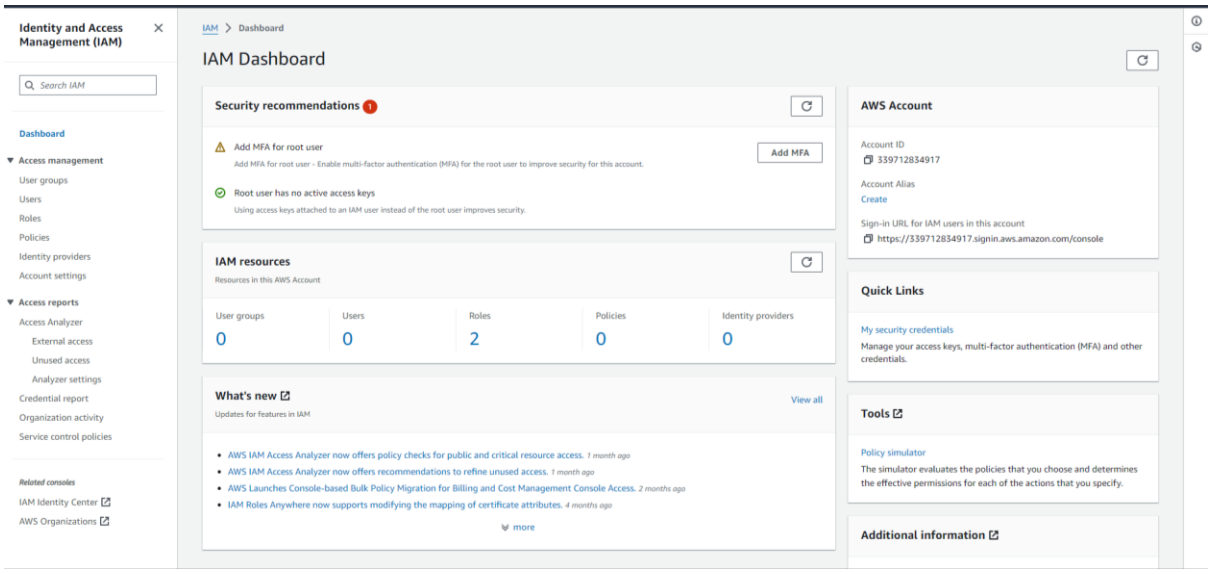
Practical-3

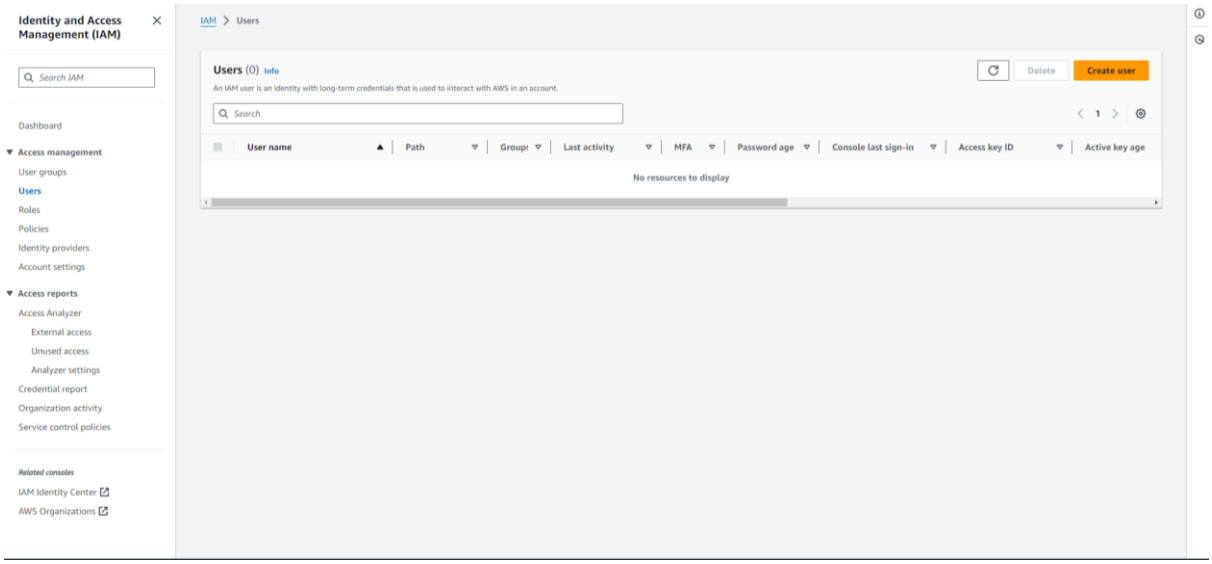
Parisi Jariwala

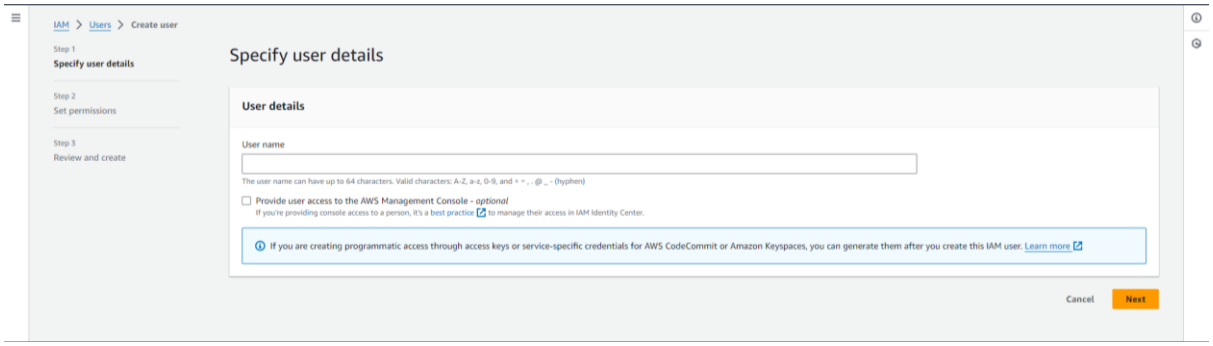
Batch 1

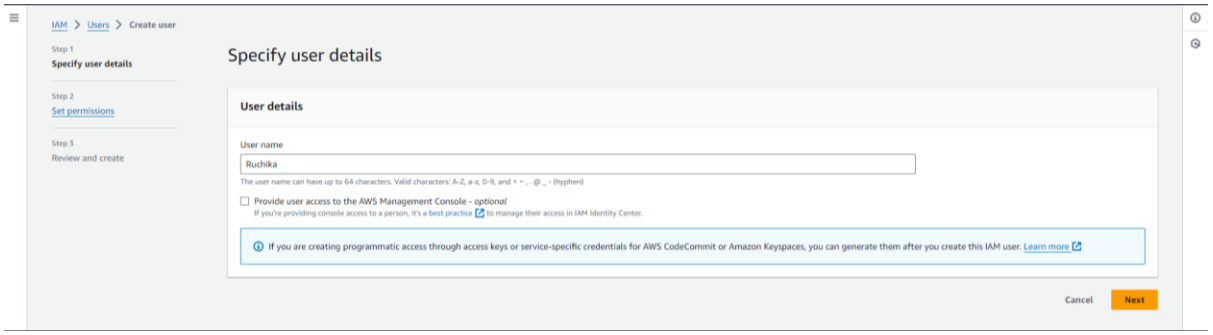
A025

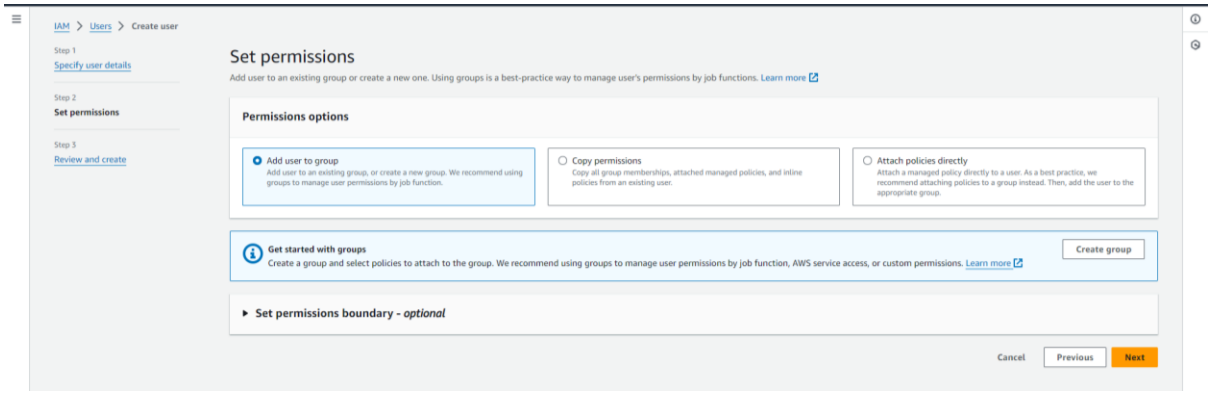
86062300057

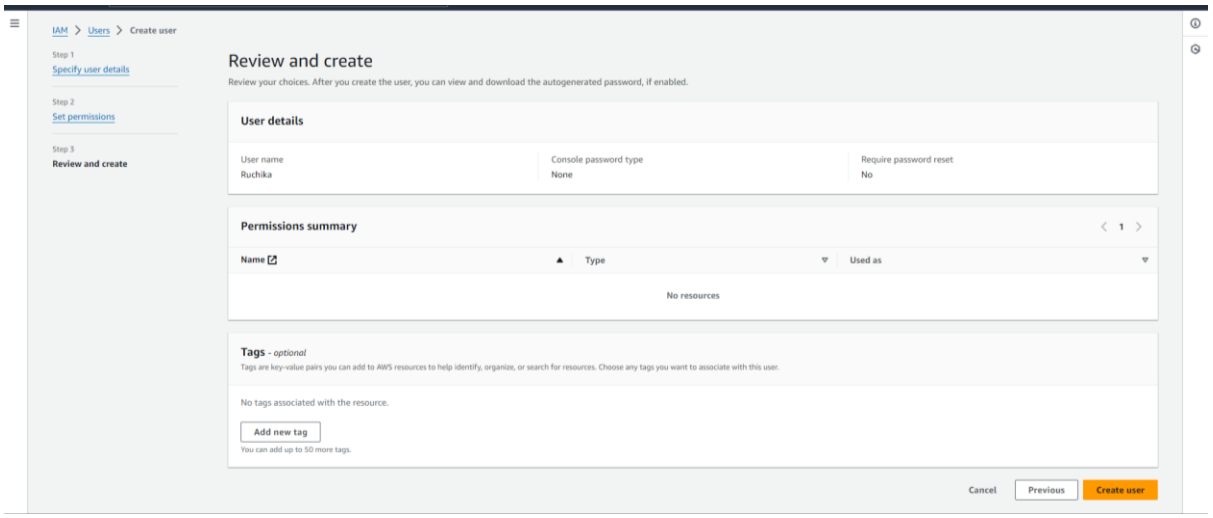


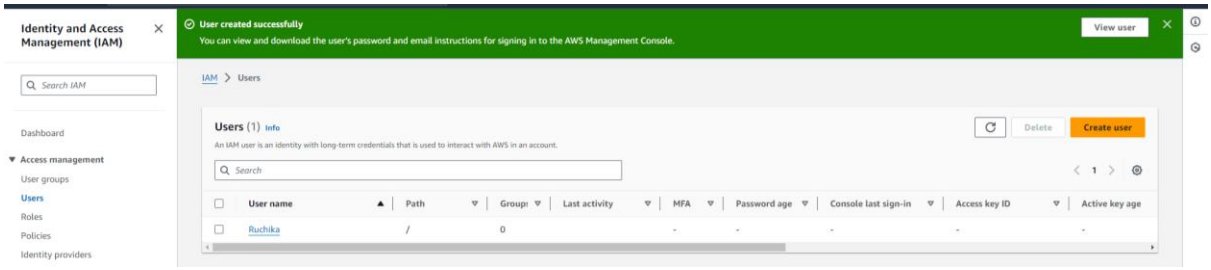


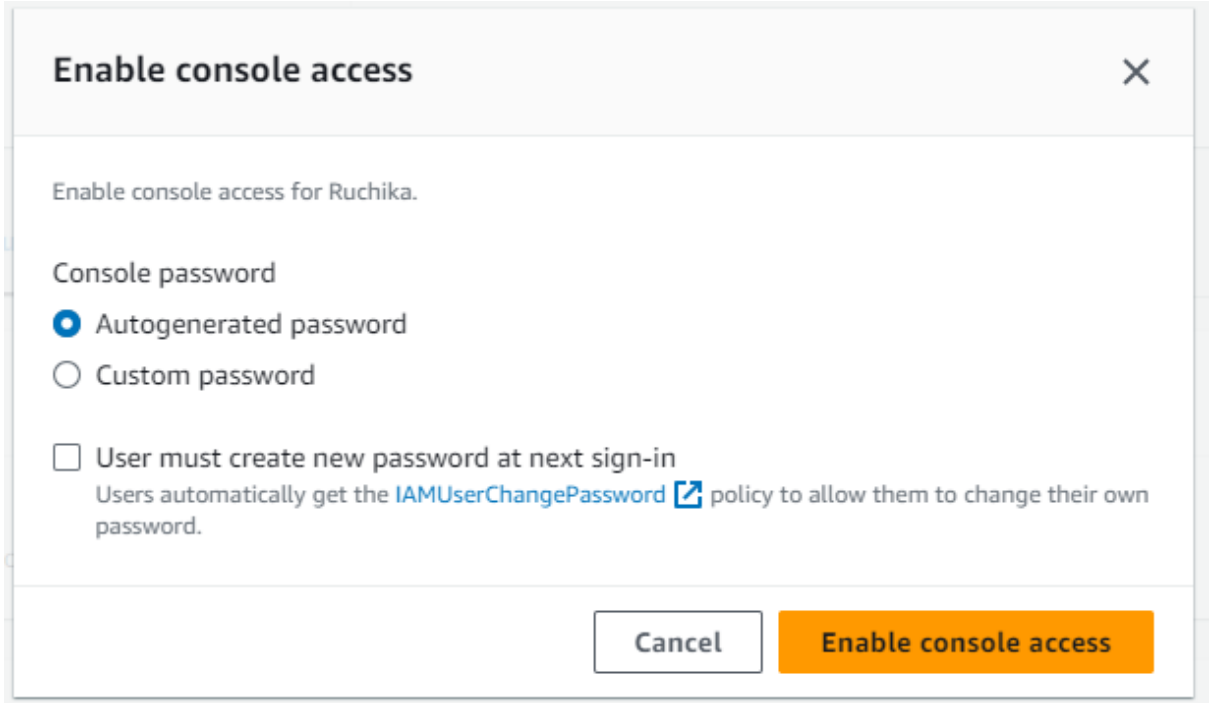

IAM > Users > Create user
Step 1
Specify user details
Step 2
Set permissions
Step 3
Review and create
Specify user details
User details
User name
The user name can have up to 64 characters. Valid characters: A-Z, a-z, 0-9, and + = , . @ _ - (hyphen)
Provide user access to the AWS Management Console - optional
If you're providing console access to a person, it's a best practice to manage their access in IAM Identity Center.
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

