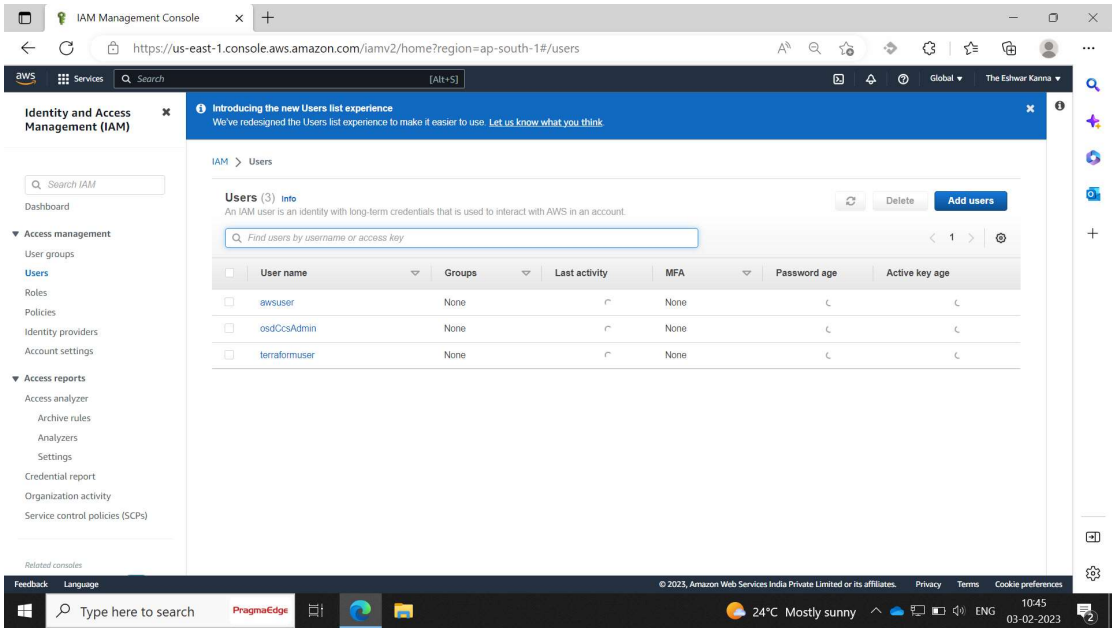
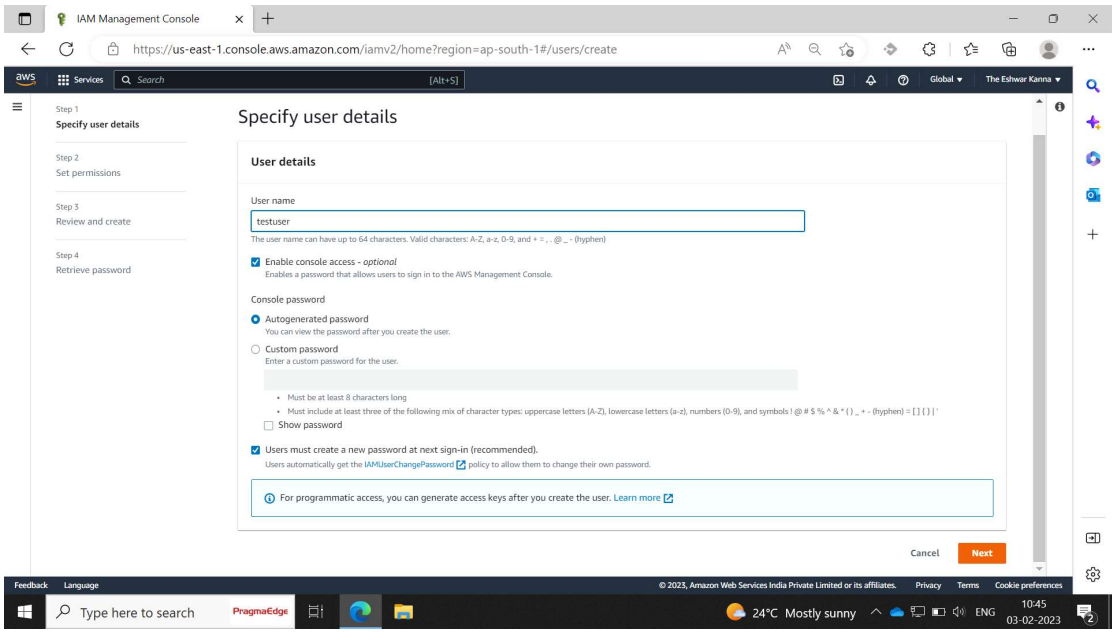
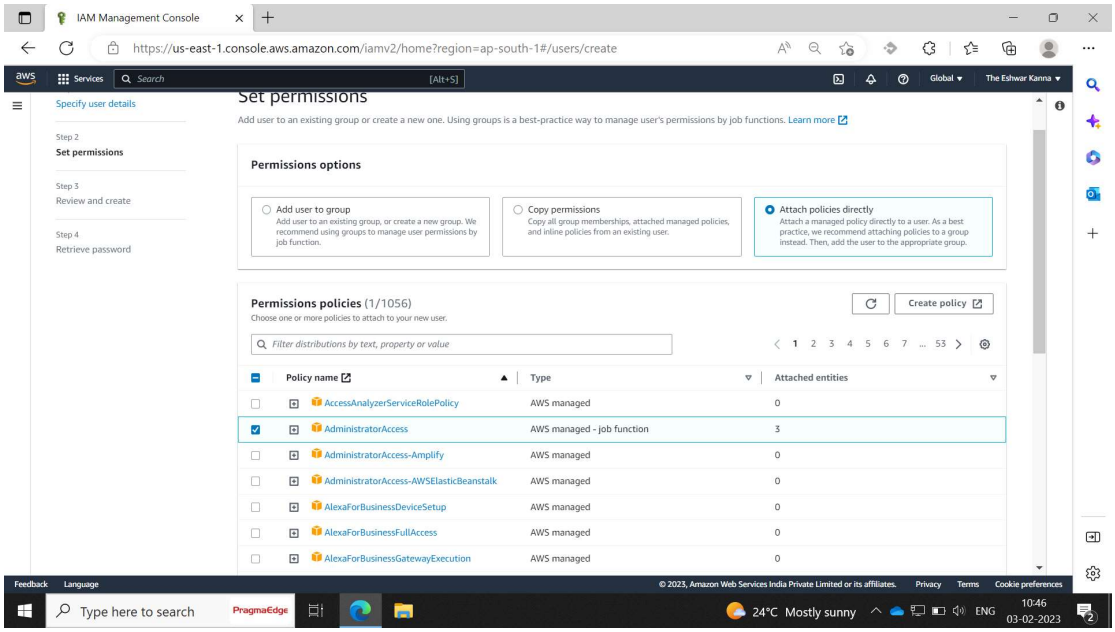
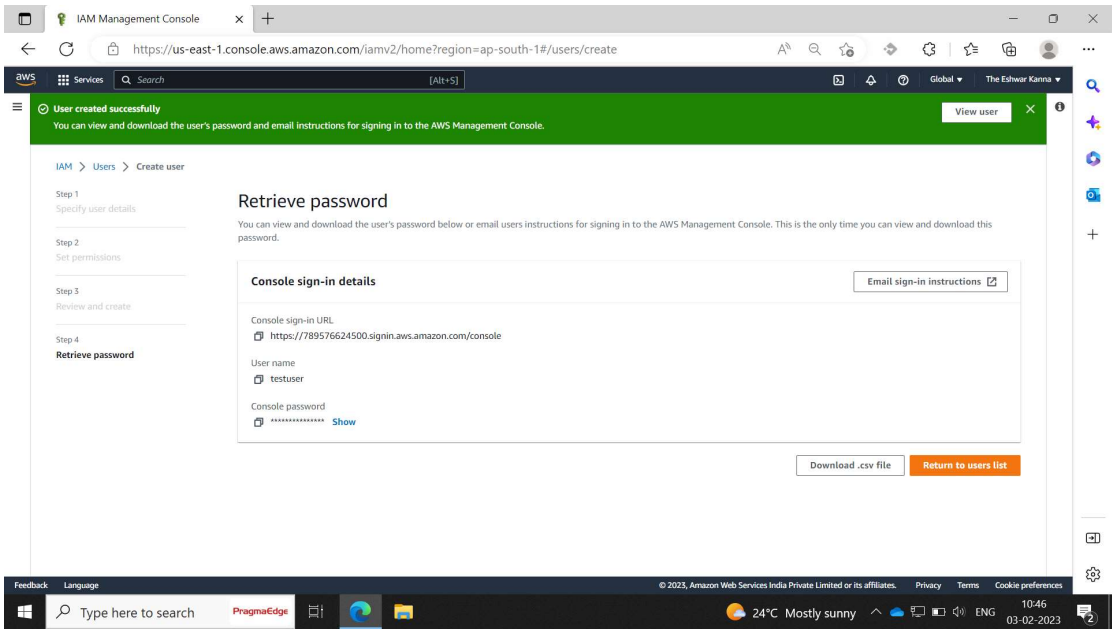
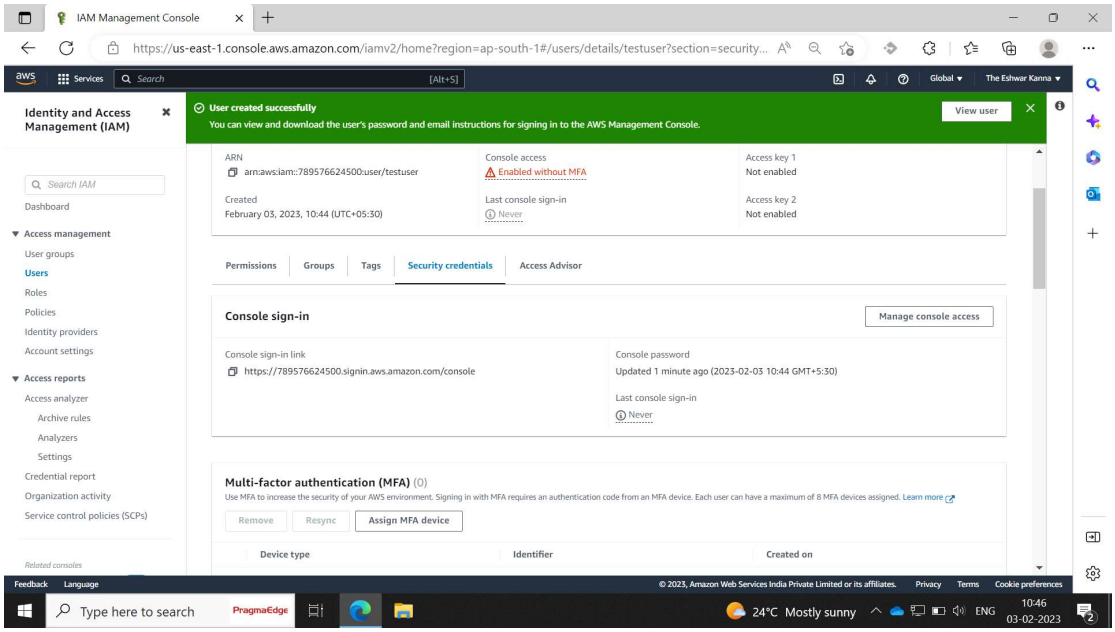
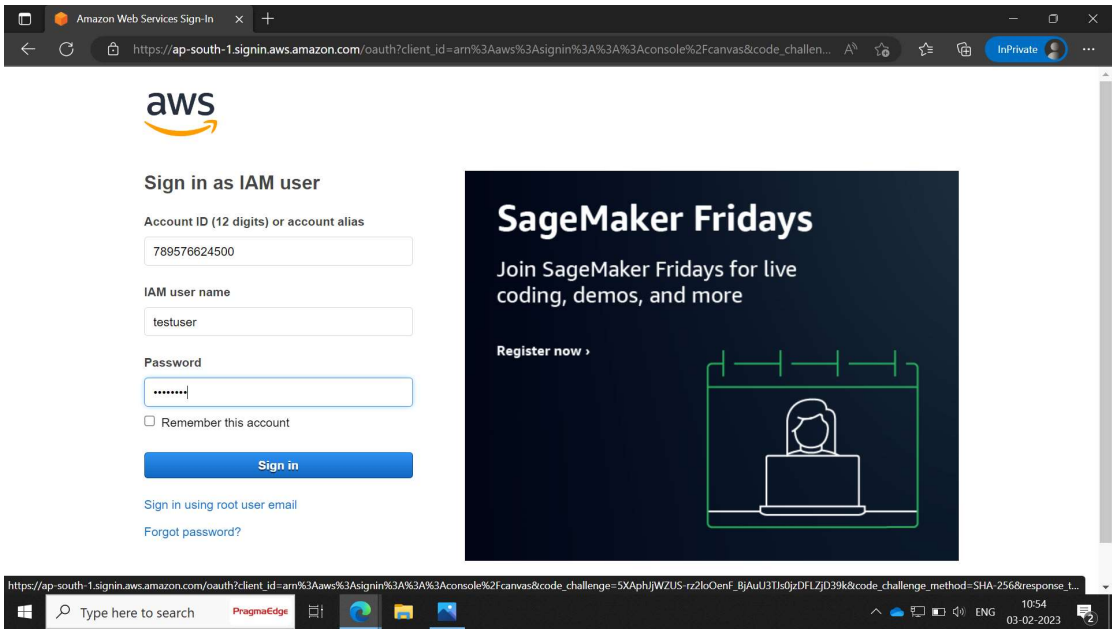

IAM Management Console
https://us-east-1.console.aws.amazon.com/iamv2/home?region=ap-south-1#/users
Identity and Access Management (IAM)
Introducing the new Users list experience
We've redesigned the Users list experience to make it easier to use. Let us know what you think.
IAM > Users
Users (3) Info
An IAM user is an identity with long-term credentials that is used to interact with AWS in an account.
Delete
Add users
Find users by username or access key
User name
Groups
Last activity
MFA
Password age
Active key age
awsuser
None
None
osdCcsAdmin
None
None
terraformuser
None
None
Dashboard
Access management
User groups
Users
Roles
Policies
Identity providers
Account settings
Access reports
Access analyzer
Archive rules
Analyzers
Settings
Credential report
Organization activity
Service control policies (SCPs)
Feedback
Language
© 2023, Amazon Web Services India Private Limited or its affiliates.
Privacy
Terms
Cookie preferences
Type here to search
24°C Mostly sunny
ENG
10:45
03-02-2023

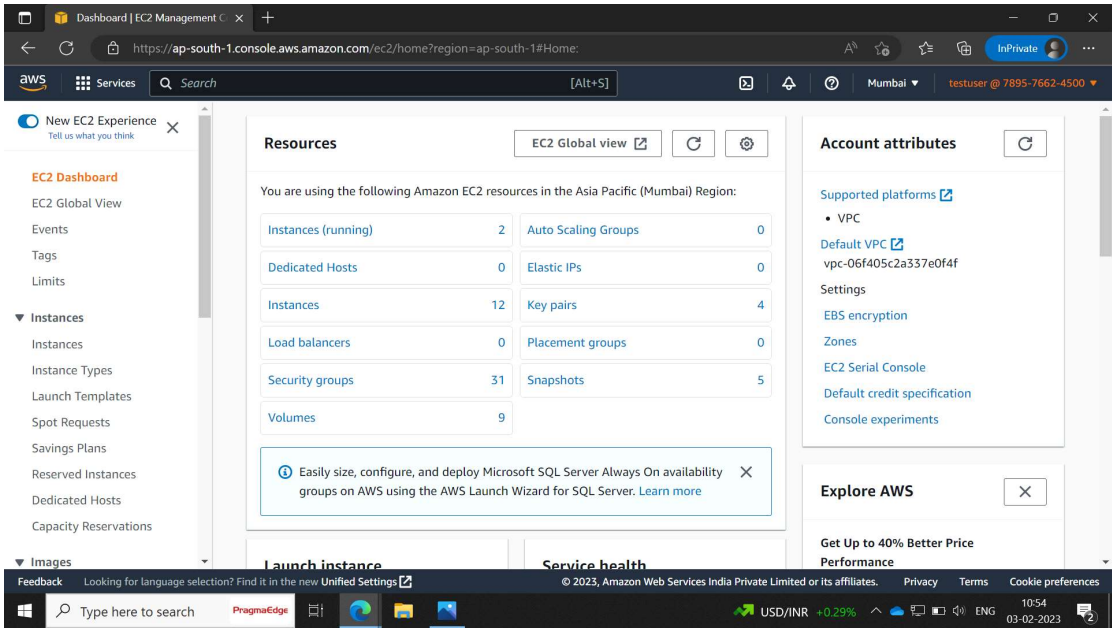

IAM Management Console
https://us-east-1.console.aws.amazon.com/iamv2/home?region=ap-south-1#/users/create
Step 1
Specify user details
Step 2
Set permissions
Step 3
Review and create
Step 4
Retrieve password
Specify user details
User details
User name
testuser
The user name can have up to 64 characters. Valid characters: A-Z, a-z, 0-9, and + = , . @ _ - (hyphen)
Enable console access - optional
Enables a password that allows users to sign in to the AWS Management Console.
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.
For programmatic access, you can generate access keys after you create the user. Learn more
Cancel
Next
Feedback
Language
© 2023, Amazon Web Services India Private Limited or its affiliates.
Privacy
Terms
Cookie preferences
Type here to search
24°C Mostly sunny
ENG
10:45
03-02-2023

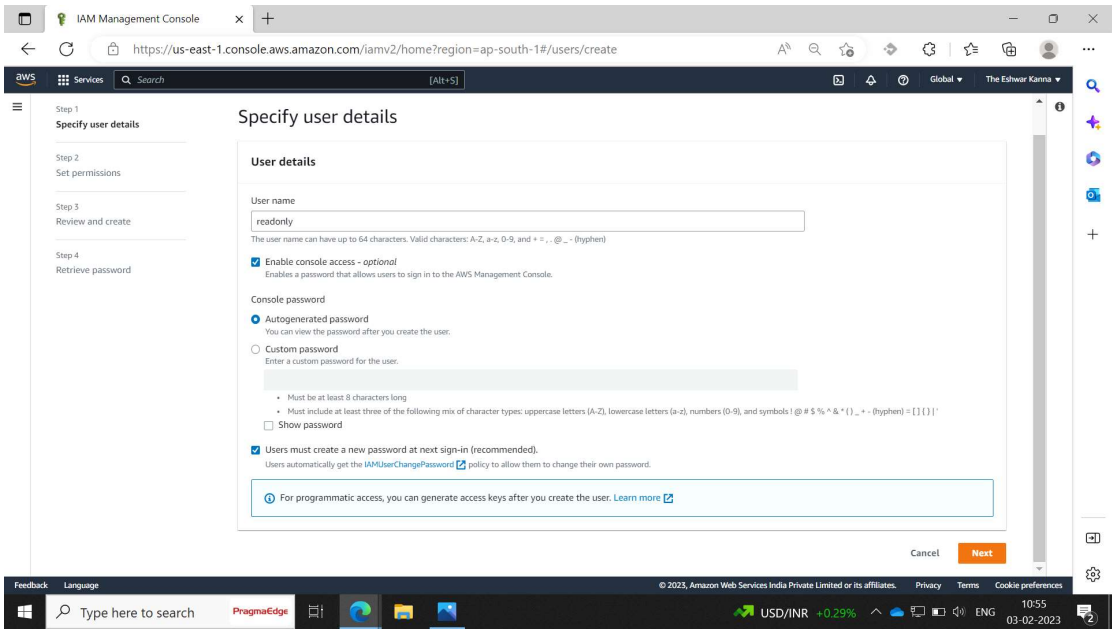

IAM Management Console
https://us-east-1.console.aws.amazon.com/iamv2/home?region=ap-south-1#/users/create
Specify user details
Step 2
Set permissions
Step 3
Review and create
Step 4
Retrieve password
Set permissions
Add user to an existing group or create a new one. Using groups is a best-practice way 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 (1/1056)
Choose one or more policies to attach to your new user.
Create policy
Filter distributions by text, property or value
Policy name
Type
Attached entities
AccessAnalyzerServiceRolePolicy AWS managed 0
AdministratorAccess AWS managed - job function 3
AdministratorAccess-Amplify AWS managed 0
AdministratorAccess-AWSElasticBeanstalk AWS managed 0
AlexaForBusinessDeviceSetup AWS managed 0
AlexaForBusinessFullAccess AWS managed 0
AlexaForBusinessGatewayExecution AWS managed 0
Feedback
Language
© 2023, Amazon Web Services India Private Limited or its affiliates.
Privacy
Terms
Cookie preferences
Type here to search
24°C Mostly sunny
ENG
10:46
03-02-2023

