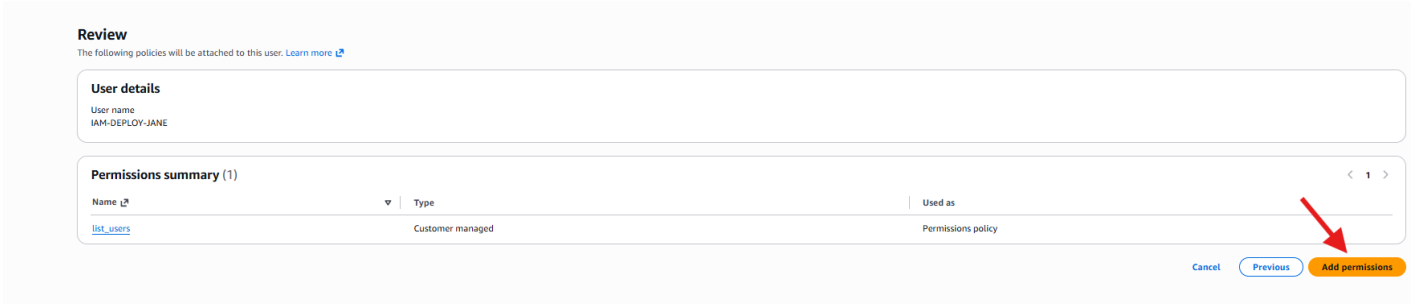

Policy list_users created.
View policy
Policies (1/1400) Info
A policy is an object in AWS that defines permissions.
Actions
Delete
Create policy
lis
Filter by Type
All types
7 matches
Policy name
Type
Used as
Description
AWSIAMIdentityCenterAllowListForIdentityContext
AWS managed
None
Provides the list of actions that are all...
AWSIoTDeviceDefenderPublishFindingsToSNSMitigationAction
AWS managed
None
Provides messages publish access to S...
AWSIoTWirelessFullPublishAccess
AWS managed
None
Provides IoT Wireless full access to pu...
AWSPriceListServiceFullAccess
AWS managed
None
Provides full access to AWS Price List S...
AWSQuickSightListIAM
AWS managed
None
Allow QuickSight to list IAM entities
AWS managed
None
You can use this policy in IAM roles tha...
list_users
Customer managed
None
Allow acces to list of users