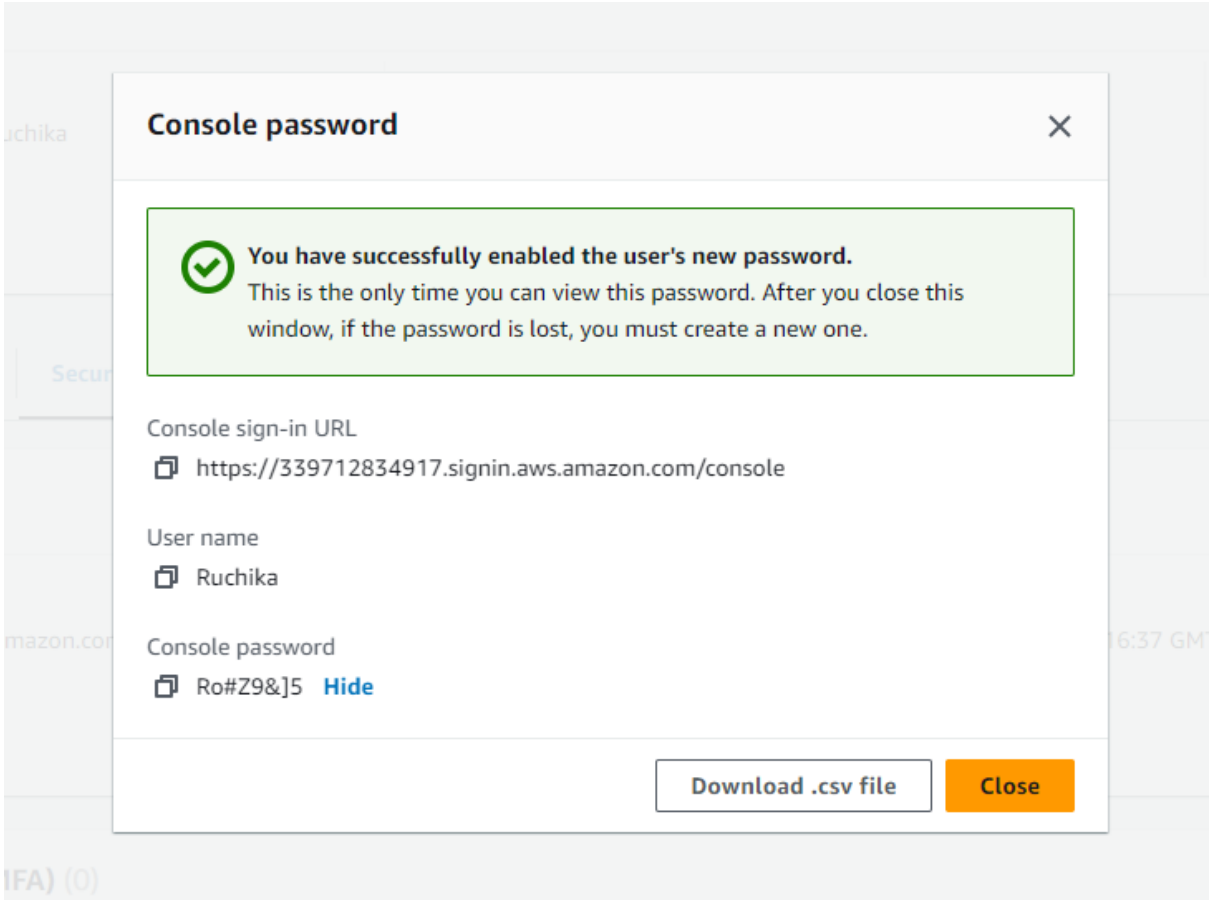

IAM > Users > Create user
Step 1
Specify user details
Step 2
Set permissions
Step 3
Review and create
Specify user details
User details
User name
Ruchika
The user name can have up to 64 characters. Valid characters: A-Z, a-z, 0-9, and + = , . @ _ - (hyphen)
Provide user access to the AWS Management Console - optional
If you're providing console access to a person, it's a best practice to manage their access in IAM Identity Center.
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

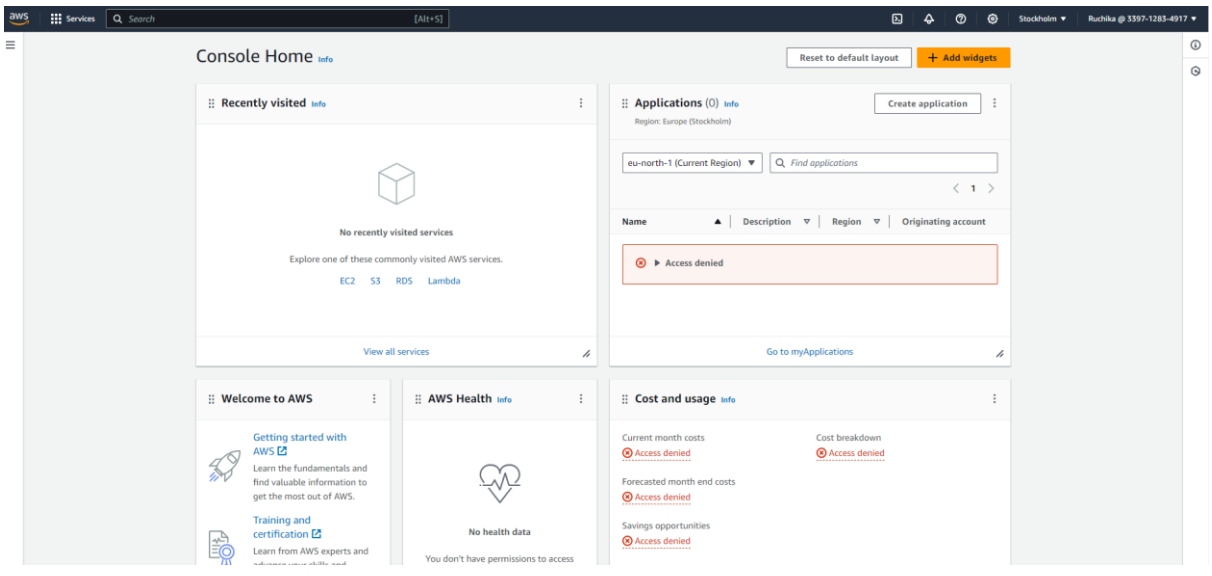

IAM > Users > Create user
Step 1
Specify user details
Step 2
Set permissions
Step 3
Review and create
Set permissions
Add user to an existing group or create a new one. Using groups is a best-practice way to manage user's permissions by job functions. Learn more
Permissions options
Add user to group
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.
Get started with groups
Create a group and select policies to attach to the group. We recommend using groups to manage user permissions by job function, AWS service access, or custom permissions. Learn more
Create group
Set permissions boundary - optional
Cancel
Previous
Next