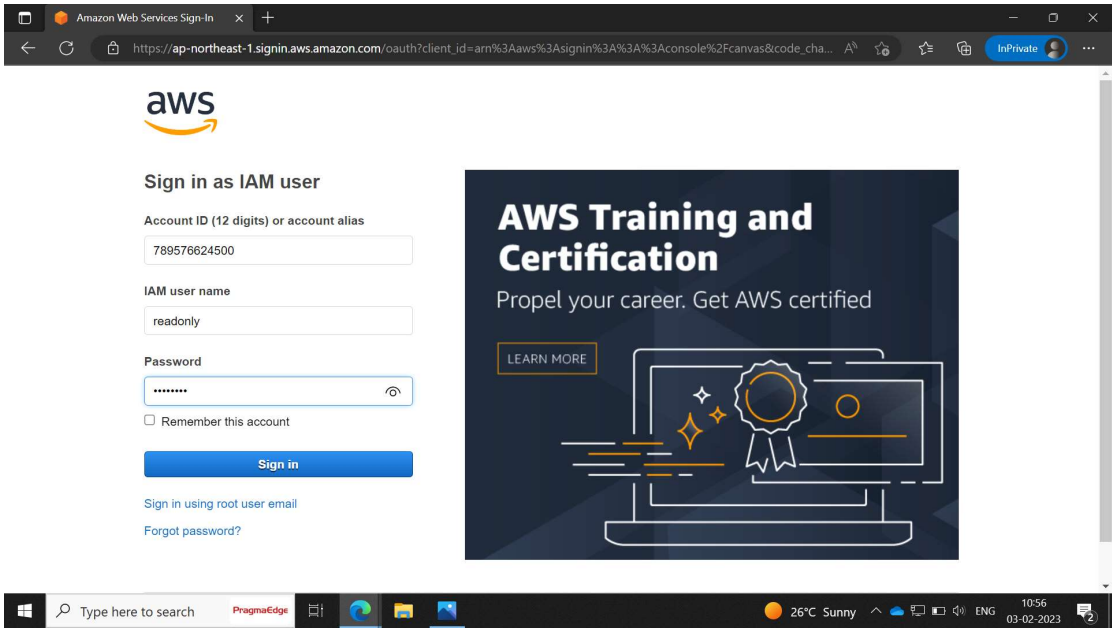

IAM Management Console
https://us-east-1.console.aws.amazon.com/iamv2/home?region=ap-south-1#/users/create
User created successfully
You can view and download the user's password and email instructions for signing in to the AWS Management Console.
View user
IAM > Users > Create user
Step 1
Specify user 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://789576624500.signin.aws.amazon.com/console
User name
testuser
Console password
Show
Download .csv file
Return to users list
Feedback
Language
© 2023, Amazon Web Services India Private Limited or its affiliates.
Privacy
Terms
Cookie preferences
Type here to search
24°C Mostly sunny
ENG
10:46
03-02-2023

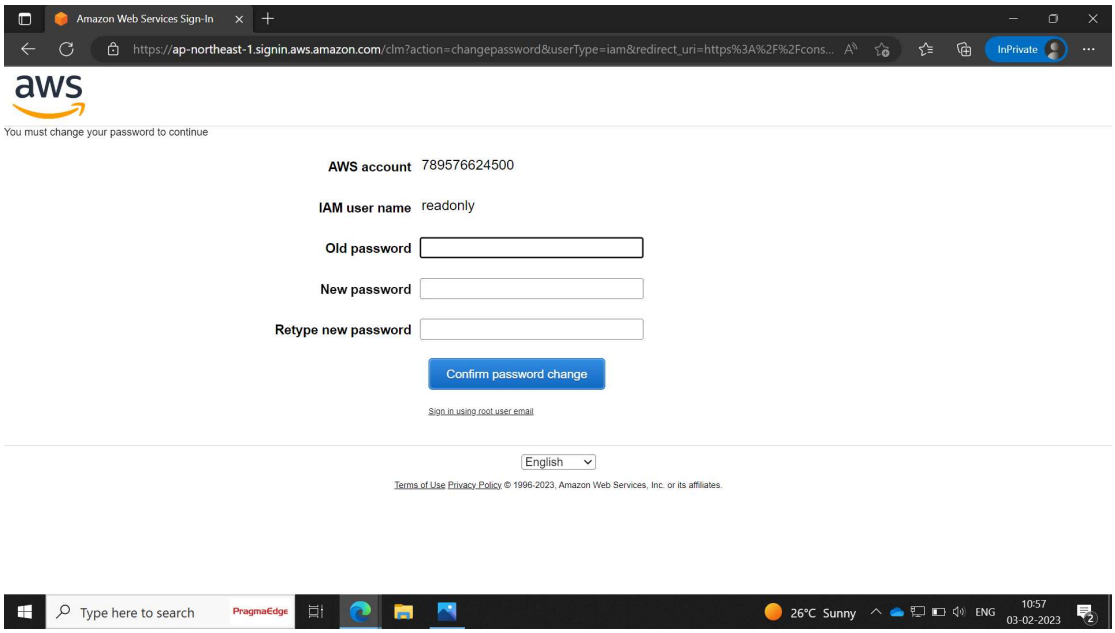

IAM Management Console
https://us-east-1.console.aws.amazon.com/iamv2/home?region=ap-south-1#/users/details/testuser?section=security...
Identity and Access Management (IAM)
User created successfully
You can view and download the user's password and email instructions for signing in to the AWS Management Console.
View user
ARN
arn:aws:iam::789576624500:user/testuser
Console access
Enabled without MFA
Access key 1
Not enabled
Created
February 03, 2023, 10:44 (UTC+05:30)
Last console sign-in
Never
Access key 2
Not enabled
Permissions
Groups
Tags
Security credentials
Access Advisor
Console sign-in
Manage console access
Console sign-in link
https://789576624500.signin.aws.amazon.com/console
Console password
Updated 1 minute ago (2023-02-03 10:44 GMT+5:30)
Last console sign-in
Never
Multi-factor authentication (MFA) (0)
Use MFA to increase the security of your AWS environment. Signing in with MFA requires an authentication code from an MFA device. Each user can have a maximum of 8 MFA devices assigned. Learn more
Remove
Resync
Assign MFA device
Device type
Identifier
Created on
Type here to search
24°C Mostly sunny
ENG
10:46
03-02-2023

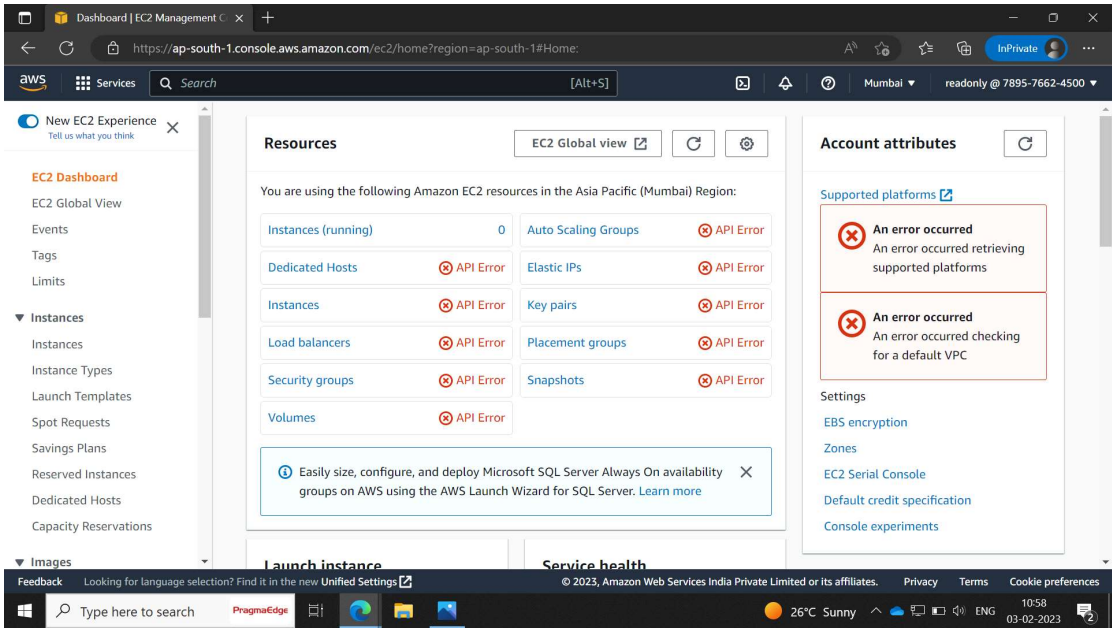

Amazon Web Services Sign-In
https://ap-south-1.signin.aws.amazon.com/oauth?client_id=arn%3Aaws%3Asignin%3A%3A%3Aconsole%2Fcanvas&code_challen...
InPrivate
aws
Sign in as IAM user
Account ID (12 digits) or account alias
789576624500
IAM user name
testuser
Password
Remember this account
Sign in
Sign in using root user email
Forgot password?
SageMaker Fridays
Join SageMaker Fridays for live coding, demos, and more
Register now ›
https://ap-south-1.signin.aws.amazon.com/oauth?client_id=arn%3Aaws%3Asignin%3A%3A%3Aconsole%2Fcanvas&code_challenge=5XAphJjWZUS-rz2IoOenF_BjAuU3TJs0jzDFLZjD39k&code_challenge_method=SHA-256&response_t...
Type here to search
ENG
10:54
03-02-2023

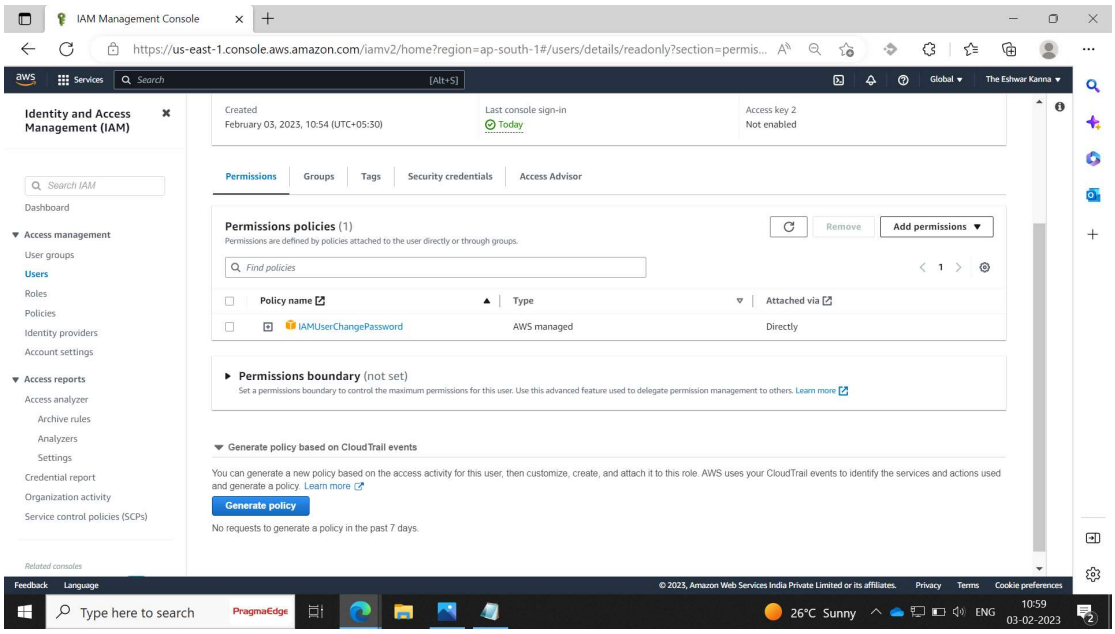

Dashboard | EC2 Management
https://ap-south-1.console.aws.amazon.com/ec2/home?region=ap-south-1#Home:
InPrivate
Services
Search
[Alt+S]
Mumbai
testuser @ 7895-7662-4500
New EC2 Experience
Tell us what you think
EC2 Dashboard
EC2 Global View
Events
Tags
Limits
Instances
Instances
Instance Types
Launch Templates
Spot Requests
Savings Plans
Reserved Instances
Dedicated Hosts
Capacity Reservations
Images
Resources
EC2 Global view
You are using the following Amazon EC2 resources in the Asia Pacific (Mumbai) Region:
Instances (running) 2
Auto Scaling Groups 0
Dedicated Hosts 0
Elastic IPs 0
Instances 12
Key pairs 4
Load balancers 0
Placement groups 0
Security groups 31
Snapshots 5
Volumes 9
Easily size, configure, and deploy Microsoft SQL Server Always On availability groups on AWS using the AWS Launch Wizard for SQL Server. Learn more
Launch instance
Service health
Account attributes
Supported platforms
VPC
Default VPC
vpc-06f405c2a337e0f4f
Settings
EBS encryption
Zones
EC2 Serial Console
Default credit specification
Console experiments
Explore AWS
Get Up to 40% Better Price Performance
Feedback
Looking for language selection? Find it in the new Unified Settings
© 2023, Amazon Web Services India Private Limited or its affiliates.
Privacy
Terms
Cookie preferences
Type here to search
PragmaEdge
USD/INR +0.29%
ENG
10:54
03-02-2023

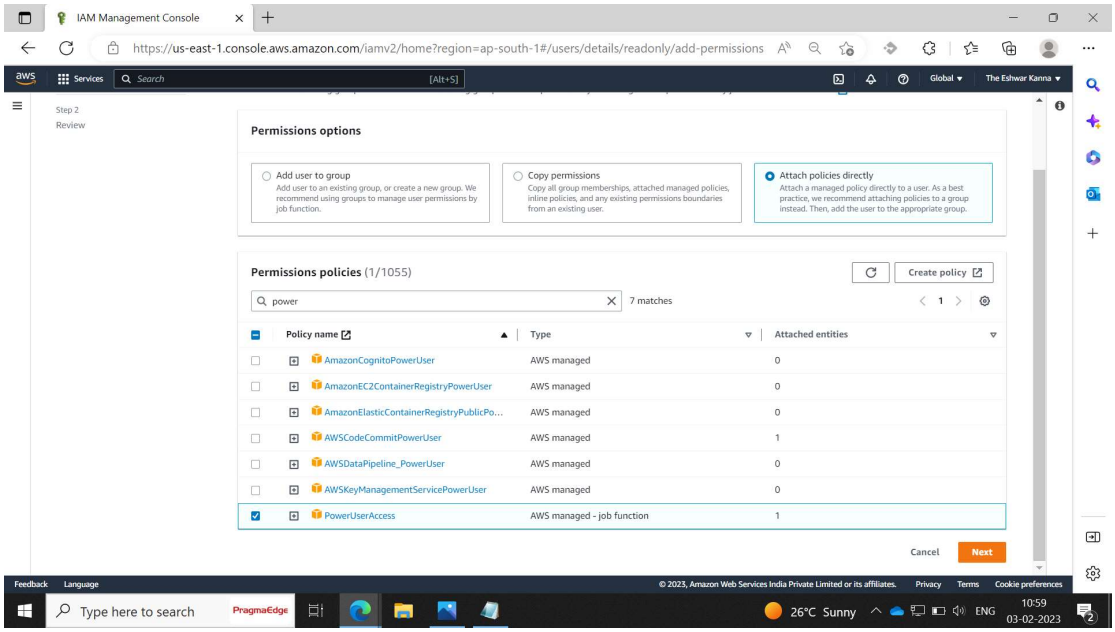

IAM Management Console
https://us-east-1.console.aws.amazon.com/iamv2/home?region=ap-south-1#/users/create
Services
Search
[Alt+S]
Global
The Eshwar Kanna
Step 1
Specify user details
Step 2
Set permissions
Step 3
Review and create
Step 4
Retrieve password
Specify user details
User details
User name
readonly
The user name can have up to 64 characters. Valid characters: A-Z, a-z, 0-9, and + = , . @ _ - (hyphen)
Enable console access - optional
Enables a password that allows users to sign in to the AWS Management Console.
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.
For programmatic access, you can generate access keys after you create the user. Learn more
Cancel
Next
Feedback
Language
© 2023, Amazon Web Services India Private Limited or its affiliates.
Privacy
Terms
Cookie preferences
Type here to search
PragmaEdge
USD/INR +0.29%
ENG
10:55
03-02-2023

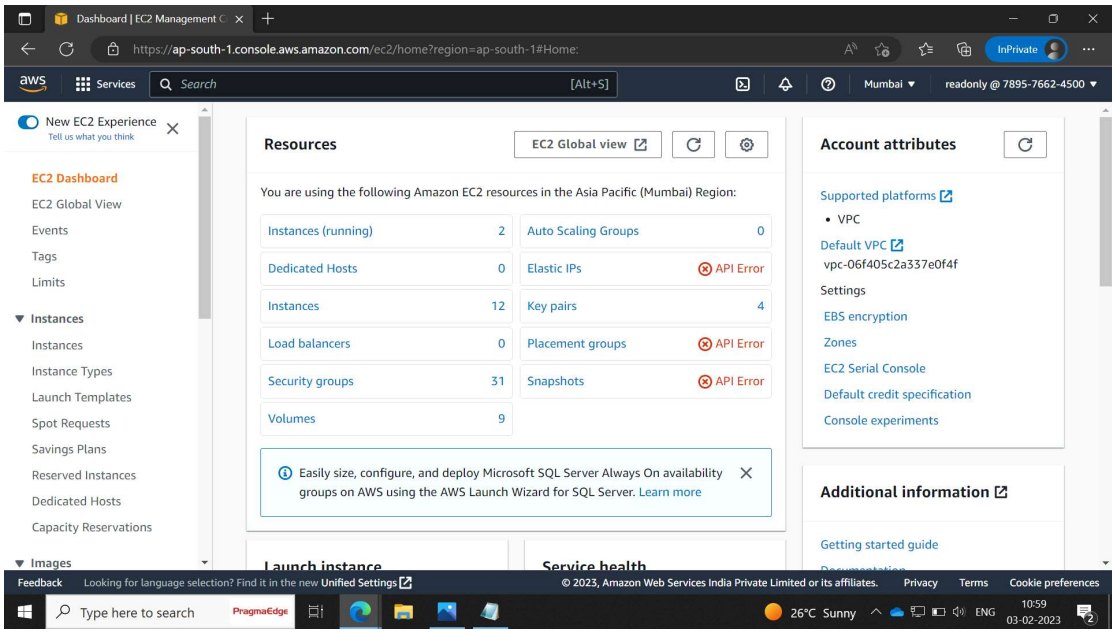

Amazon Web Services Sign-In
https://ap-northeast-1.signin.aws.amazon.com/oauth?client_id=arn%3Aaws%3Asignin%3A%3A%3Aconsole%2Fcanvas&code_cha...
InPrivate
aws
Sign in as IAM user
Account ID (12 digits) or account alias
789576624500
IAM user name
readonly
Password
Remember this account
Sign in
Sign in using root user email
Forgot password?
AWS Training and Certification
Propel your career. Get AWS certified
LEARN MORE
Type here to search
PragmaEdge
26°C Sunny
ENG
10:56
03-02-2023

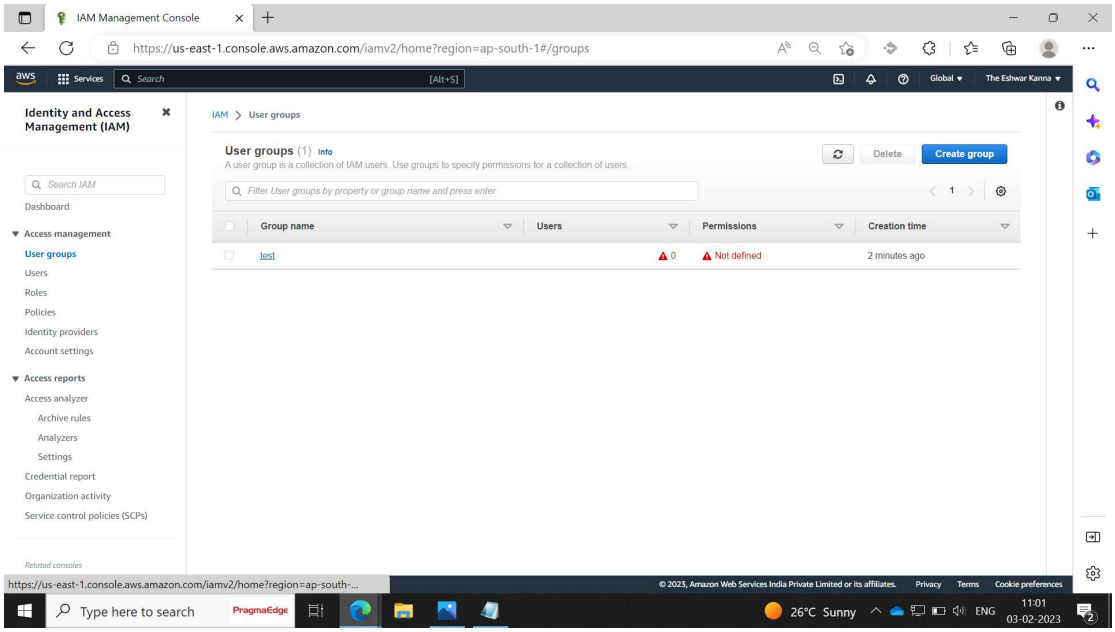

Amazon Web Services Sign-In
https://ap-northeast-1.signin.aws.amazon.com/clm?action=changepassword&userType=iam&redirect_uri=https%3A%2F%2Fcons...
InPrivate
aws
You must change your password to continue
AWS account 789576624500
IAM user name readonly
Old password
New password
Retype new password
Confirm password change
Sign in using root user email
English
Terms of Use Privacy Policy © 1996-2023, Amazon Web Services, Inc. or its affiliates.
Type here to search
PragmaEdge
26°C Sunny
ENG
10:57
03-02-2023