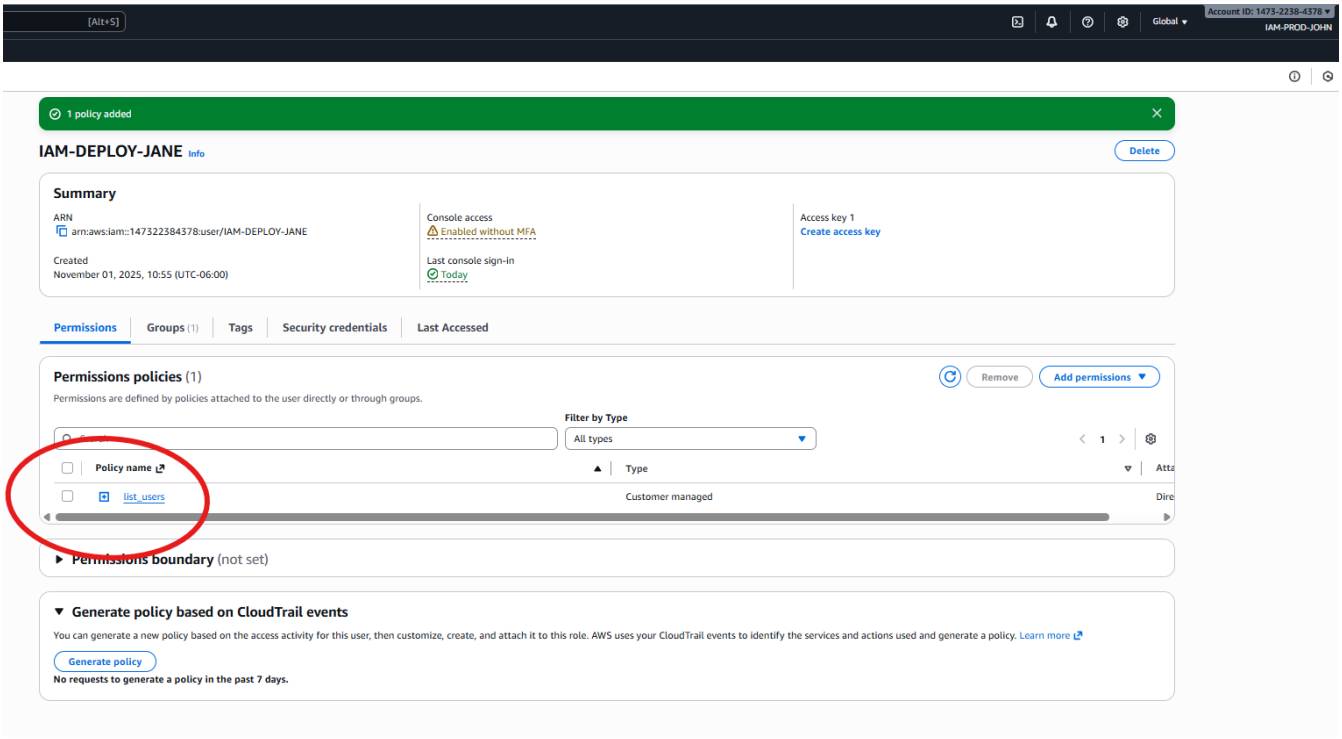
Now we attach policy to JANE



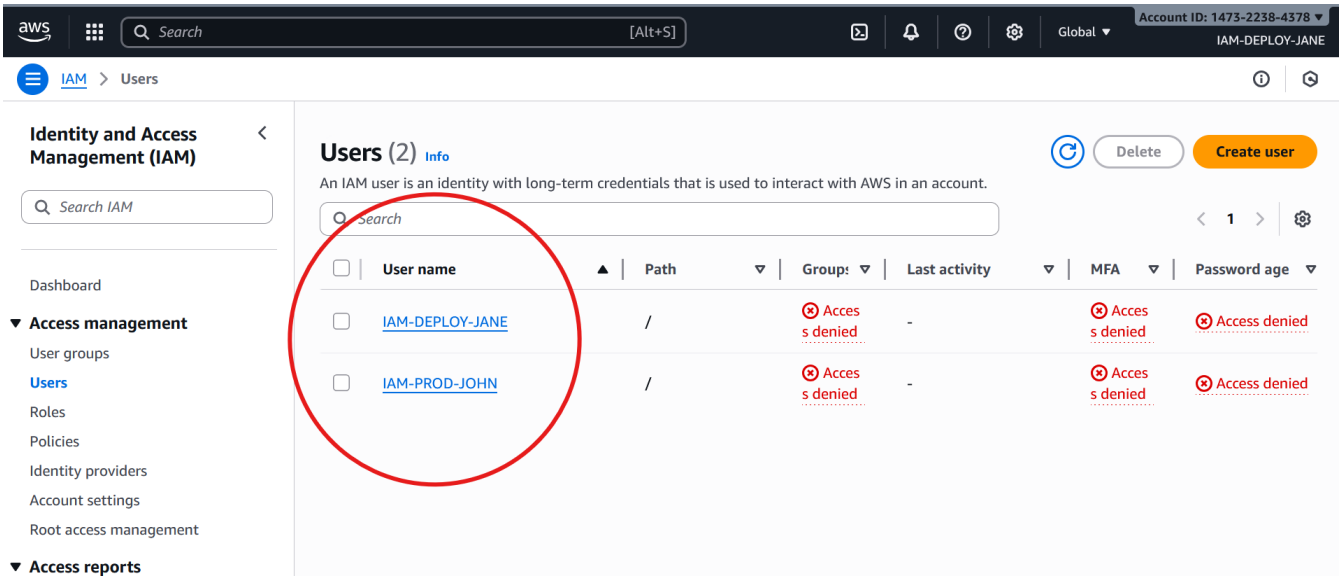





Review
The following policies will be attached to this user. Learn more
User details
User name
IAM-DEPLOY-JANE
Permissions summary (1)
Name
Type
Used as
list_users
Customer managed
Permissions policy
Cancel
Previous
Add permissions

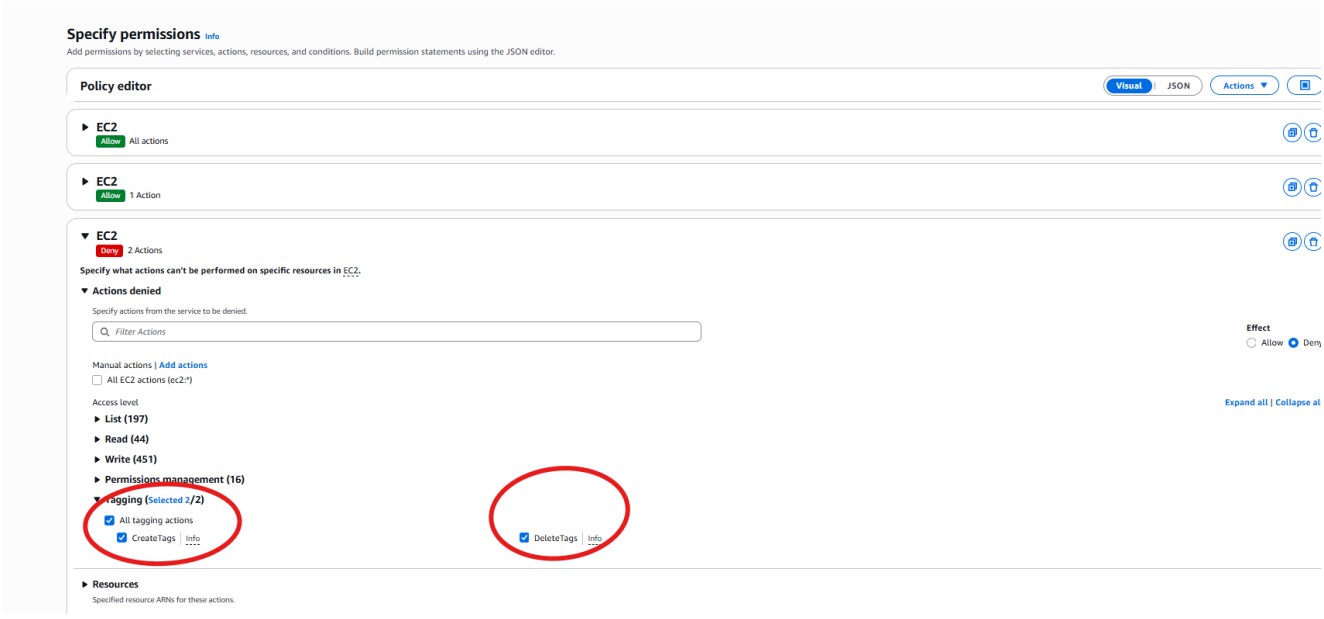

[Alt+S]
Global
Account ID: 1473-2238-4378
IAM-PROD-JOHN
1 policy added
IAM-DEPLOY-JANE Info
Delete
Summary
ARN
arn:aws:iam::147322384378:user/IAM-DEPLOY-JANE
Created
November 01, 2025, 10:55 (UTC-06:00)
Console access
Enabled without MFA
Last console sign-in
Today
Access key 1
Create access key
Permissions
Groups (1)
Tags
Security credentials
Last Accessed
Permissions policies (1)
Permissions are defined by policies attached to the user directly or through groups.
Remove
Add permissions
Filter by Type
All types
Policy name
Type
list_users
Customer managed
Permissions boundary (not set)
Generate policy based on CloudTrail events
You can generate a new policy based on the access activity for this user, then customize, create, and attach it to this role. AWS uses your CloudTrail events to identify the services and actions used and generate a policy. Learn more
Generate policy
No requests to generate a policy in the past 7 days.