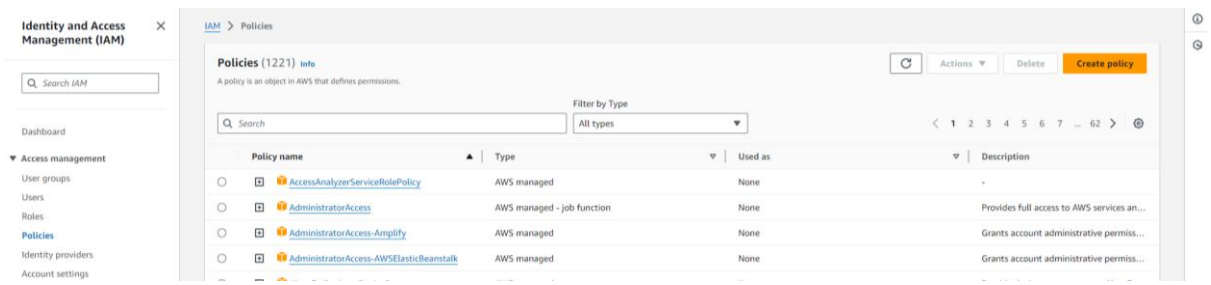

IAM > Users > Create user
Step 1
Specify user details
Step 2
Set permissions
Step 3
Review and create
Review and create
Review your choices. After you create the user, you can view and download the autogenerated password, if enabled.
User details
User name
Ruchika
Console password type
None
Require password reset
No
Permissions summary
Name
Type
Used as
No resources
Tags - optional
Tags are key-value pairs you can add to AWS resources to help identify, organize, or search for resources. Choose any tags you want to associate with this user.
No tags associated with the resource.
Add new tag
You can add up to 50 more tags.
Cancel
Previous
Create user

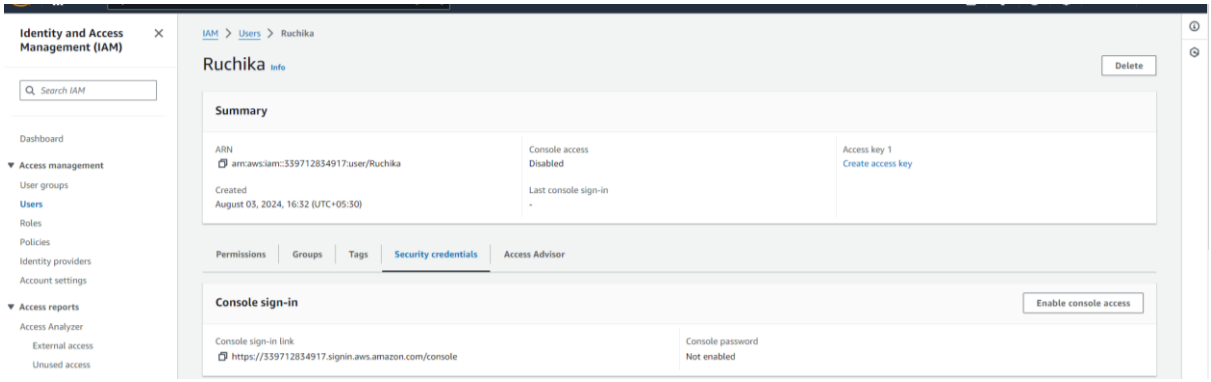

Identity and Access Management (IAM)
User created successfully
You can view and download the user's password and email instructions for signing in to the AWS Management Console.
View user
Search IAM
Dashboard
Access management
User groups
Users
Roles
Policies
Identity providers
IAM > Users
Users (1) Info
An IAM user is an identity with long-term credentials that is used to interact with AWS in an account.
Delete
Create user
Search
User name
Path
Group
Last activity
MFA
Password age
Console last sign-in
Access key ID
Active key age
Ruchika
/
0

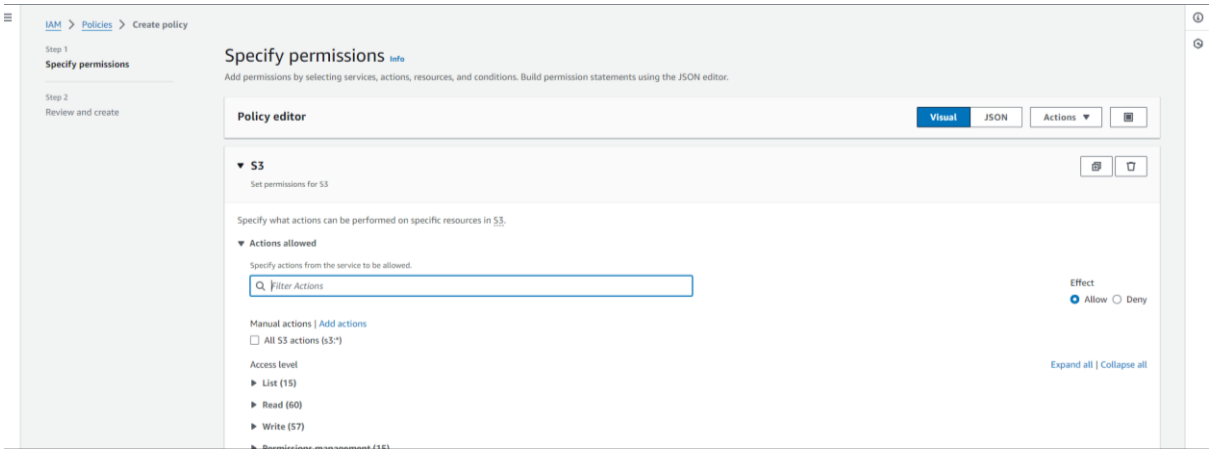

Enable console access
Enable console access for Ruchika.
Console password
Autogenerated password
Custom password
User must create new password at next sign-in
Users automatically get the IAMUserChangePassword policy to allow them to change their own password.
Cancel
Enable console access

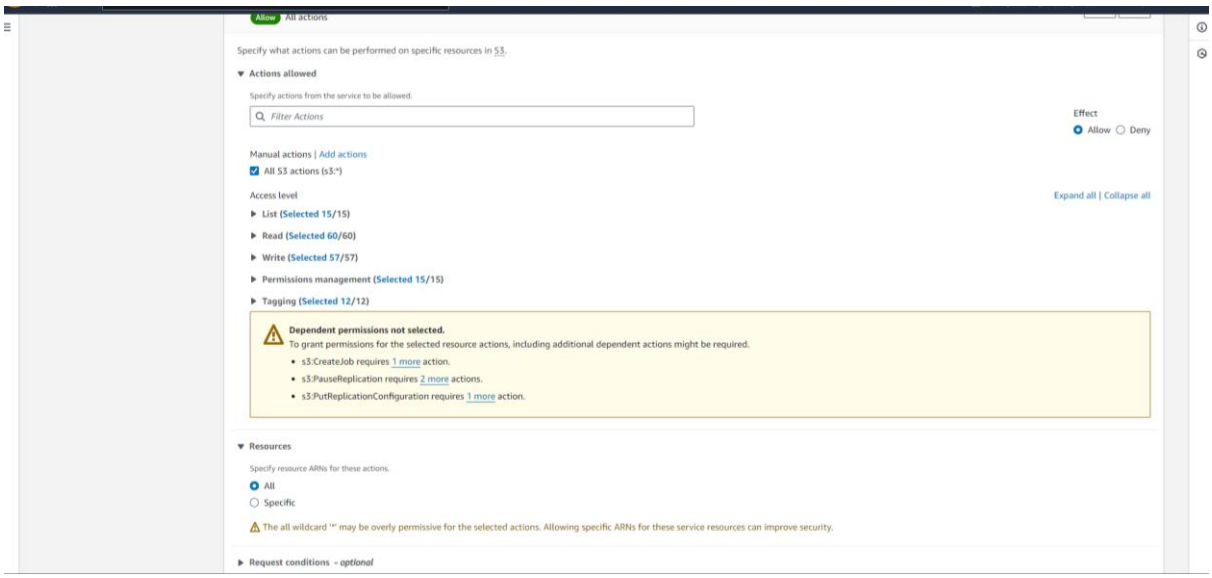

Console password
You have successfully enabled the user's new password.
This is the only time you can view this password. After you close this window, if the password is lost, you must create a new one.
Console sign-in URL
https://339712834917.signin.aws.amazon.com/console
User name
Ruchika
Console password
Ro#Z9&]5 Hide
Download .csv file
Close