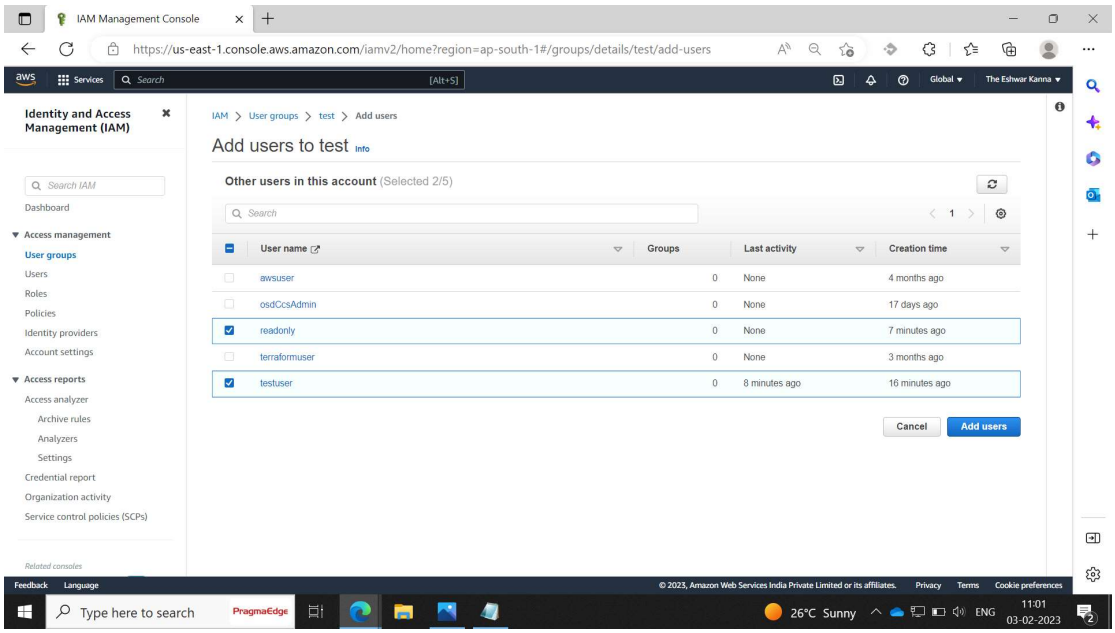

Dashboard | EC2 Management
https://ap-south-1.console.aws.amazon.com/ec2/home?region=ap-south-1#Home:
InPrivate
Services
Search
[Alt+S]
Mumbai
readonly @ 7895-7662-4500
New EC2 Experience
Tell us what you think
EC2 Dashboard
EC2 Global View
Events
Tags
Limits
Instances
Instances
Instance Types
Launch Templates
Spot Requests
Savings Plans
Reserved Instances
Dedicated Hosts
Capacity Reservations
Images
Resources
EC2 Global view
You are using the following Amazon EC2 resources in the Asia Pacific (Mumbai) Region:
Instances (running) 0
Auto Scaling Groups API Error
Dedicated Hosts API Error
Elastic IPs API Error
Instances API Error
Key pairs API Error
Load balancers API Error
Placement groups API Error
Security groups API Error
Snapshots API Error
Volumes API Error
Easily size, configure, and deploy Microsoft SQL Server Always On availability groups on AWS using the AWS Launch Wizard for SQL Server. Learn more
Launch instance
Service health
Account attributes
Supported platforms
An error occurred
An error occurred retrieving supported platforms
An error occurred
An error occurred checking for a default VPC
Settings
EBS encryption
Zones
EC2 Serial Console
Default credit specification
Console experiments
Feedback
Looking for language selection? Find it in the new Unified Settings
© 2023, Amazon Web Services India Private Limited or its affiliates.
Privacy
Terms
Cookie preferences
Type here to search
PragmaEdge
26°C Sunny
ENG
10:58
03-02-2023

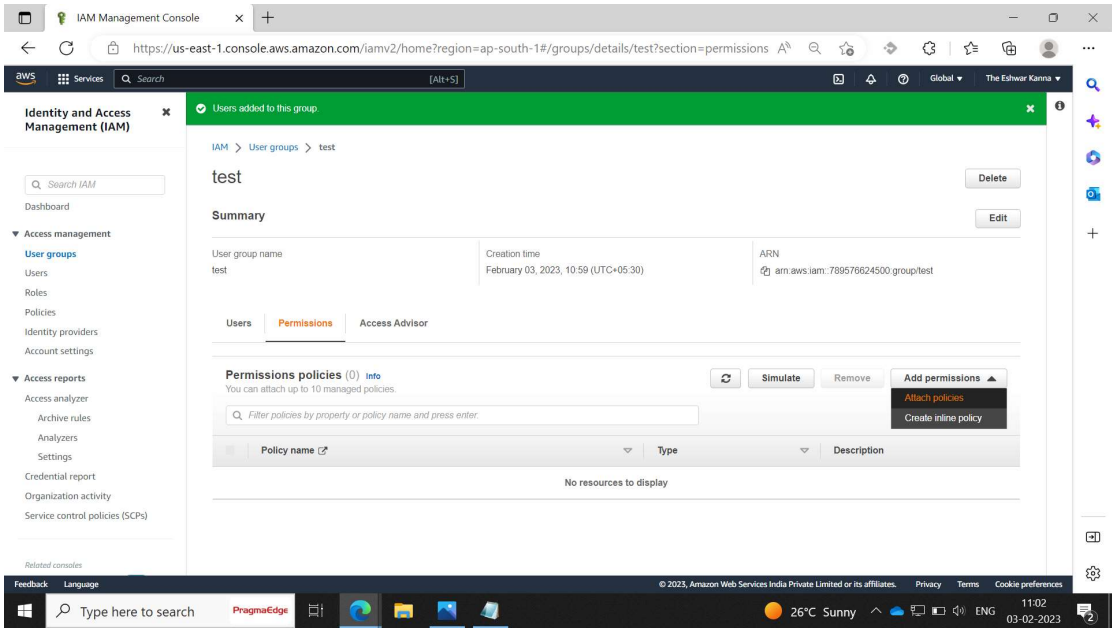

IAM Management Console
https://us-east-1.console.aws.amazon.com/iamv2/home?region=ap-south-1#/users/details/readonly?section=permis...
Services
Search
[Alt+S]
Global
The Eshwar Kanna
Identity and Access Management (IAM)
Search IAM
Dashboard
Access management
User groups
Users
Roles
Policies
Identity providers
Account settings
Access reports
Access analyzer
Archive rules
Analyzers
Settings
Credential report
Organization activity
Service control policies (SCPs)
Created
February 03, 2023, 10:54 (UTC+05:30)
Last console sign-in
Today
Access key 2
Not enabled
Permissions
Groups
Tags
Security credentials
Access Advisor
Permissions policies (1)
Permissions are defined by policies attached to the user directly or through groups.
Remove
Add permissions
Find policies
Policy name
Type
Attached via
IAMUserChangePassword
AWS managed
Directly
Permissions boundary (not set)
Set a permissions boundary to control the maximum permissions for this user. Use this advanced feature used to delegate permission management to others. Learn more
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.
Feedback
Language
© 2023, Amazon Web Services India Private Limited or its affiliates.
Privacy
Terms
Cookie preferences
Type here to search
PragmaEdge
26°C Sunny
ENG
10:59
03-02-2023

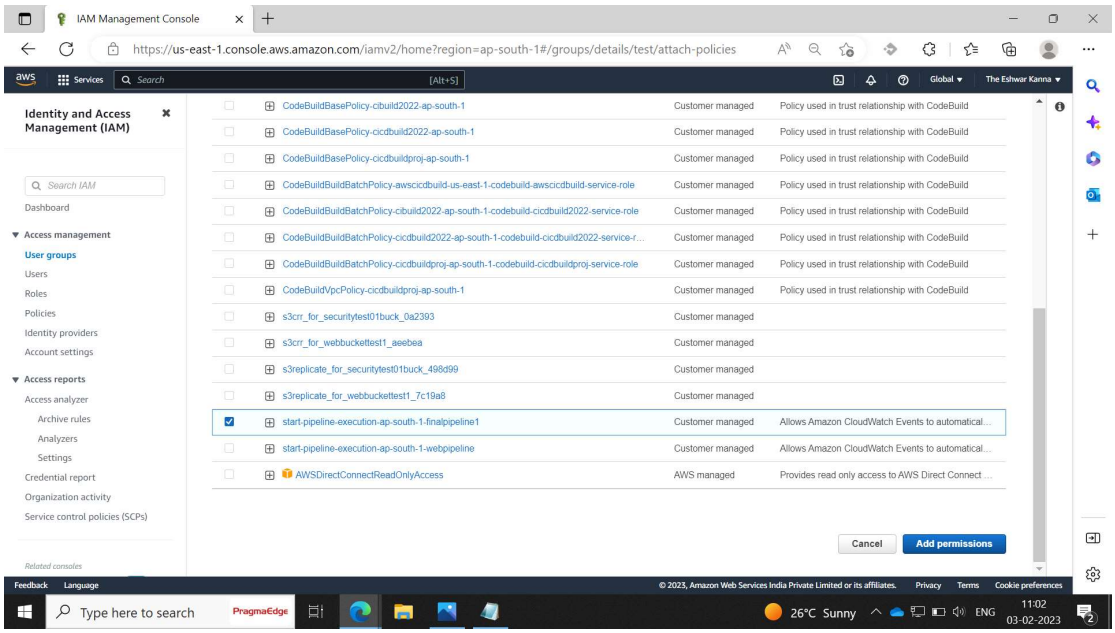

IAM Management Console
https://us-east-1.console.aws.amazon.com/iamv2/home?region=ap-south-1#/users/details/readonly/add-permissions
Step 2
Review
Permissions options
Add user to group
Add user to an existing group, or create a new group. We recommend using groups to manage user permissions by job function.
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 (1/1055)
Create policy
power
7 matches
Policy name
Type
Attached entities
AmazonCognitoPowerUser AWS managed 0
AmazonEC2ContainerRegistryPowerUser AWS managed 0
AmazonElasticContainerRegistryPublicPo... AWS managed 0
AWSCodeCommitPowerUser AWS managed 1
AWSDataPipeline_PowerUser AWS managed 0
AWSKeyManagementServicePowerUser AWS managed 0
PowerUserAccess AWS managed - job function 1
Cancel
Next
Feedback
Language
© 2023, Amazon Web Services India Private Limited or its affiliates.
Privacy
Terms
Cookie preferences
Type here to search
26°C Sunny
ENG
10:59
03-02-2023

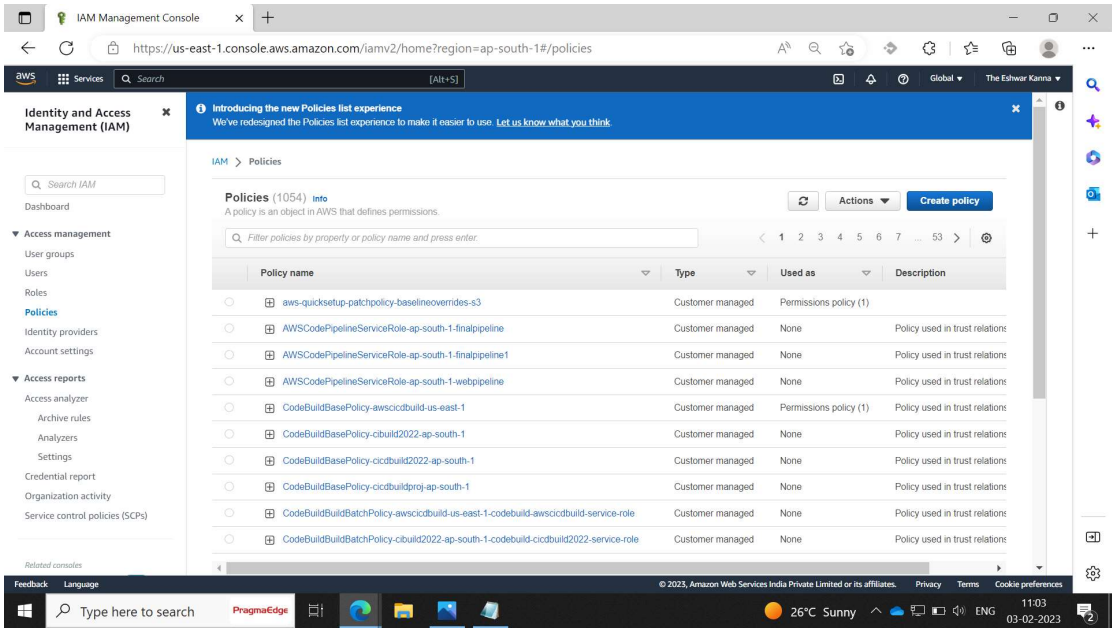

Dashboard | EC2 Management
https://ap-south-1.console.aws.amazon.com/ec2/home?region=ap-south-1#Home:
InPrivate
Mumbai
readonly @ 7895-7662-4500
New EC2 Experience
Tell us what you think
EC2 Dashboard
EC2 Global View
Events
Tags
Limits
Instances
Instances
Instance Types
Launch Templates
Spot Requests
Savings Plans
Reserved Instances
Dedicated Hosts
Capacity Reservations
Images
Resources
EC2 Global view
You are using the following Amazon EC2 resources in the Asia Pacific (Mumbai) Region:
Instances (running) 2
Auto Scaling Groups 0
Dedicated Hosts 0
Elastic IPs API Error
Instances 12
Key pairs 4
Load balancers 0
Placement groups API Error
Security groups 31
Snapshots API Error
Volumes 9
Easily size, configure, and deploy Microsoft SQL Server Always On availability groups on AWS using the AWS Launch Wizard for SQL Server. Learn more
Account attributes
Supported platforms
VPC
Default VPC
vpc-06f405c2a337e0f4f
Settings
EBS encryption
Zones
EC2 Serial Console
Default credit specification
Console experiments
Additional information
Getting started guide
Launch instance
Service health
Feedback
Looking for language selection? Find it in the new Unified Settings
© 2023, Amazon Web Services India Private Limited or its affiliates.
Privacy
Terms
Cookie preferences
Type here to search
26°C Sunny
ENG
10:59
03-02-2023

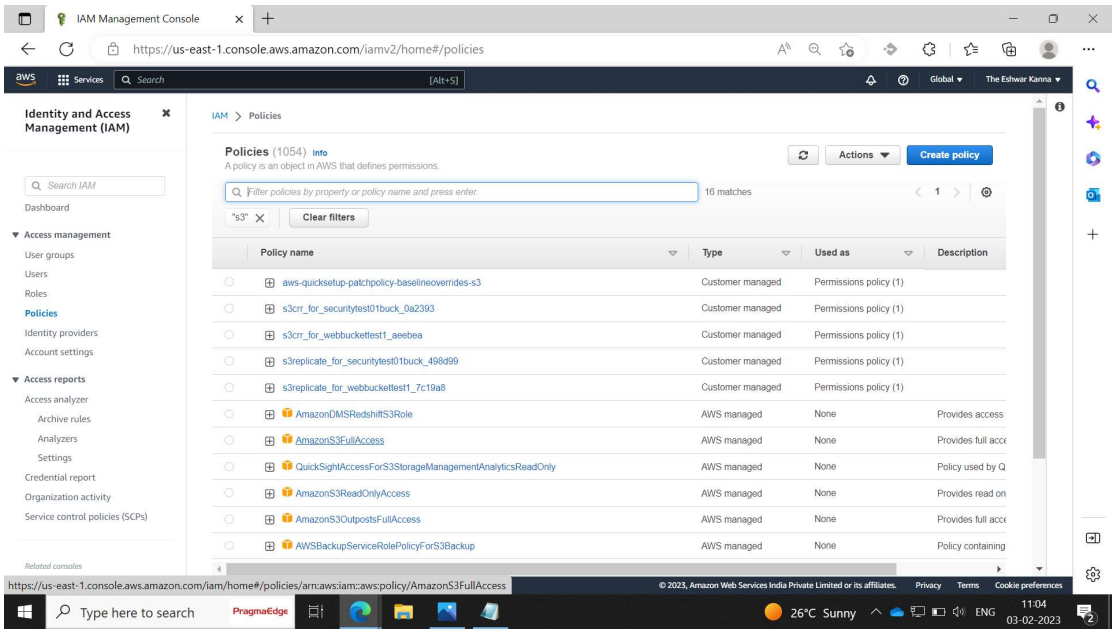

IAM Management Console
https://us-east-1.console.aws.amazon.com/iamv2/home?region=ap-south-1#/groups
Identity and Access Management (IAM)
IAM > User groups
User groups (1) Info
A user group is a collection of IAM users. Use groups to specify permissions for a collection of users.
Delete
Create group
Filter User groups by property or group name and press enter
Group name
Users
Permissions
Creation time
test
0
Not defined
2 minutes ago
Dashboard
Access management
User groups
Users
Roles
Policies
Identity providers
Account settings
Access reports
Access analyzer
Archive rules
Analyzers
Settings
Credential report
Organization activity
Service control policies (SCPs)
© 2023, Amazon Web Services India Private Limited or its affiliates.
Privacy
Terms
Cookie preferences
Type here to search
26°C Sunny
ENG
11:01
03-02-2023

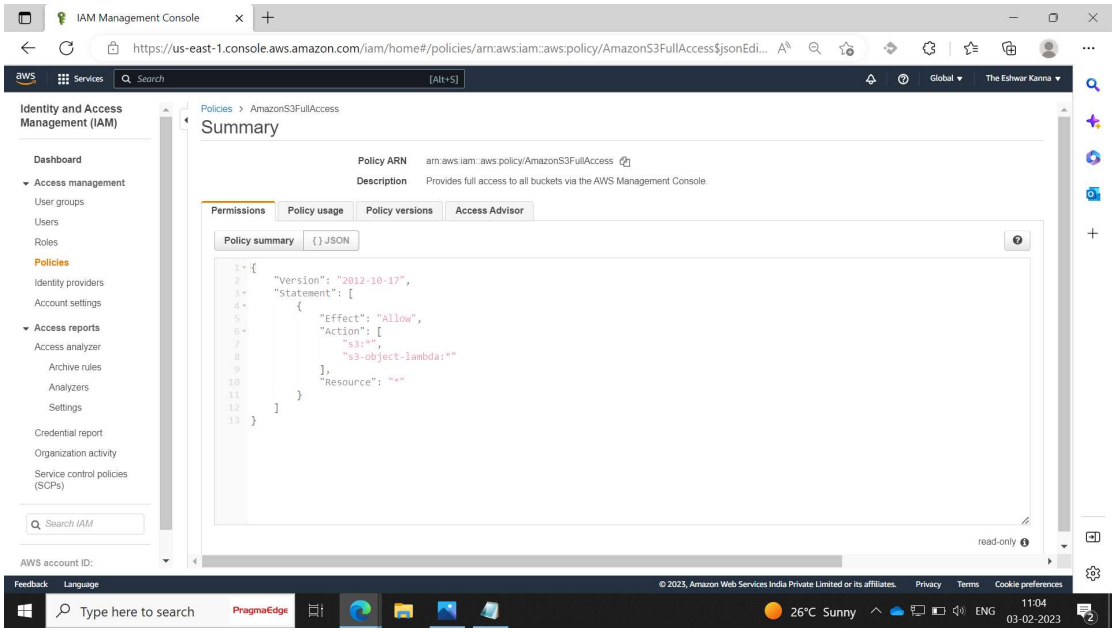

IAM Management Console
https://us-east-1.console.aws.amazon.com/iamv2/home?region=ap-south-1#/groups/details/test/add-users
Identity and Access Management (IAM)
IAM > User groups > test > Add users
Add users to test Info
Other users in this account (Selected 2/5)
User name
Groups
Last activity
Creation time
awsuser
0
None
4 months ago
osdCcsAdmin
0
None
17 days ago
readonly
0
None
7 minutes ago
terraformuser
0
None
3 months ago
testuser
0
8 minutes ago
16 minutes ago
Cancel
Add users
Feedback
Language
© 2023, Amazon Web Services India Private Limited or its affiliates.
Privacy
Terms
Cookie preferences
Type here to search
26°C Sunny
ENG
11:01
03-02-2023