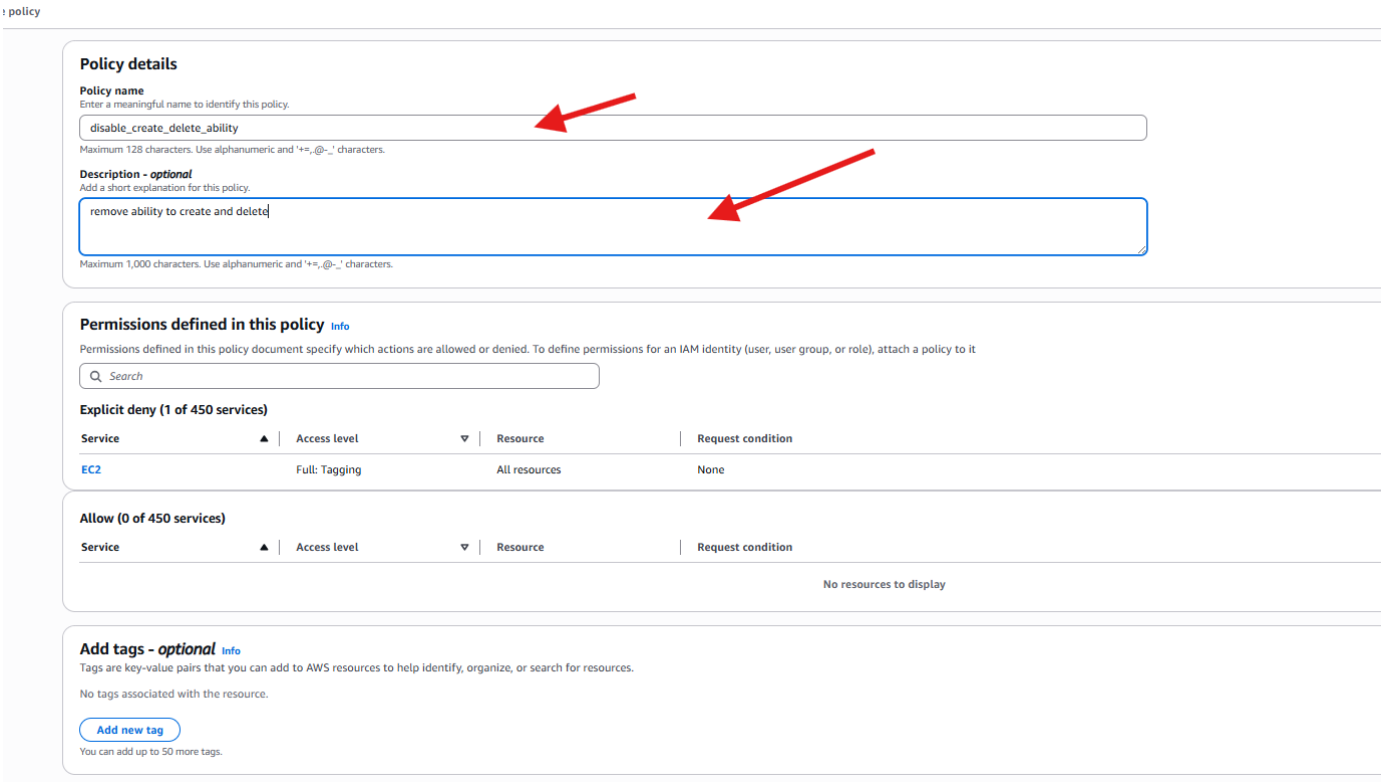
Policy is now assigned. To confirm its in effect, we log into JANE account and users list is now displayed