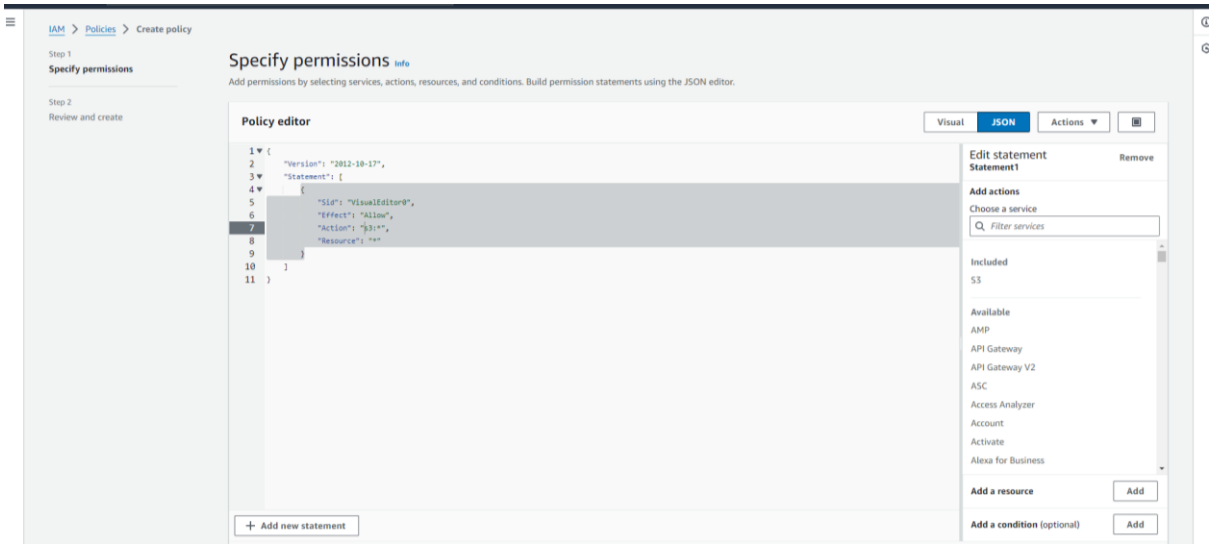

Console Home
Reset to default layout
Add widgets
Recently visited
No recently visited services
Explore one of these commonly visited AWS services.
EC2 S3 RDS Lambda
View all services
Applications (0)
Create application
Region: Europe (Stockholm)
eu-north-1 (Current Region)
Find applications
Name
Description
Region
Originating account
Access denied
Go to myApplications
Welcome to AWS
Getting started with AWS
Learn the fundamentals and find valuable information to get the most out of AWS.
Training and certification
AWS Health
No health data
Cost and usage
Current month costs
Access denied
Cost breakdown
Access denied
Forecasted month end costs
Access denied
Savings opportunities
Access denied

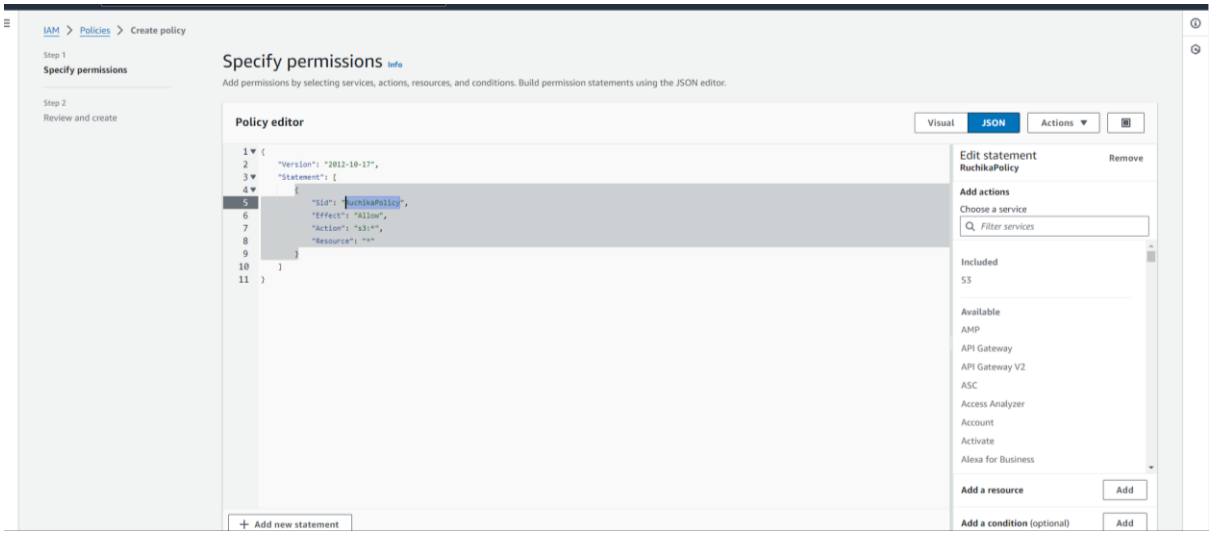

Identity and Access Management (IAM)
Search IAM
Dashboard
Access management
User groups
Users
Roles
Policies
Identity providers
Account settings
IAM > Policies
Policies (1221)
A policy is an object in AWS that defines permissions.
Actions
Delete
Create policy
Filter by Type
Search
All types
Policy name
Type
Used as
Description
AccessAnalyzerServiceRolePolicy
AWS managed
None
AdministratorAccess
AWS managed - job function
None
Provides full access to AWS services an...
AdministratorAccess-Amplify
AWS managed
None
Grants account administrative permiss...
AdministratorAccess-AWSElasticBeanstalk
AWS managed
None
Grants account administrative permiss...