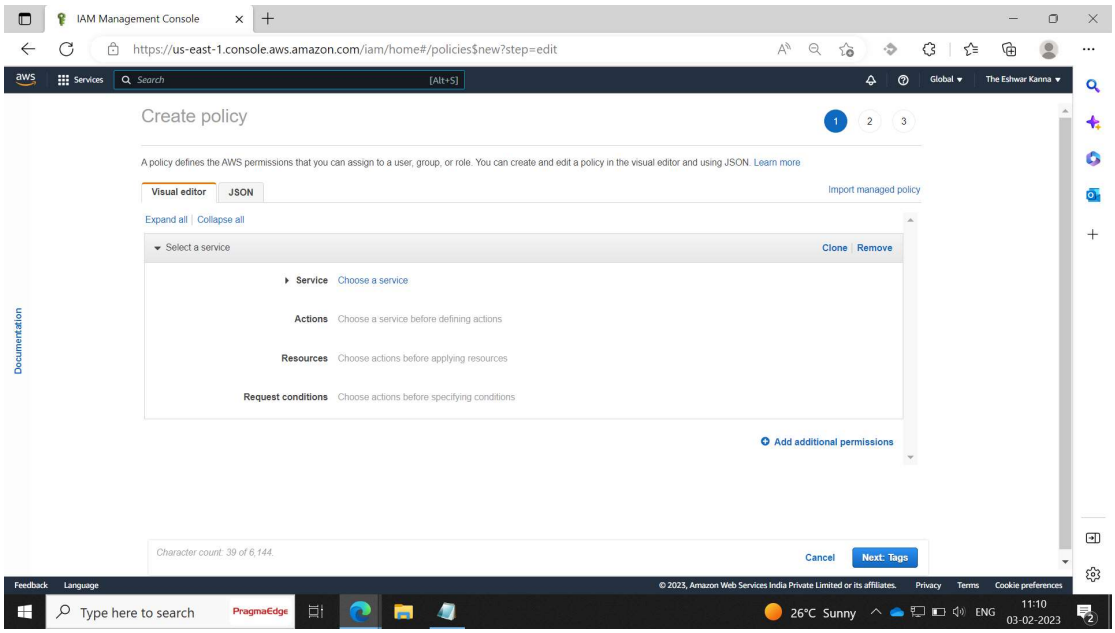

IAM Management Console
https://us-east-1.console.aws.amazon.com/iamv2/home?region=ap-south-1#/groups/details/test?section=permissions
Identity and Access Management (IAM)
Users added to this group.
IAM > User groups > test
test
Delete
Summary
Edit
User group name
test
Creation time
February 03, 2023, 10:59 (UTC+05:30)
ARN
arn:aws:iam::789576624500:group/test
Users
Permissions
Access Advisor
Permissions policies (0) Info
You can attach up to 10 managed policies.
Simulate
Remove
Add permissions
Attach policies
Create inline policy
Filter policies by property or policy name and press enter.
Policy name
Type
Description
No resources to display
Dashboard
Access management
User groups
Users
Roles
Policies
Identity providers
Account settings
Access reports
Access analyzer
Archive rules
Analyzers
Settings
Credential report
Organization activity
Service control policies (SCPs)
Feedback
Language
© 2023, Amazon Web Services India Private Limited or its affiliates.
Privacy
Terms
Cookie preferences
Type here to search
26°C Sunny
ENG
11:02
03-02-2023

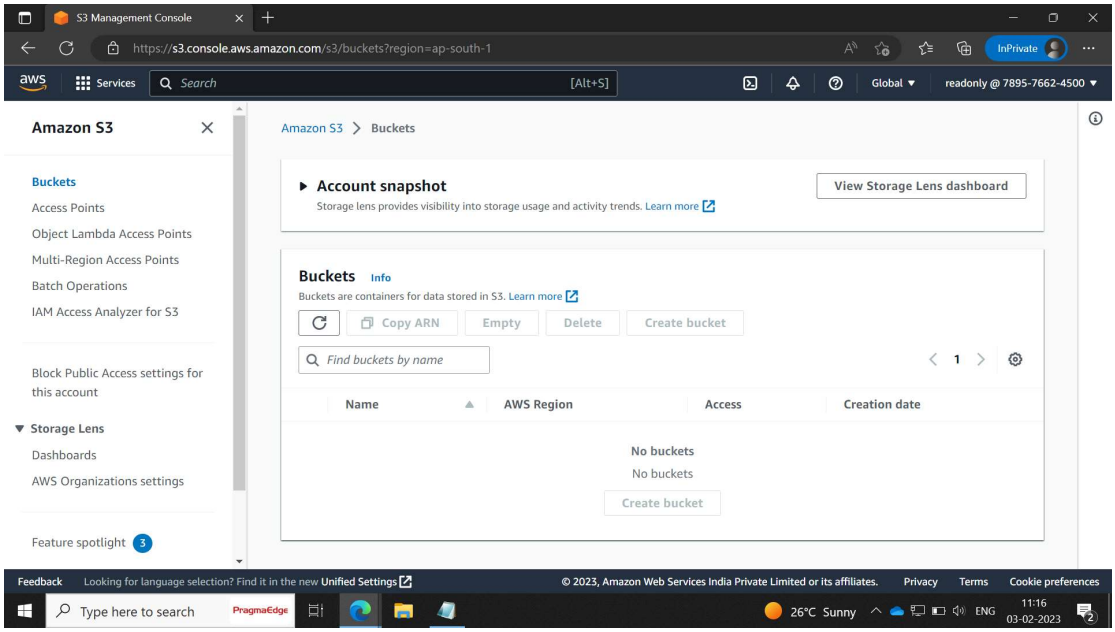

IAM Management Console
https://us-east-1.console.aws.amazon.com/iamv2/home?region=ap-south-1#/groups/details/test/attach-policies
Identity and Access Management (IAM)
CodeBuildBasePolicy-cibuild2022-ap-south-1 Customer managed Policy used in trust relationship with CodeBuild
CodeBuildBasePolicy-cicdbuild2022-ap-south-1 Customer managed Policy used in trust relationship with CodeBuild
CodeBuildBasePolicy-cicdbuildproj-ap-south-1 Customer managed Policy used in trust relationship with CodeBuild
CodeBuildBuildBatchPolicy-awscicdbuild-us-east-1-codebuild-awscicdbuild-service-role Customer managed Policy used in trust relationship with CodeBuild
CodeBuildBuildBatchPolicy-cibuild2022-ap-south-1-codebuild-cicdbuild2022-service-role Customer managed Policy used in trust relationship with CodeBuild
CodeBuildBuildBatchPolicy-cicdbuild2022-ap-south-1-codebuild-cicdbuild2022-service-r... Customer managed Policy used in trust relationship with CodeBuild
CodeBuildBuildBatchPolicy-cicdbuildproj-ap-south-1-codebuild-cicdbuildproj-service-role Customer managed Policy used in trust relationship with CodeBuild
CodeBuildVpcPolicy-cicdbuildproj-ap-south-1 Customer managed Policy used in trust relationship with CodeBuild
s3crr_for_securitytest01buck_0a2393 Customer managed
s3crr_for_webbuckettest1_aeebea Customer managed
s3replicate_for_securitytest01buck_498d99 Customer managed
s3replicate_for_webbuckettest1_7c19a8 Customer managed
start-pipeline-execution-ap-south-1-finalpipeline1 Customer managed Allows Amazon CloudWatch Events to automatical...
start-pipeline-execution-ap-south-1-webpipeline Customer managed Allows Amazon CloudWatch Events to automatical...
AWSDirectConnectReadOnlyAccess AWS managed Provides read only access to AWS Direct Connect ...
Cancel
Add permissions
Dashboard
Access management
User groups
Users
Roles
Policies
Identity providers
Account settings
Access reports
Access analyzer
Archive rules
Analyzers
Settings
Credential report
Organization activity
Service control policies (SCPs)
Feedback
Language
© 2023, Amazon Web Services India Private Limited or its affiliates.
Privacy
Terms
Cookie preferences
Type here to search
26°C Sunny
ENG
11:02
03-02-2023

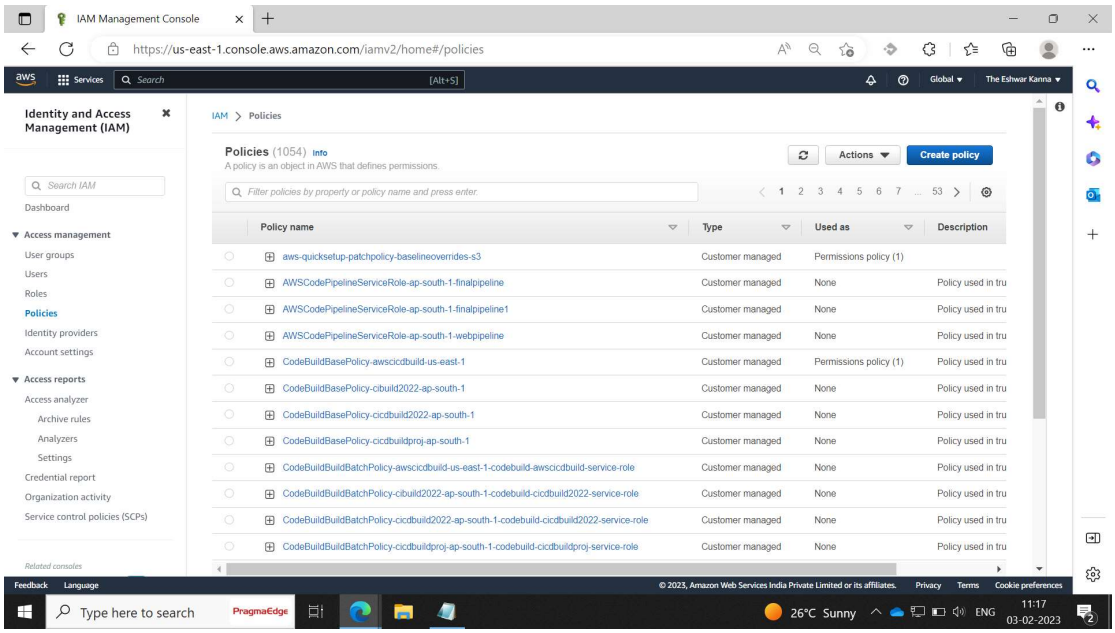

IAM Management Console
https://us-east-1.console.aws.amazon.com/iamv2/home?region=ap-south-1#/policies
Identity and Access Management (IAM)
Introducing the new Policies list experience
We've redesigned the Policies list experience to make it easier to use. Let us know what you think.
IAM > Policies
Policies (1054) Info
A policy is an object in AWS that defines permissions.
Actions
Create policy
Filter policies by property or policy name and press enter.
Policy name
Type
Used as
Description
aws-quicksetup-patchpolicy-baselineoverrides-s3
AWSCodePipelineServiceRole-ap-south-1-finalpipeline
AWSCodePipelineServiceRole-ap-south-1-finalpipeline1
AWSCodePipelineServiceRole-ap-south-1-webpipeline
CodeBuildBasePolicy-awscidbuild-us-east-1
CodeBuildBasePolicy-cibuild2022-ap-south-1
CodeBuildBasePolicy-cicdbuild2022-ap-south-1
CodeBuildBasePolicy-cicdbuildproj-ap-south-1
CodeBuildBuildBatchPolicy-awscicdbuild-us-east-1-codebuild-awscicdbuild-service-role
CodeBuildBuildBatchPolicy-cibuild2022-ap-south-1-codebuild-cicdbuild2022-service-role
Customer managed
Permissions policy (1)
None
Policy used in trust relations
Feedback
Language
© 2023, Amazon Web Services India Private Limited or its affiliates.
Privacy
Terms
Cookie preferences
Type here to search
PragmaEdge
26°C Sunny
ENG
11:03
03-02-2023

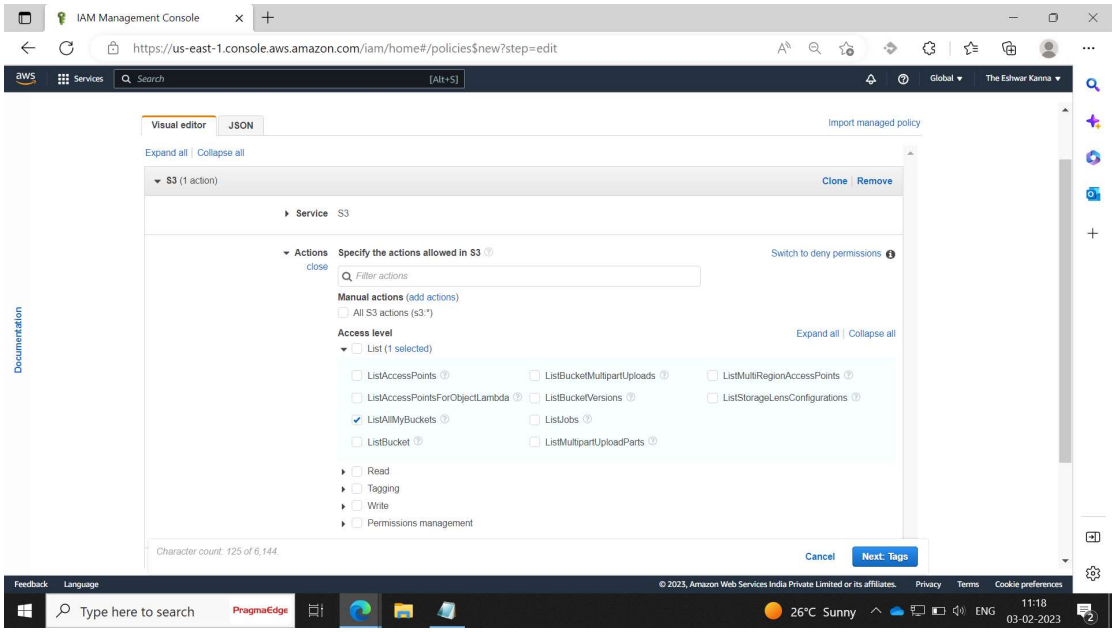

IAM Management Console
https://us-east-1.console.aws.amazon.com/iamv2/home#/policies
Identity and Access Management (IAM)
IAM > Policies
Policies (1054) Info
A policy is an object in AWS that defines permissions.
Actions
Create policy
Filter policies by property or policy name and press enter.
16 matches
"s3"
Clear filters
Policy name
Type
Used as
Description
aws-quicksetup-patchpolicy-baselineoverrides-s3
s3crr_for_securitytest01buck_0a2393
s3crr_for_webbuckettest1_aeebea
s3replicate_for_securitytest01buck_498d99
s3replicate_for_webbuckettest1_7c19a8
AmazonDMSRedshiftS3Role
AmazonS3FullAccess
QuickSightAccessForS3StorageManagementAnalyticsReadOnly
AmazonS3ReadOnlyAccess
AmazonS3OutpostsFullAccess
AWSBackupServiceRolePolicyForS3Backup
Customer managed
Permissions policy (1)
AWS managed
None
Provides access
Provides full acc
Policy used by Q
Provides read on
Policy containing
https://us-east-1.console.aws.amazon.com/iam/home#/policies/arn:aws:iam::aws:policy/AmazonS3FullAccess
© 2023, Amazon Web Services India Private Limited or its affiliates.
Privacy
Terms
Cookie preferences
Type here to search
PragmaEdge
26°C Sunny
ENG
11:04
03-02-2023

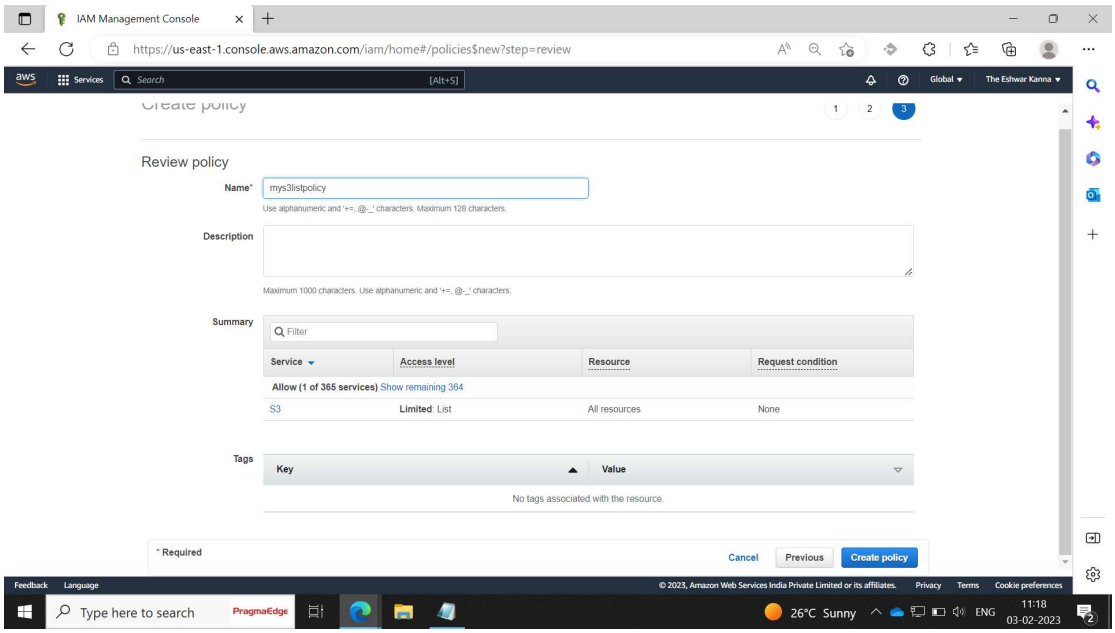

IAM Management Console
https://us-east-1.console.aws.amazon.com/iam/home#/policies/arn:aws:iam::aws:policy/AmazonS3FullAccess$jsonEdi...
Identity and Access Management (IAM)
Dashboard
Access management
User groups
Users
Roles
Policies
Identity providers
Account settings
Access reports
Access analyzer
Archive rules
Analyzers
Settings
Credential report
Organization activity
Service control policies (SCPs)
Policies > AmazonS3FullAccess
Summary
Policy ARN arn:aws:iam::aws:policy/AmazonS3FullAccess
Description Provides full access to all buckets via the AWS Management Console.
Permissions
Policy usage
Policy versions
Access Advisor
Policy summary
{} JSON
{
"Version": "2012-10-17",
"Statement": [
{
"Effect": "Allow",
"Action": [
"s3:*",
"s3-object-lambda:*"
],
"Resource": "*"
}
]
}
read-only
Feedback
Language
© 2023, Amazon Web Services India Private Limited or its affiliates.
Privacy
Terms
Cookie preferences
Type here to search
PragmaEdge
26°C Sunny
ENG
11:04
03-02-2023

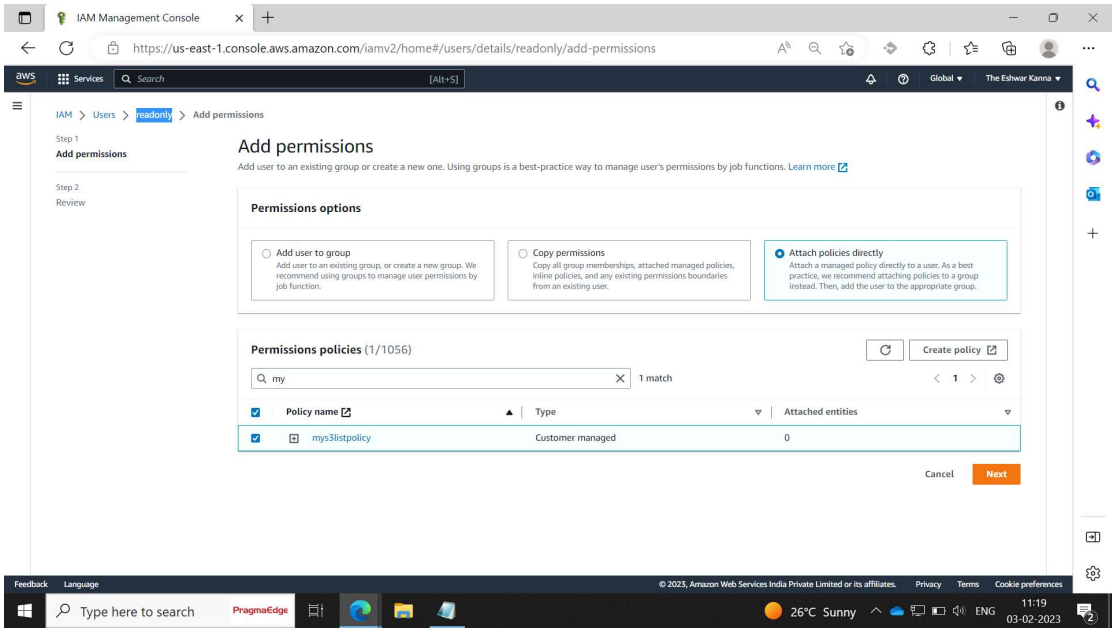

IAM Management Console
https://us-east-1.console.aws.amazon.com/iam/home#/policies$new?step=edit
Create policy
1
2
3
A policy defines the AWS permissions that you can assign to a user, group, or role. You can create and edit a policy in the visual editor and using JSON. Learn more
Visual editor
JSON
Import managed policy
Expand all | Collapse all
Select a service
Clone | Remove
Service Choose a service
Actions Choose a service before defining actions
Resources Choose actions before applying resources
Request conditions Choose actions before specifying conditions
Add additional permissions
Documentation
Character count: 39 of 6,144.
Cancel
Next: Tags
Feedback
Language
© 2023, Amazon Web Services India Private Limited or its affiliates.
Privacy
Terms
Cookie preferences
Type here to search
PragmaEdge
26°C Sunny
ENG
11:10
03-02-2023