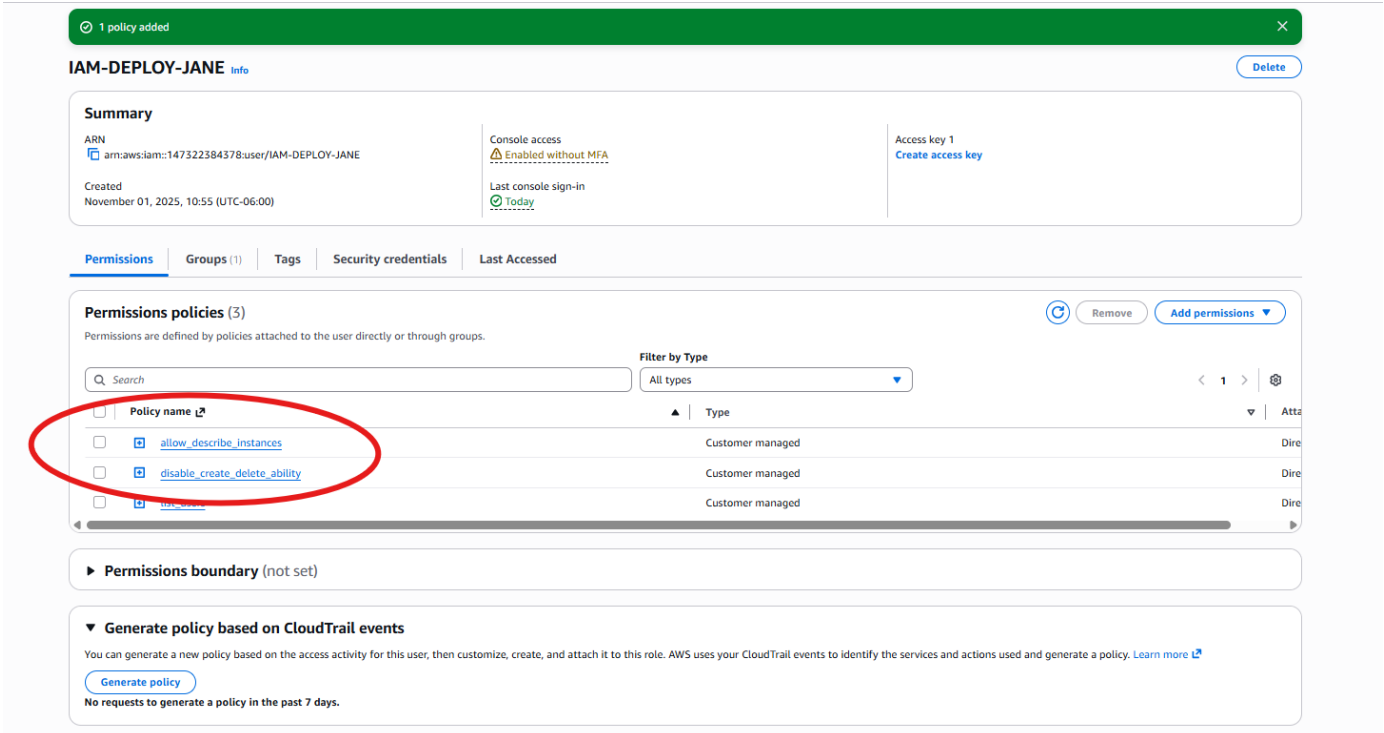
We can also create a policy that allows jane to view instances but restricts JANE from creating or deleting.

Following the same steps prior, we create an EC2 policy





All policies assigned to JANE are now listed,



Using JANE account, we try to delete an instance but we get an error