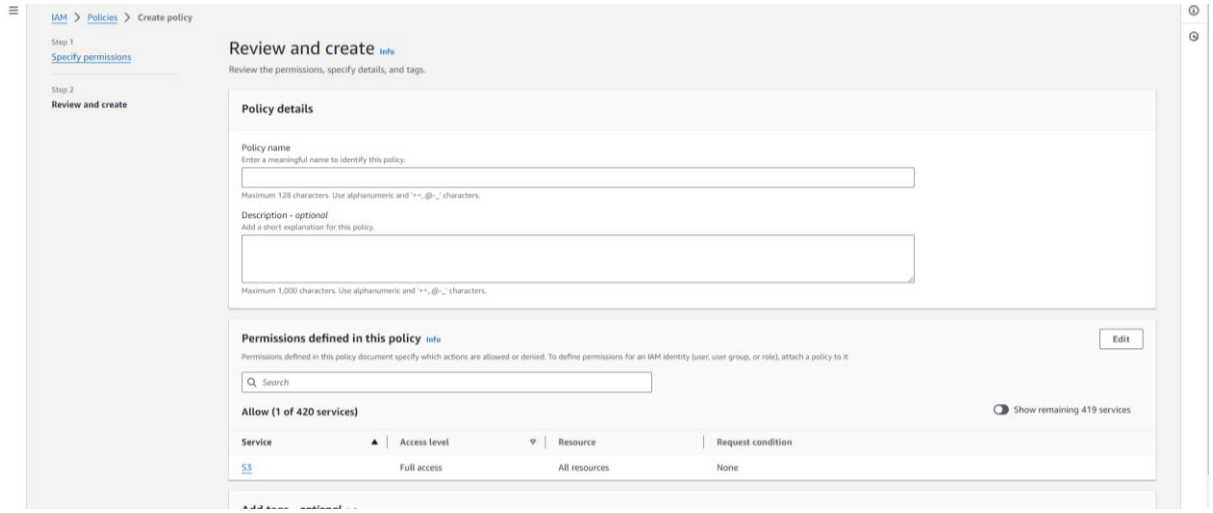

Identity and Access Management (IAM)
Search IAM
Dashboard
Access management
User groups
Users
Roles
Policies
Identity providers
Account settings
Access reports
Access Analyzer
External access
Unused access
IAM > Users > Ruchika
Ruchika Info
Delete
Summary
ARN
arn:aws:iam::339712834917:user/Ruchika
Console access
Disabled
Access key 1
Create access key
Created
August 03, 2024, 16:32 (UTC+05:30)
Last console sign-in
-
Permissions
Groups
Tags
Security credentials
Access Advisor
Console sign-in
Enable console access
Console sign-in link
https://339712834917.signin.aws.amazon.com/console
Console password
Not enabled

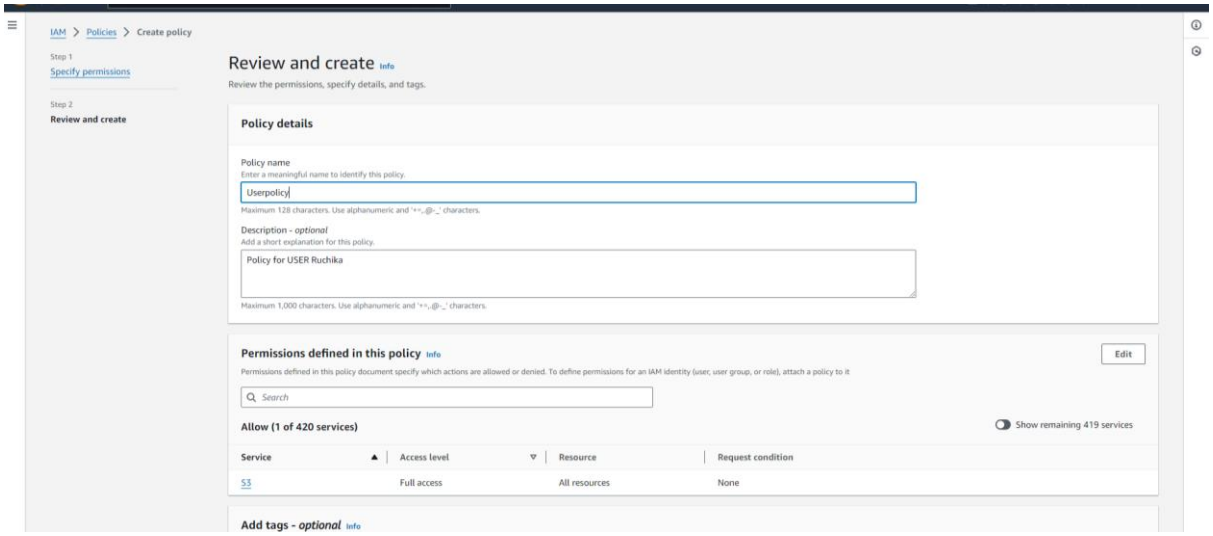

IAM > Policies > Create policy
Step 1
Specify permissions
Step 2
Review and create
Specify permissions Info
Add permissions by selecting services, actions, resources, and conditions. Build permission statements using the JSON editor.
Policy editor
Visual
JSON
Actions
S3
Set permissions for S3
Specify what actions can be performed on specific resources in S3.
Actions allowed
Specify actions from the service to be allowed.
Filter Actions
Effect
Allow
Deny
Manual actions | Add actions
All S3 actions (s3:*)
Access level
Expand all | Collapse all
List (15)
Read (60)
Write (57)

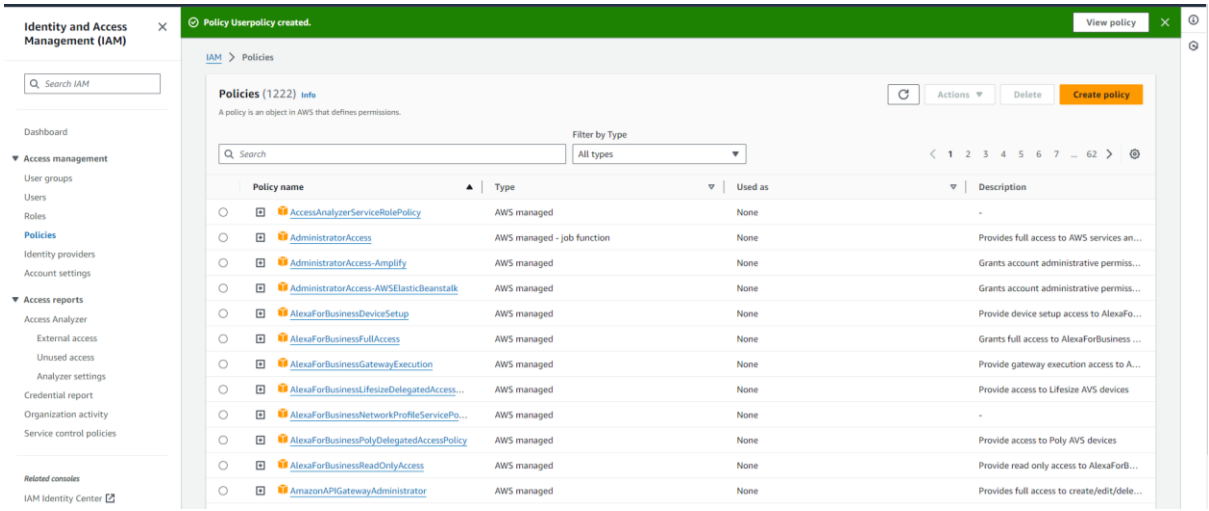

Allow All actions
Specify what actions can be performed on specific resources in S3.
Actions allowed
Specify actions from the service to be allowed.
Filter Actions
Effect
Allow
Deny
Manual actions | Add actions
All S3 actions (s3:*)
Access level
Expand all | Collapse all
List (Selected 15/15)
Read (Selected 60/60)
Write (Selected 57/57)
Permissions management (Selected 15/15)
Tagging (Selected 12/12)
Dependent permissions not selected.
To grant permissions for the selected resource actions, including additional dependent actions might be required.
s3:CreateJob requires 1 more action.
s3:PauseReplication requires 2 more actions.
s3:PutReplicationConfiguration requires 1 more action.
Resources
Specify resource ARNs for these actions.
All
Specific
The all wildcard '*' may be overly permissive for the selected actions. Allowing specific ARNs for these service resources can improve security.
Request conditions - optional