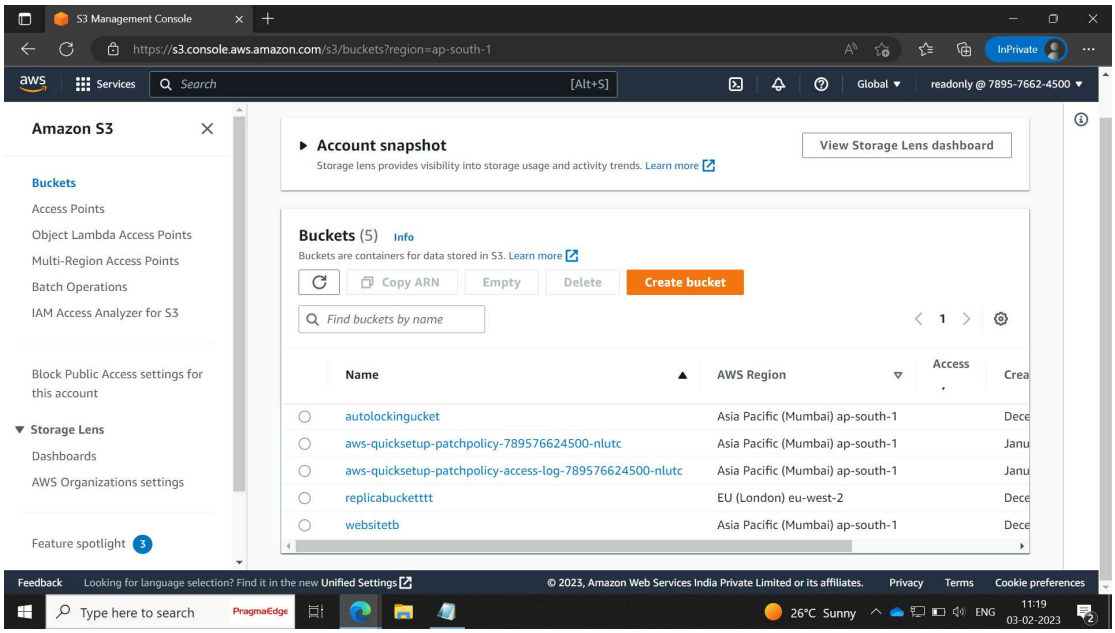

S3 Management Console
https://s3.console.aws.amazon.com/s3/buckets?region=ap-south-1
Amazon S3
Buckets
Access Points
Object Lambda Access Points
Multi-Region Access Points
Batch Operations
IAM Access Analyzer for S3
Block Public Access settings for this account
Storage Lens
Dashboards
AWS Organizations settings
Feature spotlight
Amazon S3 > Buckets
Account snapshot
Storage lens provides visibility into storage usage and activity trends. Learn more
View Storage Lens dashboard
Buckets Info
Buckets are containers for data stored in S3. Learn more
Copy ARN
Empty
Delete
Create bucket
Find buckets by name
Name
AWS Region
Access
Creation date
No buckets
No buckets
Create bucket
Feedback
Looking for language selection? Find it in the new Unified Settings
© 2023, Amazon Web Services India Private Limited or its affiliates.
Privacy
Terms
Cookie preferences
Type here to search
26°C Sunny
ENG
11:16
03-02-2023

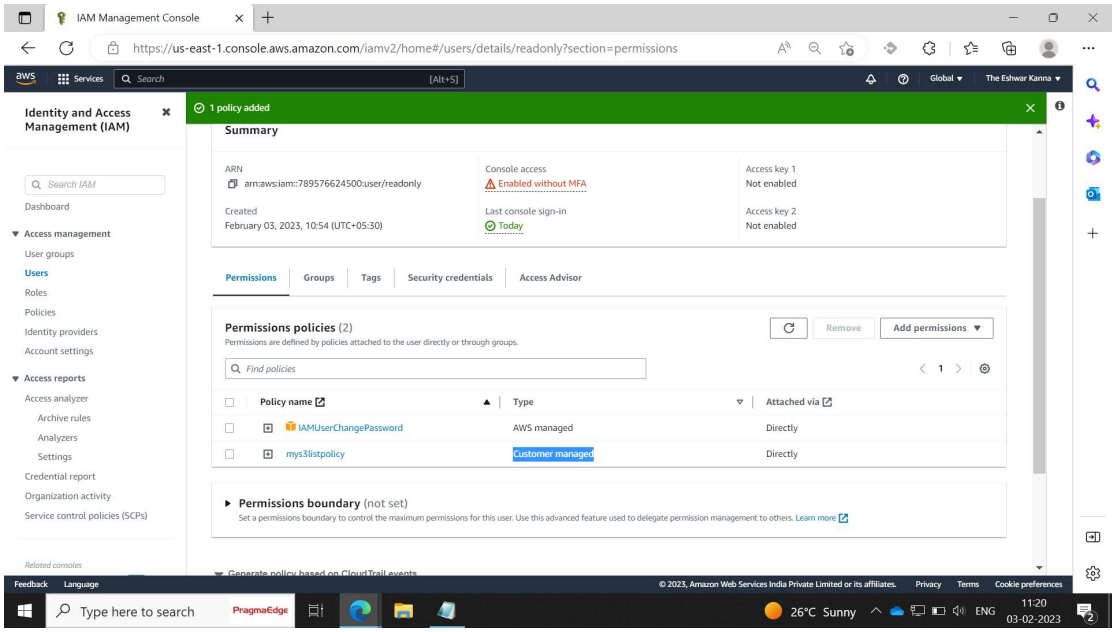

IAM Management Console
https://us-east-1.console.aws.amazon.com/iamv2/home#/policies
Identity and Access Management (IAM)
Dashboard
Access management
User groups
Users
Roles
Policies
Identity providers
Account settings
Access reports
Access analyzer
Archive rules
Analyzers
Settings
Credential report
Organization activity
Service control policies (SCPs)
IAM > Policies
Policies (1054) Info
A policy is an object in AWS that defines permissions.
Actions
Create policy
Policy name
Type
Used as
Description
aws-quicksetup-patchpolicy-baselineoverrides-s3
AWSCodePipelineServiceRole-ap-south-1-finalpipeline
AWSCodePipelineServiceRole-ap-south-1-finalpipeline1
AWSCodePipelineServiceRole-ap-south-1-webpipeline
CodeBuildBasePolicy-awscidbuild-us-east-1
CodeBuildBasePolicy-cibuild2022-ap-south-1
CodeBuildBasePolicy-cicdbuild2022-ap-south-1
CodeBuildBasePolicy-cicdbuildproj-ap-south-1
CodeBuildBuildBatchPolicy-awscidbuild-us-east-1-codebuild-awscidbuild-service-role
CodeBuildBuildBatchPolicy-cibuild2022-ap-south-1-codebuild-cicdbuild2022-service-role
CodeBuildBuildBatchPolicy-cicdbuild2022-ap-south-1-codebuild-cicdbuild2022-service-role
CodeBuildBuildBatchPolicy-cicdbuildproj-ap-south-1-codebuild-cicdbuildproj-service-role
Feedback
Language
© 2023, Amazon Web Services India Private Limited or its affiliates.
Privacy
Terms
Cookie preferences
Type here to search
26°C Sunny
ENG
11:17
03-02-2023

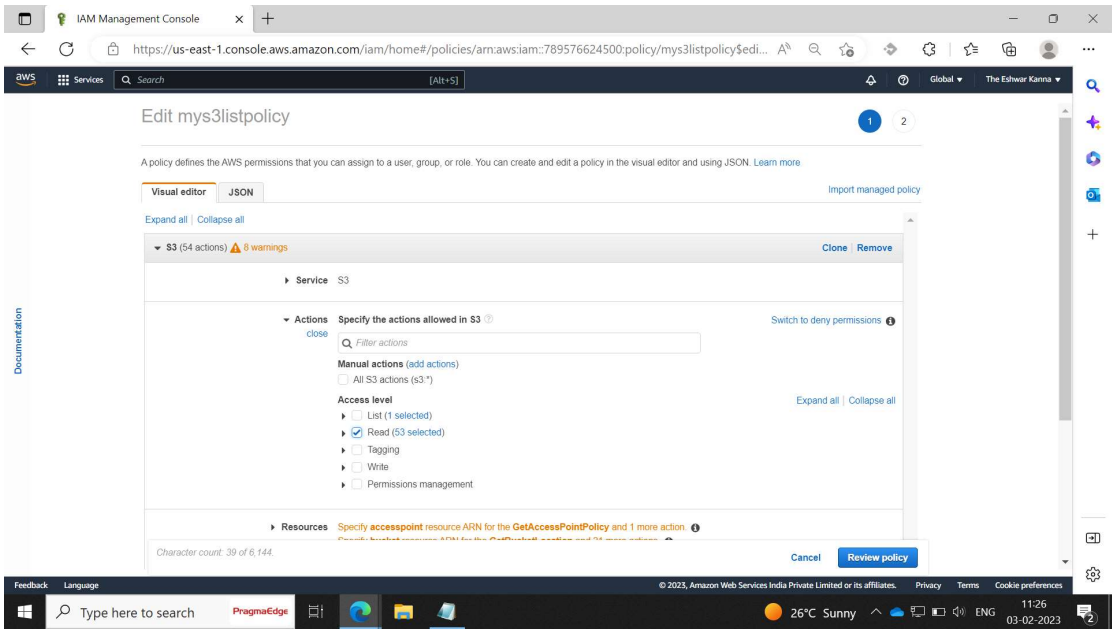

IAM Management Console
https://us-east-1.console.aws.amazon.com/iam/home#/policies$new?step=edit
Visual editor
JSON
Import managed policy
Expand all | Collapse all
S3 (1 action)
Clone | Remove
Service S3
Actions
Specify the actions allowed in S3
Switch to deny permissions
Filter actions
Manual actions (add actions)
All S3 actions (s3:*)
Access level
Expand all | Collapse all
List (1 selected)
ListAccessPoints
ListBucketMultipartUploads
ListMultiRegionAccessPoints
ListAccessPointsForObjectLambda
ListBucketVersions
ListStorageLensConfigurations
ListAllMyBuckets
ListJobs
ListBucket
ListMultipartUploadParts
Read
Tagging
Write
Permissions management
Character count: 125 of 6,144.
Cancel
Next: Tags
Feedback
Language
© 2023, Amazon Web Services India Private Limited or its affiliates.
Privacy
Terms
Cookie preferences
Type here to search
26°C Sunny
ENG
11:18
03-02-2023

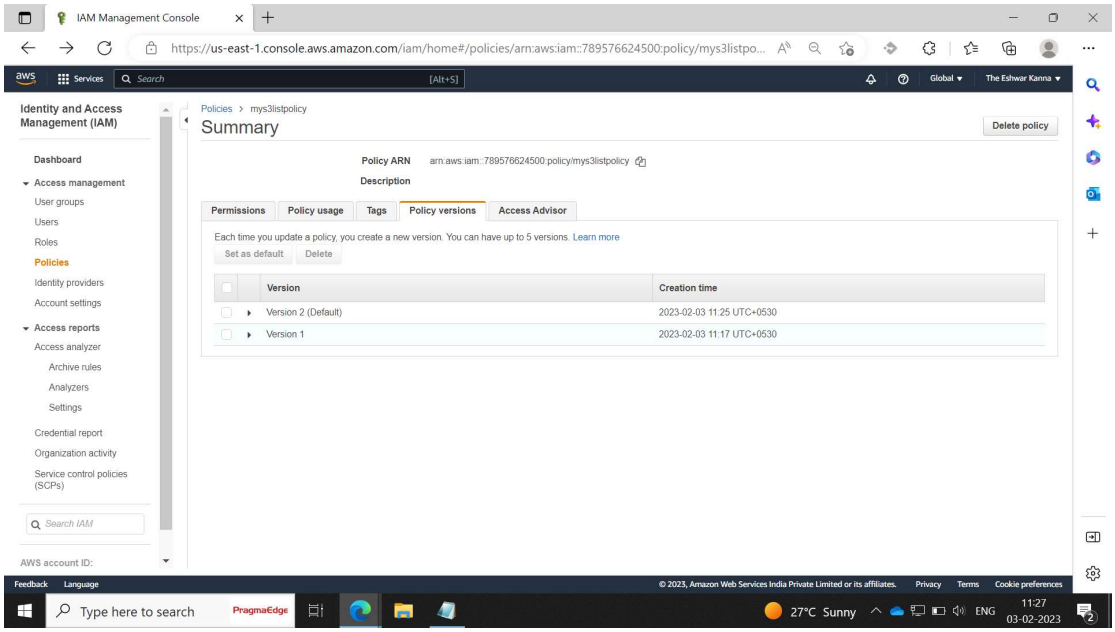

IAM Management Console
https://us-east-1.console.aws.amazon.com/iam/home#/policies$new?step=review
Review policy
Name*
mys3listpolicy
Use alphanumeric and '+=,.@-_' characters. Maximum 128 characters.
Description
Maximum 1000 characters. Use alphanumeric and '+=,.@-_' characters.
Summary
Filter
Service
Access level
Resource
Request condition
Allow (1 of 365 services) Show remaining 364
S3
Limited: List
All resources
None
Tags
Key
Value
No tags associated with the resource.
* Required
Cancel
Previous
Create policy
Feedback
Language
© 2023, Amazon Web Services India Private Limited or its affiliates.
Privacy
Terms
Cookie preferences
Type here to search
26°C Sunny
ENG
11:18
03-02-2023

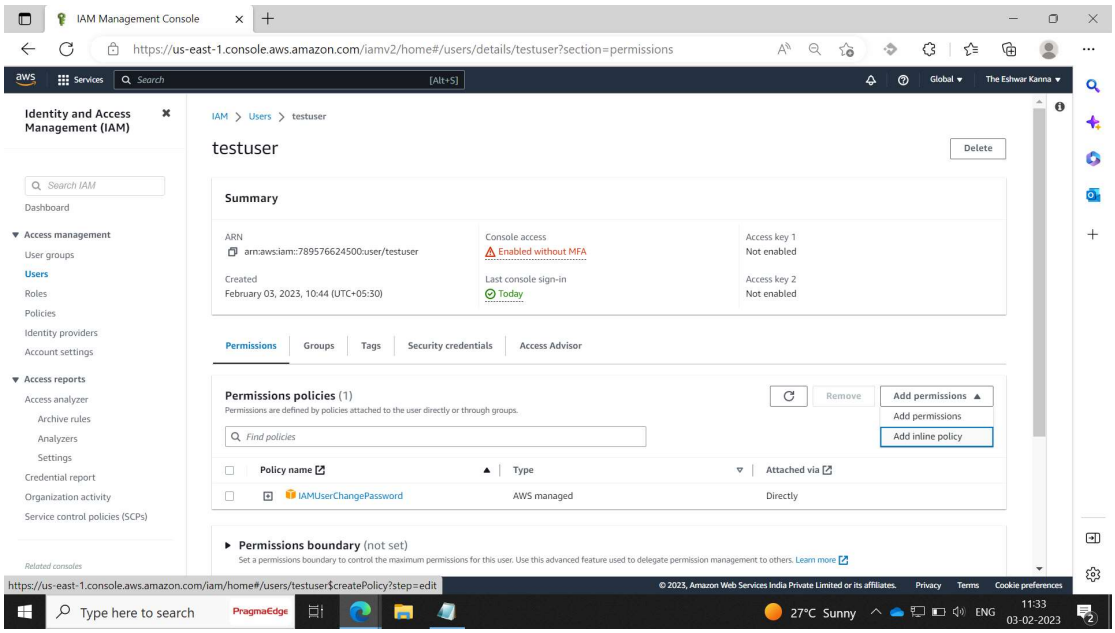

IAM Management Console
https://us-east-1.console.aws.amazon.com/iamv2/home#/users/details/readonly/add-permissions
IAM > Users > readonly > Add permissions
Step 1
Add permissions
Step 2
Review
Add permissions
Add user to an existing group or create a new one. Using groups is a best-practice way to manage 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 (1/1056)
Create policy
my
1 match
Policy name
Type
Attached entities
mys3listpolicy
Customer managed
0
Cancel
Next
Feedback
Language
© 2023, Amazon Web Services India Private Limited or its affiliates.
Privacy
Terms
Cookie preferences
Type here to search
PragmaEdge
26°C Sunny
ENG
11:19
03-02-2023

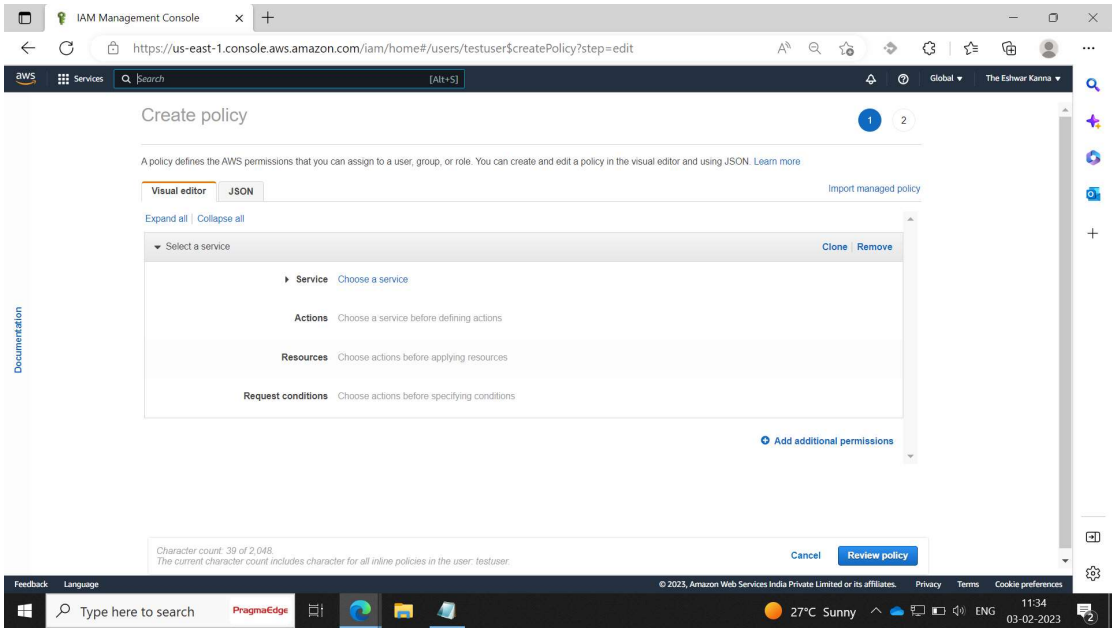

S3 Management Console
https://s3.console.aws.amazon.com/s3/buckets?region=ap-south-1
InPrivate
Services
Search
[Alt+S]
Global
readonly @ 7895-7662-4500
Amazon S3
Buckets
Access Points
Object Lambda Access Points
Multi-Region Access Points
Batch Operations
IAM Access Analyzer for S3
Block Public Access settings for this account
Storage Lens
Dashboards
AWS Organizations settings
Feature spotlight
3
Account snapshot
Storage lens provides visibility into storage usage and activity trends. Learn more
View Storage Lens dashboard
Buckets (5) Info
Buckets are containers for data stored in S3. Learn more
Copy ARN
Empty
Delete
Create bucket
Find buckets by name
Name
AWS Region
Access
autolockingucket
Asia Pacific (Mumbai) ap-south-1
aws-quicksetup-patchpolicy-789576624500-nlutc
Asia Pacific (Mumbai) ap-south-1
aws-quicksetup-patchpolicy-access-log-789576624500-nlutc
Asia Pacific (Mumbai) ap-south-1
replicabucketttt
EU (London) eu-west-2
websitetb
Asia Pacific (Mumbai) ap-south-1
Feedback
Looking for language selection? Find it in the new Unified Settings
© 2023, Amazon Web Services India Private Limited or its affiliates.
Privacy
Terms
Cookie preferences
Type here to search
PragmaEdge
26°C Sunny
ENG
11:19
03-02-2023

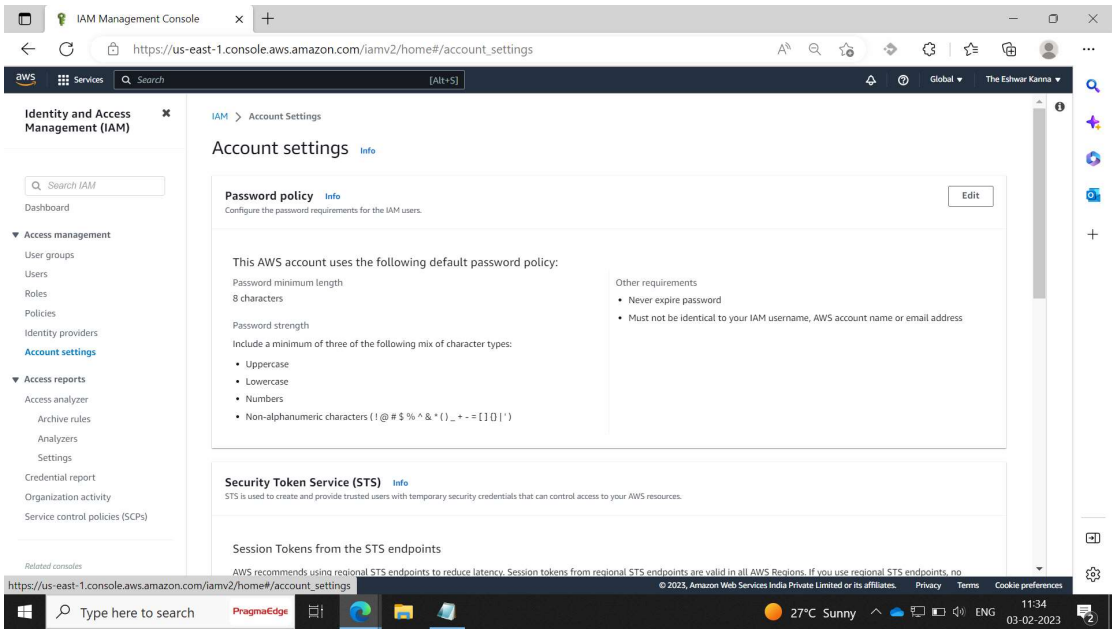

IAM Management Console
https://us-east-1.console.aws.amazon.com/iamv2/home#/users/details/readonly?section=permissions
Identity and Access Management (IAM)
1 policy added
Summary
ARN
arn:aws:iam::789576624500:user/readonly
Console access
Enabled without MFA
Access key 1
Not enabled
Created
February 03, 2023, 10:54 (UTC+05:30)
Last console sign-in
Today
Access key 2
Not enabled
Permissions
Groups
Tags
Security credentials
Access Advisor
Permissions policies (2)
Permissions are defined by policies attached to the user directly or through groups.
Remove
Add permissions
Find policies
Policy name
Type
Attached via
IAMUserChangePassword
AWS managed
Directly
mys3listpolicy
Customer managed
Directly
Permissions boundary (not set)
Set a permissions boundary to control the maximum permissions for this user. Use this advanced feature used to delegate permission management to others. Learn more
Feedback
Language
© 2023, Amazon Web Services India Private Limited or its affiliates.
Privacy
Terms
Cookie preferences
Type here to search
26°C Sunny
ENG
11:20
03-02-2023

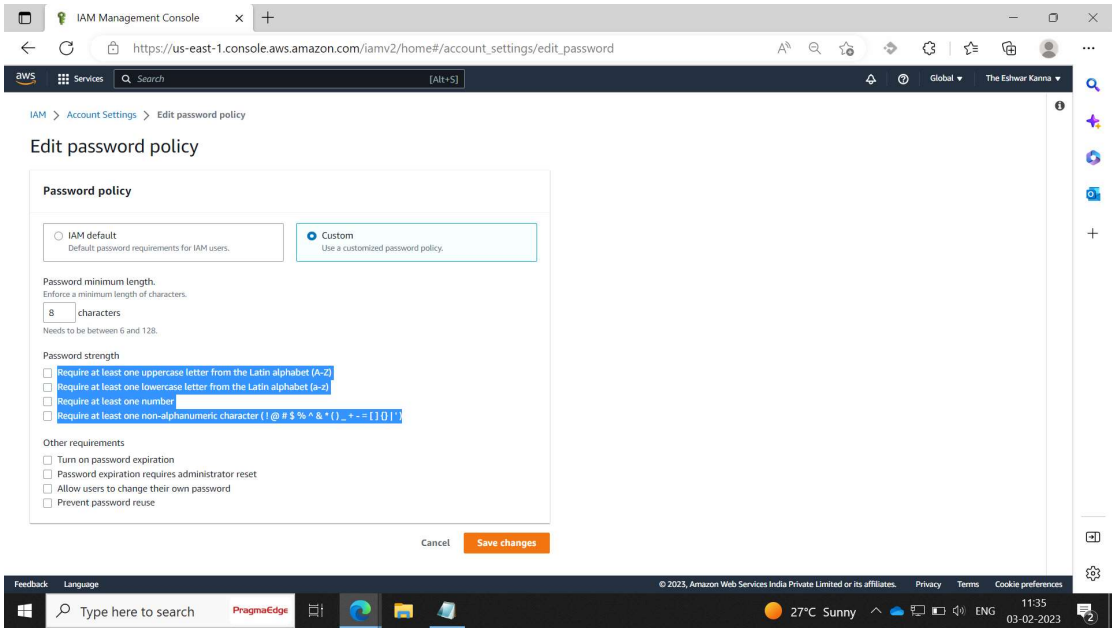

IAM Management Console
https://us-east-1.console.aws.amazon.com/iam/home#/policies/arn:aws:iam::789576624500:policy/mys3listpolicy$edi...
Edit mys3listpolicy
A policy defines the AWS permissions that you can assign to a user, group, or role. You can create and edit a policy in the visual editor and using JSON. Learn more
Visual editor
JSON
Import managed policy
Expand all | Collapse all
S3 (54 actions) 8 warnings
Clone | Remove
Service S3
Actions
close
Specify the actions allowed in S3
Switch to deny permissions
Filter actions
Manual actions (add actions)
All S3 actions (s3:*)
Access level
Expand all | Collapse all
List (1 selected)
Read (53 selected)
Tagging
Write
Permissions management
Resources
Specify accesspoint resource ARN for the GetAccessPointPolicy and 1 more action.
Character count: 39 of 6,144.
Cancel
Review policy
Documentation
Feedback
Language
© 2023, Amazon Web Services India Private Limited or its affiliates.
Privacy
Terms
Cookie preferences
Type here to search
26°C Sunny
ENG
11:26
03-02-2023

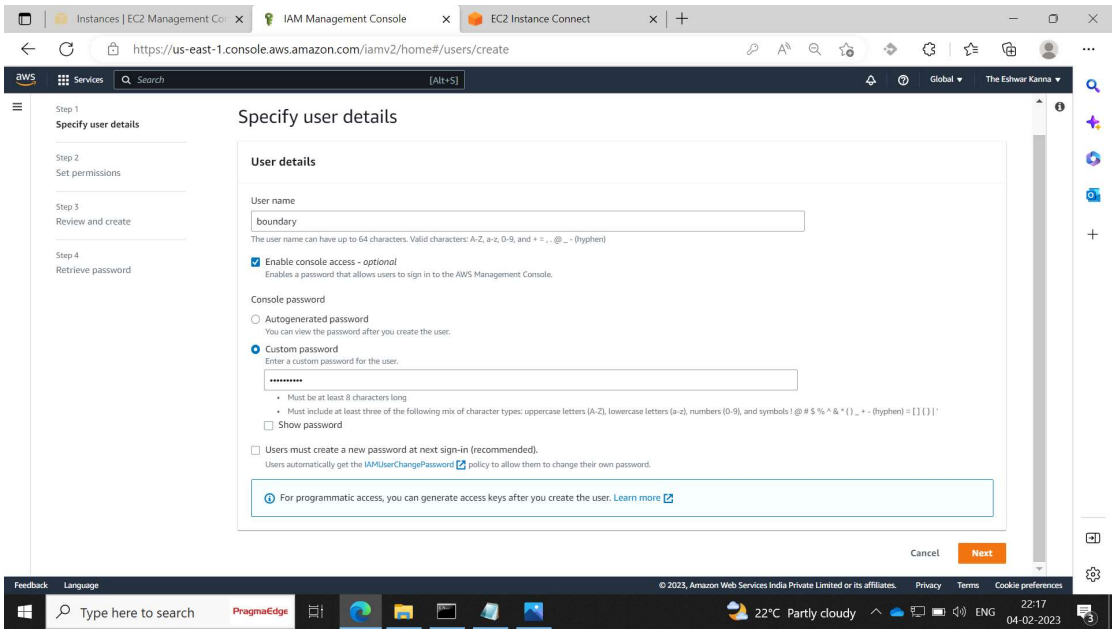

IAM Management Console
https://us-east-1.console.aws.amazon.com/iam/home#/policies/arn:aws:iam::789576624500:policy/mys3listpo...
Identity and Access Management (IAM)
Policies > mys3listpolicy
Summary
Delete policy
Policy ARN
arn:aws:iam::789576624500:policy/mys3listpolicy
Description
Permissions
Policy usage
Tags
Policy versions
Access Advisor
Each time you update a policy, you create a new version. You can have up to 5 versions. Learn more
Set as default
Delete
Version
Creation time
Version 2 (Default)
2023-02-03 11:25 UTC+0530
Version 1
2023-02-03 11:17 UTC+0530
Dashboard
Access management
User groups
Users
Roles
Policies
Identity providers
Account settings
Access reports
Access analyzer
Archive rules
Analyzers
Settings
Credential report
Organization activity
Service control policies (SCPs)
Search IAM
AWS account ID:
Feedback
Language
© 2023, Amazon Web Services India Private Limited or its affiliates.
Privacy
Terms
Cookie preferences
Type here to search
27°C Sunny
ENG
11:27
03-02-2023

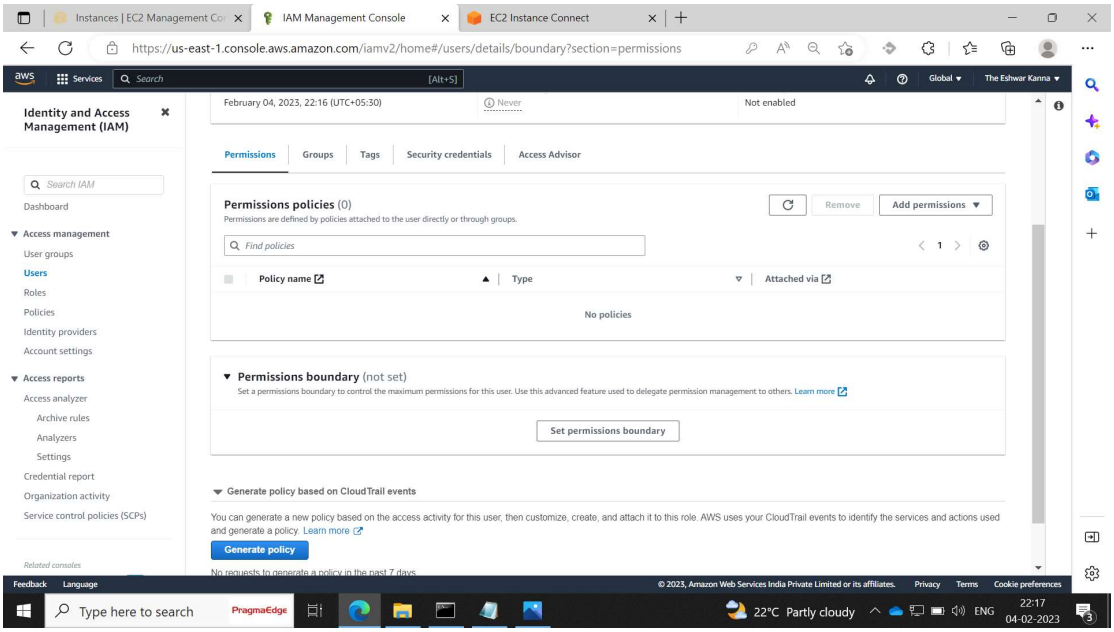

IAM Management Console
https://us-east-1.console.aws.amazon.com/iamv2/home#/users/details/testuser?section=permissions
Identity and Access Management (IAM)
IAM > Users > testuser
testuser
Delete
Summary
ARN
arn:aws:iam::789576624500:user/testuser
Console access
Enabled without MFA
Access key 1
Not enabled
Created
February 03, 2023, 10:44 (UTC+05:30)
Last console sign-in
Today
Access key 2
Not enabled
Permissions
Groups
Tags
Security credentials
Access Advisor
Permissions policies (1)
Permissions are defined by policies attached to the user directly or through groups.
Remove
Add permissions
Add permissions
Add inline policy
Find policies
Policy name
Type
Attached via
IAMUserChangePassword
AWS managed
Directly
Permissions boundary (not set)
Set a permissions boundary to control the maximum permissions for this user. Use this advanced feature used to delegate permission management to others. Learn more
https://us-east-1.console.aws.amazon.com/iam/home#/users/testuser$createPolicy?step=edit
© 2023, Amazon Web Services India Private Limited or its affiliates.
Privacy
Terms
Cookie preferences
Type here to search
27°C Sunny
ENG
11:33
03-02-2023

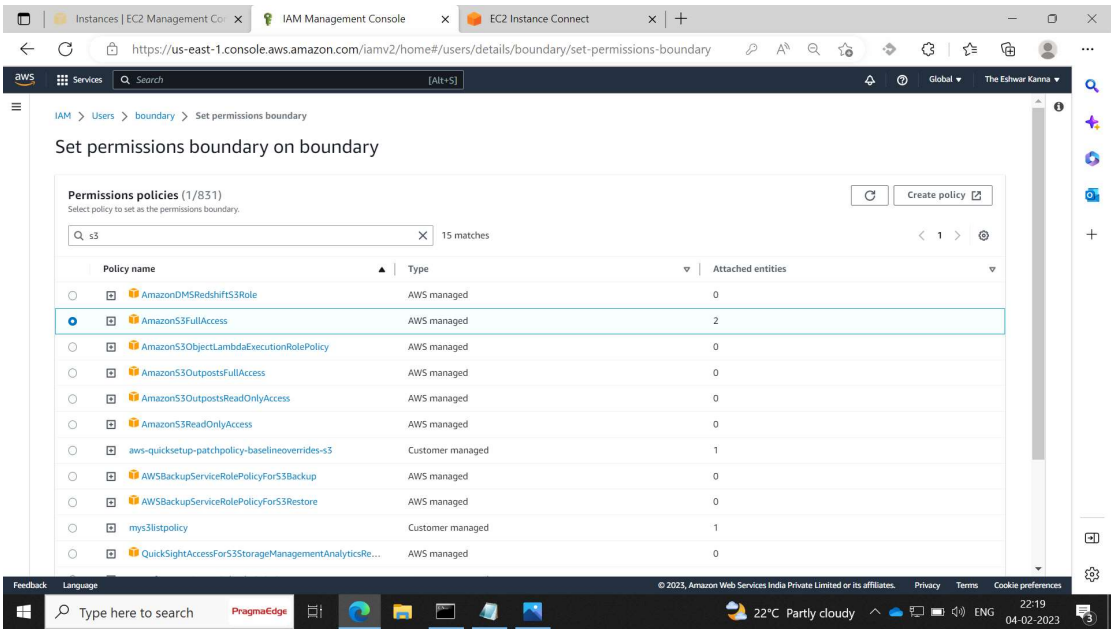

IAM Management Console
https://us-east-1.console.aws.amazon.com/iam/home#/users/testuser$createPolicy?step=edit
Create policy
A policy defines the AWS permissions that you can assign to a user, group, or role. You can create and edit a policy in the visual editor and using JSON. Learn more
Visual editor
JSON
Import managed policy
Expand all | Collapse all
Select a service
Clone | Remove
Service
Choose a service
Actions
Choose a service before defining actions
Resources
Choose actions before applying resources
Request conditions
Choose actions before specifying conditions
Add additional permissions
Character count: 39 of 2,048.
The current character count includes character for all inline policies in the user: testuser.
Cancel
Review policy
Documentation
Feedback
Language
© 2023, Amazon Web Services India Private Limited or its affiliates.
Privacy
Terms
Cookie preferences
Type here to search
27°C Sunny
ENG
11:34
03-02-2023

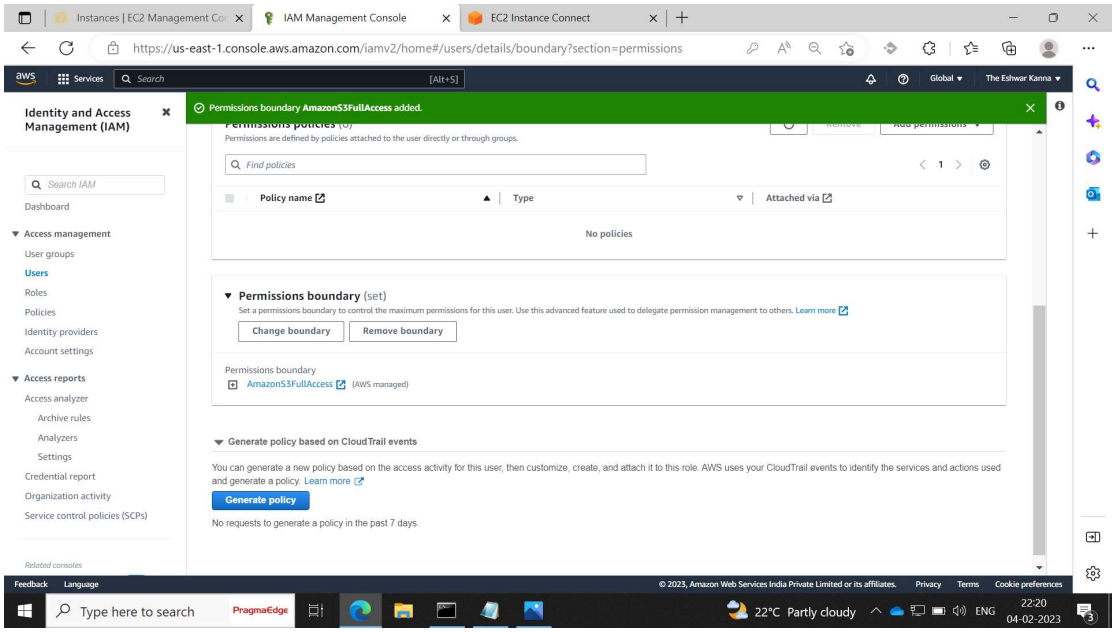

IAM Management Console
https://us-east-1.console.aws.amazon.com/iamv2/home#/account_settings
Identity and Access Management (IAM)
IAM > Account Settings
Account settings
Info
Search IAM
Dashboard
Access management
User groups
Users
Roles
Policies
Identity providers
Account settings
Access reports
Access analyzer
Archive rules
Analyzers
Settings
Credential report
Organization activity
Service control policies (SCPs)
Password policy
Info
Configure the password requirements for the IAM users.
Edit
This AWS account uses the following default password policy:
Password minimum length
8 characters
Password strength
Include a minimum of three of the following mix of character types:
Uppercase
Lowercase
Numbers
Non-alphanumeric characters (! @ # $ % ^ & * ( ) _ + - = [ ] {} | ')
Other requirements
Never expire password
Must not be identical to your IAM username, AWS account name or email address
Security Token Service (STS)
Info
STS is used to create and provide trusted users with temporary security credentials that can control access to your AWS resources.
Session Tokens from the STS endpoints
https://us-east-1.console.aws.amazon.com/iamv2/home#/account_settings
© 2023, Amazon Web Services India Private Limited or its affiliates.
Privacy
Terms
Cookie preferences
Type here to search
27°C Sunny
ENG
11:34
03-02-2023

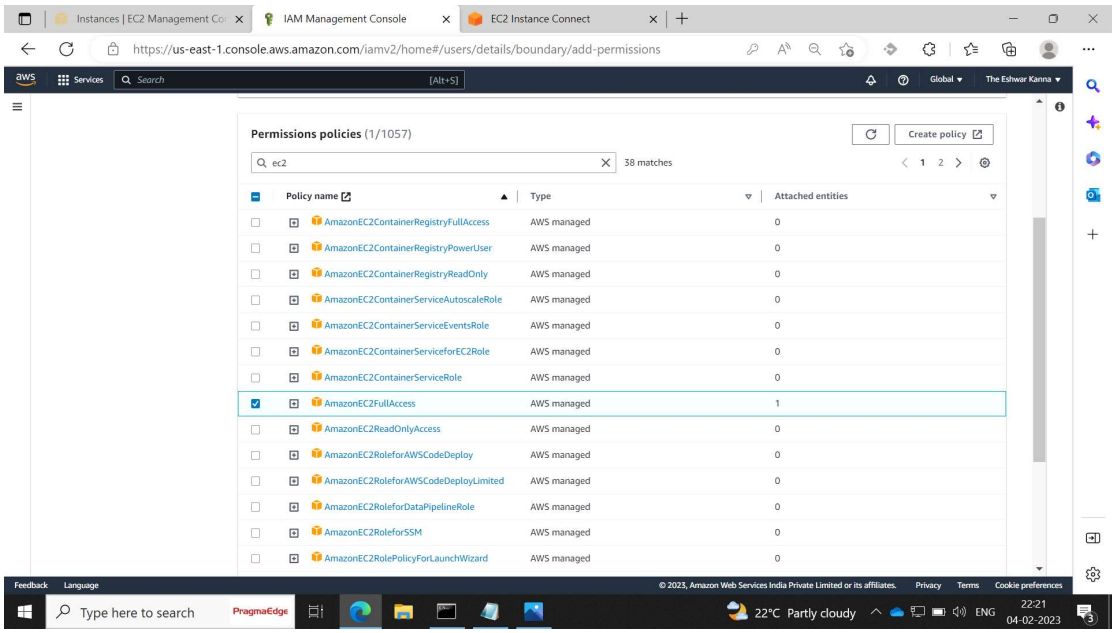

IAM Management Console
https://us-east-1.console.aws.amazon.com/iamv2/home#/account_settings/edit_password
Services
Search
[Alt+S]
Global
The Eshwar Kanna
IAM > Account Settings > Edit password policy
Edit password policy
Password policy
IAM default
Default password requirements for IAM users.
Custom
Use a customized password policy.
Password minimum length.
Enforce a minimum length of characters.
8
characters
Needs to be between 6 and 128.
Password strength
Require at least one uppercase letter from the Latin alphabet (A-Z)
Require at least one lowercase letter from the Latin alphabet (a-z)
Require at least one number
Require at least one non-alphanumeric character (! @ # $ % ^ & * ( ) _ + - = [ ] { } | ')
Other requirements
Turn on password expiration
Password expiration requires administrator reset
Allow users to change their own password
Prevent password reuse
Cancel
Save changes
Feedback
Language
© 2023, Amazon Web Services India Private Limited or its affiliates.
Privacy
Terms
Cookie preferences
Type here to search
PragmaEdge
27°C Sunny
ENG
11:35
03-02-2023