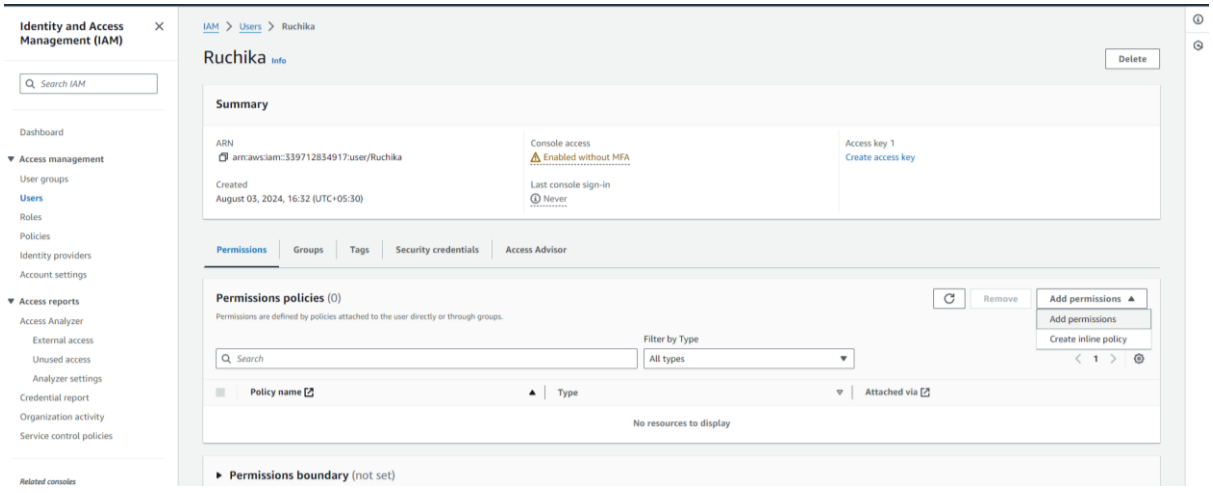

IAM > Policies > Create policy
Step 1
Specify permissions
Step 2
Review and create
Specify permissions Info
Add permissions by selecting services, actions, resources, and conditions. Build permission statements using the JSON editor.
Policy editor
Visual
JSON
Actions
{
"Version": "2012-10-17",
"Statement": [
{
"Sid": "VisualEditor0",
"Effect": "Allow",
"Action": "s3:*",
"Resource": "*"
}
]
}
Edit statement
Statement1
Remove
Add actions
Choose a service
Filter services
Included
S3
Available
AMP
API Gateway
API Gateway V2
ASC
Access Analyzer
Account
Activate
Alexa for Business
Add a resource
Add
Add a condition (optional)
Add
Add new statement

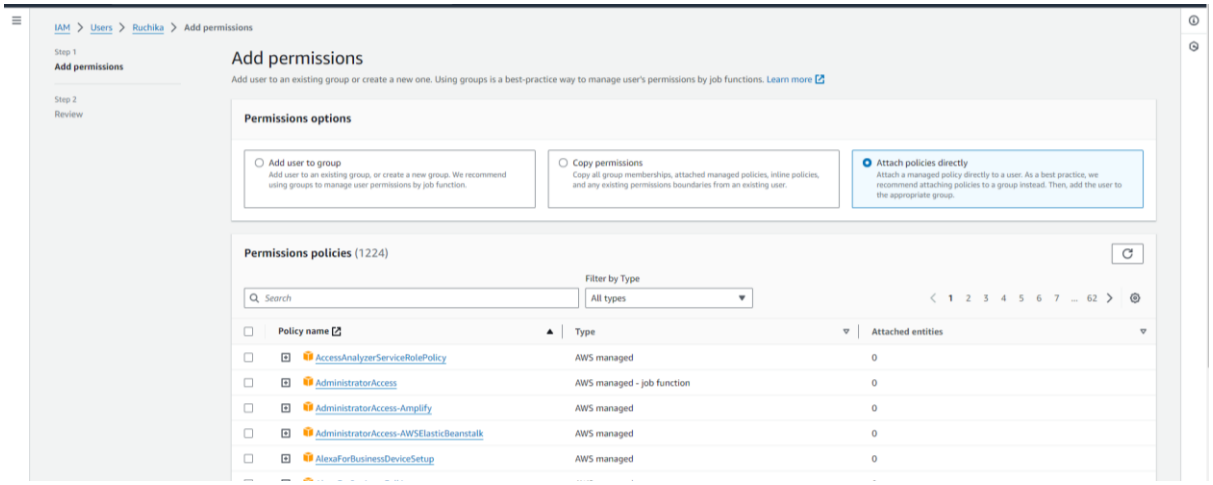

IAM > Policies > Create policy
Step 1
Specify permissions
Step 2
Review and create
Specify permissions Info
Add permissions by selecting services, actions, resources, and conditions. Build permission statements using the JSON editor.
Policy editor
Visual
JSON
Actions
{
"Version": "2012-10-17",
"Statement": [
{
"Sid": "RuchikaPolicy",
"Effect": "Allow",
"Action": "s3:*",
"Resource": "*"
}
]
}
Edit statement
RuchikaPolicy
Remove
Add actions
Choose a service
Filter services
Included
S3
Available
AMP
API Gateway
API Gateway V2
ASC
Access Analyzer
Account
Activate
Alexa for Business
Add a resource
Add
Add a condition (optional)
Add
Add new statement

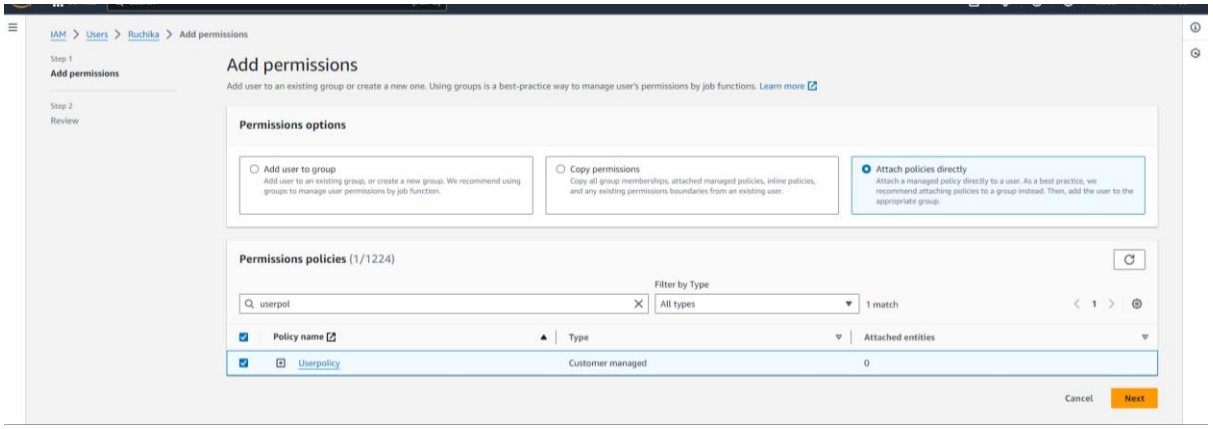

IAM > Policies > Create policy
Step 1
Specify permissions
Step 2
Review and create
Review and create Info
Review the permissions, specify details, and tags.
Policy details
Policy name
Enter a meaningful name to identify this policy.
Maximum 128 characters. Use alphanumeric and '+=,.@-_' characters.
Description - optional
Add a short explanation for this policy.
Maximum 1,000 characters. Use alphanumeric and '+=,.@-_' characters.
Permissions defined in this policy Info
Edit
Permissions defined in this policy document specify which actions are allowed or denied. To define permissions for an IAM identity (user, user group, or role), attach a policy to it
Search
Allow (1 of 420 services)
Show remaining 419 services
Service
Access level
Resource
Request condition
S3
Full access
All resources
None