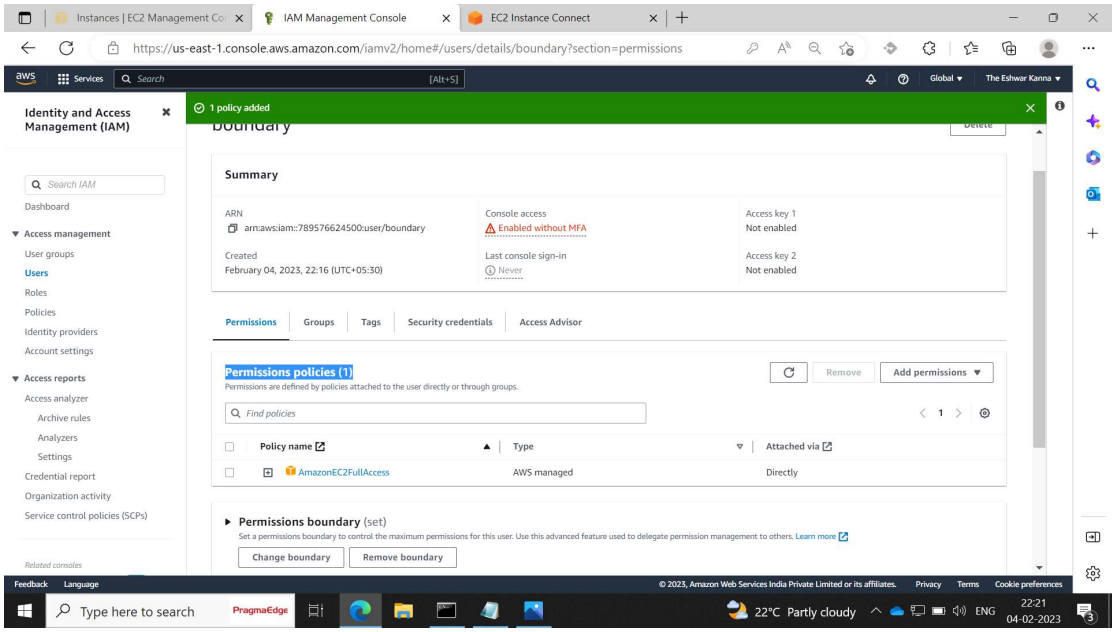

Instances | EC2 Management Co
IAM Management Console
EC2 Instance Connect
https://us-east-1.console.aws.amazon.com/iamv2/home#/users/create
Services
Search
[Alt+S]
Global
The Eshwar Kanna
Step 1
Specify user details
Step 2
Set permissions
Step 3
Review and create
Step 4
Retrieve password
Specify user details
User details
User name
boundary
The user name can have up to 64 characters. Valid characters: A-Z, a-z, 0-9, and + = , . @ _ - (hyphen)
Enable console access - optional
Enables a password that allows users to sign in to the AWS Management Console.
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.
For programmatic access, you can generate access keys after you create the user. Learn more
Cancel
Next
Feedback
Language
© 2023, Amazon Web Services India Private Limited or its affiliates.
Privacy
Terms
Cookie preferences
Type here to search
PragmaEdge
22°C Partly cloudy
ENG
22:17
04-02-2023

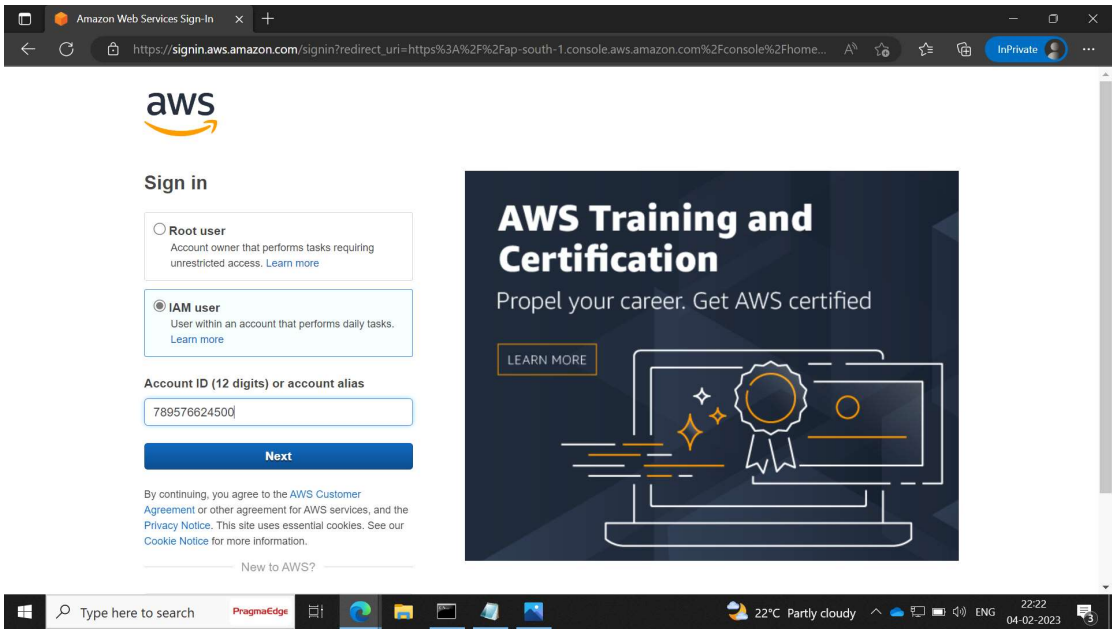

Instances | EC2 Management Co
IAM Management Console
EC2 Instance Connect
https://us-east-1.console.aws.amazon.com/iamv2/home#/users/details/boundary?section=permissions
Identity and Access Management (IAM)
Dashboard
Access management
User groups
Users
Roles
Policies
Identity providers
Account settings
Access reports
Access analyzer
Archive rules
Analyzers
Settings
Credential report
Organization activity
Service control policies (SCPs)
February 04, 2023, 22:16 (UTC+05:30)
Never
Not enabled
Permissions
Groups
Tags
Security credentials
Access Advisor
Permissions policies (0)
Permissions are defined by policies attached to the user directly or through groups.
Remove
Add permissions
Find policies
Policy name
Type
Attached via
No policies
Permissions boundary (not set)
Set a permissions boundary to control the maximum permissions for this user. Use this advanced feature used to delegate permission management to others. Learn more
Set permissions boundary
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.
Feedback
Language
© 2023, Amazon Web Services India Private Limited or its affiliates.
Privacy
Terms
Cookie preferences
Type here to search
22°C Partly cloudy
ENG
22:17
04-02-2023

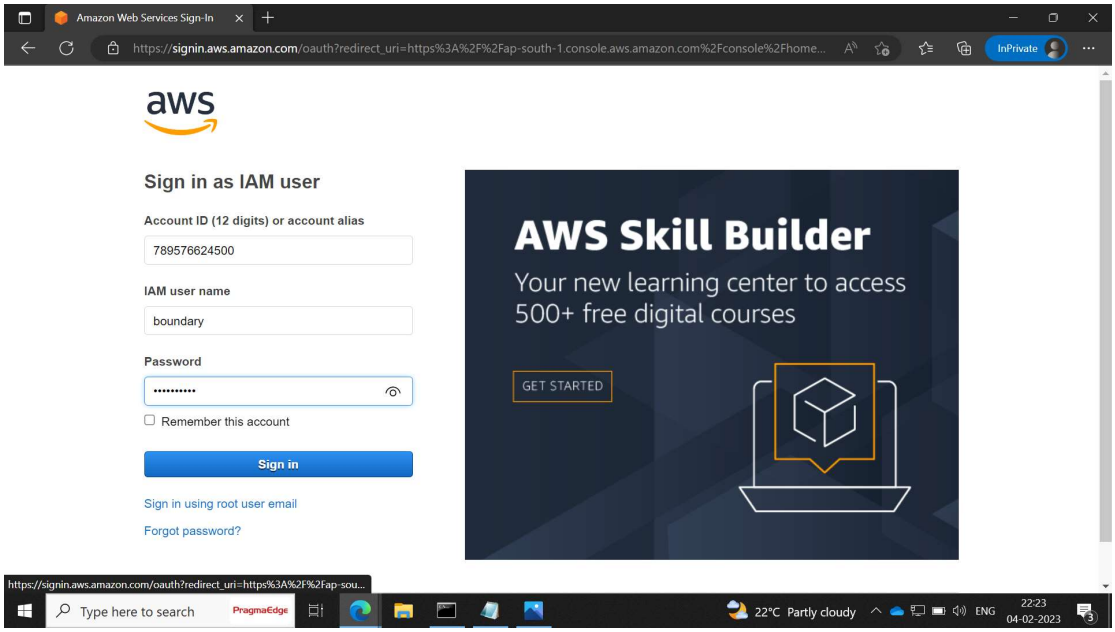

Instances | EC2 Management Co
IAM Management Console
EC2 Instance Connect
https://us-east-1.console.aws.amazon.com/iamv2/home#/users/details/boundary/set-permissions-boundary
IAM > Users > boundary > Set permissions boundary
Set permissions boundary on boundary
Permissions policies (1/831)
Select policy to set as the permissions boundary.
Create policy
s3
15 matches
Policy name
Type
Attached entities
AmazonDMSRedshiftS3Role AWS managed 0
AmazonS3FullAccess AWS managed 2
AmazonS3ObjectLambdaExecutionRolePolicy AWS managed 0
AmazonS3OutpostsFullAccess AWS managed 0
AmazonS3OutpostsReadOnlyAccess AWS managed 0
AmazonS3ReadOnlyAccess AWS managed 0
aws-quicksetup-patchpolicy-baselineoverrides-s3 Customer managed 1
AWSBackupServiceRolePolicyForS3Backup AWS managed 0
AWSBackupServiceRolePolicyForS3Restore AWS managed 0
mys3listpolicy Customer managed 1
QuickSightAccessForS3StorageManagementAnalyticsRe... AWS managed 0
Feedback
Language
© 2023, Amazon Web Services India Private Limited or its affiliates.
Privacy
Terms
Cookie preferences
Type here to search
22°C Partly cloudy
ENG
22:19
04-02-2023

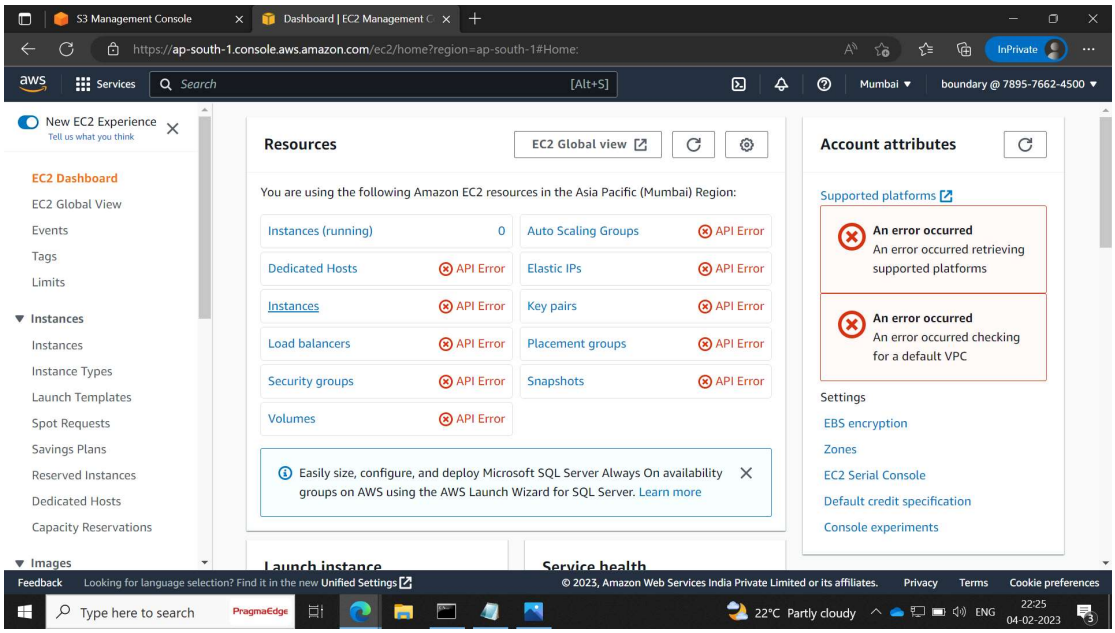

Instances | EC2 Management Co
IAM Management Console
EC2 Instance Connect
https://us-east-1.console.aws.amazon.com/iamv2/home#/users/details/boundary?section=permissions
Services
Search
[Alt+S]
Global
The Eshwar Kanna
Identity and Access Management (IAM)
Permissions boundary AmazonS3FullAccess added.
Permissions policies (0)
Permissions are defined by policies attached to the user directly or through groups.
Find policies
Policy name
Type
Attached via
No policies
Permissions boundary (set)
Set a permissions boundary to control the maximum permissions for this user. Use this advanced feature used to delegate permission management to others. Learn more
Change boundary
Remove boundary
Permissions boundary
AmazonS3FullAccess (AWS managed)
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.
Search IAM
Dashboard
Access management
User groups
Users
Roles
Policies
Identity providers
Account settings
Access reports
Access analyzer
Archive rules
Analyzers
Settings
Credential report
Organization activity
Service control policies (SCPs)
Related consoles
Feedback
Language
© 2023, Amazon Web Services India Private Limited or its affiliates.
Privacy
Terms
Cookie preferences
Type here to search
PragmaEdge
22°C Partly cloudy
ENG
22:20
04-02-2023

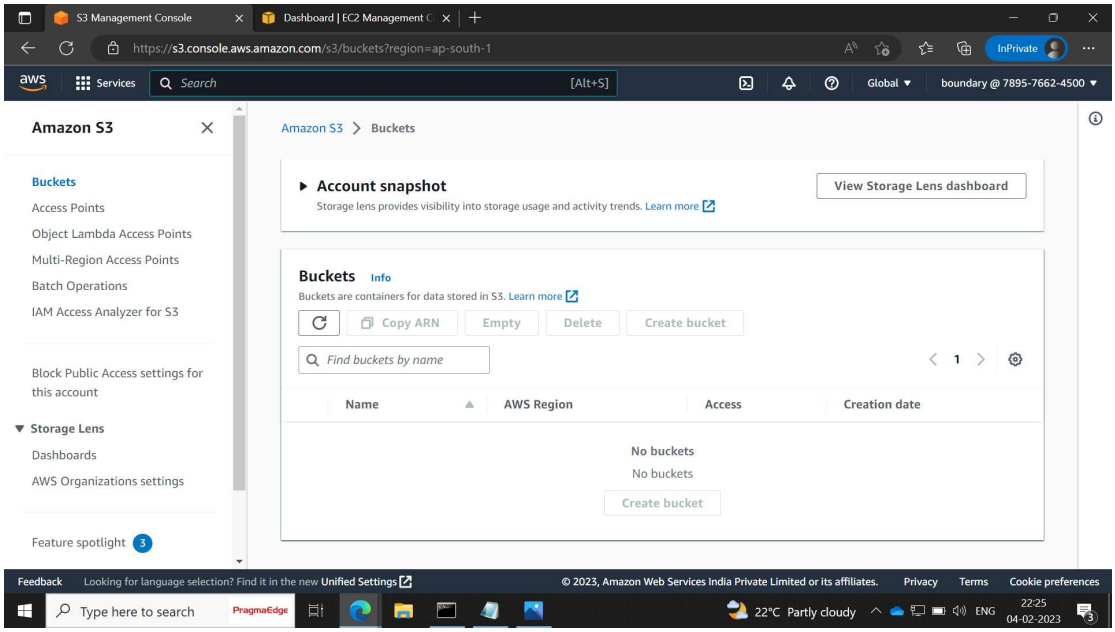

Instances | EC2 Management Co
IAM Management Console
EC2 Instance Connect
https://us-east-1.console.aws.amazon.com/iamv2/home#/users/details/boundary/add-permissions
Services
Search
[Alt+S]
Global
The Eshwar Kanna
Permissions policies (1/1057)
Create policy
ec2
38 matches
Policy name
Type
Attached entities
AmazonEC2ContainerRegistryFullAccess AWS managed 0
AmazonEC2ContainerRegistryPowerUser AWS managed 0
AmazonEC2ContainerRegistryReadOnly AWS managed 0
AmazonEC2ContainerServiceAutoscaleRole AWS managed 0
AmazonEC2ContainerServiceEventsRole AWS managed 0
AmazonEC2ContainerServiceforEC2Role AWS managed 0
AmazonEC2ContainerServiceRole AWS managed 0
AmazonEC2FullAccess AWS managed 1
AmazonEC2ReadOnlyAccess AWS managed 0
AmazonEC2RoleforAWSCodeDeploy AWS managed 0
AmazonEC2RoleforAWSCodeDeployLimited AWS managed 0
AmazonEC2RoleforDataPipelineRole AWS managed 0
AmazonEC2RoleforSSM AWS managed 0
AmazonEC2RolePolicyForLaunchWizard AWS managed 0
Feedback
Language
© 2023, Amazon Web Services India Private Limited or its affiliates.
Privacy
Terms
Cookie preferences
Type here to search
PragmaEdge
22°C Partly cloudy
ENG
22:21
04-02-2023

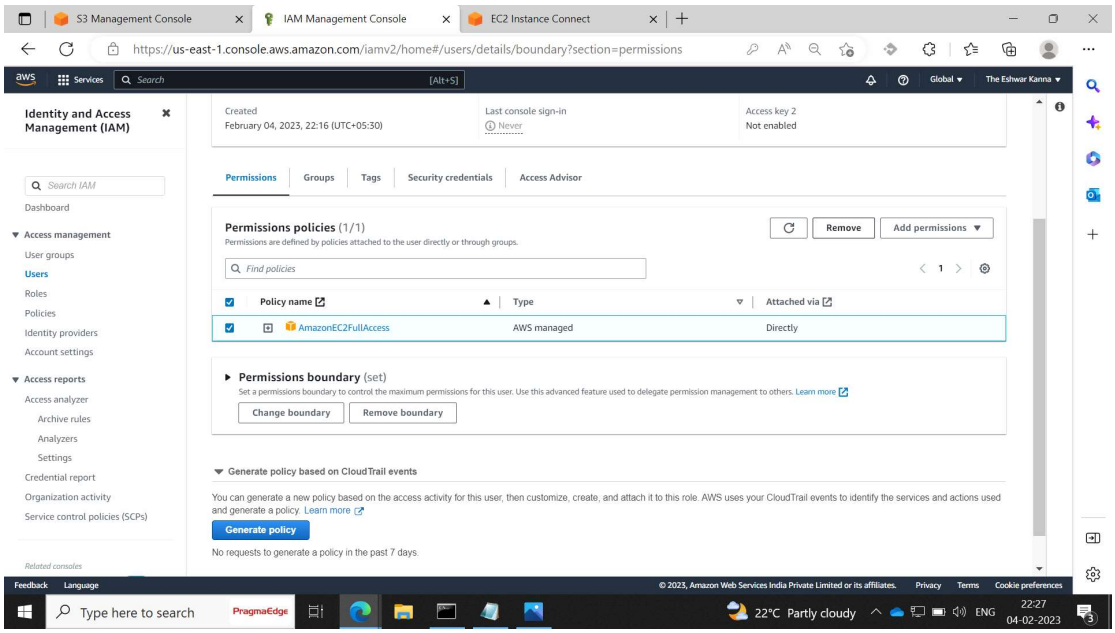

IAM Management Console
EC2 Instance Connect
https://us-east-1.console.aws.amazon.com/iamv2/home#/users/details/boundary?section=permissions
Identity and Access Management (IAM)
1 policy added
Summary
ARN
arn:aws:iam::789576624500:user/boundary
Console access
Enabled without MFA
Access key 1
Not enabled
Created
February 04, 2023, 22:16 (UTC+05:30)
Last console sign-in
Never
Access key 2
Not enabled
Permissions
Groups
Tags
Security credentials
Access Advisor
Permissions policies (1)
Permissions are defined by policies attached to the user directly or through groups.
Remove
Add permissions
Find policies
Policy name
Type
Attached via
AmazonEC2FullAccess
AWS managed
Directly
Permissions boundary (set)
Set a permissions boundary to control the maximum permissions for this user. Use this advanced feature used to delegate permission management to others. Learn more
Change boundary
Remove boundary
Feedback
Language
© 2023, Amazon Web Services India Private Limited or its affiliates.
Privacy
Terms
Cookie preferences
Type here to search
22°C Partly cloudy
ENG
22:21
04-02-2023