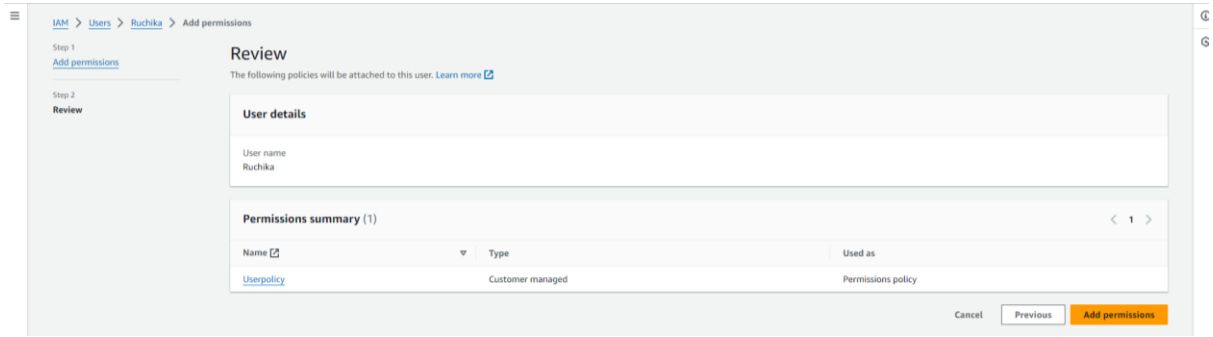

IAM > Policies > Create policy
Step 1
Specify permissions
Step 2
Review and create
Review and create Info
Review the permissions, specify details, and tags.
Policy details
Policy name
Enter a meaningful name to identify this policy.
Userpolicy
Maximum 128 characters. Use alphanumeric and '+=,.@-_' characters.
Description - optional
Add a short explanation for this policy.
Policy for USER Ruchika
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 420 services)
Show remaining 419 services
Service
Access level
Resource
Request condition
S3
Full access
All resources
None
Add tags - optional Info

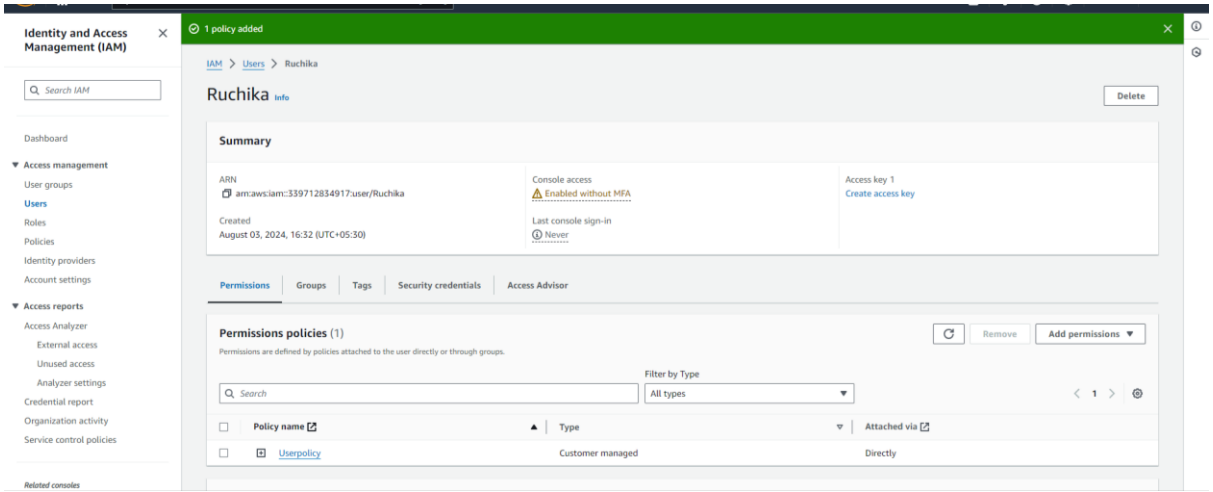

Identity and Access Management (IAM)
Search IAM
Dashboard
Access management
User groups
Users
Roles
Policies
Identity providers
Account settings
Access reports
Access Analyzer
External access
Unused access
Analyzer settings
Credential report
Organization activity
Service control policies
Related consoles
IAM Identity Center
Policy Userpolicy created.
View policy
IAM > Policies
Policies (1222) Info
A policy is an object in AWS that defines permissions.
Actions
Delete
Create policy
Search
Filter by Type
All types
1 2 3 4 5 6 7 ... 62
Policy name
Type
Used as
Description
AccessAnalyzerServiceRolePolicy
AWS managed
None
AdministratorAccess
AWS managed - job function
None
Provides full access to AWS services an...
AdministratorAccess-Amplify
AWS managed
None
Grants account administrative permiss...
AdministratorAccess-AWSElasticBeanstalk
AWS managed
None
Grants account administrative permiss...
AlexaForBusinessDeviceSetup
AWS managed
None
Provide device setup access to AlexaFo...
AlexaForBusinessFullAccess
AWS managed
None
Grants full access to AlexaForBusiness ...
AlexaForBusinessGatewayExecution
AWS managed
None
Provide gateway execution access to A...
AlexaForBusinessLifesizeDelegatedAccess...
AWS managed
None
Provide access to Lifesize AVS devices
AlexaForBusinessNetworkProfileServicePo...
AWS managed
None
AlexaForBusinessPolyDelegatedAccessPolicy
AWS managed
None
Provide access to Poly AVS devices
AlexaForBusinessReadOnlyAccess
AWS managed
None
Provide read only access to AlexaForB...
AmazonAPIGatewayAdministrator
AWS managed
None
Provides full access to create/edit/dele...


Identity and Access Management (IAM)
Search IAM
Dashboard
Access management
User groups
Users
Roles
Policies
Identity providers
Account settings
Access reports
Access Analyzer
External access
Unused access
Analyzer settings
Credential report
Organization activity
Service control policies
Related consoles
IAM > Users > Ruchika
Ruchika Info
Delete
Summary
ARN
arn:aws:iam::339712834917:user/Ruchika
Console access
Enabled without MFA
Access key 1
Create access key
Created
August 03, 2024, 16:32 (UTC+05:30)
Last console sign-in
Never
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
Add permissions
Create inline policy
Filter by Type
Search
All types
1
Policy name
Type
Attached via
No resources to display
Permissions boundary (not set)


IAM > Users > Ruchika > 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 (1224)
Filter by Type
Search
All types
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
AlexaForBusinessDeviceSetup
AWS managed
0


IAM > Users > Ruchika > 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 (1/1224)
Filter by Type
userpol
All types
1 match
Policy name
Type
Attached entities
Userpolicy
Customer managed
0
Cancel
Next


IAM > Users > Ruchika > Add permissions
Step 1
Add permissions
Step 2
Review
Review
The following policies will be attached to this user. Learn more
User details
User name
Ruchika
Permissions summary (1)
Name
Type
Used as
Userpolicy
Customer managed
Permissions policy
Cancel
Previous
Add permissions


Identity and Access Management (IAM)
Search IAM
Dashboard
Access management
User groups
Users
Roles
Policies
Identity providers
Account settings
Access reports
Access Analyzer
External access
Unused access
Analyzer settings
Credential report
Organization activity
Service control policies
Related consoles
1 policy added
IAM > Users > Ruchika
Ruchika Info
Delete
Summary
ARN
arn:aws:iam::339712834917:user/Ruchika
Console access
Enabled without MFA
Access key 1
Create access key
Created
August 03, 2024, 16:32 (UTC+05:30)
Last console sign-in
Never
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
Filter by Type
Search
All types
Policy name
Type
Attached via
Userpolicy
Customer managed
Directly

Policy changed !!