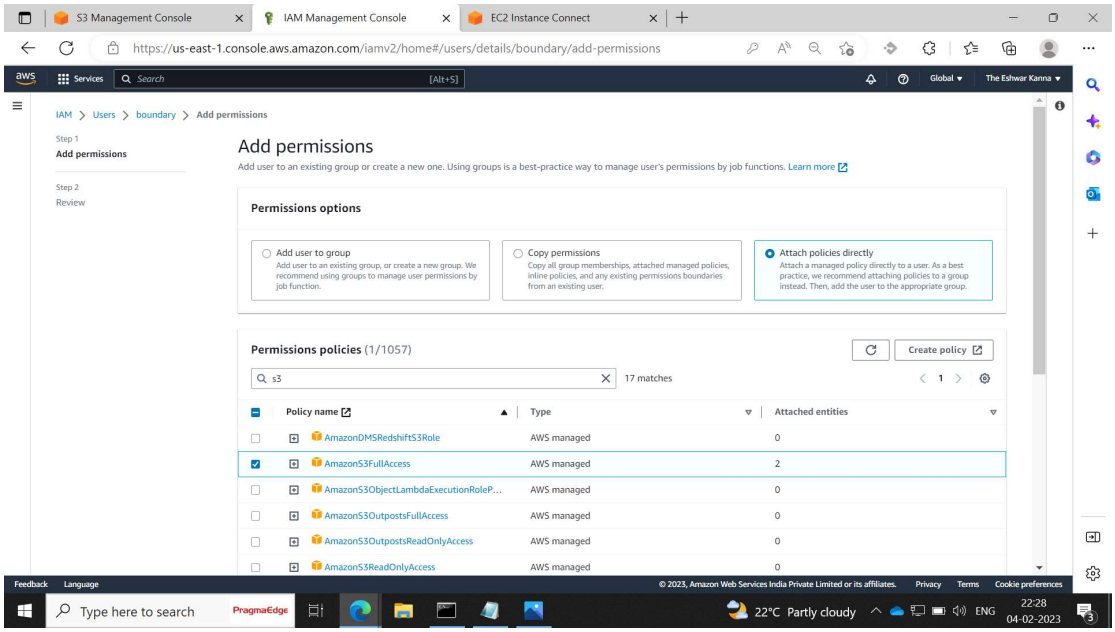

Amazon Web Services Sign-In
https://signin.aws.amazon.com/signin?redirect_uri=https%3A%2F%2Fap-south-1.console.aws.amazon.com%2Fconsole%2Fhome...
InPrivate
aws
Sign in
Root user
Account owner that performs tasks requiring unrestricted access. Learn more
IAM user
User within an account that performs daily tasks.
Learn more
Account ID (12 digits) or account alias
789576624500
Next
By continuing, you agree to the 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.
New to AWS?
AWS Training and Certification
Propel your career. Get AWS certified
LEARN MORE
Type here to search
22°C Partly cloudy
ENG
22:22
04-02-2023

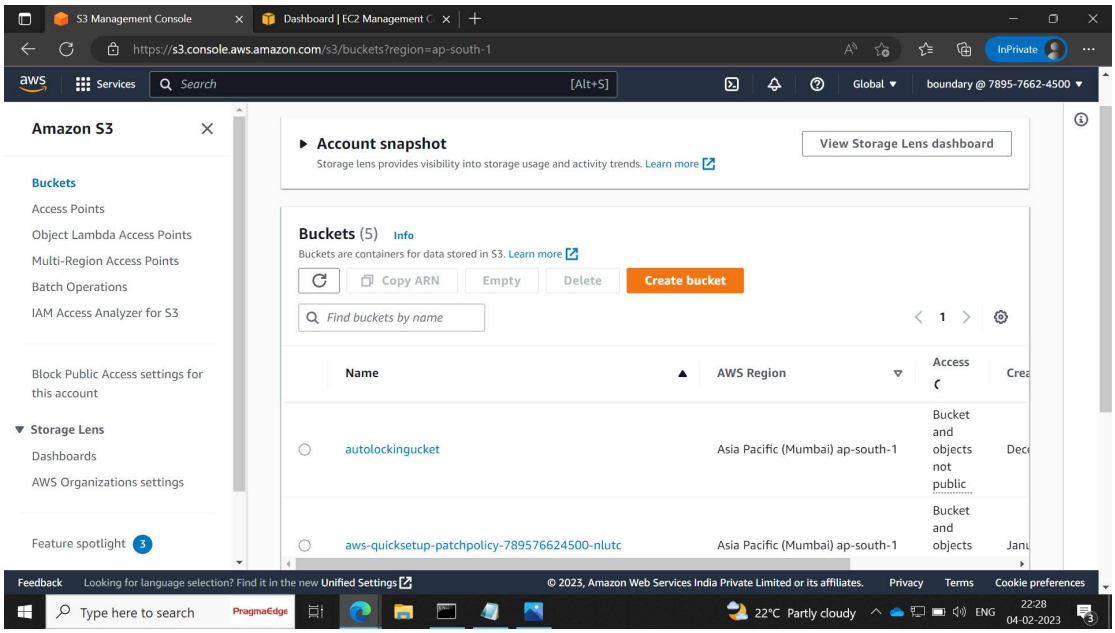

Amazon Web Services Sign-In
https://signin.aws.amazon.com/oauth?redirect_uri=https%3A%2F%2Fap-south-1.console.aws.amazon.com%2Fconsole%2Fhome...
InPrivate
aws
Sign in as IAM user
Account ID (12 digits) or account alias
789576624500
IAM user name
boundary
Password
Remember this account
Sign in
Sign in using root user email
Forgot password?
AWS Skill Builder
Your new learning center to access 500+ free digital courses
GET STARTED
https://signin.aws.amazon.com/oauth?redirect_uri=https%3A%2F%2Fap-sou...
Type here to search
PragmaEdge
22°C Partly cloudy
ENG
22:23
04-02-2023

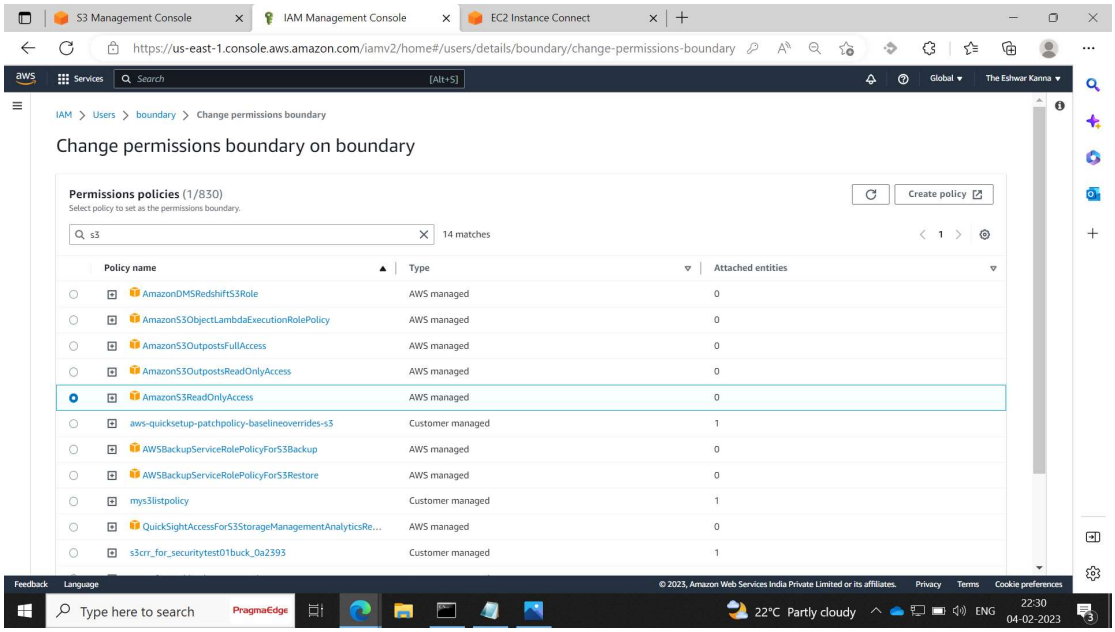

S3 Management Console
Dashboard | EC2 Management
https://ap-south-1.console.aws.amazon.com/ec2/home?region=ap-south-1#Home:
InPrivate
Services
Search
[Alt+S]
Mumbai
boundary @ 7895-7662-4500
New EC2 Experience
Tell us what you think
EC2 Dashboard
EC2 Global View
Events
Tags
Limits
Instances
Instances
Instance Types
Launch Templates
Spot Requests
Savings Plans
Reserved Instances
Dedicated Hosts
Capacity Reservations
Images
Resources
EC2 Global view
You are using the following Amazon EC2 resources in the Asia Pacific (Mumbai) Region:
Instances (running) 0
Auto Scaling Groups API Error
Dedicated Hosts API Error
Elastic IPs API Error
Instances API Error
Key pairs API Error
Load balancers API Error
Placement groups API Error
Security groups API Error
Snapshots API Error
Volumes API Error
Easily size, configure, and deploy Microsoft SQL Server Always On availability groups on AWS using the AWS Launch Wizard for SQL Server. Learn more
Account attributes
Supported platforms
An error occurred
An error occurred retrieving supported platforms
An error occurred
An error occurred checking for a default VPC
Settings
EBS encryption
Zones
EC2 Serial Console
Default credit specification
Console experiments
Launch instance
Service health
Feedback
Looking for language selection? Find it in the new Unified Settings
© 2023, Amazon Web Services India Private Limited or its affiliates.
Privacy
Terms
Cookie preferences
Type here to search
PragmaEdge
22°C Partly cloudy
ENG
22:25
04-02-2023

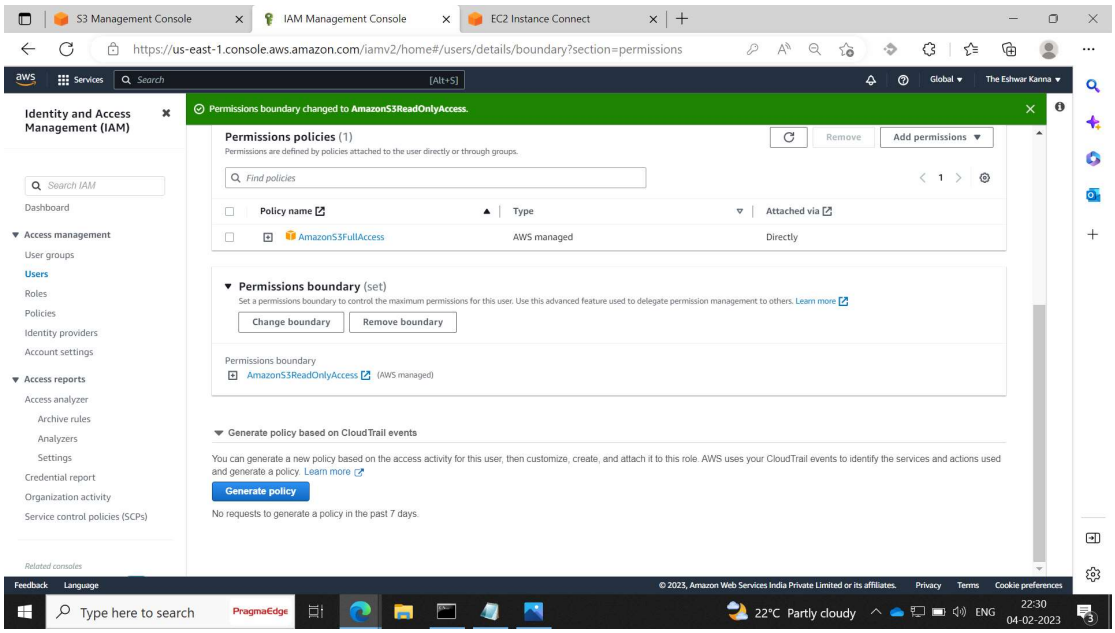

S3 Management Console
Dashboard | EC2 Management
https://s3.console.aws.amazon.com/s3/buckets?region=ap-south-1
Services
Search
[Alt+S]
Global
boundary @ 7895-7662-4500
Amazon S3
Buckets
Access Points
Object Lambda Access Points
Multi-Region Access Points
Batch Operations
IAM Access Analyzer for S3
Block Public Access settings for this account
Storage Lens
Dashboards
AWS Organizations settings
Feature spotlight
Amazon S3 > Buckets
Account snapshot
Storage lens provides visibility into storage usage and activity trends. Learn more
View Storage Lens dashboard
Buckets Info
Buckets are containers for data stored in S3. Learn more
Copy ARN
Empty
Delete
Create bucket
Find buckets by name
Name
AWS Region
Access
Creation date
No buckets
No buckets
Create bucket
Feedback
Looking for language selection? Find it in the new Unified Settings
© 2023, Amazon Web Services India Private Limited or its affiliates.
Privacy
Terms
Cookie preferences
Type here to search
22°C Partly cloudy
ENG
22:25
04-02-2023

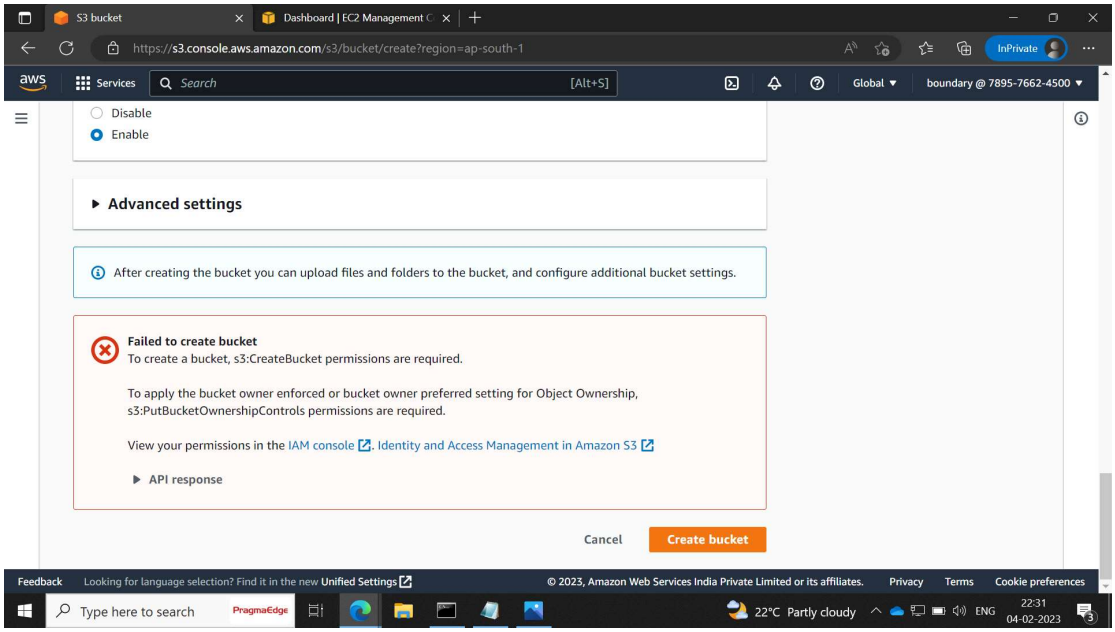

S3 Management Console
IAM Management Console
EC2 Instance Connect
https://us-east-1.console.aws.amazon.com/iamv2/home#/users/details/boundary?section=permissions
Identity and Access Management (IAM)
Search IAM
Dashboard
Access management
User groups
Users
Roles
Policies
Identity providers
Account settings
Access reports
Access analyzer
Archive rules
Analyzers
Settings
Credential report
Organization activity
Service control policies (SCPs)
Created
February 04, 2023, 22:16 (UTC+05:30)
Last console sign-in
Never
Access key 2
Not enabled
Permissions
Groups
Tags
Security credentials
Access Advisor
Permissions policies (1/1)
Permissions are defined by policies attached to the user directly or through groups.
Remove
Add permissions
Find policies
Policy name
Type
Attached via
AmazonEC2FullAccess
AWS managed
Directly
Permissions boundary (set)
Set a permissions boundary to control the maximum permissions for this user. Use this advanced feature used to delegate permission management to others. Learn more
Change boundary
Remove boundary
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.
Feedback
Language
© 2023, Amazon Web Services India Private Limited or its affiliates.
Privacy
Terms
Cookie preferences
Type here to search
22°C Partly cloudy
ENG
22:27
04-02-2023


S3 Management Console
IAM Management Console
EC2 Instance Connect
https://us-east-1.console.aws.amazon.com/iamv2/home#/users/details/boundary/add-permissions
IAM > Users > boundary > 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 (1/1057)
Create policy
s3
17 matches
Policy name
Type
Attached entities
AmazonDMSRedshiftS3Role
AmazonS3FullAccess
AmazonS3ObjectLambdaExecutionRoleP...
AmazonS3OutpostsFullAccess
AmazonS3OutpostsReadOnlyAccess
AmazonS3ReadOnlyAccess
AWS managed
Feedback
Language
© 2023, Amazon Web Services India Private Limited or its affiliates.
Privacy
Terms
Cookie preferences
Type here to search
22°C Partly cloudy
ENG
22:28
04-02-2023


S3 Management Console
Dashboard | EC2 Management
https://s3.console.aws.amazon.com/s3/buckets?region=ap-south-1
InPrivate
Services
Search
[Alt+S]
Global
boundary @ 7895-7662-4500
Amazon S3
Buckets
Access Points
Object Lambda Access Points
Multi-Region Access Points
Batch Operations
IAM Access Analyzer for S3
Block Public Access settings for this account
Storage Lens
Dashboards
AWS Organizations settings
Feature spotlight
3
Account snapshot
Storage lens provides visibility into storage usage and activity trends. Learn more
View Storage Lens dashboard
Buckets (5) Info
Buckets are containers for data stored in S3. Learn more
Copy ARN
Empty
Delete
Create bucket
Find buckets by name
Name
AWS Region
Access
autolockingucket
Asia Pacific (Mumbai) ap-south-1
Bucket and objects not public
aws-quicksetup-patchpolicy-789576624500-nlutc
Asia Pacific (Mumbai) ap-south-1
Bucket and objects
Feedback
Looking for language selection? Find it in the new Unified Settings
© 2023, Amazon Web Services India Private Limited or its affiliates.
Privacy
Terms
Cookie preferences
Type here to search
22°C Partly cloudy
ENG
22:28
04-02-2023


S3 Management Console
IAM Management Console
EC2 Instance Connect
https://us-east-1.console.aws.amazon.com/iamv2/home#/users/details/boundary/change-permissions-boundary
Services
Search
[Alt+S]
Global
The Eshwar Kanna
IAM > Users > boundary > Change permissions boundary
Change permissions boundary on boundary
Permissions policies (1/830)
Select policy to set as the permissions boundary.
Create policy
s3
14 matches
Policy name
Type
Attached entities
AmazonDMSRedshiftS3Role
AWS managed
0
AmazonS3ObjectLambdaExecutionRolePolicy
AWS managed
0
AmazonS3OutpostsFullAccess
AWS managed
0
AmazonS3OutpostsReadOnlyAccess
AWS managed
0
AmazonS3ReadOnlyAccess
AWS managed
0
aws-quicksetup-patchpolicy-baselineoverrides-s3
Customer managed
1
AWSBackupServiceRolePolicyForS3Backup
AWS managed
0
AWSBackupServiceRolePolicyForS3Restore
AWS managed
0
mys3listpolicy
Customer managed
1
QuickSightAccessForS3StorageManagementAnalyticsRe...
AWS managed
0
s3crr_for_securitytest01buck_0a2393
Customer managed
1
Feedback
Language
© 2023, Amazon Web Services India Private Limited or its affiliates.
Privacy
Terms
Cookie preferences
Type here to search
PragmaEdge
22°C Partly cloudy
ENG
22:30
04-02-2023


S3 Management Console
IAM Management Console
EC2 Instance Connect
https://us-east-1.console.aws.amazon.com/iamv2/home#/users/details/boundary?section=permissions
Services
Search
[Alt+S]
Global
The Eshwar Kanna
Identity and Access Management (IAM)
Permissions boundary changed to AmazonS3ReadOnlyAccess.
Permissions policies (1)
Permissions are defined by policies attached to the user directly or through groups.
Remove
Add permissions
Find policies
Policy name
Type
Attached via
AmazonS3FullAccess
AWS managed
Directly
Permissions boundary (set)
Set a permissions boundary to control the maximum permissions for this user. Use this advanced feature used to delegate permission management to others. Learn more
Change boundary
Remove boundary
Permissions boundary
AmazonS3ReadOnlyAccess
(AWS managed)
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.
Search IAM
Dashboard
Access management
User groups
Users
Roles
Policies
Identity providers
Account settings
Access reports
Access analyzer
Archive rules
Analyzers
Settings
Credential report
Organization activity
Service control policies (SCPs)
Related consoles
Feedback
Language
© 2023, Amazon Web Services India Private Limited or its affiliates.
Privacy
Terms
Cookie preferences
Type here to search
PragmaEdge
22°C Partly cloudy
ENG
22:30
04-02-2023


S3 bucket
Dashboard | EC2 Management
https://s3.console.aws.amazon.com/s3/bucket/create?region=ap-south-1
InPrivate
aws
Services
Search
[Alt+S]
Global
boundary @ 7895-7662-4500
Disable
Enable
Advanced settings
After creating the bucket you can upload files and folders to the bucket, and configure additional bucket settings.
Failed to create bucket
To create a bucket, s3:CreateBucket permissions are required.
To apply the bucket owner enforced or bucket owner preferred setting for Object Ownership, s3:PutBucketOwnershipControls permissions are required.
View your permissions in the IAM console. Identity and Access Management in Amazon S3
API response
Cancel
Create bucket
Feedback
Looking for language selection? Find it in the new Unified Settings
© 2023, Amazon Web Services India Private Limited or its affiliates.
Privacy
Terms
Cookie preferences
Type here to search
PragmaEdge
22°C Partly cloudy
ENG
22:31
04-02-2023